Edge Hill University

Department of Computer Science

A multi-tier trust-based management system for vehicle ad-hoc network communication

A thesis submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy

Supervisory Team:
Professor Nik Bessis
Doctor Hassan Malik
Doctor Sarah Mchale

Brian Okoyo Akwirry

Edge Hill University, UK,

3rd January 2023

Acknowledgements

I sincerely appreciate my primary supervisor, Professor Nik Bessis, who provided tremendous assistance and direction throughout the study. Your encouragement, assistance, mentorship, and autonomy in the study gave me immense confidence and learning throughout the study. I would also like to express how grateful I am to my second supervisor, Dr. Hassan Malik, for his continuous support during the study. Your guidance, intelligent discussions, and striving for excellence in my work motivated me and helped me improve my understanding of the research process. I would also like to appreciate my third supervisor, Dr. Sarah McHale, who provided incessant support during the study. I further want to thank Professor Ella Pereira for her support during the study and the enabling atmosphere. This enabled me to perform effectively throughout the study. I want to thank my colleagues with whom I have shared several thoughtful conversations on various topics over the years. In many ways, these discussions contributed to improving my research comprehension. I would further like to express my gratitude to my mother, Stella Ondimu, for their encouragement and support throughout the study. This includes her constant backing and reassurance.

It is with immense gratitude that I would like to collectively thank everyone that has been a part of this journey; it would not have been possible without the participation of each of you. Thank you all, and I appreciate you.

Abstract

Vehicle ad-hoc networks (VANETs) are a particular type of mobile ad-hoc networks (MANETs) that enable vehicles to communicate in modern road environments. By enabling communication, VANETs can provide real-time information such as traffic congestion warnings, safety messages, lane change information and infotainment. VANETs lead to optimized traffic conditions, increased road safety and improved driving conditions for road users.

Accurate and timely delivery of messages is crucial due to the importance of messages transmitted. Therefore, securing communications in VANETs is crucial for operations. Messages exchanged in VANET communications contain critical information such as road safety or road accident information. These packets must reach their intended destination without modification. VANET communications are concerned that malicious vehicles can intercept or modify messages before reaching their intended destination. Malicious behaviour can hamper VANET operations and create safety concerns.

This research proposes a multi-tier trust management system based on vehicle behaviour for the detection of malicious vehicles and to improve communication within VANET. It includes investigating VANETs while highlighting vehicle behaviour metrics. The metrics include packet delivery ratio (PDR), processing delay, forwarding rate (FR), initial and residual energy, and operational history of a vehicle. The first tier of the proposed system assigns vehicles in the VANET a trust value based on behaviour such as processing delay, packet loss and prior vehicle behavioural history. To achieve this, a set of vehicles is selected as watchdogs and observes neighbouring vehicles' behaviour. Watchdogs send this data to the roadside unit (RSU), which calculates trust values to represent vehicle behaviour. The second tier protects against malicious watchdogs in the VANET. Watchdog behaviour history identifies malicious and non-malicious watchdogs. The third security tier protects trust value calculation data. A secure watchdog selection process is proposed to enhance system robustness. This watchdog selection scheme considers vehicle behaviour and fairness while selecting watchdogs. In order to improve accuracy, the proposed system includes intelligence to identify false positives caused by network errors and malicious vehicles that recover from malicious behaviour.

Based on simulations, the developed system successfully identifies and isolates malicious vehicles in the VANET. The designed system improves the VANET packet delivery rate and reduces packet delivery delay. The proposed system's accuracy is evaluated by its ability to identify false positives and vehicles recovered from malicious behaviour. The suggested watchdog selection process successfully selects secure and fair watchdogs, improving system robustness. The proposed system enhances VANET communications. In future applications, the developed system can be applied to intelligent city environments by enabling efficient and safe transportation. Consequently improving the quality of life for its citizens.

Table of Contents

List of figures

List of tables

List of acronyms

Acronym	Details
CCM	Central control module
DDOS	Distributed denial-of-service
DSRC	Dedicated short-range communication
DOS	Denial-of-service
FR	Forwarding rate
IDS	Intrusion detection system
ITS	Intelligent transport system
IVC	Inter-vehicle communication
MANET	Mobile ad-hoc network
OBU	On-board unit
PDR	Packet delivery ratio
RREP	Route reply message
RREQ	Route request message
RSU	Road side unit
TA	Trusted Authority
VANET	Vehicle ad-hoc network
V2E	Vehicle-to-everything
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-vehicle
VRU	Vulnerable road user
WAVE	Wireless access in vehicle environment
WSN	Wireless sensor network

Publication

1. B. Akwirry, N. Bessis, H. Malik, and S. McHale, “A Multi-Tier Trust-Based Security Mechanism for Vehicular Ad-Hoc Network Communications,” Sensors, vol. 22, no. 21, p. 8285, Oct. 2022 [1].

1. Introduction

1.1. Overview

This section provides a general overview of this thesis document's contents. This introduction will contain the study background, providing a high-level discussion of Vehicular Ad-hoc Networks (VANETs). The motivation section will describe the fundamental reasons for the research. The aims and objectives answer the research questions presented. The research questions provide some succinct statements of the study's expectations. Furthermore, the contributions section presents the innovations created in this research. Chapter two will review related professional research on VANETs and the latest technologies used in VANETS. The chapter includes vulnerabilities and attacks against VANETs. The chapter discusses VANET security requirements. Chapter 3 will contain the methods used in investigating the problem and the methodology used in developing the solution to the research questions. The security solution developed comprises three modules outlined in chapters 4, 5 and 6. Chapter 4 discusses the main components of a multi-tier trust-based security system. Testing for false positives and recovering malicious vehicles is outlined in Chapter 5. Chapter 6 discusses the process of selecting watchdogs that consider fairness and vehicle history. Chapter 7 presents the research conclusion and implications.

1.2. Background

As wireless communication technology and network systems constantly evolve and progress towards a better state, VANETs have gained considerable interest from researchers, automobile manufacturers and government institutions [2], [3]. VANETs are a particular type of MANET which enables communication on roads in urban environments [2], [4]. The vehicles that belong to the same VANET can communicate with one another and with the infrastructure within its range of communication. VANETs have become increasingly significant in building intelligent cities and intelligent transportation systems (ITS) [3]. The importance of VANETs lies in providing real-time information such as traffic congestion warnings, safety messages, lane change information and infotainment [2]–[4]. Information sharing leads to optimized traffic conditions, increased road safety and improved driving conditions for road users [5]. This reduces the risk of injury and death on the roads and increases drivers and passengers' comfort. Accuracy and timely delivery of messages are crucial to reap VANET benefits [6]. A delay or drop in messages in the VANET can have dangerous consequences for all road users. Interruption of information transfer in VANETs may cause accidents on the road, resulting in injuries and deaths. VANETs have enabled Vehicle-to-Vehicle (V2V) communication and cooperation and have also been utilized in Vehicle-to-Infrastructure (V2I) contact [7]. V2V and V2I communication are vehicles' primary modes of communication, a VANET [8], [9]. Vehicle communication is made possible by the On-Board Unit (OBU) installed in most modern vehicles [10]. The OBU contains GPS, wireless communication, central control (CCM), and human-machine interface modules [11]. V2I communication is made possible by deploying Road Side Units (RSU) along roads or intersections [12]. V2I communication, in some cases, also involves communication with Trusted Authorities (TA) deployed along the road. TAs are a trusted third party deployed in VANETs equipped with networking features and computing power to manage the VANET [12]. Vehicles in the VANET communicate with other vehicles or RSUs by

dedicated short-range communication (DSRC) on a single-hop or multi-hop basis [4], [11].

One of the critical challenges facing implementing VANETS is providing secure vehicle communication [13]. The characteristics of VANET, which include rapidly changing connections, make communications susceptible to malicious attackers. Attacks on VANETs present a dangerous situation for VANETs due to the nature of the information exchanged. The information exchanged in VANETs involves critical information. Therefore, an attack-free and trusted environment increases the reliability of information transfer in the VANET [8]. Messages transmitted in the VANET require protection from modification or insertion by malicious entities. Availability, integrity, confidentiality, authentication, non-repudiation, and traceability are security requirements for VANET communication [4], [11], [14]. Security systems built for VANETs have to adhere to these security requirements. The high mobility, rapidly changing network topology, limited transmission power, volatility in network connections and boundless network size present a challenge for VANETs to achieve their security requirements [15], [16]. These security aspects require developing unique security mechanisms to achieve them.

Attacks in a VANET disrupt the normal working of the network and lead to disruptions in the VANET. These disruptions are a concern because information exchange in the VANET can save lives. Attacks in the VANET are performed by either an insider or an outsider in the network [17]. Insider vehicles in the network are authorised network members and can communicate with other vehicles [15]. In contrast, outsider vehicles do not have direct access to the network and cannot communicate with members of the VANET [15]. Since outsiders have limited access, they also have a limited capacity to attack the network; insider attacks are considered more dangerous. Some of the attacks performed on VANETs include Sybil attack, Denial-of-Service attack (DOS), Distributed Denial-of-service attack (DDOS), Blackhole attack, Wormhole attack, Message suppression attack, Message Alteration attack, Replay attack, Sybil attack, Timing attack, Man-in-the-middle attack and Eavesdropping attack [15]–[19]. These attacks decrease the vehicles' ability to deliver messages in the VANET.

Developing security mechanisms for VANETs reduces the effect of malicious attacks. Developing an optimized, secure scheme for VANETs requires some objectives to be fulfilled. These objectives include: minimization of computational and communication overhead, utilization of bandwidth, scalability, timely response and must have good capability to stop attacks [16]. Security mechanisms developed try to achieve all the security requirements, although this presents a challenge in some cases.

Cryptography and key management techniques are proposed to deal with malicious attacks in VANETs [20]–[22]. Cryptography is based on key management and involves using public, private, or shared group keys to encrypt data and avoid malicious vehicles [23]. Messages sent in the VANET are encrypted at the source using keys and decrypted at the destination using keys. However, because of the highly dynamic nature of VANET, the distribution, management and storage of keys become highly complex [20]. Increasing the number of vehicles also increases the number of compilations performed, increasing the complexity [23]. Cryptography solutions have also been ineffective against security-related problems, such as fake messages and dishonest users [24]. Another challenge cryptographic solutions face is the inability to

deal with insider attacks [25]. Therefore, cryptography and key management techniques are not the most efficient security mechanisms for VANET communication.

Trust management as a security mechanism can deal with security threats in VANETs but must be optimised to perform effectively. A trust model allows a vehicle to evaluate another vehicle's behaviour and detect malicious vehicles or false data [26]. A trust model should be able to verify whether the message's sender is legitimate and trustworthy and whether the message's contents are trustworthy [24]. By doing this, a trust model should be able to improve the security of the VANET. Evaluation of vehicles makes use of various aspects, including neighbour recommendations, interactions with other vehicles, previous dealings in the network, FR/PDR and consistency factors [25], [27], [28]. The VANET and security management system's application highly influence attribute selection. Trust management in VANETS comprises three main categories: Entity-centric, data-centric, and combined trust models [29]. Trust models use various techniques to monitor a vehicle and evaluate its behaviour. Entity-centric trust models focus on evaluating the trustworthiness of the vehicle itself. Data-centric trust models' primary focus is the trustworthiness of received data. Combined trust models evaluate the trust level of vehicles and the data's trustworthiness.

Evaluating the behaviour of a vehicle in the VANET requires monitoring vehicles and their transactions in the VANET. Security management systems, including trust management systems and intrusion detection systems (IDS), use a watchdog technique to perform monitoring tasks. The watchdog technique involves installing a watchdog agent, which enables the monitoring neighbour transactions in the VANET [30]. Although the watchdog technique effectively monitors vehicles, particular challenges must be considered during design. The first challenge exists in selecting secure watchdogs [31]. Watchdogs monitor other vehicles; therefore, a malicious watchdog would render the security management system ineffective. The other challenge within the watchdog mechanism is resource consumption [32], [33]. The watchdogs consume higher computational and storage costs to perform monitoring tasks in the VANET. Computational and storage costs are even higher if the watchdog has to perform the computations and evaluate vehicles to determine malicious and non-malicious behaviour. Implementing the watchdog technique in security management systems requires addressing the challenges mentioned. The occurrence of false positives is a phenomenon that is crucial in designing security management systems. False positives occur when the behaviour of vehicles results in identification as malicious, yet its normal behaviour [34]. False positives can occur due to network errors causing collisions or causing incorrect data collection by the watchdogs. False positives can also occur in a defamation attack. A defamation attack is where a vehicle will report a vehicle as malicious, yet the vehicle is exhibiting normal behaviour [35]. False positives cause a loss of accuracy in detecting and evaluating vehicle behaviour in the VANET. False positives also have the disadvantage of reducing the efficiency of the security management system. False identification has to be considered by security management systems during design.

1.3. Motivation

Registered vehicles worldwide will increase to about 2 billion within 10 to 20 years [29]. VANETs work as a foundation of ITSs and smart cities to improve transportation efficiency and ensure the safety of vehicles and pedestrians [27]. Accidents occur when a driver cannot identify their surroundings [28]. Furthermore, with increased traffic, people get stuck in traffic jams and waste valuable time sitting on the road. An ITS can address both of these challenges. The importance of VANETS cannot be understated.

Unfortunately, due to the highly dynamic topology nature and other unique characteristics of VANETS, malicious vehicles can easily embed themselves in the VANET [29], [36]. Once embedded in the VANET, malicious vehicles can quickly disseminate false messages or modify or drop messages in the network before reaching their intended destination. These disruptions to information exchange could reduce transportation efficiency and, in the worst-case scenario, lead to injuries and threaten human life [29]. Therefore, VANETs cannot work efficiently in the presence of malicious vehicles. Security from malicious vehicles is challenging to accomplish in VANETs [37]. Hence why securing VANETs has become a prevalent research field recently.

While VANETs present a unique challenge for identifying malicious activity, researchers have made progress in addressing these challenges. Certificate and signature methods have been used to verify the authenticity of vehicles and messages [38]. Cryptography secure systems for VANETs are used to deal with external attackers in the VANET [25], [27]. Trust management systems have been introduced to enhance the security of VANETs by facilitating the dissemination of reliable and trusted data in the network [39].

Trust management is effective against internal attackers if executed correctly [40]. Trustworthiness is essential, particularly in the autonomous driving context, as cooperation between vehicles is significant [41]. They enable vehicles to choose reliable vehicles to cooperate within the network and avoid malicious vehicles using minimal information [42]. Trust management must use minimal information as vehicles in a VANET may not spend enough time to create a long steady relationship [26]. Despite the success of trust management-based systems, not many trust management systems for VANETs have been proposed [38]. There is a lack of schemes that fulfil the requirements for VANETs [43].

Based on the above discussion, it is evident that there is a massive advantage to applying a trust management-based system to a VANET. This motivated designing the multi-tier trust-based security management system described in this thesis. This research focused on designing a multi-tier trust-based management system that required minimal information for security in the VANET. The proposed system assigned vehicles with a trust value distinguishing between non-malicious and malicious vehicles in the VANET. The proposed system selected the most trusted vehicles in the VANET as watchdogs. Watchdogs monitored message exchange between vehicles and collected data to evaluate the vehicle. Watchdogs monitored the PDR and processing delay of the neighbour vehicles. They then sent this information to a trusted authority (TA). The TA in the VANET calculated trust values for vehicles

based on data sent by watchdogs and the previous trust value of the vehicles. The TA was also responsible for managing the trust and sending it to the respective vehicles in the VANET.

A scenario where the proposed system would be beneficial is shown in Figure 1.1. Vehicle V1 detects a road hazard on the road ahead and broadcasts it across the VANET. This transmission is received by V2 and V3, which are one-hop neighbours. However, both V2 and V3 are malicious. V2, instead of forwarding messages to V5, drops the message. On the other hand, V3 delays the message before forwarding it to V5. As a result, V5 misses the road alert, potentially creating a dangerous situation for the driver. The proposed trust management system will identify malicious vehicles, thus increasing VANET communication efficiency.

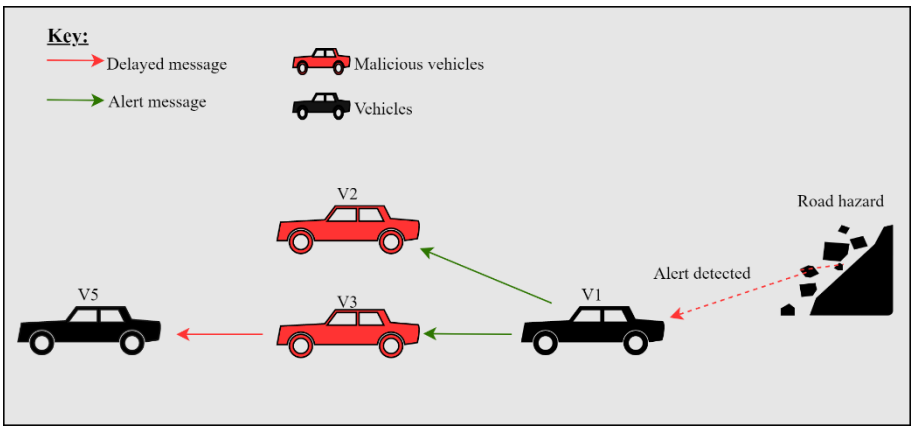

Figure 1.1 - Scenario diagram showing malicious vehicles in a VANET.

1.4. Research questions

This section discusses the research questions answered in this work.

- **Main research question:** Can a multi-tier robust trust management system be designed that will make use of multiple watchdogs, guarantee the identification of malicious vehicles, protection from malicious watchdogs, and guarantee the integrity of trust value. At the same time, it protects against false positives in the VANET.

This primary research question resulted in a smaller set of questions developed. These are presented below.

1. Can message exchange between vehicles give rise to characteristics or attributes used to identify behaviour in vehicles and determine malicious and non-malicious vehicles in the VANET?

2. What is the optimal set of vehicle characteristics to identify vehicle behaviour in the VANET while maintaining efficiency and robustness?

3. Can a trust management system include a watchdog mechanism that provides both secure watchdog selection and fairness in the selection process? A secure

and fair watchdog mechanism will improve the accuracy and efficiency of the trust management system.

4. Can federation be included in the trust management system so tasks are distributed in the VANET to increase efficiency?

5. Can a multi-tier trust management system be resilient in the presence of multiple malicious vehicles in the VANET to provide security and achieve its objective function?

6. Can the trust management system be durable to protect against malicious watchdogs in the VANET that may provide false information?

7. Can a trust management system provide integrity to the trust calculation process to ensure the accuracy of results in determining malicious and non-malicious behaviour in the VANET?

8. Can a trust management system be robust to identify false positives and protect against false positives so that they do not reduce the accuracy of the results?

In order to provide answers to the questions above and hence answer the main research question, specific objectives and aims were developed. These aims and objectives are discussed below.

1.5. Aims and objectives

This section will discuss the aim and objectives of the research conducted. The main aim of the research is listed below:

- Design, develop and test a multi-tier trust-based security management system for VANET communications. The proposed system will provide security in the VANET using three security tiers. The first tier of the proposed system assigns vehicles in the VANET a trust value based on behaviour such as processing delay, packet loss and prior vehicle behavioural history. Vehicles selected as watchdogs perform evaluation tasks in the VANET to observe the behaviour of neighbouring vehicles and collect data. The second tier is to protect the watchdogs, which is done by watchdogs' behaviour history. The third security tier is to protect the integrity of data used for trust value calculation. The trust management system will include a watchdog selection system to ensure secure watchdog selection and fairness in the selection process. The secure watchdog selection will ensure the trust management system will resist malicious watchdogs and vehicles. The trust management system should protect against false positives in the VANET. Finally, the trust management system should not interfere with standard data transmission in the VANET.

The following objectives will be necessary to achieve the above aim:

1. An in-depth critical review of the research area to identify a theoretical framework that defines the area of research interest – This was achieved by a review of the architecture of VANETs, and technologies used in VANETs. A review of attacks and their effects against VANETs. It also reviewed the

security systems developed against these attacks to identify gaps in the research.

2. Data collection from relevant sources to identify the different aspects applicable in the design of the trust management system and scenarios to test the system – This identified the techniques used in security management systems applied to VANETs and enabled the development of modules used in developing the trust management system. This objective also identified development tools needed in creating the proposed system. The data collected also facilitated the design of complex scenarios that evaluated the proposed trust management system.

3. Design and develop the set of algorithms and equations that calculates and performs security management in the VANET – These identified attributes in vehicle communication define trust in a vehicle. These attribute values calculated a composite trust value representing a vehicle's malicious or non-malicious behaviour. The objective also included the algorithms that identified false positives and recuperated malicious vehicles in the VANET.

4. Design and develop the watchdog system and TA system applied to the RSU – This featured designing the secure and fair selection system used to select watchdogs in the VANET—development of the watchdog agent, which, when applied to vehicles, enabled them to monitor their neighbours' communications. The design of the agent applied to the RSU enabled the RSU to undertake the responsibility of a TA. The agent also enabled the RSU to manage the trust values of vehicles present in the VANET.

5. Develop a working prototype of the multi-tier trust-based management system and evaluate it in different replicable scenarios to test effectiveness – This featured combining the elements designed in objectives 3 and 4 into a complete system working synchrony. The complete system was applied to a VANET populated with malicious vehicles to test effectiveness in different scenarios. Results were generated and presented from the various experiments performed.

1.6. Thesis contributions

This thesis made the following contributions:

1. Trust model for VANET communications

This contribution includes identifying the optimal vehicle characteristics and attributes representing vehicle behaviour in the VANET. In addition, equations to convert the characteristics into quantifiable values. Development of the algorithm that intelligently combines these values to form a composite value representing a vehicle's behaviour.

2. Framework for watchdog selection and maintenance

The framework enables the selection of secure and reliable vehicles as watchdogs, ensuring malicious vehicles are not selected as watchdogs in the VANET. The

framework also includes the watchdog agent that enables vehicles to work as watchdogs to monitor and collect statistics on neighbour vehicles. The watchdogs will send this data to the RSU to calculate trust values.

3. Framework for RSU agent

This agent will be installed on the RSU and will enable the application of equations and algorithms to evaluate the trust values of vehicles. The RSU agent will also create a trust ledger to store the vehicles' trust values. Furthermore, the RSU is responsible for storing a trust history for vehicles in the VANET; this includes trust value for vehicles from previous communication rounds. This history can be requested and used on a need-to basis.

4. Framework for false positive detection and recuperating of malicious vehicles

This framework will detect vehicles falsely accused as malicious yet exhibiting non-malicious behaviour through network errors or defamation attacks on vehicles. In addition, this framework will identify vehicles that behave maliciously but recover to non-malicious behaviour during VANET operations. Identifying this behaviour improves the accuracy of the system.

5. Prototype framework and Source code

This contribution features the framework and source code for creating the multi-tier trust-based security management system. The different elements are combined for synchronous performance to achieve the objective function of security management in the VANET. The prototype and source code can aid future research and improvements in the security of VANET communications.

6. Experimental summary and results

Specific metrics evaluate the proposed system to generate results. These will be the results and summary of the experiments and simulations conducted. The results provide room for future research and improvement on the proposed system. Industries can use the results to improve security in manufacturing vehicle communication systems.

Table 1.1 below shows the relationship between the research questions, objectives, and project contributions. It shows how the research questions formulated the objectives and, eventually, the contributions.

Table 1.1 - Relationship between research questions, objectives, and contribution used in this work.

Research question	Objective	Contribution
Can message exchange between vehicles give rise to characteristics or attributes used to identify behaviour in vehicles and determine malicious and non-malicious vehicles in the VANET?	An in-depth critical review of the research area to identify a theoretical framework that defines the area of research interest – This was achieved by a review of the architecture of VANETs, and technologies used in VANETs. A review of attacks and their effects against VANETs. It also reviewed the security	Trust model for VANET communications.

	systems developed against these attacks to identify gaps in the research.	
What is the optimal set of vehicle characteristics to identify vehicle behaviour in the VANET while maintaining efficiency and robustness? Can a trust management system provide integrity to the trust calculation process to ensure the accuracy of results in determining malicious and non-malicious behaviour in the VANET? Can a trust management system be robust enough to identify false positives and protect against them so they do not reduce the accuracy of the results?	Data collection from relevant sources to identify the different aspects applicable in the design of the trust management system and scenarios to test the system – This identified the techniques used in security management systems applied to VANETs and enabled the development of modules used in developing the trust management system. This objective also identified development tools needed in creating the proposed system. The data collected also facilitated the design of complex scenarios that evaluated the proposed trust management system.	Trust model for VANET communications.
Can a trust management system include a watchdog mechanism that provides both secure watchdog selection and fairness in the selection process? A secure and fair watchdog mechanism will improve the accuracy and efficiency of the trust management system.	Design and develop the watchdog system and TA system applied to the RSU – This featured designing the secure and fair selection system used to select watchdogs in the VANET— development of the watchdog agent, which, when applied to vehicles, enabled them to monitor their neighbours' communications. The design of the agent applied to the RSU enabled the RSU to undertake the responsibility of a TA. The agent also enabled the RSU to manage the trust values of vehicles present in the VANET.	Framework for watchdog selection and maintenance.
Can federation be included in the trust management system so tasks are distributed in the VANET to increase efficiency? Can the trust management system be robust enough to protect against malicious	Design and develop the set of algorithms and equations that calculates and performs security management in the VANET – These identified attributes in vehicle communication define trust in a vehicle. These attribute values calculated a	Framework for watchdog selection and maintenance. Framework for RSU agent. Trust model for VANET communications.

watchdogs in the VANET that may provide false information?	composite trust value representing a vehicle's malicious or non-malicious behaviour. The objective also included the algorithms that identified false positives and recuperated malicious vehicles in the VANET.	
Can a multi-tier trust management system be robust enough in the presence of multiple malicious vehicle presence in the VANET to provide security and achieve its objective function?	Develop a working prototype of the multi-tier trust-based management system and evaluate it in different replicable scenarios to test effectiveness – This featured combining the elements designed in objectives 3 and 4 into a complete system working synchrony. The complete system was applied to a VANET populated with malicious vehicles to test effectiveness in different scenarios. Results were generated and presented from the various experiments performed.	Prototype framework and Source code. Framework for false positive detection and recuperating malicious vehicles. Experimental conclusions and results

1.7. Thesis organization

The organization of the thesis is as follows: Chapter 2 contains a detailed critical literature review and a background overview of VANETs, attacks in VANETs and security solutions developed against these attacks. The chapter will then focus on trust management systems developed for various systems, highlighting specific hypotheses and theories related to the study. The literature review will cover work from the recent past, no further than five years, to ensure only the current state-of-the-art trust management systems. Chapter 3 dwells on the methodology and approaches used to conduct the research. It will include the data-gathering techniques and simulation tools used in the study. Additionally, this chapter discusses data management techniques. Any assumptions made in the study are also specified.

Chapter 4 discusses the proposed multi-tier trust-based security management design and concepts used to meet the thesis aims and objectives. It includes the selection of attributes to represent vehicle characteristics and the equations and algorithms used in developing the trust model. A discussion of the simulation model and the application of the proposed system to the simulation model is included. It will also feature the description and details of the scenarios used to evaluate the proposed system. The proposed system is applied to the scenarios and results presented from the simulations and experiments. The chapter discusses the hardware and software requirements and highlights the challenges experienced in applying the proposed system in the simulation environment.

Chapter 5 discusses how the proposed system will deal with false positives and malicious vehicles recuperating in the VANET. The VANET architecture and techniques used by the proposed system are detailed. An explanation of the algorithms used is provided. The simulation scenarios are presented, and the results of the experiments are discussed in this chapter.

Chapter 6 details the secure and fair watchdog selection model. The architecture of the security model applied to vehicles during the selection process is explained. The fairness model is also detailed. The watchdog selection model is applied to scenarios and simulations, and the results are presented.

Chapter 7 presents the conclusions of the study. Furthermore, it includes research outcomes and contributions of the research. It will also feature limitations to the study and any recommendations for the future of this study.

2. Background

2.1. Overview

This chapter will first review VANET communications and the importance of VANET communications to smart cities and ITSs. It will then look at the architecture of VANET communications, focusing on V2V and V2I communications as the most common communication types in VANETs. The following section in the literature review will look at the security requirements of VANET communications and the attacks that threaten these security requirements. Moreover, it will look at security proposals developed to deal with these attacks mentioned previously. The chapter will focus on state-of-the-art trust management systems developed to deal with malicious vehicles in the VANET. Then look at some of the issues facing trust management systems. As trust management systems use one-hop neighbours to watch the monitored vehicles, the following section looks at the optimal selection of one-hop neighbours. The research will then extend to the vehicle characteristics representing the vehicles' trust. The chapter will conclude with the optimal selection of trust factors to distinguish between malicious and non-malicious vehicles.

2.2. Introduction

Over the last decade, improvements in ITSs and autonomous vehicles have led to the emergence of Vehicular Ad-hoc Networks (VANETS) [19], [44]. In addition to driving, vehicles can now perform additional tasks such as navigating and communicating. Recent advances in software, hardware, communication, and sensor technology have made these additional functions possible, along with various applications and standards development. VANETs have become one of the most promising and fastest-growing areas of the subset of Ad-hoc networks [19]. The interest in VANETs has increased exponentially over the years, not only to researchers but to car manufacturers too. VANETs are an extension of MANETs associated with vehicles and RSUs. VANETs have the same characteristics as MANETs because they are self-organizing, self-management and low bandwidth transmissions [45]. The intrinsic difference is that VANETs constitute vehicles, and MANETs constitute nodes. VANETs are a significant component of smart cities and ITSs [3], [5]. The rise of VANETs is also attributed to the automotive industry, which recognizes the importance of connecting vehicles with a communication system [7]. Research in academia, governments and industrial firms are developing significant projects in VANETS and ITS [46]. The increased interest has created multiple uses and applications for VANETs in the modern world. VANETs provide traffic information, safety-critical incidents, and traffic hazards to drivers and entertainment to connected vehicles [44], [47]. In the electric vehicle (EV) industry, VANETs provide information on charging points [48]. This information could be crucial to vehicles when the battery is running low. Future vehicles connected via VANETs are anticipated to play a significant role in day-to-day human life [7]. VANETs, when deployed in urban cities and ITS, aim to solve two main safety challenges experienced by road users: Road accidents and traffic congestion.

Road accidents
Traffic accidents are one of the biggest problems across the whole world. Research by the World Bank statistics on the world economy shows that the economic loss of traffic

accidents is $500 billion worldwide per year, while WHO shows that the number of deaths is 1.24 million worldwide per year [3]. Surveys have shown that if the driver acquires information about the accident even half a second before the mishap, 60% of accidents can be avoided [11]. VANETs aim to solve the issue of road accidents by circulating information about life-threatening events on the road, increasing safety [49]. Information exchange can assist drivers and autonomous vehicles in avoiding accidents on the road. In addition to communicating life-threatening events, VANETs can also communicate driver behaviour and driving conditions, which increases traffic safety [5]. Safety-related applications of VANETs require low latency, high reliability and delay tolerance [7]. However, malicious vehicles in the VANET make it increasingly difficult to disseminate information about life-threatening events [49]. Malicious vehicles threaten the high reliability and increase delays in VANETs. Disruptions in the information exchange threaten the VANET solutions developed to reduce road accidents.

Traffic congestion
Traffic congestion has also become a global problem, causing time delays, wasted fuel consumption and unnecessary environmental pollution. VANETs can avoid traffic jams by sharing traffic information, saving time and fuel [50]. Reduced emissions benefit both the health of the driver and aid environment conservation.

VANETs also have the non-safety category of applications, including infotainment, internet on the move, toll collection, and vehicle diagnostics [51]. These non-safety applications, however, do not have the delay and communication demands of safety applications. VANETS are an encapsulation of Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I), Vehicle-to-Pedestrian (V2P) and Vehicle-to-Everything (V2X) communications [44], [52]–[54]. V2I and V2V communications are the two main communications in VANETs. The section below describes the different aspects of VANETs in detail.

2.3. VANET communication

2.3.1. Vehicle-to-infrastructure communication

V2I communication comprises vehicles in the VANET exchanging information with RSUs or Trusted Authorities (TA) [52]. RSUs, which act as base stations, are installed at road intersections, traffic lights or other sections such as petrol stations or bus stations [53]. RSUs are connected to the backbone of the internet and can receive and transmit different information from and to nearby vehicles as they pass by. V2I provides high data rates and low-latency communications [54]. These characteristics are attributed to RSUs being mainly not battery-powered as they are permanently installed, have a steady electricity supply, and can offer higher bandwidth. V2I communication is suitable for real-time applications because it is a reliable communication technology [53]. The high data rate and low latency characteristics of VANETs provide good communication reliability.V2I communication also provides an interface for vehicles to connect with external networks via the RSUs [55]. The ability to make external connections increases the applications of VANETs, such as connections with cloud applications.

2.3.2. Vehicle-to-pedestrian communication

V2P communication is made up of communication between vehicles and Vulnerable Road User (VRU) groups [56], [57]. VRU groups include pedestrians, cyclists, and motorized two-wheeler operators. V2P communication prevents collisions between vehicles and VRU groups by sending alerts and crucial messages [58].

2.3.3. Vehicle-to-everything communication

V2X communication encompasses sharing of information between V2I, Vehicle-to-Vehicle (V2V), Vehicle-to-Pedestrian (V2P), Vehicle-to-Self (V2S) and Vehicle-to-RSUs (V2R) [59]. V2X consist of all communication made by vehicles in the VANET. V2X concept uses the latest generation of information and communication to realize omnidirectional communication [60]. It creates a safer and more comfortable transportation environment by improving traffic efficiency and reducing accident rates.

2.3.4. Vehicle-to-vehicle communication

V2V communication, or Inter-Vehicle Communication (IVC), comprises peer-to-peer or multiple-hop communication between vehicles [61]. Vehicle communication in V2V is a crucial component of VANETS as vehicles can exchange messages and information such as speed, location, hazardous conditions, vehicle breakdowns, travel direction and acceleration [44]. This information improves road safety, traffic efficiency and collision avoidance. V2V communications have the unique characteristics of high mobility, dynamic network topology and unpredictable vehicle movements [18], [62]. These unique characteristics often lead to frequently disconnected networks and rapid topology changes [13] during communication rounds. New algorithms and protocols have been developed to deal with this characteristic of V2V communications. One of the critical challenges faced in V2V communications is ensuring secure communications between vehicles in the VANET [13].

2.4. Architecture of vehicle communication

Vehicle communications in the VANET are made possible via wireless links mounted on each vehicle [46]. Every vehicle in the VANET acts as a router and a participant as they communicate via one hop mechanism with vehicles in their transmission range. Vehicles in the VANET include two main components the OBU and the Application Unit (AU) [11]. The OBU comprises GPS, wireless communication, CCM, and human-machine interface modules. It controls information processing, memory management, decision-making, and communication capabilities. It gathers information to form messages transmitted to neighbouring vehicles [63].

2.5. Technologies in VANET communication

Due to the vehicle speed in VANETS and rapidly dynamic changing topology, new communication protocols have been developed to cope. Wireless Access in Vehicular Environment (WAVE) is a protocol developed to adapt to wireless communication in VANET communications and support ITSs [64], [65]. It is based on the IEEE 802.11p

standard and provides the basic radio standard for DSRC operating in the 5.9GHz frequency [66], [67]. The federal communications commission (FCC) reserves this communication spectrum for VANET communication [68]. WAVE protocol supports safety applications and provides low-latency communication in V2V and V2I communication [69]. WAVE protocol can support a data rate of up to 27Mbps for vehicles with a speed of up to 200 km/hr [55]. WAVE communication protocol is, therefore, practical for VANET communication.

VANETS use autonomous vehicles in operation. Although these vehicles provide sufficient energy, it is crucial to consider the entire system's energy requirements. Sensors play a critical role in various aspects of vehicle operation, including safety, performance, and efficiency. However, they are not the only components consuming energy within the vehicle. There are other power-hungry systems, such as propulsion, communication, and auxiliary systems, that also rely on available energy [70], [71]. In addition to this, the charging of electric vehicles consumes much power. Such that simultaneously charging several vehicles will strain the electricity grid [72]. Highlighting the energy constraints will highlight potential issues, challenges and trade-offs that arise when allocating energy resources among these different systems. Ignoring the energy constraint could lead to imbalanced power allocation, compromising the system's performance, reliability, and efficiency. It is crucial to optimize energy distribution to ensure the effective and reliable operation of all components of the vehicle.

2.6. VANET communication security requirements

Securing communications is crucial for VANETS because messages exchanged between vehicles hold critical information, and it is essential that these packets must reach the intended target without any modification or insertion of data [11]. VANET applications depend highly on cooperative data and vehicle information exchange [51]. A significant concern for VANET communications is that messages are intercepted or modified before they arrive at their intended destination [44]. The following are identified as characteristics that VANETs must satisfy to be secure in communication.

Availability: In VANET communication, real-time data is crucial for many purposes; therefore, the data must be available and accessible when needed [73]. Applications of VANET communication require a quick reaction from vehicles to the data provided. Hence, any delay in the data, even for a few seconds, could render the data useless.

Authentication: This guarantees that data generated and forwarded by vehicles in the network is by an exact vehicle [74]. It is imperative that data is generated from an exact vehicle as vehicles in the network react to the data they receive.

Integrity: This ensures the recipient's and the sender's data is the same and that data is altered by only authorized vehicles [11].

Non-Repudiation (NR): The purpose of this is to prevent vehicles identified as malicious from refusing the offences [11], [73]. Once a vehicle has been correctly identified as malicious, it cannot masquerade as an innocent vehicle and transmit packets in the VANET. Senders of messages cannot deny being the sender.

Confidentiality/Privacy: This guarantees that authorised vehicles will only access the data and that vehicle privacy will be maintained [4].

Several threats exist to these security requirements of vehicle-to-vehicle communications in the form of malicious attacks launched. The threats will be detailed below.

2.7. Attacks in VANETs

Attacks refer to any malicious activity meant to cause harm to the system. The main idea behind executing these attacks is to intercept, drop, or modify the messages for their selfish purposes [73]. Vehicle communications in VANETs are vulnerable to attacks because of the high mobility with frequent disconnections; vehicles only communicate with each other for a limited time [16]. These attacks tarnish the security requirements of vehicle-to-vehicle communications. Attackers may be categorised as follows:

2.7.1. Insider/outsider attack

These attacks depend on the membership of the vehicle to the VANET. Attacks can be perpetrated by an insider or an outsider in the network. An insider attacker has authentication by the network and knows all communication details in the network, while an outsider attacker does not have network authentication [10]. Insider attacks are more dangerous than outsider attacks since the vehicles are already internal network members. Outsider attackers are not network members and therefore have limited scope to attack the VANET [17]. The proposed trust management system works to identify insider and outsider attacks.

2.7.2. Active/passive attack

These attackers are categorized based on the activity performed in the network. Active attackers attempt to modify packets sent in the network or disturb the normal operations of the VANET [75]. While passive attackers only listen to the network traffic to steal information or identify patterns in information in the VANET, they do not alter the network traffic [17]. Passive attackers are much more challenging to identify than active attackers [75]. The trust system proposed will work to identify active attackers in the VANET.

2.7.3. Malicious/rational attack

These are attackers based on the intentions of the attack. Malicious attackers will attack a VANET without any intentions or personal benefit, while rational attackers will attack the VANET with personal intentions or for personal benefit [17], [73], [75]. The trust system proposed will identify malicious and rational attackers in the VANET. Some of the attacks that can affect vehicle-to-vehicle communication are explored below.

DOS attack

This attack is one of the most common attacks that take place in VANETs [16]. This attack's main motive is to jam communication between vehicles in the network [10], [73]. DOS attacks deny regular vehicles in the network access to resources. DOS attacks are achieved by sending many unusable messages to the network. They can lead to vehicles dropping and delaying messages in the VANET.

DDOS attack

A DDOS attack is similar to a DOS attack, but its performed by various vehicles in the VANET [4], [10]. DDOS is much more severe than a DOS attack. The vehicles may be in different locations and time slots; preventing or tracing the attack is much more complex [17].

Black hole attack

In this attack, the source vehicle will broadcast route request messages (RREQ) to one hope neighbours in search of the shortest route to the destination [76]. One of the intermediate vehicles is malicious, which transmits a false route reply message (RREP) to the source vehicle claiming to have the shortest path to the destination. The source vehicle transmits all packets to the malicious vehicle, thus never transmitting them to the intended receiver [4], [76]. The malicious vehicle will then drop all the packets and not transmit them to the destination.

Wormhole attack

This attack is similar to a black hole attack but performed by two vehicles. In this attack, two or more malicious vehicles collude and form a tunnel, transmitting data from one malicious vehicle to another at the end of the tunnel [10], [23]. Thus never transmitting the messages to the intended target destination.

Message suppression or alteration attack

In this attack, a malicious vehicle will receive messages to forward to the destination vehicle; the malicious vehicle will either suppress the message by dropping the messages or altering them to fulfil their agenda [4]. This attack will cause vehicles to drop messages in the VANET.

Replay attack

In this attack, the malicious vehicle will receive a message, and instead of forwarding it, the malicious vehicle will store the message to send it later [18]. The main aim of the malicious vehicle is to take advantage of the VANET condition when the message was sent by delaying the effect of the message [12], [77].

Sybil attack

This attack consists of a vehicle which sends multiple copies of the same message, each with a different fabricated identity [13], [77]. The aim of the attack is for the

malicious vehicle to reinforce its malicious message by making the destination think the message came from multiple sources.

Timing attack

This attack delays messages in the VANET. In this attack, the malicious vehicle will add delays to the messages sent without altering the message's contents [13]. The attack's primary purpose is to make the destination vehicle receive the message later than was intended by the source vehicle [4].

Man-in-the-middle Attack

The attack happens when a malicious vehicle positions itself between two communicating vehicles to access the messages sent [16]. The two regular vehicles will still assume they communicate directly, while the malicious vehicle can alter packets sent between them [17].

Eavesdropping attack

In this attack, the malicious vehicle will passively intercept and examine messages in the VANET without altering the messages [18]. The attacker aims to gain as much information from the VANET for future attacks or to steal the information for personal use. A summary of the attacks and effects on messages is presented in Table 2.1.

Table 2.1 - Summary of attacks in VANET communication and the effects of the attacks on VANET messages.

Attack	**Insider/Outsider**	**Active/Passive**	**Drop/Delay in messages**
DOS attack	Insider	Active	Both
DDOS attack	Insider	Active	Both
Black Hole attack	Insider	Active	Drop
Worm Hole attack	Insider	Active	Drop
Message Suppression/Alteration	Insider	Active	Delay
Replay attack	Insider	Active	Both
Sybil attack	Both	Active	None
Timing attack	Insider	Active	Delay
Man-in-the-middle attack	Both	Passive	Delay
Eavesdropping attack	Both	Passive	Delay

2.8. Security proposals in VANET

Security is a significant issue in VANET communication as the vehicles exchange sensitive information about themselves and its surrounding with other vehicles [78]. Malicious vehicles cause disruptions in the regular operation of the VANET; hence, security mechanisms had to be developed to detect and isolate these malicious vehicles from the VANET. However, before designing security systems for VANETS, specific characteristics that make VANETS unique networks are considered. These are listed below.

High Mobility: Vehicles in a VANET are usually fast-moving, and this high mobility presents a unique challenge in identifying and detecting malicious vehicles [78].

Dynamic network topology: Because of the high mobility rate, the network topology is always rapidly changing [79]. This highly distributed and dynamic network creates a challenge in designing security systems.

Low bandwidth and transmission range: VANET communication suffers from low bandwidth communication due to the technologies used [80]. The low bandwidth and transmission range means that large amounts of data are challenging to exchange between vehicles in the VANET.

Resource constraints: Vehicles in the VANET are resource constrained with limited storage and storage capacity [78]. Therefore, security systems designed must be resource efficient in their design. Security systems should ensure less communication and computation overheads [48].

Lack of well-defined boundaries: VANET networks are open networks with no fixed borders controlling the vehicles in the network [78]. This characteristic also needs to be considered when defining a secure system.

Due to the unique characteristics of VANETs, traditional security mechanisms are rendered unusable, and new security schemes had to be developed. Authentication of vehicles in the VANET is an integral step because vehicles use authentication before accessing or sending messages and can prevent malicious vehicles [81], [82]. Proper authentication schemes have the ability to quickly identify malicious vehicles and illegitimate messages, therefore, providing security in the VANET. Cryptography as an authentication scheme has shown great ability to prevent external attacks but is not as efficient in insider attacks [25], [83]. The following section will look at some recent cryptographic solutions developed.

In order to prevent wormhole attacks, [23] used secure message broadcasting using a cryptographic technique. A shared key is distributed to the vehicles in the network via a public key cryptosystem. Packets shared in the network are encrypted with the shared key by the source vehicle and the same key by the destination vehicle to decrypt the message. The packets also contain the identifier ID and expected time used by the destination vehicle to decide if the vehicle is secure or not. The limitation of the above method is that the computational overhead increases with the number of vehicles in the network.

Timed Efficient Asymmetric Cryptography (TEAC) is an asymmetric cryptography technique proposed by [22]; in addition to security in the VANET, the scheme also provides sender privacy. The vehicles will communicate with the RSU to form secure connections in this scheme. The sender of packets uses a pool of private-public keys to encrypt data sent with its unique ID. When a vehicle is in proximity to an RSU, it will be handed a temporary ID (used to obscure its identity) and shares its pool of keys with the RSU and temporary ID. The pool of keys is time limited and expires after the time limit. Every time it expires, a new pool of keys is generated in the network. When

a destination vehicle receives a packet, it will verify the sender's identity using the temporary ID and request a key from the RSU, which decrypts the message received.

An anonymous key-sharing cryptography technique has been used in [20] to secure vehicle communications in VANETS. The technique uses several certificates and their private and public keys in a vehicle so that the vehicle can use them to avoid attacks. The certificates are anonymous to hide the identity of vehicles in the network. However, the frequent key changes make this a complex process where a vehicle must store many keys.

Trustworthy VANET routing with group authentication (TROPHY) uses a group management technique to store certificates and keys to provide secure communications in the VANET [84]. It uses a central TA responsible for creating, updating, maintaining, and distributing messages to maintain the authentication process. The central authority also keeps hold of a shared routing key used by all vehicles to authenticate messages—the routing key updates after certain intervals. Cryptography solutions provide a level of authentication and are effective against internal attackers or vehicles which join the VANET for the first time [51]. Cryptography solutions alone cannot solve the security concerns in VANETS due to the dynamic behaviour of vehicles, lack of reliable infrastructure and insider attacks [27], [85]. However, cryptography solutions can be combined with trust management solutions to increase effectiveness against malicious vehicles.

Trust management has been proven efficient in handling both internal and external attacks. The following section shall review some recent trust management schemes developed and the factors considered in designing a trust management system.

2.9. Trust management as a security solution

Trust in VANET communications refers to the ability of a vehicle to put belief in another vehicle that the vehicle is not malicious and can accept its messages and forward them to the intended destination [42]. Trust management has become integral in providing secure vehicle communication in VANETS [61]. Trust management is needed to maintain reliable, secure and faithful communication in VANET [50]. It identifies malicious behaviour by providing a secure connection between trusted vehicles and isolating malicious vehicles [86]. Therefore, the main aim of a trust management system is to empower each vehicle in the network to identify malicious vehicles and impose a punishment for malicious vehicles so they can regularly behave in the future [85]. Trust management schemes also can detect insider and outsider attacks in the VANET [61]. However, for trust management-based solutions to be effective, they need to fulfil the following properties [68]:

Efficiency – The trust management system should be efficient enough to work in different conditions in the presence of malicious vehicles in the VANET.

Robustness – The system should resist attackers aiming to deceive the vehicles in the VANET or deceive the trust management system.

Anonymity – It should be able to keep the identities of the vehicles secret from other vehicles in the network. Only the TA is in charge of managing vehicle trusts should know the identity of the vehicles. This method is termed conditional anonymity.

Simple, light and fast – The trust management scheme should quickly identify malicious vehicles while being light in computing and complexity requirements [50]. The system should minimize overheads as much as possible.

Trust management solutions involve two significant steps: establishment/calculation/computation and management of this trust value among vehicles [51]. Trust calculation refers to the steps taken to obtain a value representing a vehicle's trust. The storage of the trust value and components that store the trust value covers the trust management part.

Trust models are categorized into three main categories based on how they model trust values: Entity-centric trust models, Data-centric trust models and hybrid trust models [26], [27], [29].

2.9.1. Trust models

The following section shall discuss different trust models and their strengths and weaknesses.

Entity-centric models

Entity-centric trust models focus on modelling the trustworthiness of vehicles based on past direct interactions and recommendations by neighbour vehicles [26]. The main aim is to measure the behaviour tendency and exclude malicious vehicles to ensure the reliable delivery of data packets [27]. Due to the high mobility of vehicles in the VANET, it becomes difficult to collect the real-time reputation of a specific vehicle.

Data-centric models

These trust models are focused on identifying malicious vehicles by estimating the quality and trustworthiness of data transferred in VANETS [26], [63]. In order to verify the trustworthiness of data, cooperation is needed among neighbour vehicles to gather information from various sources [29]. By doing this, data-centric trust models can assess the authenticity and accuracy of the information transmitted by a particular vehicle [27]. Data-centric trust models, however, increase latency in VANETS. The latency may be because the large amounts of data shared between vehicles may contain much redundant information [29].

Hybrid trust models

Hybrid trust models evaluate the trust level of vehicles and the trustworthiness of data transmitted by vehicles [27], [87]. Therefore, they benefit from both the advantages of data-centric and entity-centric models. Hybrid trust models can identify dishonest and malicious vehicles while also identifying malicious messages in the network [83]. The work presented here is a hybrid trust model.

Trust management schemes can also be either centralized or decentralized. Centralized trust management schemes rely on infrastructure, such as a TA, to manage trust values and vehicles [85]. Decentralized trust models do not rely on any central infrastructure for trust management, but the vehicles perform the management themselves [8]. The following section will examine recent trust management models created to support vehicle communication in VANETs.

[88] suggested a trust management system using two concepts: reputation and trust. In their system, reputation refers to the quantitative representation of the trustworthiness of a vehicle. This reputation will change depending on the behaviour of a vehicle. Trust in their scheme refers to the trustworthiness of the messages sent by the vehicles in the VANET. It uses a reputation management centre responsible for collecting interaction data among vehicles, evaluating the reputation of all vehicles, and recording evaluation results. They used a range of 0-50 to represent the trust values, with all vehicles having an initial reputation value of 20. The reputation was based on events recorded by the vehicle and if the neighbours reported the same event.

In [89], their trust management scheme estimated a vehicle's trust level based on its neighbouring vehicles' opinions; they then isolated malicious vehicles by putting all trusted vehicles in a single cluster. The scheme does not use a central trusted management centre, but all vehicles are responsible for managing their trust levels and the trust levels of neighbours. The trust level is determined by the number of positive experiences with neighbour vehicles, which are actual events reported by the vehicle. The trust value of vehicles is a value between 0-1. Initially, vehicles are set to a trust value of 0.5 to their neighbours and a value of 1 to themselves.

The trust management system in [90] selected a reputation value for the vehicles between -3 to 3, with -3 to 0 representing a malicious vehicle, 0 a neutral vehicle and 0 to 3 being a trusted vehicle. They used a clustering method where a vehicle reported an event, a cluster head was selected, and vehicles close to the event were sent to verify the event's credibility. Vehicles identified as malicious are blocked for some time, after which their trust value is set to neutral (0).

[40] assumes that vehicles can only have two levels, trusted and untrusted, and each time a vehicle is evaluated, it is considered an independent process. A central TA manages vehicles' trust values and builds a trust link graph for the vehicles in the VANET. The trust is calculated as a ratio of the number of authentic messages sent to the total messages sent. Trust monitoring happens via seed vehicles selected as the most reliable vehicles in the VANET.

BARS is a blockchain-based reputation system for trust management suggested by [29]; it uses the blockchain network instead of a central trust management system. Their trust management system consists of a punishment and reward mechanism. Vehicles that forward messages honestly and actively and those that disclose misbehaviours and forged messages get rewarded. While vehicles which are dishonest or that abuse disclosure messages receive punishment. The reputation value is between 0 - 50, where 50 are considered trusted vehicles while closer to 0 are considered dishonest vehicles.

In work by [42], a set of evaluator vehicles was selected by the RSU to store and calculate the vehicles' trust details by the duration they stayed in the VANET. The evaluator vehicle has its copy of the trust database, but they continuously share information to keep the databases updated. Vehicles' trust values range between 0 and 1 and are calculated based on the current trust level, reward points of honest event alerts and punishment factor for any false alarms raised. Vehicles closer to 1 are considered more trustworthy than vehicles with a trust value closer to 0. The trust management scheme uses RSUs, which are assumed to be completely trusted.

The trust management scheme suggested in [85] uses neighbour vehicles to broadcast a test message to calculate the trust value of vehicles. The trust value is normalized between 0 and 1, with 1 being a trusted vehicle and 0 being a malicious vehicle. A TA manages the trust values of vehicles. Table 2.2 summarises the trust management systems' functionality and objective functions.

Table 2.2 - Summary of trust management systems, their functionality, and objective functions.

Trust model	Description	Experiments	Parameters considered	Year
Trustworthy Event-information dissemination in VANETs [89].	• Decentralized – each vehicle accumulates trust levels of neighbouring vehicles. • Mitigating message modification attacks and fake generation attacks. • Considers trustworthiness of messages.	• Message overhead. • False decision probability. • Two different scenarios (Highway and Urban).	Comparing the event reported to direct observation of an event spot or announcement from a public and reliable group.	2017
Distributed trust management scheme for VANET [36].	Decentralized using blockchain technology.	Verified that the model works using a case study.	Comparing events reported by vehicles to events detected by neighbour vehicles. If the same increase in trust value.	2018
Secure and stable NSNRT clustering algorithm [91].	Decentralized – each vehicle decides its trust factors.	• Cluster stability – the average time a cluster head maintains state and the average time a member vehicle stays in a cluster. • Communication overhead.	Vehicle similarity between neighbours. The relative speed, distance, and acceleration with neighbours. Used to select cluster head.	2018

		• Cluster head election time. • The number of compromised vehicles elected as cluster head. • Packet delivery rate in the presence of malicious vehicles.		
BARS: a blockchain-based anonymous reputation system [29].	• Centralized – has a Law Enforcement Authority. • Makes use of blockchain for anonymous authentication of vehicles.	• Storage and transmission overhead (by memory taken by messages). • Computation overhead (time taken).	Uses the receiver to validate the authenticity of a message received Uses private and public keys for authentication.	2018
Trust management scheme in VANET [85].	Centralized – has agents of the trust authority. And a TA.	• It does not perform any simulation but has a chapter on expected results. • The expected results of the algorithm significantly reduce transmission and computation overheads. • Expected results vehicle authentication, message integrity and privacy protection are expected.	It uses a test message to verify vehicles' trustworthiness. If vehicles forward a message to the destination, it is considered trustworthy.	2018
Trust management based on vehicles stay time in VANET [92].	• Decentralized – Chooses a set of evaluator vehicles in the network that store trust values. • Evaluator vehicles were selected as vehicles which have stayed most	• Communication overhead (ratio of the total size of header bytes to the total size of the whole safety message).	Evaluator nodes exchange public and private keys to verify vehicles and give trust values.	2018

	prolonged in the network.			
A machine learning approach for software-defined vehicular ad-hoc networks with trust management [86].	Centralized – has an SDN controller.	• The PDR is used to compare. • Network throughput.	Uses position and forwarding ratio of vehicles to determine trust value.	2018
A hybrid trust management heuristic for VANETS [27].	Trust metric is used to select cluster head. It does not mention if trust value is stored.	Used malicious vehicles to validate the algorithm.	Uses vehicle behaviour determined by information shared by a vehicle monitored by the neighbour's vehicle.	2019
Anti-attack trust management [40].	• Centralized. • Uses local trust values stored in vehicles and RSUs. • Global trust values are stored centrally by a trust manager.	• Pairwise orderedness (good vehicles are ranked higher than bad vehicles). • Three malicious attacks to test for effectiveness (newcomer attack, on-off attack, collusion attack).	• Uses the total number of messages sent compared to the total number of true messages sent. True messages are determined by probability distribution. • Uses the speed of vehicles as well. Vehicles going above the speed limit are considered untrustworthy.	2020
Event trust model for VANET based on statistical model [88].	• Centralized • It uses both reputation and trust. • Reputation refers to the trustworthiness of vehicles. • Trust refers to the trustworthiness of messages issued by vehicles.	• Time taken to identify malicious vehicles. • The number of deceived vehicles compared to the number of malicious vehicles. • Verifying that the trust model works.	Comparison between neighbour data to determine reputation.	2021

	• Reputations are updated every 120 seconds.			

Table 2.3 below summarizes the advantages and disadvantages of the reviewed trust management systems.

Table 2.3 - Advantages and disadvantages of reviewed trust management systems.

Trust management system (year).	**Advantages**	**Disadvantages**
Trustworthy Event-information dissemination in VANETs (2017) [82].	Makes use of beacon messages to calculate trust. Therefore, event messages are not affected.	Vehicles are responsible for calculating trust values. This method increases the overheads incurred by vehicles. This increases the resource consumption of vehicles.
Distributed trust management scheme for VANET (2018) [36].	Makes use of federation by electing cluster heads responsible for calculating vehicle trust.	• Uses event messages to calculate the trust of vehicles. • The elected cluster head has to control the behaviour of vehicles for a period in order to compute trust. Giving vehicle control to a third party may cause unwanted effects. • Vehicles elected as cluster heads are responsible for calculating and managing the trust. This method may increase the overheads of vehicles.
Secure and stable NSNRT clustering algorithm (2018) [84].	Considers communication capabilities of a vehicle in trust calculation.	• Uses event messages to calculate trust. This means that an event must happen for trust to be calculated. • Any vehicle can calculate the trust of another vehicle in the VANET. Malicious vehicles can take advantage of this to spread false information.
BARS: a blockchain-based anonymous reputation system (2018) [29].	• Considers historical interactions as well as current interactions when calculating trust values.	• It uses blockchain technology to store information. Loss of connection or delays in connection to the

	• It uses a federation by employing blockchain technology, a law enforcement agency, and a certificate authority to calculate trust.	blockchain ledgers will affect the security system's performance. Therefore requires a constant network connection to be secure.
Trust management scheme in VANET (2018) [78].	• It uses a federated model in its design, using RSUs, TAs, agents of the TA, area post office and regional transport office in calculating vehicle trust. • Considers a vehicle's history and current factors to calculate trust in the VANET.	• Trust can only be calculated after the information is collected from at least 100 neighbours of a vehicle in the VANET. This means trust cannot be calculated if 100 vehicles are absent in the VANET.
Trust management based on vehicles stay time in VANET (2018) [85].	• It uses a federated model in its design employing a government trust agent to manage RSUs, and RSUs are responsible for managing evaluator vehicles.	• Employs evaluator vehicles to calculate trust. This method may increase the overheads incurred by the vehicles. • Uses event messages to calculate trust in the VANET. This means an event must be triggered for trust to be calculated.
A machine learning approach for software-defined vehicular ad-hoc networks with trust management (2018) [79].	Makes use of machine learning in the calculation of trust values.	Only establishes a secure route from one vehicle to another. Route establishment is done every time a vehicle wants to send a message. This is a time-consuming method of calculating trust.
A hybrid trust management heuristic for VANETS (2019) [27].	Trust calculation can be optimized to be more secure or less secure, according to the VANET application.	• Makes use of vehicles to calculate trust, thus increasing vehicle overheads incurred in the VANET. • Makes use of event messages to calculate trust. This means an event must be triggered in order to calculate trust.
Anti-attack trust management (2020) [38].	• It uses a federated design model using a TA and RSU to calculate trust values. • It calculates both a local and global trust value, increasing its security. • Takes into consideration driver behaviour while	• Any vehicle can watch another vehicle in the VANET. Malicious vehicles can use this to spread false information about other vehicles. • Newcomer vehicles with no information cannot have their behaviour evaluated.

	calculating the trust values.	• Assumes public vehicles, e.g. buses and taxis, are more secure than private vehicles, which may not always be accurate.
Event trust model for VANET based on statistical model (2021) [81].	• Employs federation using a central management authority and RSU to calculate vehicle trust. • It uses both behaviours of a vehicle and messages trustworthiness to calculate trust.	• Requires an event to be triggered to evaluate the trust of vehicles. This means trust cannot be calculated unless an event is triggered. • RSUs have the task of monitoring vehicles yet have no security mechanisms present.

In trust management systems in VANET communications, some vehicles are assigned the task of monitoring other vehicles in their vicinity to detect malicious activity performed by them. The vehicle works promiscuously and can overhear communications of neighbour vehicles [78]. Different researchers give these vehicles several names; seed vehicles [40], evaluator vehicles [42], agents of TA [85], and watchdogs [61], [78], [93]. In this work, vehicles that evaluate their neighbour vehicles are called watchdogs. The process of watchdog selection used by different security management techniques is detailed in Chapter 2.12 of this work.

2.10. Trust value range

The trust value range is the numerical value that represents a vehicle's trustworthiness. Several researchers have designed trust management schemes with a trust value between 0 and 1 [94]–[97]. In these schemes, trusted vehicles have a trust value of 1 or closer to 1, and malicious or dishonest vehicles have a trust value of 0 or closer to 0. During the network initialization phase, some researchers initialize their vehicles with an initial trust value of 1 at the start of operations [94], [98]. The advantage of this method is that all vehicles are trusted at the beginning of the operation and can participate in normal network operations. In schemes like the one designed in [96], the initial trust value is 0, and vehicles must gain trust to participate in normal network operations. There are other trust value ranges proposed in other schemes. The work in [99] proposes a trust value between 0 and 10, with 0 vehicles closer to 0 being malicious and ones closer to 10 considered trusted in the network. While in BARS, the trust value is between 0 and 50, with vehicles closer to 50 being more trusted than vehicles closer to 0. Assigning the trust value between 0 and 1 remains the most popular method. Therefore, to enable correlation and comparison with other trust management systems, the trust values of vehicles are between 0 and 1 in the proposed trust management system.

2.11. Trust calculation factors

In order to calculate the trust value of a vehicle, certain factors must be considered to confirm its authenticity. The validity of the trust management system depends on the proper selection of trust metrics [25]. However, the more trust factors selected, the

higher the network overheads and energy consumption [25]. The factors are looked at in detail below.

2.11.1. Message authenticity compared to neighbours

To evaluate the trustworthiness of vehicles, some researchers have tried to determine the authenticity of messages broadcasted by a vehicle compared with its neighbours [29], [36], [92]. Trust management scheme based on the clustering mechanism for VANET (TCMV) determines message authenticity by comparing messages sent by a vehicle with messages from its neighbour vehicles [36]. How it works is a vehicle reports a message to the cluster head, the cluster head will wait an amount of time, and if no messages are received from the neighbour vehicles, it will send observers to check on the event. The trust value is then calculated based on the observer's report and reputation. In blockchain-based anonymous reputation (BARS), when a receiver receives a message, it can dispute the authenticity of a message [29] and report it to a TA.

2.11.2. Forwarding rate/packet delivery ratio

The PDR or FR is the ratio of data packets delivered to the destination to those generated at the source [100]–[103]. Because communications between vehicles in the VANET happen on a multi-hop basis, vehicles develop a FR depending on packets that are received packets forwarded to the destination. Analysing the PDR/FR determines if a vehicle performs malicious attacks such as selective forwarding attacks, blackhole attacks and DOS attacks [25], [96]. The PDR/FR determines any attack that involves packets' dropping. Joint trust: an approach for trust-aware routing uses a FR to calculate the trust value [104]. It calculates the feedback packets sent to the source after forwarding packets. [25] Also, the FR is used by acknowledgements sent back to the source node after forwarding packets to the destination to determine the trust values. In [96], the PDR was calculated by the number of successful packets delivered from one node to the other compared to the total number of packets sent from the same node to the other.

2.11.3. Message integrity/message correctness

Message integrity and correctness involve determining that a message has not been tampered with during forwarding. In work by [104], to determine if a malicious actor has tampered with a message. The source examines the specific time taken to transmit a packet. This method works because if a malicious vehicle tampers with a message, the transmission time will be greater than regular vehicles forwarding packets without modification. [42] also used a timestamp in forwarded messages compared to the current time to rate the confidence of a message. The closer the timestamp is to the current time, the more confidence in the message.

2.11.4. Consistency factor

The consistency factor is used to determine the trust of a vehicle because data between neighbour vehicles in a network is highly correlated [25], [105]. The correlation of data means data collected between neighbour vehicles determine if vehicles are malicious in the VANET. The consistency factor has been used to determine the trust

value of a vehicle in a VANET [104]. They compare the behaviours of neighbour vehicles in the network to identify malicious vehicles. While in [25], neighbour vehicles compare the data collected between vehicles in the VANET. If the difference between the two is within a specific range, there is an agreement between the vehicles and no malicious behaviour. However, if there is a disagreement, then one of the vehicles is considered malicious. [106] used the consistency of events reported to identify malicious vehicles. When a vehicle reports an event, the following vehicles that pass the same area are expected to report the same event to identify trust. Once a certain number of vehicles has reported the same event based on location, the event is verified, and the vehicle can be trusted. [105] used the spatiotemporal correlation of data collected between adjacent vehicles to determine the trust value of sensor vehicles in the network. They compared data collected by vehicles in the same region and employed time-related data. The mobility similarity, defined as the speed, distance and acceleration of vehicle neighbours, was used to calculate the trust of vehicles [91]. A vehicle with speed and acceleration closer to its neighbour vehicles and maintains a closer distance to its neighbours receives a higher trust score.

2.12. Watchdog selection

Several security management solutions, including trust management solutions, make use of vehicles to monitor other vehicle transactions in the VANET [8], [21], [40]. When a vehicle is selected to monitor its neighbour vehicle communications, it is commonly known as a watchdog [93], [107]. Using a watchdog in the VANET for security solutions allows vehicles to watch the neighbours determine malicious or non-malicious behaviour [18], [108]. The watchdogs have the ability to monitor neighbours located within only the coverage area of the watchdog [109]. The watchdogs have a limited coverage area and cannot cover a large-scale VANET area. The selection and maintenance of watchdogs in an ad-hoc network is not an easy task [110]. This characteristic is due to the networks' dynamic nature, such as node mobility, node failures and link failures.

Watchdogs have become popular in monitoring networks, including MANETs and VANETs. In addition to monitoring tasks, the watchdog can have additional tasks. Tasks include analysing the traffic to distinguish the malicious behaviour, storing this information and disseminating it to the VANET when required [104], [105]. However, these additional tasks add computational and storage overheads to the vehicles selected as watchdogs. Some advantages and limitations of the watchdog identified are discussed below:

Advantages

- The watchdog technique is efficient in building security management systems [32].

- The watchdog technique supports collaboration between multiple watchdogs [111]. Collaboration between watchdogs enhances the system's security as the detection process when shared between neighbouring watchdogs. An additional benefit of collaborative watchdog use is that it can assist in detecting malicious behaviour that may be invisible to a particular vehicle.

Limitations

- The watchdog technique does not perform optimally in high-mobility scenarios [112]. Due to the high mobility, the watchdog can report false positives in the VANET, directly degrading the system throughput and performance [112], [113].

- The watchdog technique introduces much resource consumption to watchdogs [32]. Resource consumption directly contradicts the energy-efficient design principle in VANETs. Therefore energy efficient techniques are essential for optimal watchdog selection and application. Watchdogs must operate using algorithms that provide minimal overhead operation [109].
- Watchdogs are limited by the vehicle's coverage area or node that activates the watchdog agent. This coverage problem means that a single watchdog cannot monitor a large-scale area.

The main principle behind the watchdog technique is that a watchdog agent is installed on all vehicles in the VANET. The agent can then be dynamically enabled to monitor its neighbours' communications. The watchdog agent is activated via various techniques; it can decide based on predetermined patterns or rules [109]. The watchdog agent is only installed in predefined nodes and no other nodes in the network [109]. In this system, the watchdog agent is activated only where it is installed. Another technique used to activate the watchdog agent involves using the already selected cluster heads and activating the watchdog agent on the cluster heads [114]. Another identified technique is watchdogs are selected as all the vehicles in the VANET; in this scenario, each vehicle is responsible for monitoring its neighbours' communications [108]. Watchdogs are only enabled as any vehicle that is a packet source in the VANET [115]. In this instance, once a vehicle sends a packet, it automatically becomes a watchdog to watch the vehicle transactions to which it sent the packet. A further technique identified involves selecting watchdogs according to where an event occurs [116]. Once a vehicle reports an event, its neighbours are selected as watchdogs to monitor the vehicle.

Several security schemes have selected watchdogs in their security design without considering malicious or non-malicious behaviour before the selection process [27], [35], [115]–[117]. However, randomly selected watchdogs, which are assumed as trusted, might be malicious and affect the performance of the security solution [18]. Some researchers have also noted that for a watchdog to function optimally, it should be secure and exhibit non-malicious behaviour [40], [42], [85]. Therefore, a security system's performance must ensure that only certain vehicles are selected. However, secure watchdog selection is one of the challenges experienced by security management techniques in VANETs. Table 2.4 below summarises the use of watchdogs for security management techniques.

Table 2.4 - Summary of watchdog selection techniques used in recent research.

Paper	Network Type	Selection technique	Secure selection	Fairness consideration
Towards a self-adaptive trust management	VANET	Watchdogs were selected according to where events occurred. The neighbours of a	It does not consider the behaviour of vehicles	Fairness is not considered in selecting watchdogs.

model for VANETs (2017) [109].		vehicle that has sensed an event are selected as watchdogs.	before the selection of watchdogs.	
Prevention of attacks on dynamic routing in self-organizing ad-hoc networks (2018) [112].	Self-organizing ad-hoc networks, including MANET, VANET, IoT and mesh networks.	All vehicles were considered watchdogs and could monitor each other in the VANET.	It does not consider the behaviour of vehicles before the selection of watchdogs.	Fairness is not considered in selecting watchdogs.
Using dynamic watchdog optimization technique for secure data transfer in MANET (2018) [32].	MANET	Dynamic watchdog allocation is based on the shortest communication path to the source of the message/packet.	It does not consider the behaviour of vehicles before the selection of watchdogs.	Optimizes watchdog frequency and redundancy, promoting fairness.
Hybrid trust management heuristic for VANETs (2019) [108].	VANET	Neighbours of vehicles involved in communications were selected as watchdogs.	It does not consider the behaviour of vehicles before the selection of watchdogs.	Fairness is not considered in selecting watchdogs.
A hybrid intrusion detection system against egoistic and malicious nodes (2020) [27].	VANET	Every vehicle that sends a packet automatically becomes a watchdog.	It does not consider the behaviour of vehicles before the selection of watchdogs.	Fairness is not considered in selecting watchdogs.
An anti-attack trust management scheme in VANET (2020) [38].	VANET	Neighbours of vehicles involved in communications were selected as watchdogs.	It does not consider the behaviour of vehicles before the selection of watchdogs.	Fairness is not considered in selecting watchdogs.
A reputation system using Bayesian statistical filter in vehicular networks (2020) [101].	VANET	All vehicles were considered watchdogs and could monitor each other in the VANET.	It does not consider the behaviour of vehicles before the selection of watchdogs.	Fairness is not considered in selecting watchdogs.
Entity-centric	Self-organizing ad-	All vehicles were considered watchdogs	It does not consider the	Fairness is not considered in

combined trust algorithm to prevent packet-dropping attacks in VANETs (2020) [111].	hoc networks, including MANET, VANET, IoT and mesh networks.	and could monitor each other in the VANET.	behaviour of vehicles before the selection of watchdogs.	selecting watchdogs.
A scalable blockchain-based trust management in VANET routing protocol (2021) [35].	VANET	Neighbours of vehicles involved in communications were selected as watchdogs.	It does not consider the behaviour of vehicles before the selection of watchdogs.	Fairness is not considered in selecting watchdogs.
Secure opportunistic watchdog production in wireless sensor network (2021) [102].	Wireless sensor network (WSN)	Every node that sends a packet automatically becomes a watchdog.	It does not consider the behaviour of vehicles before the selection of watchdogs.	Fairness is not considered in selecting watchdogs.

Another challenge experienced by watchdogs is that the watchdog process of monitoring exhibits higher computational and storage overheads leading to increased energy consumption [33], [110]. This increased energy consumption reduces the security management system's efficiency by using the watchdog technique. The optimal selection of watchdogs in a network can reduce resource consumption during monitoring tasks and improve the efficiency of the security management system [93]. Therefore, the selection process of watchdogs in the VANET must be optimised to reduce resource consumption. Optimization ensures the efficiency of the security management system, making use of the watchdog technique.

Cooperativeness between watchdogs enhances the effectiveness of security management techniques used for VANETs. Cooperation involves aggregating the evidence between watchdogs and making cooperative decisions [64]. Cooperative watchdogs have several advantages to security systems, including cooperative watchdogs can help reduce the rate of false positives in the VANET [118]. In some scenarios, attacks can deceive watchdogs into reporting false information [18]. Cooperativeness between watchdogs can be advantageous in identifying watchdogs that have been deceived.

The watchdog mechanism in security management systems performs monitoring tasks. Monitoring network activities is an integral part of the security management system. It is, therefore, important that the watchdog mechanism is secure against malicious activity. Monitoring activities consume higher storage and computational resources. It is essential that the watchdog selection process is optimised to reduce resource consumption in the VANET. The above challenges presented motivation for

designing a watchdog selection scheme that includes secure, fair, and cooperative watchdog selection.

2.13. False positives

False positives are experienced in watchdog and trust management systems developed for VANETs. False positives occur when vehicles are identified as malicious, yet they exhibit non-malicious behaviour; this can be identified as false alarms in the VANET. False positives can occur due to a variety of reasons. Using a watchdog system may sometimes fail in a complex network by generating false positives, which may lead to performing wrong operations [112]. False positives can also occur in a bad-mouthing or defaming attack. In a defaming/bad-mouthing attack, a vehicle can generate false trust scores for an honest vehicle making it seem malicious [35]. False positives not only decrease the accuracy of detection and evaluation of a security management system. They also decrease the efficiency of the security model. Providing minimal false positive rates in the VANET is a requirement for security management systems developed [78]. Reducing the false positive rate improves the accuracy of the security management system in detecting malicious vehicles. A method to detect false positives within trust models improves the accuracy of assessment and evaluation results [8]. The ability of a trust model to also have identified false positives also improves its efficiency of the trust model [8].

2.14. Summary

The concluded chapter has discussed VANETs and their applications while highlighting the importance of their safety applications. It has looked at the architecture of VANETS, concentrating on the two primary forms of communication: V2V and V2I communication. These two forms of communication will be utilized in the proposed trust management system. It also looked at the communication protocols used in VANETs, and the security requirements required to provide reliable, efficient, and optimal communication. The attacks that threaten these security requirements have been discussed in detail—state-of-the-art security schemes developed to deal with malicious vehicles in VANETs. The effect of these attacks is that malicious vehicles in the network lead to delays or the dropping of critical information in the VANET. These could lead to increased traffic and even more severe injuries or loss of life.

The chapter focused on trust management schemes as security systems against malicious vehicles. Trust management systems must satisfy the following conditions to be highly effective: simple, light, and fast while being robust, efficient, and providing anonymity. Trust management makes use of a variety of techniques to achieve its core objectives. The use of watchdogs to perform monitoring tasks is one of the popular techniques used in trust management systems. The popularity is because the watchdog technique has been proven highly effective in monitoring tasks. However, some challenges exist in selecting secure watchdogs and ensuring fairness in the watchdog selection. These challenges are crucial when using the watchdog technique in trust management systems. The occurrence of false positives was also discussed in this chapter. False positives decrease the accuracy of detecting and evaluating malicious vehicles. False positives also decrease the efficiency of trust management systems, decreasing the efficiency of the VANET.

Due to the abovementioned conditions, the watchdog selection process and trust calculation and evaluation have become increasingly important in designing a trust management system. The above factors determine the accuracy and efficiency of the trust management system. These factors motivate designing a multi-tier trust management system that addresses all the above concerns.

The literature survey and background provided in this chapter enhanced the deep understanding of the research presented in this work. A summary of the chapter and its addition to knowledge is given below:

- It strengthened understanding of VANETS, techniques and technologies used in VANET communication. This further enhanced the understanding of the benefits of efficient security management techniques for VANETs.

- It enhanced understanding of the requirements of VANET security management systems. It also included the current state of proposed VANET security management techniques, which identified gaps in the literature that could be filled. This further shaped the strategies for designing the proposed multi-tier trust-based security management techniques.

- It enhanced the understanding and identifying attributes of vehicles that could represent malicious or non-malicious behaviour. This influenced the attributes and metrics the proposed system would employ to identify vehicle behaviour.

- It added to understanding watchdog selection strategies and the factors that influence them. It included the current state of watchdog selection strategies, advantages, and limitations. This identified gaps in watchdog selection strategies that the proposed system could fill.

- Strengthen understanding of the challenges and limitations experienced in applications of trust management systems. It supported the understanding of trust management systems applications. An additional benefit is that it assisted in predicting challenges experienced in applying the multi-tier trust-based system proposed.

- It added to the knowledge in developing scenarios for evaluating the proposed system. After developing the proposed system, testing and evaluation in complex scenarios are necessary to validate the system.

The summary mentioned above directly influenced the proposed system in this work. The following chapter discusses the methodology used in designing the proposed multi-tier trust-based management system, and the following chapters expound on this concept.

3. Methodology

3.1. Overview

This chapter introduces the research methodology used in this study, giving readers a clear understanding of how the research was conducted. The chapter will also help future researchers know the precise steps to replicate the study. The chapter will begin with a brief introduction to the research questions mentioned in Chapter 1. The chapter will also discuss the methods, tools, techniques, and data used to meet the study's objectives and aims. Hardware components and software requirements are identified to achieve study outcomes. The model development and analysis tools are identified for planning to achieve study results. The steps taken to source data, analyse it and apply it to the project are discussed. A summary of the expected outcomes concludes this chapter.

3.2. Study design

The study design utilized to complete the proposed model featured the following activities. Data collection from various sources and experiments was carried out during various phases of the study. Simulation modelling and simulation analysis were utilized to develop VANETs used in the study. Using simulation modelling, scenarios were identified for which the algorithm was applied to evaluate the proposed system. Simulation analysis assisted in identifying optimal trust factor and watchdog selection, which was paramount for trust management system design. It also contributed to the design of the simulation of false positives and recovering malicious vehicles. Following simulation modelling and analysis, an intelligent algorithm for the trust management system was designed. Experimental testing was then employed to verify the algorithm design and evaluate the proposed system in different complex scenarios.

The structure described below was employed by several security management systems designed for VANETs [27], [28], [36], [65]. The structure consists of the following steps.

1. Defining of project goal – This usually consists of defining the project's title, research questions, aims, and objectives. The project goal is defined in the introduction chapter.

2. Problem definition – The study background is defined and explained, including the current state of the related work. The study identifies gaps in the literature, leading to the problem statement's description.

3. Data gathering – This involves the collection of data related to the project. Data is collected via various methods, usually by reviewing the literature related to the project—an experimental data-gathering technique used.

4. Simulation modelling and analysis – this involves defining the scope of the study, the assumptions made in the study, the project variables, the network models, the use case scenarios, and the identification of simulation tools.

5. Algorithm design – This involves the design and description of algorithm components. Algorithm design includes any variables and equations used in the study.

6. Simulation experiments – the study's proposed design comprises the algorithms applied to complex scenarios and models. Simulation experiments were used to evaluate the proposed system.

7. Results analysis and evaluation – the results of the simulation experiments are analysed and discussed in detail. This work presents results using tables and graphs.

Table 3.1 below summarizes some security management systems that employ this similar structure.

Table 3.1 - Study design used in the following current state-of-the-art security management systems for VANETs.

Trust management system	**Study design**
VANSec – Attack-resistant VANET security algorithm in terms of trust computation error and normalized routing overhead (2018) [65].	Project goal definition Problem description Data gathering Simulation modelling Algorithm design Simulation experiments Results analysis and discussion
Toward a distributed trust management scheme for VANET (2018) [36].	Project goal definition Problem description Data gathering Simulation modelling Algorithm design Simulation experiments Results analysis and discussion
A hybrid trust management heuristic for VANETS (2019) [27].	Project goal definition Problem description Data gathering Algorithm design Simulation experiments Results analysis and discussion
StabTrust – A stable and centralized trust-based clustering mechanism for IoT-enabled vehicular Ad-Hoc Networks (2020) [28].	Project goal definition Problem description Data gathering Simulation modelling Algorithm design Simulation experiments Results and analysis
A kind of event trust model for VANET based on statistical method (2021) [88].	Project goal definition Problem description Data gathering Algorithm design Simulation experiments Results and analysis

3.3. The rationale for the selected methodology

The methodology used in this work will be inspired by reviewing state-of-the-art security systems. The strengths of the selected methodology can be attributed to the successful design of trust management systems in [27], [28], [36], [65], [88], which employed similar methodologies. Additionally, quantitative data was collected via experiments to identify patterns and correlations. The type of data used influenced the methodology selection. The research objectives also aligned with the chosen methodology, which was further attributed to the selection of the chosen methodology in the study.

Figure 3.1 summarizes the study design. The study design led to several stages of development. Figure 3.2 describes these development stages.

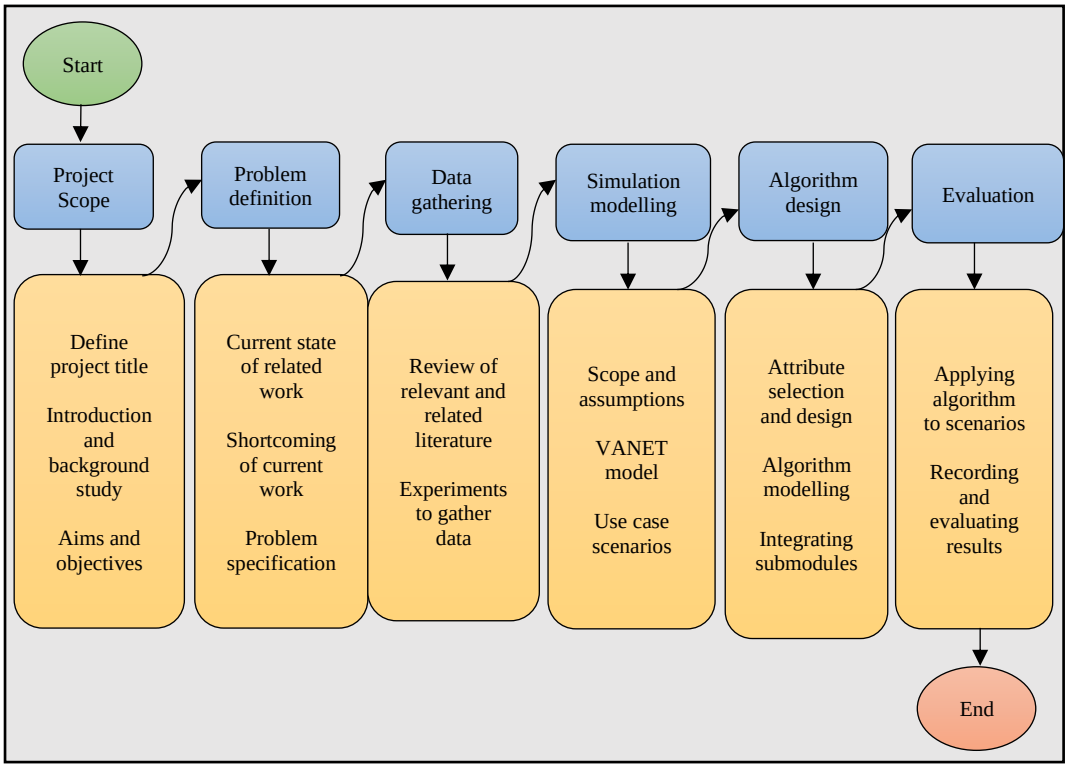

Figure 3.1 - Summary of the proposed study design used in this thesis.

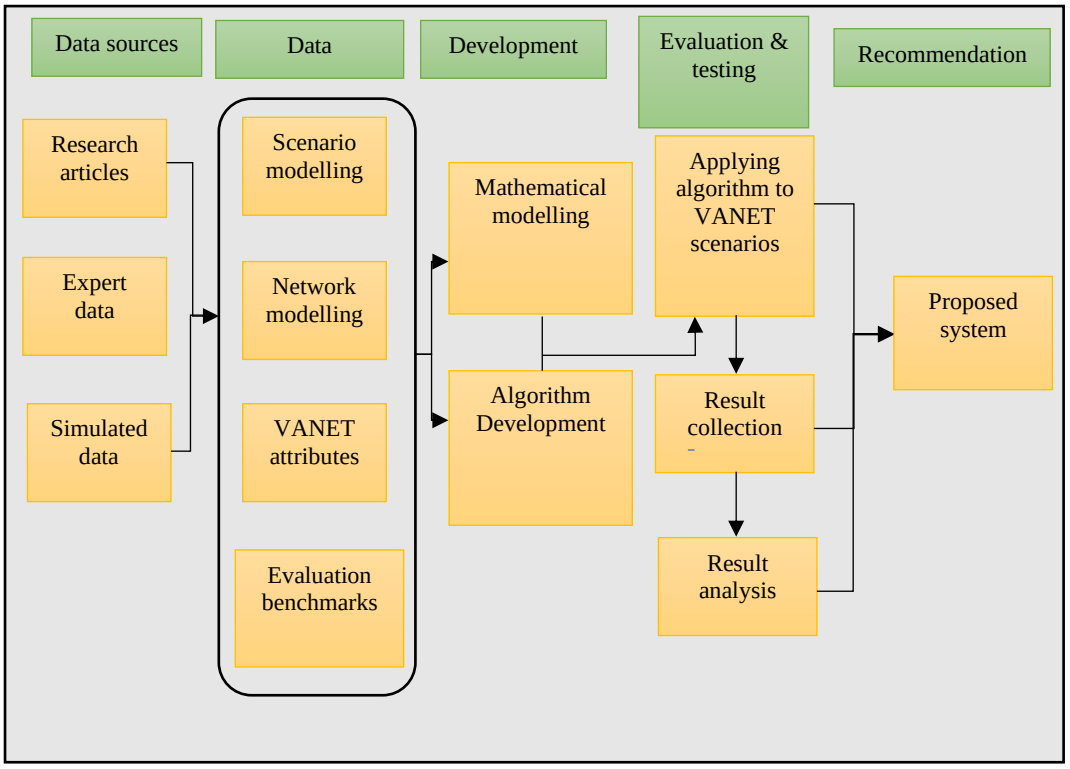

Figure 3.2 - Proposed summary of algorithm development stages used in the study.

3.4. Data sources

The following section will outline the data sources used in the design of the proposed system.

Articles and journals

Identifying appropriate data sources was the first step in designing the proposed system. Identifying and defining the scope of data collection were integral in avoiding the collection of obsolete data that would be unusable for the thesis. The data sources used in this project were research papers and journals published by researchers and experts in VANETs. Using previous researchers' work provided an expert opinion on the scope of VANETs, attacks on VANETs and security proposals against attacks on VANETs. The research selected state-of-the-art security management systems relevant to the study. The time scope included research conducted within the past five years. This scope ensured that only the latest literature reviewed was relevant for this time. The journals were sorted from online repositories such as ResearchGate, IEEE Xplore, Elsevier/Science Direct, Springer and SAGE journals.

Expert sources

Expert sources included the practical applications of VANETs in real-life scenarios. They identified real-life attributes of VANETs that modelled the simulation and scenarios. Expert sources provided relevant real-life information considered in the design of the system. Some expert sources included the international organization of motor vehicle manufacturers (OICA) and the European automobile manufacturers association (ACEA). These were relevant in acquiring the latest statistics and information on vehicle development.

Simulated data

Simulated data consisted of data generated and obtained from the simulation environment. The proposed system was applied to a VANET in various defined scenarios—the data and results generated, observed and recorded. The data collected from various sources aided the development of the proposed system. Further details on how data will influence the development are shown in

Figure 3.3. In addition, the data collected from experiments improved and enhanced the system. Storage and management of data to enable further analysis and identification of significant patterns that will aid the research is crucial. The data management techniques made use of in the research are discussed below.

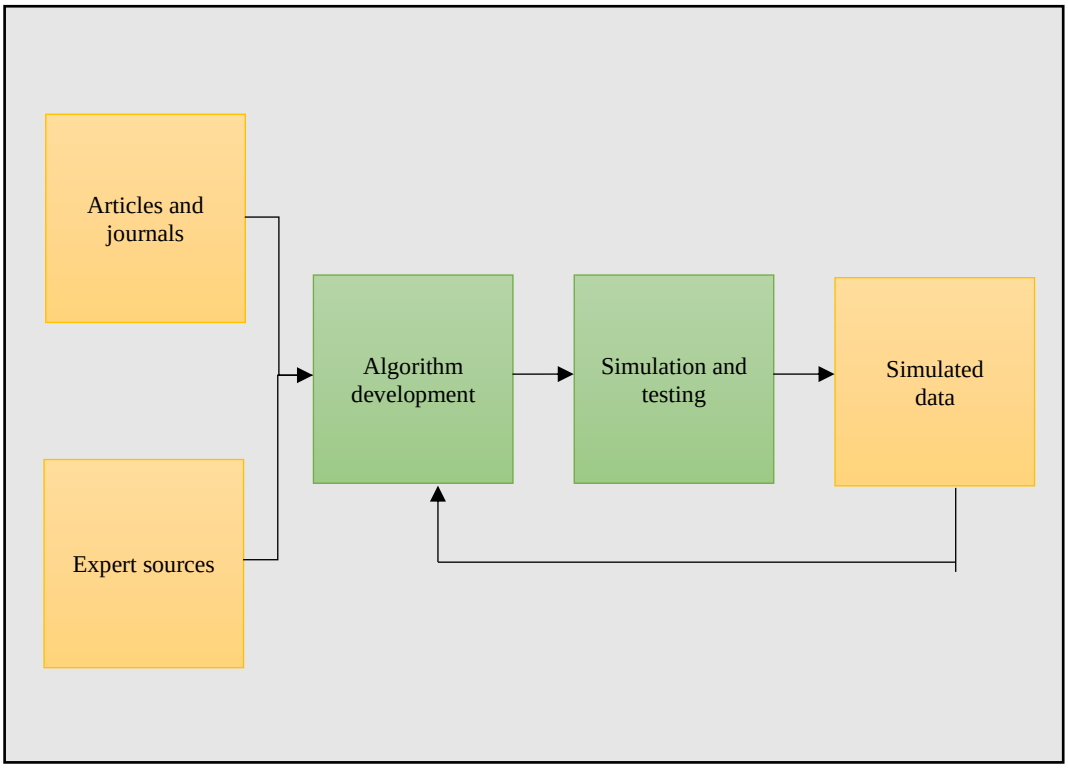

Figure 3.3 - Data details showing how data aided the thesis's development.

3.5. Data management

Data management involves two different aspects: document storage tools and reference management tools.

Document storage

Microsoft one drive was the primary tool used to store journal articles, research documents, image files, simulation data, and simulation code, with a secondary storage point being the principal researcher's computer. The reason for the two points of data storage is data redundancy in case of data loss from one of the data storage sources. Microsoft one drive provides features such as; preinstalled security features

that offer data protection. The researcher's computer is password protected for data protection and privacy. The security measures ensured that all research data was safe and secure. Microsoft one drive also provides cross-platform data availability and access.

Storage format – The journal articles collected as part of the background study and literature review were stored in PDF format—simulation experiment source code was stored in C++ format. At the same time, the simulation results were stored and analysed in the simulator-specific format. Further analysis of simulation results was conducted via Microsoft Excel and Python. Hence files were stored in CSV and python (.py) format.

Result file format – The simulation results were stored in textual, line-oriented files. OMNET++ did the data storage, and the main advantage of this text-based line-oriented format is that it is accessible and easy to parse with a wide variety of tools and languages. While still providing enough flexibility to represent the data it needed. The numerical data were exported to CSV and JSON files and enabled results analysis and graphs plotted via Python and Excel.

Reference management

Reference management was performed by the reference management tool Mendeley. The tool selection was the researchers' preference and ability to store articles in the application. It can add articles via drag and drop (Digital Object Identifier) DOI reference and from internet sources. Mendeley also has automatic document lookups to enhance the accuracy of citations. It also features a Microsoft Word plugin that provides automatic synchronization between different documents. It is noted that software such as Zotero and RefWorks may provide the same features that Mendeley does; therefore, the primary researcher selected Mendeley due to its perceived ease of use.

This data collection and management enabled simulation modelling. Simulation modelling identified the assumptions used in the study, the data range, and the relationship between the data and network models. Simulation modelling is discussed further below.

3.6. Simulation modelling

This section will define various factors involved in the simulation design and experiments. The areas covered in simulation modelling included the network model design, the assumptions made by the thesis, parameter specifications, variable definitions, performance metrics, and tools used at various project stages.

Tool Selection

Various tools were required to achieve the defined objectives during the different stages of conducting this study. Different tools were studied and reviewed to select the most optimal tools. Further discussion of the tools follows below.

Operating system

The operating system selection was based on the researcher's preference and ease of use. Windows 10 was used for the proposed thesis's writing, simulation, and results analysis.

Writing tools

Several writing tools could be selected, and the following tools were selected based on the researcher's preference.

Microsoft Word – This was used for all the writing work done during the thesis. Tables and images were also presented using Microsoft Word.

TexMaker – This is a latex client for the Windows operating system. Latex was used for writing the equations that make up the intelligent algorithm.

Overleaf – This designed the equations and algorithms used in the proposed system. Overleaf will also be used in writing up publications.

Draw.io – This free online and desktop client is used for flowcharts, process diagrams, charts, and network diagrams. The motivation for using draw.io is that it is open-source software that provides quality figures.

Simulation tools

In order to perform the VANET simulations, the OMNET++ simulator was selected. Several other tools considered for this purpose include MATLAB, NS3, OPNET and NS2. OMNET++ was selected for this purpose based on the following advantages [119], [120]:

- OMNET++ is open source and free to use. This feature is a significant advantage as it means no extra costs are needed to build the algorithms and simulate the VANET.

- OMNET++ is one of the fastest simulators in the domain of wireless networks [120].

- Several simulation models and model frameworks have been built on top of OMNETT++ by researchers in diverse areas such as MANETs, mesh networks, WSNs, resource modelling and vehicle networks. Therefore, it shows OMNET++ is successful in providing a simulation environment.

- OMNET++ provides up-to-date pdf documentation and regular updates, adding more features and improving the simulator.

- OMNET++ contains inbuilt documentation and result analysis components, so results do not need to be exported to third-party software to be analysed.

- OMNET++ has a graphical user interface (GUI) that enables the visualization of simulations. This help in understanding highly complex simulations.

As part of OMNET++, the INET framework is also used in the simulation. INET framework is one of the most comprehensive and helpful model frameworks, and it provides protocols, agents, and other models for working with communication networks. It is beneficial when designing and validating protocols or exploring exotic scenarios. INET framework can also be extended to suit different directions; for example, it can be extended to suit VANETs.

Data visualization tools

Data visualization tools are crucial to displaying and analysing results from the simulation. Data generated from the simulation was stored within the simulation environment. Furthermore, necessary online backups were made. OMNET++ has built-in result-recording tools for simulation results via output scalars and vectors. While output scalars are a summary of results computed during the simulation and written after the simulation ends, e.g., the total number of packets received/sent. Output vectors are time series data recorded from the simulation, e.g., end-to-end delay, round time of packets, queue lengths and packet drops.

For further sophisticated analysis and if customized reports were required, OMNET++ allows exporting results in python format for use in Python or (R) programs such as NumPy, SciPy and MatPlotLib.

OMNET++ also contains a tool known as a scavetool which can filter and export results in formats understood by other tools, e.g. CSV format for excel files.

Intelligent algorithm development

In order to develop the intelligent algorithm, a high-level programming language had to be selected. The selection of the simulation tool significantly influenced the algorithm development, as the algorithm was developed in the simulation tool IDE. The algorithm was developed in a C++ environment. NED language is a high-level programming language unique to OMNET++, and it describes the network structure to be simulated [119].

Network modelling

The scope of the network developed is a VANET with several vehicles as members of the VANET. The VANET existed with regular vehicles which sensed data in the environment and forwarded the data to intended destinations. A malicious agent exists that can be activated on vehicles. The malicious agent enabled the vehicles to behave maliciously; this represented vehicles performing various attacks in the VANET. Different types of malicious vehicles existed in the VANET: one type dropped messages instead of forwarding them to the intended destination. The other type of malicious vehicle delayed messages instead of forwarding them to the intended destination. The malicious vehicles represented different attacks in the VANET. A watchdog agent existed that could be applied to vehicles in the VANET. The watchdog agent enabled vehicles to monitor their neighbour transactions. The VANET also

consisted of an RSU, representing the TA in the VANET. The RSU was responsible for performing complex computations and oversaw managing vehicle security in the VANET.

Performance metrics

The purpose of performance metrics was to evaluate the proposed security scheme to prove the proposed system's functionality. Performance metrics will enable improvements to be made to the proposed system. The following performance metrics were considered:

Ability to identify malicious vehicles – The first metric used to validate the objective function of the proposed system is its ability to distinguish between standard vehicles and malicious vehicles in the VANET. This metric has been used by researchers in their proposed systems [27], [38], [116]. Malicious vehicles should be identified and ranked lower in the VANET than non-malicious vehicles.

PDR – The ratio of successful messages received to the total messages sent in the VANET. It is an indicator that a VANET is facilitating successful message delivery. PDR has been used as a performance metric in [2], [9], [68]. The PDR was evaluated when the proposed system was applied to a VANET with malicious vehicles.

Delay/Time taken to deliver messages – The average time vehicles take to deliver messages in the VANET. Vehicles in the VANET do not spend much time together in the same VANET; therefore, message delivery should take the least time possible. The proposed system was applied to a VANET with malicious vehicles, and the delay was evaluated. Figure 3.4 shows the relationship between the different stages of the simulation modelling phase. The following section shall detail the algorithm development stage.

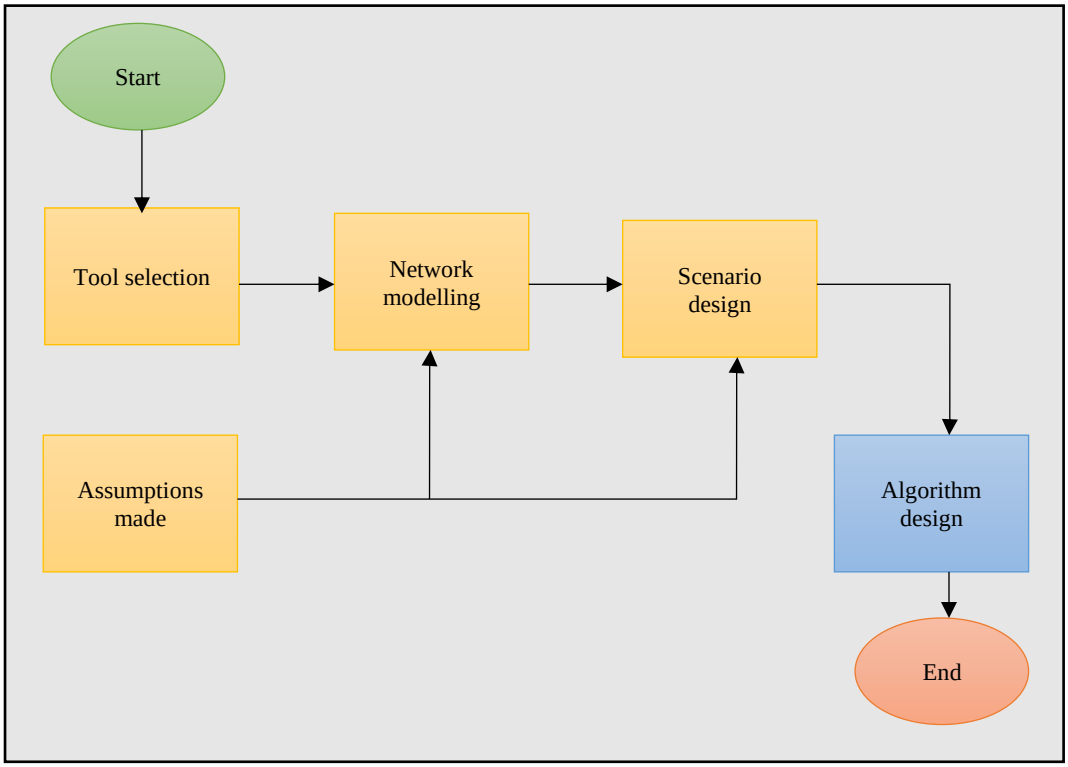

Figure 3.4 - Proposed simulation modelling stages used in the design of the proposed system.

3.7. Algorithm development

In order to develop the intelligent algorithm that will make up the trust management system, various approaches were used, including experimental analysis, a stepwise approach and a stepwise refinement approach. The stepwise approach to developing the algorithm included dividing the overall goal into smaller submodules. The smaller submodules were developed and evaluated via experimental analysis. Stepwise refinement was applied by adding details to the smaller submodules, increasing their complexity and functionality. The submodules were integrated to form the high-level algorithm. Initial experiments were run on the high-level algorithm to test for integration within the submodules. Criteria were defined to develop benchmarks to measure the proposed algorithm's effectiveness and success. The benchmarks were related to the study's objectives and benchmarks set by other trust management systems that other researchers have proposed.

The algorithm was developed in C++ and used OMNET++ as the integrated development environment. The following developments and experiments were planned during the algorithm development phase:

- The identification and selection of vehicle attributes to represent vehicle behaviour. It is developing the equations to calculate trust value from vehicle attributes. It included intelligent methods to identify false positives and malicious vehicles recuperating to non-malicious behaviour.

- Developing algorithms for the watchdog agent. The watchdog agent allowed the vehicles to monitor the vehicle neighbours' transactions. The watchdogs monitored vehicles within their communication range.

- The development of algorithms for secure and fair watchdog selection in the VANET.

- Developing algorithms for the RSU that enabled management of the trust values for vehicles in the VANET.

- Integrating the submodules mentioned above forming the complete multi-tier trust-based security management system.

Figure 3.5 shows the different components that make up the algorithm development stage. It also demonstrates how the different stages relate to each other to create the proposed system.

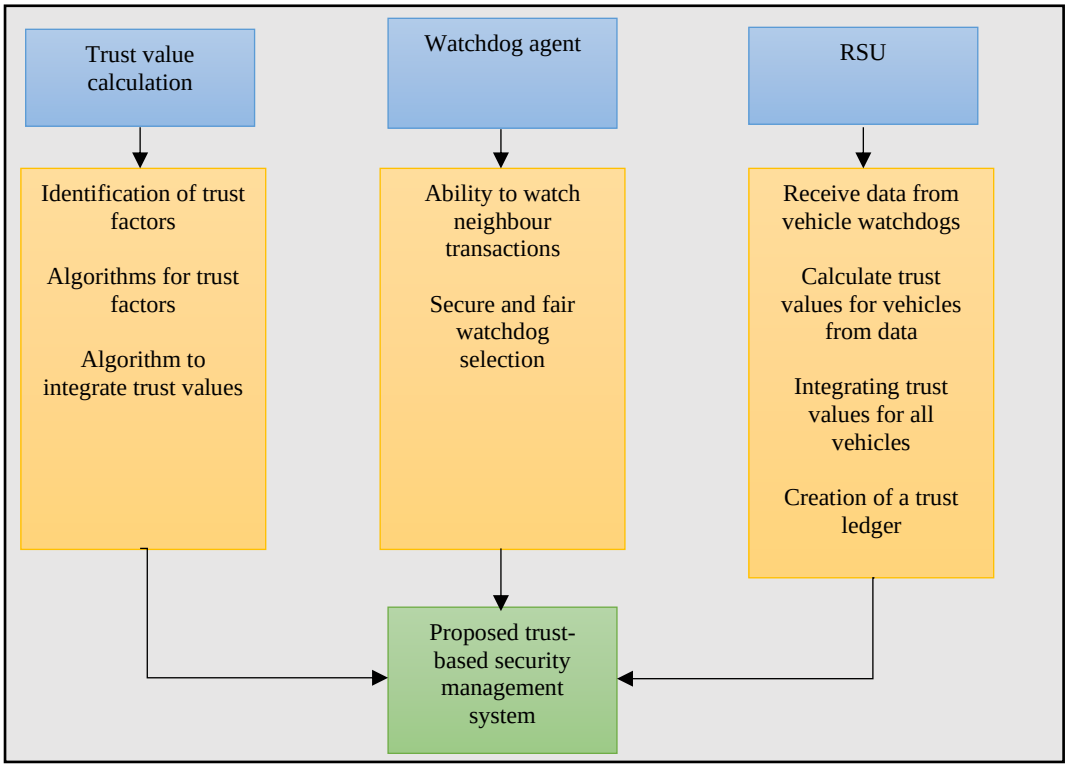

Figure 3.5 - Proposed algorithm development stages and how the different stages interact.

3.8. Experimental analysis

This stage involved applying the proposed system to a VANET and evaluating various scenarios and use cases. Evaluation of the proposed system was performed using defined benchmarks. These benchmarks were defined from real-life scenarios as references. The proposed system was executed to determine the success criteria and evaluation parameters. Stepwise refinement was used to add features to the proposed trust management system after evaluation to enhance the system. Figure 3.6 summarises the experimental analysis process.

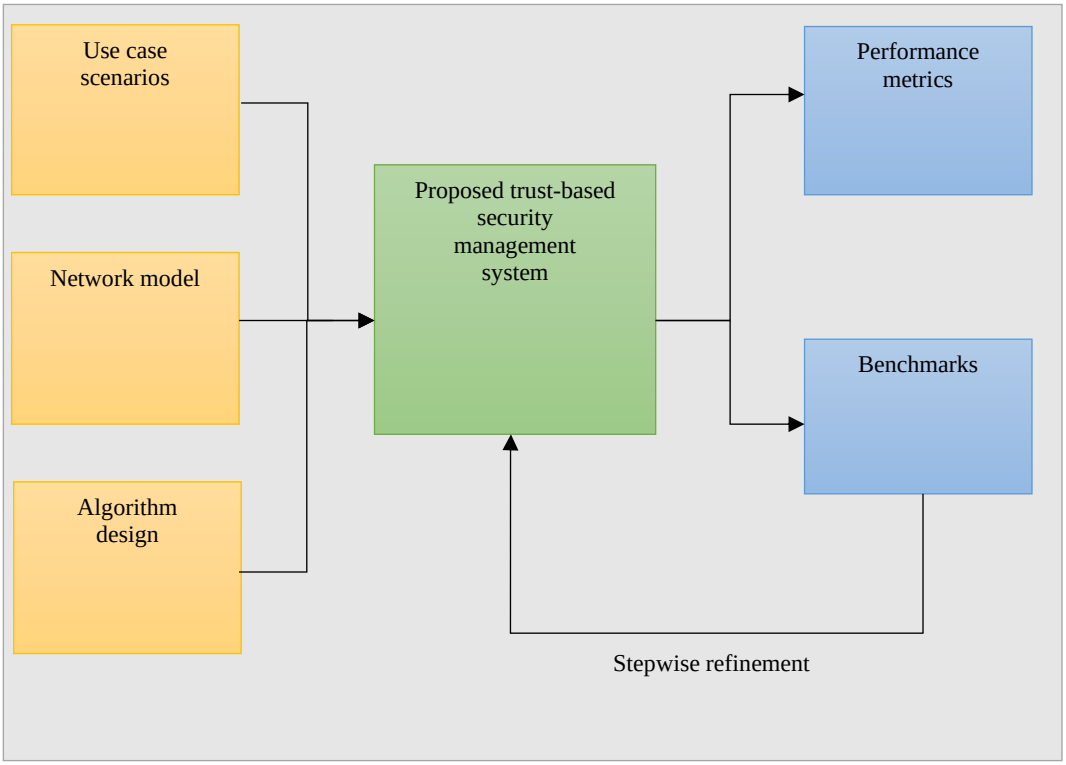

Figure 3.6 - Proposed experimental analysis process used to create the proposed system.

3.9. Model design

The objective functions of the proposed system highly influenced the model design. The model's objective function was to identify malicious vehicles in the VANET. Malicious vehicles were isolated during network communications to improve the PDR and minimize the delay. Therefore, identifying malicious and non-malicious vehicles forms the primary function of the proposed system.

The second objective function that influenced the model design is the reduction of resource consumption by reducing the storage and computational overheads incurred by the proposed system. The functions were divided among different vehicles and the RSU. The proposed system, therefore, took a federated model design. Federation ensured the proposed system achieved its objective of identifying malicious vehicles while minimizing resource consumption in the VANET.

The following section will look at the functions of some of the state-of-the-art trust management systems proposed recently. This analysis will lead to detailing the functions of the proposed system.

3.10. Functions of the proposed system

The primary objective function of recently proposed state-of-the-art trust management systems developed was to identify malicious and non-malicious vehicles in the VANET [8], [85], [91], [121]–[123]. By identifying the honest and malicious vehicles, the trust management schemes also assisted in identifying false messages in the VANET, which improved the accuracy of data and ultimately enhanced the security of the VANET. At the same time, some trust management systems have only focused on one primary objective: identifying malicious and honest vehicles [40], [106]. Some trust management employed additional functions in addition to their primary function.

Additional functions improved trust management systems by providing extra security features. The work in [121] had secondary trust management system functions that reduced the computational trust error, defined as the mean square error between predicted/calculated trust values and known/observed trust values. Reducing the computational trust error improved the reliability of the trust management scheme. End-to-end delay, the time taken for alert messages to travel from the source vehicle to the destination vehicle, can improve the trust management scheme by providing fast trust evaluation. Providing low delay has been used as a secondary function of the trust management schemes in works by [26], [121]. The work in [91] also aimed to improve the reliability of their trust management system as a secondary function. Fairness was used as a secondary function of the trust management system in the proposed system [122]. In their work, they also aimed to improve the traceability of the detection process in the trust model they proposed. In addition to identifying malicious vehicles, [123], [124] improved the energy efficiency of their trust management scheme by making it more energy aware in its functionality. Their proposed system aimed to balance energy consumption with their trust management scheme. [85] aimed to provide authentication as a secondary function for vehicles in the network and trust management in the VANET. Improving resource utilization by reducing resource consumption is an additional function of the trust management system suggested by [27]. Low network overhead is another function of the trust management system proposed in [27]. Table 3.2 below summarizes all the functions of trust management systems, in addition to identifying malicious and non-malicious vehicles.

Table 3.2 - Summary of the reviewed trust management systems and their functions.

Trust management system	Objective functions
A Secure Routing Protocol with Trust and Energy Awareness for WSN (2016) [124].	Reduce the energy consumption of the trust management scheme.
Using trust model to ensure reliable data acquisition in VANETs (2017) [26].	Providing reduced delay in calculating trust values.
Trust management scheme in VANET: Neighbour communication-based approach (2017) [38].	Provide authentication in addition to trust management.
ARV2V: Attack resistant vehicle to vehicle algorithm, performance in terms of end-to-end delay and trust computation error in VANETs (2018) [121].	• Reliability of trust management scheme. • Providing low delay in calculating trust values.
Secure and stable Vehicular Ad Hoc Network clustering algorithm based on hybrid mobility similarities and trust management scheme (2018) [91].	Reliability of the trust management system.
A Hybrid Trust Management Heuristic for VANETs (2019) [27].	• Reduce the network overhead of the trust management system. • Reduce the resource consumption of the trust management system.

Blockchain trust model for malicious node detection in WSN. (2019) [122].	Fairness of the trust management scheme.
An Energy-Aware Trust Based Secure Routing Algorithm for Effective Communication in WSNs (2019) [96].	Reduce the energy consumption of the trust management scheme.

The primary objective function of the proposed trusted management in this work remains to identify honest vehicles in the network in the presence of malicious vehicles. The proposed trust management system employed non-complex calculations to provide quick and reliable vehicle trust value calculations. The trust values distinguished between malicious and non-malicious vehicles in the VANET. A federated model in design ensured that the proposed system achieved its secondary objective function. Therefore, the secondary objective function of the proposed trust management system was defined as reducing storage and computational overheads, which led to reduced resource consumption. In order to reduce resource consumption, accuracy and efficiency must be accomplished by the proposed system. Achieving accuracy created the additional function of identifying false positives and recuperating malicious vehicles in the VANET.

The trust management system used a watchdog agent in its operation; this created additional functions for the system. Due to the dependence on highly accurate data from the watchdogs, protecting the watchdog agent against malicious vehicles is crucial. A malicious watchdog can cause failures and inaccurate reporting by the proposed system. Protecting against malicious watchdogs created the additional function of secure watchdog selection and management in the VANET. This function ensured that the watchdog agent was only activated in non-malicious vehicles. The proposed system had additional controls to protect against malicious watchdogs during the trust value calculation phase. The watchdog agent also adds additional resource consumption to the VANET. Additional resource consumption goes against the proposed system's goal of minimizing resource consumption in the VANET. A fairness mechanism was introduced during the watchdog selection process and ensured the watchdog agent did not drain a vehicle's resources during operation.

In addition to the above functions, the proposed system protected the integrity of the calculated trust values representing vehicle behaviour. Additional controls will do this during the trust calculation phase.

The following section will look at the assumptions made during the model design of the proposed system.

3.11. Assumptions

While creating and simulating trust management systems, assumptions are necessary to simulate real-world scenarios. As long the assumptions made do not affect the validity of the proposed systems. This section shall examine the various assumptions state-of-the-art trust management systems have made in their design. Assumptions made in the study were briefly mentioned in the methodology section, but detailed explanations are given below. In the design of the following trust management system, the following assumptions were made [42]:

- Multiple vehicles sensed the same alert, which, when compared, provided the ability to detect if any vehicles had sent false information.

- Most vehicles in the network were honest, with minimal malicious vehicles present in the VANET.

- Vehicle sensors always read the correct information and send correct alerts unless tampered with by malicious actors.

- Every vehicle had its own personal private and public keys.

To design their trust management system, the following assumptions are made in both trust management systems [29], [68]:

- Adversaries cannot compromise more than half the vehicles present in the VANET.

- Authorities and RSUs in the VANET were equipped with higher processing and computing power than standard general-purpose computers.

- The law enforcement agency (LEA) had enough security levels such that it could not be malicious.

To detect Sybil attacks in a VANET, the trust management system proposed in [125] made the following assumptions about the vehicles and VANET:

- Every vehicle had a GPS with precise location accuracy at all times.

- Every vehicle had a computing platform with an equal level of computational power.

- Every vehicle equipped with an event data recorder (EDR) could record real-time event occurrences.

- Every vehicle had an equal transmission range for each vehicle.

- A single identity was available for each vehicle.

- There are no communication failures in the network; every message was transmitted successfully in the VANET.

While the trust model used in the VANET in the following work made the following assumptions [26]:

- All vehicles were equipped with all necessary tools, including a GPS module that enabled them to join and participate in a VANET.

- The communication range of vehicles was 200m, and all communications within a 20m range were perceived correctly.

- All vehicles were time synchronized and were in the same time zone.

The trust management system proposed by [87] had the following assumptions to make their system work:

- The vehicles and servers assumed a secure communication channel, so trust evidence cannot be intercepted.

- The central authority is assumed to be fully trusted and attack resistant.

In Stabtrust – a stable centralized trust-based clustering mechanism for VANETS there were two primary assumptions made for the trust management system to work [28]:

- The vehicles were capable of LTE and 802.11p communication.

- All vehicles were equipped with a GPS module.

Assumptions can be made about the VANET and vehicles that belong to the VANET. As shown by the above examples, assumptions are necessary to build and simulate a trust management system in a VANET. The assumptions made in this work are discussed below:

<u>Assumptions on the VANET</u>

1. The RSU was assumed to be a TA in the VANET – This TA will not be influenced by attackers and remain trusted throughout the whole VANET operation. The TA was responsible for managing the trust values for all vehicles in the VANET.

2. Densely populated trusted Authorities were assumed in the VANET – This assumed that the setting of the VANET application had trusted authorities widely distributed.

<u>Assumptions on the vehicles in the VANET</u>

1. Vehicles are assumed to be equipped with computing modules, smart sensors, wireless communication modules, and GPS systems – This enabled vehicles to join a VANET and communicate with other vehicles accurately.

2. Vehicles were assumed to have the same processing and computing power, meaning that vehicles took the same amount of time to process and forward packets in the VANET. The vehicles had the same behaviours unless influenced by a malicious vehicle.

3. Vehicles were assumed to communicate with the latest communication protocols – Vehicles communicated using DSRC, WAVE technology, and based on the IEEE 802.11p standard and operated in the 5.9GHz frequency.

4. Vehicles had a single identity – Vehicles in the network had a numeric ID that does not change during VANET operations and can be used to identify vehicles. The ID is only available to the TA.

3.12. Malicious activity detection

Several types of attacks can be perpetrated against VANETs; it is, therefore, impossible to protect against every attack. At the same time, it is vital for a trust management system to not only protect against one specific attack but should be scalable to protect against multiple types of attacks [107]. However, some researchers have proposed trust management systems against specific attacks, such as trust management systems built to provide privacy for vehicles in the VANET [2]. A trust management system was proposed to protect vehicles against gray-hole attacks in the VANET [45]. Other trust management systems have been proposed against dishonest and malicious vehicles [40], [65], [126]. In comparison, some trust management systems have also been designed to deal with forged messages or false event messages in the VANET and ensure message integrity [26], [29], [106]. As mentioned above, trust management systems can be proposed to stop multiple types of attacks. Such as the one proposed in [85], which protects against malicious vehicles and the integrity of messages in the VANET. [66] proposed a trust management system that protected against multiple attacks: including falsified event information attacks, message modification attacks and fake message generation attacks. The percentage of malicious vehicles in the VANET varies between different applications. In [39], the number of malicious vehicles used was below 10%. 10% to 50% of malicious vehicles were used in [40], [87], [89], [91], [127], as opposed to [128], where more than 50% of malicious nodes are selected. The trust management system in this work selects malicious vehicles between 10% and 50%. The most popular range allows comparing and correlating other trust management systems with the proposed system. The trust management system proposed in this work protected against multiple attacks, making it robust. The system dealt with the following malicious attacks:

- It protected against malicious and dishonest vehicles in the VANET. These vehicles dropped packets instead of forwarding them to the correct destination. Therefore, any attack that led to vehicles dropping packets in the VANET.

- The proposed system offered protection against message modification attacks and fake message generation attacks in the VANET. Hence, the system detected any attacks that led to message alteration by malicious actors.

- It also protected against message delays in the networks caused by attacks. Consequently, any attacks that led to message delays in the VANET were detected.

3.13. Vehicle attributes

The main goal of trust management systems in VANETs is to use specific attributes of vehicles to distinguish between malicious and non-malicious vehicles in the network. The selection of vehicle attributes is a significant part of the trust management system to achieve objective and correct trust evaluation. The number of vehicle attributes also selected highly affects the resource consumption of the proposed system. There are two main methods of establishing trust factors, using the sensed data from the environment or using dedicated security messages to establish trust. Both methods will be looked at below, highlighting the benefits and limitations.

Using sensed data

It compares the information a vehicle shares regarding an event to determine if it is a malicious or non-malicious vehicle [27]. Various researchers have made use of the events sensed by vehicles and also reports sent by vehicles after the sensing of data to establish some vehicle attributes [26], [29], [61], [99. However, sensed data may contain safety or time-critical messages in the VANET. Using this data to establish trust values in the VANET may lead to some of these messages being passed to malicious vehicles and not reaching their destination. Therefore, the use of sensed data reduces the efficiency of the VANET.

This method's significant advantage is that no extra messages are needed to establish vehicle attributes as trust metrics. The method assists the trust management system reduce resource consumption in the VANET.

While the main disadvantage is that using sensed data to identify malicious vehicles can get access to messages containing sensed data before the identification of malicious behaviour.

Using dedicated trust messages

Dedicated messages involve using dedicated messages to establish vehicle metrics that establish trust metrics [38], [126]. It uses particular dedicated messages instead of sensed data to establish trust. The significant advantage of this technique is that when transmission of safety messages in the VANET, it is only transmitted to established honest vehicles. The safety messages transmitted in the VANET serve their purpose of safety and do not undertake additional tasks. The disadvantage of this technique is that extra messages are transmitted to establish trust in the VANET.

The proposed trust management system took the approach of using dedicated trust messages to establish trust. Lightweight trust messages were developed for the purpose of establishing vehicle attributes that represented trust. The messages were generated in the VANET and forwarded to vehicles. The messages were then used to extract vehicle metrics applied to equations to establish trust in the VANET. The reasons for selecting dedicated trust messages over the sensed data are listed below:

- The proposed system did not want to interfere with the objective functions of the VANET to which it is applied. The objective function of VANETs is to transmit safety messages, traffic warnings, and data sensed by vehicles.

- The specially dedicated messages were made lightweight, so they did not increase the resource consumption of the VANET.

- The proposed system's primary purpose was to ensure that sensed data transmitted in the VANET was at the correct destination and not intercepted by malicious vehicles. Using dedicated trust messages has the advantage of ensuring that sensed data was not used for any other functions.

The proposed system required vehicle attributes to be established from the behaviour of vehicles in the VANET. The trust metrics used in this trust management system are discussed below, including the reasons for selecting the metrics.

3.13.1. Packet delivery ratio as a vehicle attribute

The literature review defines PDR as the number of messages successfully delivered with the ratio of total messages sent. It can be used to examine whether a vehicle successfully forwards messages to the destination or drops them. The PDR of vehicles has been used in the following trust management systems to identify malicious vehicles [26], [28], [51], [107].

The proposed system used the PDR to identify vehicles that dropped packets. Vehicles generated trust messages in the VANET with the watchdog agent activated. The messages were forwarded to the destination vehicle via the vehicles with the watchdog agent not activated. Whenever a vehicle forwarded a message to the destination, the watchdogs could watch the transactions and record the number of messages received and successfully forwarded.

3.13.2. Processing delay as a vehicle attribute

Processing delay is the time taken to forward a message in the VANET. Processing delay was used to determine message integrity in the VANET. Message integrity refers to the fact that a message has not been forged or tampered with in the VANET. Determining the processing delay in the proposed system required the time to forward a message to the destination. Processing delay has been used to determine the trust values of vehicles in designing trust management systems [40], [91]. In the proposed trust management system, the watchdogs monitored the timestamps of the messages forwarded from the source to the destination vehicle. These timestamps were used to calculate the processing delay of vehicles in the VANET.

3.13.3. Consistency factor as a vehicle attribute

Consistency involves comparing data generated between neighbour vehicles or vehicles that generate correlated data to identify malicious vehicles. A comparison of correlated data has been used to identify malicious vehicles in trust management systems developed in [25], [91], [104]–[106]. In the proposed system design, consistency offered protection against malicious watchdogs. The data collected by watchdogs in the VANET was highly correlated if from the exact vehicle. The RSU compared this data to identify malicious watchdogs that fabricated data.

3.13.4. Vehicle history as a vehicle attribute

The proposed trust management system also considered the history of the vehicle. Vehicle history involved considering the vehicle's previous trust values and representing the vehicle's behaviour in previous communication rounds. Using the vehicle history helped counter malicious vehicles that tried to act normal for one communication round to fool the system. The RSU will store the previously calculated trust value that represented vehicles. The vehicle history was then integrated into the trust value calculation.

The above vehicle attributes determined a trust value representing vehicle behaviour. The trust value indicates whether the vehicle exhibits malicious or non-malicious behaviour.

3.14. Trust modules

VANETS contain components, including vehicles with different functions and RSUs. In this work, the VANET comprises different vehicles and a TA. The proposed module used a federated approach to achieve its objectives. The details of modules used in the proposed system are detailed below.

VANET messages

Two types of messages make up the information exchange in the VANET. Both messages were necessary for the functioning of the VANET and the proposed system.

Messages containing sensed data – These messages are transmitted messages containing sensed information, such as traffic, accident, and highway alerts.

Trust messages – are lightweight messages explicitly sent to establish vehicle attributes representing trust in the VANET. The advantage of using trust messages instead of standard messages is that standard messages may contain important emergency information that may be interfered with during the trust value calculation. The messages were designed to be lightweight, not to increase the resource consumption for the vehicles in the VANET.

Vehicles

The VANET was populated with vehicles performing different functions. All vehicles can perform the fundamental task of forwarding and receiving messages in the VANET. Information exchange enabled communication and sharing of important network messages. Vehicles had unique identities used to identify them, and these identities do not change throughout VANET operations. On the other hand, subsets of vehicles are equipped with special functions discussed below.

Malicious vehicles

Malicious vehicles represent vehicles in the VANET that were attacked by an adversary and did not perform the normal functions of vehicles in the VANET. They

are used to represent different attacks in the VANET. In order to represent different attacks, multiple types of malicious vehicles will be used. These are described below.

- Malicious vehicles that dropped messages – They received messages but will drop them instead of forwarding them to the destination. These will represent the following attacks that may cause the dropping of messages in a VANET: DOS attack, DDOS attack, blackhole attack, wormhole attack, and replay attack.

- Malicious vehicles that delayed messages – These malicious vehicles received messages, but instead of forwarding them directly to the destination vehicle, they delayed the message for a certain amount of time before forwarding it. These vehicles represented the following attacks that may cause delays in messages transmitted in a VANET: DOS attack, DDOS attack, message suppression/alteration attack, replay attack, timing attack, man-in-the-middle attack, and eavesdropping attack.

Watchdogs

These vehicles in the VANET activated the watchdog agent and switched to a listening mode to monitor their neighbours' message transactions. They monitored specific attributes of the neighbour vehicles used for trust establishment. The vehicle watchdogs were selected as the most trusted vehicles in the VANET via a secure watchdog selection method. Watchdogs had direct access to the RSU and constantly communicated with the RSU. A secure and fair watchdog selection algorithm ran iterations to determine selected watchdogs in the VANET. The watchdog selection scheme is discussed in chapter 6 below.

RSU

RSUs' acted as the TA in the VANET. It was the infrastructure that made up part of the VANET. It was assumed to be fully trusted and attack resistant. The RSU received trust factors from the vehicle watchdogs and calculated trust values for the vehicles in the VANET. The RSU was also responsible for storing previously calculated trust values of vehicles and integrating them with the new trust values it calculated. The RSU was the only member of the VANET that had the unique IDs of the vehicles. It was also responsible for producing a trust ledger with trust values corresponding to all the vehicles in the VANET. The RSU had a higher processing and computational power than other members of the VANET. The higher processing and computational power enabled the RSU to perform its functions and complex calculation in the VANET.

3.15. Performance evaluation

In order to prove the functionality of the proposed trust management system, its performance was evaluated within specific criteria. The proposed system was applied to a VANET, and the results were evaluated. This section will detail how trust management was evaluated and what criteria will be used to evaluate the system.

Ability to identify malicious vehicles

It was the first criterion used to evaluate the trust management system. In these criteria, the success of the trust management system was evaluated by its ability to distinguish non-malicious vehicles from the presence of malicious vehicles in the VANET. If unsuccessful, the trust management system cannot distinguish between malicious and honest vehicles. This criterion was evidenced by the trust values given to the vehicles in the VANET during operation.

VANET Trust value

The proposed system should improve the trust value of the VANET in the presence of malicious vehicles. This criterion involved measuring the overall trust value of the VANET. If the trust value dropped below the required threshold, malicious vehicles had taken over the VANET and no longer performed their required functions.

Packet delivery ratio

The PDR has been extensively discussed in this work—the lower the PDR, the lower the chances of packets being delivered successfully. The proposed system should improve the PDR in the presence of malicious vehicles in the VANET to be considered successful.

Delay

The delay is the time a vehicle takes to send a packet. A higher delay means fewer chances that messages will be received in the correct time frame. VANET messages are time-sensitive. The proposed system should lower the delay of vehicles and the VANET in the presence of malicious vehicles in the VANET. Table 3.3 summarises the performance metrics and their respective metric values.

Table 3.3 - Performance metrics used to evaluate the proposed system.

Performance evaluation metric	**Metric value**
Ability to identify malicious vehicles	Trust value. (A rational number with a value between 0 and 1)
PDR	The ratio between 1 and 0
Delay	Time in seconds (s)

3.16. Summary

This chapter discussed the model design, detailing all aspects of the trust management system. First, the trust management system's functions were detailed, including distinguishing between malicious and non-malicious vehicles. At the same time, it reduced the overall resource consumption of the VANET. The assumptions made in the study were discussed in detail. As shown, it is challenging to simulate all aspects of a VANET; therefore, assumptions are necessary for building a trust management system. The attacks prevented by the trust management system include attacks that cause vehicles to drop messages and attacks that cause vehicles to delay messages. The trust management system will use dedicated lightweight trust messages to establish vehicle attributes and calculate trust values. The components that make up

the VANET include sensed data and trust messages. The VANET contains different types of vehicles with different functions in the VANET. Regular vehicles usually act by forwarding messages to the intended destination vehicle. Malicious vehicles present in the VANET to represented different attacks. Malicious vehicles that dropped messages instead of forwarding them to the destination. Malicious vehicles that delayed messages before forwarding them. Malicious vehicles in the VANET can recover to normal behaviour and exhibit non-malicious behaviour during VANET operations. The purpose of this unique vehicle was to prove that the trust management system would allow malicious vehicles to recover their trust values if they started exhibiting normal behaviour in the VANET. A watchdog agent exists that can be activated in vehicles in the VANET to watch message transactions of vehicles. The message transactions revealed vehicle attributes, specifically the PDR and processing delay used to identify malicious and honest vehicles. Consistency and data correlation between the vehicle watchdogs were used to identify honest and malicious vehicle watchdogs in the VANET. The proposed system also used a secure and fair watchdog selection and management scheme.

The RSU provided infrastructure and TA in the VANET. RSUs were responsible for trust management in the VANET. It calculated the trust values for the vehicles from the data received by the vehicle watchdogs. It also created a trust ledger that featured the final trust values for all vehicles in the VANET. The trust factors also had a weight attached to the values. The purpose of the weight is to make the trust management system adaptable to different scenarios. If the trust management system application was more concerned about the vehicles and delivery of messages, the weight value of the PDR could be increased. While if the application of the proposed system were more inclined to processing delay, the weight value of the message integrity trust factor would be increased. The trust value range was discussed and set to a value range between 0 and 1. The malicious vehicles had a trust value closer to 0, while trusted vehicles had a trust value closer to 1. This method is in line with most trust management systems developed recently. Initial trust values of vehicles at the beginning of VANET operation were discussed. Vehicles can initially be set to fully trusted, neutral, and untrusted. The RSU should also be able to optimally provide the ability to test for correlation of the data produced by the watchdog. Chapters 4, 5, and 6 discuss the development and evaluation of the proposed system.

4. A multi-tier trust management system for identifying malicious vehicles in VANET communication.

4.1. Overview

This chapter presents the formal analysis of the multi-tier trust management system. It will involve a discussion of all the concepts that make up the trust management system. These concepts were related via mathematical models, and they are presented in this chapter. This chapter will also include a performance evaluation of the proposed trust management system. This chapter includes various equations and mathematical concepts. Appendix A defines some of the symbols used in this chapter. If any additional symbols are used in this chapter, an explanation will be provided alongside the symbol.

The chapter will define the components of the intelligent algorithm. Some of these components, such as trust establishment, trust factors and values, have been presented in a previous chapter of this work. The interactions between these elements are revisited in more detail to emphasize their relevance to the design of the intelligent algorithm. The intelligent algorithm's first task was calculating numerical values based on the trust metrics selected: the PDR, processing delay and consistency factor. The intelligent algorithm was applied to vehicles and RSUs. The algorithm allowed vehicle watchdogs to monitor their neighbour transactions and extract data regarding these transactions via equations and mathematical modelling. The data was then forwarded to the RSU. The algorithm allowed the RSU to calculate a trust value from vehicle watchdog data. The RSU unit keeps a record of all vehicle trust values, making up the trust history of vehicles. The RSU also created a trust ledger comprising all the trust values for vehicles in the VANET. This trust ledger was used by vehicles to ensure they only broadcast packets to trusted vehicles. Following this, the trust management system architecture is discussed. The discussion will include how the various components were related and joined to form the complete trust management system. The chapter will conclude with a performance evaluation of the proposed trust management system.

4.2. Contributions

The main contributions of the work in this chapter are detailed below.

- The work proposed a multi-tier trust-based security mechanism in VANET communications.
- The work proposed a security mechanism for protecting data integrity within the defined requirement of trust management in VANET communication.
- The work proposed a security scheme to protect against malicious watchdogs in the VANET.
- The work proposed a multi-vehicle model comprehensively reviewing the system with critical VANET factors, PDR and delays.

4.3. VANET architecture

The VANET model in this research is defined as a vehicle network comprising vehicles and RSUs. The trust management system will be designed within instances of the VANET discussed below. Each vehicle undertakes a different role in the VANET. In area (A), a set of vehicles (V_n) exists where $n = \{1, 2 \dots \dots, V_n\}$ and $n \in \mathbb{N}$, along with a set of RSU (R_s) where, $s = \{1, 2 \dots \dots, R_s\}$ and $s \in \mathbb{N}$. Within the collection of vehicles a set of watchdogs (V'_n) is selected, where, $V'_n \in V_n$. Within the VANET (R_s) will calculate trust of (V_n) using the methods described below.

4.4. Trust value calculation

This section will discuss the rational number calculation representing vehicle behaviour in the VANET. The trust value lies in the range between 0 and 1. If the trust value falls closer to 0, the vehicle is considered malicious and cannot be trusted. The vehicle is considered non-malicious and may be trusted if the trust value is closer to 1. The VANET RSU calculates the trust value. The trust value is calculated from selected trust metrics: PDR, processing delay and vehicle history. The vehicle watchdogs monitor the selected metrics from the vehicles before sending them to the RSU for processing and trust value calculation. The calculation of the trust value representing vehicle behaviour is performed by the equations and algorithms presented below.

4.4.1. Packet delivery ratio calculation

The PDR will be calculated by monitoring the number of acknowledgements and trust messages exchanged between vehicles. The watchdogs are randomly selected in the VANET to act as a source and destination in the VANET. The watchdogs also monitor vehicle communications in the VANET. The watchdog will generate trust messages and broadcast them to the VANET vehicles. The vehicles are responsible for forwarding trust messages to their destination. After successfully forwarding the message, an acknowledgement is generated and sent to the watchdog. The PDR is calculated by comparing the ratio of received messages to successfully delivered messages. This is done by monitoring the ratio of acknowledgements (A_x) to trust messages (T_y) received. The PDR of V_n is therefore given by:

$$PDR(V_n) = \sum_x^X \sum_y^Y \left(\frac{A_x}{T_y}\right) \qquad \text{Equation 1}$$

Where:

$$x = \{1,2, \dots, X\}, y = \{1,2, \dots, Y\},\ and\ X, Y \in \mathbb{N}$$

4.4.2. Processing delay calculation

Processing delay ensures message integrity. It is the time a vehicle takes to process a message before sending it to its destination. Processing delay is necessary to determine if a vehicle tampers with the message before forwarding it. A vehicle adding additional data or changing the data contained in a message will take additional time to forward the message. Processing delay consists of finding the difference between the time a vehicle receives a message (γ_j) to the time a vehicle forwards the message to the destination (λ_i). Therefore, the processing delay (PD) is given by:

$$PD(V_n) = \sum_i^I \sum_j^J \left(\frac{\lambda_i - \gamma_j}{i}\right) \quad \text{Equation 2}$$

Where:

$$i = \{1,2,\dots,I\}, j = \{1,2,\dots,J\} \; and \; I,J \in \mathbb{N}$$

The *PDR* and processing delay are used to calculate a trust value for V_n as shown in the following section.

4.4.3. Trust value calculation

The PDR and processing delay are integrated to form a trust value using the equation described below. Two weights are introduced, the weight of PDR (β) and weight of processing delay (θ), where $\beta + \theta = 1$. The purpose of the weights is that they can be adjusted depending on the application. If the application is more concerned about the number of packets delivered, the weight (β) can be increased. If the application is concerned about altering the packets, the weight (θ) can be increased. Under normal conditions, both (β) and (θ) are equal to 0.5. Multiple watchdogs are used in the operation of the proposed system. Therefore for every (V_n), a $\left(TV\left(V_{n,z}\right)\right)$ is calculated where, (z) represents the iterations from multiple watchdogs.

$$TV\left(V_{n,z}\right) = \beta * \text{PDR}\left(V_{n,z}\right) + \theta * \text{PD}\left(V_{n,z}\right) \quad \text{Equation 3}$$

The proposed system makes use of multiple watchdogs (V'_n) in the VANET, therefore, for every V_n in the VANET, the following trust matrix (T) is created:

$$T(V_n) = \begin{bmatrix} TV\left(V_{n,z}\right) \\ \dots \\ TV\left(V_{n,Z}\right) \end{bmatrix}, z = \{1,2,3,\dots,Z\} \; and \; Z \in \mathbb{N}$$

The multiple values from different watchdogs must be integrated to form a value representing the trust of a vehicle. The values of $\left(T(V_n)\right)$ are integrated using the equation below:

$$TV(V_n) = \frac{\sum_z^Z (TV(V_{n,z}))}{z} \quad \text{Equation 4}$$

Where:

$$z = \{1,2,\dots,Z\} \; and \; Z \in \mathbb{N}$$

4.4.4. Vehicle history calculation

Vehicle history involves considering the past trustworthiness of a vehicle. Considering the vehicle history ensures the vehicle must constantly exhibit non-malicious behaviour to be classified as a non-malicious vehicle in the VANET. If a vehicle does not have a history, it is not considered until one has been formed. The previously recorded trust value(ω) is combined with the newly calculated trust value(TV) using the equation described below:

$$TV(V_n) = \frac{\omega(v_n) + TV(V_n)}{2} \quad \text{Equation 5}$$

Where:

$$n = \{1,2, \dots, N\} \; and \; N \in \mathbb{N}$$

The $TV(V_n)$ represents the trustworthiness of the vehicle (V_n) . The value represents the behaviour of a vehicle in the VANET. The proposed system includes controls to ensure the integrity of the trust value.

4.4.5. Data integrity calculation

Trust value defines vehicle behaviour; therefore, this value is fundamental to the trust management system and VANET. Trust integrity should be protected from malicious behaviour. The trust management system has proposed and implemented controls to protect trust values. The controls ensure that the data used to calculate the trust value is legitimate and not fabricated by a vehicle or watchdog. The first control is applied before equation 1 is processed. This control ensures that the total number of acknowledgements is never more than the number of trust messages sent. This control is based on the fact that a vehicle can only create an acknowledgement message after forwarding a message successfully. Therefore, the total number of messages forwarded should always be more than or equal to the total number of acknowledgements received. The vehicle is considered malicious if the number of acknowledgements received exceeds the number of messages. The control equation is described as follows: $(T_y \geq A_z)$.

The second control is implemented before equation 2 is executed. This control checks that the acknowledgement time stamp is always higher than the trust message time stamp. The acknowledgement time stamp should always be greater than the trust message time stamp. The vehicle could be regarded as malicious and fabricating data if the acknowledgement time stamp exceeds the time stamp for the message forwarded. The control equation is presented as follows: $(\lambda_i \geq \gamma_j)$

The third control applied is used to confirm the integrity of the data obtained by VANET watchdogs. Data collected by multiple watchdogs is compared to implement the control. The comparison is done each time the RSU receives data from the watchdogs. The data collected by watchdogs about an evaluated vehicle should be correlated and similar as data collection happens under similar conditions. The third control is applied after the trust matrix is calculated. Trust values from different watchdogs are compared for $z = \{1, 2, 3, \dots, Z\}, and \; Z \in \mathbb{N}$ is $TV(V_{n,z}) == TV(V_{n,Z})$.

The three above controls enable the proposed system to protect the trust value calculation integrity. The controls offer additional security by identifying malicious vehicles or watchdogs that fabricate data.

4.4.6. Trust threshold calculation

The proposed system uses a trust threshold to distinguish between malicious and non-malicious vehicle behaviour. The trust threshold depends on its application and strictness. For example, military applications have higher trust thresholds than entertainment applications. The trust value calculated in equation 5 $(TV(V_n))$ is

compared against the threshold using the following $TV(V_n) \geq threshold$. Vehicles with a trust value greater than the threshold are considered non-malicious. In contrast, vehicles with a trust value below the threshold will be considered malicious. Based on these equations, the proposed system employs the following algorithms.

4.5. Algorithm design

This section will detail the algorithms used by the proposed trust management system. The equations above are combined to create the complete algorithm the trust management system uses. The main algorithms used by the trust management system are discussed below.

4.5.1. Algorithm 1

The primary purpose of this algorithm 1 is to create the trust matrix (TV_m). Algorithm 1 assists the vehicle in achieving its objective function of identifying malicious and non-malicious behaviour in vehicles. Algorithm 1 consists of the use of equation 1, equation 2 and equation 3. The algorithm also makes use of control 1 and control 2. Algorithm 1 is shown in Algorithm 4.1. Figure 4.1 shows the proposed algorithm 1 process.

Algorithm 1: Calculating trust value matrix (TV_m)

Input: Vehicle map (V_n, R_s), β , θ
Output: $TV(V_{n,z})$ for every V_n
While $t \in T$ **do**
    TV_m:
    Select V'_n from V_n
    //V'_n collects data on V_n
    //V'_n forward data to R_s
    If $V_n(T_y \geq A_z)$ **then**
        Calculate $PDR(V_n)$ by equation 1
    End if
    If $V_n(\lambda_i \geq \gamma_j)$ **then**
        Calculate $P(V_n)$ by equation 2
    End if
    For $V'_n \in V_v$ **do**
        Update trust matrix $TV(V_{n,z})$ by equation 3
    End for
End while

Algorithm 4.1 - Proposed algorithm 1 to calculate trust value matrix

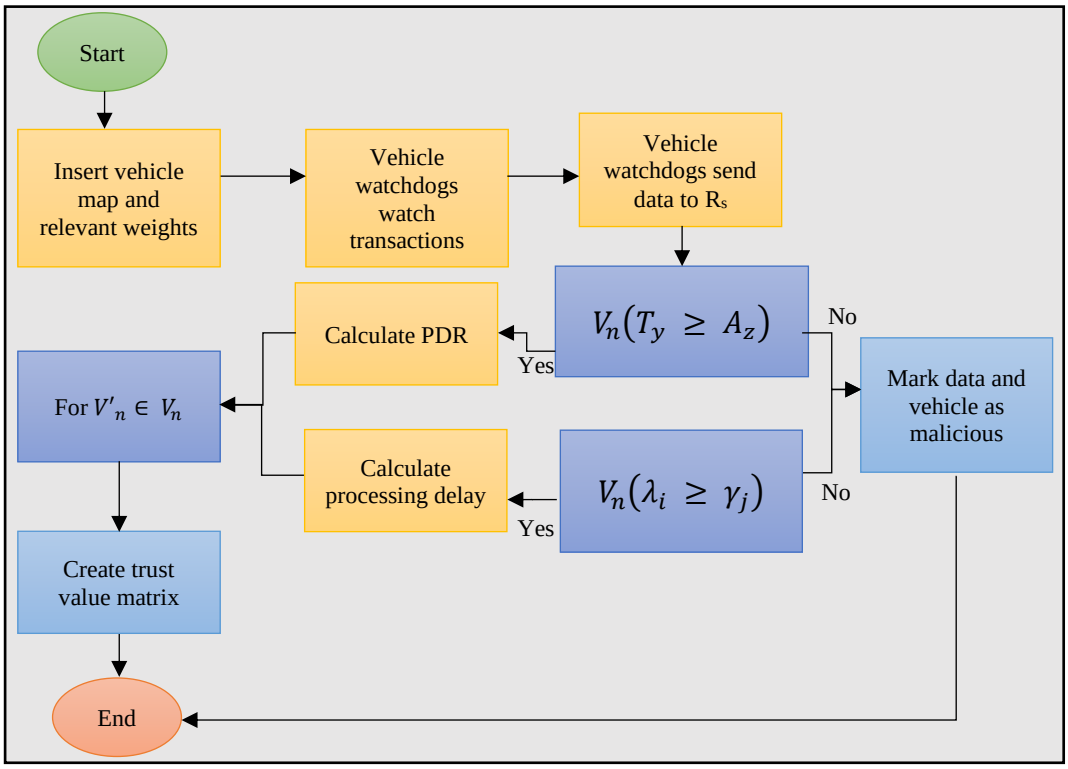

Figure 4.1 - Algorithm 1 process diagram used in calculating vehicle trust values.

4.5.2. Algorithm 2

The primary purpose of algorithm 2 is to integrate the trust matrix into a single trust value representing vehicle behaviour. Algorithm 2 will use equation 4 and equation 5 to achieve its objective function. Algorithm 4.2 shows the proposed algorithm 2, and Figure 4.2 shows the process diagram for algorithm 2.

Algorithm 2: Calculating trust value $(TV(V_v))$
Input: Vehicle map $(V_n,\ R_s), \omega$
Output: $TV(V_n)$
For $TV(V_{n,z})$ **do**
    If $TV(V_n)$ exists in the database, **then**
        Update label to $\omega(V_v)$
    End if
    If $TV(V_{n,z}) == TV(V_{n,Z})$ **then**
        Calculate $TV(V_n)$ by equation 5
    End if
    If $\omega(V_n)$ exists in the database, **then**
        Calculate $TV(V_n)$ by equation 6
    End if
    Update $TV(V_n)$
End for

Algorithm 4.2 - Proposed algorithm for vehicle trust value calculation

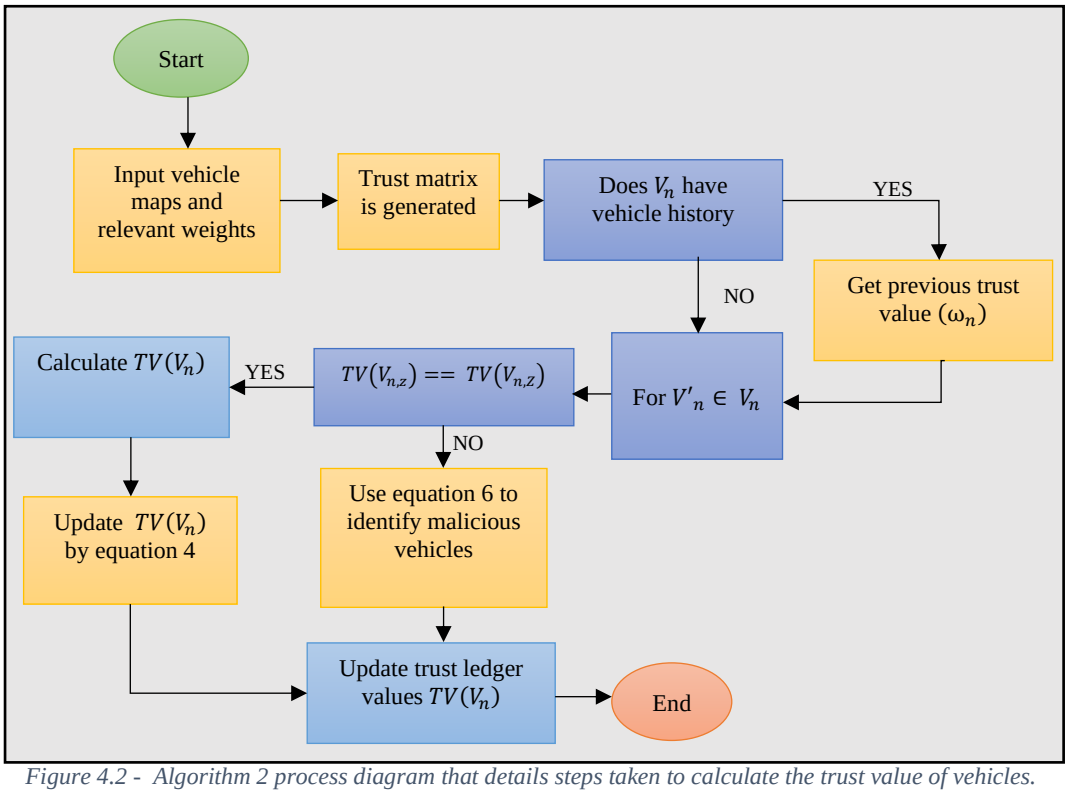

Figure 4.2 - Algorithm 2 process diagram that details steps taken to calculate the trust value of vehicles.

4.6. Simulation model

The hardware and software requirements used to simulate the VANET and proposed system are first discussed. An analysis of the simulation model follows this.

Hardware specifications

The development of the proposed system, VANET models and scenarios happened on the same hardware platform. The development and simulation took place on a Windows 10 64-bit platform, and simulation software was installed directly on the windows operating system. Further hardware details are provided in Table 4.1 below.

Table 4.1 - Specification of hardware used in the project.

Hardware specification	**Details**
Platform/Operating system	Windows 10 Home (x64), 64-bit
Processor	Intel Core i7-7500U CPU @ 2.70GHz 2.90 GHz
RAM	16.0 GB
Hard disk drive	250GB (30GB Free)

Software specification

Different software components are used to develop the different components of the trust management system. These are detailed in Table 4.2 below.

Table 4.2 - Details of software used in the study.

Software specification	Details
Trust management system	
Development environment	Omnet++
Environment version	Omnet++-5.6.2
Development programming language	C++
Simulation software	
Simulation environment	Omnet++
Environment version	Omnet++ 5.6.2
Programming language	Network descriptive language (NED), C++
Frameworks/Namespace	C++ standard libraries, Omnet++ libraries, INET libraries

The trust management software is designed to be a stand-alone application based on C++ language. It should run on any applications and IDEs that support C++ applications. When applied to a VANET, the application can run without human interaction, with default weights selected. There is the option for human interaction to edit the weights of various components of the trust management system depending on application-specific requirements.

Development challenges and constraints

Regarding the hardware and software specifications listed in the above section, a few challenges were experienced in simulation and design. These challenges are discussed below.

- OMNET++ programming language – Omnet++ is based on C++, so it uses all the libraries and namespaces available in C++. In addition, Omnet++ has its classes, libraries and namespace that needed to be studied before the simulation began. The additional components constituted a steep learning curve, which created a few delays before the simulation work could begin.

The following section contains the simulation details. The simulation was run assuming a dynamic topology in the network. The proposed trust management took advantage of a cluster formation to evaluate vehicles in the VANET. A cluster is made up of vehicles and RSUs. Among the vehicles will include those selected as watchdogs and those that will be evaluated. The cluster formation should have multiple watchdogs in the VANET for the proposed trust management system to function optimally. The details of the watchdog selection process are detailed in chapter 5. Malicious behaviour will be simulated in randomly selected vehicles in the VANET. Simulating malicious behaviour will be used to evaluate the proposed system's ability to identify malicious behaviour in vehicles. Three types of malicious vehicles will be simulated in the VANET.

Malicious vehicles that drop messages/packets – These malicious vehicles will receive messages from the source but drop them instead of forwarding them to the destination vehicle. Vehicles will be simulated to drop messages at different rates during VANET operations. These represent the following attacks that may cause messages to be lost in a VANET: DOS attack, DDOS attack, blackhole attack, wormhole attack, and replay attack.

Malicious vehicles that delay messages/packets – These malicious vehicles will receive messages from the source. Instead of forwarding the messages directly to the destination vehicle, they delay them for a certain amount before forwarding them. Vehicles will be simulated to delay messages at different rates in the VANET. These vehicles represent the following attacks that may cause delays in messages transmitted in a VANET: DOS attack, DDOS attack, message suppression/alteration attack, replay attack, timing attack, man-in-the-middle attack, and eavesdropping attack.

Malicious vehicles that both delay and drop messages – These malicious vehicles will behave like vehicles that delay and drop packets. They will drop and delay messages at different times and rates during VANET operations. These vehicles simulate multiple attacks on a vehicle.

Figure 4.3 depicts the operations of the trust management system in detail. The source of trust messages will have one-hop communication with the vehicles being evaluated and can send direct messages to them. The vehicles being evaluated will have one-hop communication with the destination and must forward messages directly to the destination. The vehicle watchdogs will be in communication range with vehicles and can monitor the message transactions of vehicles. The watchdog will also be in communication range with the RSU and can communicate directly with them. The RSU can communicate with all VANET members due to its superior processing and computational power.

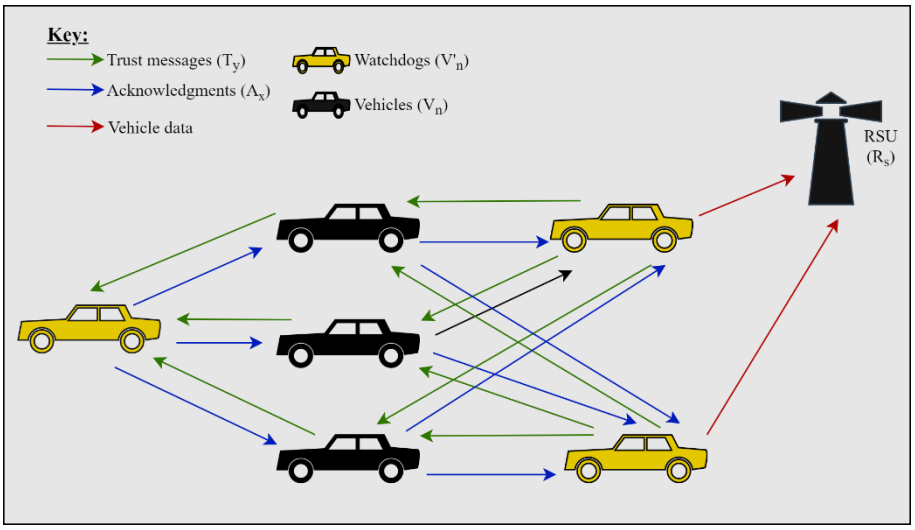

Figure 4.3 - Proposed communication in the multi-tier trust-based security management system.

The proposed system was set to work when vehicles are at a standstill or moving at low speeds. Stand-still and slow-moving traffic happen during traffic congestion scenarios; traffic light stops, parking garages, parking lots, or drive-through locations. These moments present an opportunity when vehicles are least likely to exchange critical information in the VANET. Simulation parameters are summarised in Table 4.3 below:

Table 4.3 - Simulation parameters used in the multi-tier trust management system.

Parameters	Value
Area of network	$200m^2$
Number of vehicles	8
Transmission range	20m
Number of watchdogs	3
Initial trust value	1.0 (Trusted)
Trust threshold	0.7
Simulation time	360s
Malicious vehicles	3
Evaluated vehicles	4
MAC protocol	IEEE802.11p
Vehicle speed	0.5m/s

The percentage of malicious vehicles in the simulation was 37% of VANET vehicles. This percentage was similar to the percentage selected by state-of-the-art trust management systems reviewed in the work. According to experiments conducted by [40], [88], 30% of malicious vehicles were selected. In comparison, experimental studies conducted in [66] indicated that the percentage of malicious vehicles varied between 5% and 50%. As a result, 37% of malicious vehicles were considered sufficient to evaluate the proposed system.

The trust threshold can be altered depending on the application. For applications such as military applications requiring exceptional security, the trust threshold can be raised to a higher value. While if the system requires a standard amount of security, e.g. entertainment application, the trust threshold can be lowered. Researchers have used different thresholds from the evaluated trust management systems in their experiments. [27] used a threshold of 0.1 to identify malicious vehicles. In contrast, AATMS used the average trust values of vehicles in the VANET as the threshold value [40]. In an experiment conducted in [66], the trust threshold was set to 0.5. The trust threshold depends on the application of the VANET. In the experiment in this work, the trust threshold was set to 0.7.

4.7. Performance evaluation

To characterize and validate the performance of the proposed system, the model was evaluated over several scenarios described below.

The developed system was evaluated against its objective function, identifying malicious vehicle behaviour. It should distinguish between malicious and non-malicious vehicles. The proposed system should also identify the overall VANET state. The proposed system should be able to detect a VANET taken over by malicious vehicles. A VANET that malicious vehicles have taken over cannot perform its intended functions.

The first experiment involved applying the proposed system to a VANET of vehicles exhibiting harmful and non-malicious behaviour. Malicious behaviour involved the vehicle dropping messages at different rates in the VANET. Figure 4.4 shows the results of 4 evaluated vehicles, V1, V2, V3 and V4. The orange line represents V1 in the figure. It maintained a constant one value throughout VANET operations. V1, therefore, was identified as exhibiting non-malicious behaviour. V3, represented by

the green line, at 60 seconds, the trust value dropped below the threshold. The trust value remained below the threshold throughout VANET operations. The trust value indicated that V3 displayed malicious behaviour. V2 and V4, represented by the brown and blue lines, exhibited the same behaviour as V3. At the 120s and 180s of the VANET operation, V2 and V4's trust values dropped below the trust threshold. Both their trust values were maintained below the threshold during the VANET operation. This indicated malicious behaviour. In this experiment, V2, V3, and V4 were identified as malicious vehicles that dropped packets, while V1 was identified as non-malicious. This indicated that the proposed system successfully identified non-malicious and malicious vehicles when malicious vehicles dropped packets.

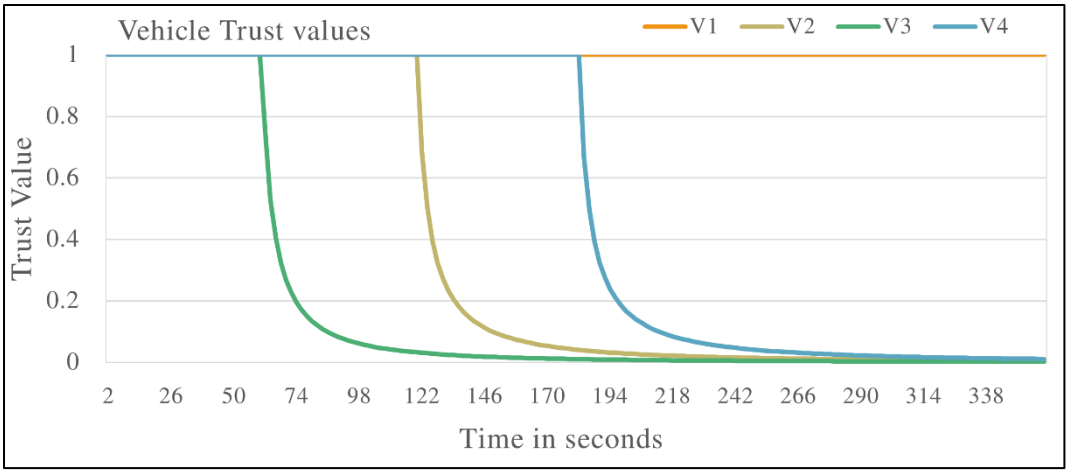

Figure 4.4 - Vehicle trust values in the experiment where malicious vehicles dropped messages instead of forwarding them to the destination.

The number of messages received and successfully forwarded to the destination by individual vehicles is shown in Figure 4.5.

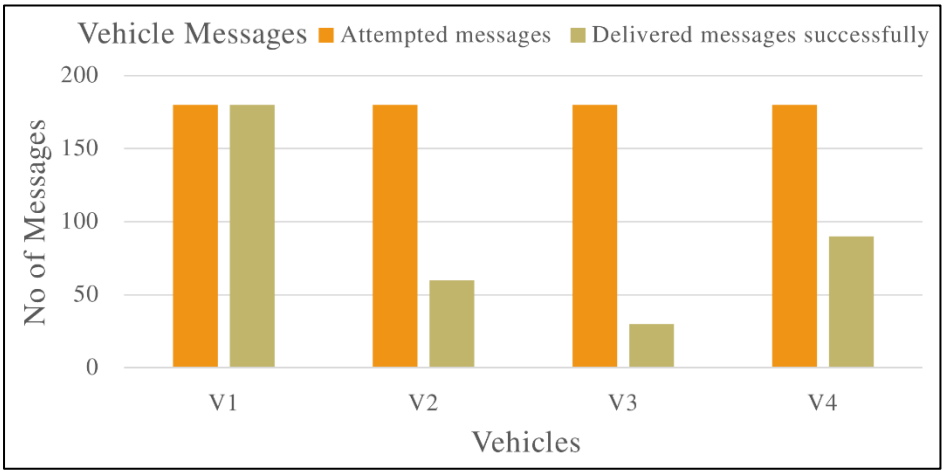

Figure 4.5 - Vehicle messages transmitted in VANET where malicious vehicles exist and are dropping messages.

Figure 4.5 further confirms the results in Figure 4.4. V1, identified as non-malicious, successfully forwarded 100% of messages received throughout the VANET operation. V2, V3 and V4 were identified as malicious vehicles, as they delivered only a percentage of messages received successfully. Results indicated that these vehicles dropped messages in the VANET and behaved suspiciously.

In the second experiment, the VANET was run in three instances. The first instance created a baseline system with only non-malicious vehicles in the VANET. The second instance ran with vehicles that dropped packets in the VANET. The proposed system was then applied to the VANET with malicious vehicles in the third instance. Figure 4.6 displays the results of this experiment.

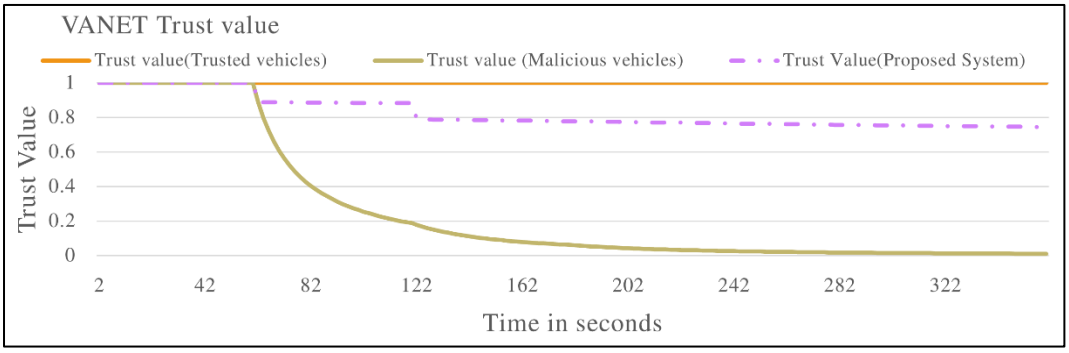

Figure 4.6 - VANET Trust value in the experiment where malicious vehicles dropped messages instead of forwarding them to the destination.

The baseline system populated by all vehicles exhibiting non-malicious behaviour is represented by the orange line labelled Trust value (Trusted vehicles). The trust value remained constant at 1 throughout the VANET operation. It shows that the VANET was in a non-malicious state and functioned optimally to achieve its objectives. The second instance, the VANET populated with malicious vehicles, is represented by the green line labelled Trust value (Malicious vehicles). It shows a declining trust value to a level below the trust threshold. The declining trust value indicates that malicious vehicles have taken over the VANET to the point that it cannot perform its normal functions. The third instance, where the proposed system is applied to the VANET with malicious vehicles present, is represented by the dotted line labelled Trust value (Proposed system). Although the trust value dropped, it did not drop below the trust threshold. The proposed system identified and isolated malicious vehicles, thus preventing them from taking over the VANET. The VANET could perform its normal functions even with malicious vehicles. Figure 4.7 shows the number of messages attempted to be delivered and the number of messages successfully delivered from the previous experiment.

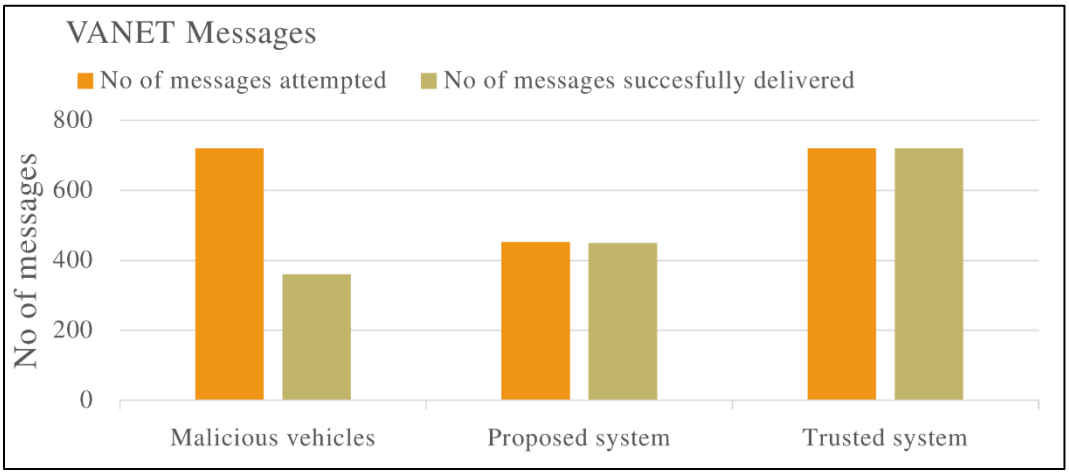

Figure 4.7 - Total messages transmitted in VANET with malicious vehicles present that are dropping messages.

In VANET, 100% of the messages were delivered successfully in the first instance. It attempted and effectively transmitted 720 messages throughout the VANET operation. In the second instance, labelled malicious vehicles, 50% of the messages were transmitted without error. 720 messages were tried, while only 360 were delivered successfully. In the third instance of the experiment, 98% of the messages were transmitted successfully. Although the number of total messages attempted was less than in the first instance, the number of delivered messages significantly improved in the presence of malicious vehicles. The result indicates the effectiveness of the proposed system in improving the PDR of a VANET with malicious vehicles present.

In the third experiment, the proposed system was evaluated against vehicles that exhibited malicious behaviour and delayed messages in the VANET. A selection of vehicles delayed messages at different rates in the VANET. Figure 4.8 shows the vehicle trust values when the VANET was populated with vehicles exhibiting malicious behaviour and delaying packets in the VANET. The results are presented below.

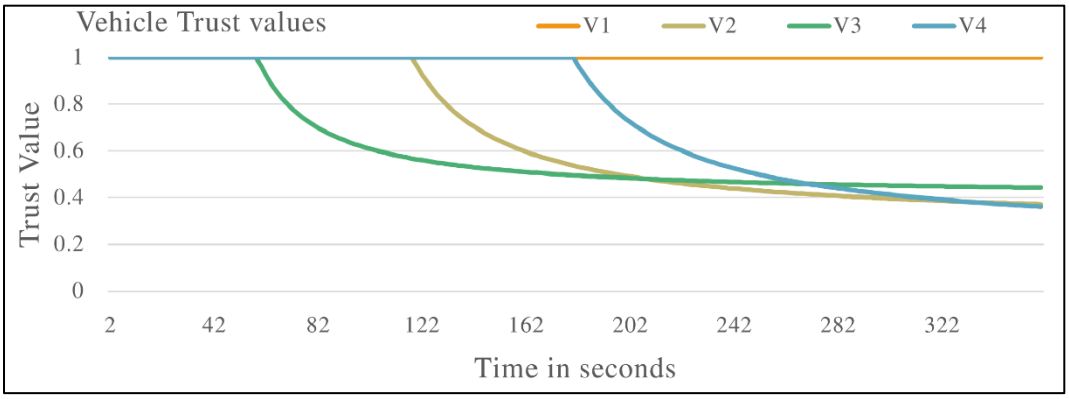

Figure 4.8 - Vehicle trust values experiment where malicious vehicles delayed messages instead of forwarding them to the destination.

V1's trust value, represented by the orange line, remained constant at 1 throughout the VANET operation. The trust value did not fall below the trust threshold; consequently, V1 was identified as a non-malicious vehicle. V3's trust value, represented by the green line, started to drop in the 60s of VANET operation until it was below the trust threshold. At the 120s and 180s of the VANET operation, V2 and V4's trust values dropped until they were below the trust threshold. This indicated that V2, V3, and V4 were identified to exhibit malicious behaviour and delayed packets in VANET. Figure 4.9 shows the processing delay of the vehicles in the VANET from this experiment.

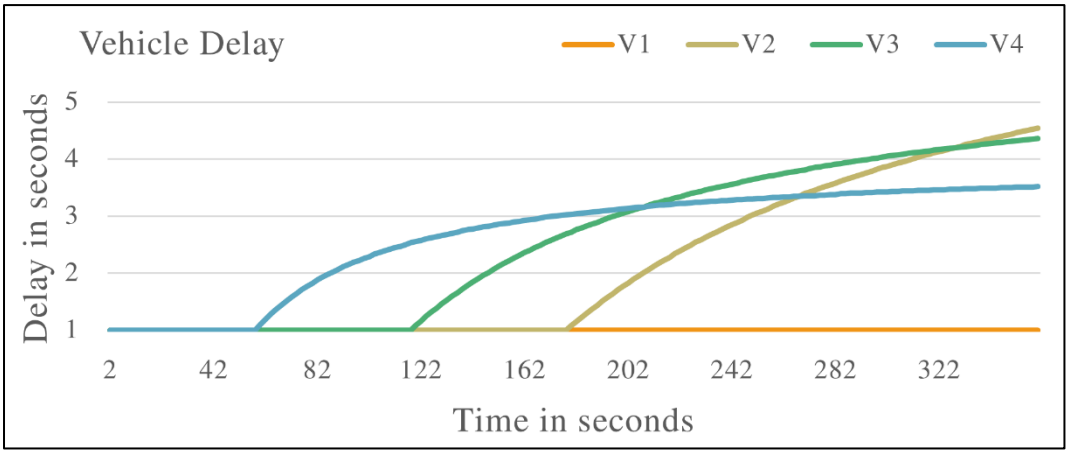

Figure 4.9 - Vehicle delays where malicious vehicles delayed messages before forwarding them to the destination.

V1 maintained a constant processing delay of 1s throughout VANET operations, indicating it exhibited non-malicious behaviour. V2, V3 and V4 at 180s, 120s and 60s, respectively, experienced a rise in processing delays. The rise in processing delay indicated that the vehicles delayed messages before forwarding them to their destination. The results solidified the results in Figure 4.9 identifying vehicles that delayed messages in the VANET. There is an inverse relationship between the delay and the level of trust. Messages will be delayed if a vehicle takes longer to forward them, reducing the trust value of the vehicle. The relationship can be observed by comparing the delay of vehicles shown in Figure 4.9 with the trust values shown in Figure 4.8.

In the fourth experiment, three instances of the VANET were executed. The first instance ran with only non-malicious vehicles present in the VANET. The first instance created a baseline system when the VANET operated optimally. The second instance ran with malicious vehicles that are delayed packets, which showed the state of the VANET when taken over by malicious vehicles. The third instance ran with the proposed system applied to the VANET with malicious vehicles. VANET statistics were recorded. Figure 4.10 shows the trust value of the VANET from the experiment.

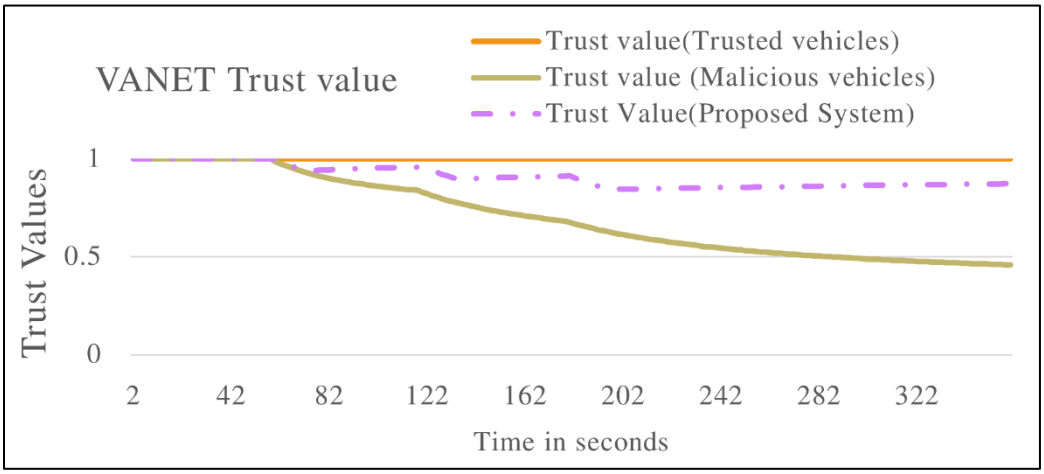

Figure 4.10 - VANET trust value experiment where malicious vehicles delayed messages instead of forwarding them to the destination.

The orange line labelled Trust value (Trusted Vehicles) represented the trust value of the VANET when all the vehicles exhibited non-malicious behaviour. The trust value remained at 1.0; this meant the VANET operated under optimal conditions. The green line, Trust value (malicious vehicles), shows the VANET trust value when malicious vehicles are present. The trust value dropped below the trust threshold, indicating malicious vehicles had taken over the VANET, and it could no longer perform routine operations. The grey dotted line labelled Trust value (Proposed system) represents the trust value of the VANET with malicious vehicles present and the recommended system applied. The proposed system identified and isolated malicious vehicles that delayed messages, preventing trust values from dropping below the trust threshold. The proposed system successfully identified malicious vehicles that delayed messages and prevented the VANET from being taken over by malicious vehicles. Figure 4.11 shows the delay of the VANET from the above scenario.

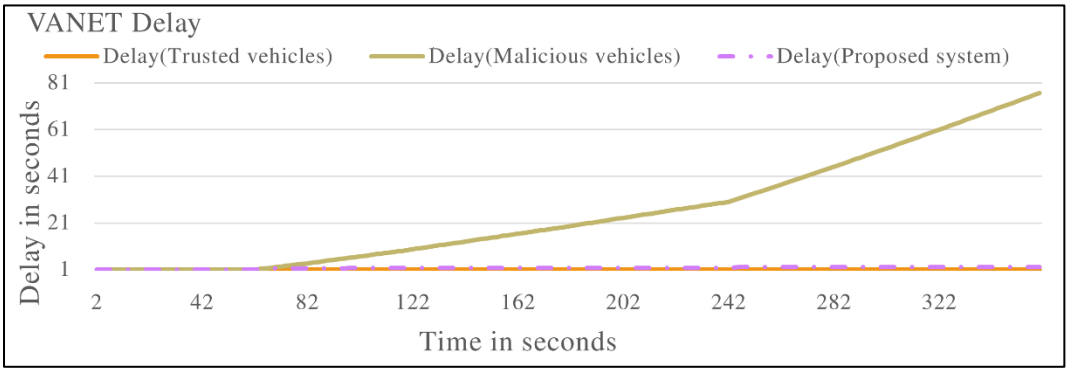

Figure 4.11 - VANET delay in the experiment where malicious vehicles delayed messages before forwarding them to the destination.

The orange line represents the first instance of the experiment, Trust value (Trusted Vehicles). When all vehicles displayed non-malicious behaviour, VANET exhibited this delay. VANET delay is the average time to deliver a message in the VANET. The delay in this instance remained at 1.0s throughout the operation. The constant value of 1 means vehicles do not delay messages before forwarding them to their destination. The green line represents the second instance, which shows the VANET delay with malicious vehicles present. The delay increased consistently during the VANET operation. The increase in delay showed that the average time to deliver messages in the VANET increased as the VANET operated. It meant vehicles delayed messages, taking longer to deliver them to their destination. The dotted line represents the third instance, which illustrates the VANET delay with malicious vehicles present and the proposed system applied. The proposed system helped improve the VANET delay even in the presence of malicious vehicles. The above results further supported the results in Figure 4.10, showing proposed system kept the VANET running close to optimal conditions even in the presence of malicious vehicles. The relationship between the VANET delay and the trust value was identified as inversely correlated. A VANET which increased its delay and took longer to deliver messages will have its trust value drop. The inversely proportional behaviour is seen in Figure 4.9 and Figure 4.10; when the VANET delay increased, the trust value of the VANET dropped.

Malicious behaviours include dropping packets, delaying packets, or both dropping and delaying packets. In the third experiment, multiple malicious vehicles were applied to a VANET. Figure 4.12 shows the trust value of 4 vehicles in the VANET.

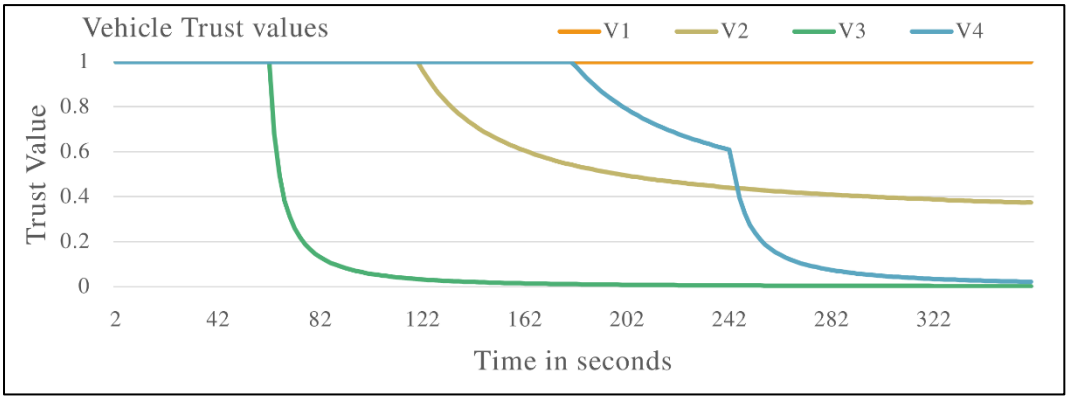

Figure 4.12 - Vehicle trust values in the experiment comprised multiple types of malicious vehicles.

Vehicle V1's trust value maintained constant at 1 throughout the VANET operation. This indicated that V1 exhibited non-malicious behaviour throughout VANET operations. V2's trust value began operation at one but decreased as the VANET operated below the trust threshold. Vehicles V3 and V4 followed the same pattern, dropping their trust values below the trust threshold. V2, V3 and V4 were identified as exhibiting malicious behaviour in the VANET. The proposed system identified malicious vehicles in the presence of multiple types of attacks in the VANET.

In the next experiment, three instances of the VANET were executed. The first instance ran with only non-malicious vehicles present in the VANET. The first instance created a baseline system when the VANET operated optimally. The second instance was run with malicious vehicles that delayed packets, dropped packets or both; this showed the state of the VANET when taken over by malicious vehicles. The third instance ran with the proposed system applied to the VANET with malicious vehicles. The results from this experiment were recorded and presented in Figure 4.13, Figure 4.13, and Figure 4.14. Figure 4.13 shows the trust value of the VANET from the above experiment.

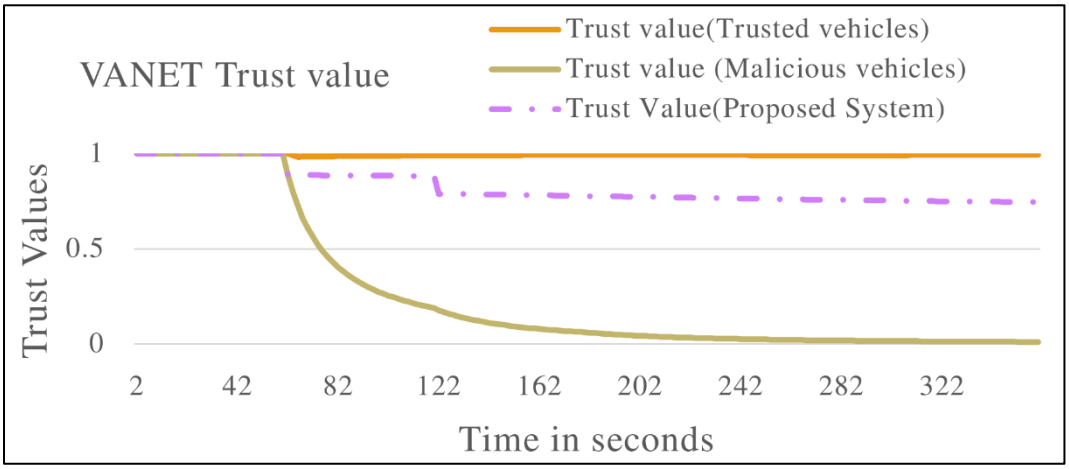

Figure 4.13 - VANET trust value in the experiment comprised multiple types of malicious vehicles.

The orange line in Figure 4.13 represents the trust value of the VANET in the first instance where all vehicles exhibited non-malicious behaviour. The trust value maintained a value of 1 throughout operations. The constant value indicated that the VANET performed optimally and achieved its objectives. The second instance is represented by the green line, which shows the trust value of the VANET when malicious vehicles are introduced. This malicious behaviour caused the trust value of the VANET to drop below the trusted threshold. This indicated that the VANET could

no longer perform normal operations as malicious vehicles had taken over. The dotted line represents the third instance, where the proposed system was introduced to a VANET with malicious vehicles. Although the trust value dropped, it did not decrease to a level below the trust threshold. The proposed system effectively identified and isolated malicious vehicles; therefore, the VANET remained trusted throughout the operation. The VANET can therefore perform its functions even in the presence of malicious vehicles. Figure 4.14 shows the PDR of the VANET in the above experiment.

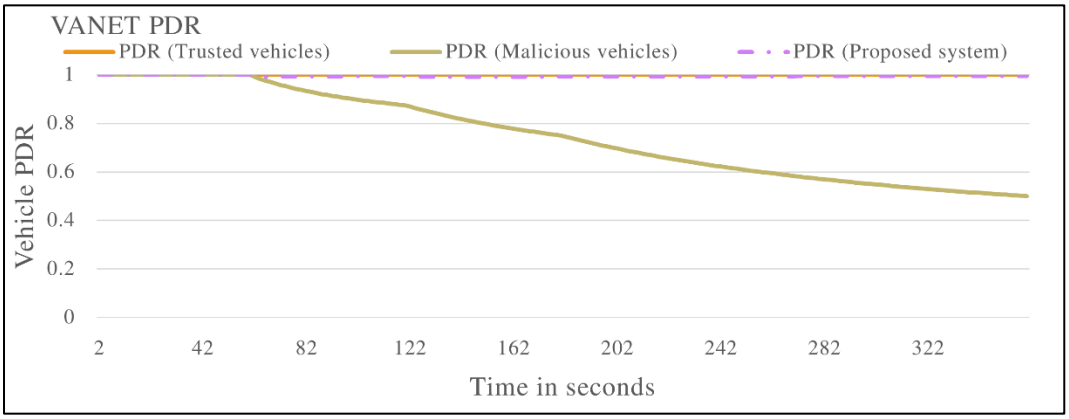

Figure 4.14 - VANET PDR in the experiment comprised multiple malicious vehicles.

The orange line represents the first instance where all vehicles are non-malicious. The PDR remained at 1, meaning all the packets in the VANET were delivered successfully. The green line represents the second instance. The PDR decreased in the presence of malicious vehicles, meaning fewer packets were delivered successfully. The dotted line represents the third instance with the proposed system applied to a VANET with malicious vehicles present. The proposed system improved the PDR of the VANET in the presence of malicious vehicles in the VANET. The VANET PDR is proportional to the VANET trust value. A drop in the PDR leads to a drop in the trust value of the VANET. Figure 4.15 shows the processing delay of the VANET from the experiment, as mentioned above.

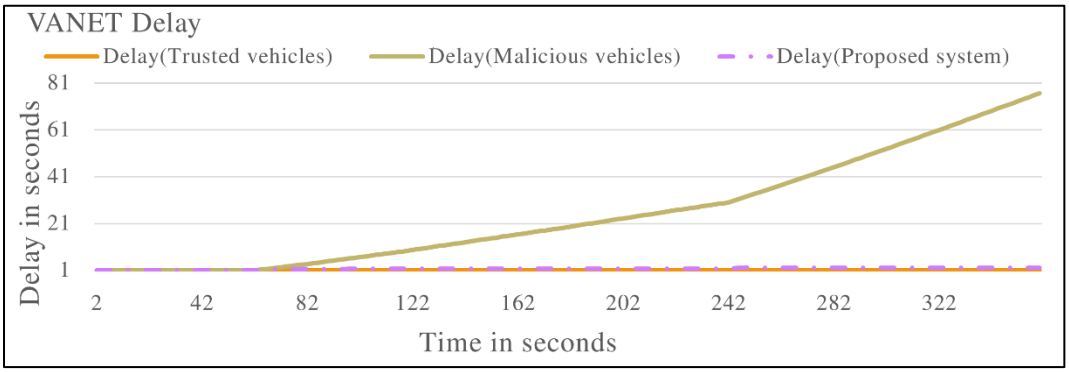

Figure 4.15 - VANET Delay in the experiment comprised of multiple malicious vehicles.

The orange line represents the first instance where all vehicles are non-malicious. The processing delay remained at 1s, meaning all the packets in the VANET were delivered without delay, with malicious vehicles in the VANET represented by the green line. The delay increased as vehicles held up messages before delivering them to the destination. The dotted line represents the third instance. The processing delay and VANET trust value have an inversely proportional relationship. An increase in

the delay of the VANET will lead to a decrease in the trust value of the VANET. The proposed system identified and isolated the malicious vehicles and kept the processing delay from increasing. The proposed system improved the processing delay even in the presence of malicious vehicles.

In many real-world applications, the efficiency of an algorithm is critical for its practical use. By analysing the algorithm, efficiency can be determined, and performance can be predicted on different inputs. The following section shall feature an analysis of the algorithm complexity of the developed algorithms. The algorithms will also be compared against the state-of-the-art trust management system: An anti-attack trust management scheme in VANET (AATMS) [40]. The algorithm was selected as it was closest in functionality to the proposed system.

Table 4.4 - Comparison of algorithm complexities.

System	Time complexity	Space complexity
Proposed work		
Algorithm 1: Calculating trust value matrix (TV_m)	$O(n^2)$	O(n)
Calculating trust value $(TV(V_v))$	O(n)	$O(n^2)$
AATMS		
Algorithm 1: Calculation of local trust value	$O(n^2)$	O(n)
Algorithm 2: The calculation of global trust value	$O(n^3)$	$O(n^2)$

The algorithm complexity is concerned with the worst-case scenario. Therefore, the algorithm complexities of the systems are represented in Figure 4.16 and Figure 4.17.

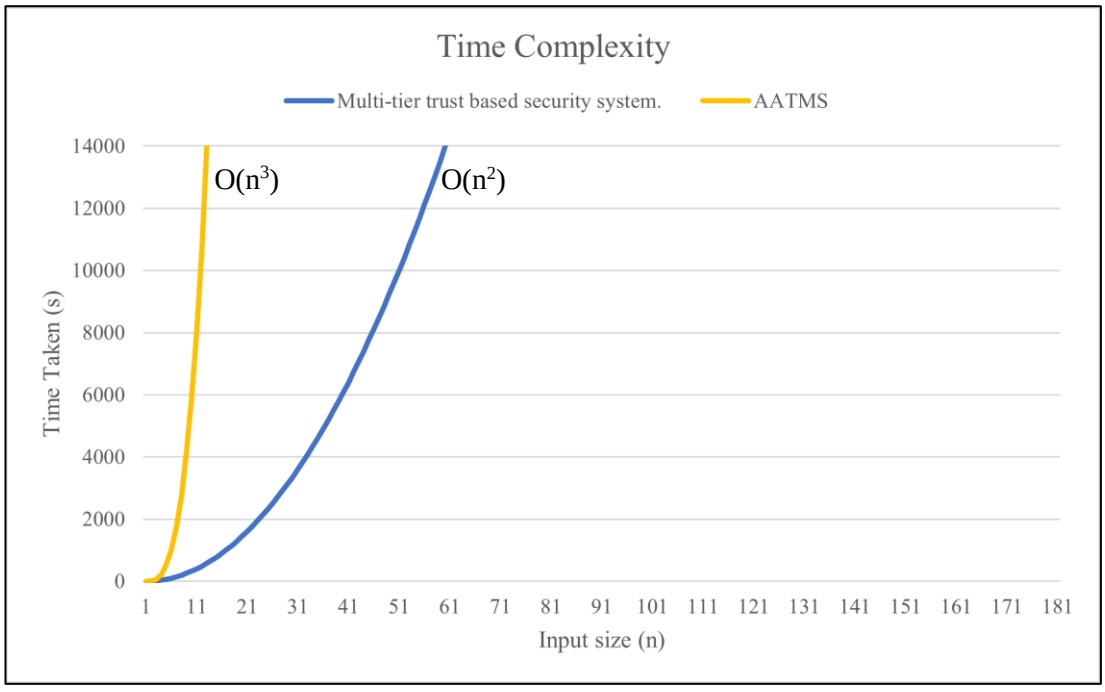

Figure 4.16 - Time complexity of the proposed system compared to AATMS.

Figure 4.16 shows the time complexity of both the proposed system and AATMS. AATMS has a time complexity of O(n3), meaning that the algorithm's running time increases in proportion to the cube of the input size. While the proposed system has a

time complexity of O(n2), the algorithm's running time increases in proportion to the square of the input size. The algorithm's time complexity grows moderately as the input size grows. According to the results, the proposed system is more efficient regarding time complexity than AATMS.

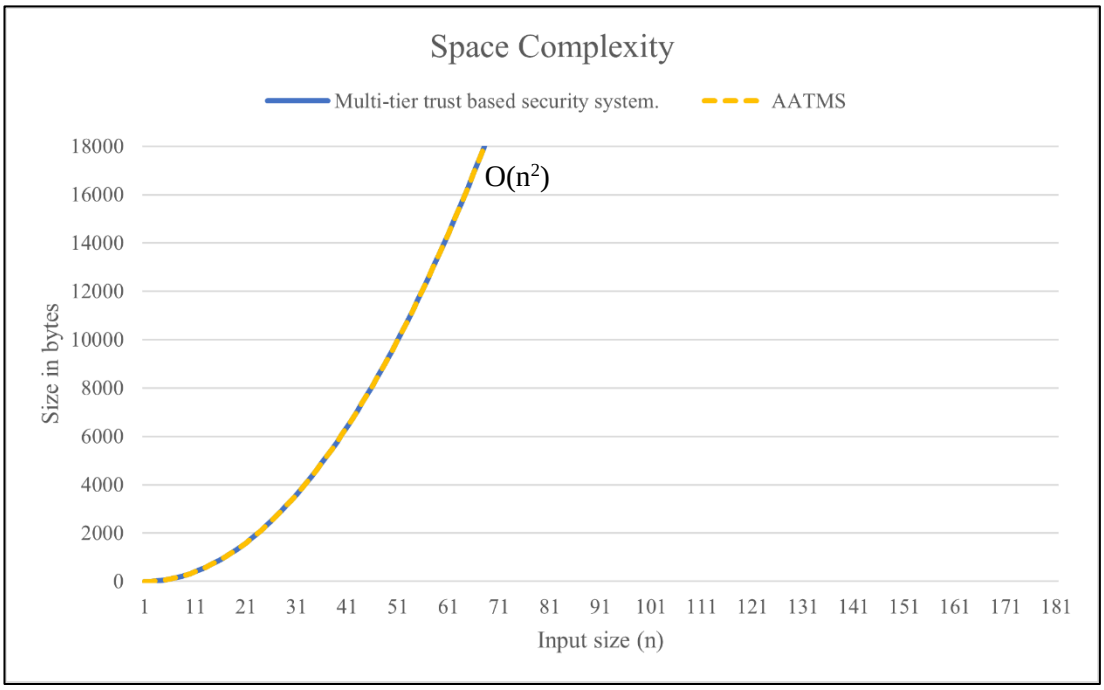

Figure 4.17 - Space complexity of the proposed system compared to AATMS.

Figure 4.17 shows the space complexity of both the proposed system and AATMS. Both algorithms have a space complexity of $O(n^2)$. The space complexity means that the amount of memory required by the algorithms will increase in proportion to the square of the input size.

The comparisons with AATMS show that despite having similar space complexities, the proposed system is more efficient regarding time complexity.

4.8. Summary

This chapter provides multi-tier trust management to evaluate non-malicious and malicious vehicles in a VANET. The trust management system uses the PDR, processing delay and history factor to calculate a trust value representing the behaviour of a vehicle in a VANET. The trust management system uses vehicle watchdogs in the VANET to track message transactions between vehicles and monitor transaction statistics. To enhance the trust management system's security, RSU verified the data collected. Data verification ensured the data was legitimate and not falsified by the vehicles. The vehicle watchdogs forwarded this data to the RSU in the VANET, which calculated the trust values of the monitored vehicles. As an additional security measure, the RSU compares the data received from the vehicle watchdogs. This identifies a vehicle watchdog that may falsify data.

The simulation results showed that the proposed trust management system improved VANET operations by distinguishing between honest and malicious vehicles. The proposed system improved the PDR and delay of a VANET with malicious vehicles

present. The multi-tier trust-based security system described in this chapter provides robust VANET security. The experiments and analysis revealed an opportunity to enhance the system with additional features. These additional features improve the proposed system's robustness and applicability. They will include an algorithm for identifying false positives and recovering malicious vehicles and a secure and fair watchdog selection algorithm. These are described in chapters 5 and 6, respectively.

The following section looks at false positive recovery and recovering malicious vehicles.

5. Testing for false positives and recuperating malicious vehicles

5.1. Overview

This section features a detailed explanation of the algorithms used by the proposed system to deal with network errors and vehicles that have been previously malicious. However, they recover from exhibiting malicious behaviour. The chapter will include all the equations and mathematical underpinnings of the system. The proposed system incorporates this to improve accuracy in identifying malicious and non-malicious behaviour. Network errors can cause vehicles to drop messages or take longer to deliver. Network errors can lead to false positive identification in the VANET. False positives happen when a vehicle is identified as harmful but exhibit non-malicious behaviour. These vehicles should be identified to ensure non-malicious vehicles are not isolated from network communications. The symbols used in this chapter are described in Appendix B.

The proposed system has the ability to distinguish malicious and non-malicious behaviour in vehicles that belong to a VANET, as shown in chapter 4.7. Malicious vehicles can, however, recover in a VANET and begin to exhibit non-malicious behaviour. This recovery process is made possible by node recovery schemes [128], [129] or malicious entities that abandon vehicles due to a lack of resources. It is imperative that these vehicles be identified in the VANET and allowed to recover their trust value. Identifying vehicles that recover will ensure that non-malicious vehicles in the VANET are not unnecessarily punished by isolation from communication. Establishing vehicles recovering from malicious behaviour enables the proposed system to represent the current, accurate state of the VANET constantly.

This chapter is organised as follows: it begins by defining contributions. VANET architecture will be explained in detail. Simulation scenarios are presented. Performance evaluation of the proposed system against defined scenarios is shown. Results are presented, and the chapter concludes.

5.2. Contributions

The contributions of this chapter are defined below:

- The chapter proposed a system that identified network errors by identifying false positives to enable constant and accurate representation of the VANET at all times. False positives occur when a vehicle can be inaccurately identified as malicious, even exhibiting non-malicious behaviour in the VANET. The proposed system ensures that network errors and false positives do not affect identifying malicious and non-malicious behaviour.

- The chapter proposed a recovery system that enabled recuperating malicious vehicles to regain trust values if behaving honestly. Vehicles behaving maliciously in the VANET have their trust values decreased to a value closer to 0. Alternatively, if a vehicle begins to behave honestly, the trust value should

increase closer to 1. The proposed system should be able to identify this and represent the vehicle behaviour accurately at all times.

5.3. VANET architecture

The proposed system is designed to work within a VANET. In this scenario, the VANET consisted of autonomous vehicles, (V_n) distributed within a particular area where $n = \{1, 2 \dots \dots, V_n\}$ and $n \in \mathbb{N}$. Among the vehicles in the VANET, watchdogs (V'_n) are selected from (V_n) such that: $V'_n \in V_n$. A different set of vehicles $(V"_n)$ sense data from the environment and broadcast it to other vehicles. The set of vehicles sensing data exists such that: $V"_n \in V_n$.

Autonomous vehicles and RSUs available in the area communicate with each other. The purpose of the watchdogs is to gather data on vehicles in the VANET and send the data to the RSU, which calculates a trust value to represent the trustworthiness of a vehicle. The proposed system uses multiple watchdogs to watch to gather data on vehicles.

During the trust message communication round, vehicles not selected as watchdogs automatically act as vehicles being evaluated. The vehicle watchdogs watch these vehicle transactions. During communication rounds where a vehicle has sensed data, the rest of the vehicles in the VANET become destinations for the vehicle broadcast.

5.4. Trust message architecture

This section discusses the details of the architecture and design of trust messages used by the proposed system. The proposed system uses trust messages to calculate the trust values of vehicles. Trust messages are designed to be lightweight to reduce the overheads incurred by the system. The messages are designed to be 160 bits and subdivided into section blocks of 32 bits each. The details of the message are shown in Figure 5.1.

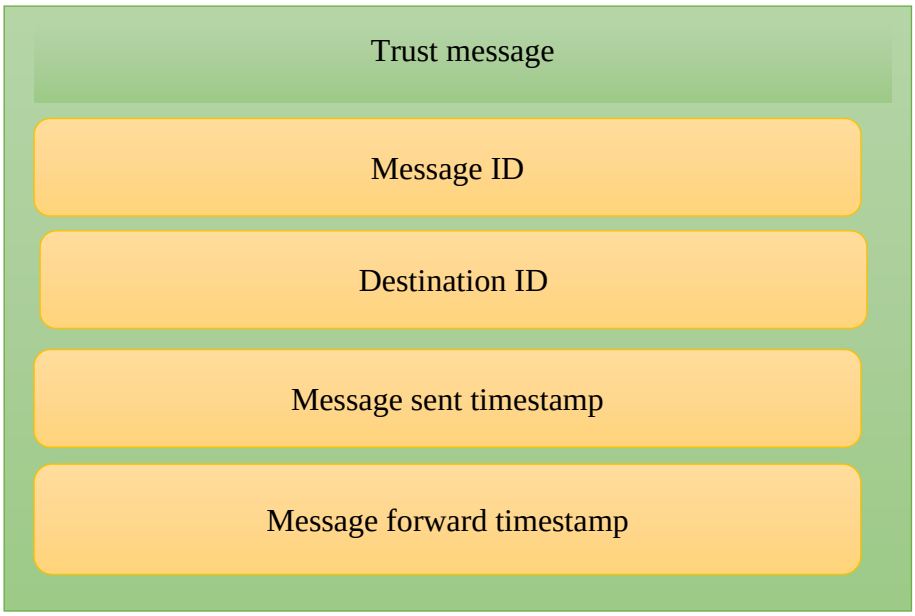

Figure 5.1 - Trust message architecture used by the proposed system.

Further details of the architecture of the trust message are presented in Table 5.1 below.

Table 5.1 - Proposed trust message architecture details.

Name	Description	Size (bits)
Message ID	This is the unique ID that represents the message. Two different messages cannot have the same message ID.	32
Destination ID	This is the unique ID that represents the destination of the message. It indicates to the vehicle where to forward the message.	32
Message sent timestamp	This is the timestamp of the message when sent from the source.	32
Message forward time stamp	This is the timestamp when the message is forwarded by a vehicle to its destination.	32

5.5. Algorithm design

The proposed system uses two algorithms to identify vehicles reporting false positives and recuperating malicious vehicles. These algorithms are presented below:

5.5.1. Algorithm 3

This algorithm aims to create and distribute trust messages in the VANET. This enabled the proposed system to gather data used in algorithms 1 and 2 in calculating trust values. The use of trust messages has the following advantages:

- Trust messages are made to be lightweight so they do not increase the overheads incurred by the proposed system.
- Trust messages promote fairness by enabling the recovery of previously identified malicious vehicles and false positives in the system.
- Using trust messages avoids tampering with network messages that may contain critical data. Algorithm 5.1 details the algorithm responsible for creating and distributing trust messages. Figure 5.2 details the process of the algorithm.

Algorithm 3: Creation and distribution of trust messages

Input: Vehicle map (V_n, R_s)
While $t \in T$: **do**
Output: Trust messages
If $Q_v = \emptyset$ **then**
For $V'_n \in V_n$ **do**
R_s selects V'_n
Source forwards trust messages to V_n
V'_n watch V_n transactions
V'_n sends data to R_s
R_s calculates trust values for V_n via equation 1 – 5
End for
End if
End while

Algorithm 5.1 - Proposed algorithm 3 for the creation and distribution of trust messages

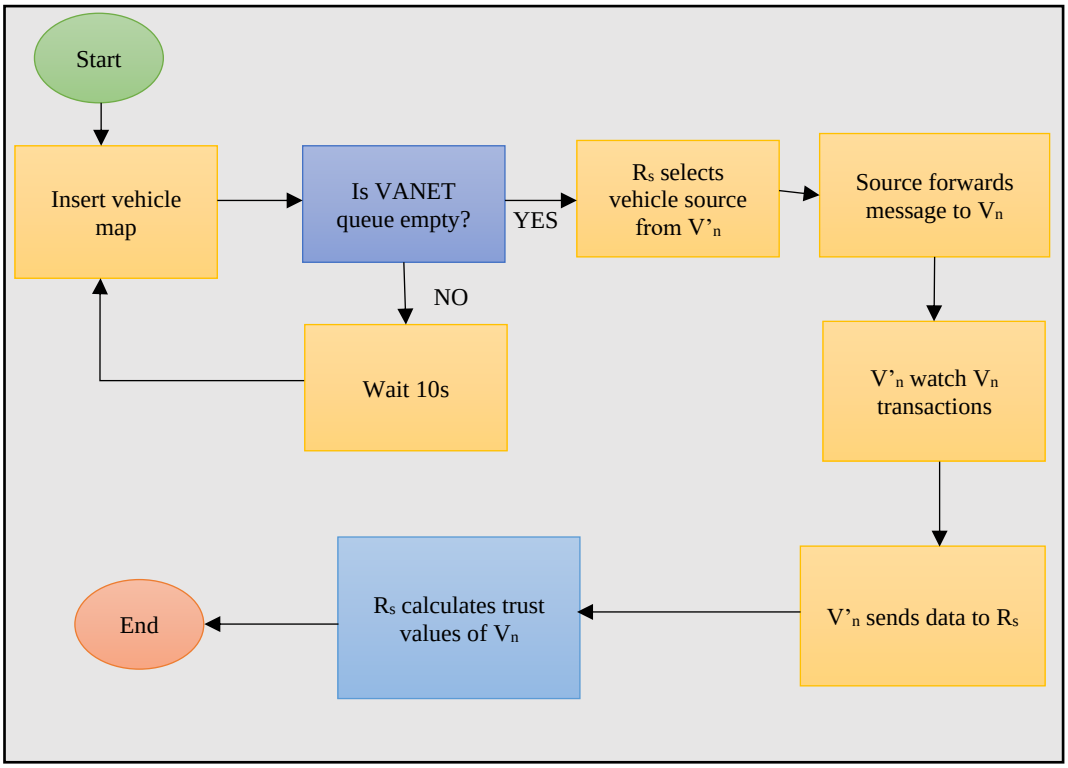

Figure 5.2 - Algorithm 3 process showing the creation and distribution of trust messages in the VANET.

5.5.2. Algorithm 4

This algorithm is used by vehicles during the creation and distribution of network messages. Algorithm 4 will enable vehicles in the VANET to consider trust values before broadcasting network messages. This algorithm in the proposed system allows the vehicles to avoid malicious vehicles when sending messages. Algorithm 5.2 shows the proposed algorithm Figure 5.3 further details the process of algorithm 5.

Algorithm 4: Creation and distribution of network messages

Input: Vehicle map (V_n, R_s)
While $t \in T$: **do**
Output: Network messages

For $V_n, R_s \in N$ **do**
R_s has trust values for all V_n
$V"_n$ senses data in the environment
$V"_n$ requests trust ledger from R_s
$V"_n$ forwards sensed data to trusted V_n
End for
End while

Algorithm 5.2 - Proposed algorithm for the creation and distribution of network messages

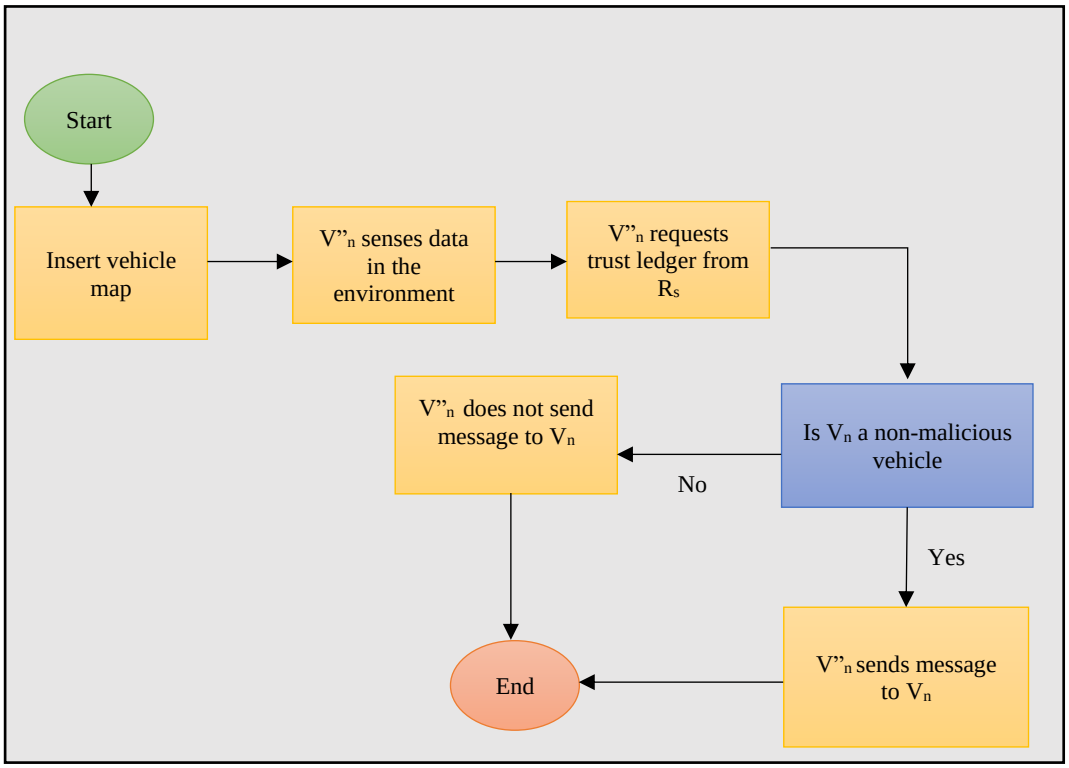

Figure 5.3 - Algorithm 4 process showing the creation and distribution of network messages.

The proposed system combines the algorithms to calculate vehicle trust values in the VANET and allow network messages to be transmitted. The proposed system ensures that the network messages are not currently in transmission or a queue before transmitting trust messages. This method ensures minimal message collisions in the VANET; this improves the efficiency of the VANET—the evaluation of the proposed system requires simulation scenarios to be used. The simulation scenarios are described below.

5.6. Simulation scenario

The hardware and software used to carry out the simulation will be the same hardware specified in the hardware and software specification section in chapter 4.6.
In order to evaluate the trust management system, the scenarios described below were used.

Scenario 1

This scenario evaluated the proposed system against its ability to recover the trust value of vehicles affected by network errors and have encountered false positives. These vehicles behaved honestly in the VANET. However, at specific points in time, due to network errors, the vehicles either dropped messages or took more time to deliver messages. This caused the vehicles to be reported as false positives; they were reported as malicious when they exhibited non-malicious behaviour. This behaviour caused the trust values to drop closer to 0. False positives were simulated in a set of vehicles in the VANET. All vehicles began simulation as fully trusted, with a trust value of 1 and operated honestly in the VANET. Vehicles were simulated to report false trust values at points in time during the simulation—this simulated false positives in the VANET.

Scenario 2

In this scenario, the trust management system was evaluated by its ability to identify vehicles that have been malicious but have recuperated to honest behaviour. Three VANET scenarios were used to investigate this phenomenon.

- VANETs were populated with both malicious and non-malicious vehicles. Malicious behaviour involved the vehicles dropping messages at different rates in the VANET. The vehicle then stopped the malicious behaviour and exhibited non-malicious behaviour in the VANET.

- VANETs with vehicles portray both malicious and non-malicious behaviour. Malicious behaviour in this scenario will involve vehicles delaying messages at different rates in the VANET. At random points in time, the malicious behaviour will drop the behaviour and exhibit non-malicious behaviour.

- VANETs were made up of vehicles exhibiting both malicious and non-malicious behaviour. Malicious behaviour in this scenario involved the vehicle dropping and delaying messages at different rates in the VANET. The malicious vehicles during the VANET operation recovered to exhibit non-malicious behaviour.

The vehicles began operations as fully trusted, with a trust value of 1. The vehicles exhibited normal behaviour at the start of VANET operations. A set of vehicles exhibited malicious behaviour for periods of VANET operations. The set of vehicles went back to exhibiting normal behaviour. Further simulation details are given in Table 5.2 below.

Table 5.2 - Simulation details of the experiment that checked for false positives and recuperating malicious vehicles.

Parameters	Value
Area of network	200m^2
Number of vehicles	8
Transmission range	20m
Number of watchdogs	3
Initial trust value	1.0 (Trusted)
Trust threshold	0.7
Simulation time	360s
Malicious vehicles	3
Evaluated vehicles	4
Number of vehicles sensing data	1

5.7. Performance evaluation

This section will feature the results from the performance evaluation of the proposed system concerning the simulation scenarios described above in section 5.6.

False positives

In this experiment, the evaluated vehicles began operations as fully trusted and exhibited non-malicious behaviour. The vehicles exhibited honest behaviour throughout VANET operations.

Network errors were simulated in the VANET and caused vehicles to drop and delay messages in the VANET. These led to the vehicles being identified as malicious at specific times, even though they exhibited non-malicious behaviour. Hence, these network errors caused false positives in the VANET. Figure 5.4 displays the results of this experiment.

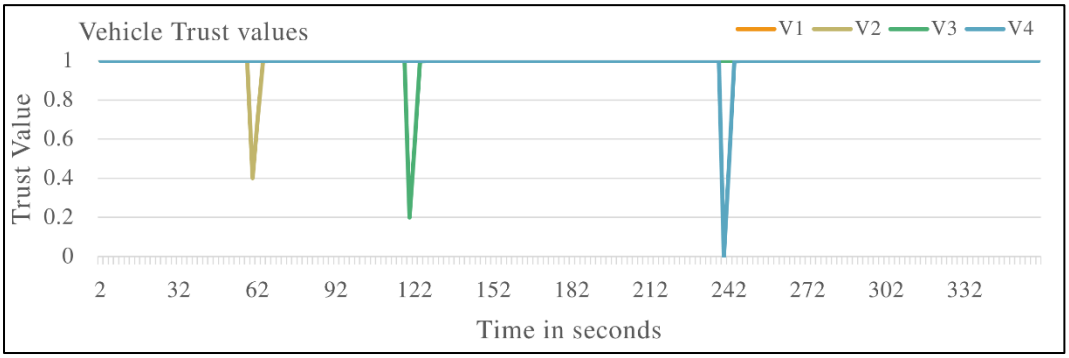

Figure 5.4 - Vehicle trust values in the experiment simulating false positives occurring in the VANET.

Figure 5.4 shows that V2, V3 and V4 experienced a sudden drop and rise in their trust values at 60s, 120s and 240s, respectively. The vehicles were identified as false positives in the VANET due to sharp drops and rises. Malicious behaviour and the subsequent recovery of malicious behaviour resulted in a more gradual drop and rise in the trust value, as shown in Figure 4.4, Figure 4.8, and Figure 4.12. The VANET maintained a constant one throughout operations. The above results showed that network errors during VANET operation did not affect the proposed system. The trust value of the VANET was not affected by network errors and false positives. In real-world scenarios, network errors can be caused by interferences, failures or obstacles

that limit communication for a short time. As a result, false positives may be reported in the VANET.

Recovering malicious vehicles

In this experiment, the proposed system was evaluated against vehicles that exhibited malicious behaviour and then recovered to exhibit non-malicious behaviour. Among the evaluated vehicles, a set started operations exhibiting non-malicious behaviour. At random points, the vehicles exhibited malicious behaviour for a limited amount of time, and after some time, the vehicles recovered to exhibit non-malicious behaviour.

The first experiment evaluated the proposed system against vehicles that exhibited malicious behaviour and delayed messages. The vehicles began operations fully trusted and behaved non-maliciously. During VANET operations, the vehicles exhibited malicious behaviour and delayed messages. The vehicles then recovered and exhibited non-malicious behaviour. The results of this experiment are shown below. Figure 5.5 shows the trust values of vehicles from this experiment.

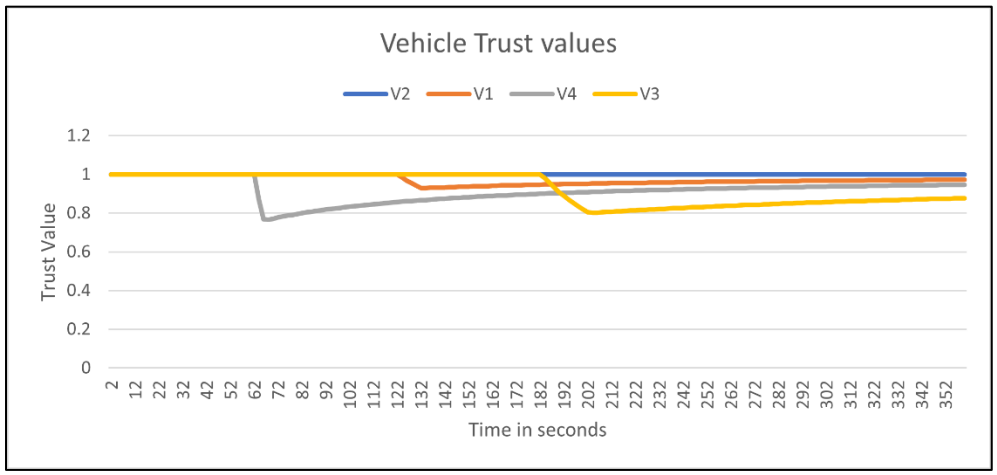

Figure 5.5 - Vehicle trust values in the experiment where malicious vehicles recuperated to non-malicious behaviour (vehicles delayed messages before forwarding to destination).

V2 was identified as a vehicle exhibiting non-malicious behaviour as it maintained a trust value 1.0 throughout VANET operations. During VANET operations, V4, V1, and V3 dropped their trust values indicating the vehicles exhibited malicious behaviour. This happened at 60s – 65s, 120s – 130s and 180s – 200s respectively. The vehicles then began to recover their trust values. This indicates that the vehicles had recovered and were now exhibiting non-malicious behaviour. The proposed system successfully identified vehicles that recovered from malicious behaviour when the malicious behaviour involved vehicles delaying messages in the VANET. Figure 5.6 shows the overall trust value of the VANET from the above experiment.

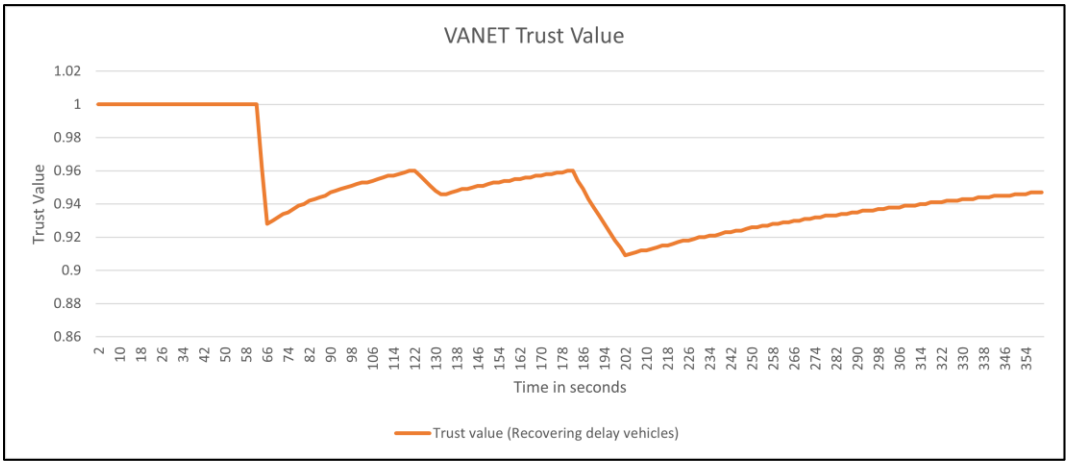

Figure 5.6 - VANET trust value in the experiment where malicious vehicles recuperated to non-malicious behaviour (vehicles that delayed messages before forwarding to destination).

The VANET at the beginning of operations indicated no malicious vehicles present, as the trust value remained at a constant value of 1.0. At 60s - 65s, the VANET trust value dropped, indicating a vehicle behaving maliciously in the VANET. The drop happened at 120s – 130s and 180s – 200s, indicating the presence of malicious vehicles in the VANET. After the 65s, 130s and 200s, the VANET trust value rose, indicating that the vehicles in the VANET are now behaving non-maliciously. Each time a vehicle behaved maliciously in the VANET, the trust value dropped to indicate the current state of the VANET. Once the vehicle exhibited non-malicious behaviour, the trust value rose. The proposed system succeeded in identifying the current state of the VANET constantly throughout VANET operations. The PDR was a constant 1 and indicated all packets were successfully delivered to the destination. It is true because although vehicles delayed messages in the VANET, they were still forwarded successfully to the destination. Figure 5.7 shows the delay of the VANET in the above experiment.

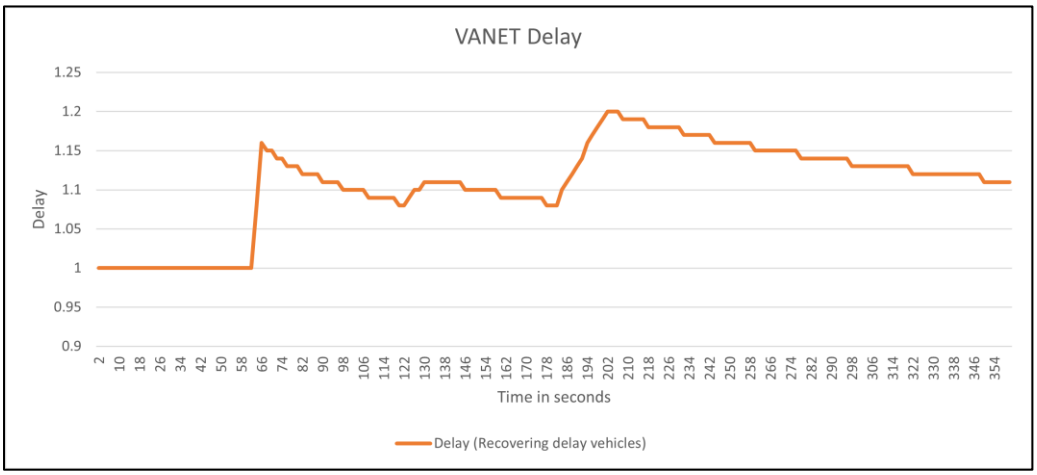

Figure 5.7 - VANET Delay in the experiment where malicious vehicles recuperated to non-malicious behaviour (vehicles that delayed messages before forwarding to destination).

The delay of the VANET indicated the current state of the VANET. When vehicles exhibited malicious behaviour and delayed packets, the overall delay of the VANET increased. As soon as vehicles began behaving non-maliciously, the overall delay of the VANET dropped. This confirmed Figure 5.5 that vehicles exhibited malicious behaviour but recovered to non-malicious behaviour during VANET operation.

The following experiment applied the proposed system to a VANET of vehicles exhibiting malicious and non-malicious behaviour. Malicious behaviour in this experiment involves vehicles dropping messages rather than forwarding the messages to the intended destination. Vehicles began operations exhibiting non-malicious behaviour. At specific points, the vehicles exhibited malicious behaviour dropping messages at different rates. The vehicles then recovered to non-malicious behaviour. The results of this experiment are presented below. Figure 5.8 shows the trust values of the vehicles from the experiment.

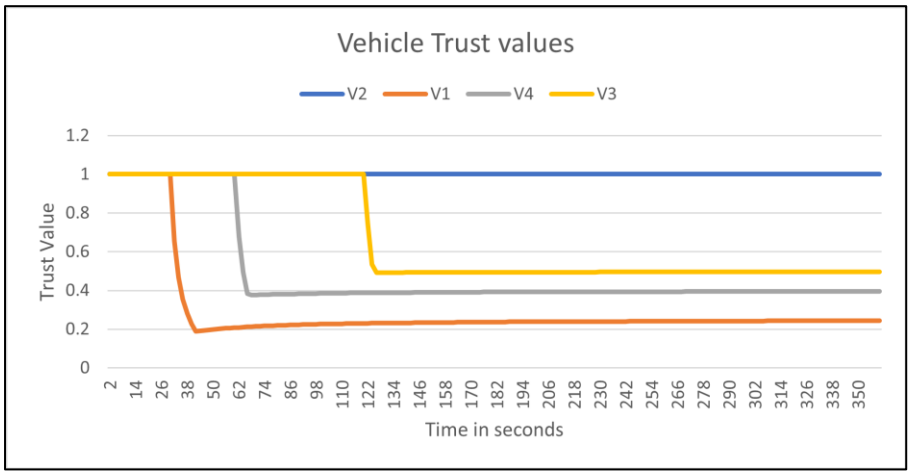

Figure 5.8 - Vehicle trust values in the experiment where malicious vehicles recuperated to non-malicious behaviour (vehicles dropped messages before forwarding to destination).

V2 is identified as a vehicle exhibiting non-malicious behaviour throughout VANET operations, as its trust value is constantly 1. V1's trust value fells sharply between 30s – 40s, indicating malicious behaviour in the vehicle. After 40s, the trust value improved, indicating V1 started to exhibit non-malicious behaviour. The same behaviour observed in V4 and V3, which dropped packets between 60s – 65s and 120s – 122s, respectively, indicates malicious behaviour during those periods. Once both vehicles recovered to non-malicious behaviour, their trust values improved. It is noted that the vehicles' trust values did not recover to a level above the trust threshold. This challenge has opened up a future research direction to optimise the recovery of trust value for vehicles that are dropping packets. Figure 5.9 shows the overall trust value of the VANET from the above experiment.

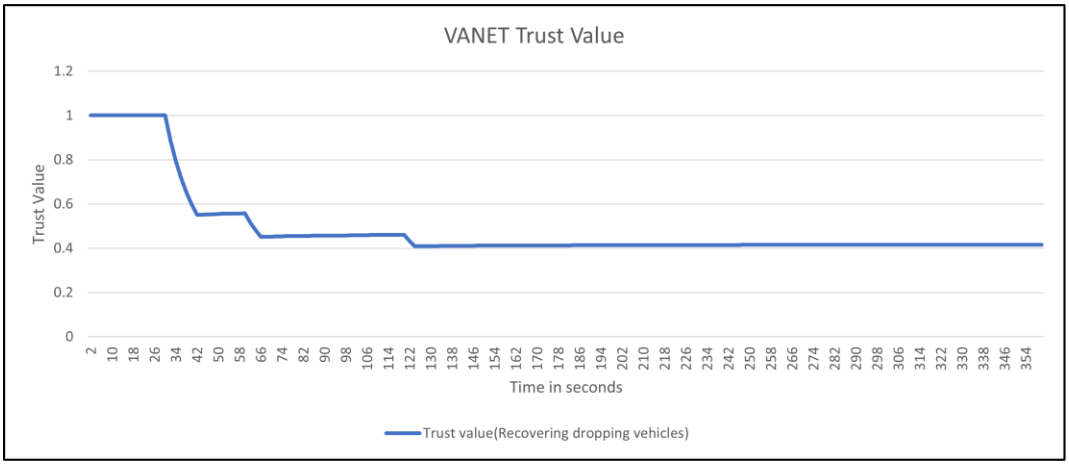

Figure 5.9 - VANET trust value in the experiment where malicious vehicles recuperated to non-malicious behaviour (vehicles that dropped messages before forwarding to destination).

The trust value of the VANET was at a constant 1.0 at the beginning up to 30s of VANET operations; this indicated all vehicles were exhibiting non-malicious behaviour. During the time periods, 30s – 40s, 60s – 65s and 120s -122s indicated a presence of vehicles exhibiting malicious behaviour in the VANET. At 40s – 60s, 65s – 120s, and after 122s, the trust value of the VANET improved. This indicated that vehicles in the VANET exhibited non-malicious behaviour in the VANET. These results were further analysed by looking at the overall PDR of the VANET shown in Figure 5.10.

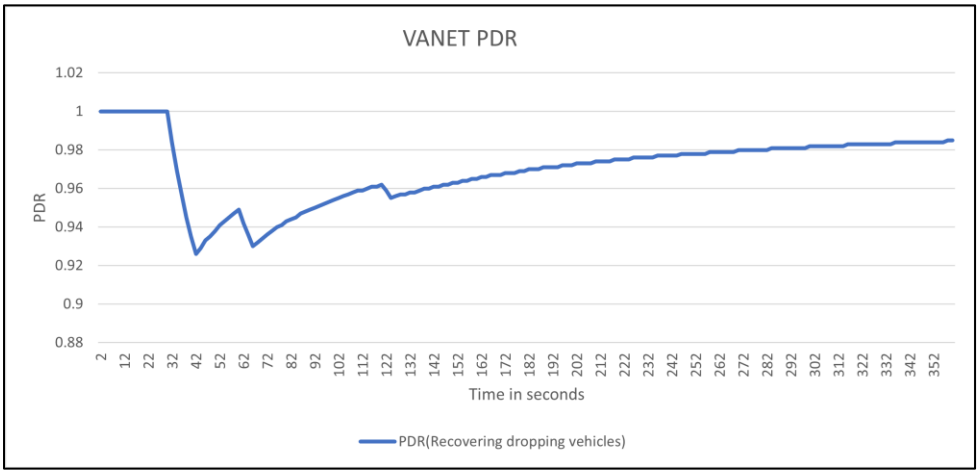

Figure 5.10 - VANET PDR in the experiment where malicious vehicles recuperated to non-malicious behaviour (vehicles that dropped messages before forwarding to destination).

The VANET PDR confirmed that malicious vehicles dropped messages in the VANET. When vehicles exhibited malicious behaviour between 30s – 40s, 60s – 65s and 120s -122s, the PDR of the VANET declined as vehicles dropped messages in the VANET. Once the vehicle recovered to non-malicious behaviour and began delivering messages to the destination, the PDR of the VANET increased to reflect this. The proposed system successfully accurately represented the PDR of a VANET in the presence of malicious vehicles that began with non-malicious behaviour dropping messages at different rates before recovering to non-malicious behaviour. The trust values of the VANET and individual vehicles did not recover to a level above the trust threshold. This challenge will be investigated and optimised in future research.

In the next experiment, the proposed system was evaluated against a VANET that contained malicious vehicles, both delaying and dropping messages. Among the evaluated vehicles, a set was selected to exhibit malicious behaviour randomly during VANET operations. Malicious behaviour in the VANET involved delaying messages, dropping messages and both delaying and dropping packets at time intervals. Although the proposed system was successful in scenarios where malicious vehicles were dropping and delaying messages independently, it is necessary to evaluate the proposed system against multiple types of malicious vehicles present. Figure 5.11 shows the trust value of the evaluated vehicles in the VANET.

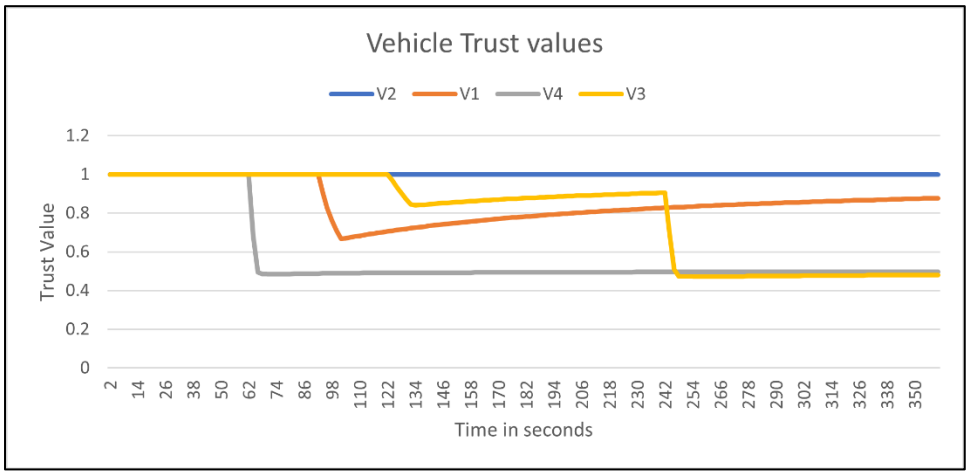

Figure 5.11 - Vehicle trust values in the experiment where malicious vehicles recuperated to non-malicious behaviour (multiple malicious behaviours).

V2 maintained a trust value of 1.0 throughout the VANET operation. This indicated that V2 was exhibiting non-malicious behaviour throughout the VANET operations. V4 began operations behaving non-maliciously. However, the trust value dropped rapidly to 60s – 65s. This indicated that V4 exhibited malicious behaviour. After 65s, the trust value of V4 began to improve as the VANET operated. This indicated that V4 started to exhibit non-malicious behaviour. V1 began operations behaving non-maliciously as its trust value was constant at 1.0. However, in 90s, its trust value dropped, indicating it started to behave maliciously. At the 100s, its trust value rose, indicating V1 exhibited non-malicious behaviour. V3 began operations behaving in a non-malicious manner; this was indicated in its trust value at constant 1.0. At 120s of VANET operations, V3's trust value dropped, indicating the vehicle exhibited malicious behaviour. At 130s, V3 trust value began to rise, indicating the vehicle recovered to non-malicious behaviour. Between 240s – 245s, the trust value of V3 dropped to indicate the vehicle was behaving maliciously. At 245s, the trust value rose, indicating the vehicle exhibited non-malicious behaviour. Figure 5.12 shows the overall trust value of the VANET in the experiment above.

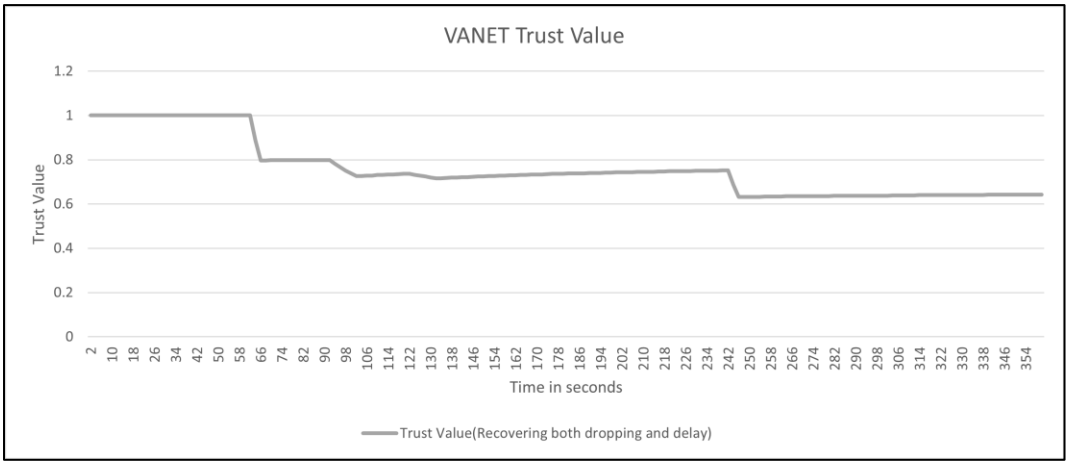

Figure 5.12 - VANET trust value in the experiment where malicious vehicles recuperated to non-malicious behaviour (multiple malicious behaviours).

A drop in the trust value was noted in the 60s, 90s, 120s and 240s of VANET operations. This indicated that the VANET had been taken over by vehicles exhibiting malicious behaviour. As soon as vehicles recovered to non-malicious behaviour, the trust value of the VANET rose. These results indicated the current state of the VANET. Figure 5.13 and Figure 5.14 show the PDR and delay of the VANET, respectively.

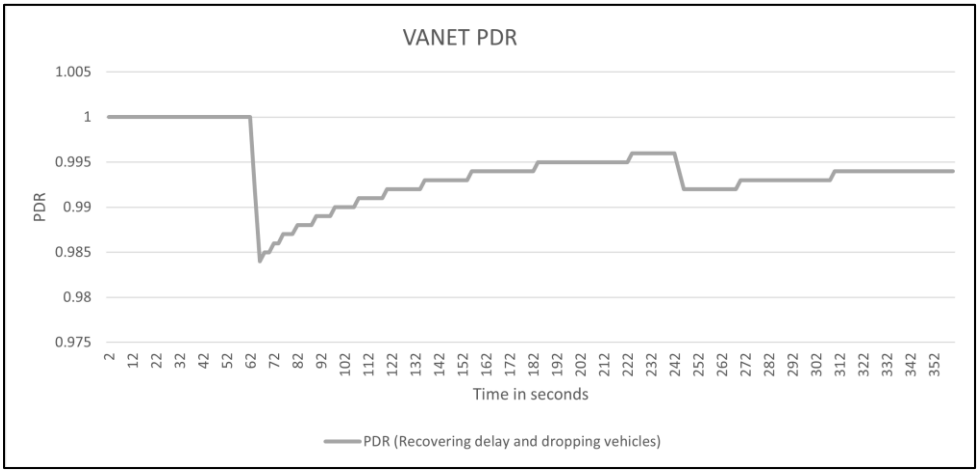

Figure 5.13 - VANET PDR in the experiment where malicious vehicles recuperated to non-malicious behaviour (multiple malicious behaviours).

The VANET PDR indicated the current state of the VANET. Whenever malicious vehicles were present in the VANET dropping messages, the PDR of the VANET dropped to reflect this. Once vehicles recovered to non-malicious behaviour, the PDR increased to reflect this. Similar results were shown in the delay of the VANET in Figure 5.14. When malicious vehicles were present in the VANET delaying messages, the delay of the VANET increased. The delay meant messages in the VANET took longer to be delivered to the destination. Once vehicles recovered to non-malicious behaviour and vehicles stopped delaying messages. The VANET delay decreased to reflect that messages took less time to deliver.

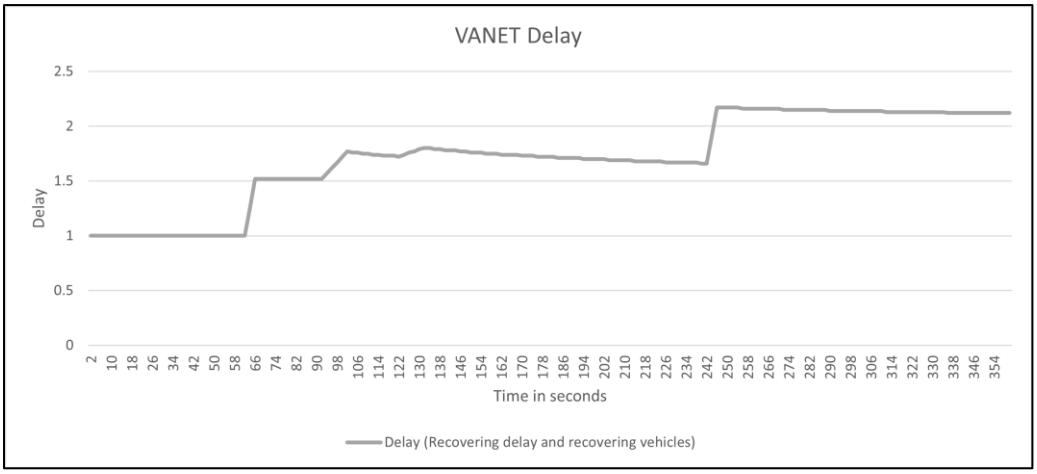

Figure 5.14 - VANET Delay in the experiment where malicious vehicles recuperated to non-malicious behaviour (multiple malicious behaviours).

The process of recovering from malicious behaviour to non-malicious behaviour is made possible by the system's ability to give malicious vehicles a chance to recover their trust values. It is made possible by isolating vehicles during network message transmission. The isolation of malicious vehicles ensures network messages are not transmitted to malicious vehicles. Vehicles regained trust values while transmitting trust messages. If the vehicles successfully transmitted trust messages, the trust value rose, and the vehicles returned to the pool of non-malicious vehicles. While if they exhibited malicious behaviour by dropping or altering trust messages, the trust value dropped.

The following criteria used to evaluate the proposed algorithms will be the complexity analysis. This analysis will assist in identifying the resource consumption of the algorithm in relation to the input size. Two sets of complexities were used for this purpose, time complexity and space complexity.

Table 5.3 - Algorithm complexity for algorithms 4 and 5.

Name	Time complexity	Space complexity
Algorithm 3: Creation and distribution of trust messages.	$O(n^2)$	$O(n)$
Algorithm 4: Creation and distribution of network messages.	$O(n)$	$O(n^3)$

The algorithm complexity considers the worst-case scenario for an algorithm. Therefore the worst-case scenario of the algorithm is shown in Figure 5.15 and Figure 5.16.

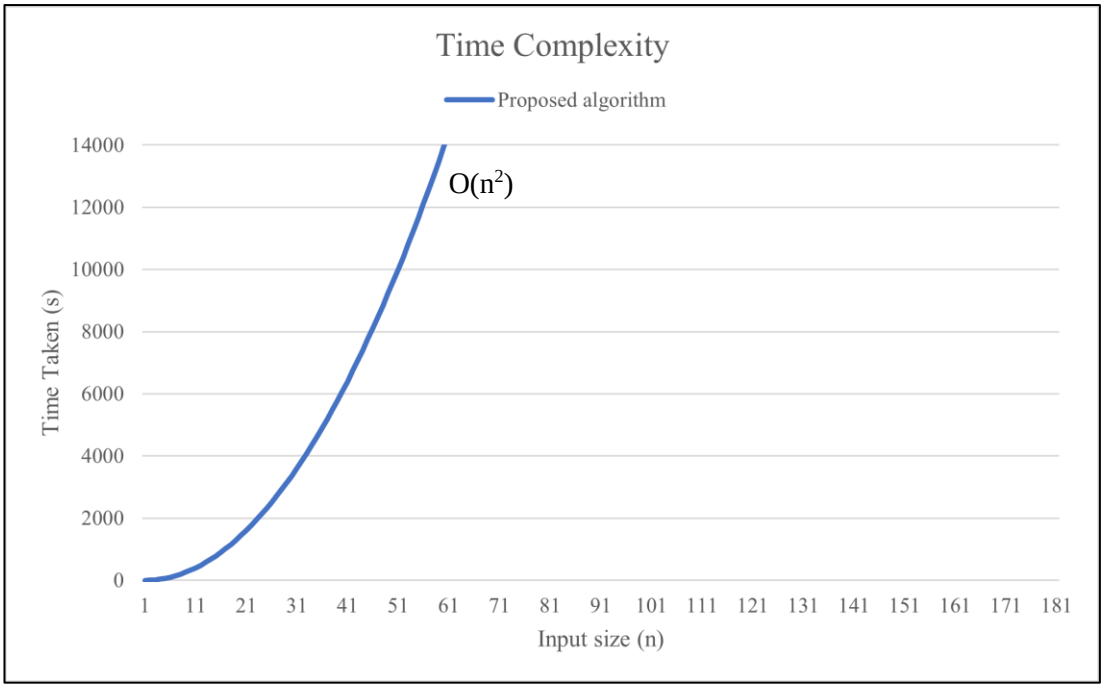

Figure 5.15 - Time complexity of the proposed algorithms 3 and 4.

The time complexity is identified as $O(n^2)$. The time complexity means the algorithm's runtime will proportionally grow to the square of the input size. Figure 5.16 shows the space complexity of the algorithm. The space complexity was found to be $O(n^3)$. The space complexity means that the algorithm requires more memory proportional to the cube of the input size.

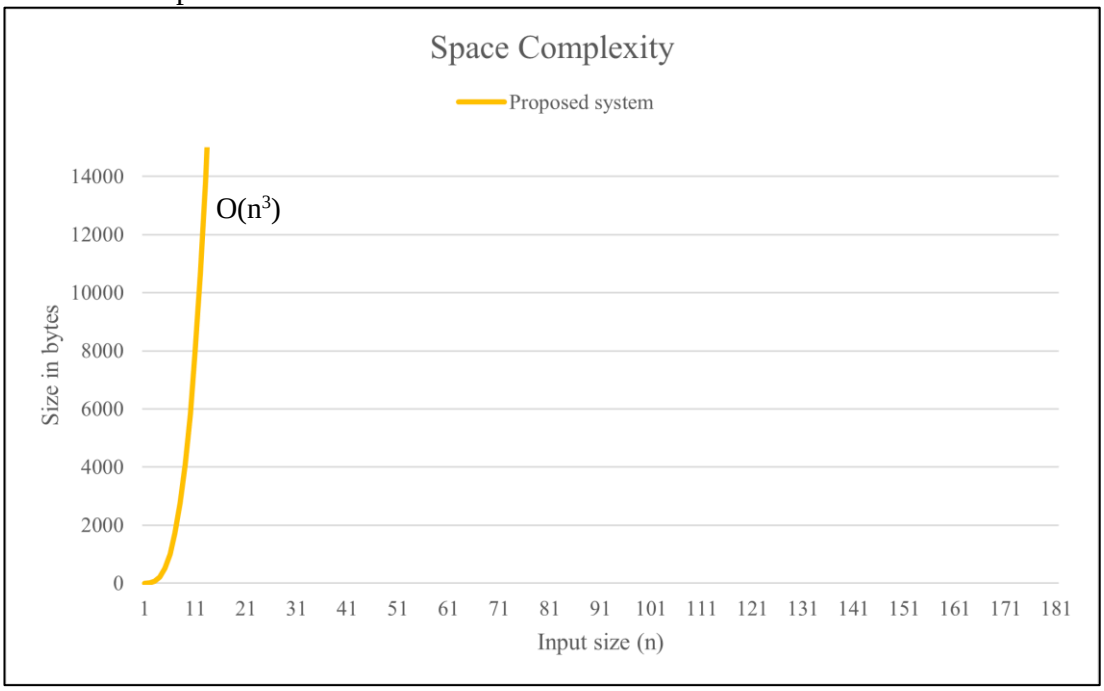

Figure 5.16 - Space complexity of algorithms 3 and 4.

5.8. Summary

This chapter has presented an extension of the proposed system in chapter 4 of this work. It presented the trust management system's ability to identify false positives caused by network errors in the VANET. Additionally, it presented the proposed

system's ability to identify recuperating malicious vehicles that have previously acted malicious but have recovered to non-malicious behaviour. The proposed system was applied to different scenarios, including experiments that simulated false positives via network errors. The proposed system was also applied to a VANET of malicious vehicles that recovered to non-malicious behaviour. Malicious behaviour included vehicles that are dropped and delayed messages and vehicles that are both dropped and delayed.

The results of these experiments were presented and discussed. Results showed that the proposed system successfully identified vehicles affected by network errors that are reported false positives. The proposed system also successfully identified malicious vehicles that recovered to non-malicious behaviour. However, vehicles that dropped packets find it hard to recover to a fully trusted status. This challenge will be investigated in future work.

6. Watchdog selection process that includes fairness and historical behaviour of vehicles.

6.1. Overview

The watchdog selection process is a crucial part of the proposed trust management system to enhance security. It formally discusses the watchdog selection process for the proposed trust management system. It includes all the concepts that make up the selection and monitoring process. The chapter outlines all mathematical concepts and underpinnings. Each vehicle in the VANET has a watchdog agent and can be enabled dynamically to monitor neighbour vehicles if selected. It is, therefore, crucial to ensure optimal watchdog selection.

The proposed watchdog selection system uses an RSU as a centralised processing point. The RSU makes computations at a single point, reducing the overhead experienced by individual vehicles. Certain vehicles will be identified within a cluster in the proposed system, and the watchdog agent will be enabled in these vehicles. This will enable the trust management system to execute its next phase of operations. Watchdogs are identified as one-hop neighbours to the RSU.

The proposed system utilizes two methods to select watchdogs in the VANET, direct and indirect watchdog selection. Direct watchdog selection is preferred, but indirect watchdog selection is employed when not available. Direct watchdog selection involves using the previous operational history of the vehicle and residual energy to calculate the viability of a vehicle to become a watchdog. Indirect watchdog selection is used when VANET vehicles lack an operational history. In this case, the vehicle's history must be established before being selected as a VANET watchdog. Vehicle evaluation is done by collecting vehicle data and calculating a value representing vehicle behaviour. This data includes the PDR and processing delay of packets sent. This data, including the vehicle's residual energy, is calculated to establish optimal watchdogs in the VANET.

In the same way, AODV uses RREQs and RREPs to establish routes in a VANET. The proposed system uses specialized RREQ and RREP packets to select the most optimal watchdogs. The RREQ packets request a trust value from vehicles to establish the operational history of the vehicle; residual energy is also requested in the RREQ packet. The vehicles reply to the RSU with trust value and residual energy in the RREP packet. If the vehicle has no operational history, it will only return residual energy. The RSU will use the RREQ and RREP message details to calculate the optimal watchdogs. It will do this by comparing the number of RREP messages received to the number of RREP messages sent. It will also establish the time taken to reply to RREP messages by vehicles. This data will help the RSU select optimal watchdogs for the VANET. In order to promote fairness, vehicle residual energy is also considered. Vehicles with higher residual energy are more likely to be considered watchdogs than vehicles with lower residual energy. The watchdog agent consumes slightly more energy collecting data and sending it to the RSU for processing. Therefore, watchdog vehicles may have less residual energy than other trusted vehicles in the VANET. By considering residual energy, other trusted vehicles were given a chance to be selected as watchdogs. Previously selected watchdogs may have

less residual energy and will not be selected; therefore, they are also evaluated before being watchdogs again. The RSU uses this data to determine the optimal vehicle watchdogs for the VANET. The following section outlines this chapter's contributions in detail.

6.2. Contributions

The main contribution of this chapter is described below.

- The chapter proposed a watchdog selection strategy that considered trustworthiness and fairness to ensure the optimal selection of watchdogs in the VANET. The watchdogs were selected based on their operational history. That is, did they behave non-maliciously or maliciously in previous communication rounds. Fairness was ensured by considering the residual energy of vehicles in the VANET.

6.3. VANET architecture

In this scenario, the VANET comprises a set of autonomous vehicles (V_n) and RSUs (R_s), where $n = \{1, 2, 3, \dots, V_n\}$, $n \in \mathbb{N}$ and $s = \{1, 2, 3, \dots, R_s\}$, $s \in \mathbb{N}$. A set of watchdogs must be selected among these vehicles by the RSU. Before selecting the watchdogs, the RSU considers the trust value from previous communication rounds and the residual energy. The selection process is further discussed below.

6.4. Watchdog selection

The two methods used to select watchdogs are discussed in this section.

6.4.1. Direct watchdog selection

This section will feature the selection criteria and process the RSU will execute to select the watchdogs in the VANET. This section features the direct watchdog selection process. The first step is the RSU (R_s) will request the trust values (ω_x), residual energy (γ_i), and initial energy (β_j) from vehicles in the VANET. The data is gathered by a particular type of packet created for this purpose. RREQ packets are extended to where vehicles must include their trust value and residual energy in the RREP sent back to the source. The packets are designed to be lightweight, so the overall overhead incurred by the proposed system will not be significantly affected. Once RSU receives the data, it identifies the viable watchdogs via the following equation. For each V_n in the VANET, its watchdog viability is:

$$\underset{\text{validity}}{watchdog} = \omega_x + \sum_i^I \sum_j^J \left(\frac{\gamma_i}{\beta_j}\right) \qquad \text{Equation 6}$$

Where: $x = (1,2, \dots, \omega_x), i = (1,2, \dots, I), j = (1,2, \dots, J)\ and\ x, I, J \in \mathbb{N}$

The higher the value of this equation, the more likely a vehicle will be selected to be a watchdog in the VANET. This conclusion is because a higher value indicates the vehicles with the highest energy and highest trust value. A high trust value indicates a secure and optimal vehicle to be selected as a watchdog. The R_s in the VANET must

select at least two watchdogs; therefore, the highest values of equation 6 are selected as watchdogs. If any other vehicles match the highest values, they are also selected as watchdogs. The set of selected watchdogs exists in the VANET such that:

$$V'_n \ where\ n = \{1, 2, \ldots \ldots N, \}\ and\ V'_n \in V_n$$

Direct watchdog selection is used when vehicles already have an operational history in the form of a trust value present from previous communication rounds. In cases where vehicles have no operational history and less than two vehicle watchdogs have been selected, indirect watchdog selection is used.

6.4.2. Indirect watchdog selection

In indirect watchdog selection, RSU must create some operational history to select a secure watchdog. To achieve this, the R_s will forward a set of RREQ packets (X_a) to vehicles in the VANET. The RSU records the time of sending RREQ (Ty). Vehicles will reply with RREP packets sent to R_s. The number of RREP packets received (Y_b) and time of RREP receipt (T_z) is recorded by R_s. The watchdog viability of a vehicle (V_n) is given by:

$$\underset{\text{validity}}{watchdog} = \left(\sum_a^A \sum_b^B \left(\frac{Y_b}{X_a}\right)\right) + \left(\sum_z^Z \sum_y^Y \left(\frac{T_z - T_y}{Z}\right)\right) + \left(\sum_j^J \sum_i^I \left(\frac{\gamma_i}{\beta_j}\right)\right) \quad \text{Equation 7}$$

Where:

$$a = (1,2, \ldots, A), b = (1,2, \ldots, B), z = (1,2, \ldots, Z), y = (1,2, .., Y) and\ A, B, Z, J \in \mathbb{N}$$

The vehicles with the highest values of this equation are selected to be watchdogs in the VANET. A higher value indicates the vehicles with the highest energy, the quickest time to reply, and the highest ratio of RREQ replies. These high values indicate a secure and optimal vehicle to be selected as a watchdog. The R_s in the VANET must select at least two watchdogs; therefore, the highest values of equation 6 are selected as watchdogs. If any other vehicles match the highest values, they are also selected as watchdogs. The set of selected watchdogs exists in the VANET such that:

$$V'_n \ where\ n = \{1, 2, \ldots \ldots N, \}\ and\ V'_n \in V_n$$

The following section presents the algorithm the proposed system uses to achieve its objectives.

6.5. Algorithm design

This algorithm aims to select the most secure and optimal watchdogs in the VANET. This algorithm uses equations 6 and equation 7 to achieve its purpose. Selecting secure and optimal watchdogs enables the trust management system proposed in Chapter 4 of this work to perform its objective function. This algorithm is shown in Algorithm 6.1. The algorithm is further detailed in the process diagram in Figure 6.1.

Algorithm 5: Watchdog selection (V'_n)

Input: Vehicle map (V_n, R_s)
While $t \in T$: **do**
Output: (V'_n)
    For $R_s \in N$ **do**
        For $V_n \in N$ **do**
        R_s sends RREQ messages to V_n
        V_n sends RREP messages to R_s
        If V_n has trust value present **then**
            R_s calculates V'_n via equation 6
        End if
        If V_n has no trust value present **then**
            R_s calculates V'_n via equation 7
        End if
    End for
End while

Algorithm 6.1 - Proposed algorithm for watchdog selection

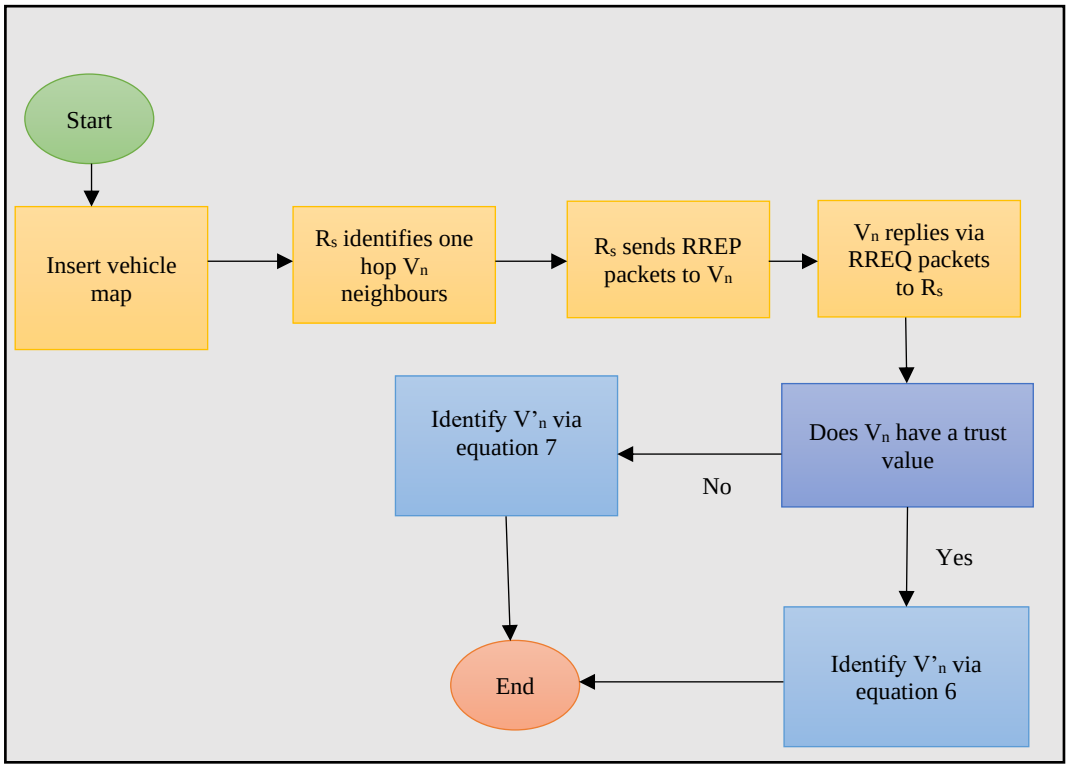

Figure 6.1 - Algorithm 5 process used to select secure and fair vehicle watchdogs in the VANET.

6.6. Simulation scenario

The proposed system was evaluated against its ability to select watchdogs in a VANET. The simulation scenario consisted of five vehicles and one RSU. In the simulation scenario, the RSU selected watchdogs from a set of vehicles. Figure 6.2 shows details of the simulation scenario.

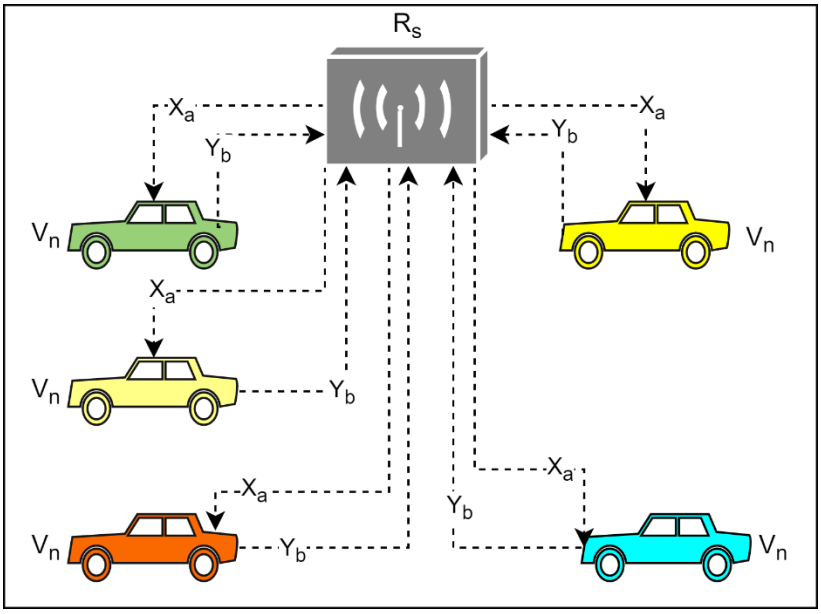

Figure 6.2 - VANET topology used in the watchdog selection process.

Vehicle behaviour was varied in the simulations to evaluate the proposed system's ability to select secure and optimal watchdogs. The behaviour was varied by fluctuating variables ω_x, γ_i, β_j, T_y, Y_b. The evaluation of this is presented in the next section.

6.7. Performance evaluation

This section shall feature the performance evaluation of the proposed system within different scenarios. Table 6.1 shows the simulation details of vehicles during the initial deployment of VANET. These values were used to create a baseline value for the proposed system as it assumes the perfect behaviour of vehicles. The simulation ran for 10 seconds.

Table 6.1 - Initial vehicle baseline attributes for the vehicle watchdog experiment.

Vehicles	RREQ packets (X_a)	RREP packets (Y_b)	Time taken to reply RREP (X_z)-(T_y)	residual energy (γ_i),	initial energy (β_j)
V_1	45.0	45.0	2.0	80.0	100.0
V_2	45.0	45.0	2.0	80.0	100.0
V_3	45.0	45.0	2.0	80.0	100.0
V_4	45.0	45.0	2.0	80.0	100.0
V_5	45.0	45.0	2.0	80.0	100.0

RREP Packets – This scenario involved varying the number of RREP packets sent as replies to RREQ packets sent by the vehicles in the VANET. Vehicles that replied to all RREQ packets, with RREP packets, indicated non-malicious behaviour in the VANET. Malicious vehicles tended to drop packets in the VANET, therefore, did not send RREP packets in the VANET. In the first instance, vehicles ran operations while transmitting all RREO replies to RREQs sent by R_s. In concurrent instances, some vehicles in the VANET were randomly assigned to drop RREQ packets and not send RREP packets. These vehicles should not be selected as watchdogs by the proposed

system. Vehicles which do not reply to RREQ packets should not be selected as watchdogs in the VANET. Figure 6.3 shows the results of this experiment.

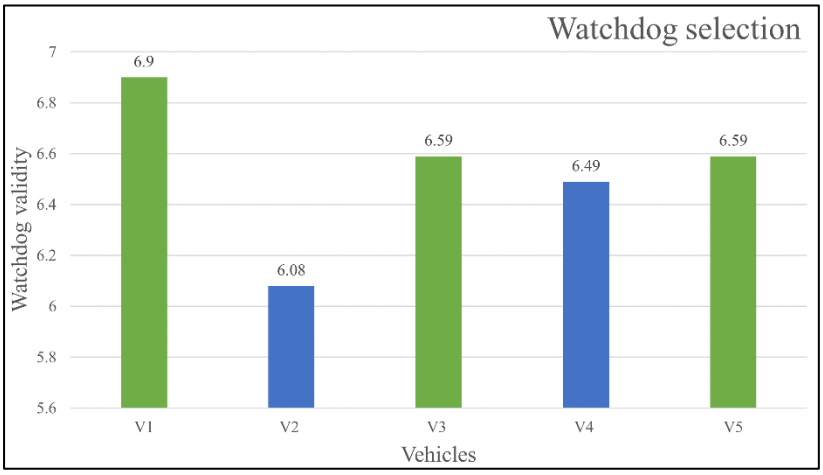

Figure 6.3 - Vehicle watchdogs in the experiment that varied the RREP packets from each vehicle.

This experiment selected V1, V3 and V5 as watchdogs in the VANET. V1 had the highest viability to be selected as a watchdog. Vehicles V3 and V5 had the same watchdog viability and were also selected as watchdogs. Vehicles V2 and V4 were identified as not replying to RREQ messages. The vehicles were, therefore, not selected as watchdogs; they were added to the set of vehicles to be evaluated.

Time taken to reply to RREQ packets – In this scenario, the time taken to reply to RREQ packets was varied to evaluate the performance of the proposed system. Vehicles which took shorter times to reply to RREQ packets should be given priority to be watchdogs in the VANET, and shorter reply times indicated non-malicious behaviour. Malicious vehicles tend to spend more time replying to RREQ packets. Shorter times to reply to RREQ packets also indicated optimal watchdog selection. The vehicles began operations with equal packet reply times in the first instance. In concurrent instances, randomly selected vehicles had increased packet reply times to RREQ packets. The increased reply times were achieved by delaying the RREP packets. These vehicles should not be selected to be watchdogs by the proposed system. Figure 6.4 shows the results of this experiment.

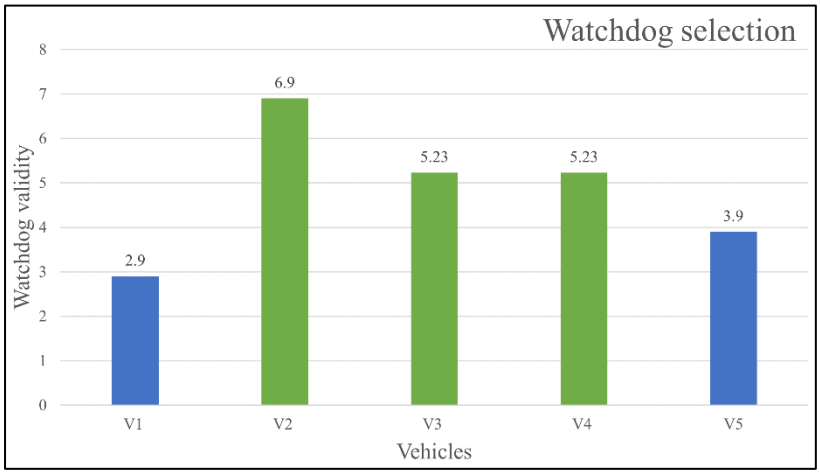

Figure 6.4 - Vehicle watchdogs in the experiment where the time taken to reply to RREQ packets was varied between vehicles.

In this experiment, vehicles V2, V3 and V4 were selected as watchdogs in the VANET for the communication round. V2 had the highest watchdog viability, while V3 and V4 had the second highest. Vehicles V1 and V5 were identified as vehicles that took longer to reply to RREP messages. The vehicles were, therefore, not selected as watchdogs; they were added to the set of vehicles to be evaluated.

Residual energy – All vehicles began operations with an initial energy of 100J. The vehicles in the VANET all exhibit the same behaviour in the VANET, except for the residual energy. The vehicles have used some energy to navigate roads and previous communication rounds, therefore having different residual energy levels. Vehicles with higher residual energy should be selected as watchdogs over vehicles with lower residual energy. This is because performing watchdog duties consumes additional resources from the vehicles; therefore, a vehicle should have enough resources before being selected as a watchdog. Residual energy will also promote fairness, ensuring the exact vehicle is not selected as a watchdog in too many continuous rounds and depletes its resources. The simulation was run for five rounds, and Figure 6.5 shows the results from the first round of communication.

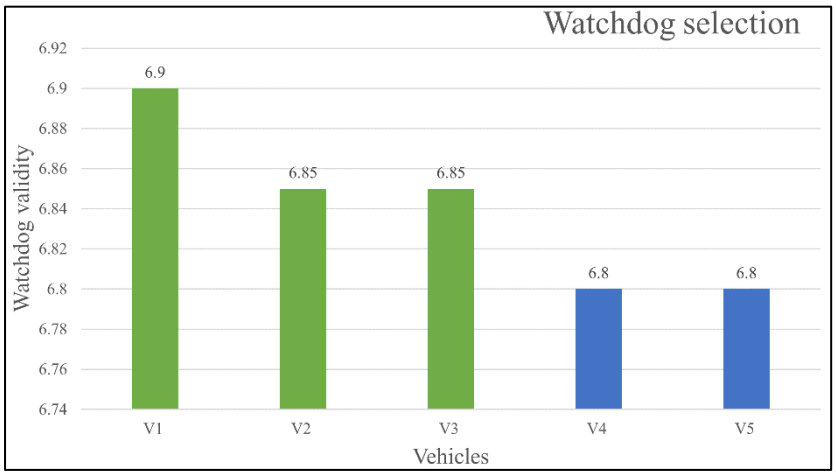

Figure 6.5 - Vehicle watchdogs first round of communication in the experiment varying the residual energy of vehicles.

Vehicle V1 was identified as the vehicle with the highest residual energy, therefore, was selected as a watchdog for the first round of communication. Vehicles V2 and V3 had the second-highest residual energy and were selected as watchdogs in the VANET for this communication round. V4 and V4 had lower residual energy and were not selected as vehicle watchdogs for this communication round. The results from the second round of communication are presented in Figure 6.6.

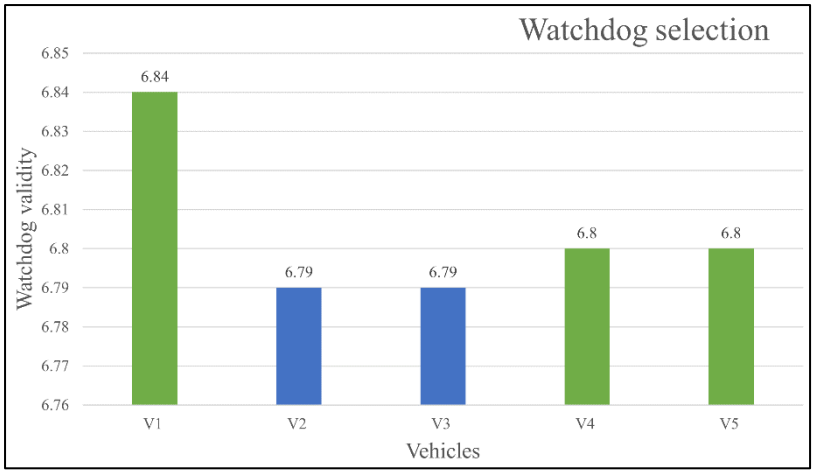

Figure 6.6 - Vehicle watchdogs second round of communication in the experiment varying the residual energy of vehicles.

In the second round of communication, V1 had the highest residual energy and therefore was selected as a watchdog for the communication round. Vehicles V4 and V5 had the second-highest residual energy and were selected as watchdogs for this communication round. Vehicles V2 and V3 had lower residual energy, therefore, were not selected as watchdogs for the communication round. The results from the third round of communication are shown in Figure 6.7.

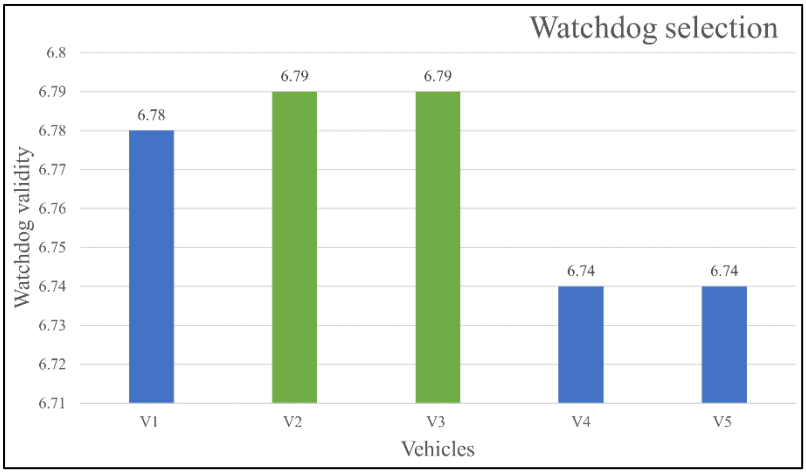

Figure 6.7 - Vehicle watchdogs third communication round in the experiment varying the residual energy of vehicles.

In the third communication round, V2 and V3 were identified as the vehicles with the highest residual energy. The vehicles were therefore selected as watchdogs for this communication round. V1, V4, and V5 were identified to have lower residual energy; they were, therefore, not selected as watchdogs for that communication round. The results from the fourth round of communication are shown in Figure 6.8.

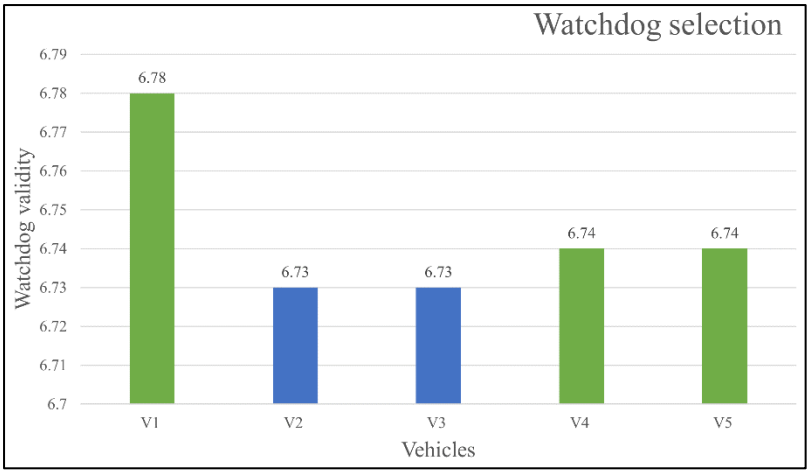

Figure 6.8 - Vehicle watchdogs fourth communication round in the experiment varying the residual energy of vehicles.

In the fourth communication round, V1 had the highest residual energy, therefore, was selected as a watchdog. V4 and V5 had the second-highest residual energy and were also selected as watchdogs. V2 and V3 were identified as having lower residual energy; they were, therefore, not selected as watchdogs for this communication round. The results from the fifth round of communication are shown in Figure 6.9.

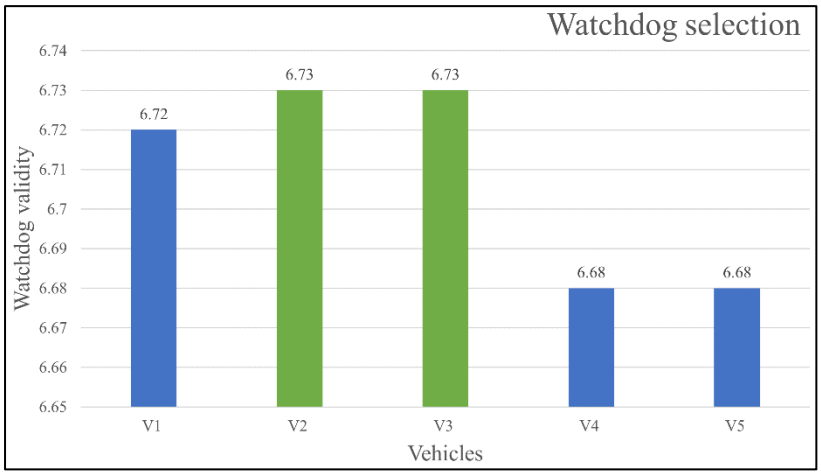

Figure 6.9 - Vehicle watchdogs fifth communication round in the experiment varying the residual energy of vehicles.

In the fifth communication round, vehicles V2 and V3 were found to have the highest residual energy. They were therefore selected as watchdogs in the VANET. V1, V4 and V5 were identified to have lower residual energy and therefore are not selected as watchdogs in the VANET. The proposed system accordingly made use of residual energy in order to promote fairness in the VANET.

The subsequent evaluation was an algorithm complexity analysis of the proposed system. The evaluation was done in two forms time complexity and space complexity. The complexity analysis will assist in identifying the resource consumption of the proposed system in relation to the input size. The algorithm complexity is further detailed in Table 6.2.

Table 6.2 - Algorithm complexities of the watchdog selection process.

Name	Time complexity	Space complexity
Algorithm 5: Watchdog selection.	$O(n^2)$	$O(n^3)$

This algorithm complexity can further be visualized in Figure 6.10 and Figure 6.11.

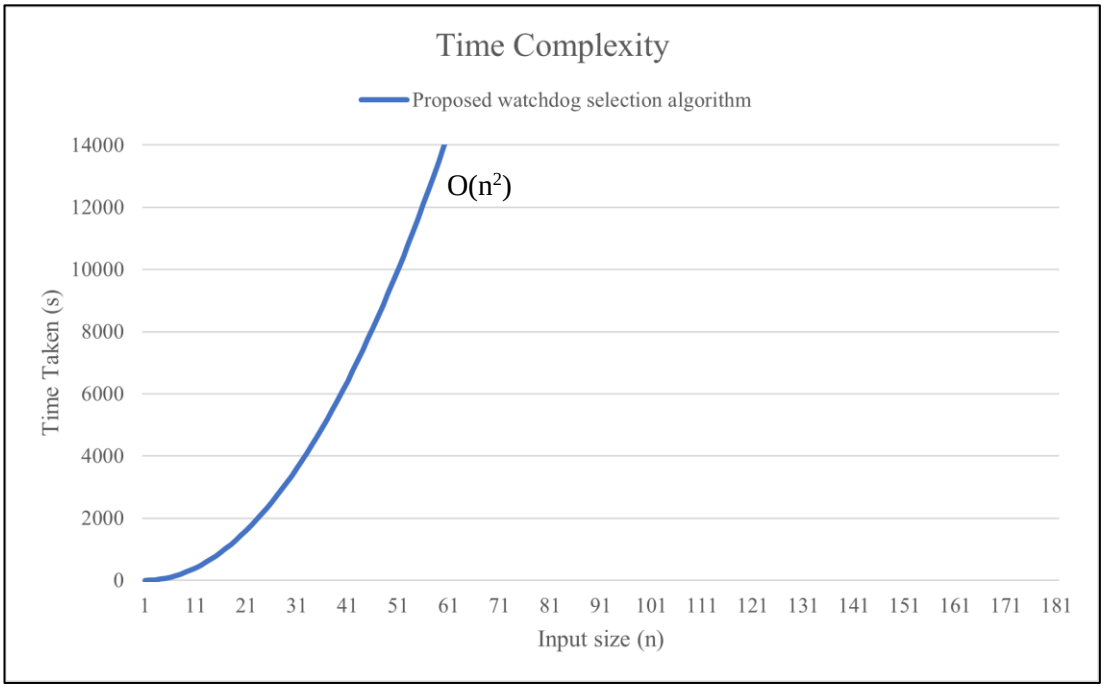

Figure 6.10 - Time complexity of the proposed watchdog selection algorithm.

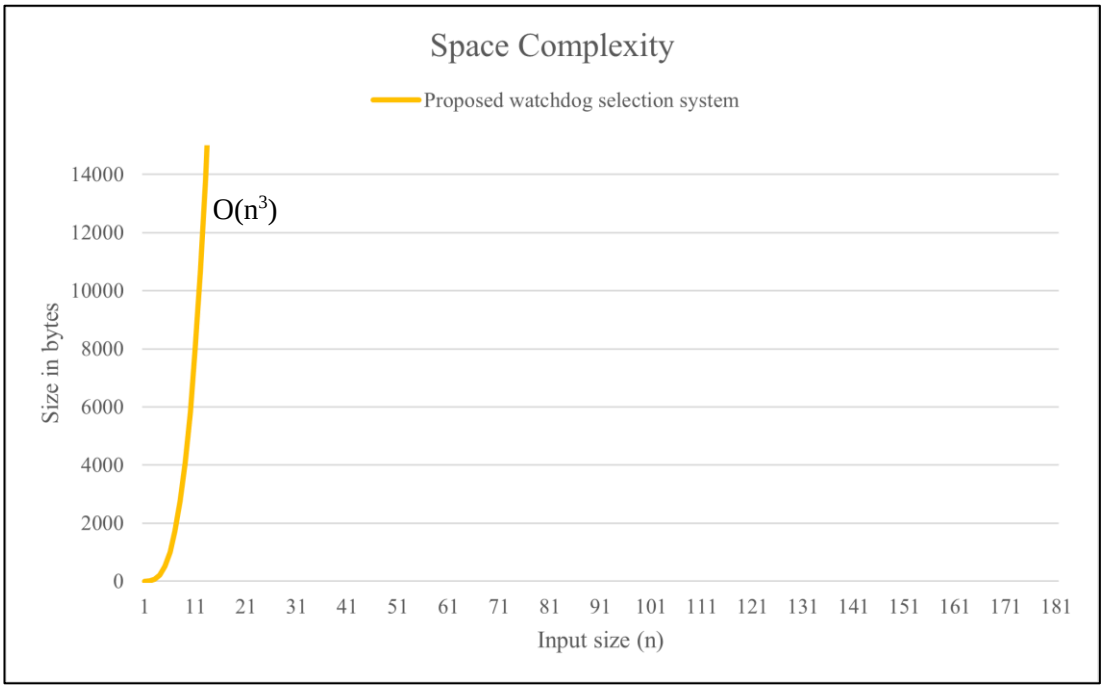

Figure 6.11 - Space complexity proposed watchdog selection algorithm.

The proposed algorithm has a time complexity of $O(n^2)$ and a space complexity of $O(n^3)$. While the memory required to run the algorithm will proportionally grow to the

cube size of the input. The space complexity means the algorithm runtime will increase proportionally to the square of the input size.

6.8. Summary

This section will feature a summary of the proposed system in this chapter. This chapter detailed the watchdog selection process of the proposed system. Watchdogs were used by the proposed system and many security systems to watch transactions in the VANET. The watchdog selection process should consider selecting secure and optimal watchdogs. The proposed system considered a vehicle's history, that is, previous messages successfully delivered, and the average time to reply to messages, to select the optimal and secure watchdogs. This selection method is known as direct watchdog selection. If vehicle history were unavailable, the proposed system would use RREQ and RREP messages to determine the secure and optimal watchdogs in the VANET. This selection method is known as indirect watchdog selection. The proposed system also included fairness in the watchdog selection process. Fairness was achieved by considering the residual energy of vehicles. The watchdog process consumes slightly more energy; therefore, a vehicle should not deplete its resources by performing watchdog duties. The proposed system also promoted fairness in the VANET by considering the residual energy. Performance evaluation of the proposed system was conducted, and results were presented. The proposed system successfully selects secure and optimal watchdogs in the VANET. The following section shall feature a summary of the research.

7. Conclusion

7.1. Overview

This section will feature the conclusion of the research conducted in this work. It discusses how the research outcomes and results address the study's aims and objectives. VANETs have been extensively researched. This includes VANET components, architectures, and technologies. Due to the nature of VANETs, malicious actors could perpetrate attacks and have adverse effects on VANETs. These attacks render the VANET incapable of performing its objective functions. The research explored security techniques to mitigate malicious attacks on VANETs. This exploration included identifying critical characteristics to consider when addressing these dangerous entities. A model was then developed to achieve the objectives based on the research.

VANETs sense environmental phenomena and share data between vehicles. The VANET faces threats from malicious vehicles. Malicious vehicles cause delays and drops in messages communicated between vehicles. This research aimed to develop a multi-tier trust management system to identify malicious vehicles in the VANET. The research explored different methods of identifying malicious vehicles in the VANET that provided robust security. The proposed system in this work considered federated resource management in the design. It included vehicle behavioural history and data integrity while calculating trust values. The overall calculation of trust value was done at RSU, which is more resourceful, and watchdogs were used for forwarding the data. The significance of this is the improvement in PDR and end-to-end delay in VANET populated with malicious vehicles. The proposed system is also self-sufficient, low maintenance and self-optimized.

The rest of this chapter describes the results obtained from specific experiments and how this relates to research aims and objectives. It will discuss any challenges experienced in the research process. The chapter will conclude by discussing the future recommendations of the research.

7.2. Research Summary

The research objectives were undertaken meticulously, and a summary of the research is presented below.

1. A thorough examination of the literature showed a gap in designing efficient trust management systems for VANET communications. Due to the unique applications of VANETs, attacks can be propagated against vehicles. If not dealt with, these attacks cause vehicles to drop or delay messages during communications. Delays or drops in the essential information communicated in VANETs can increase unsafe situations or road accidents. The attacks on VANETs justified the research investigating a new approach to providing security for VANET communications.

2. After an extensive literature review, it was discovered that VANET required special techniques to secure its communications. This was realised during the research and validated via experiments. The need for special security techniques

formed the fundamental basis on which a new approach to VANET security could be examined. Data was collected, and a set of features that make up VANET communication was identified. Using this data, several sophisticated VANET scenarios could be modelled. Attributes that could be used to model vehicle behaviour were explored at this stage. Using experiments, the optimal attributes to determine vehicle behaviour were discovered.

3. Models were developed to simulate VANET behaviour in several scenarios Based on the data generated and acquired. The models were used to simulate the network's performance under different scenarios. The resultant data was collected and used to evaluate the performance of the proposed system.

4. A multi-tier trust-based security management system for VANET communications was developed based on the models created. The multi-tier trust-based security management system used various algorithms and mathematical concepts. Attributes were modelled using equations to determine the behaviour of a vehicle. The equations resulted in a value determining whether a vehicle is malicious or non-malicious.

5. A working model of the multi-tier trust-based system was developed. The model was applied to a VANET using the scenarios developed. The experiments evaluated the system and the results presented.

7.3. Results

The results obtained in the study are presented below.

I. Following the background and literature review conducted in Chapter 2, it was confirmed that a security system for VANET is integral to operations. The security system should be able to offer complete protection while maintaining its efficiency. However, due to the nature of VANETs, security systems are challenging to implement in VANETs. Therefore, a gap exists in designing efficient security systems for VANET operations.

II. It was discovered that there is a direct correlation between vehicle behaviour and identifying malicious and non-malicious vehicles. Observing vehicle behaviour in the VANET makes identifying attributes that indicate malicious vehicles possible. This set of attributes was used to calculate a value to indicate vehicle behaviour.

III. It was observed that federated roles could be applied to the VANET to increase efficiency. Vehicles in the VANET monitored neighbouring vehicle transactions. These vehicles are known as watchdogs. Watchdogs monitor attributes used to identify malicious behaviour. The watchdogs forward gathered data to the RSU. The RSU calculates the trust value of vehicles in the VANET. The trust value represents vehicles' behaviour, i.e. if they exhibit malicious or non-malicious behaviour.

IV. It was noted that to provide a robust security model, it is necessary to protect the watchdogs in the VANET. In addition, the security system's integrity should also be protected.

7.4. Contributions

1) Multi-tier trust-based security system.

A new methodology was developed for the security management of vehicles within VANET communications. The proposed system identified malicious and non-malicious vehicles by assigning vehicles in the VANET with a trust value representing a vehicle's behaviour. The proposed system also provided a security system for the watchdog vehicles in the VANET by protecting against malicious watchdogs. Another advantage of the proposed system is that it protects the data integrity of the trust value calculation within the defined limit. Protecting the watchdog and data integrity can be applied to future or past-developed security schemes to enhance their security.

2) Detection of network errors and recovering malicious vehicles

An intelligent model was developed that identified network errors via false positive detection. Network errors can cause delays or drops of messages within communication between vehicles. This can lead to false positives, where vehicles are identified as malicious yet exhibit non-malicious behaviour. The intelligent model allowed for recuperating malicious vehicles to be identified. During VANET operations, malicious vehicles can recover back to non-malicious behaviour. These vehicles should be identified to represent the correct state of the VANET and vehicles at all times. Identifying false positives and recuperating malicious vehicles increased the accuracy of the proposed system. The intelligent model can also be applied to previously developed or future-developed security management models for VANETs.

3) Watchdog selection strategy

A framework for watchdog selection that considers the behaviour of vehicles and promotes fairness during the selection of watchdog in the VANET. Watchdogs have the responsibility of monitoring other vehicle communications in the VANET. By considering random watchdogs in the VANET, the validity of a security management system is reduced as a malicious vehicle can be selected as a watchdog. Monitoring other vehicles in the VANET consumes slightly more energy in the VANET. Vehicles must not deplete their resources in the watchdog process. The framework also assisted in promoting fairness in the watchdog selection process.

4) Experimental summary

The findings of this study led to an understanding and realisation of the possibility of designing multi-tier security management solutions for VANET communications. This contribution allows for further research to develop more intelligent VANET communications systems. The results from this study can be used for guidance and comparison of future-developed security management systems for VANETs.

5) Beyond academia

The conclusions developed in this research can be used as an influence or guidance in manufacturing vehicle OBUs. Strengthening VANET security has broad ramifications regarding improving VANET operations and ensuring the VANET is resistant to attacks. Applying security mechanisms for VANETs will improve packet delivery and end-to-end delay in the presence of malicious vehicles. It can lead to VANET security being more ubiquitous and resistant to attacks.

7.5. Limitations and recommendations

7.5.1. Limitations

This research proposed a multi-tier trust-based management system to enable the identification of malicious vehicles in the VANET. The results of the proposed system have shown that it can improve the PDR and end-to-end delay of a VANET in the presence of malicious vehicles. However, some limitations of the study have been identified. These are presented below.

1) RSU distribution

The proposed system uses a federated method of operations, where the RSU is responsible for performing various tasks. The proposed system assumes RSUs are densely populated and easily accessible within road networks. Sparsely distributed RSUs may introduce some constraints to the proposed system in areas where RSUs are unavailable.

2) Inclusion of more vehicles

The current study has evaluated the proposed system in a small-scale VANET comprised of a compact number of vehicles. Including more vehicles has been planned as the next phase of the research, extending the proposed system to a large-scale VANET. In order to enhance the performance of the proposed system for more applications, it would be necessary to apply the system to large-scale VANETs. Testing in a large-scale VANET would ensure the proposed system works in large-scale VANETs.

3) Agent installation

For the proposed system to function optimally to achieve its objective functions, vehicles and RSUs in the VANET must have the agent installed. In vehicles' current hardware and software specifications, OBUs, trust management agents, and watchdog agents are not preinstalled. The same case is present in RSUs software and hardware specifications.

7.5.2. Recommendations

The limitations above presented an opportunity for recommendations on the subject matter presented in this research.

1) The multi-tier trust-based system presented in this research was developed with a federated model; the RSUs are responsible for executing the algorithms presented. However, in some areas, RSUs are not densely populated. To make the proposed system more applicable and practical, it would be worthwhile to integrate the system into a cloud-based system. The algorithms and equations could be performed on a cloud system, and vehicles could query it for recommendations. The efficiency of vehicles and the VANET could benefit immensely by publishing and consuming data directly from a cloud system. A cloud-based system would also benefit the installation of the proposed system. The installation could be pushed to all vehicles and RSUs via cloud push service regardless of location.

2) The proposed system used a small-scale VANET of fewer than ten vehicles. Although this would work for a sparsely populated area, the proposed system could benefit from being expanded to a large-scale VANET. The proposed system could employ a clustering mechanism to tackle large-scale VANETs. Scalability to a large-scale network would improve the applicability of the proposed system to real-world environments.

3) The proposed system can redistribute certain weights during the execution of algorithms to match the functionality of the VANET. The redistribution of these weights currently relies on user input in the proposed system. The proposed system would benefit from a machine learning approach to select the best weight concerning the VANET application.

7.6. Summary

In this chapter, the results of the study have been presented and discussed. These results were aligned with the aims and objectives of the research. The conclusions made by the study were found to achieve the stated aims and objectives. The contributions were discussed regarding academia and the relationship to the broader community of VANET systems. This chapter evaluates the limitations encountered during the study and those expected with the proposed system. The future research and development opportunities concerning the proposed system are discussed.

In conclusion, this chapter has summarised that the objectives and aims stated by the research have been met. At the same time, it provided enhancement and improvement recommendations for the proposed system.

References

[1] B. Akwirry, N. Bessis, H. Malik, and S. McHale, "A Multi-Tier Trust-Based Security Mechanism for Vehicular Ad-Hoc Network Communications," *Sensors*, vol. 22, no. 21, p. 8285, Oct. 2022.

[2] M. A. Al-Shareeda, M. Anbar, S. Manickam, and A. A. Yassin, "VPPCS: VANET-Based Privacy-Preserving Communication Scheme," *IEEE Access*, vol. 8, pp. 150914–150928, 2020.

[3] D. Zhang, T. Zhang, and X. Liu, "Novel self-adaptive routing service algorithm for application in VANET," *Applied Intelligence*, vol. 49, no. 5, pp. 1866–1879, 2019.

[4] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "VANet security challenges and solutions: A survey," *Vehicular Communications*, vol. 7, pp. 7–20, 2017.

[5] M. S. Sheikh and J. Liang, "A comprehensive survey on VANET security services in traffic management system," *Wireless Communications and Mobile Computing*, vol. 2019, 2019.

[6] S. Sumithra and R. Vadivel, "An Overview of Various Trust Models for VANET Security Establishment," *2018 9th International Conference on Computing, Communication and Networking Technologies, ICCCNT 2018*, 2018.

[7] O. S. Al-Heety, Z. Zakaria, M. Ismail, M. M. Shakir, S. Alani, and H. Alsariera, "A Comprehensive Survey: Benefits, Services, Recent Works, Challenges, Security, and Use Cases for SDN-VANET," *IEEE Access*, vol. 8, pp. 91028–91047, 2020.

[8] F. Ahmad, J. Hall, A. Adnane, and V. N. L. Franqueira, "Faith in Vehicles: A Set of Evaluation Criteria for Trust Management in Vehicular Ad-Hoc Network," *Proceedings - 2017 IEEE International Conference on Internet of Things, IEEE Green Computing and Communications, IEEE Cyber, Physical and Social Computing, IEEE Smart Data, iThings-GreenCom-CPSCom-SmartData 2017*, vol. 2018-Janua, pp. 44–52, 2018.

[9] X. Feng, C. yan Li, D. xin Chen, and J. Tang, "A method for defensing against multi-source Sybil attacks in VANET," *Peer-to-Peer Networking and Applications*, vol. 10, no. 2, pp. 305–314, 2017.

[10] A. N. Upadhyaya and J. Shah, "Attacks on VANET Security," *International Journal of Computer Engineering & Technology (IJCET*, vol. 9, no. 1, pp. 8–19, 2018.

[11] Deeksha, A. Kumar, and M. Bansal, "A review on VANET security attacks and their countermeasure," *4th IEEE International Conference on Signal Processing, Computing and Control, ISPCC 2017*, vol. 2017-Janua, pp. 580–585, 2017.

[12] M. A. Al-Shareeda, M. Anbar, I. H. Hasbullah, S. Manickam, N. Abdullah, and M. M. Hamdi, "Review of prevention schemes for replay attack in vehicular ad hoc networks (VANETs)," *2020 3rd IEEE International Conference on Information Communication and Signal Processing, ICICSP 2020*, pp. 394–398, 2020.

[13] M. A. Hezam Al Junaid, A. A. Syed, M. N. Mohd Warip, K. N. Fazira Ku Azir, and N. H. Romli, "Classification of Security Attacks in VANET: A Review of Requirements and Perspectives," *MATEC Web of Conferences*, vol. 150, pp. 1–7, 2018.

[14] A. Balaram and S. Pushpa, “Sybil attack resistant location privacy in VANET,” *International Journal of Information and Communication Technology*, vol. 13, no. 4, pp. 389–406, 2018.
[15] M. A. Shahid, A. Jaekel, C. Ezeife, Q. Al-Ajmi, and I. Saini, “Review of potential security attacks in VANET,” in *Proceedings of Majan International Conference: Promoting Entrepreneurship and Technological Skills: National Needs, Global Trends, MIC 2018*, 2018, pp. 1–4.
[16] M. S. Sheikh, L. Jun, and W. Wang, “A Survey of Security Services , Attacks ,” *sensors Review*, vol. 19, 2019.
[17] T. Zaidi and S. Faisal, “An overview: Various attacks in VANET,” *2018 4th International Conference on Computing Communication and Automation, ICCCA 2018*, pp. 1–6, 2018.
[18] F. Sakiz and S. Sen, “A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV,” *Ad Hoc Networks*, vol. 61, pp. 33–50, 2017.
[19] M. Arif, G. Wang, M. Zakirul Alam Bhuiyan, T. Wang, and J. Chen, “A survey on security attacks in VANETs: Communication, applications and challenges,” *Vehicular Communications*, vol. 19, p. 100179, 2019.
[20] B. Alaya and L. SELLAMI, “Clustering method and symmetric/asymmetric cryptography scheme adapted to securing urban VANET networks,” *Journal of Information Security and Applications*, vol. 58, p. 102779, 2021.
[21] M. Gillani, A. Ullah, and H. A. Niaz, “Trust Management Schemes for Secure Routing in VANETs - A Survey,” *12th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics, MACS 2018 - Proceedings*, pp. 1–6, 2019.
[22] S. V. Mahagaonkar and N. Dongre, “TEAC: Timed efficient asymmetric cryptography for enhancing security in VANET,” *2017 International Conference on Nascent Technologies in Engineering, ICNTE 2017 - Proceedings*, 2017.
[23] S. Ali, “Wormhole Attack by using Cryptographic Technique,” pp. 520–523, 2017.
[24] R. Hussain, J. Lee, S. Zeadally, J. Lee, and S. Zeadally, “Trust in VANET : A Survey of Current Solutions and Future Research Opportunities,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 5, pp. 2553–2571, 2021.
[25] X. Cheng, Y. Luo, and Q. Gui, “Research on Trust Management Model of Wireless Sensor Networks,” *Proceedings of 2018 IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference, IAEAC 2018*, no. Iaeac, pp. 1397–1400, 2018.
[26] X. Yao, X. Zhang, H. Ning, and P. Li, “Using trust model to ensure reliable data acquisition in VANETs,” *Ad Hoc Networks*, vol. 55, pp. 107–118, 2017.
[27] A. Mahmood, B. Butler, W. E. Zhang, Q. Z. Sheng, and S. A. Siddiqui, “A Hybrid Trust Management Heuristic for VANETs,” *2019 IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom Workshops 2019*, pp. 748–752, 2019.
[28] K. A. Awan, I. Ud Din, A. Almogren, M. Guizani, and S. Khan, “StabTrust-A Stable and Centralized Trust-Based Clustering Mechanism for IoT Enabled Vehicular Ad-Hoc Networks,” *IEEE Access*, vol. 8, pp. 21159–21177, 2020.
[29] Z. Lu, Q. Wang, G. Qu, and Z. Liu, “BARS: A Blockchain-Based Anonymous Reputation System for Trust Management in VANETs,” *Proceedings - 17th*

IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2018, pp. 98–103, 2018.
[30] M. Mohamed Musthafa, K. Vanitha, A. M. J. M. D. Zubair Rahman, and K. Anitha, "An efficient approach to identify selfish node in MANET," *2020 International Conference on Computer Communication and Informatics, ICCCI 2020*, pp. 2020–2022, 2020.
[31] R. Soundararajan, N. Palanisamy, R. Patan, and M. S. Khan, "Secure and concealed watchdog selection scheme using masked distributed selection approach in wireless sensor networks," 2020.
[32] C. Gayathri, "Using Dynamic Watchdog Optimization Technique for Secure Data Transfer in MANET," vol. 13, no. 23, pp. 16312–16317, 2018.
[33] J. Govindasamy and S. Punniakodi, "Optimised watchdog system for detection of DDOS and wormhole attacks in IEEE802.15.4-based wireless sensor networks," *International Journal of Mobile Network Design and Innovation*, vol. 8, no. 1, pp. 36–44, 2018.
[34] H. Bangui, M. Ge, and B. Buhnova, "A hybrid machine learning model for intrusion detection in VANET," *Computing*, vol. 104, no. 3, pp. 503–531, 2022.
[35] S. Kudva, S. Badsha, S. Sengupta, H. La, I. Khalil, and M. Atiquzzaman, "A scalable blockchain based trust management in VANET routing protocol," *Journal of Parallel and Distributed Computing*, vol. 152, pp. 144–156, 2021.
[36] A. Kchaou, R. Abassi, and S. Guemara, "Toward a distributed trust management scheme for VANET," *ACM International Conference Proceeding Series*, 2018.
[37] C. Gupta, L. Singh, and R. Tiwari, "Malicious Node Detection in Vehicular Ad-hoc Network (VANET) using Enhanced Beacon Trust Management with Clustering Protocol (EBTM-CP)," *Wireless Personal Communications*, no. 0123456789, 2023.
[38] S. Tangade, "Trust Management Scheme in VANET : Neighbour Communication Based Approach," pp. 741–744, 2017.
[39] W. Ahmed, W. Di, and D. Mukathe, "A Blockchain-Enabled Incentive Trust Management with Threshold Ring Signature Scheme for Traffic Event Validation in VANETs," *Sensors*, vol. 22, no. 17, 2022.
[40] J. Zhang, "AATMS : An Anti-Attack Trust Management Scheme in VANET," vol. 8, pp. 21077–21090, 2020.
[41] A. Hbaieb, S. Ayed, and L. Chaari, "A survey of trust management in the Internet of Vehicles," *Computer Networks*, vol. 203, no. October 2021, p. 108558, 2022.
[42] B. Koirala, S. S. Tangade, and S. S. Manvi, "Trust Management Based on Node Stay Time in VANET," *2018 International Conference on Advances in Computing, Communications and Informatics, ICACCI 2018*, pp. 242–248, 2018.
[43] W. Ahmed, W. Di, and D. Mukathe, "Privacy-preserving blockchain-based authentication and trust management in VANETs," *IET Networks*, vol. 11, no. 3–4, pp. 89–111, 2022.
[44] S. Zeadally, J. Guerrero, and J. Contreras, "A tutorial survey on vehicle-to-vehicle communications," *Telecommunication Systems*, vol. 73, no. 3, pp. 469–489, 2020.
[45] A. K. Ahmed, M. N. Abdulwahed, and B. Farzaneh, "A distributed trust mechanism for malicious behaviors in VANETs," *Indonesian Journal of*

Electrical Engineering and Computer Science, vol. 19, no. 3, pp. 1147–1155, 2020.

[46] I. A. Abbasi and A. S. Khan, "A review of vehicle to vehicle communication protocols for VANETs in the urban environment," *Future Internet*, vol. 10, no. 2, 2018.

[47] M. Arshad, Z. Ullah, N. Ahmad, M. Khalid, and H. Criuckshank, "Open Access A survey of local / cooperative-based malicious information detection techniques in VANETs," pp. 1–17, 2018.

[48] F. Azam, S. Kumar, K. P. Yadav, N. Priyadarshi, and S. Padmanaban, "An Outline of the Security Challenges in VANET," in *2020 IEEE 7th Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON)*, 2020, pp. 1–6.

[49] R. Shrestha, R. Bajracharya, A. P. Shrestha, and S. Y. Nam, "A new type of blockchain for secure message exchange in VANET," *Digital Communications and Networks*, vol. 6, no. 2, pp. 177–186, 2020.

[50] S. Soni, "Trusted Location Selection in Vehicular ad-hoc Network," *American Journal Of Advanced Computing*, vol. 2, no. 1, 2015.

[51] R. Hussain, J. Lee, and S. Zeadally, "Trust in vanet: A survey of current solutions and future research opportunities," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 5, pp. 2553–2571, 2021.

[52] I. Ali and F. Li, "An efficient conditional privacy-preserving authentication scheme for Vehicle-To-Infrastructure communication in VANETs," *Vehicular Communications*, vol. 22, p. 100228, 2020.

[53] E. Ndashimye, S. K. Ray, N. I. Sarkar, and J. A. Gutiérrez, "Vehicle-to-infrastructure communication over multi-tier heterogeneous networks : A survey," *Computer Networks*, vol. 112, pp. 144–166, 2017.

[54] Y. Wang, K. Venugopal, A. F. Molisch, and R. W. Heath, "MmWave Vehicle-to-Infrastructure Communication: Analysis of Urban Microcellular Networks," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 8, pp. 7086–7100, 2018.

[55] J. W. Kim, J. W. Kim, and D. K. Jeon, "A cooperative communication protocol for QoS provisioning in IEEE 802.11p/wave vehicular networks," *Sensors (Switzerland)*, vol. 18, no. 11, pp. 1–19, 2018.

[56] P. Sewalkar and J. Seitz, "Vehicle-to-pedestrian communication for vulnerable road users: Survey, design considerations, and challenges," *Sensors (Switzerland)*, vol. 19, no. 2, 2019.

[57] I. Othersen, A. S. Conti-Kufner, A. Dietrich, P. Maruhn, and K. Bengler, "Designing for Automated Vehicle and Pedestrian Communication: Perspectives on eHMIs from Older and Younger Persons," *Proceedings of the Human Factors and Ergonomics Society Europe Chapter 2018 Annual Conference*, vol. 4959, pp. 135–148, 2018.

[58] P. Sewalkar, S. Krug, and J. Seitz, "Communication for Crash Prevention Systems," pp. 404–409, 2017.

[59] W. Tong, A. Hussain, W. X. Bo, and S. Maharjan, "Artificial Intelligence for Vehicle-To-Everything: A Survey," *IEEE Access*, vol. 7, pp. 10823–10843, 2019.

[60] J. Wang, Y. Shao, Y. Ge, and R. Yu, "A survey of vehicle to everything (V2X) testing," *Sensors (Switzerland)*, vol. 19, no. 2, pp. 1–20, 2019.

[61] M. Gillani, A. Ullah, and H. A. Niaz, "Trust Management Schemes for Secure Routing in VANETs - A Survey," *12th International Conference on*

Mathematics, Actuarial Science, Computer Science and Statistics, MACS 2018 - Proceedings, pp. 7–12, 2019.

[62] D. Zheng, C. Jing, R. Guo, S. Gao, and L. Wang, "A Traceable Blockchain-Based Access Authentication System with Privacy Preservation in VANETs," *IEEE Access*, vol. 7, pp. 117716–117726, 2019.

[63] Z. Lu, G. Qu, and Z. Liu, "A Survey on Recent Advances in Vehicular Network Security, Trust, and Privacy," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 2, pp. 760–776, 2019.

[64] S. P., P. N., and S. J., "Rising Issues in VANET Communication and Security: A State of Art Survey," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 9, pp. 245–252, 2017.

[65] S. Ahmed, M. U. Rehman, A. Ishtiaq, S. Khan, A. Ali, and S. Begum, "VANSec: Attack-Resistant VANET Security Algorithm in Terms of Trust Computation Error and Normalized Routing Overhead," *Journal of Sensors*, vol. 2018, 2018.

[66] R. Shrestha and S. Y. Nam, "Trustworthy Event-Information Dissemination in Vehicular Ad Hoc Networks," vol. 2017, 2017.

[67] M. A. Al-shareeda, M. Anbar, S. Manickam, and I. H. Hasbullah, "Review of Prevention Schemes for Man-In-The-Middle (MITM) Attack in Vehicular Ad hoc Networks," *International Journal of Engineering and Management Research*, vol. 10, no. 3, pp. 153–158, 2020.

[68] Z. Lu, W. Liu, Q. Wang, G. Qu, and Z. Liu, "A privacy-preserving trust model based on blockchain for VANETs," *IEEE Access*, vol. 6, pp. 45655–45664, 2018.

[69] Y. Wang, Z. Ding, F. Li, X. Xia, and Z. Li, "Design and implementation of a VANET application complying with WAVE protocol," *Proceedings of the 2017 International Conference on Wireless Communications, Signal Processing and Networking, WiSPNET 2017*, vol. 2018-Janua, pp. 2333–2338, 2018.

[70] I. Miri, A. Fotouhi, and N. Ewin, "Electric vehicle energy consumption modelling and estimation—A case study," *International Journal of Energy Research*, vol. 45, no. 1, pp. 501–520, 2021.

[71] E. E. Michaelides, "Thermodynamics and energy usage of electric vehicles," *Energy Conversion and Management*, vol. 203, no. November 2019, p. 112246, 2020.

[72] J. A. Sanguesa, V. Torres-Sanz, P. Garrido, F. J. Martinez, and J. M. Marquez-Barja, "A review on electric vehicles: Technologies and challenges," *Smart Cities*, vol. 4, no. 1, pp. 372–404, 2021.

[73] R. Kaur, M. Scholar, T. Pal, M. Singh, V. Khajuria, and M. Scholar, "Network (VANET)," no. Icoei, pp. 884–889, 2018.

[74] A. Aarthy Devi, A. K. Mohan, and M. Sethumadhavan, "Wireless Security Auditing: Attack Vectors and Mitigation Strategies," *Procedia Computer Science*, vol. 115, pp. 674–682, 2017.

[75] A. K. Goyal, A. K. Tripathi, and G. Agarwal, "Security Attacks, Requirements and Authentication Schemes in VANET," *IEEE International Conference on Issues and Challenges in Intelligent Computing Techniques, ICICT 2019*, 2019.

[76] P. Tyagi and D. Dembla, "Performance analysis and implementation of proposed mechanism for detection and prevention of security attacks in routing protocols of vehicular ad-hoc network (VANET)," *Egyptian Informatics Journal*, vol. 18, no. 2, pp. 133–139, 2017.

[77] A. Quyoom, A. A. Mir, and D. A. Sarwar, “Security Attacks and Challenges of VANETs : A Literature Survey,” *Journal of Multimedia Information System*, vol. 7, no. 1, pp. 45–54, 2020.
[78] S. Sharma and A. Kaul, “A survey on Intrusion Detection Systems and Honeypot based proactive security mechanisms in VANETs and VANET Cloud,” *Vehicular Communications*, vol. 12, pp. 138–164, 2018.
[79] M. R. Ghori, K. Z. Zamli, N. Quosthoni, M. Hisyam, and M. Montaser, “Vehicular Ad-hoc Network (VANET): Review,” 2018.
[80] R. Hussain, F. Hussain, and S. Zeadally, “Integration of VANET and 5G Security: A review of design and implementation issues,” *Future Generation Computer Systems*, vol. 101, pp. 843–864, 2019.
[81] R. Al-Mutiri, M. Al-Rodhaan, and Y. Tian, “Improving vehicular authentication in VANET using cryptography,” *International Journal of Communication Networks and Information Security*, vol. 10, no. 1, pp. 248–255, 2018.
[82] S. S. Manvi and S. Tangade, “A survey on authentication schemes in VANETs for secured communication,” *Vehicular Communications*, vol. 9, pp. 19–30, 2017.
[83] 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. 9293–9307, 2016.
[84] P. Cirne, A. Zúquete, and S. Sargento, “TROPHY: Trustworthy VANET routing with group authentication keys,” *Ad Hoc Networks*, vol. 71, pp. 45–67, 2018.
[85] S. Tangade and S. S. Manvi, “Trust management scheme in VANET: Neighbour communication based approach,” *Proceedings of the 2017 International Conference On Smart Technology for Smart Nation, SmartTechCon 2017*, pp. 741–744, 2018.
[86] D. Zhang, F. R. Yu, and R. Yang, “A Machine Learning Approach for Software-Defined Vehicular Ad Hoc Networks with Trust Management,” *2018 IEEE Global Communications Conference, GLOBECOM 2018 - Proceedings*, 2018.
[87] F. Gai, J. Zhang, P. Zhu, and X. Jiang, “Ratee-based trust management system for internet of vehicles,” *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 10251 LNCS, pp. 344–355, 2017.
[88] X. Yan, X. Gu, J. Wang, J. Wan, and L. Chen, “A Kind of Event Trust Model for VANET Based on Statistical Method,” *Wireless Personal Communications*, vol. 118, no. 1, pp. 489–503, 2021.
[89] R. Shrestha and S. Y. Nam, “Trustworthy event-information dissemination in vehicular Ad Hoc networks,” *Mobile Information Systems*, vol. 2017, 2017.
[90] A. Kchaou, R. Abassi, and S. Guemara, “Towards the performance evaluation of a clustering and trust based security mechanism for VANET,” *ACM International Conference Proceeding Series*, 2020.
[91] S. Oubabas, R. Aoudjit, J. J. P. C. Rodrigues, and S. Talbi, “Secure and stable Vehicular Ad Hoc Network clustering algorithm based on hybrid mobility similarities and trust management scheme,” *Vehicular Communications*, vol. 13, pp. 128–138, 2018.
[92] A. Mahmood *et al.*, “Trust Management Based on Node Stay Time in VANET,” *2018 International Conference on Advances in Computing, Communications*

and Informatics, ICACCI 2018, pp. 242–248, 2018.
[93] M. Hasan, S. Member, H. T. Mouftah, and L. Fellow, "Optimization of Watchdog Selection in Wireless Sensor Networks," vol. 6, no. 1, pp. 94–97, 2017.
[94] F. Zawaideh and M. Salamah, "An efficient weighted trust-based malicious node detection scheme for wireless sensor networks," *International Journal of Communication Systems*, vol. 32, no. 3, pp. 1–13, 2019.
[95] C. Science and M. Studies, "Identification Technique for All Passive Selfish Node Attacks In a Mobile Network," vol. 7782, no. April, pp. 46–51, 2015.
[96] M. Selvi, K. Thangaramya, S. Ganapathy, K. Kulothungan, H. Khannah Nehemiah, and A. Kannan, "An Energy Aware Trust Based Secure Routing Algorithm for Effective Communication in Wireless Sensor Networks," *Wireless Personal Communications*, vol. 105, no. 4, pp. 1475–1490, 2019.
[97] T. Gaber, S. Abdelwahab, M. Elhoseny, and A. E. Hassanien, "Trust-based secure clustering in WSN-based intelligent transportation systems," *Computer Networks*, vol. 146, pp. 151–158, 2018.
[98] S. Otoum, B. Kantarci, and H. T. Mouftah, "Hierarchical trust-based black-hole detection in WSN-based smart grid monitoring," *IEEE International Conference on Communications*, no. May, 2017.
[99] M. Singh, A. R. Sardar, K. Majumder, and S. K. Sarkar, "A Lightweight Trust Mechanism and Overhead Analysisfile:///C:/Users/User/Desktop/Backup/PhD/2018-2020/Vanets based on fog.pdf file:///C:/Users/User/Desktop/Backup/PhD/2018-2020/Arshad2018_Article_ASurveyOfLocalCooperative-base.pdf file:///C:/Users/User/De," *IETE Journal of Research*, vol. 63, no. 3, pp. 297–308, 2017.
[100] C. Lal, V. Laxmi, and M. S. Gaur, "A node-disjoint multipath routing method based on AODV protocol for MANETs," *Proceedings - International Conference on Advanced Information Networking and Applications, AINA*, pp. 399–405, 2012.
[101] V. Arora and C. R. Krishna, "Performance evaluation of routing protocols for MANETs under different traffic conditions," *ICCET 2010 - 2010 International Conference on Computer Engineering and Technology, Proceedings*, vol. 6, pp. 79–84, 2010.
[102] J. Shen, H. Tan, J. Wang, J. Wang, and S. Lee, "A novel routing protocol providing good transmission reliability in underwater sensor networks," *Journal of Internet Technology*, vol. 16, no. 1, pp. 171–178, 2015.
[103] Y. A. Huang and W. Lee, "A cooperative intrusion detection system for ad hoc networks," *Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Security of Ad Hoc and Sensor Networks (in Association with 10th ACM Conference on Computer and Communications Security)*, pp. 135–147, 2003.
[104] P. Rodrigues and J. John, "Joint trust: an approach for trust-aware routing in WSN," *Wireless Networks*, vol. 26, no. 5, pp. 3553–3568, 2020.
[105] W. Zhang, S. Zhu, J. Tang, and N. Xiong, "A novel trust management scheme based on Dempster–Shafer evidence theory for malicious nodes detection in wireless sensor networks," *Journal of Supercomputing*, vol. 74, no. 4, pp. 1779–1801, 2018.
[106] X. Yan, X. Gu, J. Wang, J. Wan, and L. Chen, "A Kind of Event Trust Model for VANET Based on Statistical," pp. 489–503, 2021.
[107] C. Gong, C. Xu, Z. Zhou, T. Zhang, and S. Yang, "A reputation management

scheme for identifying malicious nodes in VANET," *IEEE International Conference on High Performance Switching and Routing, HPSR*, vol. 2019-May, 2019.
[108] Y. Begriche, R. Khatoun, A. Rachini, and L. Khoukhi, "A Reputation System Using a Bayesian Statistical Filter in Vehicular Networks," *2020 6th International Conference on Mobile and Secure Services, MOBISECSERV 2020*, no. July, pp. 2–9, 2020.
[109] S. Rajasoundaran, A. V. Prabu, G. S. Kumar, P. P. Malla, and S. Routray, "Secure Opportunistic Watchdog Production in Wireless Sensor Networks: A Review," *Wireless Personal Communications*, vol. 120, no. 2, pp. 1895–1919, 2021.
[110] R. Soundararajan, N. Palanisamy, R. Patan, G. Nagasubramanian, and M. S. Khan, "Secure and concealed watchdog selection scheme using masked distributed selection approach in wireless sensor networks," *IET Communications*, vol. 14, no. 6, pp. 948–955, 2020.
[111] H. Bangui, M. Ge, and B. Buhnova, "A hybrid machine learning model for intrusion detection in VANET," *Computing*, vol. 104, no. 3, pp. 503–531, 2022.
[112] C. Nimje and P. Junghare, "A review on node activity detection, selfish & malicious behavioral patterns using watchdog algorithm," *Proceedings of the International Conference on Inventive Systems and Control, ICISC 2017*, pp. 1–5, 2017.
[113] A. Christopher Paul, D. Bhanu, R. Dhanapal, and D. Jebakumar Immanuel, "An Efficient Authentication Using Monitoring Scheme for Node Misbehaviour Detection in MANET," in *International Conference on Computing, Communication, Electrical and Biomedical Systems. EAI/Springer Innovations in Communication and Computing.*, Springer, Cham, 2022, pp. 627–633.
[114] A. Katiyar, D. Singh, and R. S. Yadav, "State-of-the-art approach to clustering protocols in VANET: a survey," *Wireless Networks*, vol. 26, no. 7, pp. 5307–5336, 2020.
[115] M. Houmer and M. L. Hasnaoui, *A Hybrid Intrusion Detection System Against Egoistic and Malicious Nodes in VANET*. Springer International Publishing, 2020.
[116] I. Souissi, N. Ben Azzouna, and T. Berradia, "Towards a self-adaptive trust management model for VANETs," *ICETE 2017 - Proceedings of the 14th International Joint Conference on e-Business and Telecommunications*, vol. 4, no. Icete, pp. 513–518, 2017.
[117] F. G. Ghajar, J. S. Sratakhti, and A. Sikora, "SBTMS: Scalable blockchain trust management system for VANET," *Applied Sciences (Switzerland)*, vol. 11, no. 24, 2021.
[118] K. Sireesha and S. Malladi, "A Survey of VANET Security Models and its Issues on Node Level Data Transmission," *Proceedings of the 2nd International Conference on Artificial Intelligence and Smart Energy, ICAIS 2022*, pp. 1409–1417, 2022.
[119] A. Varga, *A practical introduction to the OMNeT++ simulation framework*. 2019.
[120] C. Obermaier and C. Facchi, "Observations on OMNeT++ Real-Time Behaviour," no. Ivc, 2017.
[121] M. U. Rehman, S. Ahmed, S. U. Khan, S. Begum, and A. Ishtiaq, "ARV2V: Attack resistant vehicle to vehicle algorithm, performance in term of end-to-end delay and trust computation error in VANETs," *2018 International*

Conference on Computing, Mathematics and Engineering Technologies: Invent, Innovate and Integrate for Socioeconomic Development, iCoMET 2018 - Proceedings, vol. 2018-Janua, no. July, pp. 1–6, 2018.
[122] W. She, Q. Liu, Z. Tian, J. Sen Chen, B. Wang, and W. Liu, "Blockchain trust model for malicious node detection in wireless sensor networks," *IEEE Access*, vol. 7, pp. 38947–38956, 2019.
[123] M. Selvi, K. Thangaramya, S. Ganapathy, K. Kulothungan, H. Khannah Nehemiah, and A. Kannan, "An Energy Aware Trust Based Secure Routing Algorithm for Effective Communication in Wireless Sensor Networks," *Wireless Personal Communications*, vol. 105, no. 4, pp. 1475–1490, 2019.
[124] A. Ahmed, K. A. Bakar, M. I. Channa, and A. W. Khan, "A Secure Routing Protocol with Trust and Energy Awareness for Wireless Sensor Network," *Mobile Networks and Applications*, vol. 21, no. 2, pp. 272–285, 2016.
[125] G. D. Putra and S. Sulistyo, "Trust based approach in adjacent vehicles to mitigate Sybil attacks in VANET," *ACM International Conference Proceeding Series*, pp. 117–122, 2017.
[126] C. Abdelaziz, A. Lakas, N. Lagraa, and E. Barka, "UAV-assisted technique for the detection of malicious and selfish nodes in VANETs," *Vehicular Communications*, vol. 11, pp. 1–11, 2018.
[127] E. Nii, T. Kitanouma, N. Adachi, and Y. Takizawa, "Cooperative detection for falsification and isolation of malicious nodes for wireless sensor networks in open environment," in *Asia-Pacific Microwave Conference Proceedings, APMC*, 2017, pp. 521–524.
[128] P. Qi, F. Wang, and S. Hong, "A Novel Trust Model Based on Node Recovery Technique for WSN," *Security and Communication Networks*, vol. 2019, 2019.
[129] P. K. Srivastava, R. P. Ojha, K. Sharma, S. Awasthi, and G. Sanyal, "Effect of Quarantine and Recovery on Infectious Nodes in Wireless Sensor Network," *International Journal of Sensors, Wireless Communications and Control*, vol. 8, no. 1, pp. 26–36, 2018.

Appendices

Appendix A – List of symbols used in Chapter 4

Symbols made use of in designing the multi-tier trust management system. (Referred to from section 4.3.

Symbol	Definition	Description
N	Vehicle network	This will represent the vehicle network considered for applying the trust management system.
TV	Trust value	This represents the value associated with the behaviour of a vehicle. It is used to represent vehicle honesty or malicious nature.
PDR	Packet Delivery Ratio	This is the ratio of successfully delivered messages/packets by a vehicle to the number of messages/packets received to be forwarded by the vehicle. It is one of the attributes used to calculate the trust value of a vehicle.
PD	Processing Delay	This is the time a vehicle takes to process a message and forward it to the destination. It is another of the attributes that are used to calculate the trust value of a vehicle.
T_y	Trust message	These messages are forwarded from the vehicle source to the destination via the vehicles in the VANET. It is used to identify the trust metrics used to calculate the trust value of vehicles.
R_s	RSU	This is an infrastructure member of the VANET. This is to calculate the trust values of the vehicles in the VANET. It receives data from the vehicle watchdogs and calculates the trust value.
A, L, W	Area, Length, Width	The length and width represent the area where the VANET is applied to. The length and width represent the edges of the area, and the area represents the total area. Such that A = L * W where L and W are given in meters.
V_n	Vehicles	These are the vehicles that belong in the VANET and occupy the area.
V'_n	Watchdogs	These are the watchdogs selected by the RSU. They will watch other vehicle communications in the VANET.
γ_j	Message receive time	This is the timestamp a vehicle receives a message from the source. It is used to calculate the processing delay of a vehicle.

λ_i	Message send time	This is the timestamp when a vehicle forwards a packet to its intended destination. It is used to calculate the processing delay of a vehicle.
A_x	Acknowledgements	These are acknowledgements sent by vehicles to the source of the message. They indicate successfully receiving and forwarding messages to the intended destination.

Appendix B – List of symbols in Chapter 5

Symbols used in the identification of false positives and recuperating malicious vehicles. (Referred to from section 5.3)

Symbol	Definition	Description
N	Vehicle network	This will represent the vehicle network considered for applying the trust management system.
TV	Trust value	This represents the value associated with the behaviour of a vehicle. It is used to represent vehicle honesty or malicious nature.
T_y	Trust message	These messages are forwarded from the vehicle source to the destination via the vehicles in the VANET. It is used to identify the trust metrics used to calculate the trust value of vehicles.
R_s	RSU	This is an infrastructure member of the VANET. This is to calculate the trust values of the vehicles in the VANET. It receives data from the vehicle watchdogs and calculates the trust value.
A, L, W	Area, Length, Width	The length and width represent the area where the VANET is applied to. The length and width represent the edges of the area, and the area represents the total area. Such that A = L * W where L and W are given in meters.
V_n	Vehicles	These are the vehicles that belong in the VANET and occupy the area.
V'_n	Watchdogs	These are the watchdogs selected by the RSU. They will watch other vehicle communications in the VANET.
V''_n	Sensing vehicle	This vehicle in the VANET has sensed environmental data and will broadcast it to other vehicles in the VANET.
Q_v	VANET Queue	This is a list of messages or actions yet to be performed in the VANET. An empty VANET queue indicates that no message communications are happening at the current time. This provides an opportunity for the trust management system to start operations.

Appendix C – List of symbols used in Chapter 6

Symbols used in the watchdog selection process. (Referred to from section 6.3)

Symbol	Definition	Description
ω_x	Packets received by a vehicle in previous communication rounds.	This is a part of the operational history of a vehicle; it represents the packets received by a vehicle to be forwarded.
μ_m	Packets successfully forwarded by a vehicle in previous communication rounds.	This is part of the operational history, representing the total number of packets a vehicle forwarded.
α_t	Processing delay.	This is a part of the operational history. It is the amount of time taken to process a packet before forwarding.
γ_i	Residual energy	This is the total amount of energy remaining in a vehicle.
β_j	Initial energy	This is the total amount of energy the vehicle started operations with.
V_n	Vehicles	These are the vehicles that make up the VANET.
V'_n	Watchdogs	This is the set of vehicles that have the watchdog agent activated.
R_s	RSU	This is the set of RSUs in the VANET.
X_a	RREQ packets	This is the number of route request packets sent by the RSU.
Y_b	RREP packets	This is the number of route reply packets received by the RSU.
T_y	RREQ packets send time	This is the RREQ packet send time.
z_d	RREP packets receive time	This is the RREP packet receive time.