2019

Fixed Cluster Based Cluster Head Selection Algorithm in Vehicular Adhoc Network

MUHAMMAD ANWAR SHAHID
University of Windsor

Fixed Cluster Based Cluster Head Selection Algorithm in Vehicular Adhoc Network

By

Muhammad Anwar Shahid

A Thesis
Submitted to the Faculty of Graduate Studies
through the School of Computer Science
in Partial Fulfillment of the Requirements for
the Degree of Master of Science
at the University of Windsor

Windsor, Ontario, Canada

2019

Fixed Cluster Based Cluster Head Selection Algorithm in Vehicular Adhoc Network

by

Muhammad Anwar Shahid

APPROVED BY:

_____

J. Pathak

Oddette School of Business

_____

I. Ahmad
School of Computer Science

_____

A. Jaekel, Advisor
School of Computer Science

April 18, 2019

DECLARATION OF ORIGINALITY

I hereby certify that I am the sole author of this thesis and that no part of this thesis has been published or submitted for publication.

I certify that, to the best of my knowledge, my thesis does not infringe upon anyone's copyright nor violate any proprietary rights and that any ideas, techniques, quotations, or any other material from the work of other people included in my thesis, published or otherwise, are fully acknowledged in accordance with the standard referencing practices. Furthermore, to the extent that I have included copyrighted material that surpasses the bounds of fair dealing within the meaning of the Canada Copyright Act, I certify that I have obtained a written permission from the copyright owner(s) to include such material(s) in my thesis and have included copies of such copyright clearances to my appendix.

I declare that this is a true copy of my thesis, including any final revisions, as approved by my thesis committee and the Graduate Studies office, and that this thesis has not been submitted for a higher degree to any other University or Institution.

ABSTRACT

The emergence of Vehicular Adhoc Networks (VANETs) is expected support variety of applications for driver assistance, traffic efficiency and road safety. For proper transmission of messages in VANET, one of the proposed solutions is dividing the network into clusters and then selecting a cluster head (CH) in each cluster. This can decrease the communication overhead between road side units (RSUs) and other components of VANETs, because instead of every node communicating with RSU, only CH communicates with RSU and relays relevant messages. In clustering, an important step is the selection of CH. In this thesis, we implemented vehicle to vehicle (V2V), cluster head to road side unit and road side unit to trusted authority authentication for the clustered network. We also presented a heuristic algorithm for selecting a suitable vehicle as the cluster head in a cluster. For the selection of head vehicle, we used weighted fitness values based on three parameters; trust value, position from the cluster boundary and absolute relative average speed. Simulation results indicate that the proposed approach can lead to improvements in terms of QoS metrics like delay, throughput and packet delivery ratio.

DEDICATION

I dedicate this thesis to my parents Mr. and Mrs. Shahid, for their prayers and motivational guidance on each step in my life. To my beloved wife, Mahwish for the sacrifice and unconditional support throughout the study period. To my children, Ayaan, Ehaan and Affan for giving me the reason to spend more time on studies outside of their soccer class.

ACKNOWLEDGEMENTS

First of all, I would like to thank Almighty God for giving me strength, ability and will to complete my graduate degree.

My supervisor Dr. Arunita Jaekel for the knowledge, guidance and support to complete my program. I really appreciate the way you taught me to handle complications with easy and smooth approach. Special thanks for your valuable time and efforts specially during your sabbatical leave to bring me at this stage.

My committee members Dr. Jagdish Pathak and Dr. Imran Ahmad for their valuable time.

All secretaries in School of Computer Science for all the support during my study period.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS/SYMBOLS

AODV	Adhoc On-Demand Vector) protocol
BSM	Basic Safety Message
CA	Certificate Authority
CBR	Cluster Based Routing
CH	Cluster Head
CHSA	Cluster Head Selection Algorithm
C-ITS	Cooperative Intelligent Transportation System
CM	Cluster Member
DoS	Denial of Service
DSRC	Dedicated Short Range Communication
ECDSA	Elliptic Curve Digital Signature Algorithm
FCC	Federal Communication Commission
GPS	Global Positioning System
ITS	Intelligent Transportation System
LT	Life Time
MAC	Medium Access Control
MANET	Mobile Adhoc Network
OBU	On Board Unit
OMNET++	Objective Modular Network Testbed
OSM	Open Street Map
PDR	Packet Delivery Ratio

QoS	Quality of Service
RSU	Road Side Unit
SDMA	Spatial Division Multiple Access
SUMO	Simulation of Urban MObility
TA	Trusted Authority
TDMA	Time Division Multiple Access
TV	Trust Value
V2I	Vehicular to Infrastructure
V2V	Vehicular to Vehicular
V2X	Vehicular to any component in VANET
VANET	Vehicular Adhoc Network
VEINS	Vehicles In Network Simulation
WAVE	Wireless Access in Vehicular Environment

CHAPTER 1
INTRODUCTION

1.1 Overview

Intelligent Transportation System (ITS) involves the application of modern digital technologies to increase safety and control on the roads among vehicles. Major objectives of ITS include traffic safety, congestion control, efficiency in traffic flow, reduced air pollution and improved energy efficiency [23]. Cooperative Intelligent Transportation System (C-ITS) handles all the communication in ITS, among different devices in the system [22]. Emerging application of Vehicular Adhoc Network (VANET) is perfectly aligned with the purpose of ITS because it provides such platforms for safer roads with minimum losses. VANET is attracting significant interest from manufacturers and researchers in the wireless networks due to the growing number of applications designed for the safety of passengers. VANETs are adhoc networks that are highly dynamic, with limited access to the network infrastructure and offer multiple services. VANET is a special branch of Mobile Adhoc Network (MANET) and provides us with a platform for improving road safety and better movement of vehicles on the road [1]. VANET, is a special branch of ad hoc network, where network nodes consist of vehicles (with on-board units or OBUs) Road-side units (RSUs) and other infrastructure nodes.

Dedicated Short Range Communication (DSRC) technology [13] is an emerging technology that has been developed for highly dynamic networks, to support fast link establishment and to minimize communication latency. DSRC is designed to ensure the reliability of safety applications, taking into consideration the time constraints for this type of applications.

Quality of Service (QoS), for VANET safety messages is considered as the successful delivery of broadcast messages over a communication channel. There are many QoS metrics that are helpful in assessing and evaluating the service quality in any wireless communications, such as throughput, packet loss ratio and delay [11]. To improve the QoS in VANET, many researchers have proposed the use of various clustering techniques which are available in the literature [3]–[5]. Cluster formation can help reduce the network load and increase the overall efficiency. Each cluster has two or more members and selects its cluster head, which is responsible for faster communication with minimum delay.

1.2 Motivation

In recent years, VANET has found widespread popularity in both industry and academic applications ranging from e-health [42] to intelligent transportation system [22] and itinerary planning [26]. The primary objective of a vehicular ad hoc network is to provide comfort and safety to vehicle passengers. The system components of VANET are [1]-[3][16]:

- OBU: On-Board Unit (OBUs) is a communication device which is fixed in the vehicle so that vehicle can communicate with other nodes in the VANET infrastructure.
- RSU: Road-Side Unit (RSU) is found alongside the road typically over the street lights. This device is a stationary component in VANET and enables OBU to get connected with network/internet.
- Application Unit (AU): It is mounted in the vehicle. It gives access to different application to enhance safety and control.
- Trusted Authority (TA): TA provides secure communications between nodes in VANET.

These components can communicate with external resources and Internet [1]-[3]. Furthermore, a third trusted party i.e. trusted authority is deployed in the vehicular ad hoc network.

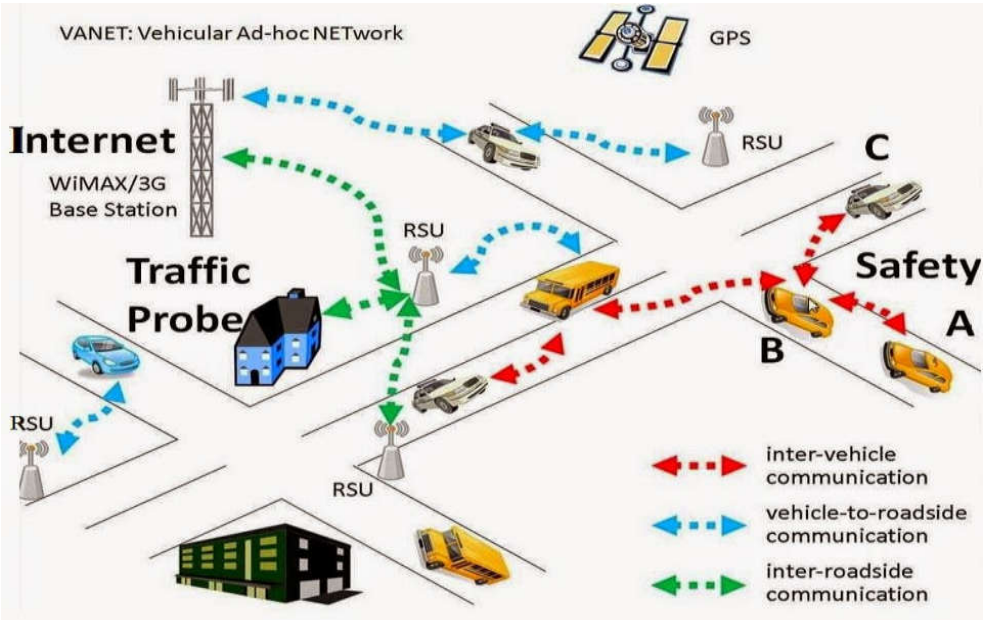

Figure 1. 1: Formation of VANET on the road [1]

Figure 1.1 shows a structure of typical VANET. There are two communication modes used in VANET: vehicle-to-vehicle communication (V2V) and vehicle-to-infrastructure communication (V2I). However, V2V and V2I communications are vulnerable to malicious attackers, who can easily modify the message sent from a vehicle and/or can disguise as a vehicle for receiving sensitive information via RSU [26]. Hence, in VANETs proper authentication is necessary to determine whether a message can be trusted or not.

It is very difficult to communicate efficiently especially in a sparse network. To overcome this problem, many researchers proposed clustering of nodes. Clustering is a grouping of nodes according to some criteria based on different approaches like average speed, location, direction and destination [5]. Each node communicates with vehicles within its own cluster; then cluster head is responsible for communication with other clusters. This way, communication is faster and

less overhead can be observed due to short range of communication [41]. Each cluster head in the cluster is responsible to communicate with its members, RSU and cluster heads of other clusters. This communication can include different types of messages like Broadcast messages, Hello messages, Basic Safety messages (BSM) etc. Reliable dissemination of messages in VANET is essential in order to avoid serious events like accidents and potential loss of life. So, it is important to develop suitable techniques for reliable *cluster head* (CH) selection, based on average speed and trust values [40].

1.3 Problem Statement

Challenges in VANET include signal fading, bandwidth limitations, connectivity, security and privacy issues [23]. Effective routing and congestion control techniques help to alleviate some of these challenges and allow each vehicle to send and receive safety related messages using V2V communication. FCC (Federal Communication Commission) has developed a Dedicated Short Range Communication (DSRC) protocol [17].to handle such V2V communication.

Hierarchical cluster based routing protocols have demonstrated certain advantages for vehicular communication, in terms of congestion control, security and privacy, routing and reliability. A *cluster* can be defined as the group of nodes, which perform some specific tasks under set rules and regulations [7]. The technique of gathering a collection of nodes such as mobile gadgets, devices, automobiles etc. into a single group is known as *clustering*. In VANET, clusters can be established using different algorithms [25]. An efficient clustering protocol allows nodes to form a stable cluster that sustains the current structure ensuring the less overhead. Each Cluster is equipped with *cluster head* (CH) and multiple *cluster members* (CM) [13]. Clustering algorithms are also typically responsible for selecting the cluster head for a given cluster. The way a cluster

is formed has a significant impact on the reliability of the related communication. In this thesis, our goal is to develop a new clustering algorithm for VANETs that can improve vehicular communication.

1.4 Solution Outline

There are many existing clustering techniques including predictive clustering [13], MAC based clustering [5], secure clustering [43] etc. available in the literature. In predictive clustering, grouping depends on traffic information, future destination or/and position of nodes. Position based clustering is considered as a sub-type of predictive clustering. In our approach, we use a position-based clustering, where the road segment is divided into clusters of 300m each. We propose a heuristic algorithm that uses information about vehicle parameters to choose the cluster head. The performance of the proposed approach is evaluated by comparing with existing techniques and shows significant improvements in terms of standard metrics such as throughput, delay and packet delivery ratio.

1.5 Thesis Organization

The remainder of this thesis is organized as follows. In Chapter 2, we discuss background literature on VANET and give an overview of existing clustering techniques. Chapter 3 will describe the proposed approach. We will discuss the results in Chapter 4 and present our conclusions and directions for future work in Chapter 5.

CHAPTER 2
BACKGROUND

2.1 Intelligent Transportation System

ITS has been established to improve transportation safety and efficiency on the roads. Cooperative ITS (C-ITS) and VANET are critical components to help achieve this goal [22]. Many countries are investing in this growing technology that will allow transportation assets to become increasingly integrated and communicate through a wireless communications system. Travellers and goods carriers will have knowledge of system performance and will be able to plan their journeys accordingly. C-ITS requires coordinated communication among vehicle OBUs, RSUs and other infrastructure. In this chapter, we will review some basic technology and protocols that enable such communication.

2.1.1 Dedicated Short Range Communications (DSRC)

In the USA, FCC (Federal Communication Commission) has allocated 75MHz of spectrum allocated for *Dedicated Short Range Communications* (DSRC) [23], as shown in Fig. 2.1, to handle vehicular communication.

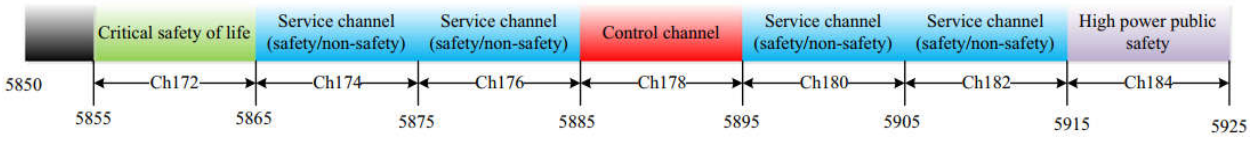

Figure 2. 1: DSRC spectrum band and channels [13]

IEEE 802.11p, which is based on IEEE 802.11 [13], is the protocol used for DSRC. This radio technology is equipped with a total bandwidth of 75 Mhz using 5.9 GHz frequency band. This band has been divided into seven different channels, where each channel is of 10 MHz, as shown

in Fig. 2.1. Out of these 7 channels, one channel (channel 178), known as the control channel, is reserved for high priority safety messages. The remaining six channels are known as service channels, which serve for data communication [44].

2.1.2 DSRC/WAVE Architecture

Recently IEEE established a standard communication architecture for VANET. It is called WAVE (Wireless Access in Vehicular Environment) architecture, which is responsible for *vehicle-to-vehicle* (V2V) and *vehicle-to-infrastructure* (V2I) communication in VANET. WAVE belongs to IEEE 802.11p standard.

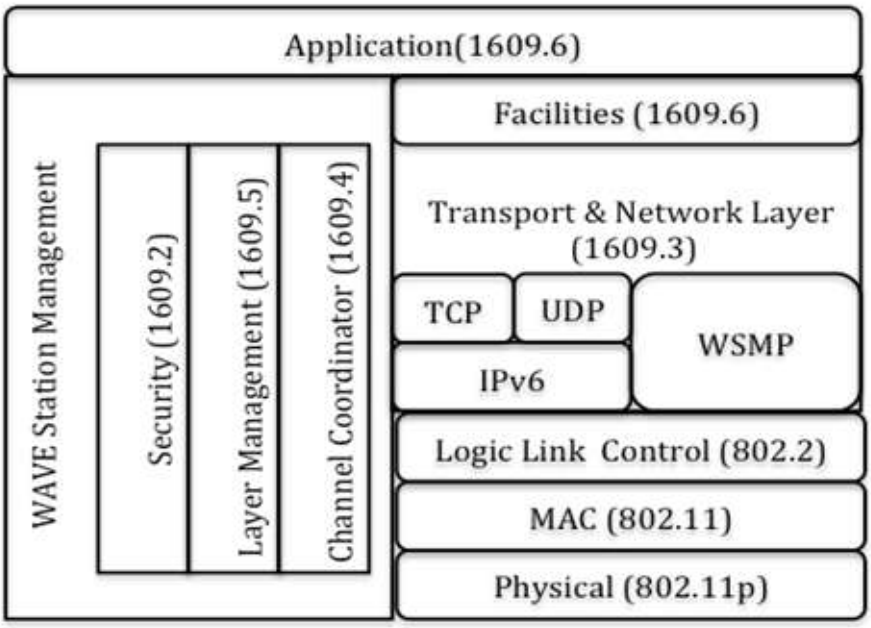

Figure 2. 2: WAVE Architecture [IEEE 1609.0-2013][1][2]

Figure 2.2 shows WAVE architecture with IEEE 802.11p standard. It also specifies MAC and Physical layer standards for communications. It a is protocol stack for DSRC. There was a need to develop new protocol because of transmission range which can be up to 1000m in VANET [44]. Here, we have physical and MAC layer along with standards for these layers like 802.11p and 802.11. Security services are covered by the standard IEEE 1609.2. This layer is basically

responsible for data encryption and key management. 802.11 protocol is an amendment to the WiFi standard 802.11 which is build for VANET communication. Physical and MAC layers of 802.11p are derived from 802.11a and consist of 3 different channels widths: 5, 10 and 10 MHz. It supports 8 different data rates which are 3, 4.5, 6, 9 , 12, 18, and 27 Mbps [44].

2.2 Types of Communications in VANETs

Vehicle-to-vehicle (V2V) communications has a wireless connection with other vehicles and through it, they can directly exchange information regarding their positions, speed and other characteristics. Through V2V connection, vehicles are able to send or receive safety critical information in a timely fashion. Such information is used by different safety applications, e.g. collision avoidance algorithms [38] to ensure safety and security of drivers and vehicles.

Vehicle-to-infrastructure (V2I) communication occurs between vehicles and other infrastructure that is available to support C-ITS. Such infrastructure can include roadside units (RSUs), traffic lights, cameras and readers etc. V2I also uses short range communication (DSRC) frequencies to transfer data, similar to V2V. Information and advisory notices regarding accidents, traffic blockage and other weather conditions can be sent to vehicles using V2I communication. V2I can also be used with other with external systems. For example, it can establish a connection with pedestrians, cyclists, lights and even buildings [37].

V2V and V2I communication are often collectively referred to as V2X communication in the literature. V2X communication is expected to enhance both safety applications (e.g. collision avoidance) and service applications (e.g. of automatic payments for parking and tolls). Protocols for V2X communication must be designed with security, privacy and efficiency in mind to meet

the requirements of timely and reliable message delivery. Figure 2.3 shows the different components of a V2X communication system, using DSRC.

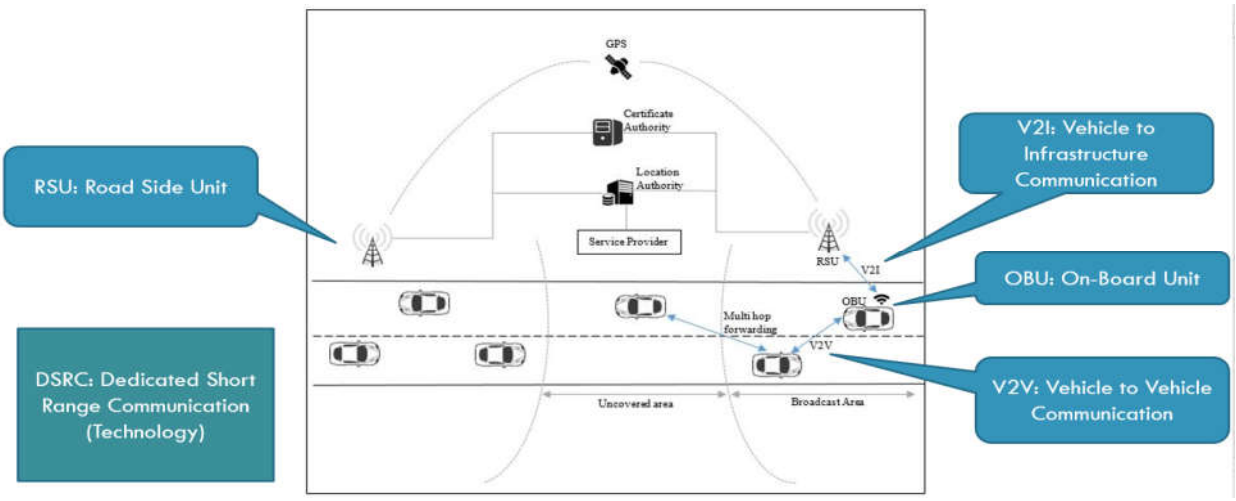

Figure 2. 3: VANET structure showing types of communications using DSRC

2.3 Characteristics of VANETs

There are number of unique characteristics of VANET nodes and network topology that must be taken into consideration when designing suitable communication technologies. In this section, we will discuss some of these important features.

A. High Mobility and Rapidly Changing Network

Vehicles on the road move with high speed and change their position rapidly. As a result, the network topology is highly unstable and may become disconnected at times. VANET communication protocols must be able to handle such rapid changes in topology. The inclusion of infrastructure nodes, whose positions are fixed, can help to address some of these challenges [4]. VANET nodes generally travel at high speeds. This makes it more difficult to predict location of the node and protect personal information of the node. Node location changes frequently because

of high mobility of node and arbitrary vehicle speed. As a result, the network topology of the VANET tends to change frequently.

B. Network Size and Exchange of Information

Network size in VANET has no well-defined geographical boundaries. It can consist of town, cities, provinces or even countries. Information exchange in this rapid network is frequent, because signals originate from other vehicles as well as RSUs and other infrastructure nodes. To reduce the risk on the road, it is necessary to convey this information to all relevant nodes in an accurate and timely fashion. In addition of lack, there is no specific duration during which vehicles must remain connected. They can be in network for limited time or for long time. Some vehicles can join, while some other vehicles can exit the network any time. Such variability in terms of network size and structure lead to challenges for effective communication.

C. Processing Power and Energy

Network nodes or vehicles in VANET are assumed to have sufficient power to run complex authentication algorithms and calculations [15]. Therefore, unlike some other types of networks, such as sensor networks, minimizing power usage is typically not an important consideration for VANET. VANET is intended to work in wireless environments. Nodes communicate with each other wirelessly and any security measures should be taken for secure communication. Availability of enough energy and computational resources allows for the use of technologies such as Elliptic Curve Digital Signature Algorithm (ECDSA) implementations, RSA, in VANET [15].

D. Physical Location and Position

We assume that the network nodes in VANET are aware of their location and position, for example through use of GPS [2].

2.4 Algorithm Performance Analysis using QoS metrics

Performance analysis must be done to assess the efficiency of a proposed algorithm. Many different Quality of Service (QoS) metrics can be used to evaluate the performance [11]. Some of the widely used metrics for evaluation of communication protocols are discussed below.

1. **Delay**: The delay is an essential factor in the transmission of messages from source to destination. It is defined as the time taken to send a packet successfully from one node to another [26]. The delay is computed based on the amount of time taken for a packet to reach its destination from its source. Practically, it is defined by the difference between the reception time of the packet at the destination node and the transmission time of a packet at the sending node. It is computed as follows [26]:

$$\text{Delay} = \sum_{i=1}^{n_p} (T_{reci} - T_{sendi})/n_p$$

Here n_p represents number of packets, T_{reci} and T_{sendi} denote receiving and sending time of a packet i, respectively.

2. **Throughput**: Throughput is computed as the number of bits transmitted per second. It should be higher in a secure network to obtain improved QoS performance. It can be expressed mathematically as follows [26]:

$$\text{Throughput} = (n_r \times n_p)/T_d$$

Here n_r is the total packet received, n_p is packet size and T_d is the total time (in seconds).

3. **Packet Delivery Ratio (PDR):** PDR is the ratio between the total number of packets delivered to that total number of packets received by the node. Greater value of PDR shows the better performance of network efficiency. It is calculated as follows [26]:

$$\text{PDR} = [\sum Pkt_{reci}/n] / \sum Pkt_{senti}$$

Where Pkt_{reci} and Pkt_{senti} are packets received and sent by a vehicle *i*.respectively. *n* denotes the number of nodes.

In this thesis, we have used the above metrics to evaluate the performance of the proposed algorithm.

2.5 Security in VANETs

VANET communication should ensure security in terms of availability, confidentiality, authentication and integrity [1], because compromised communication can pose a serious threat to safety and well-being of users.

Availability: To ensure the access of the authorised entities to the network resources with adequate quality of service. For availability, legitimate users should have access to the required information. Availability discusses the proper processing of each message so that it should reach the destination on-time. Potential security attacks are Denial of Service (DoS), Jamming, Broadcast Tempering, Malware, Spamming and Black Hole Attack [1].

Confidentiality: To ensure that only the authorised parties can access the data transmitted through the network. Confidentiality handles the rules associated to use different assets like OBU, RSU etc. It can be vulnerable to Eavesdropping, Information Gathering, Traffic Analysis etc [1].

Authentication: To allow network members to ensure the proper identity of the members with whom they communicate. Authentication is related to valid and authentic origin of sender or receiver. Authentication allows legitimate users to generate messages. In VANET, the vehicle responds to information from other vehicles and must be certified. It involves attacks like Replay, GPS spoofing, Position Faking, Masquerade, Tunneling, Key/Certificate Replication, Message Tempering etc [1].

Non-Repudiation: To ensure that issuer cannot deny being the issuer of the message. It can be vulnerable to loss of events traceability. Non-repudiation means that a node cannot deny that it is not sending a message. It may be important to determine the exact order of the collision reconstruction [1].

Integrity: To ensure that exchanged data is not altered, either intentionally or accidently. It allows the recipients to detect the data manipulation performed by unauthorised entities and discard the corresponding packets. It can be vulnerable to Message Suppression, Message Alteration, Message Fabrication, Masquerade, Replay [1]. Integrity can be enforced by using digital signatures [6].

In V2V communication, the exchanged information (emergency message, safety messages etc.) through wireless channels requires a secure environment to avoid attacks on V2V network. Such attacks include [1]:

i. injection of erroneous messages containing false information to cause an accident or to redirect the traffic in a way to release the used route.

ii. the revelation of the identity and the geographical position of the other vehicles. For example, a car rental company that wants to follow its own vehicles in an illegitimate manner.

iii. the unauthorised access, where the malicious entities access the network services without having the rights and privileges.

iv. the usurpation of the identity of a node (spoofing and impersonation), where the attacker tries to impersonate another node in order to receive messages or to get privileges that are not granted to him.

v. the denial of services (DoS), which make the resources and the services unavailable to the users in the network either by jamming or "Sleep Deprivation" [18][6].

In this context, secure communication requires the implementation of certain mechanisms to achieve the security requirements.

2.6 Clustering Techniques in VANETs

The technique of garnering the group of nodes with same characteristics (destination, direction, speed etc.) is known as *clustering* [2]. The clustering algorithm creates the various virtual sets called *clusters*. Each cluster contains one cluster head (CH), and several cluster members (CMs). In most of the cases, one CM is nominated as a CH. CH selection can depend on different properties, for example the node possessing the best relative average speed may have a higher chance to be selected as CH, compared to other CMs. Every cluster has its defined size in terms of area or number of nodes, which is dependent on the node's transmission range [5]. The

communication efficiency of VANETs can be enhanced through vehicular node clustering, if the clusters are reliable and possess longevity [17]. The stability of a cluster is enhanced by the proper selection of CH and CMs in order to form a specific cluster.

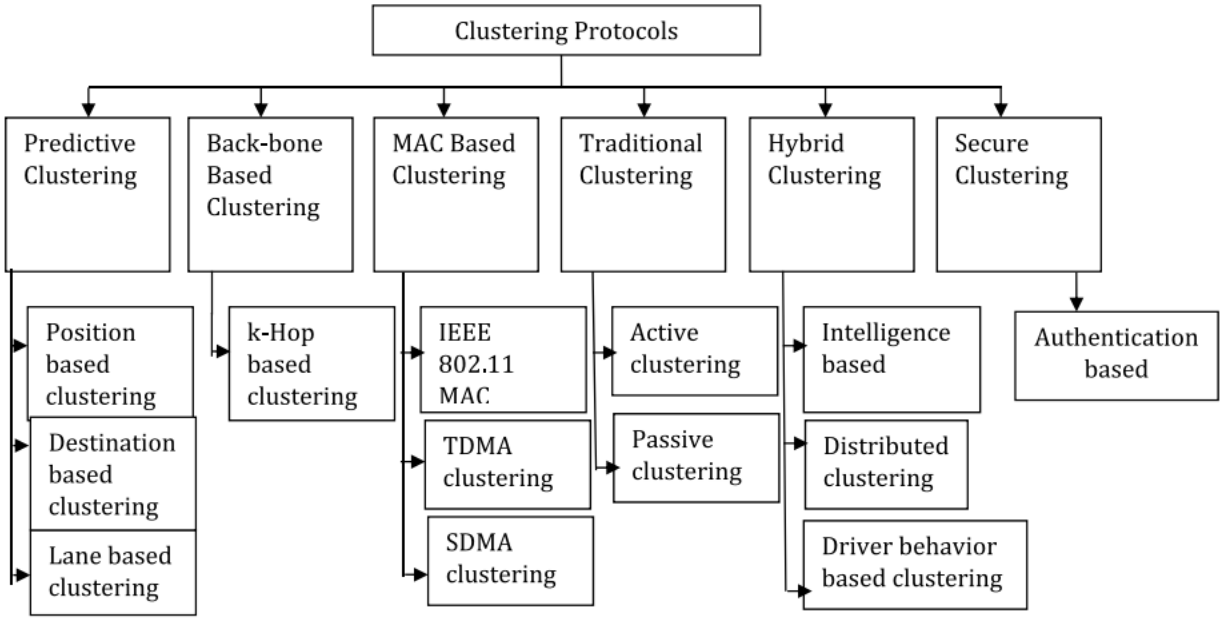

Figure 2. 4: Taxonomy of existing clustering approaches for VANETs [9]

There are a wide variety of clustering protocols available in the literature. A taxonomy of existing clustering approaches is shown in Figure 2.4. Clustering algorithms can be broadly classified into the following groups [9]:

- Predictive clustering: It is based on position of nodes and their future behaviour. These attributes are used in formation of clusters in VANET. Position based clustering, Destination based clustering and Lane based clustering are most famous types of predictive clustering [13].

- Back-bone base clustering: In this clustering technique, a communication back-bone is set up, which can be helpful in election of CH. k-hop or multi-hop [13] is an example of this type of clustering, in which hop distance is used to form a cluster.
- MAC-based clustering: Medium Access Control (MAC) based clustering utilizes IEEE 802.11 MAC protocol to form clusters. It includes IEEE 802.11 MAC, TDMA (Time Division Multiple Access) and SDMA (Spatial Division Multiple Access) clustering techniques [9].
- Traditional clustering: It depends on the nature of vehicles. It is based on active and passive clustering techniques associated with behaviour of vehicles. Active clustering further sub-divided into Beacon based, Mobility based, Density based and Dynamic Behaviour based clustering [9].
- Hybrid clustering: In this technique, two or more techniques like fuzzy logic and AI are used to form clusters. It is sub-categorized as intelligence based, Distributed and Driver behavior based clustering techniques [9].
- Secure clustering. It involves security parameters to establish clusters in the network. Trusted Authority (TA) and Certificate Authority (CA) are usually involved in this clustering approach. Authentication based clustering is one of the example in this category.

The proposed approach in this thesis is based on *predictive* clustering. So, we will look at this approach in more detail in this section.

Predictive clustering protocol based on the geographic position of nodes and future behaviour of nodes. Now we will discuss further categories of this clustering technique.

1. **Position Based Clustering**

Position based clustering is the building block of clustering techniques in VANET. Node position or geographical location is very important in this technique. Many researches have been done on different parameters to form clusters, but position based clustering techniques have more impact on clustering than any other technique. Some of algorithms related to position based clustering are summarized in table 2.1.

Table 2. 1: Comparison of Position Based Clustering Algorithm

Schemes	**Node density**	**Cluster stability**	**Node speed**	**Transmission overhead**
Cluster Gathering Protocol (CGP) [24]	high	high	high	high
Position Based Prioritized Clustering (PPC) [39]	low	high	low	medium
Dynamic Cluster Algorithm (DCA) [25]	low	medium	high	high
Modified Clustering Based on Direction (C-Drive) [27]	low	medium	high	high

2. **Destination Based Clustering**

Destination based clustering considers three parameters for cluster formation. These parameters are node location, speed and the destination. It can take advantage of navigation devices in vehicles to improve performance. By using information from navigation devices, we can know the destination of moving node in advance. Because of similar destinations, cluster time span can be improved. Table 2.2 illustrate some algorithms which showcases destination based clustering techniques:

Table 2. 2: Comparison of Destination Based Clustering Algorithm

Schemes	**Node density**	**Cluster stability**	**Node speed**	**Transmission overhead**
Cluster Based Location Routing (CBLR) Algorithm [29]	high	high	high	high
Robust Localization using Cluster Analysis LICA [31]	low	high	low	medium

Lane Based Clustering

This type of clustering needs the information about lanes and its availability. It can have less number of changes in selection of CH because of fixed structure of lanes on the road. Transmission overhead in this technique is reported less because usually node maintains its speed as constant being in the same lane. Table 2.3 shows two different algorithm which implemented lane based clustering technique:

Table 2. 3: Comparison of Lane Based Clustering Algorithm

Schemes	**Node density**	**Cluster stability**	**Node speed**	**Transmission overhead**
Lane Based Clustering [35]	low	high	low	medium
Broadcast Decision Algorithm (BDA) [36]	medium	high	medium	medium

The effectiveness of the clustering algorithm can be measured in terms of *cluster stability*, which also increases the performance level of the cluster [20].

2.7 Literature Review

In the literature, VANET clustering has been performed with different purposes, such as load balancing, quality-of-service support, and information dissemination in high-density vehicular networks [28]. Generally, it has been observed that Clustered Based Routing (CBR) [2] divides the massive network into small areas, called *clusters*. Cluster Heads help in establishing a connection between clusters, and also collaborate with other members of a cluster. An inter-cluster routing protocol is used by the CHs. The pivotal role of a cluster is to lessen the control overhead and to maximize the stability of a network.

In VANET, numerous algorithms have been suggested for electing the CH [2][3][6][13][19][20][21]. The cluster heads are selected according to the proposed protocol and they also observe the movements of vehicles and link between them. They also exchange messages, try to maintain an acceptable PDR, while observing the MAC layer contention time of all vehicles.

Wang et.al [39] proposed a position based clustering technique, based on geographic position of vehicles and some additional attributes like travel duration and variation in the node speed. Higher level of these attributes can decide the CH in each cluster. One drawback of this approach is high communication overhead due to rapidly changing CH and clusters.

H. Hasrouny [6] proposed the idea of group-based authentication in V2V communication. They created the groups or clusters of 300 m of diameter. CH selection depended on current location and speed of vehicles. This approach is good for group authentication, but it increases packet loss because of CH handling bidirectional traffic. Also, they consider very first vehicle in the cluster as CH, which may not always be the best choice.

In [7], R. Sugumar described a clustering approach in authenticated VANET, where CH selection is based on trust degrees only. They introduced trust degree as a combination of direct and indirect trust degrees. Direct trust degree is reported directly by neighbours considering past experience, whereas indirect trust degree is based on recommendation from near neighbouring nodes.

Ahmad Abuashour et al, [2] proposed Cluster based life time Routing (CBLTR). CBLTR is a two directional segmentation-based clustering algorithm, where cluster heads are selected based on maximum life time (LT). This protocol divides the road segments into bi-directional parts and then each part is divided into different groups. Range of each cluster or group has not been mentioned in the work. Each group has a pre-defined threshold boundary. Every node must be the part of one of the clusters and calculate its life time value, which is considered as the distance between its current position and the threshold boundary. A node having maximum LT value is elected as CH. This approach decreases the issue with number of clusters and increases the life span of the CH. If any node is between the threshold and the boundary of the next cluster, it is still in previous cluster but can not be considered for CH election.

In [12], Tao et al. has introduced CBDRP (Cluster-Based Directional Routing Protocol), which is useful for highway traffic scenario where a new CH is selected for a group of cars moving in the same direction. In this approach, current CH selects a new CH based on the central position of a node among its neighbors. The approach is compared with AODV (Adhoc On-Demand Vector) protocol [32] and shows better performance.

Yuyi Lue et al. in [4], also introduced an innovative protocol named CBR (Cluster Based Routing) protocol. The election process of CH is completed by picking a fellow CH, which has a suitable angle which observes the angle between destination node and cluster center.

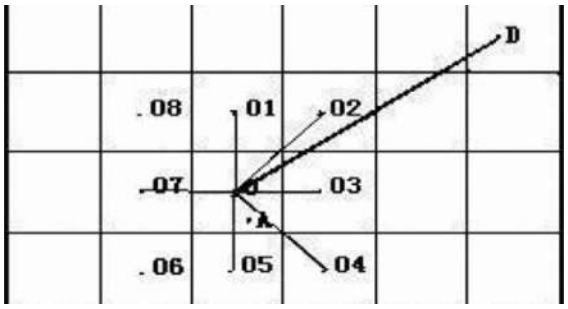

Figure 2. 5: select the optimal neighbor cluster header [4]

The main purpose of selecting such angle is to deliver the data from the main source to the destination node rapidly.

Ahmed et. al. [8], has suggested an algorithm, which is based on clustering, to establish stable connections in VANET. AODV for cluster maintenance in VANET(AODV-CV) has been proposed in this work. CH selection was considered dependable on two important factors: actual speed and the average velocity of the nodes. They reported better performance in terms of throughput when compared to AODV protocol.

Moezjerbi et al.[10] presented GYTAR (Greedy Traffic-aware Routing Protocol) based on road intersection and its geographical information. It is another position based clustering algorithm and it used distance from the cluster centre as a parameter to select CH. One of the responsibilities of CH was to estimate the cost of clustering segment from one intersection to another.

Rawashdeh Y. [20] introduced a clustering technique for highway based VANET scenario. Clusters are formed by nodes travelling in the same direction under one-way traffic scenario. This technique considers the speed difference to create relatively stable cluster. CH selection is based on a multi-metric mechanism.

CHAPTER 3
PROPOSED AUTHENTICATED CLUSTERING TECHNIQUE

3.1 Introduction

Due to the high demand for VANET, it is vital to look for a mechanism that can enhance the efficiency of communications among different components of VANET like RSU, OBU, AS etc. Clustering techniques can play a vital role in VANET communication. It is important for any clustering technique to select a cluster head wisely, because the cluster head (CH) will be responsible for communicating with RSU and other clusters. Information that goes through CH should be secure and appropriate. Authentication of nodes and CH is also an important factor. There are many parameters which can be considered in the selection of CH. In this thesis, we propose an algorithm for selecting the CH based on vehicle position, average speed and trust values in authenticated V2V communication. The proposed scheme can be useful in:

1. Reducing the number of clusters:39

   The proposed fixed cluster approach means we can have only 4 clusters within the transmission range of RSU, while some current approaches, such as [19]-[21], have more than 20 clusters in their proposed work.

2. Increasing throughput

   One of the goals of clustering technique is to obtain stable clusters throughout the communication [26]. It gives stable connectivity of all CM to its CH, which helps to increase the overall throughput of the system.

3. Decreasing inter-packet delay

   More inter-vehicle communication can lead to increased delay in packet transmission [32]. Clustering techniques can reduce inter-packet delay because it offers reduced communications within clusters. The reason behind this is the inter-cluster and intra-cluster communications by CH.

4. Improving the packet delivery ratio

   As discussed earlier, stable cluster can provide stable connections between CH and CMs. It can ultimately increase the bandwidth availability and reduce the data collision. In fixed cluster approach, we can have stable clusters and hence it can provide more PDR for the system.

The common goal of clustering techniques in VANET is to have a smaller number of clusters and less change in the election of CH, since frequent changes in clusters and/or cluster heads can lead to increased communication overhead.

3.2 Fixed Clustering Approach

In this thesis, we use a fixed cluster model, where the entire road network is divided into adjoining *segments*. Each segment S_i is under the control of a single RSU, and is further subdivided into 4 clusters, as shown in Fig. 3.1. We make the following simplifying assumptions:

1. Enough infrastructure is available so that road network can be divided into adjoining segments, without gaps.
2. We currently consider only 'straight' road segments, so partitioning into quadrants can be preformed relatively easily.
3. We consider bi-directional traffic, with one lane in each direction.

4. Each vehicle knows geographical information, such as cluster boundaries and unique identity of each cluster. Such information may be broadcast by RSUs at regular intervals.
5. At any given time, each vehicle will be part of one and only one cluster.
6. There is a unique ID for each vehicle and cluster.

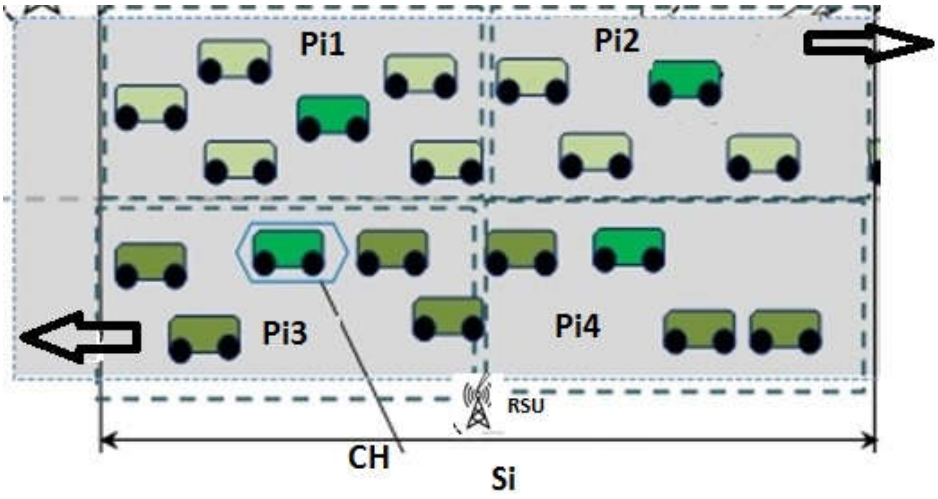

Figure 3. 1: Fixed Clusters on the road

Fig 3.1 shows road segment S_i divided into 4 clusters P_{i1}, P_{i2}, P_{i3} and P_{i4}. Any vehicle which is within the boundary of the cluster can be considered as part of the cluster.

3.3 Authentication in Fixed Clustering Approach

V2X communication technology provides not only road situation information, weather information, surrounding location information, but also facilitate with the information about emergency situations and lane change assistance. Services which are closely related to such emergency warnings should be provided in a secure way. It should not be exposed or tampered with malicious attackers. A suitable authentication mechanism is needed to ensure only legitimate

vehicles can send and receive the relevant communication messages in a cluster. In VANET, the vehicle responds to information from other vehicles and must be certified.

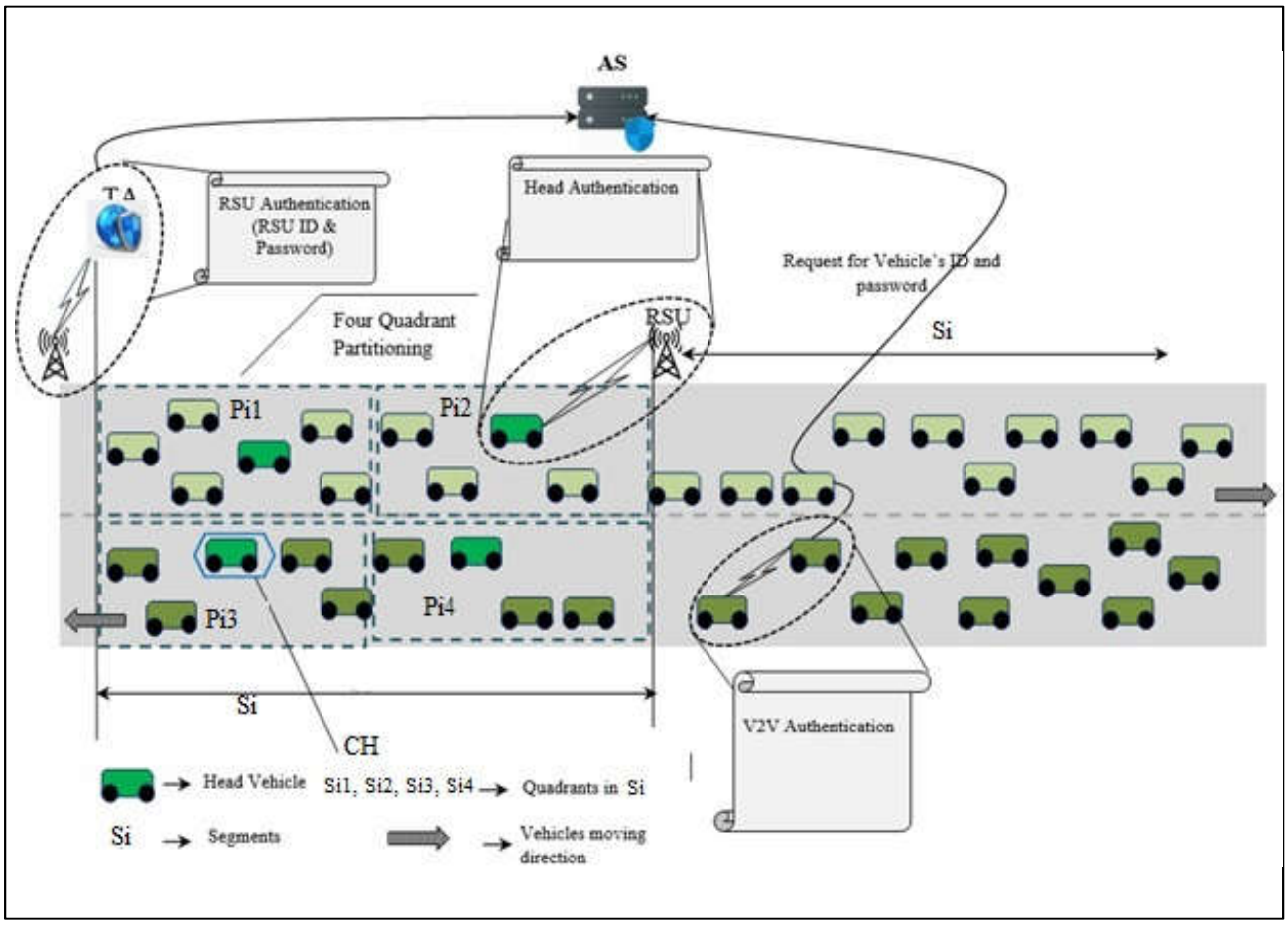

Figure 3. 2: A typical VANET authentication Scenario

Fig 3.2 shows the different participants involved in authentication in VANET. The proposed system comprised of four components: Vehicles, Roadside Units (RSU), Trusted Authority (TA) and Authentication Server (AS). Each vehicle and RSU is registered to TA and the information is shared with AS for the purpose of authentication. Vehicle registers with a unique Identity, whereas RSU registers with a unique identity and password. The RSU's password is static and it cannot be changed. Authentication is provided between the following entities (1) Vehicle to Vehicle

authentication, (2) Head Vehicle to RSU authentication and (3) RSU authentication. Different levels of authentication are required, as mentioned below.

- V2V authentication: Vehicle to Vehicle (V2V) communication is involved in VANET for sharing information between vehicles. This basic authentication is based on vehicle identity and location. Within the same cluster, each vehicle will share its identity and location to be authenticated within the same cluster. The parameters taken in account for this authentication are *id*, *Geolocation, time and status* of the vehicle.
- Vehicle authentication by RSU: This authentication is performed using an ID and password. On entering into the road, each node has to perform basic authentication with RSU then RSU will pass this information to CH.

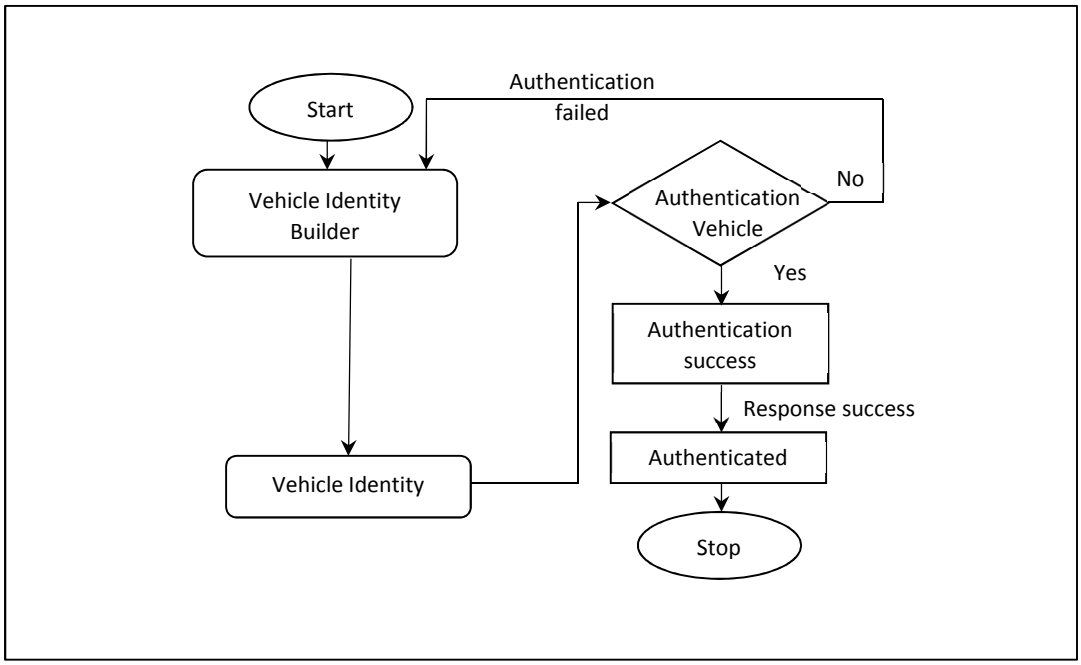

Figure 3. 3: Flow chart for vehicle authentication

Fig 3.3 shows a flow chart of the vehicle identity verification process. In the start, each vehicle gets its ID and password and then using these credentials it can join and be the part of the cluster.

In the case of authentication failure, the vehicle will start getting the identity from TA. After getting the new credentials, it will then be authenticated. This process will keep on going till the successful authentication.

- RSU authentication by Trusted Authority: RSU is authenticated by TA periodically to ensure that RSU is legitimate in the network. RSU ID and Password is verified for authenticating an RSU; here encryption is not used since the channel between them is secure.

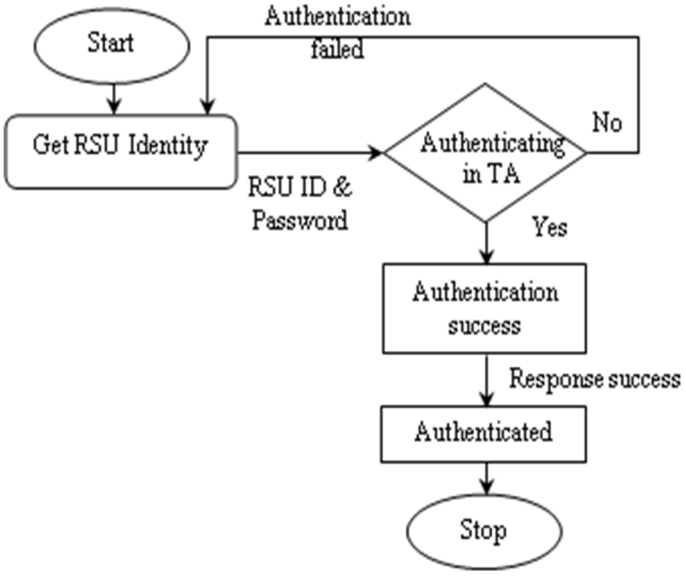

Figure 3. 4: Flow chart for RSU authentication

As described in Fig. 3.4, RSU is authenticated by TA based on its unique id and password. This authentication is performed on a secure channel so these credentials are not encrypted. Once authentication is done, RSU will get success response from TA.

3.4 Clustering Processes

In this section, we discuss the three main processes in maintaining/updating clusters. The process of joining and leaving a cluster are straightforward and are briefly outlined below. The main focus of this work is the cluster head selection process, which is described in detail in sec. 3.4.1.

- Joining a cluster: Since vehicles are aware of cluster boundaries and identity of each cluster, each vehicle will send a HELLO message when entering a new cluster. If it gets acknowledgment from CH, then it will be considered as a cluster member. Otherwise, it will request the RSU to start a new cluster head election process.
- Leaving a cluster: A vehicle *v* does not need to notify the RSU or cluster head explicitly, when it is leaving the cluster. A vehicle is removed from a cluster if:
    - no beacons are received from *v* for a specified period of time,
    - the CH or RSU receives a beacon from *v* and location of *v* is outside of the cluster.
- Cluster head (CH) selection: The cluster head for each cluster is selected by the RSU associated with that cluster, based on several factors. The RSU runs the CH selection algorithm, selects the CH and notifies it of its status. The selected vehicle then starts functioning as the CH, until a new CH is selected. The CH selection is run at regular time intervals, or if a request is received from a vehicle in the cluster.

3.4.1 Cluster Head Selection Algorithm

The cluster head is selected by the RSU, from the set of vehicles V in a given cluster. We use the following notation in the cluster head selection algorithm.

- V = Set of vehicles in the given cluster that are candidates for becoming the next cluster head.

- N_v = Number of vehicles in the cluster.
- v_i = The i^{th} vehicle in the cluster, $v_i \in V$
- s_i = Speed of vehicle v_i
- s_{avg} = Average speed of all vehicles in V.
- (x_i, y_i) = Coordinates of the current position of vehicle v_i.
- d_i = Distance from the current position of vehicle v_i to the cluster boundary (travelling in forward direction).
- TV_i = Trust value of vehicle v_i.

The RSU evaluates the suitability of each vehicle v_i to become the CH, based on its fitness value F_i, as given in equation 3.1.

$$F_i = w_1 \cdot TV_i + w_2 \cdot d_i - w_3 \cdot |s_i - s_{avg}| \qquad (3.1)$$

Here $w_1, w_2,$ and w_3 are weights denoting the relative importance of each component of the fitness function, where $0 \leq w_1, w_2, w_3 \leq 1$ and $w_1 + w_2 + w_3 = 1$. The higher the fitness value of a vehicle, the more suited it is to be selected as cluster head. The three components of the fitness function are:

1. **Trust value (TV_i) of a vehicle**: The trust value of a vehicle is a metric that estimates how reliably the vehicle will deliver messages, if selected as a CH. Vehicles with a higher trust value are more reliable, and hence more suited to function as CH. Calculating an accurate trust value is a complex task, based on factors such as past actions of the vehicle, its reputation as perceived be other vehicles, reports of malicious behaviour etc, and is out of the scope of this thesis. For our simulations, we have randomly assigned trust values ($10 \leq TV_i \leq 100$) to each vehicle.

2. **Distance (d_i) to cluster boundary**: This value is calculated based on the current position (x_i, y_i) of vehicle v_i and the cluster boundary that is ahead of the vehicle. If the value of d_i is higher, it means that the vehicle is farther from the boundary and is likely to remain in the current cluster for a longer period of time. This makes it a better candidate for CH, since if the CH leaves the cluster a new CH must be selected, leading to more overhead. Thus, a higher value of d_i increases the fitness value of the vehicle.

3. **Relative speed of vehicle in the cluster**: This metric measures how the speed of a vehicle compares with the other vehicles in a cluster. In general, it is desirable if the speed of the cluster head is similar to those of it's neighboring vehicles, as it is more likely it will be travelling together with its cluster members for a longer time. Thus, if the difference in vehicle speed (s_i) and the average vehicle speed (s_{avg}) of the cluster is very high, the vehicle is not a good candidate to be the CH. Hence in our fitness function (eqn 3.1), the fitness value of vehicle v_i is decreased as $| s_i - s_{avg}|$ increases.

1. Preprocessing phase:
    a. Set suitable values for w_1, w_2, and w_3
    b. Set T = cluster head selection interval
2. If (life time of current CH $\geq$ T) or (request for a new CH received):
   Run CH selection algorithm (steps 3 – 7)
    3. Determine the set (V) of vehicles currently in the cluster
    4. Initialize parameters
        a. $N_v = |V|$
        b. $s_{avg} = (\sum_{v_i \in V} s_i)/N_v$
        c. *current_best* = -9999
        d. CH = ϕ
    5. For each vehicle $v_i \in V$
        a. d_i = calc_dist_to_ boundary(x_i, y_i)
        b. $F_i = w_1 \cdot TV_i + w_2 \cdot d_i - w_3 \cdot |s_i - s_{avg}|$
        c. If F_i > *current_best*
            i. *current_best* = F_i
            ii. CH = v_i
    6. Return CH and reset lifetime of current CH.
    7. Go back to step 2.
8. Else:
    a. Go back to step 2.

Figure 3. 5: Outline of Cluster Head Selection Algorithm (CHSA)

Fig. 3.5 gives an overview of our proposed *cluster head selection algorithm* (CHSA). The first step is a pre-processing phase, where the relative weights for the 3 components of the fitness function are set. Also, the RSU sets the time interval T, which determines how often the CHSA is run. Once a CH is selected, it will typically continue as CH for a duration of T sec. Step 2 checks

if it is necessary to run the CHSA again. This will occur if T sec has elapsed since selection of current CH. Another reason may be if a vehicle requests it. This may occur, for example, if the current CH has left the cluster or has not responded to any messages for some time. If the conditions are satisfied, then CHSA is run (steps 3 – 7); otherwise the RSU continues to monitor the conditions (step 9).

In step 3, the RSU creates the set (V) of all vehicles in the cluster. This can be determined from the periodic safety beacons that are broadcast by all vehicles. These safety beacons also specify the location (x_i, y_i) and speed (s_i) for each vehicle v_i. In step 4, some relevant parameters are initialized, such as the number of vehicles (N_v) currently in the cluster and the average speed (s_{avg}) of the vehicles. Also, the current CH value is set to null, and the fitness for the current CH is set to a very low negative number.

Step 5 is repeated for each vehicle $v_i \in V$ and evaluates the fitness of each vehicle to be CH. In step 5a, the distance remaining to the cluster boundary is calculated for vehicle v_i, based on its current position and the location of the cluster boundary. As mentioned earlier, both of these parameters are known to the RSU. Next the fitness value F_i for the current vehicle v_i is calculated. If F_i is better than any of the fitness values obtained so far, then v_i is set as the potential cluster head and the *current_best* fitness value is set to F_i.

After all the vehicles have been considered, the one with the highest fitness is selected as CH by the RSU and a notification is sent accordingly. Also, the elapsed life time for the current CH is reset to 0.

3.5 Illustrative Example

In this section, we illustrate the operation of the proposed approach with a simple illustrative example. Figure 3.6. shows a cluster with 5 vehicles. The cluster boundary is shown as a dashed line on the left hand side of the figure. Vehicle speeds range from 25 km/h to 40 km/h. The trust value, speed and distance from the cluster boundary, for each vehicle, are as shown in the figure. Based on these values, the average speed of the vehicles is calculated as s_{avg} = 34.4 km/hr.

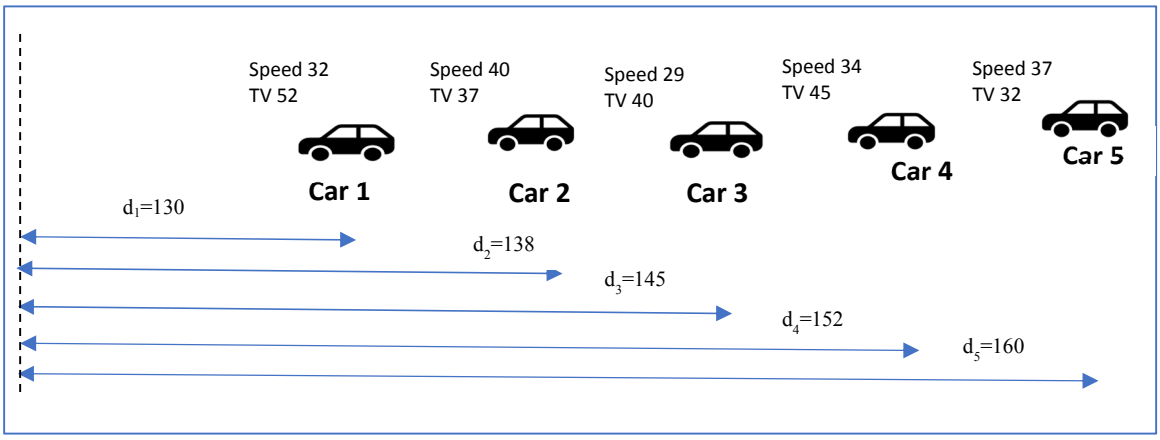

Figure 3. 6: Status of nodes in a cluster at time t_1

Different node parameters and corresponding fitness values, using equation (3.1), where w_1 = 0.3, w_2 = 0.4 and w_3 = 0.3, are indicated in the rightmost column of Table 3.1. Since fitness value of Car 4 is currently the highest, it will be selected as CH.

Table 3. 1: Node Attributes with Fitness values

	Trust Value (TV_i)	**Distance from cluster boundary (d_i)**	**Abs. Rel. Speed ($\|s_i - s_{avg.}\|$)**	**Fitness Value $F_i = 0.3*tv_i + 0.4*d_i - 0.3*(\|s_i - s_{avg.}\|)$**
Car 1	52	130	2.4	66.88
Car 2	37	138	5.6	64.62
Car 3	40	145	5.4	68.38
Car 4	**45**	**152**	**0.4**	**74.18**
Car 5	32	160	2.6	72.82

After some time, suppose the new positions and speeds of the vehicles are as shown in Fig. 3.7:

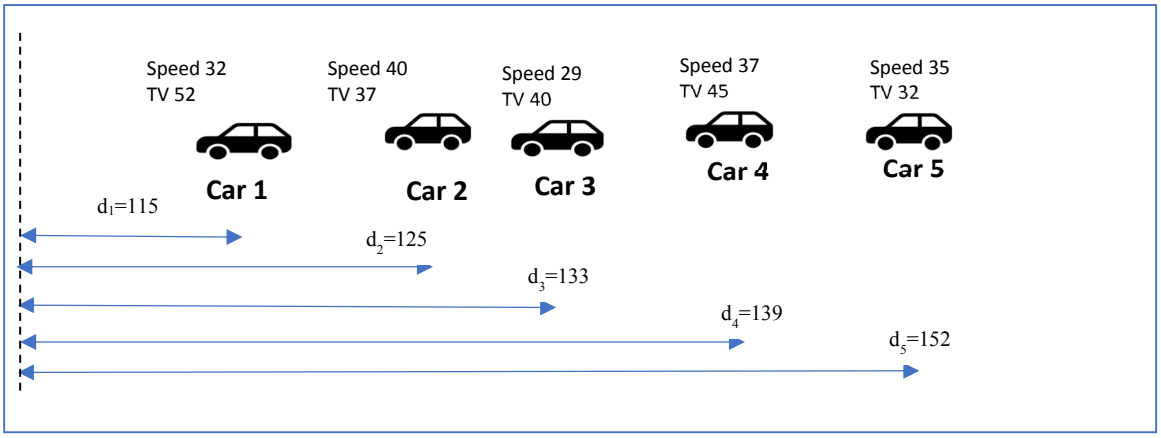

Figure 3. 7: Status of nodes in a cluster at time unit t_2

The new average speed of the vehicles is calculated as s_{avg} = 36.6 km/hr and the corresponding fitness values, using equation (3.1), where w_1 = 0.3, w_2 = 0.4 and w_3 = 0.3, are indicated in the rightmost column of Table 3.2. Since fitness value of Car 5 is currently the highest, it will be selected as CH.

Table 3. 2: Node Attributes with Fitness values

	Trust Value (TV_i)	**Distance from cluster boundary (d_i)**	**Abs. Rel. Speed ($\|s_i - s_{avg.}\|$)**	**Fitness Value $F_i = 0.3*tv_i + 0.4*d_i - 0.3*(\|s_i - s_{avg.}\|)$**
Car 1	52	115	2.6	60.82
Car 2	37	125	5.4	59.48
Car 3	40	133	5.6	63.52
Car 4	45	139	2.4	68.38
Car 5	**32**	**152**	**0.4**	**70.28**

CHAPTER 4
SIMULATION SETUP AND RESULTS

4.1 Simulation

Practical deployment of VANET scenario is expensive and needs many resources. A practical alternative approach to evaluate VANET performance is the use of simulators, which are cost effective, safe and comparatively easy to implement. There are many simulators available in the market, such as MATLAB, NS-2, and OMNET++/VEINS.

One of the challenges in VANET simulation is to combine the traffic and network model for simulation. In our work, we use *Simulation of Urban MObility* (SUMO [45] as the road traffic model generator and *Objective Modular Network Testbed* (OMNET++) [46] as the network simulator. SUMO is widely used in research field, because it is open source and can import real world maps easily. It has an explicit feature of microscopic multi-model simulation to simulate different types of nodes under VANET environment. OMNET++ is a C++ based discrete event network model, which is extensively used by scientific community to build almost every type of network. Finally, we use *Vehicles In Network Simulation* (VEINS) [47]framework to integrate SUMO with OMNET++. It connects SUMO and OMNET by a TCP socket, which allows bi-directionally coupled simulation. Fig. 4.1 shows the overall architecture of the simulator and the relationship among the different components.

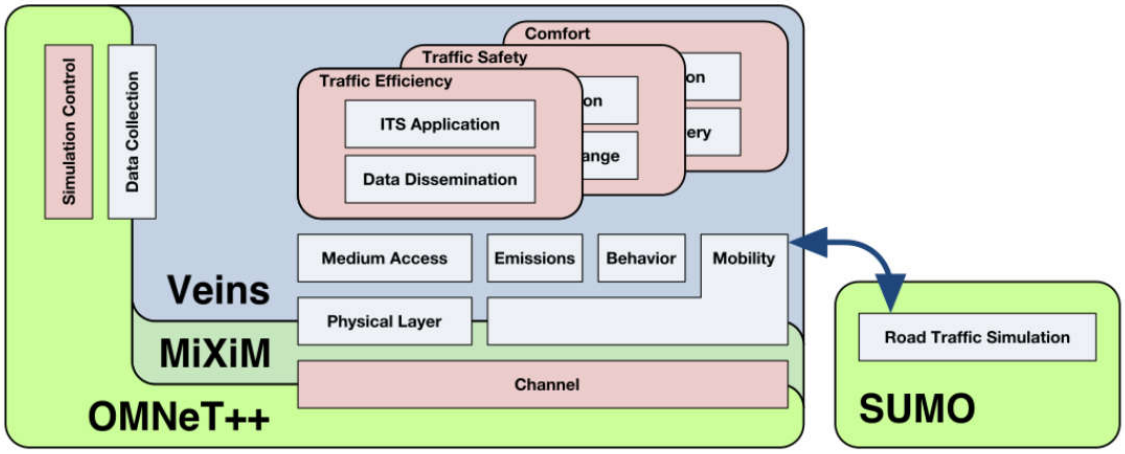

Figure 4. 1: simulation of SUMO and OMNET using VEINS [47]

VEINS also provides excellent support for DSRC/WAVE standard. OpenStreetMap (OSM) [48] is an online repository, which contains real world traffic maps. We have used OSM to import the road networks used in our simulations. In our simulations, vehicle communication is held in two phases; first transmission of broadcast (HELLO) messages and then, transmission of data messages (Request and Reply) after establishing the connection with CH and CMs.

4.1 Simulation Setup

We set up the simulation by running SUMO version 0.32, OMNET++5.5 and VEINS version 4.7.1. The very first step of VANET simulation is the creation of real world map. We downloaded the map from OSM by using coordinates (-84.836040, 42.418759, -84.659617, 42.495445). The map represents an area of 7000m x 5000m.

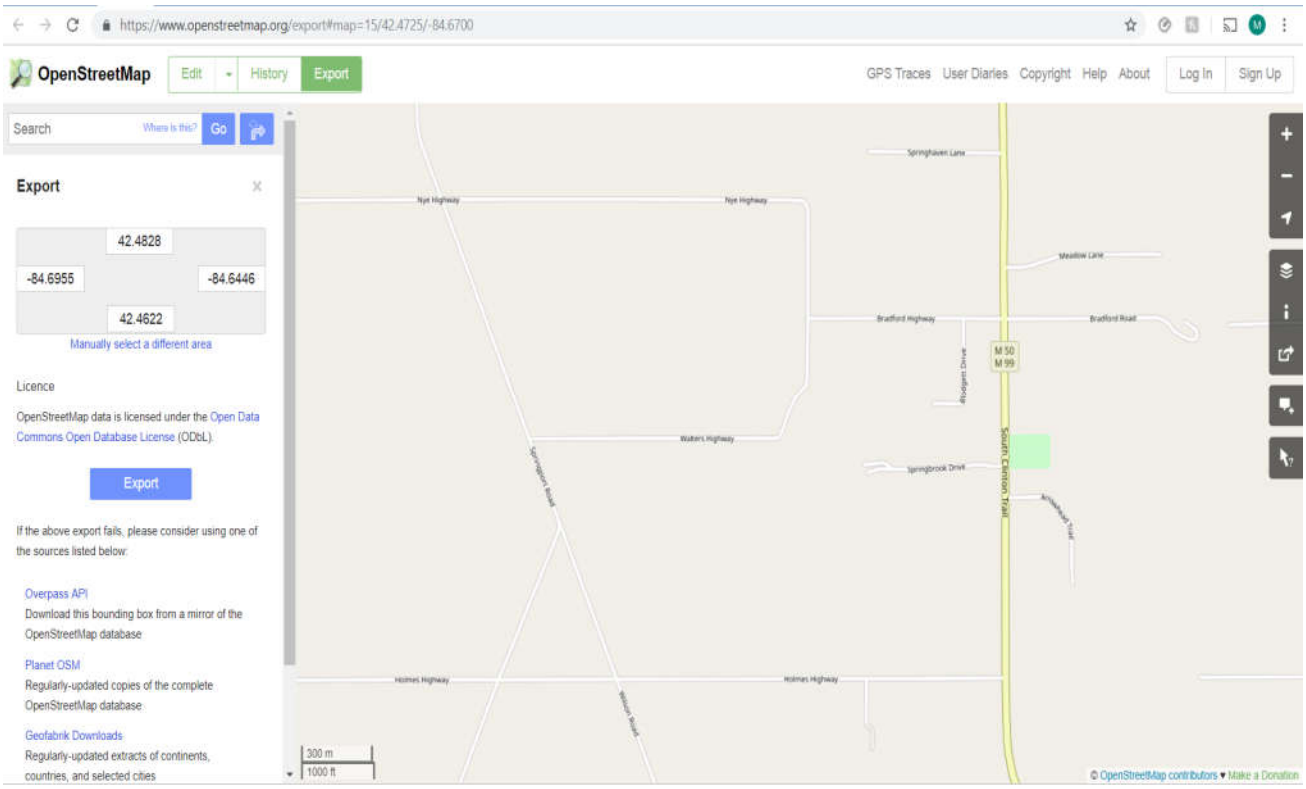

Figure 4. 2: .osm *file of real world map downloaded from OSM [48]*

The extension of downloaded map is *.osm,* which is shown in Figure 4.2. In the next step, we use *.osm* file to generate *(.net.xml, .rou.xml, .poly.xml*) to feed SUMO to generate sumo.cfg file. The traces of SUMO traffic model file are given in Figure 4.3.

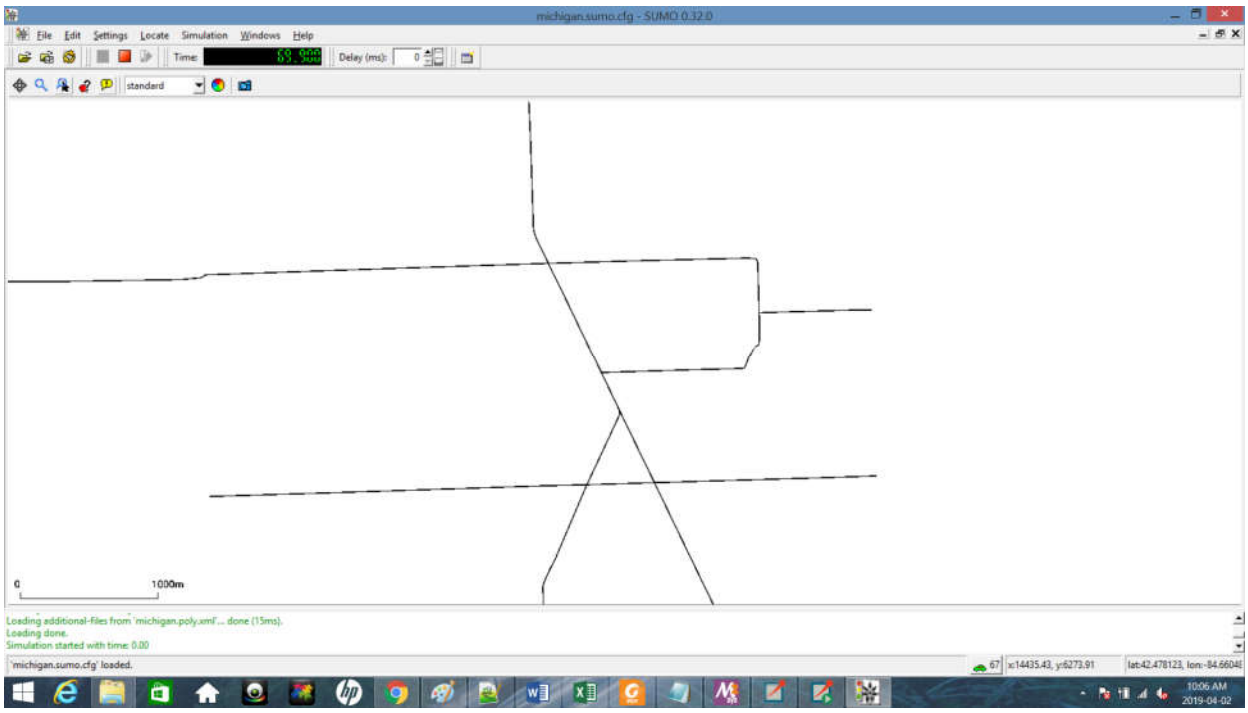

Figure 4. 3: .sumo.cfg *traffic model configuration file*

We consider the following attributes while generating the SUMO configuration file:

- Two way traffic with single lane on both sides of the road.
- Maximum Speed of a vehicle is 40km/h.
- Node generation interval is 1 sec.
- Addition of vehicle is random based on the available space in any lane.

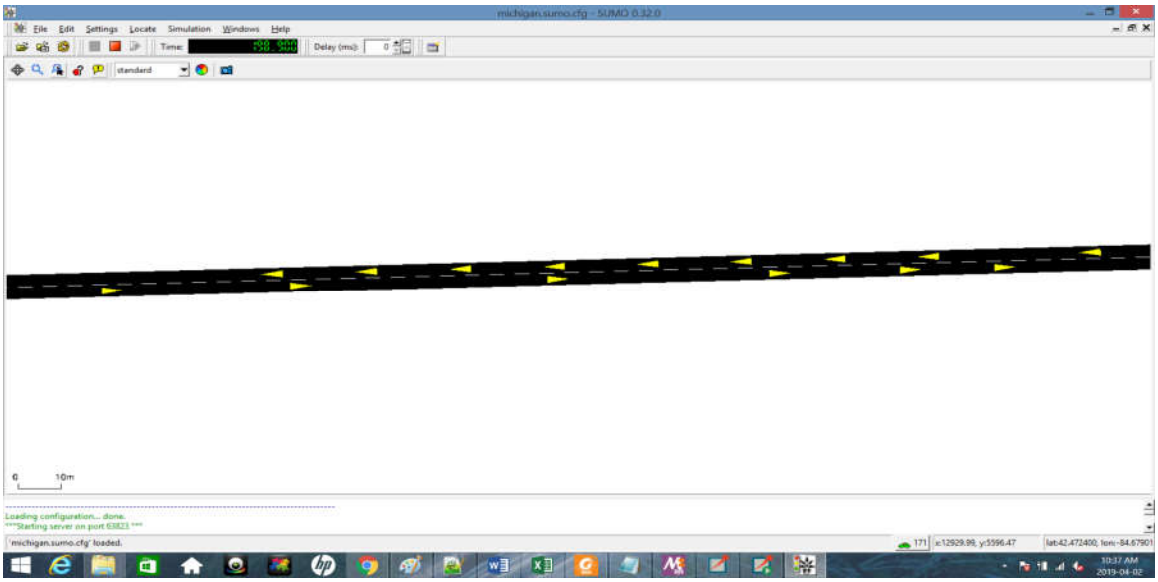

Figure 4. 4: SUMO road structure with nodes

Figure 4.4 displays the road structure with nodes in SUMO traffic model.

The following parameters in OMNET++ are used in our simulation:

Table 4. 1: Table of parameters used in simulation

Parameters	Value
Simulation Time	300 sec
Data Rate	6Mbps
Message Size	144 bytes
Transmission Power	20mW
Thermal Noise	-110dBm
Sensitivity	-89dBm
Transmission Rate	10Hz
Maximum number of vehicles	200
Number of RSUs	2

4.2 Simulation Results

The results reported in this section are based on the average of three simulation runs. We compare the results of our approach given in Sec. 3.4 (*Proposed*) with following existing approaches:

- Cluster Based Life-Time Routing Protocol CBLTR (*LT Based* [3])
- Random Selection of CH (*Random*)

We considered the following QoS metrics to evaluate the performance of our algorithm:

- End to End Packet Delay
- Throughput
- Packet Delivery Ratio (PDR)
- Number of Clusters

4.2.1 Number of Packets Generated

Figure 4.5 shows the number of packets generated in each simulation scenario. We see that for each scenario, the number of packets generated by all 3 approaches is the same. However, the number of packets increase consistently as the vehicle density increases.

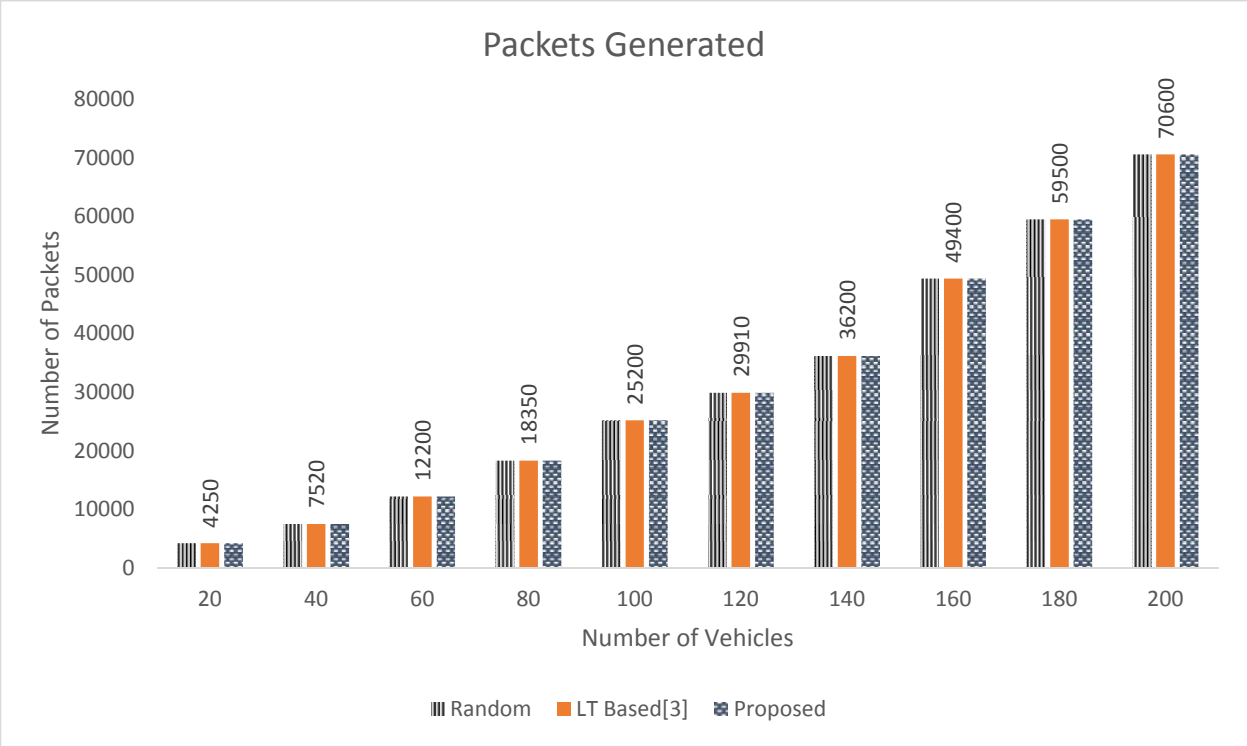

Figure 4. 5: Packets Generated in all three scenarios

4.2.2 End To End Delay

The End to End Delay of transmitted packets is defined as the difference between the reception time of the packet at the destination node and the transmission time of a packet at the sending node. It is computed as follows [26]:

$$\text{Delay} = \sum_{i=1}^{n_p} (T_{reci} - T_{sendi})/n_p$$

Here n_p represents number of packets, T_{reci} and T_{sendi} denote receiving and sending time of a packet i, respectively. The delay was calculated for different vehicle densities, ranging form 20 to 200 vehicles.

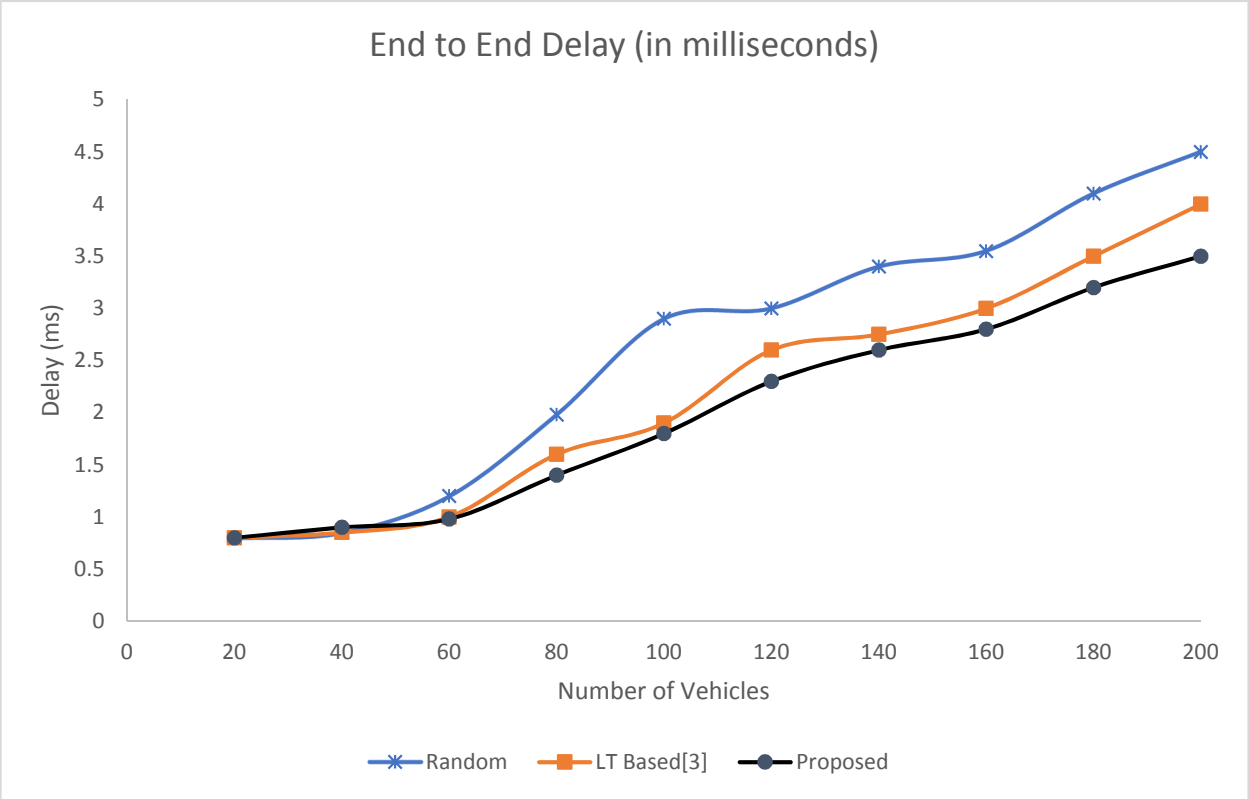

Figure 4. 6: End to End Packet Delay

As we can see in Figure 4.6, for 1 to 40 vehicles, the performances of all approaches are very close. This could be because of less number of packets transmitted by nodes. From nodes 40 to 200, the proposed algorithm had lower delay. The reason of getting better result is the position factor of a node. Since we are giving more weight to position of a node in the cluster, it means that packet will travel more distance towards its destination. Hence it can reduce the overall delay [26]. We can notice that delay factor increases with the increase in number of nodes, because nodes can exchange more messages and hence, can face more congestion.

4.2.3 Throughput

Throughput is another metric to analyze performance of proposed algorithm. Throughput is computed as the number of bits transmitted per second. It should be higher in a network to obtain improved QoS performance. It can be expressed mathematically as follows [26]:

$$\text{Throughput} = (n_r \times s_p)/T_d$$

Here n_r is the total packet received, ns_p is packet size and T_d is the total time (in seconds).

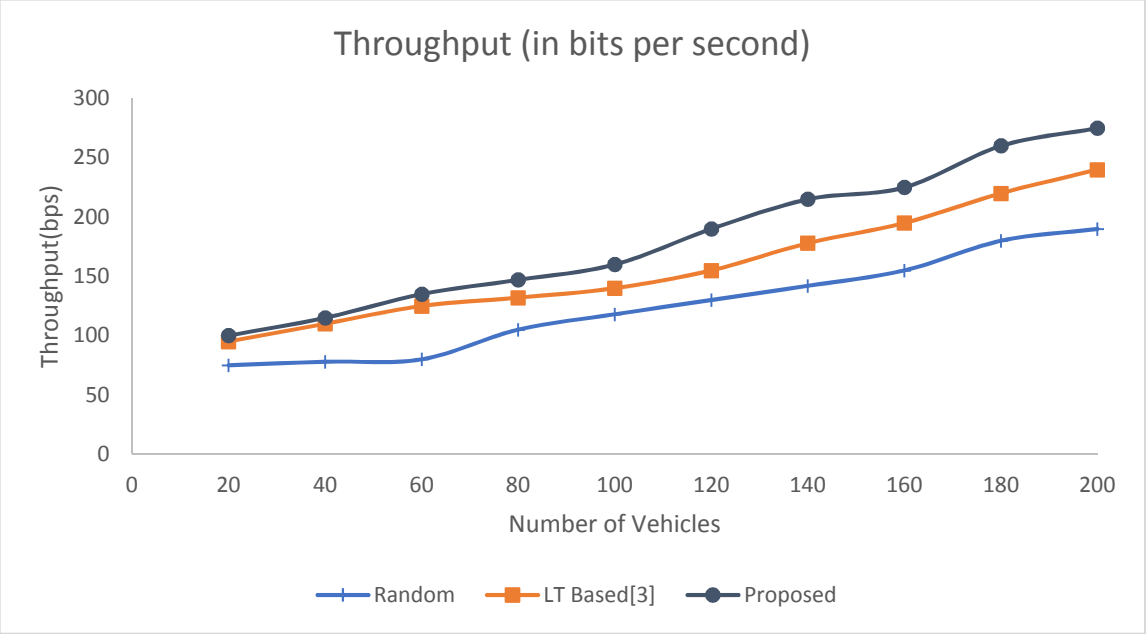

Figure 4. 7: Graph showing the throughput

Figure 4.7 shows the comparison of different approaches with the proposed one. Our proposed algorithm outperformed in terms of throughput because of more transmission of messages among CMs and CH. Throughput increases with increase in number of nodes because of getting more exchange of messages.

4.2.4 Packet Delivery Ratio (PDR)

Another metric to perform analysis of proposed approach is the packet delivery ratio. PDR is the ratio between the total number of packets delivered to that total number of packets received by the node. Greater value of PDR shows the better performance of network. It is calculated as follows [26]:

$$\text{PDR}=[\sum Pkt_{reci}/n] / \sum Pkt_{senti}$$

Here Pkt_{reci} and Pkt_{senti} are packets received and sent by a vehicle I respectively. n denotes the number of nodes.

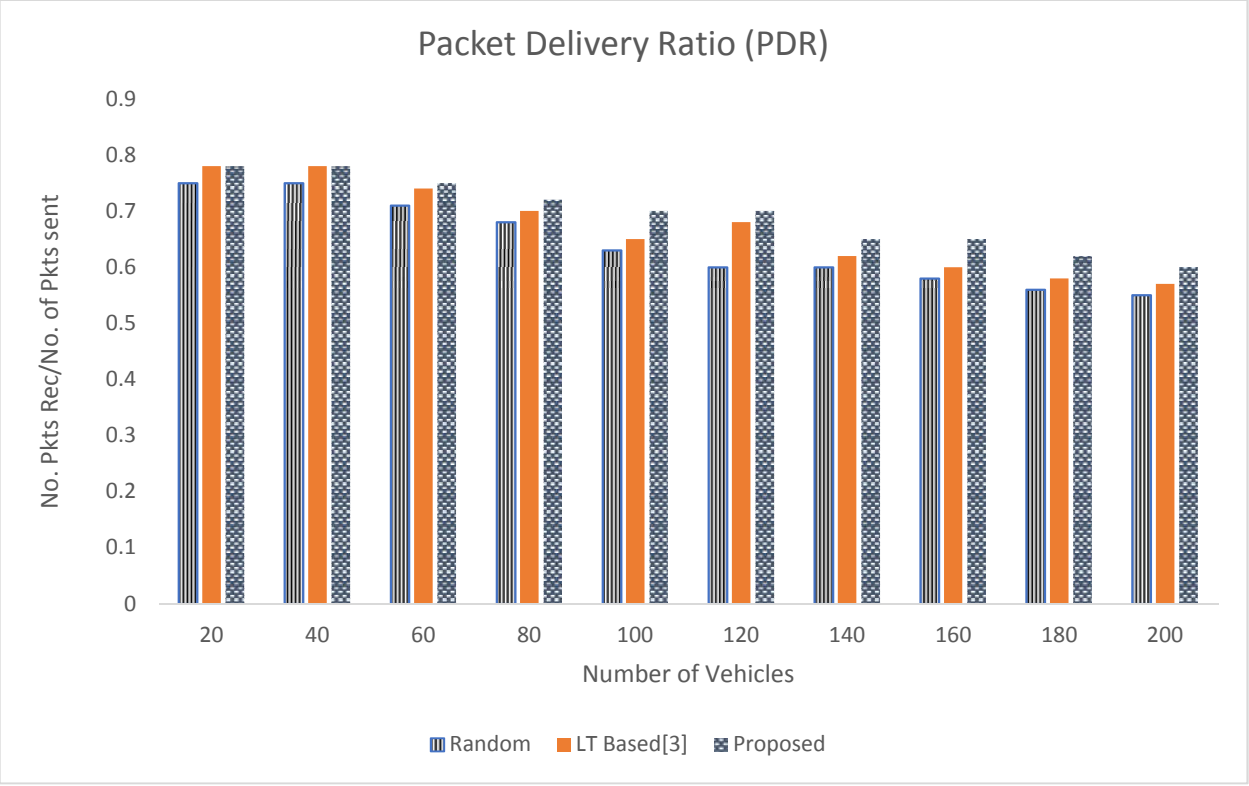

Figure 4. 8: Packet Delivery Ratio (PDR) of different scenarios

Figure 4.8 shows the PDR, where we can see our proposed scheme performed better as compared to other approaches. In other words, our approach has a lower packet loss during the simulation. One possible reason for this is that the connectivity between nodes lasts for a longer time. Average speed factor provides stable connectivity between nodes and vehicles travel at relatively the same speed as the cluster head. PDR decreases with the increase in number of vehicles, because of channel congestion so nodes face more packet loss.

4.2.5 Number of Clusters

We also compared the number of clusters formed as compared to other approaches in literature.

Table 4. 2: Comparison of number of clusters

Technique	**Transmission Range**	**No. of Clusters**
CBLTR [3]	1000 m	4
CLPSO [11]	600 m	25
CACONET [12]	600 m	20
Proposed	600 m	4

It can be seen in Table 4.1 that our proposed approach has the same number of clusters as CBLTR [3] but has less number of clusters as compared to other approaches. Fixed cluster approach can generate relatively fewer clusters, as shown in this work.

CHAPTER 5

CONCLUSION AND FUTURE WORK

5.1 Conclusion

Vehicular Ad Hoc Networks (VANETs) are expected to support variety of applications for driver assistance, traffic efficiency and road safety. In this thesis, we have proposed an authenticated clustering technique based on fixed clusters. Authentication plays a major role in VANET for providing secured communication among vehicles. We implemented vehicle to vehicle (V2V), cluster head to road side unit and road side unit to trusted authority authentication for the clustered network.

We also presented a heuristic algorithm for selecting a suitable vehicle as the cluster head in a cluster. For the election of head vehicle, we used a weighted fitness values based on three parameters; trust value, position from the cluster boundary and absolute relative average speed. Our goal was to select CH in an efficient way, which can increase the QoS metrics like delay, throughput and PDR. We tested our approach against random selection of CH and other approaches available in the literature. Our simulation results indicate that the proposed approach resulted in more reliable transmissions and stable clusters.

5.2 Future Work

In this thesis, we have presented a new approach for cluster head selection in VANET. The initial investigations have yielded some promising results. In this section, we identify some directions for future research that can be carried out to extend our work, as follows:

1. We implemented our work under single lane scenario. It can be further enhanced in future under multi-lane scenario.
2. Our work is based on single straight road. It can be improved under road intersection scenario, which is more closer to the real world.
3. This work also needs improvement in terms of highway road type where vehicle speed is more than 100km/h
4. Instead of giving random trust values, we can implement incidence reporting mechanism in simulation, which can assign actual trust values on each incident to the vehicle. Then we can perform analysis on performance of trust value based approach.
5. We considered only single-hop scenario in our approach. In future, it can be improved by considering multi-hop situation in VANET network.
6. We can also develop a routing protocol for this work and compare the performance with existing clustering protocols.
7. Vehicle density can also be considered for future work. We can increase the vehicle density and transmission range in each cluster and compare the result to see the improvement.

References

[1] M. A. Shahid, A. Jaekel, C. Ezeife, Q. Al-Ajmi and I. Saini, "Review of potential security attacks in VANET," *2018 Majan International Conference (MIC)*, Muscat, 2018, pp. 1-4.

[2] Mejri, Mohamed Nidhal, Jalel Ben-Othman, and Mohamed Hamdi. "Survey on VANET security challenges and possible cryptographic solutions." *Vehicular Communications* 1.2 (2014): 53-66.

[3] Abuashour, Ahmad, and Michel Kadoch. "A cluster-based life-time routing protocol in VANET." *2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)*. IEEE, 2016.

[4] Luo, Yuyi, Wei Zhang, and Yangqing Hu. "A new cluster based routing protocol for VANET." *2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing*. Vol. 1. IEEE, 2010.

[5] Vodopivec, Samo, Janez Bešter, and Andrej Kos. "A survey on clustering algorithms for vehicular ad-hoc networks." *2012 35th International Conference on Telecommunications and Signal Processing (TSP)*. IEEE, 2012.

[6] Hasrouny, Hamssa, et al. "Group-based authentication in V2V communications." *2015 Fifth International Conference on Digital Information and Communication Technology and its Applications (DICTAP)*. IEEE, 2015.

[7] Sugumar, Rajendran, Alwar Rengarajan, and Chinnappan Jayakumar. "Trust based authentication technique for cluster based vehicular ad hoc networks (VANET)." *Wireless Networks* 24.2 (2018): 373-382.

[8] Louazani, Ahmed, Sidi Mohammed Senouci, and Mohammed Abderrahmane Bendaoud. "Clustering-based algorithm for connectivity maintenance in vehicular ad-hoc networks." *2014 14th International Conference on Innovations for Community Services (I4CS)*. IEEE, 2014.

[9] Bali, Rasmeet S., Neeraj Kumar, and Joel JPC Rodrigues. "Clustering in vehicular ad hoc networks: taxonomy, challenges and solutions." *Vehicular communications* 1.3 (2014): 134-152.

[10] Jerbi, Moez, et al. "Towards efficient geographic routing in urban vehicular networks." *IEEE Transactions on Vehicular Technology* 58.9 (2009): 5048-5059.

[11] Malik, Aqsa, et al. "QoS in IEEE 802.11-based wireless networks: a contemporary review." *Journal of Network and Computer Applications* 55 (2015): 24-46.

[12] Song, Tao, et al. "A cluster-based directional routing protocol in VANET." *2010 IEEE 12th International Conference on Communication Technology*. IEEE, 2010.

[13] Liu, Jianqi, et al. "A survey on position-based routing for vehicular ad hoc networks." *Telecommunication Systems* 62.1 (2016): 15-30.

[14] R, Megha et. " Clustering Techniques Used in Vehicular Ad-hoc Network A Survey." *INTERNATIONAL JOURNAL OF COMPUTER SCIENCES AND ENGINEERING* (2018): 141-145

[15] Vijayakumar, Pandi, et al. "Computationally efficient privacy preserving authentication and key distribution techniques for vehicular ad hoc networks." *cluster computing* 20.3 (2017): 2439-2450.

[16] Thandil, Rizwana Kallooravi. "Security and Privacy in Vehicular Ad Hoc Network (VANET): A Survey." *International Journal of Computer Applications* 975 (2015): 8887.

[17] Harding, John, et al. *Vehicle-to-vehicle communications: readiness of V2V technology for application*. No. DOT HS 812 014. United States. National Highway Traffic Safety Administration, 2014.

[18] Jawandhiya, Pradip M., et al. "A survey of mobile ad hoc network attacks." *International Journal of Engineering Science and Technology* 2.9 (2010): 4063-4071.

[19] Fahad, Muhammad, et al. "Implementation of evolutionary algorithms in vehicular ad-hoc network for cluster optimization." *2017 Intelligent Systems Conference (IntelliSys)*. IEEE, 2017.

[20] Rawashdeh, Zaydoun Y., and Syed Masud Mahmud. "A novel algorithm to form stable clusters in vehicular ad hoc networks on highways." *EURASIP Journal on Wireless Communications and Networking* 2012.1 (2012): 15.

[21] Aadil, Farhan, et al. "CACONET: ant colony optimization (ACO) based clustering algorithm for VANET." *PloS one* 11.5 (2016): e0154080.

[22] Lang, Ulrich, and Rudolf Schreiner. "Managing security in intelligent transport systems." *2015 IEEE 18th International Conference on Intelligent Transportation Systems*. IEEE, 2015.

[23] Aadil, Farhan, Shahzad Rizwan, and Adeel Akram. "Vehicular Ad Hoc Networks (VANETs), Past Present and Future: A survey." (2011).

[24] Salhi, Ismail, Mohamed Cherif, and S. Senouci. "Data collection in vehicular networks." *Proc. ASN symposium*. 2007.

[25] Fan, Wei, et al. "A mobility metrics based dynamic clustering algorithm for VANETs." (2011): 752-756.

[26] Wazid, Mohammad, et al. "Design of lightweight authentication and key agreement protocol for vehicular ad hoc networks." *IEEE Access* 5 (2017): 14966-14980.

[27] Maslekar, Nitin, et al. "Modified C-DRIVE: Clustering based on direction in vehicular environment." *2011 IEEE Intelligent Vehicles Symposium (IV)*. IEEE, 2011.

[28] Al-Kharasani, Nori, et al. "An efficient framework model for optimizing routing performance in VANETs." *Sensors* 18.2 (2018): 597.

[29] Santos, R. A., R. M. Edwards, and A. Edwards. "Cluster-based location routing algorithm for vehicle to vehicle communication." *Proceedings. 2004 IEEE Radio and Wireless Conference (IEEE Cat. No. 04TH8746)*. IEEE, 2004.

[30] Kachitvichyanukul, Voratas. "Comparison of three evolutionary algorithms: GA, PSO, and DE." *Industrial Engineering and Management Systems* 11.3 (2012): 215-223.

[31] Ahammed, Farhan, Javid Taheri, and Albert Zomaya. "LICA: robust localization using cluster analysis to improve GPS coordinates." *Proceedings of the first ACM international symposium on Design and analysis of intelligent vehicular networks and applications*. ACM, 2011.

[32] Perkins, Charles, Elizabeth Belding-Royer, and Samir Das. *Ad hoc on-demand distance vector (AODV) routing*. No. RFC 3561. 2003.

[33] Chiti, Francesco, et al. "Context aware clustering in VANETs: A game theoretic perspective." *2015 IEEE International Conference on Communications (ICC)*. IEEE, 2015.

[34] Jenefa, J., and EA Mary Anita. "Secure Vehicular Communication Using ID Based Signature Scheme." *Wireless Personal Communications* 98.1 (2018): 1383-1411.

[35] Mohammad, S. Almalag, and C. Weigle Michele. "Using traffic flow for cluster formation in vehicular ad-hoc networks." *IEEE Local Computer Network Conference*. IEEE, 2010.

[36] Fan, Peng. "Improving broadcasting performance by clustering with stability for inter-vehicle communication." *2007 IEEE 65th Vehicular Technology Conference-VTC2007-Spring*. IEEE, 2007.

[37] Zimmer, Michael T. "Personal information and the design of vehicle safety communication technologies: An application of privacy as contextual integrity." *Proceedings of AAAS Science & Technology in Society* (2005): 222-226.

[38] Yin, Jijun, et al. "Performance evaluation of safety applications over DSRC vehicular ad hoc networks." *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*. ACM, 2004.

[39] Wang, Zhigang, et al. "A position-based clustering technique for ad hoc intervehicle communication." *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)* 38.2 (2008): 201-208.

[40] Chen, Xianbo, Hazem H. Refai, and Xiaomin Ma. "A quantitative approach to evaluate DSRC highway inter-vehicle safety communication." *IEEE GLOBECOM 2007-IEEE Global Telecommunications Conference*. IEEE, 2007.

[41] Cooper, Craig, et al. "A comparative survey of VANET clustering techniques." *IEEE Communications Surveys & Tutorials* 19.1 (2017): 657-681.

[42] Yan, Gongjun, et al. "WEHealth: A secure and privacy preserving eHealth using NOTICE." *Proceedings of the International Conference on Wireless Access in Vehicular Environments (WAVE), Dearborn, MI, USA*. Vol. 89. 2008.

[43] Cheng, Xiaolu, and Baohua Huang. "A Center-Based Secure and Stable Clustering Algorithm for VANETs on Highways." *Wireless Communications and Mobile Computing* 2019 (2019).

[44] IEEE Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments," in *IEEE Std 802.11p-2010 (Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k-2008, IEEE Std 802.11r-2008, IEEE Std 802.11y-2008, IEEE Std 802.11n-2009, and IEEE Std 802.11w-2009)* , vol., no., pp.1-51, 15 July 2010.

[45] SUMO-Simulation of Urban Mobility. (2019).

Retrieved from https://sumo.dlr.de/index.html (last accessed on March 28, 2019)

[46] Veins. (2019). Retrieved from https://veins.car2x.org/ (last accessed on March 28, 2019)

[47] OMNeT++ Discrete Event Simulator. (2019). Retrieved from https://omnetpp.org/ (last accessed on March 28, 2019)

[48] OpenStreetMap. (2019). Retrieved from https://www.openstreetmap.org/ (last accessed on March 28, 2019)

Vita Auctoris

Anwar Shahid completed his Master in Computer Science (course based) in 2004 and Masters in Educational Assessment in 2006. He completed these degrees from University of Punjab, Pakistan. He also has Bachelors of Education (B-Ed) degree earned from University of Punjab, Pakistan. He worked as Data Analyst and a teacher for more than 7 years. Currently he is serving as a Mentor to a robotics team for First Robotics Canada (FRC).