ANONYMITY ASSURANCE USING EFFICINET PSEUDONYM CONSUMPTION IN INTERNET OF VEHICLES

By

MEHREEN MUSHTAQ

NATIONAL UNIVERSITY OF MODERN LANGUAGES

ISLAMABAD

JULY, 2022

Anonymity Assurance using Efficient Pseudonym Consumption in Internet of Vehicles

By

Mehreen Mushtaq

MSCS, National University of Modern Languages, Islamabad,

A THESIS SUBMITTED IN PARTIAL FULFILMENT OF

THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE
In **Computer Science**

To
FACULTY OF ENGINEERING & COMPUTER SCIENCE

NATIONAL UNIVERSITY OF MODERN LANGUAGES ISLAMABAD

NATIONAL UNIVERSITY OF MODERN LANGUAGES

FACULTY OF ENGINEERING AND COMPUTER SCIENCE

THESIS AND DEFENSE APPROVAL FORM

The undersigned certify that they have read the following thesis, examined the defense, are satisfied with overall exam performance, and recommend the thesis to the Faculty of Engineering and Computer Sciences for acceptance.

Thesis Title: Anonymity Assurance using Efficient Pseudonym Consumption in Internet of Vehicles

Submitted By: Mehreen Mushtaq **Registration #:** 38 MS/CS/F20

Master of Science in Computer Science (MSCS)
Title of the Degree

Computer Science
Name of Discipline

Dr. Ata Ullah _____
Name of Research Supervisor Signature of Research Supervisor

Dr. Basit Shahzad _____
Name of Dean (FE&CS) Signature of Dean (FE&CS)

_____ _____
Name of Pro-Rector Academics Signature of Pro-Rector Academics

AUTHOR'S DECLARATION

I Mehreen Mushtaq

Daughter of Muhammad Mushtaq

Registration # 38 MS/CS/F20

Discipline Computer Science

Candidate of **Master of Science in Computer Science (MSCS)** at the National University of Modern Languages do hereby declare that the thesis **Anonymity Assurance using Efficient Pseudonym Consumption in Internet of Vehicles** submitted by me in partial fulfillment of MSCS degree, is my original work, and has not been submitted or published earlier. I also solemnly declare that it shall not, in future, be submitted by me for obtaining any other degree from this or any other university or institution. I also understand that if evidence of plagiarism is found in my thesis/dissertation at any stage, even after the award of a degree, the work may be cancelled and the degree revoked.

_____
Signature of Candidate

Mehreen Mushtaq
Name of Candidate

_____
Date

ABSTRACT

Internet of vehicles (Iov) is an emerging technology that allows vehicles to travel while communicating with other vehicles, pedestrians, OBU, cloud and RSU. This intelligent transport system (ITS) has increased road safety while road accidents have decreased to a large extent. Through vehicles communication, surrounding vehicles get information about each other's location, position and velocity to avoid accidents and road congestion. When vehicles travel on roads they share their information with neighbor vehicles through beacon messages that includes their position, speed, acceleration. As this technology is governing, there is a huge security risk that makes the information of vehicles vulnerable. Any adversary after knowing information about vehicles can easily harm vehicles or can use this information for any negative purpose, that's why security of vehicles is an important concern that cannot be neglected. For security purpose, vehicles change their pseudonym, but only frequently changing pseudonym is not enough because an attacker can link previous pseudonym with new one to get information. To resolve security issues and enhance vehicles anonymity there are many techniques to change pseudonym efficiently but some of them have high pseudonym consumption like Cooperative pseudonym change scheme based on number of neighbors (CPN) and WHISPER. High pseudonym consumption has bad impact upon performance of system and it also disturbs Qos because pseudonym needs high system overhead and memory it also needs that these pseudonym should be authenticated by certificate authority (CA). The proposed solution EPCP has low pseudonym consumption and reduces traceability ratio to maintain anonymity of vehicles. To check the effectiveness of proposed scheme EPCP, OMNet 5.0++, SUMO 0.25.0 and PREXT are used that was built upon Veins 4.4 version. The results showed that proposed scheme EPCP is better in consuming resources and providing protection against adversary attacks.

TABLE OF CONTENT

LIST OF TABLES

TABLE NO. **TITLE** ` **PAGE**

LIST OF FIGURES

Figure **TITLE** **Page No.**

LIST OF ABBREVIATIONS

VANET	Vehicular Ad-hoc Network
ITS	Intelligent Transport System
V2V	Vehicle to Vehicle
V2I	Vehicle to Infrastructure
V2X	Vehicle to Everyone
BSM	Basic Safety Message
IOV	Internet of Vehicles
CAM	Cooperation Awareness Mechanism
RSU	Road side Unit
TA	Trusted Authority
OBU	Onboard Unit
QoS	Quality of Services
CPN	Cooperative Pseudonym Change
DSRC	Dedicated short range communication
LBS	Location Based Services
RNS	Request New Pseudonym
CS	Control Servers
GID	Group Identity
GH	Group head
PID	Pseudonym Identity
VID	Vehicle identity
PU	Pseudonym Update
CS	Control Server
AS	Anonymity Set
GPA	Global Passive attacker
CA	Control Authority
DDOS	Distributed Denial of Service
GL	Group Leader
GPS	Global Positioning System

EPCP	Efficient Pseudonym Consumption Protocol
PREXT	Privacy Extension
SUMO	Simulation of Urban Mobility
OMNet++	Objective Modular Network Testbed in C++
GH	Group Head

LIST OF SYMBOLS

α	adaptive beaconing rate
μ	Friction coefficient between road and tires
g	gravitational force of earth
Γs	threshold vehicles
Γt	threshold time
Ψi	set of neighbor vehicles of v_i,
T_0	initiator vehicle
τv	traceability time of vehicle v
L(v)	lifetime of v
S_{th}	speed threshold

ACKNOWLEDGMENT

First of all, I wish to express my gratitude and deep appreciation to Almighty Allah, who made this study possible and successful. This study would not be accomplished unless the honest espousal that was extended from several sources for which I would like to express my sincere thankfulness and gratitude. Yet, there were significant contributors for my attained success and I cannot forget their input, especially my research supervisor, Associate Prof. Dr. Ata Ullah who did not leave any stone unturned to guide me during my research journey.

I shall also acknowledge the extended assistance from the administrations of Department of Computer Sciences who supported me all through my research experience and simplified the challenges I faced. For all whom I did not mention but I shall not neglect their significant contribution, thanks for everything.

This thesis work is dedicated to my parents and my teachers throughout my education career who have not only motivated me unconditionally but whose good examples have taught me to work hard for the things that I aspire to achieve.

CHAPTER 1

INTRODUCTION

1.1 Overview

In this chapter, firstly VANET is discussed with its communication types, then internet of vehicles is deliberated along with its architecture, applications as well as its limitations. After it, problem background, its bad impact on intelligent transport system is mentioned and then problem scenario is explained. Then, research objectives are described afterwards aim of research and research questions are stated. After it, scope of research objectives is described. Finally, organization of theses is explained.

1.1.1 Vehicular Ad-hoc network

Vehicular Ad-hoc network is also known as network of vehicles in which vehicles travel by communicating with other vehicles as well as infrastructure. VANET is a sub-category of Mobile Ad-hoc Network (MANET) in which mobile nodes communicate with each other without any fixed AP (access point). The word VANET is introduced by 2001[1], as an application of Mobile Ad-hoc Network. As technology prospers, it also brings revolution in field of transport system and promises to make intelligent transport system ITS possible. Due to vast advantages, the technology is increasing rapidly. It is estimated that in 2020, up to 250 million vehicles are connected to VANET [2] and estimated that most vehicles moves to intelligent paradigm till now are up to 1 billion while this number increases to 2 billion at the end of 2035 [3]–[5]. In a report published by WHO (world health organization), it is stated that road accidents is a major reason of

death and loss of life[6][7], so to reduce the chances of this loss, VANET introduced in transport that reduced ratio of accidents remarkably by warning drivers at appropriate time [8].

Due to road safety and accident avoidance, vehicles communicate with each other. VANET basically supports communication that are Vehicle to vehicle (V2V) , Vehicle to Road side unit (V2R) and Vehicle to infrastructure (V2I) [8]–[10]. In vehicle to vehicle communication beacon message is exchanged among vehicles to inform each other about situation of road and traffic density while in vehicle to infrastructure communication allows vehicles to connect to internet and take services while in vehicle to Roadside unit communication, vehicles communicate with RSU in order to know about situation of roads and unfortunately if any accident occurs, RSU timely inform to vehicles in its range about it, so they may take alternative route at time[2], [10]–[12]. This communication feature has increased reliable driving services to its users.

In VANET, the communication is carried out by WAVE between vehicles or among vehicles and RSU. All communication for road safety is done through this protocol, system modules majorly contain OBU, AU and RSU. Each vehicle is equipped with OBU (Onboard Unit) and sensors. The functions of sensors and OBU to inform about road situation as well as hurdles on road. For inter-communication among vehicles or for inter-communication, OBU plays an important role. AU, a dedicated device is installed on vehicles to assist performing smooth communication over network. RSU devices are mounted on infrastructure or installed on electrical towers in order to globally know about traffic position and inform vehicles in case of any emergency situation. These infrastructure exists on parking areas or along the roadside[2], [3], [8], [9], [11]. VANET architecture with communication scenario is presented in Figure 1.1.

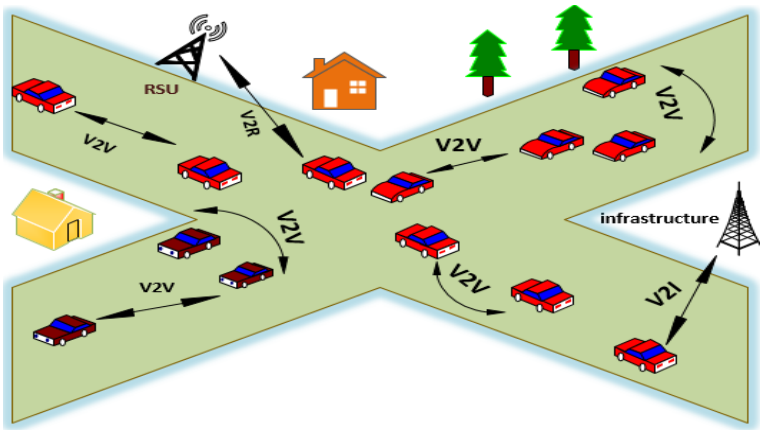

Figure 1.1: VANET architecture along with communication scenario

Vehicles use beacon safety message to transmit information from vehicle to vehicle or to take from infrastructure. These BSM contains precise information to reduce chances of road accidents[2], [13]. As this technology is spreading very fast, VANET is not enough to accommodate it because it only supports limited type of communication as well as not able to tackle huge data generated by these vehicles which is increasing with passage of time. It also creates problem in compatibility with some gadgets and network services connection is also not much consistent in it. From urban perspective, VANET is not much efficient because in cities traffic jams and road congestion is frequent along with complex, huge buildings are present that affect the performance of VANET. Though from rural point of view, it performs better because of comparatively less complex scenario[3], [12], [14] . These are limitations that exist in VANET and affect its performance, to enhance capabilities of VANET and overcome its problems, an innovative term Internet of Vehicles (IoV) came into being[15].

Internet of Vehicles (IoV) also referred as network of cars, an improvement in VANET that uses concept and principles of VANET and IOT (internet of things), that transmit and receive data from vehicles, RSU, Infrastructure and able to handle it. IoT features make it possible to collect data anywhere, anytime principle and it covers wide range as compared to VANET in order to provide better services[16]. Vehicles communicate with each other by message to inform about its position as well as location. This message is named as BSM (Basic safety Message) or heartbeat

message in United States, CAM (Cooperation Awareness Mechanism) or beacon in Europe[17][18], all communication is done through this. The components of a BSM is shown in Figure 1.2.

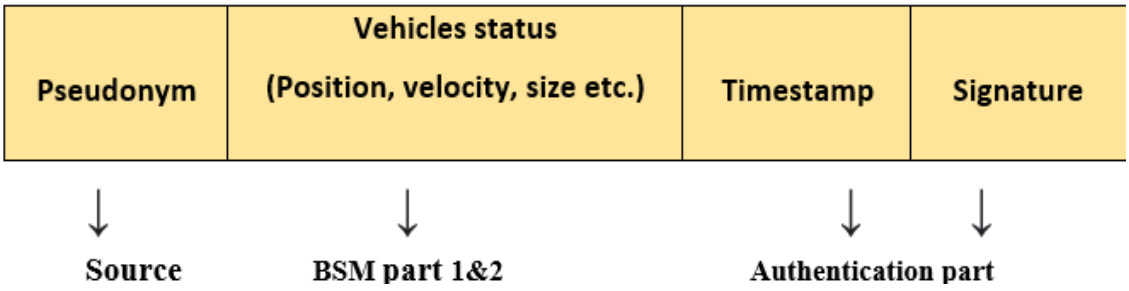

Figure 1.2: Components of BSM

A vehicle can use this information to set their speed according to traffic situation as well as keep an eye of neighboring vehicles speed and a vehicle also able to know about number of neighbors[19][20]. BSM contains sensitive information in plain text form, if an adversary able to eavesdrop BSM, they know each bit of information regarding vehicle, driver as well as passengers. Through beacons, adversary can get information about frequency of a vehicle visiting a place, whereabouts as well as travelling time of vehicle and attacker can use this information for some negative purpose[21], [22]. An adversary can be local or global that is spying information and able to plan either active or passive attack. Local adversary has access to a limited area of VANET whereas global adversary has access to huge or whole portion of VANET[16], [23], [24]. There are different security attacks that an adversary can do to harm other human beings like Sybil attack, Masqueraded attack and some other impersonation attack that can disturb privacy[25]. To maintain privacy and anonymization, vehicles changes its pseudonym. Only one Pseudonym is not enough, rather it is changed after every time t to prevent adversary from tracking vehicles[17]. Although strong adversary can plan pseudonym linking attack even after changing pseudonym. To prevent pseudonym linking attack, strong context or zone should be created in order to increase probability of confusion for an adversary to trace target vehicles[10][19]. For this purpose, a lot of researches has done to maintain vehicles anonymity in addition to avoid adversary attacks.

1.2 Motivation

Privacy of location has its own importance in internet of vehicles (IoV). For maintaining anonymity, vehicles used to change its pseudonym and inform neighbors through BSM. If an active or passive attacker is able to access these pseudonym, that attacker can get complete information of target vehicle. Through this information, he can harm passengers or drivers physically or economically. Though to avoid these attacks several schemes were presented in context of security and anonymity, but all of these have some limitations and cannot fully save vehicles from such attacks. Instead of existing strategies, privacy is still an open issue that requires further research and need of solution that provides better security and confidentiality as well as economical. These are causes that motivates to do research in field of vehicles anonymity in IoV.

1.2.1 Architecture of internet of vehicles

Internet of vehicles supports communication of vehicles with other components for better driving and ensures safe driving[14][21][23]][26]. IOV allows vehicles to communicate with car driver, foot-travelers, infrastructures and cloud. Intra-vehicle communication allows vehicles to communicate with its sensors and OBU in order to keep information about internal condition of vehicles any if any part is faulty, it indicates at time and inform car owner. In Vehicle to vehicles (V2V) communication, a vehicle communicate with its neighbors to share information regarding speed, velocity, acceleration and location for better driving. Vehicle to Pedestrians communication (V2P) is a type of communication between vehicle and persons on road in order to provide them warning about upcoming vehicle to avoid accidents. Vehicle to infrastructure communication known as (V2I) in which vehicles are informed about accidents or warnings given to them in case if any unpleasant incident happens. Vehicle to cloud (V2C) is used to get information or infotainment services from cloud[8], [14], [19], [21], [22], [27]. These communication is collectively known as V2X communication, which is presented in Figure 1.3. Trusted Authority (TA) is part of IoV architecture that is responsible of allocating pseudonym to vehicles, and register all vehicles in network. If later on, any vehicle acts suspiciously, RSU informs Trusted Authority

(TA) and in response TA cancel credentials of that vehicles and inform vehicles by RSU[8], [19], [22].

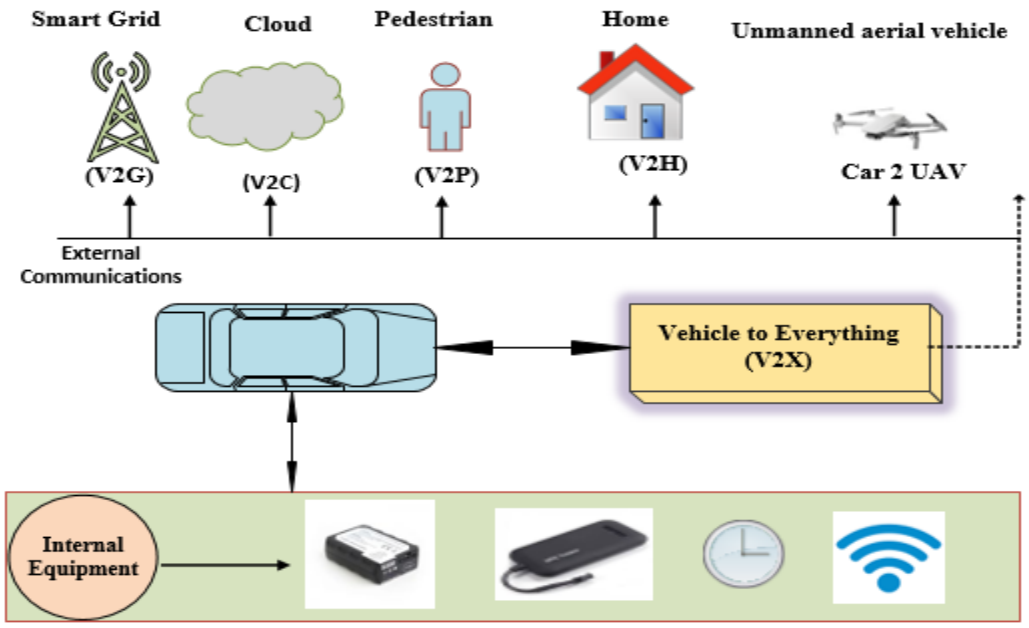

Figure 1.3: Vehicle to Everything (V2X) communication Scenario

The internet of vehicles (IOV) architecture consists of five layers that assist them in maintaining communication and provide infotainment services. These layers are described below:

i) Perception Layer

First layer of internet of vehicles that contains actuators, sensors embedded in vehicle. The responsibility of this layer is to collect data regarding vehicles speed, velocity acceleration and monitor traffic situation. It is also responsible to sense by using sensors vehicles density and warn in case of any danger[3], [7], [9].

ii) Network layer

The function of this layer is to make vehicles visible in a network and transfer lower layer data to artificial intelligence layer. Different components in IOV are using different networks for communication that include 4G/5G/Zigbee/Bluetooth. This layer creates synchronization among these different networks so they can communicate easily[3], [9], [20].

iii) Artificial intelligence Layer

This layer has vital importance in IOV, as it plays main role by taking data from previous layers, analyze it and on its basis it takes critical and important decision regarding shortest destination to reach destination, avoid traffic jam paths[3], [7], [28].

iv) Application layer

This layer provides infotainment services to passengers and decisions taken by AI layer regarding anything is fulfilled by this layer.it also recognizes other vehicles, people or any other hurdle to give directions to brakes, accelerators to take timely actions[3], [7] [12][14].

v) Security layer

This layers has connection with all layers and it function is to maintain vehicles privacy and anonymity in the network. It observes all beacons, if found something malicious it reports this information to Central authority (CA) so they can cancel credentials of malicious node and out them from vehicles network[2], [3], [5], [29].

1.2.2 Applications of internet of vehicles

There are vast applications of Internet of vehicles that has facilitated passengers with comfortable journey and ensures to make ride safe from accidents. For this purpose, vehicles communicate with other vehicles and infrastructure to get notifications and warning on time so to avid tragic incidents to happen[3], [5], [7], [9], [12], [14], [15], [22], [30]. There are a lot of services that IoV is providing which are majorly divided into two classes i) Safety Applications ii)Non Safety Applications

i) Safety-oriented Applications

These applications are relevant to safety of vehicles by timely inform drivers about dangers and possible collisions at time to make journey safe. For this purpose different type of warnings are generated. Cooperation Forward collision is warning that is generated to inform driver about possibility of accident due to very low distance from next vehicle. This notification helps driver to slow down its speed to avoid collision[9] [7][30]. Danger Location Notification is garnered to inform drivers about condition of road in case road is not smooth, this notification informs about holes on road in which vehicle can stuck, vehicle transmit this information to other vehicles that are in transmission range sharing same road[20][30]. This notification is much effective in case of rural areas. Pre-crash warning notification is generated in case if accident cannot be prevented so driver can take precautionary measurements to save from serious injuries[10]. Post-crash warning notification generated by victim vehicle to inform other vehicles about accident to avoid rush on that area and other vehicles take alternative route to reach at time on destination[29]. Emergency vehicle signal is used to inform drivers about an emergency vehicle is coming so clear road for that vehicle and emergency vehicle will pass even if red traffic signal is on[3][30].

In-Vehicle Ambert warning is issued by infrastructure to vehicles with the help of RSU, if a suspicious or a vehicle that is involved in some crime is present in the network, this alert is issued to all automobiles that are in proximity of that vehicle except that one, in order to make them

careful. Pedestrian vicinity alert informs driver about pedestrian close to vehicle and can hit by vehicle so avoid this problem, vehicle need to slow down its speed. In smoggy areas, driver cannot see coming vehicles and due to this problem a lot of accidents can occur, in IoV it is notified to vehicles about road density, coming vehicles distance and speed so to avoid accidents. When a vehicle want to change its lane, notification generated that contains density of intended lane, and if changing in lane any danger exist, it is informed through this notification[3][10]. If a non-emergency vehicle ignored traffic signal and passes even if red light is on, then infrastructure issues warning against that vehicle to inform it about situation of road to prevent any unpleasant event[3][29][31].

ii) Non-Safety Applications

Non-safety application involves those services that are relevant to comfort and providing entertainment to passengers and drivers. Some of these applications require high internet bandwidth in order to work smoothly[7][9]. If a driver is travelling to a new city, he may not exactly know about path or the best hotels that provide good services to passengers. Non-safety applications provides this service by displaying best hotels and shortest safe to travel[7]. If driver needs to park vehicle in parking area, through navigation service he can find nearest vacant parking area[9]. When vehicle passes through Malls, by advertising facility he can get updates about latest sales and variety available in Marts, Malls etc. at toll plaza, there is huge rush of vehicles that waste time and increase frustration, to prevent this IoV provides facility of E-toll payment. Through it, vehicles passing through E-tolls are scanned and receipt is generated with payment amount and collection place is printed on it[12] [29].

To provide entertainment, online gaming and facility of video streaming is also available but it requires high bandwidth to play without buffering. Intersection of road information is managed intelligently to prevent road congestion[3]. In case of emergency or health issue, nearest hospital information is provided to vehicles so patient can get medical aid as soon as possible

Passengers can send E-mail, use internet[30] and enjoy songs easily. Drivers can get weather updates as well, map of traveling place can also be downloaded to reach any new area[3][15].

1.2.3 Constraints of internet of vehicles

IoV is an emerging term that has a lot of benefits which cannot be neglected, although it performs well but there are some areas in Iov that not fully explored till now and need further research to eliminate existing vulnerabilities. Some of these constraints are discussed below:

i) Security issue

For safety purpose, vehicles communicate with each other to inform about location, all this information is in plain text which if an attacker get access of it, all information will be leaked and prove harmful for drivers and passengers. Many researches are done like silent period, mix zone and mix context, but all of them are not enough to completely eliminate these attacks, these attack are passive, active, Sybil, masqueraded, DDOS attack. Security and privacy cannot be neglected so there is need of further research and such schemes that fully resolve this issue[15][3][22].

ii) Lack of Location precision

Existing GPS localization is not enough to fulfill precision requirements that are needed in internet of vehicle environment. GPS provides accuracy of an object maximum at 5m while vehicular environment needs accuracy of more than that. Another issue is that GPS performance worst in case if vehicle is passing from tunnel or underpass. GPS performance also decline in case of urban area because of the presence of complex buildings[3].

iii) High dynamic network structure

In internet of vehicles, each vehicle has its own speed, acceleration and velocity. Some vehicles are moving fast, some are medium and some are slow. There is always uncertainty about vehicles speed it varies. Therefore, topology of IoV is much dynamic that changes frequently. So defining a constant routing algorithm is not possible. Though different routing protocols are available but each has some limitations. There is need of such protocol that able to send data from source to destination without compromising on QoS and prevents delay and packet loss to increase road safety. Till now, no such robust protocol is present that follows all these parameters[22][28].

iv) Computation overhead

The aim of IoV to incorporate multiple vehicles and take their data to take important decisions, while in dense traffic vehicles communicate each other and share information, which in result create huge amount of data that is difficult to tackle as it requires additional memory to keep it and analyze. Additional memory requirement, upgrading devices makes technology extra complex and costly to accomplish[1].

v) Fixed Message Dissemination Frequency

Vehicles transmit BSM for providing safety information and about changing pseudonym. This BSM is transmitted with a frequency of 1-10 per second[21], which increases vulnerability ad weaken the security[23]. Majority of anonymity preserving schemes are using this frequency to disseminate beacons, that gives a clue to attacker to plan and perform pseudonym linking attack in order to trace target vehicle.

vi) Enormous Rebroadcast BSM

When vehicle have any safety related information received, that vehicle send it to neighbors that are in transmission range. Many other vehicles send it again to that vehicles that received this beacon already, which creates a storm of BSM that badly degrades QoS and possibility of packet loss and received delay ratio increases[15][20].

1.3 Problem background

Basic safety message (BSM) is basically used for giving information about vehicle's speed, location by using current pseudonym. Vehicles send and receive BSM and changes pseudonym cooperatively. This cooperation is useful in order to confuse adversary. BSM are commonly sent in range of 300m, while with frequency of 1-10 Hz. Before vehicle v transmit BSM, it waits for some time (known as beacon interval time), after it transmit BSM to neighbors.

In WHISPER[21], vehicle v adjust its transmission range after receiving BSM. For adjustment of transmission range and sending BSM to neighbor vehicles, only speed is considered. This parameter is not enough to send BSM, neighbors number or estimated next position should also need to consider, so that chances of adversary accessing this BSM becomes reduced. Privacy issue is not catered efficiently in this issue and can have bad impact on anonymity in following ways.

1.3.1 Bad effects of problem

i) Maximum Pseudonym consumption

Pseudonym is pair of public and private key. Public key is used as pseudonym whereas private key is used for verification. These pseudonym is generated by Trusted Authority (TA) and at the time of vehicles registration, these pseudonym is allocated to them. When vehicles communicate with each other, they used these pseudonym instead of real identity to avoid security risks. Vehicles tend to change pseudonym instead of keeping only one at a time to avoid linkability between pseudonym and real id. This connection is only familiar to TA. When BSM is received by irrelevant vehicles[21], they also changes pseudonym which in result increases pseudonym consumption. A vehicle have pool of allocated pseudonyms that will finish soon and they demand new set from TA through RSU that increases communication overhead as well. Pseudonym consumption is essential component and needed to be managed efficiently.

ii) High Packet loss

Vehicles have limited memory to store BSM, when vehicles receives BSM from irrelevant vehicles frequently it may happen that those BSM occupied limited memory of vehicles and important message from relevant vehicle is not received by vehicle v [21] so there is high possibility that relevant vehicle's BSM have some safety information regarding accident and due to memory capacity is full, it is not received by vehicle v at appropriate time. If vehicles storage capacity is full for long time that many important message may get dropped or may receive delay when there is no use of that message.

1.4 Problem Identification

For safety purpose, vehicles communicate to each other and inform about current location, and current pseudonym to other vehicles. All this information is disseminated by BSM (Basic Safety Message). Through BSM, vehicles decide where to change its pseudonym. If an adversary can access BSM it can cause serious security threats and harm users. To solve this issue, many solution are presented. These schemes are not enough to completely prevent passive or active

attacks. As in WHISPER[21], this technique does not consider actual distance with neighbors but only observe vehicles speed before sending BSM. Only this parameter is not enough to consider before transmitting BSM. In internet of vehicles (IoV), the topology of network is very dynamic because each vehicle moves with different speed and follow different routes so it may happen that number of vehicles that was neighbor for some time are no more neighbors of each other due to large distance but they are still receiving beacon that has bad impact on Qos and increases pseudonym consumption of vehicles. This situation also disturb anonymity of vehicles and adversary can able to know the location of target vehicle and can threaten drivers or passengers.

1.5 Research Questions

The main research questions of our work based on research objectives enumerated are as follows:

- What are impacts of high pseudonym consumption?
- What are possible ways to reduce adversary attacks as compared to previous schemes?
- How to diminish attacker's traceability in order to increase vehicles anonymity?

1.6 Aim of Research

This research aims to develop a solution that considers relevant vehicles before disseminating BSM, which helps to minimize pseudonym consumption, maintain QoS by reducing the probability of packet loss. When BSM is sent to vehicles that are in transmission, it help to overcome target vehicle's traceability and enhance anonymity of vehicles.

1.7 Research objectives

The defined research objectives of our work are mentioned below:

- To develop a strategy that minimizes pseudonym consumption.
- To ensure that BSM is transmitted to closest vehicles to lessen adversary attacks.
- To enhance vehicles anonymity by decreasing traceability.

1.8 Scope of Research

This study focuses on enhancing vehicles anonymity with minimum pseudonym consumption as well as reducing traceability rate. The scope of study is restricted only to vehicles that are connected to IoV system. Furthermore, this research only considers security threats by adversary planned by using antennas to eavesdrop BSM from area of interest but does not cater the situation in which adversary tries to follow the target vehicle in person.

1.9 Thesis organization

The remaining thesis is organized as follows: Chapter 2 describes existing schemes based on pseudonym change, their comparison and major problems of this area as well as research gap. Chapter 3 presents proposed schemes methodology, chapter 4 provides details about proposed scheme, in Chapter 5 results of proposed scheme is discussed, in chapter 6 future work and conclusion is elaborated. At the end, references are given.

CHAPTER 2

LITERATURE REVIEW

2.1 Overview

In this chapter, initially VANET is explained in addition with major research challenges in perspective of vehicles anonymity. Subsequently, existing studies based on pseudonym changing mechanism to maintain privacy of vehicles are presented, which are classified into two main categories, main difference between both categories are described with their relevant schemes. Then, analysis of existing schemes is presented with positive points and limitations. After it, research gap in existing study is discussed. Finally, whole section is summarized briefly.

2.2 Vehicular Ad-hoc network (VANET)

Vehicular Ad-hoc network (VANET) supports enormous protocols (IEEE 802.11 P, IEEE 1609.4) and various communication types V2V, V2I etc. to facilitate transportation. Internet of vehicles (IOV) a sub-category of VANET, is a network of vehicles in which vehicles communicate with each other to share their information for safe driving, to lessen the chances of accidents and to make intelligent transport system (ITS) possible [17]. Intelligent transport system (ITS) architecture comprises of On-Board Equipment (OBE), Certificate authority (CA), Road side

Environment (RSE) [11]. Vehicular Ad-hoc network (VANET) communication architecture contains On-Board Unit (OBU), Application unit (AU) and road side unit (RSU). On-Board Unit (OBU) comprises of read/write memory for saving vehicles information. This module also provides information to vehicles about hurdles on road, road congestion information and assist in dedicated short range communication (DSRC) with other vehicles. Application unit (AU) is dedicated device present inside vehicles to run different applications. AU can able to communicate to network by OBU[9]. Location Based Services (LBS) provide location information to vehicles[32]–[34]. Roadside unit (RSU) is installed in parking areas and along with roads, its main function is to globally monitor traffic[35], in case of road accidents, it sends information to vehicles in its region so they may take alternative routes and able to communicate with other RSU[9], [24].

For enhancement of road safety, vehicles sent beacons that contains exact location, speed and pseudonyms that vehicles are currently using, so that other vehicles able to knows about its neighboring nodes and adjust its speed accordingly to avoid accidents[16], [17], [23], [36], [37]s But generally all this information is in form of plain text instead of encrypted format. If any passive or active attacker is eavesdropping this information, that adversary easily know about every chunk of Basic safety Message (BSM), which in turn increase chances of attacks and may harm the passenger or drivers and also disturb anonymity of vehicles[21]. To avoid these attacks, pseudonym is changed by vehicles frequently, but changing pseudonym again and again is not enough to maintain anonymity of vehicles[23].

2.2.1 Lack of privacy

When vehicles share BSM, it contains all information. If an adversary is listening these beacons, it may put life of drivers in danger. As one vehicle is associated with one driver, they able to know whereabouts, social circle, religious belief and daily routine of driver. They also able to know at current time, where vehicle is travelling. If frequency of going at a place in a day is higher, it give clues to attacker about driver. It causes serious security threat for lives of drivers as well as

passengers. The private information of drivers may be used by third party in order to abuse and harm them[4], [17], [21], [23].

2.2.2 The syntactic linking attack

Vehicles frequently changes its pseudonym to avoid adversary attacks, but after changing pseudonym there still chances that an attacker steal information of vehicles. If a vehicle A is travelling on road, after time t it changes its pseudonym from A to B among three vehicles that are currently on road. By this information adversary can guess that Vehicle B had former pseudonym A that is changed at time t and at Δ+t time, vehicle B changed its pseudonym [17], [23], [26], [36], [38]–[41]. This attack is usually occur when vehicles do not change pseudonym cooperatively.

2.2.3 The semantic linking attack

It is considered as powerful attack as compared to syntactic attack because adversary able to know location of vehicles and relevant information even vehicles change pseudonym with cooperation. In this attack, adversary after listening BSM of target vehicle link it with new pseudonym of vehicles by using probabilities and tracking methods[17], [23], [26], [36], [38]–[42].

2.2.4 Existence of Malicious nodes in network topology

In internet of vehicles (IOV), each vehicle is receiving information about its neighboring nodes, if any vehicle in topology is controlled by adversary, it becomes dishonest and malicious node. A dishonest node able to reveal all information of network. Adversary can listen all received BSM to that dishonest node and have information about neighbors and their current location.

Similarly, it can modify the information of malicious vehicle and send BSM with wrong speed or location, which can cause accidents[27], [36], [43], [44].

2.2.5 Accident chances increase during silence mode

When vehicles travels, they share BSM with frequently changing pseudonym to confuse adversary. Some schemes stay silence for some time after changing pseudonym to avoid security attack. This silence mode may improve security but if vehicles become silent at critical areas like road intersection there is any important message regarding safety or speed of surrounding vehicles, vehicles in silence mode cannot receive it and accidents may occur[13], [21], [33], [38], [45]–[47].

2.2.6 High pseudonym consumption

Vehicles have a pool of pseudonyms that is assigned to them by Central Authority (CA). Central authority (CA) is an unbiased body and its main function is to provide vehicles with verified certificates or pseudonym[21], [32], [39], [40], [44], [47]. Vehicles have limited memory for keeping pseudonyms, for communication with other vehicles and infrastructures. When vehicles changes pseudonym frequently, it increase pseudonym consumption as a result, their pool of pseudonym may finish too soon. They have to request central authority to refill these pseudonyms, this extra communication require extra memory [21], [48]. So pseudonym consumption is an important factor that cannot be neglected, utilization of pseudonym should be efficient to avoid resource consumption[34].

2.2.7 Compromise upon quality of service (QoS)

Quality of service is crucial factor to check performance of scheme. Limited memory of vehicles can be full due to unnecessary message. Vehicles consists of sensors, OBU that allow them to interact with surroundings. Sometimes, it happens that other vehicles and RSU transmit important road safety messages, but due to memory in continuously full, those data packets start losing [21], [23]. There is high possibility that those data packets have road safety information and vehicle is unable to receive them at time and it may cause road accidents.

2.3 Pseudonym changing schemes for Vehicular Ad-hoc network (VANETs)

Privacy and anonymity are key features that cannot be compromised. Now in era of technology, privacy has been reduced , it is a serious security issue [17]. Similarly in VANET, when vehicles communicate with each other and share important information, it can be accessed by third party, which create hesitation for drivers in using it. From security perspective, it is important that vehicles changes its pseudonym. Pseudonym is a pair of public and private key which Trusted Authority (TA) assigned to vehicles. These assigned pseudonyms are verified which depicts that vehicles in network are authentic [24], [25], [32], [37], [44], [49], [50]. The purpose of changing pseudonym is to maintain anonymity of vehicles as well as low traceability of target vehicles by rival [21], [51] Numerous studies have been conducted to provide best scenarios in which pseudonym can be changed effectively. The existing pseudonym changing techniques are broadly classified into two main categories that are i) Mix Context Based Techniques ii) Mix-Zone Based Techniques.

2.3.1 Mix Context Based Pseudonym changing Techniques

Mix context based schemes are those that changes its pseudonym when some defined conditions are met. If those conditions are not fulfilled, vehicles do not change its pseudonym until current pseudonym do not exceed than maximum stable time. When it exceeds, vehicle changes its

pseudonym to avoid chances that adversary guess target vehicle. Mix context based techniques are also called user centric approach[17], [32], [34], [36], [37], [52].

Many researches are done in category of context based techniques that are described in this section. Vehicles changes its pseudonym when met trigger, so those vehicles that met trigger independently changes its pseudonym. This ideas is known as non-cooperative pseudonym change (NCPN). This strategy is not useful as it do not efficiently provide anonymity. To deal with this issue, Pan et al. presented a technique named Cooperative Pseudonym Change Scheme Based on number of neighbors (CPN)[48], in which vehicles changes pseudonym with cooperation of its neighbors. The number of neighbors considered as base of anonymity. When vehicle T gets trigger (considered k neighboring vehicles) to change pseudonym, it enables its neighboring nodes to change pseudonym. It is said that neighboring nodes cooperated with vehicle T. similarly when vehicle A gets trigger to change its pseudonym, it enables vehicle T to do cooperation. As a result anonymity increases. Advantage of this scheme is that it provides high security in case of dense traffic but not suitable in case of sparse density.

When pseudonym consumption is high, it affects quality of service (QoS) and causes packets to reach late at destination. To avoid this issue, Zidani et al. proposed a technique in which vehicles are allowed to change its pseudonym when there is variation in speed and number of surrounding vehicles. Vehicle v that intended to change its pseudonym, checks number of neighbors, afterwards their next position is determined by Kalman Filter, if they are same or too some extent they are travelling on same trajectory, vehicle v considers it as neighbor for changing pseudonym synchronously. Each vehicle's pseudonym has limited life span, when it expires that vehicle changes its pseudonym. One more innovation in this scheme is that instead of constant beacon interval, it uses adaptive beaconing interval, which is described in equations (1) to (4). I denotes beaconing interval, α represents adaptive beaconing rate, d denotes stopping distance, t_d represents thinking distance, b_d represents braking distance, v denotes speed when braking is applied, μs shows friction coefficient between roads and tires and g denotes gravitational force of earth.

$$I=\frac{1}{\alpha * d} \quad (1)$$

$$d = t_d + b_d \quad (2)$$

$$b_d = \frac{v2}{2\mu g} \quad (3)$$

$$I=\frac{2\mu g}{\alpha(2td\mu g+v2)} \quad (4)$$

If vehicle *v* transmit a beacon at time *t*, next beacon will sent at time *t+I*. So, beaconing interval is different for BSM, this adaptive beaconing brings advantage that attacker cannot link two pseudonyms of a vehicle[23].

To avoid adversary attacks, some schemes switch to silence mode after changing pseudonym that is risky because they may miss safety message. To resolve this issue [21] is presented that restricts transmission range of vehicles. Vehicle V checks speed of neighbor vehicles and adjust its transmission range. During high speed, vehicle v sends safety beacons to neighbors to avoid accidents, which silence based schemes don't consider during silent mode. When vehicle v receives BSM from neighbors, it first checks distance between itself and neighboring nodes (v_j). If distance lies in general or close neighboring radius, it shows that v_j are in proximity so it will consider it for transmission adjustment, otherwise ignore it.

To improve vehicles privacy, [39] is proposed, combination of two techniques that are Cooperative Pseudonym Exchange CPE and Scheme Permutation SP. In CPE, vehicles that want to exchange pseudonym transmits beacon with ready_to_change bit on. All nearest neighbors are involved in it. Each vehicles has a set of unused and currently used pseudonym. Unused pseudonym are used to exchange process, when neighbors are greater than threshold value, pseudonyms are randomly exchanged and distributed. Vehicles having short-range of pseudonym may not participate in this process. In scheme permutation, vehicles change its pseudonym by its own

collection either by RSP (Random silent pseudonym) or by periodical pseudonym change method. Each scheme is valid for one time slot. Scheme permutation is more beneficial in case of sparse traffic. In CPESP, CPE and SP algorithm run equivalently, unused pseudonym shuffles, randomly scheme selected from RSP and periodical pseudonym change for changing pseudonym.

To avoid pseudonym linking attack, Walid et al. suggested a scheme named in which vehicles uses three different pseudonym that are Rpseud (Real pseudonym), Ipseued (Initial pseudonym) and Npseued (New pseudonym) generated by TA, RSU and OBU respectively. When vehicle needs to change its pseudonym, it requests to TA to generate Rpsued, TA provides vehicle with Rpseued. Afterwards, vehicle requests to RSU, in response RSU first validates from TA either vehicle is validated or not. If validated RSU provides vehicle with Ipseued. After it, vehicle checks its surrounding neighbors, if they exist it changes Npsued generated by OBU. When vehicle finds new RSU, the lifespan of previous pseudonym expires. Cycle of pseudonym changing process is shown in **Figure 2.1**.

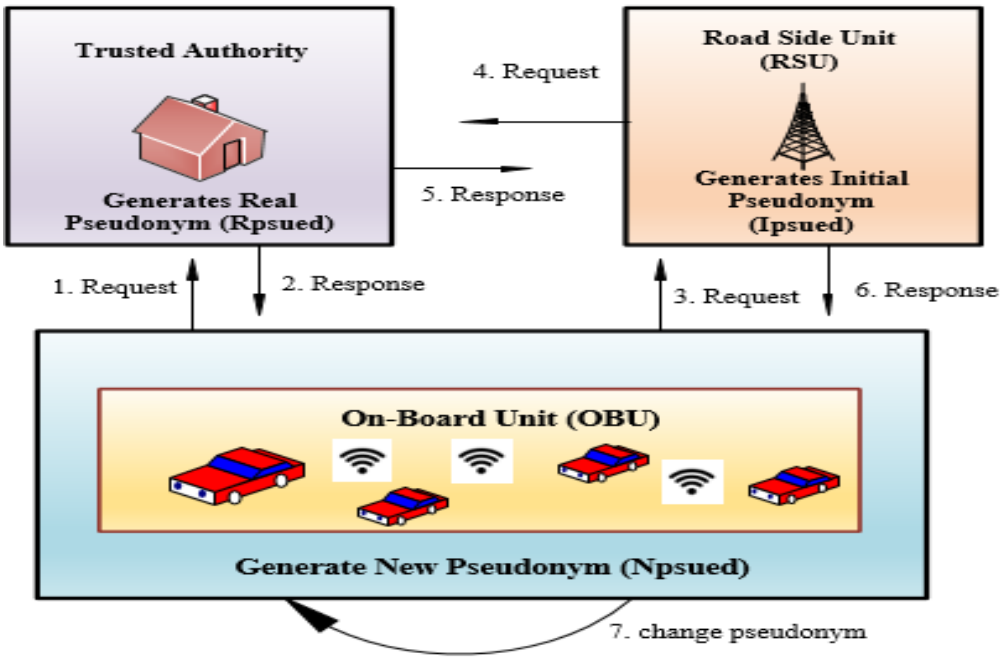

Figure 2.1: Pseudonym changing cycle

At every phase, before issuing new pseudonym, vehicles authentication is done to avoid security attacks. The advantage of this strategy is that traceability of vehicles by adversary is not possible as well as it provides high security, but it increase pseudonym consumption, computation overhead as well as it is costly to implement[44].

For improved privacy and low traceability, Context-adaptive privacy scheme (CADS) for Vehicular Ad-hoc network is proposed. CADS uses traffic density and number of neighbors' information to consider vehicles eligibility for pseudonym. Vehicles turn to silent mode but this silence duration is smaller to avoid compromise on road safety beacons. CADS strategy takes drivers privacy preference into consideration for providing security. When drivers enter into some sensitive areas, privacy preferences will be high that scheme will detect b parameters value and provide better security. Advantage of scheme is that it reduces traceability too much extent[51].

I.Ullah et al. proposed a technique in which Group of vehicles are created and one vehicle is selected as group head (GH). All vehicles in a group are assigned with Group ID (GID), when a vehicle wants to join a group, GH check its credentials if they are valid, that vehicle join the group. So communication inside a group cannot be listened by outside vehicles. Vehicles changes its pseudonym by checking its neighbors if it is higher than threshold value, vehicles simply changes its pseudonym otherwise virtual pseudonym changing mechanism is implemented in which each member creates two message with different velocities and speed are created that is randomly exchanged. Vehicles that are far is selected for exchange process. If all vehicles have same distance then randomly a vehicle is nominated. Advantage of this scheme is that vehicles that are outside of group cannot listen communication of a group. Drawback of this scheme is that it increases computation cost in case of virtual pseudonym exchange because it creates two beacons that additionally increase overhead [32].

To resolve issue of pseudonym linkability, Xinghua et al. presented a technique in it, vehicles swap their pseudonym with other vehicles that are in range of vehicle Vi. The infrastructure consists of vehicles, RSU and Registration authority (RA). RA provides vehicles with legal pseudonym and data center part of RA will keep records of vehicles true identity and pseudonyms assigned to them. Pseudonym mapping database is used to ensure linkage of vehicles before and after pseudonym swap for accountability. When a vehicle Vi wants to swap its pseudonym, it broadcast request message Reqi and send its VID, pseud to RSU. When in range vehicles receives this Reqi send assist reply with its all information to RSU to show willingness of participation in pseudonym swap process. Vehicles that are participating in this process are known by Vswap, their pseudonym is collected by RSU and then swapped pseudonym on basis of driving similarity of vehicles. For driving similarity, speed, position and location similarity calculated by adding some random weights. All this procedure will try to make vehicles indistinguishable and increase chances to confuse adversary. Similarity utility, exponential utility, utility value normalization, probability sampling as well as mechanism of differential privacy are used for selection pseudonym from ppseu (pseudonym pool). Benefit of this technique includes provide high unlinkability between new and old pseudonym [23].

To solve traceability issue, CMC is presented in which two different cases are catered differently, in first scenario vehicles at low speed that are at intersection of road with high neighbors are considered. In second case, vehicles in low speed with few neighbors are considered. In scheme, architecture consists of vehicles, RSU and TA. Each vehicle is equipped with OBU (Onboard unit). It is assumed that adversary has global coverage and able to access beacons (information include pseudonym, speed, location) to link vehicles. Vehicle before changing pseudonym checks neighboring vehicles in transmission range having same speed, direction and traffic density (heavy or low). Vehicles with high traffic send beacon with bit PU=1 to inform other vehicles about changing pseudonym. In case of low density, real and virtual two pseudonyms are created and swapped randomly among each other. True pseudonym is accepted by neighbors and false one is rejected. After pseudonym exchanging, vehicles inform central authority about it, so no malicious node can move in. Advantage of proposed scheme is that traceability is not possible by adversary.

The scheme is only confined to vehicles that is in low speed. Vehicles having high speed is not considered[36].

In [25], author presented strategy to maintain vehicles privacy during travelling to make VANET system secure. CPS scheme is categorized into five phases contains initialization phase, Registration phase, Handshake phase, congestion detection phase and authentication phase. In first phase, entities like RSU, vehicles and TA are initialized. RSU have information of all neighbors that are in its transmission range. RSU and vehicles are registered from TA, it provides pool of pseudonym and secret key to vehicles in registration phase. When vehicles enter in range of RSU, it transmit beacon so vehicle can communicate with it. After receiving beacon, vehicle send BSM to roadside unit contains VID, pseudonym, location and speed. By this information, RSU verifies either it is valid vehicle. After verification, trip time *Ti* is calculated by equation (5).

$$\mathrm{Ti} = \frac{\text{Range RSU}}{\text{Speedvehicle}} \qquad (5)$$

Trip time basically provides information about when vehicles exits from RSU. $Range_{RSU}$ is transmission range of RSU while $Speed_{vehicle}$ is speed of vehicle. RSU extract VID of vehicle, if trip time is expired but vehicle do not exit from range of current RSU then , again BSM send to extend vehicles lifespan in that range. If vehicle is not registered by TA, then RSU send this information to TA for taking action. Vehicle is monitoring its speed frequently, if it is less than some threshold speed Vs. it will enter in congestion detection phase and start sending congestion awareness message with its location PID, speed and road identity. RSU checks vehicle is registered and then send a reply so vehicle not send this message again and again. For authentication of congestion, RSU waits until 30% of vehicles send congestion message to RSU, through it, RSU sure about traffic jam and warns other vehicles about it so they can take different route. Vehicles communicate only when enter in RSU and changes pseudonym that advantage of this scheme it decreases communication overhead.

Yang et al. [53] proposed scheme named DPSZ in which vehicles are provided by pseudonym from CA that is considered as honest body, vehicles have OBU for communication that may be accessed by adversary for planning passive or active attack on vehicles so they may act as dishonest body while RSU are semi-honest. Vehicles share their information and pseudonym with neighboring vehicles. Vehicle swap its pseudonym by creating a temporary zone. Before creating a swapping zone vehicle vi checks two conditions if they fulfilled it means those neighbors can participate in swapping. First condition is to check vehicles connected time against a threshold time value ɼt and second is available number of vehicles. Second condition is that number of vehicles are not less ɼs (threshold vehicles). If these two conditions are satisfied, then vehicles are allowed to create a swap zone. Those vehicles that want to participate in swap zone authenticates initiator vehicle by its digital signal and then reply it. After checking these conditions, vehicle that want to swap its pseudonym send swap signal to its neighbors. All information is encrypted, vehicles that are interested in swapping, send reply to initiator. After receiving replies by initiator vehicle vi selects randomly vehicle vr, whose information is correct. When swapping process is completed successfully, then all information regarding swapping, vr, vi and their pseudonym is send to CA, so central authority able to link new and pervious pseudonym of vehicles. If any misbehavior from vr or vi is observed by CA or received any accusing message from anyone of them, such malicious vehicles are expelled from system, backlist, revoke its certificate, cancel its swapping and inform to victim vehicle then assign it new pseudonym. So vehicles will remain secure from internal attacks as well. When initiator vehicle vi is at intersection road, there are many vehicles at that point, to communicate with them causes high computation and resource cost. So to reduce this cost, initiator vehicle vi adds only eligible vehicles to whom communication is important to done. Eligible vehicles can evaluate ability to respond by Equation 6. *Pr* is probability of vehicles to reply initiator, $|\Psi i|$ symbolizes set of neighbor vehicles of v_i, $ɼs$ is vehicles threshold to create a swap zone while e (Euler's constant) is constant. This equation shows that when $\mathbf{|\Psi i| \geq ɼs}$ then vehicles have low probability to reply.

$$pr = \begin{cases} 1, & |\Psi i| = ɼs \\ e^{1\frac{|\Psi i|}{ɼs}}, & |\Psi i| \geq ɼs \end{cases} \qquad (6)$$

As number of vehicles increases, probability of reply is getting decrease, so it is inversely proportion. Advantage of this scheme is that it provides high security from internal attacks as well as external attacks. Drawback of this scheme is that it only swap its pseudonym with neighboring vehicles when vehicles reached to a specific threshold ɼ**s**. This ideal situation is not possible every time.

For better resource consumption and improve vehicles anonymity, TAPCS is presented, it make use of silence mode, if speed of vehicles are slow than threshold speed threshold v_c for time threshold t_c vehicles assume that traffic congestion occurs. This is confirmed by other vehicles if they issue congestion message. After confirmation of congestion, vehicle have to select an initiator, if no initiator message has been received, vehicle waits for certain amount of time d_{max}, at the end of d_{max} vehicles checks initiator message, vehicle having minimum position is considered initiator (T_0), the function of is to create a silence zone for vehicles to change its pseudonym. Initiator stop broadcasting safety message and transmit s_notification to vehicles that includes speed threshold, location and position of initiator. Vehicles with lowest speed than threshold stop broadcasting safety message and changes their pseudonym, while vehicles having high speed than threshold value are allowed to send safety message to avoid accidents. With passage of time there is possibility of silent zone got filled and may be new vehicles are not in range of initiator. Therefore a new initiator is selected. After selection of new initiator, previous one stop sending any notification now this duty will performed by new initiator. When congestion ends, old initiator informs vehicles about traffic congestion has ended. So vehicles that are currently in congestion phase now silent from silent mode able to send and receive safety message. Proposed schemes works well only in case of traffic congestion[38].

When many vehicles enter in silence mode there are high chances that they miss important safety messages. To avoid this problem, vehicles able to change pseudonym when at least k neighbors exit and secondly traffic scenario is dynamic and change time to time, so when new vehicles enter in silent period they are used to increase anonymity set. As anonymity set directly proportional to adversary confusion. At time t, let k Free State neighbors exist to change

pseudonym, then in next t+at time vehicles take decision independently either to change pseudonym or not, if they broadcast with probability p, it shows willingness to change pseudonym and this process is known as flickering. At t+nT, vehicles set HT=1 and share it with new neighbors. Vehicles t+(n+1)t time, changes cooperatively pseudonym. As vehicles increase, anonymity set increases. Silent period is kept short as compared to existing techniques so avoid negative impact on safety beacons. As silent time period is kept shorter, so it is able to broadcast beacons safely[54]. Simulation results showed as value of k increases, anonymity start increasing and scheme showed lowest traceability.

To maintain vehicles anonymization, Adaptive Grouping and Pseudonym Changing Policy for Protection of Vehicles Location information in VANETs [55] is proposed, in which vehicles adopt a group according to its speed, transmission range and position. Each group has a Group Leader (GL) that gives vehicles permission to join a group. Each vehicle has same probability of elected as GL. All communication to LBS are done through Group identity in order to hide true identity of vehicle. A vehicle may change its group according to its speed and join some other group. When vehicle leaves a group and join some other group, it changes its pseudonym. There are three possibilities a vehicle consider for changing pseudonym, vehicles monitor group members that exist in transmission range if low, time threshold and speed is monitored after which pseudonym is changed, if have high number of members it increases anonymity set of vehicles. If low speed vehicles exist at road intersections, then safety beacons dissemination and pseudonym changing done less frequently. In dense traffic anonymity set is huge so traceability is not possible, to confuse adversary and maintain anonymity in sparse traffic, dummy data is also added. Benefit of this strategy is efficient pseudonym consumption as well as sparse traffic situation is also considered.

2.3.2 Mix Zone Based Pseudonym changing schemes

In Mix zone pseudonym changing schemes, specific places are decided earlier where vehicles enter and changes its pseudonym. Mainly vehicles stay silent before changing pseudonym, after changing it start transmitting beacons again. Different places like gas station, parking areas are selected for staying silent and changing pseudonym. These schemes are considered most effective in case if implemented in cities[16], [17], [23], [32], [36], [43], [51], [56], [57] Various researches have been done in this area to improve security issues that exist to disturb anonymity of vehicles. Existing mix zone studies are mentioned in this section.

Many schemes are presented to change pseudonym but some of them compromise on safety message and some have high resource consumption and computation overhead. To tackle these drawbacks, on basis of mix zone by setting front of traffic lights areas as silent zone. All vehicles slows down or completely stop when traffic light turn red. In this stage if vehicles do not communicate to each other, it will not be harmful. Mix zone length is dynamic as it depends on traffic flow. During green traffic light, flow of traffic is monitored to know about mix zone length during red light, information about traffic flow is gathered through road side unit. When red traffic lights set, TLSA sends SilentZoneStart signal ISM =1, vehicles that are in silent zone stop transmitting beacons and will change pseudonym. After receiving SilentZoneStop signal ISM =0, vehicles are now exit from block state and continue to send beacons. Those vehicles that satisfy these condition will change its pseudonym i) Vehicles received SilentZoneStop signal ISM =1, ii) vehicles are currently in mix zone area. It will make trajectory privacy more secure and create confusion for attacker who want to access information. All vehicles have pool of pseudonym, if it is finished request is sent to RSU after verification it is forwarded to trusted authority through RSU pseudonym module, TA checks information and generate a set of pseudonym and delivered to vehicle through closet RSU. This scheme tried best that silent zone do not negatively impact safety beacons. , for measuring traceability rate, equation 7 is used. N represents total traces available in dataset, v is vehicle, $L(v)$ shows lifetime of v and τv shows traceability time of vehicle v.

$$\Pi = \frac{1}{N} \sum_{v \in V} \lambda_v \text{ X } 100, \qquad \lambda_v = \begin{cases} 1 \; if \; \frac{\tau v}{L(V)} & \geq 0.90 \\ 0 & otherwise \end{cases} \tag{7}$$

For checking efficacy of TLSA scheme, it is compared with conventional silence based schemes including RSP, Mix-zone and SLOW. In case of traceability, TLSA shows good results comparatively other two aforementioned techniques, in TLSA traceability starts decreasing when Mix-zone length starts increasing. In case of vehicles anonymity, TLSA and SLOW is much better than RSP scheme. Advantage of this scheme is that during silent period, vehicles do not suffer for safety messages. Drawback of this scheme is that it performs well when there are maximum number of vehicles in mix zone, it is not much useful in case of light traffic flow[43].

To increase vehicles anonymity and reduces pseudonym consumption, K.Emara et al. proposed a scheme CAPS, vehicles keeps information of its neighbors speed. Vehicles become silent and change its pseudonym in case they find best zone to do it. If vehicle found any silent neighbor it also becomes silent and change its pseudonym. Pseudonym assigned to vehicles has lifespan, when it expires pseudonym changing process occurs to avoid security attack. Vehicle come back with new pseudonym and transmit safety beacon. Proposed scheme utility is checked against RSP, CAPS show better result in terms of traceability [56].

For enhancing vehicles privacy and maintain confidentiality, vehicles virtually create Cryptographic Mix zone when vehicles pseudonym needed to change. Architecture of this scheme contain Road side unit (RSU), Control servers (Cs) and trusted authority (TA). When vehicle want to change its pseudonym. It send request to control server (Cs), that send nearest vehicles COMMAND message to create a virtual cryptographic mix zone, in this zone vehicles do not switch to silent mode, but it continually broadcast safety messages that are in encrypted form. Vehicles in zone cooperatively changes pseudonym and move out from dynamic zone with new pseudonym[45]. Drawback of this scheme is that it takes extra time to decrypt safety beacon.

In order to increase vehicles security and to improve scenarios in which vehicles should change pseudonym a technique named Vehicular Location Privacy Zone (VLPZ) is presented. It is an infrastructure based strategy in which vehicular network is divided into many grids. Each cell or grid contains VLPZ zone. Vehicles that are is in zone changes pseudonym with synchronization and motivate other vehicles to enter in VLPZ zone. For motivation, some incentive mechanism is used to encourage vehicles in VLPZ zone. Those vehicles that enter in this zone, rewarded with high incentives otherwise their incentive values are reduced. Each vehicle has a pool of pseudonym which is allotted by TA. Vehicle transmit safety beacon after t time to neighbors. VLPZ zone contains TA_R (Regional $_{trusted}$ authority) that act as intermediator between TA and VLPZ. Vehicles currently in zone changes pseudonym after every δ minutes. Additional TA_R is added to increase secure communication that take place between VLPZ and TA. There may be one or more VLPZ in a grid and each VLPZ have RSU_{vz} that broadcast information about zone to vehicles that are currently in. The VLPZ infrastructure consists of router through which vehicles can enter in zone and one aggregator through which they exit and contains lanes (l>1). VLPZ infrastructure is shown in **Figure 2.2.**

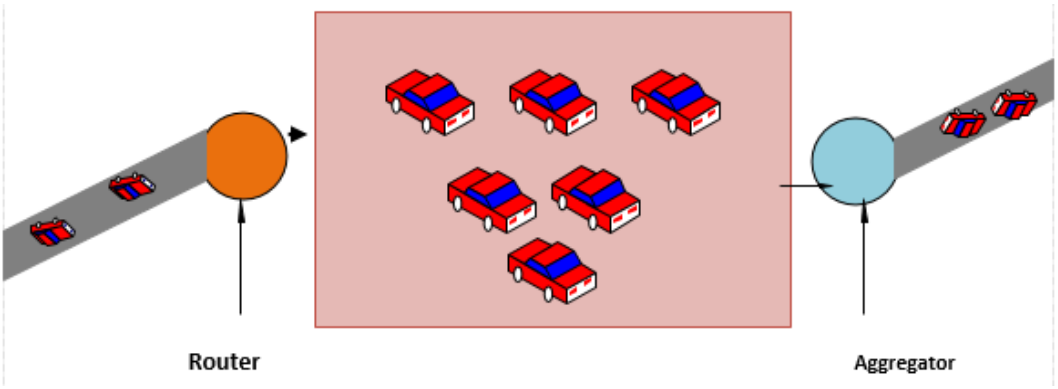

Figure 2.2: VLPZ infrastructure

After changing pseudonym vehicles exit through aggregator after random amount of time to avoid FIFO attacks. Vehicles then send safety beacons with new pseudonym. Existing RSU can be used for this scheme, but it is recommended to install separately for security enhancement the achieved traceability of proposed scheme is checked by Equation (8). *d* represents the degree of

anonymity, *k* denotes capacity of vehicular zone and |*AS*| represents occupancy of vehicular zone.

$$d=\frac{log2(|AS|)}{log2(k)} \qquad (8)$$

This scheme is better in providing security against pseudonym inking attacks but if new RSU are deployed it becomes costly to implement[47].

As many vehicles changes pseudonym together, it increases anonymity size as well as confuses adversary to correctly target vehicle. Pseudonym allocated to vehicles are limited in range, so it finishes after frequently change. Due to this reason, many vehicles don't participate in pseudonym changing process. Such vehicles are termed as Selfish node. To motivate selfish nodes to participate in pseudonym changing process, an approach Reputation-based scheme is suggested. Before entering in vehicular network, all vehicles need to get register from trusted authority. This scheme motivates selfish nodes to participate in pseudonym change during mix one by using some incentive/credit mechanism. When a vehicle wants to change its pseudonym, it creates a dynamic mix zone and observes number of vehicles that are in zone. Vehicle sends RNP (Request new pseudonym) request to control server and in turn control server send COMMAND to other vehicles in zone to ask them to cooperate change pseudonym. CS monitors number of vehicles that have responded COMMAND by RNP to know about vehicle changed pseudonym as well as those have not changed. Cooperated vehicles are assign them with incentive value, at initial, all vehicles incentive value is zero it increase if it continually cooperates. A threshold value ε is to determine either a vehicle is selfish or not. If vehicles reputation values is ≥ threshold values all vehicles of respective zone have to change pseudonym otherwise vehicles independently can take decision by keeping in notice about reaming pseudonym lifetime, value of incentive. Results showed that RPCLP provides better energy consumption. Advantage of this scheme is that it provides better anonymity size which confuses adversary and provide better privacy[57].

Another scheme to maintain secure trajectory for vehicles is proposed. Vehicles are moving in different pace, some are slow and some are fast. The author categorized vehicles on the basis of its velocity. Vehicles having same velocity are placed in one group in a transmission range T_x. *r* represents radius of transmission range. T_x is defined in Equation (9).

$$T_{x=} \pi r^2 \qquad (9)$$

. Vehicles according to its current velocity opt a group. Grouping of vehicles inside VBPC is shown in **Figure 2.3.**

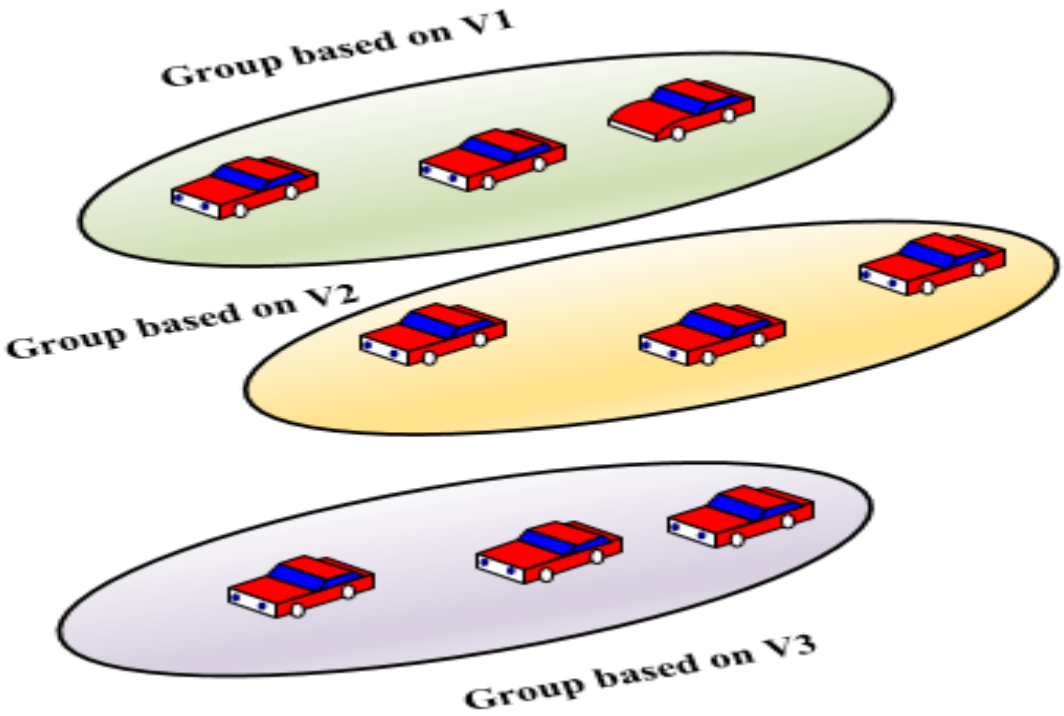

Figure 2.3: Vehicles Grouping Based on Velocity

A vehicles is eligible to change pseudonym according to following conditions. If vehicle has changed its group, in new group it is allotted new pseudonym. S_{th} represnts speed threshold, if $S_{th} \leq 1$, vehicles will not change its pseudonym but if $S_{th} > 1$, all vehicles in respective group are liable to change pseudonym. Drawback of this scheme is that it is suitable only for vehicles that are travelling for long distances, not appropriate in case of short distance[40].

To reduce pseudonym consumption and improve location privacy, another scheme Urban pseudonym changing srtategy for location privacy is presented. Vehicles can update its pseudonym

only in front of red traffic signals at singalized instersection area. Red traffic signal is considered as silent zone, any vehicle that enters in silent zone get notification from RSU_{SM} , stop broadcasting BSM and send message to RSU about its current lane, pseudonym id. All vehicles in red zone remain silent and update pseudonym either changing it or by exchaging with some other vehicles that is currently in mix zone. If vehicle selects to exchange pesudonym it is done through swappping protocol. Vehicles that have intebtion to exchange pseudonym send their private key, pseudo id to RSU , in reply RSU exchange their pseudonym randomly. For exchanging pseudonym, atleast two vehicles should be in silent zone. Silent zone remain valid till red light. It exit on green or yellow traffic light. After silent zone ended, vehicle starts again broadcasting beacon with updated pseudonym. In case of exchaniging pseudonym computation cost and pseudonym consumption reduced [41].

To resolve issue of location privacy as well as drivers information secrecy ,another approach uses idea of mix-zone by considering signalized intersection, tool booths, traffic jams as silent zone. When vehicle enters in these mix zone, vehicles speed are taken under consideration and according to vehicles speed, they are treated. In case vehcle is in very low speed (lies between 20 km/h to 40 km/h), such vehicles enter into silent mode and changes pseudonym synchronously with neigboring vehicles. If vehicles is in medium speed (lies between >40km/h to 60km/h) then further condition of existance of k neighnors chesked if it exists, then it sets Readyflag=1 annd cooperatively change pseudonym with surrounding neighbors and the last case is that if vehicles speed >60km/h, Readyflag bit-0 and pseudonym change occur. CRSMZ performed well in creating confusion for adversary, minimum achieved traceability in case of having high neighbors in mix zone[58].

To efficintly utilize memory and pseudonym, a Privacy Conserves pseudonym Acquistion scheme is presneted [49] in which vehicles are provided with one pseudonym by pseudonym certificate authority (PCA), when vehicles need more pseudonym then Gao algorithm creates multiple pseudonym rndomly by taking that one pseidonym. RSU and PSA are not involved in this process. All communication that is carried out is encrypted. Vehicles do not need pool of

Pseudonym as other techniques, Gao algorithm created pseudonym are enough for ten days. This scheme provides strong defense aginast syntactic attacks as well as confuse adversay. RSU are not overloaded and pseudonym usage is much efficient.

2.4 Comparison of Pseudonym based strategies in Vehicular Ad-hoc Network

In previous section, existing schemes were presented on basis of pseudonym changing mechanism. These schemes were classified into two main categories that are Mix-Context and Mix-Zone based strategies. Schemes belongs to these categories were elaborated as in which scenario they will change its pseudonym. In this section, summary of existing schemes is presented along with its basic idea, mechanism as well as positive points and weaknesses. Summary of existing studies is given below in table 2.1.

Table 2.1: Summary of pseudonym based techniques

Scheme	Basic idea	Mechanism	Advantages	Limitations
CPN [48]	Changes pseudonym with neighbor's cooperation.	When vehicle v met trigger, it changes pseudonym along with neighbors.	Anonymity size increases. Provide high location privacy.	Pseudonym consumption is high. Depends on neighboring vehicles.
EneP-AB [23]	Usage of Adaptive beacon interval.	Pseudonym changes when variation in speed, number of estimated neighbors and position.	Provide protection again pseudonym linking attacks. Packet loss is low.	Not much effective in case of sparse traffic.
WHISPER[21]	Restrict vehicles transmission range.	Vehicle v check neighbors speed, if vehicles sharing same road id or radius, it shows that vehicles are in proximity so it changes pseudonym.	Prevent road accidents by transmitting beacons earlier when vehicle is in high speed.	Pseudonym utilization should be efficient.

CPESP [39]	Exchange pseudonym cooperatively and scheme permutation.	Vehicles exchange pseudonym with neighbors when > than threshold, in scheme permutation vehicle change pseudonym either by RSP or periodical pseudonym changing process.	Reduced communication overhead. SP has improved performance in case of sparse traffic.	In SP phase, more schemes should add to increase degree of confusion for adversary.
RIN [44]	Vehicles uses three pseudonyms generated by RSU, TA and OBU.	At each step, authentication of previous pseudonym is done before generating new one to avoid entrance of malicious vehicles in network.	Provide high security against adversary attacks. Traceability is not possible.	High pseudonym consumption. Need extra memory to tackle computation overhead.
CADS [51]	Silent period is used for changing pseudonym.	Drivers are allowed to select privacy level either high or low, during silent mode pseudonym along with neighbor changes.	Reduces traceability to a large extent.	Make compromise on QoS during high privacy preference.
DGVP [32]	Dynamic grouping based on road context information.	Based on vehicles position, speed groups are created. If vehicles are greater than threshold value, simply pseudonym are changed otherwise virtual pseudonym change strategy is opted.	Low location traceability of vehicles.	Suitable only for low traffic region.
PAPU [37]	Swap pseudonym in range vehicles with same driving matrices.	V_i sends request to close vehicles, provide its id to RSU, intended vehicles reply with assist message to join swapping and provide its real id to RSU.	Maximum unlinkability of vehicles. Low Pseudonym consumption.	Depends on RSU, can overload it. Not effective in case of sparse traffic.
CMC [36]	Pseudonym updated based on high or low neighbors in locality.	Vehicles having low speed with high neighbors for a threshold time can change pseudonym cooperatively, in case vehicles are low	Provide protection against attacks planned by adversary.	Not catered for scenario with vehicles having high speed.

		pseudonym is exchanged randomly with neighbors.		
CPS [25]	Vehicles communicate only when necessary otherwise remain silent.	Vehicles send BSM when enter in range of RSU, through which RSU validates about vehicle's authenticity. Trip time of vehicle is calculated. If road congestion occurs, it broadcast road congestion beacon.	Reduced communication overhead and location traceability.	Majorly depend on RSU, can overload it.
DPSZ [53]	Swapping of Pseudonym among vehicles.	If vehicles are > ɼv for time > ɼt then vehicles can participate in swapping. Initiator vehicle v_i after receiving messages from v_r, randomly selects any vehicle for exchanging pseudonym, TA is informed about swapping.	Low communication cost. Reduce pseudonym consumption.	Swapping is possible only If vehicles are > ɼv, that is not possible every time.
TAPCS [38]	Use silent mode for changing pseudonym.	If vehicles speed $<v_c$ for time t_c, it indicates vehicles is in congestion so it stop dissemination of BSM and change pseudonym. Vehicles having high speed than v_c, continue to send BSM.	Provide protection against semantic and syntactic linking attacks.	Vehicles not in congestion are not catered by this technique.
TLAS [43]	Switch to Silent mode at Red traffic light.	Vehicles stop during red signal, stop sending BSM and change pseudonym.	Provide secure trajectory without compromising on safety beacons.	During low traffic flow, it is not much useful as traceability decreases only when mix zone length is high.
CAPS [56]	Uses silence mode for changing pseudonym.	Vehicles when find best zone to change pseudonym, it switch to silence mode. When v find neighboring vehicle as silent, it also become	Provide better result of traceability comparatively other silence techniques.	High pseudonym consumption. Negative impact on QoS.

		silent and change pseudonym.		
DMLP [45]	Virtual CMIX zone create to change pseudonym.	Vehicles that want to change pseudonym request to CS by sending RNP message which in turn send COMMAND message to RSU to create CMIX zone and change pseudonym. Vehicles send BSM in CMIX zone but in encrypted format.	Vehicles don't switch to silent mode during CMIX zone to avoid compromise on safety.	Decryption of BSM may take extra time.
VLPZ [47]	Uses silent mode. To motivate vehicles Incentive is provided.	Vehicles enter in zone through router, become silent, change pseudonym and exit from aggregator.	Anonymity increases in case vehicles cooperate.	Costly to implement if special RSU are deployed.
RPCLP [57]	Motivate selfish nodes to participate in pseudonym changing process.	Incentive is given to vehicles which changes pseudonym, cooperatively in a dynamic mix zone.	Anonymity size increases. Protect against adversary attacks.	Consumption of pseudonym is high.
VBPC [40]	Vehicles opt group based on their velocity.	Pseudonym change occur when vehicle join a new group, $S_{th}>1$ or stable time expired.	Anonymity increases if vehicles remain in a group for long time.	Not appropriate for short range distance.
UPCS[41]	Silent zone created at signalized intersection.	Red traffic light is considered as silent zone, vehicles opt to change or exchange pseudonym in the zone.	Pseudonym consumption is reduced in exchange mode.	Not effective in case of sparse traffic. Vehicles change pseudonym at red signal. So traceability other than red signal is possible.

Flickering Context Based Mix strategy [54]	Silent period is kept short for changing pseudonym.	Vehicles when transmit beacon with Probability p, it shows intention to change pseudonym, vehicle set HT=1 and send to neighbors to cooperatively change pseudonym.	As anonymity set increases, traceability reduces. Shorter silent period do not highly impact on safety messages.	Not much effective in case of sparse densities.
CRSMZ[58]	Traffic jams, highway considered as mix zone.	Speed in mix zone is cheeked, either lowest, medium or highest and treated accordingly.	Only low speed vehicles switch to silent mode, so not highly impact safety beacons.	Not effective if vehicle are low in number.
AGPC[55]	Dynamic grouping of vehicles on basis of traffic condition.	Traffic situation and speed of vehicles monitored for pseudonym change.	Provides high location privacy in dense traffic. Add dummy data to increase anonymity in case of sparse traffic.	If GL becomes dishonest, it reveal information of whole group.
Privacy Conserves Pseudonym Scheme [34]	Gao algorithm used for pseudonym replication	PCA provides vehicles with only one pseudonym after encryption, which Gao algorithm convert into multiple pseudonym that are useable for 10 days.	Memory efficient scheme, Do not dependent on RSU.	Randomization of pseudonym is a challenge.

As different schemes are presented each of them has its own positive and negative points. These schemes are basically divided into two main categories. Schemes [21], [23], [25], [32], [34], [36]–[39], [44], [48], [51], [54] are considered as Mix-context techniques while [34], [40], [41], [43], [45], [47], [56]–[58] are considered as Mix-Zone strategies. Each schemes has its own conditions about where vehicles should change pseudonym to maintain anonymity as well as privacy. Both schemes provide high security but have high pseudonym consumption that in result increases computation overhead as well extra memory is required to tackle this overhead that make these techniques costly to implement [48][44], similarly [56][57] have also high pseudonym consumption which in result make compromise on Qos. To increase adversary confusion these

techniques uses [25], [38], [41], [43], [47], [51], [54], [56], [58] silence period to change pseudonym.

During silent mode, vehicles don't send and receive safety beacons and many techniques compromise upon safety and prevention against road accidents. When vehicles travel on road they passes through different scenarios where traffic is dense or sparse. Some techniques[23], [32], [37], [38], [41], [43], [54], [58] performed well in case of high vehicles but not well when traffic is sparse. To reduce pseudonym consumption, these schemes [32], [36], [37], [39], [43] exchange pseudonym to avoid high computation overhead and make sure efficient utilization of pseudonym. To avoid pseudonym linking attacks, strategies [23], [34], [36], [38], [44], [57]performs well. Communication cost is lower in these schemes [34], [36], [39], [41], [53] as compared to other above mentioned techniques. Techniques [21], [23], [25], [32], [34], [36]–[39], [44], [48], [51], [54] [34], [40], [41], [43], [45], [47], [56]–[58] uses fixed beaconing interval which may have a negative impact on QoS including packet loss, packet delay and limited storage space of vehicles may remain full.

2.5 Research Gap and Directions

As VANETs improved transport system and minimize road accidents to a large extent but security of vehicles, driver's information as well as passengers cannot be neglected. The ITS system has improved standard of life but still there are vulnerabilities in ITS which cannot be ignored. The main concern is vehicles anonymization in vehicular network. Many researches are done to improve security and enhance anonymity but quiet it is an open challenge. In [21], vehicles do not take actual distance between vehicles into consideration and send BSM including sensitive information, that make it possible for adversary to spy information present in BSM which can harm driver or passengers.

2.5.1 Effect of problem

Due to not considering enough parameters before sending BSM, it may prove harmful for passengers as well as create many other problems. When vehicles send BSM to other vehicles, there is a probability that the adversary has installed eavesdropping antennas that capture information about the target vehicle, through accessing vehicles BSM adversary can harm the target vehicle. Vehicles that receive BSM change their pseudonym even if their direction is different, it increases pseudonym consumption. Vehicles have a limited buffer to process BSM when a vehicle receives irrelevant beacons from other vehicles it causes the buffer to be full which ultimately increases the delay in receiving important BSM when there is no benefit in receiving them or may lose beacons. The lost BSM packets may have safety information, which loss can cause accidents. All these situations also increase bandwidth utilization. Due to high pseudonym consumption, vehicles are quickly short in available pseudonyms and they have to appeal to RSU to request trusted authority to provide vehicles with a new set of pseudonyms. It increases communication costs and pseudonym computation as well.

2.6. Summary

Internet of vehicles has increased ease in transportation and reduces road accidents. As in ITS privacy is main concern, for this purpose CA provides pseudonyms to vehicles to maintain anonymization. A lot of researches has been done for changing pseudonym in order to fulfill privacy needs but till now, there is no such techniques that completely eliminates adversary from doing active or passive attacks completely. All existing schemes have some weaknesses which have been highlighted in section of comparison.

CHAPTER 3

METHODOLOGY

3.1 Overview

In this chapter, the research methodology is described which is used throughout the research procedure. This chapter presents detailed information about literature review, problem identification, and the proposed solution and used simulators in evaluating research along with results.

3.2 Operational Framework

The internet of vehicles (IoV) has brought many comforts and changed the pattern of life by expanding services for mankind. Though it reduces the accidental rate and reduces the death rate from road accidents still there are privacy and security issues that may prove a serious threat to drivers or passengers. Vehicles communicate by BSM and share their important information to take safety measurements in time but if a malicious vehicle exists in-network with an intention to eavesdropping these BSM and extract important information to harm the target vehicle or adversary may deploy spying antennas to receive BSM from its area of interest to track the trajectory of vehicles. To avoid spy attacks planned by an adversary, there is a serious need to further research on the privacy and security enhancement of Iov. However, there is huge literature available and many schemes are presented earlier to avoid adversary attacks but each scheme has some

limitations that increase the need for studying security schemes in IoV and further research in this domain. Operational framework is presented in figure 3.1 below:

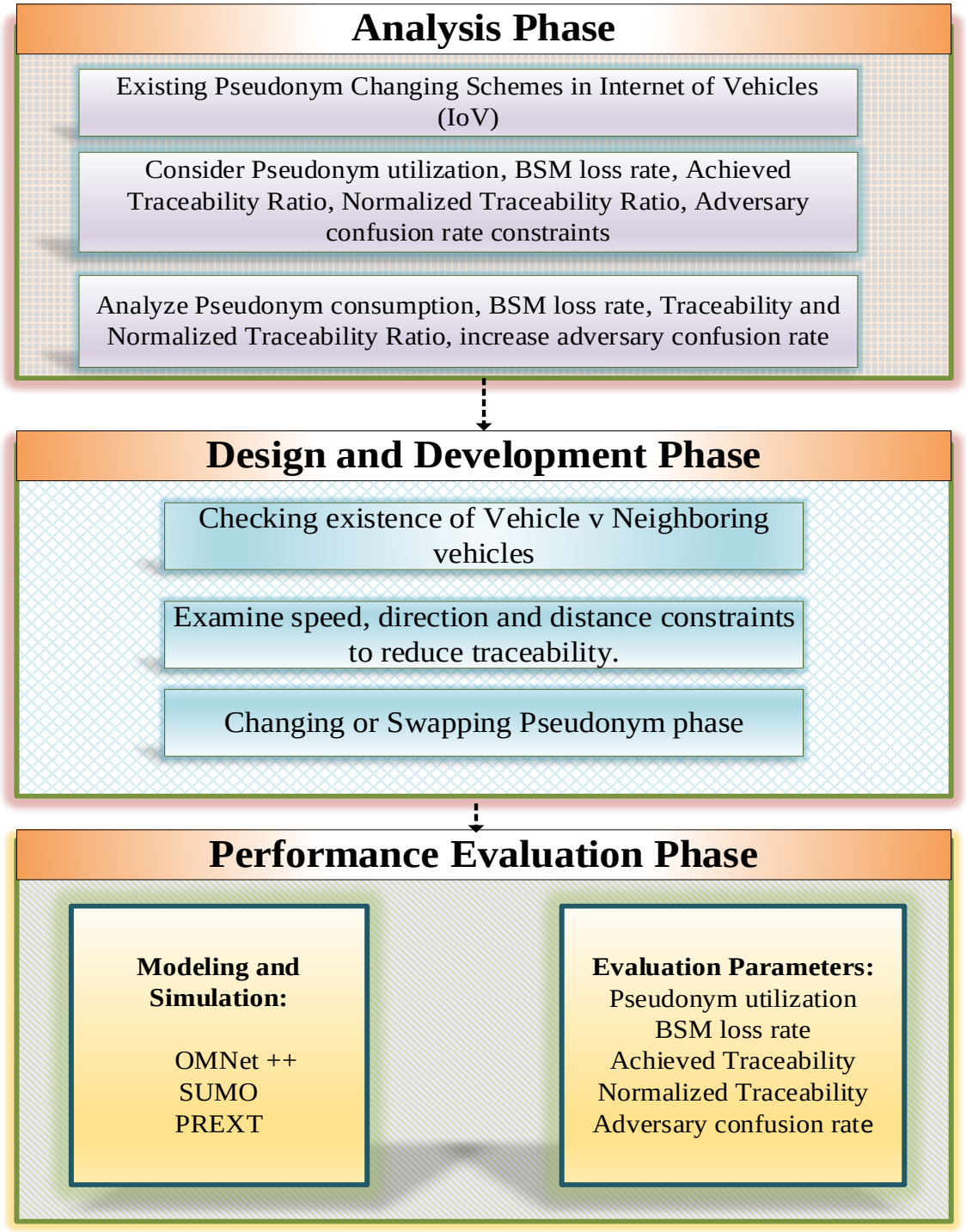

Figure 3.1: Working Outline of the Research

3.2.1 Comprehensive review of literature

The latest research Papers on vehicular security and privacy are studied, and their title, abstract, basic methodology, and summary are studied to gain an idea of the paper. About 50 papers are studied and 20 papers are most relevant. Based on the summary of those papers, the problem is identified and formulated. Papers are searched based on keywords and the latest papers are also considered from references. After studying research papers, a paragraph having an overview of the scheme along with which problem is identified and solved is written, after it a table of analysis is also created in which basic idea, mechanism, pros and cons of each paper are presented. Subsequently, analytical descriptions of schemes are presented in the form of paragraphs having the same advantages or disadvantages of schemes along with their references.

3.2.2 Problem identification

Based on the literature, the problem is identified which is mapped into the WHISPER scheme. The bad effects of the problem include high pseudonym consumption which ultimately increases communication cost while communicating TA, can increase traceability ratio by an adversary, and increase BSM loss rate. These side effects set the foundation to consider this problem and take possible steps to overcome it.

3.3 Proposed Solution

In the existing scheme WHISPER, the pseudonym changing trigger is called by just checking speed parameter which is not a sufficient parameter to adjust transmission range and send BSM. So to avoid this problem in the proposed scheme vehicles consider the neighbor's next state before pseudonym changing trigger. Vehicle v and its neighbor's speed are also taken into consideration before sending BSM. When all these conditions are fulfilled then send a BSM message to minimize adversary attack. In case there is no neighboring vehicle existing in the

vicinity of vehicle v, then in such case vehicle v changes its pseudonym after vehicle v pseudonym lifetime exceeds a specified limit.

By putting these checks, the vehicle's high pseudonym consumption is controlled at one end as well as adversary attack will not prove much successful and reduces communication cost as well.

3.4 Selection of Simulation tool

To validate the performance of the proposed protocol, Simulation method is used. For this purpose, OMNet++, SUMO and PREXT used which are built upon Veins. The reason behind selecting these tools is that they are very flexible and efficient to implement urban traffic scenarios. PREXT is an extension of Veins which helps to evaluate security metrics of a scheme and how much a scheme is secured from adversary attacks. It already contains GPA adversary that eavesdrop BSM by antennas set in range of 300m. Though there are some limitations in PREXT developed by Emara et al. PREXT is only compatible with Ubuntu version 16.o4, VEINS version 4.4, OMNet++ version 5 and SUMO version 0.25.0. To check the proposed scheme, these versions are considered.

SUMO is the best free and reliable tool for implementing traffic, road, and vehicle scenarios containing buildings and polygons to show the same setup as in the real world. SUMO is command line interface that just shows information about vehicles while SUMO-GUI contains graphical interface that contains roads, buildings of map imported from OSM and presents vehicles mobility in road like in real world scenario. OMNet++ is a network simulator and provides IDE to integrate different modules to show wired, wireless nodes communication. All these are extensions of Veins and built upon it. Veins have various extension includes SUMO, OMNet++, PREXT and many others. It allow SUMO and OMNET++ to run parallel and communicate with each other via TCP socket. When vehicles takes trip in SUMO and travels on road, it shows same scenario in OMNet++ in the form of nodes. A visual presentation of the simulation environment is shown in Figure 3.2.

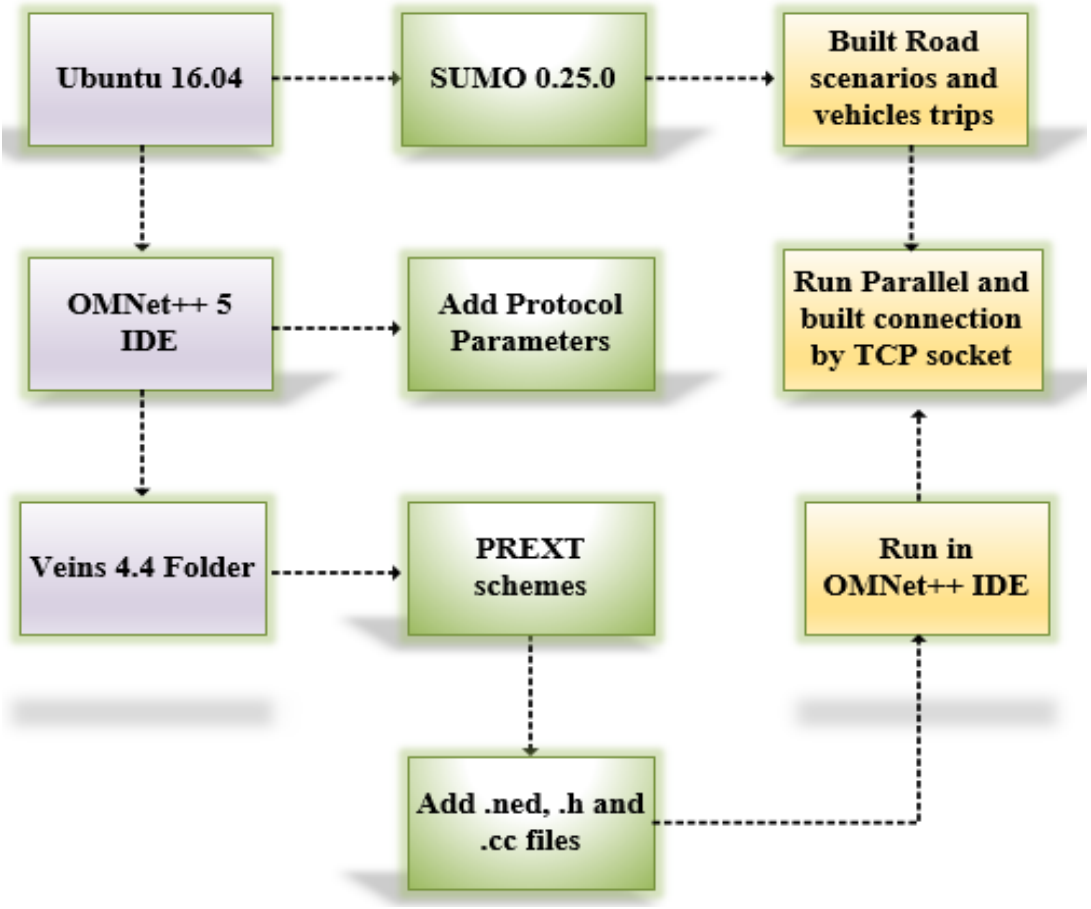

Figure 3.2: Simulation Environment

3.4.1 Evaluation Metrics

For checking the performance of the proposed protocol, different metrics that are more crucial from a security and anonymity perspective are considered. These metrics include pseudonym consumption, BSM loss rate, Percentage of attackers attaining traceability, Average confusion for adversary by pseudonym change, percentage of attackers attaining normalized traceability and proportion of vehicles changed pseudonym. Based on these metrics proposed protocol is compared to existing schemes to check efficiency. Results are presented and compared with previous schemes by graphs.

3.5 Summary

This chapter is intended to provide detailed information regarding literature review, problem identification and simulation setup. By solving this problem, security and anonymity issues are minimized and ultimately urge people to use IoV services.

CHAPTER 4

Efficient Pseudonym Consumption Protocol (EPCP)

4.1 Overview

This chapter includes proposed solution, system model of proposed scheme as well as a stepwise algorithm that aims to resolve issue of high pseudonym consumption. Each step of algorithm is also described in detail. A list of notation is listed to enhance understanding. At the end, whole chapter is also included.

4.2 Efficient Pseudonym Consumption Protocol

In internet of vehicles, vehicles share their information by BSM (basic safety message) to other vehicles for better driving experience. This BSM contains all important information of vehicle which includes velocity, speed, location and pseudonym as well. Pseudonym is basically a pair of private and public key generated by Trusted Authority (TA) and allotted to vehicles at the time of registration. Instead of using real identity, vehicles make use of pseudonym for communication with vehicles and infrastructure for increasing security. In existing studies, different schemes are presented to maintain vehicles anonymity, but in most of them pseudonym consumption is increased which has many negative impacts.

To avoid wastage of pseudonym and to make proper use of it, EPCP scheme is proposed. The proposed scheme checks the vehicle v neighboring nodes and their distance before sending pseudonym changing alert. In first phase vehicle v neighboring status is checked and if other vehicles are in general neighboring radius, it means those vehicle are nearby and considered as neighbors. Afterwards in second phase, neighbor vehicles speed and direction is checked to know vehicles is still in transmission range. In third phase, neighboring vehicles are greater than threshold value then they are allowed to change pseudonym, if less than a threshold value they will swap their pseudonym with any other vehicle randomly that exist in transmission range. If no vehicle exist in premises of general neighbor radius, in such case vehicle v pseudo lifetime is checked if it exceeds than defined lifetime then vehicle v allowed to change pseudonym.

Table 4.1: List of notations

Notation	**Abbreviation**
Tx	Transmission range
K	Number of Neighbors
GeneralNR	General Neighbor Radius
min_threshold_speed	Minimum threshold speed
max_threshold_speed	Maximum threshold speed
vehiclev_pseudolife	Vehicle v pseudonym lifetime
Neighborthreshold	Neighbor threshold value

4.3 System Model

In this unit, System model of proposed solution is explained which consists of following entities. These entities include Trusted Authority (TA), Vehicles, Location based services (LBS) and Infrastructure.

4.3.1 Trusted Authority

Trusted authority is also known as Control authority. It is governmental body and its function is to provide pseudonym to vehicles when they enter into network. At the time of entrance, vehicles are allotted with a set of valid pseudonym, it also performs function of accountability. If it receives report that any vehicle is doing suspicious activities, it cancels that vehicles credentials and inform other entities. This entity also contains link between old and new pseudonym of vehicles.

4.3.2 Vehicles

Vehicles are considered as main part of IOV environment, it is supposed that each vehicle equipped with OBU (On-Board Unit), Sensors and GPS. Vehicles can communicate with other vehicles (V2V), Vehicle to Infrastructure (V2I) for secure communication. The communication mechanism is supported by 802.11p protocol.

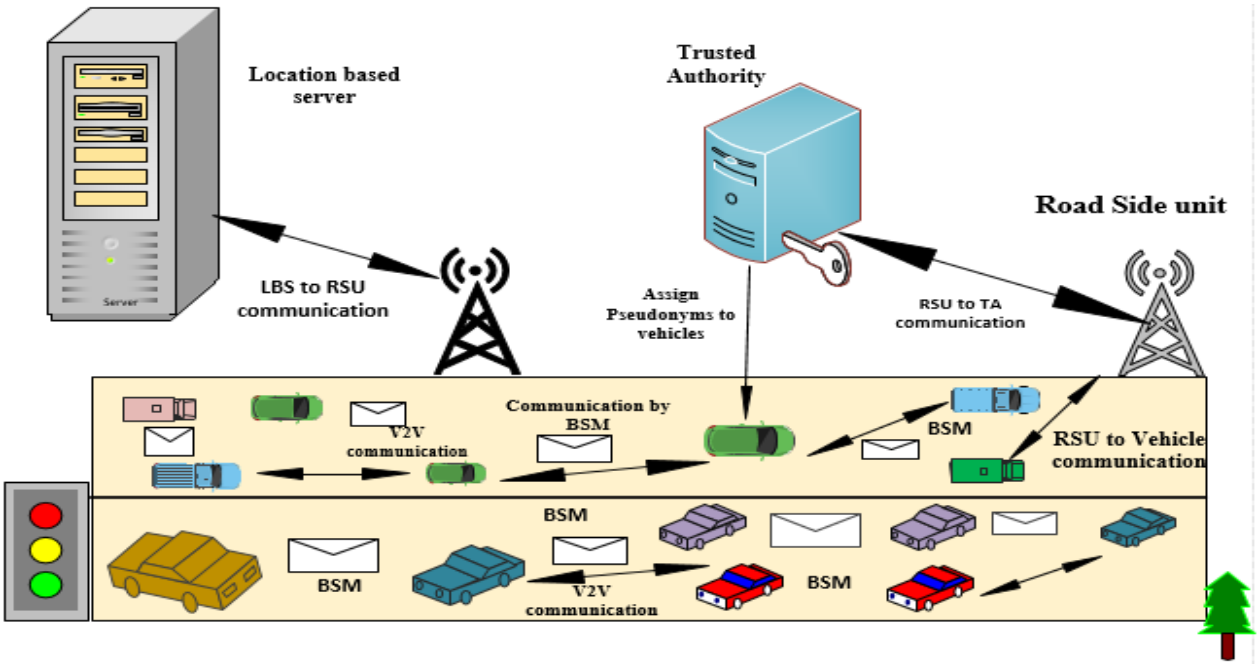

Figure 4.1: System Model

4.3.3 Location based services

When vehicles travel on road, they need to get information about right destination, LBS is considered to provide these services. When vehicles need to find location, they request to RSU, which in turn request to LBS for finding location to reach at destination.

4.3.4 Infrastructure

This entity consists of different components like RSU, towers installed at side of road. Its function is to globally monitor traffic in its transmission range. If vehicles pseudonym are insufficient, it requests to TA to provide more pseudonyms to vehicles. In case of any misbehavior done by any vehicle, it informs TA to take strict action to avoid security issues. All these entities are used for better and secure driving.

4.4 Adversary Model

An adversary is a person who wants to access vehicles BSM with intention to harm users and to observe vehicles trajectory. After receiving BSM, an adversary try to link it with vehicle's previous pseudonym to get full information.

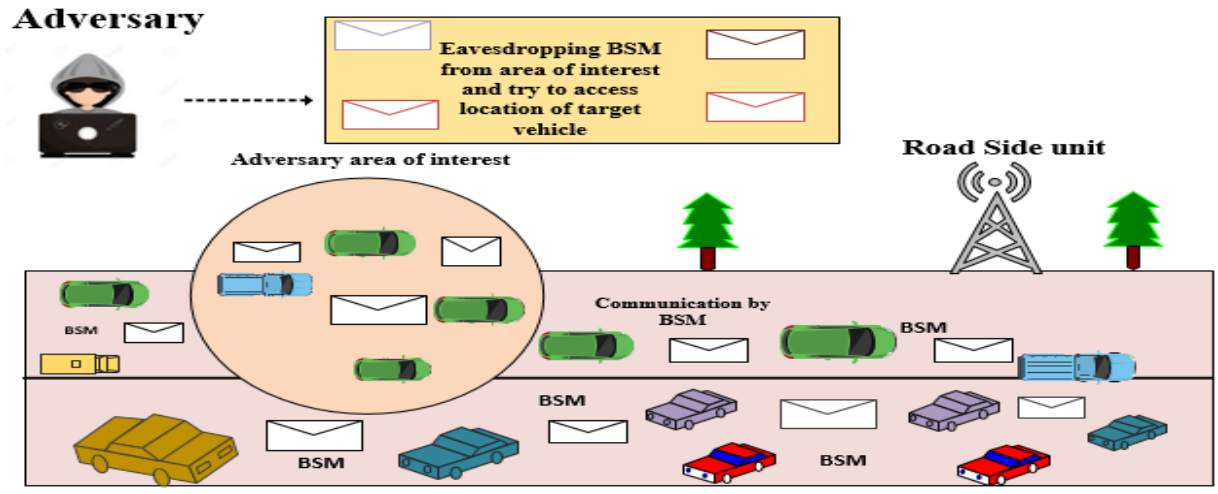

Figure 4.2: Adversary Model

For this purpose, adversary has deployed cheap eavesdropping sensors in path to access BSM. Adversary model is presented in Figure 4.2. In this research, adversary is considered as passive attacker that only check BSM but not try to modify information present in it. Attacker is considered as Global Passive Attacker (GPA) that try to intercept bacons of its own area of interest.

4.5 Flowchart of EPCP

When vehicles OBU unit is on, wait for some time known as beacon interval time, then prepare beacon safety message to send to neighbors. If neighbors are greater than specified threshold value k, by using kalman filter estimate neighbors next state and then calculate distance between new position of neighbors and current position.

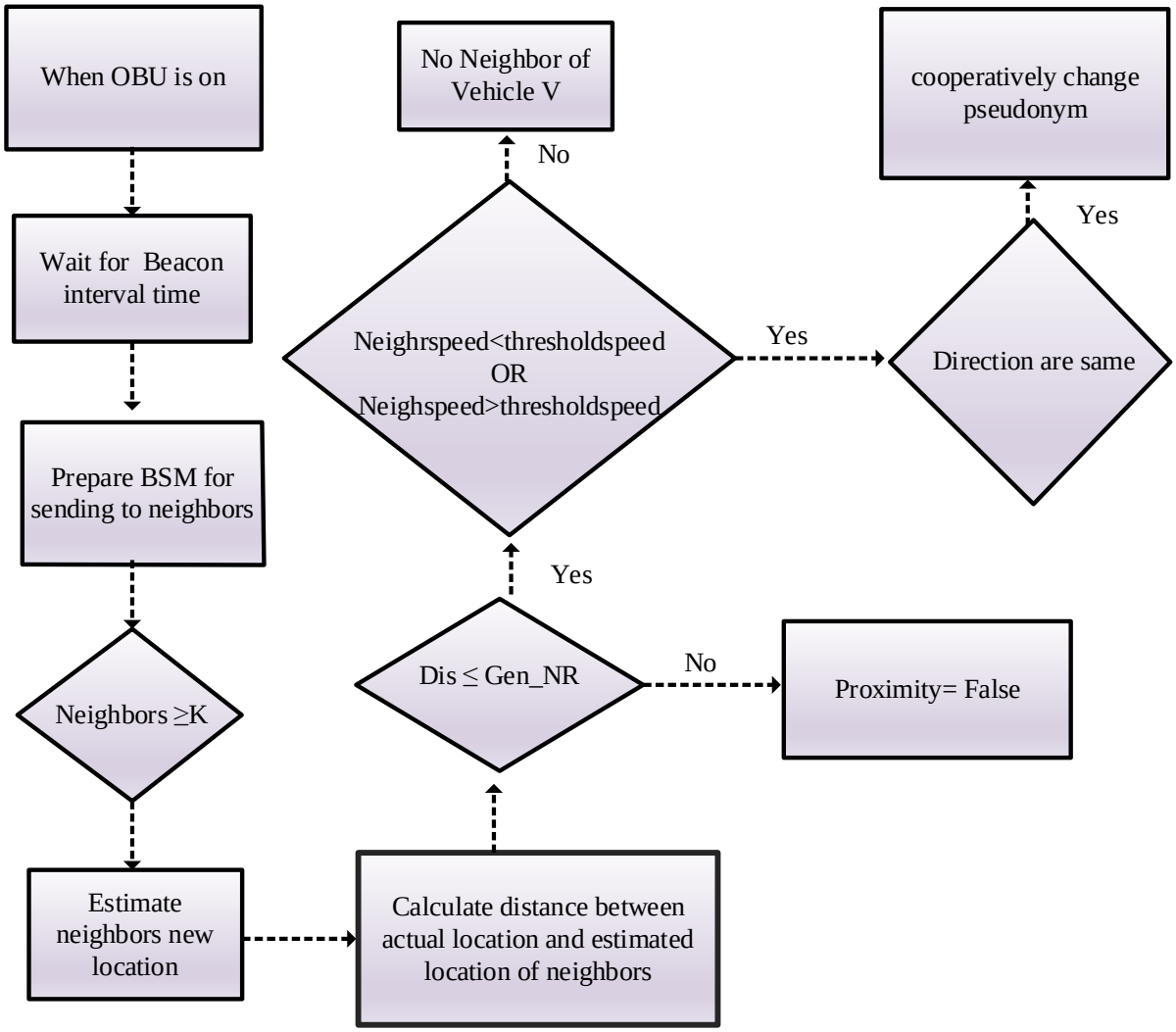

Figure 4.3: Flowchart of EPCP

If this distance lies in range of general neighbor then keep it in trust array, then further check speed parameter, if speed is less than min_threshold value or greater than max_threshold value, it means that such vehicle is not in proximity of vehicle v, if condition false it means they are near to vehicle v and cooperatively pseudonym changed. Flowchart of proposed scheme EPCP is presented in Figure 4.3.

4.6 Algorithm for Efficient Pseudonym Consumption Protocol

In step 1-7, when vehicle v receives BSM from surrounding vehicles, it checks the current position of sender vehicles and find out distance between itself and sender. If the sending vehicles lies in adjusted transmission range (T_x) of vehicle v it is considered as neighbor and neighbors are incremented. If received BSM does not lie in transmission range that vehicle is not considered as neighbor. In this case, BSM is discarded.

In step 8-17, when vehicle v intended to send BSM it is checked either onboard unit (OBU) is on for ensuring smooth communication with vehicles, afterwards it waits some time and prepare a Basic Safety Message to. Before sending BSM, neighbors are checked that send BSM in previous timeslot to vehicle v against a threshold parameter (k), if number of neighbors are greater than or equal to k, then next position of these neighboring nodes are estimated. For estimating next state, kalman filer is used. Thus it keeps in trust the beacons of all the vehicles that will be located in general neighbor radius. This allows eliminating vehicles that will move far away from this vehicle.

In step 18-32, if trust is not empty check then further neighbor vehicles speed parameter is checked against threshold minimum speed threshold or maximum speed threshold value, if this condition is true then neighbors are now out of range for vehicle v. so BSM will be delayed until neighboring vehicles exist in range. If this condition is false, it is further checked that Neighbors are moving in the same direction of vehicle v, if this condition is true further number of neighbor vehicles are checked if it is greater than or equal to Neighborthreshold value neighbors and both vehicles have readyflag=1, in this case pseudonym changed cooperatively otherwise pseudonym

will randomly swapped among vehicles in transmission range and after changing or exchanging pseudonym Readyflag bit set as zero.

In step 33-40, if trust[] is empty it means that no vehicle has fulfill the set criteria so it is assumed no neighboring vehicle exist till now. Allocated pseudonym to vehicles has limited lifetime, if vehicles current_pseudonym life span has reached the defined lifetime, vehicle v will change its pseudonym and set Readyflag bit as 0 to avoid adversary linking attack.

4.7 Summary

This chapter is intended to provide detailed description of proposed solution. Initially system model is described along all entities with detail. After it, adversary model is described. Later on, flowchart for proposed protocol EPCP is provided with description. Subsequently, algorithm for proposed solution is stated with comprehensive explanation of each step.

```
// When vehicle V Receive BSM

1.  His_pos=BSM.senderpos ();
2.  neighbor_distance=dis(my_pos, His_pos)
3.  If (neighbor_distance <=Tx) then
4.      Neighborvehicles++
5.      scan ← scan + Neighborvehicles ;
6.  Else discard BSM.
7.  End if

// When vehicle V intends to transmit BSM in next timeframe

8.  while (OnBoardUnit is on) do
9.      wait (beacon interval time)
10.     Prepare (Beacon);
11.   If (Neighborvehicles ≥ k) then
12.     neighbors_trajectories ← kalman_predict(scan);
13.     for i ← 1 to Neighbor do
14.       if (euclid(neighbors_trajectories(i).pos, actual_state.pos) < GeneralNR) then
15.       trust ← trust + neighbors_trajectories(i);
16.       End if
17.     End for
18.     if (!trust.empty()) then
19.       If (Neighbor_speed < min_threshold_speed) OR (Neighbor_speed
    max_threshold_speed) then
20.         BSM (Delay)
21.       Else
22.         His_direction=BSM.senderdirection ();
23.         If (std:: equal(my_direction, His_direction)) then
24.           If (Neighbor >=Neighborthreshold && (Neighbor (Readyflag) &&
    vehiclev_readyflag==1) then
25.             Change cooperatively pseudonym ();
26.             Readyflag=0;
27.             elseif (Neighbor < Neighborthreshold && (Neighbor (Readyflag) &&
    vehiclev_readyflag==1)
28.           Swapping of pseudonym randomly(Vi, Vj)
29.           Readyflag=0
30.         End if
31.       End if
32.     End if
33.  If (trust.empty()) then
34.     Vicinity← False      // no vehicle is in transmission range of vehicle v
35.  End if
36.  If (vehiclev_pseudolife >stable_pseudotime) then
37.    Change pseudonym ();
38.    Readyflag=0
39.  End if
40. End if
```

41. **End while**

CHAPTER 5

Performance Evaluation of Efficient Pseudonym Consumption Protocol (EPCP)

5.1 Overview

This chapter includes comparison of previous schemes with proposed technique. Analysis and results are formed by using simulation method. Evaluation is done on the basis of flaws and shortcomings of base paper algorithm with proposed algorithm. This chapter provides detailed information of simulation tools and parameters on the basis of simulation is performed and results are drawn.

5.2 Simulation tools and Environment

To investigate the performance of proposed protocol EPCP, an extensive simulation is done which consists of OMNet++, SUMO and PREXT simulator tools which is built upon VEINS. OMNet++ is used as network simulator, it is a free source and reliable simulator build on C++ library and framework used for creating network models. For checking mobility of vehicles on road as in real world scenario, Simulation of Urban Mobility (SUMO) simulator is used. SUMO is considered as reliable traffic mobility simulator, it helps in observing large traffic models. For checking some of privacy metrics, Privacy Extension-PREXT is used. PREXT is only compatible with Ubuntu operating system. PREXT, is an extension of Veins, developed by Emara et al.[59] PREXT supports changing pseudonym scenarios, a Global Passive Adversary (GPA) who tries his best to spy BSM and able to know vehicles identity. OMNet++ and SUMO has ability to run

simultaneously and communicate by TCP socket. The Pictorial representation of simulation tools are shown in Figure 5.1.

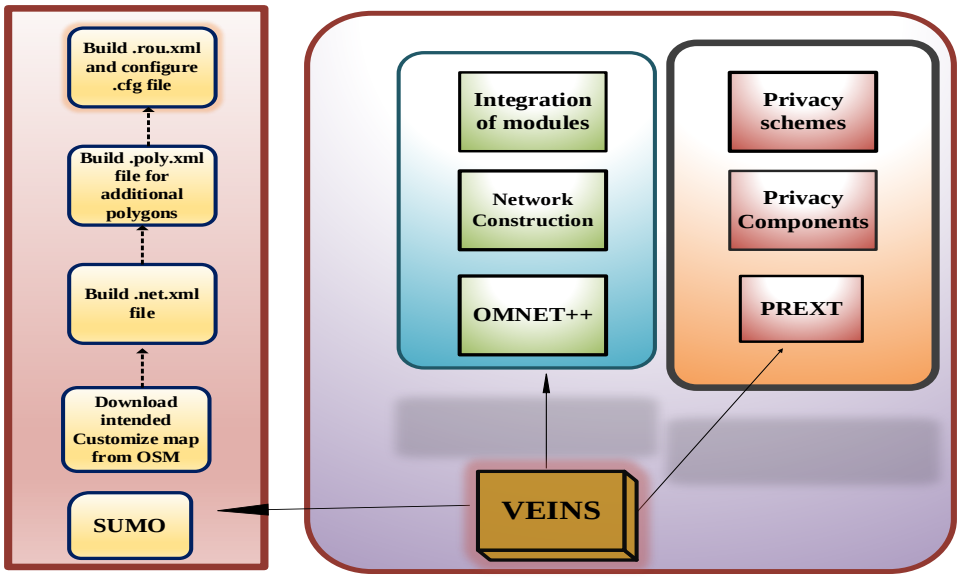

Figure 5.1: Simulation tools used in EPCP

Simulation parameters that are used to check effectiveness of proposed scheme are shown in table 5.1.

Table 5.1: Simulation parameters

Simulation Environment	
Parameters	**Values**
Number of vehicles	50,100,150,200
Transmission range	300m
Minimum speed threshold	20 m/s
Maximum speed threshold	30 m/s
Pseudonym stable time	60s

General Neighbor radius	30m
No. of neighbors (k)	1

5.3 Percentage of attacker's attains traceability

Traceability is a term referred as probability of adversary predicting target vehicles trajectory correctly by snooping BSM [51]. If vehicles trajectory is correctly identified by adversary it means that vehicles has low security. High attacker traceability is inversely proportion to vehicles anonymity. Adversary can harm driver or users of target vehicles by predicting path accurately. It is clearly seen in Figure 5.2 that EPCP has performed well comparatively CPN and WHISPER.

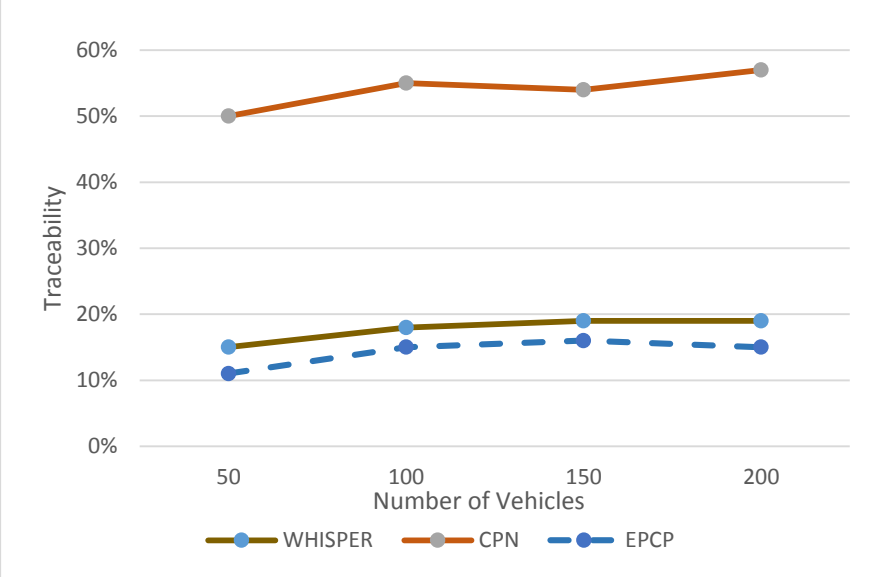

Figure 5.2: Percentage of attacker's attains traceability

In case of sparse traffic (vehicles density is up to 50), CPN attains 50% traceability range, meanwhile WHISPER lies in range of 15% to 19% and EPCP achieves traceability between 10%-

12%. In case of dense traffic (when number of vehicles are 200), CPN has considerable traceability probability lies within range of 55%-60%, WHISPER attains traceability up to 20% while proposed scheme EPCP has lower traceability lies in rage of 10-15%. CPN has highest traceability ratio while WHISPER and EPCP has lowest achieved traceability.

5.4 Percentage of attacker's attains normalized traceability

Some vehicles do not participate in process of pseudonym change and it makes easy for adversary to predict trajectory of target vehicle easily and reduces privacy level, not including them increase level of privacy, this concept is termed as normalized traceability [51]. Considering this concept, simulation is conducted and results presented in Figure 5.3 which shows that EPCP and WHISPER has much better normalized traceability relatively CPN scheme.

Under sparse traffic (when vehicles are about 50), CPN achieves normalized traceability range between 50%-55%, WHISPER get range up to 10% and proposed scheme EPCP lies within 6% to 9%. The results showed that in case of normalized traceability, EPCP and WHISPER outperformed in comparison with CPN.

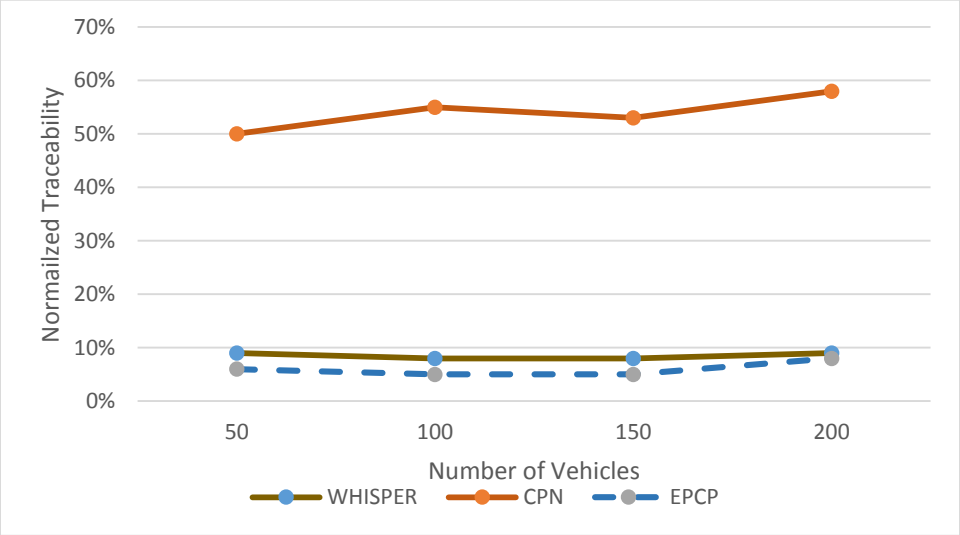

Figure 5.3: Percentage of attacker's attains normalized traceability

5.5 Pseudonym utilization

Vehicles uses pseudonym to communicate each other. A set of public and private key is allocated to vehicles by trusted authority (TA) at the time of registration. The public key is used as pseudonym. Vehicles changes its pseudonym to avoid adversary attack. Vehicles have limited pseudonym, if expired they asks trust authority through RSU to refill it. If pseudonym consumption is high it effects quality of service (QoS) and increases communication overhead. In existing schemes CPN has very high pseudonym consumption because it changes pseudonym when trigger of K neighbors is fulfilled and value of K is considered as 2. WHISPER pseudonym consumption is less than CPN but still it needs to be minimum this scheme only considers vehicles speed before checking pseudonym change. The proposed scheme EPCP has better performance as compared to both schemes because it considers both speed and direction of neighbor vehicles before changing pseudonym. In case of pseudonym utilization proposed scheme EPCP is more efficient as compared to both schemes CPN and WHISPER which is clearly shown in Figure 5.4.

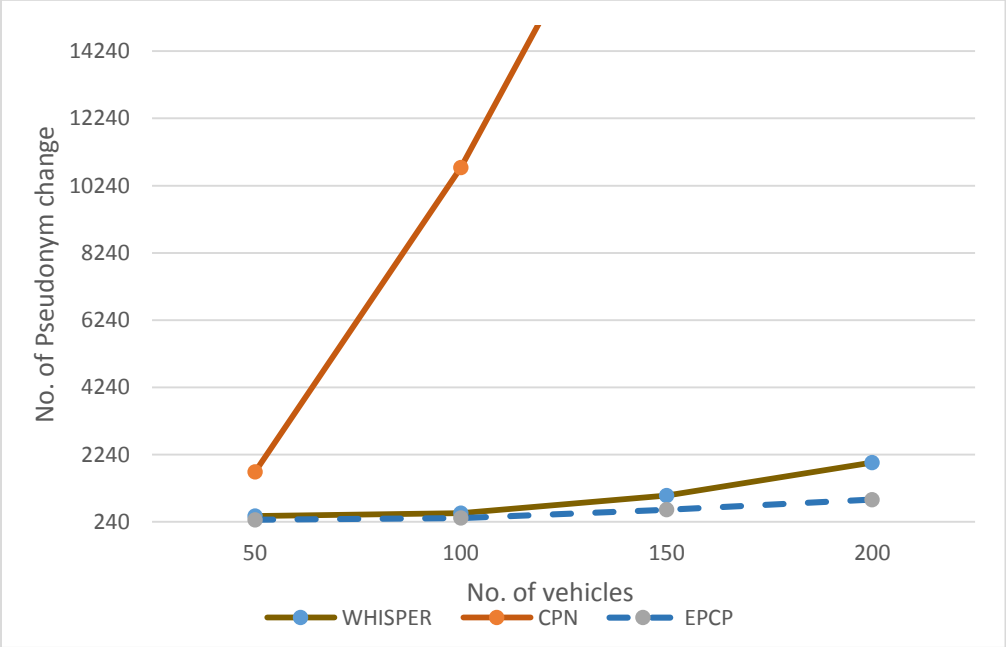

Figure 5.4: Pseudonym utilization

When vehicles density is near to 50, pseudonym consumption in CPN is 1720, while in WHISPER it is 409 and in proposed scheme EPCP it is 300. In case vehicles density is up to 200, which shows that it is dense traffic pseudonym consumption is 35000, 2000 and 900 in CPN, WHISPER and EPCP schemes respectively.

5.6 Average confusion for adversary by pseudonym change

The basic purpose of pseudonym change is to create uncertainty for adversary so that he cannot able to collect information of target vehicle. It is an important metric that is evaluated to know about how much efficient EPCP scheme in creating confusion for adversary. The results are shown in Figure. 5.5 that depicts proposed scheme EPCP has created better average confusion level for adversary. To consider real life scenario, different traffic levels (sparse, mediocre and dense) are considered to check confusion level. When there is low traffic (vehicles are considerably 50) WHISPER attains an average value of 10.2, while EPCP has an average value of 20.8. When vehicles density is mediocre (vehicles are 150 in number) WHISPER has an average value of 15.5 and EPCP has an average confusion rate is 28.5. In case of high traffic density (vehicles are up to 200), an average confusion rate for adversary remains 25.5 and 35.5 in WHIPSER and EPCP respectively.

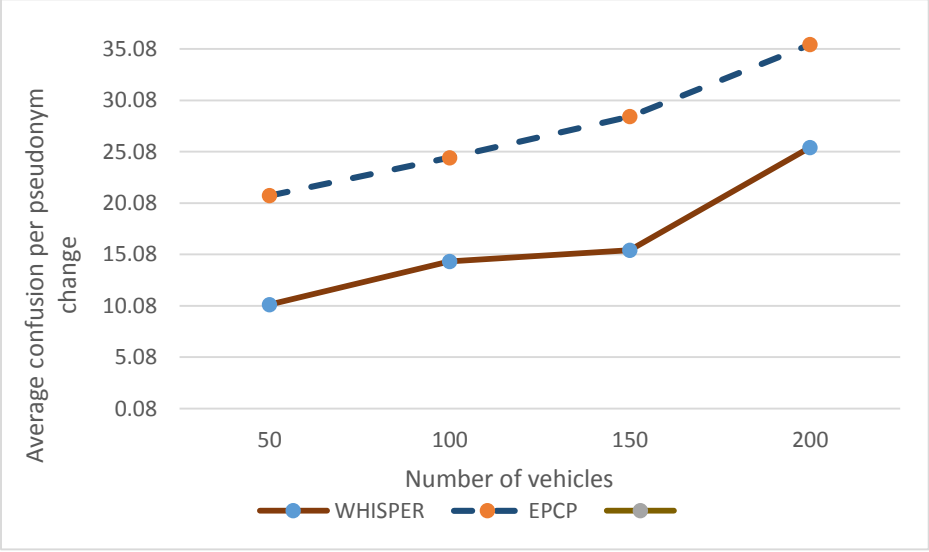

Figure 5.5: Average confusion for adversary by pseudonym change

5.7 BSM Loss Rate

Vehicles contains limited buffer to handle BSM. If a vehicle receive many unimportant beacons it may lead to delay or even loss beacons that may contain important emergency or accident relevant message, but due to full buffer of vehicle it can loss that may cause serious issues. The proposed scheme is evaluated and checked BSM loss ratio as compared to WHISPER. In general as shown in Figure. 5.6, BSM loss rate in EPCP is low than WHISPER. The X-axis represents number of vehicles while Y-axis shows packet loss rate.

BSM loss rate in WHISPER is up to 400, 2400, 12000 and 19000 with vehicles density up to 50,100, 150 and 200 respectively. The loss rate in EPCP remain up to 200, 2000, 10000 and 17000 along with traffic density 50, 100,150 and 200 in proposed scheme EPCP. The result represents that EPCP has better than WHISPER.

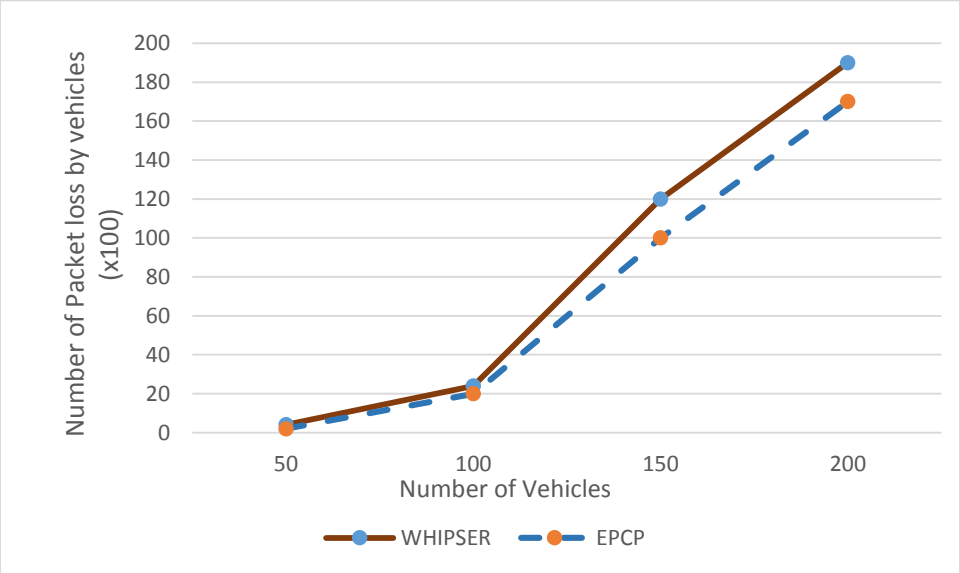

Figure 5.6: BSM loss rate

5.8 Proportion of vehicles changed pseudonym

When vehicles changes their pseudonym, some such vehicles exist that do not willing to change their pseudonym and do not participate in this process. Such vehicles are termed as selfish

nodes[57]. Selfish nodes reduces the location confidentiality level that increases chances of adversary tracking.

Proposed scheme EPCP has stable proportion of vehicles that changed their pseudonym under different vehicles density. When vehicles density is up to 50, 100, 150 and 200, ratio of vehicles that have changed their pseudonym lies in range of 80%, 83%, 84% and 85 respectively. In case of WHISPER scheme ratio remains 75%, 80%, 83% and 83% under traffic density of 50,100, 150 and 200 respectively. In case of EPCP, the ratio of vehicles that have changed their pseudonym remains stable under sparse to dense traffic situation and succeeded in maintaining vehicles location anonymous to avoid adversary attack. Figure 5.7 shows graph scenario that represents propose scheme has better result than WHISPER.

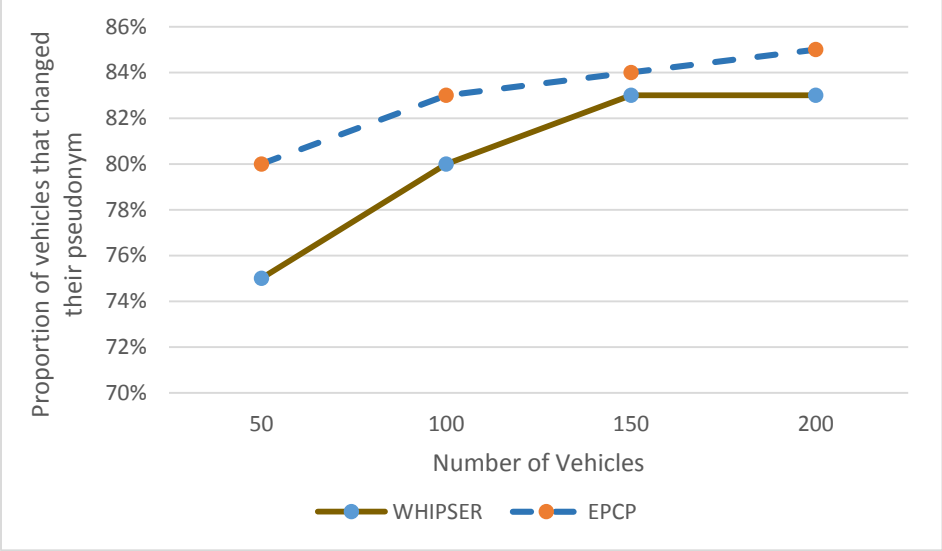

Figure 5.7: Proportion of vehicles changed pseudonym

5.9 Summary

In this chapter, Proposed Scheme EPCP is compared with some other schemes and presented the results in the form of graphs. For comparison, different important evaluation metrics

are considered including BSM loss rate, pseudonym utilization, vehicles proportion of changing pseudonym, traceability and normalized traceability. Evaluation is done by setting simulation environment in SUMO, OMNet++ and PREXT which are built on VEINS. The compatible version are selected to avoid any problem. The results showed that EPCP performed better than WHISPER and CPN.

CHAPTER 6

CONCLUSION AND FUTURE WORK

6.1 Overview

This chapter provides conclusion of research work and future work. The basic purpose of this research is to control pseudonym consumption and reduce traceability by adversary to increase vehicles anonymity. To analyze the performance of proposed scheme EPCP, simulation is used. The performance of proposed scheme is analyzed by using SUMO, OMNET++ and PREXT by considering different metrics including Pseudonym consumption, Achieved Traceability, Normalized Traceability, BSM loss rate and confusion rate by adversary. By comparing with previous schemes, results showed that EPCP performed better.

6.2 Summary of Research work

Internet of vehicles is an innovative technology that makes travelling safe and reduces road accidents by communicating using BSM. This timely BSM communication lessens road accidents because BSM contains all important information that are shared with surrounding vehicles. Different safety and non-safety applications of IoV bring ease for mankind. Besides these advantages, there is constant security threat if an adversary spies BSM and uses it to harm people. These security issues may cause hesitation among people to use services of IoV. To resolve issue of security and maintaining vehicles anonymity, several researchers provided different schemes

some of them are mix-context and some of them belong to category of mix-zone. Some of the schemes have high pseudonym consumption which ultimately increases communication overhead. By considering this issue, Efficient Pseudonym Consumption Protocol (EPCP) is presented. EPCP is a mix context scheme that checks number of neighboring vehicles, their next state and speed before sending pseudonym changing information. These checks help in reducing pseudonym consumption and reduce traceability. To evaluate the performance of proposed scheme EPCP, simulation method is used. For this purpose, OMNet++, SUMO and PREXT simulators are used. Furthermore, different evaluation metrics are considered including attacker's attains traceability, normalized traceability, Pseudonym utilization, and Average confusion for adversary by pseudonym change, BSM loss rate and Proportion of vehicles changed pseudonym. For checking efficiency of EPCP scheme, it is compared with WHISPER and CPN scheme.

6.3 Future Work

In the future, encouraging selfish nodes to participate in pseudonym changing mechanism will be introduced to enhance effectiveness of proposed scheme. Besides this, some other evaluation metrics including total transmitted BSM, TA to RSU 2-way communication cost and impact of high or low anonymity set on adversary traceability will be considered, a part from this the proposed scheme EPCP is compared with some other latest robust anonymity schemes are some of our future strategies.

REFERENCES

[1] J. A. Fadhil and Q. I. Sarhan, “Internet of Vehicles (IoV): A Survey of Challenges and Solutions,” *Proc. - 2020 21st Int. Arab Conf. Inf. Technol. ACIT 2020*, pp. 1–10, 2020, doi: 10.1109/ACIT50332.2020.9300095.

[2] 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, doi: 10.1109/ACCESS.2020.2992580.

[3] S. Sharma and B. Kaushik, “A survey on internet of vehicles: Applications, security issues & solutions,” *Veh. Commun.*, vol. 20, no. 100182, pp. 100182, 2019, doi: 10.1016/j.vehcom.2019.100182.

[4] T. Garg, N. Kagalwalla, P. Churi, A. Pawar, and S. Deshmukh, “A survey on security and privacy issues in IoV,” *Int. J. Electr. Comput. Eng.*, vol. 10, no. 5, pp. 5409–5419, 2020, doi: 10.11591/IJECE.V10I5.PP5409-5419.

[5] J. Contreras-Castillo, S. Zeadally, and J. A. Guerrero-Ibanez, “Internet of Vehicles: Architecture, Protocols, and Security,” *IEEE Internet Things J.*, vol. 5, no. 5, pp. 3701–3709, 2018, doi: 10.1109/JIOT.2017.2690902.

[6] J. Wang, Y. Shao, Y. Ge, and R. Yu, “A survey of vehicle to everything (V2X) testing,” *Sensors (Switzerland)*, vol. 19, no. 2, pp. 334, 2019, doi: 10.3390/s19020334.

[7] O. Kaiwartya *et al.*, “Internet of Vehicles: Motivation, Layered Architecture, Network Model, Challenges, and Future Aspects,” *IEEE Access*, vol. 4, pp. 5356–5373, 2016, doi: 10.1109/ACCESS.2016.2603219.

[8] H. Talat, T. Nomani, M. Mohsin, and S. Sattar, “A Survey on Location Privacy Techniques Deployed in Vehicular Networks,” *Proc. 2019 16th Int. Bhurban Conf. Appl. Sci. Technol. IBCAST 2019*, pp. 604–613, 2019, doi: 10.1109/IBCAST.2019.8667248.

[9] B. Ji *et al.*, “Survey on the Internet of Vehicles: Network Architectures and Applications,” *IEEE Commun. Stand. Mag.*, vol. 4, no. 1, pp. 34–41, 2020, doi:

10.1109/MCOMSTD.001.1900053.

[10] S. Khan, I. Sharma, M. Aslam, M. Z. Khan, and S. Khan, “Security challenges of location privacy in vanets and state-of-the-art solutions: A survey,” *Futur. Internet*, vol. 13, no. 4, pp. 96, 2021, doi: 10.3390/fi13040096.

[11] G. Karagiannis *et al.*, “Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions,” *IEEE Commun. Surv. Tutorials*, vol. 13, no. 4, pp. 584–616, 2011, doi: 10.1109/SURV.2011.061411.00019.

[12] R. Gasmi and M. Aliouat, “Vehicular Ad Hoc NETworks versus Internet of Vehicles-A Comparative View,” *Proc. - ICNAS 2019 4th Int. Conf. Netw. Adv. Syst.*, pp. 1–6, 2019, doi: 10.1109/ICNAS.2019.8807870.

[13] M. Garip *et al.*, “BOTVEILLANCE : A Vehicular Botnet Surveillance Attack against Pseudonymous Systems in VANETs,” *11th IFIP Wirel. Mob. Netw. Conf.*, pp. 1–8, 2019.

[14] Z. Afzal and M. Kumar, “Security of Vehicular Ad-Hoc Networks (VANET): A survey,” *J. Phys. Conf. Ser.*, vol. 1427, no. 1, pp. 012015, 2020, doi: 10.1088/1742-6596/1427/1/012015.

[15] W. Liang, Z. Li, H. Zhang, S. Wang, and R. Bie, “Vehicular Ad Hoc networks: Architectures, research issues, methodologies, challenges, and trends,” *Int. J. Distrib. Sens. Networks*, vol. 11, no. 8, pp. 745303, 2015, doi: 10.1155/2015/745303.

[16] J. A. Fadhil and Q. I. Sarhan, “Internet of Vehicles (IoV): A Survey of Challenges and Solutions,” *Proc. - 2020 21st Int. Arab Conf. Inf. Technol. ACIT 2020*, pp. 1–10, 2020, doi: 10.1109/ACIT50332.2020.9300095.

[17] A. Boualouache, S. M. Senouci, and S. Moussaoui, “A Survey on Pseudonym Changing Strategies for Vehicular Ad-Hoc Networks,” *IEEE Commun. Surv. Tutorials*, vol. 20, no. 1, pp. 770–790, 2018, doi: 10.1109/COMST.2017.2771522.

[18] L. Buttyán, T. Holczer, A. Weimerskirch, and W. Whyte, “SLOW: A practical pseudonym changing scheme for location privacy in VANETs,” *2009 IEEE Veh. Netw. Conf. VNC 2009*, pp. 1–8, 2009, doi: 10.1109/VNC.2009.5416380.

[19] M. A. Ferrag, L. Maglaras, and A. Ahmim, “Privacy-Preserving Schemes for Ad Hoc Social Networks: A Survey,” *IEEE Commun. Surv. Tutorials*, vol. 19, no. 4, pp. 3015–3045, 2017, doi: 10.1109/COMST.2017.2718178.

[20] M. S. Talib, A. Hassan, B. Hussin, and A. A. H. Hassan, “Vehicular Ad-hoc networks: Current challenges and future direction of research,” *J. Adv. Res. Dyn. Control Syst.*, vol. 10, no. 2, pp. 2065–2074, 2018.

[21] M. Babaghayou, N. Labraoui, A. A. A. Ari, M. A. Ferrag, L. Maglaras, and H. Janicke, “Whisper: A location privacy-preserving scheme using transmission range changing for internet of vehicles,” *Sensors*, vol. 21, no. 7, pp. 2443, 2021, doi: 10.3390/s21072443.

[22] J. Liang, M. S. Sheikh, and W. Wang, “A survey of security services, attacks, and applications for vehicular ad hoc networks (VANETs),” *Sensors (Switzerland)*, vol. 19, no. 16, pp. 3589, 2019, doi: 10.3390/s19163589.

[23] F. Zidani, F. Semchedine, and M. Ayaida, “Estimation of Neighbors Position privacy scheme with an Adaptive Beaconing approach for location privacy in VANETs,” *Comput. Electr. Eng.*, vol. 71, no.17, pp. 359–371, 2018, doi: 10.1016/j.compeleceng.2018.07.040.

[24] J. H. Song, V. W. S. Wong, and V. C. M. Leung, “Wireless location privacy protection in vehicular Ad-Hoc networks,” *Mob. Networks Appl.*, vol. 15, no. 1, pp. 160–171, 2010, doi: 10.1007/s11036-009-0167-4.

[25] A. Wahid, H. Yasmeen, M. A. Shah, and M. Alam, “Holistic approach for coupling privacy with safety in VANETs,” *Comput. Networks*, vol. 148, pp. 214–230, 2019, doi: 10.1016/j.comnet.2018.08.017.

[26] M. Babaghayou, N. Labraoui, A. Adamou, A. Ari, and N. Lagraa, “Pseudonym change-based privacy-preserving schemes in vehicular ad-hoc networks : A survey,” *J. Inf. Secur. Appl.*, vol. 55, no. 102618, pp. 102618, 2020.

[27] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen, “Pseudonym changing at social spots: An effective strategy for location privacy in VANETs,” *IEEE Trans. Veh. Technol.*, vol. 61, no. 1, pp. 86–96, 2012, doi: 10.1109/TVT.2011.2162864.

[28] M. Z. Khan, O. H. Alhazmi, M. A. Javed, H. Ghandorh, and K. S. Aloufi, “Reliable

internet of things: Challenges and future trends," *Electron.*, vol. 10, no. 19, pp. 2377, 2021, doi: 10.3390/electronics10192377.

[29] F. B. Günay, E. Öztürk, T. Çavdar, Y. S. Hanay, and A. ur R. Khan, "Vehicular Ad Hoc Network (VANET) Localization Techniques: A Survey," *Arch. Comput. Methods Eng.*, vol. 28, no. 4, pp. 3001–3033, 2021, doi: 10.1007/s11831-020-09487-1.

[30] T. Yeferny and S. Hamad, "Vehicular Ad-hoc Networks: Architecture, Applications and Challenges," *IJCSNS Int. J. Comput. Sci. Netw. Secur.*, vol. 20, no. 2, pp. 1–7, 2020.

[31] Z. Wu, S. Jiang, and L. Wang, "Resilient Data Retrieval in Vehicular Named Data Networking," *Proc. - 2020 Int. Conf. Netw. Netw. Appl. NaNA 2020*, pp. 464–469, 2020, doi: 10.1109/NaNA51271.2020.00085.

[32] I. Ullah, M. A. Shah, A. Khan, C. Maple, and A. Waheed, "Virtual pseudonym-changing and dynamic grouping policy for privacy preservation in vanets," *Sensors*, vol. 21, no. 9, pp. 3077, 2021, doi: 10.3390/s21093077.

[33] L. Huang, K. Matsuura, H. Yamanet, and K. Sezaki, "Enhancing wireless location privacy using silent period," *IEEE Wirel. Commun. Netw. Conf. WCNC*, vol. 2, April 2005, pp. 1187–1192, 2005, doi: 10.1109/WCNC.2005.1424677.

[34] M. S. Alencar and V. C. Da Rocha, "Communication systems," *Commun. Syst.*, pp. 1–416, 2022, doi: 10.1007/b138483.

[35] S. Abbasi, A. M. Rahmani, A. Balador, and A. Sahafi, "Internet of Vehicles: Architecture, services, and applications," *Int. J. Commun. Syst.*, vol. 34, no. 10, pp. 1–31, 2021, doi: 10.1002/dac.4793.

[36] I. Ullah, M. A. Shah, A. Khan, C. Maple, A. Waheed, and G. Jeon, "A distributed mix-context-based method for location privacy in road networks," *Sustain.*, vol. 13, no. 22, pp. 1–32, 2021, doi: 10.3390/su132212513.

[37] X. Li *et al.*, "PAPU: Pseudonym Swap with Provable Unlinkability Based on Differential Privacy in VANETs," *IEEE Internet Things J.*, vol. 7, no. 12, pp. 11789–11802, doi: 10.1109/JIOT.2020.3001381.

[38] A. Boualouache and S. Moussaoui, “TAPCS: Traffic-aware pseudonym changing strategy for VANETs,” *Peer-to-Peer Netw. Appl.*, vol. 10, no. 4, pp. 1008–1020, 2017, doi: 10.1007/s12083-016-0461-4.

[39] P. K. Singh, S. N. Gowtham, T. S, and S. Nandi, “CPESP: Cooperative Pseudonym Exchange and Scheme Permutation to preserve location privacy in VANETs,” *Veh. Commun.*, vol. 20, no. 100183, pp. 100183, 2019, doi: 10.1016/j.vehcom.2019.100183.

[40] I. Ullah, A. Wahid, M. A. Shah, and A. Waheed, “VBPC: Velocity based pseudonym changing strategy to protect location privacy of vehicles in VANET,” *2017 Int. Conf. Commun. Technol.*, pp. 132–137, 2017.

[41] A. Boualouache and S. Moussaoui, “Urban pseudonym changing strategy for location privacy in VANETs,” *Int. J. Ad Hoc Ubiquitous Comput.*, vol. 24, no. 1–2, pp. 49–64, 2017, doi: 10.1504/IJAHUC.2017.080914.

[42] J. Yang, C. Huang, and X. Fan, “Reliable security mechanism for pseudonym change in urban vehicular ad hoc networks,” *IET Intell. Transp. Syst.*, vol. 13, no. 9, pp. 1383–1393, 2019, doi: 10.1049/iet-its.2018.5484.

[43] Y. Li, Y. Yin, X. Chen, J. Wan, G. Jia, and K. Sha, “A Secure Dynamic Mix Zone Pseudonym Changing Scheme Based on Traffic Context Prediction,” *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 7, pp. 9492–9505, 2022, doi: 10.1109/TITS.2021.3125744.

[44] W. Bouksani and B. A. Bensaber, “RIN: A dynamic pseudonym change system for privacy in VANET,” *Concurr. Comput. Pract. Exp.*, vol. 31, no. 24, pp. e4719, 2019, doi: 10.1002/cpe.4719.

[45] B. Ying, D. Makrakis, and H. T. Mouftah, “Dynamic mix-zone for location privacy in vehicular networks,” *IEEE Commun. Lett.*, vol. 17, no. 8, pp. 1524–1527, 2013, doi: 10.1109/LCOMM.2013.070113.122816.

[46] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, “AMOEBA: Robust location privacy scheme for VANET,” *IEEE J. Sel. Areas Commun.*, vol. 25, no. 8, pp. 1569–1589, 2007, doi: 10.1109/JSAC.2007.071007.

[47] A. Boualouache, S. M. Senouci, and S. Moussaoui, “Towards an efficient pseudonym

management and changing scheme for vehicular ad-hoc networks," *Proc. 2016 IEEE Glob. Commun. Conf. GLOBECOM 2016* , pp. 1–7, 2016, doi: 10.1109/GLOCOM.2016.7842339.

[48] Y. Pan and J. Li, "Cooperative pseudonym change scheme based on the number of neighbors in VANETs," *J. Netw. Comput. Appl.*, vol. 36, no. 6, pp. 1599–1609, 2013, doi: 10.1016/j.jnca.2013.02.003.

[49] L. Benarous, B. Kadri, S. Bitam, and A. Mellouk, "Privacy-preserving authentication scheme for on-road on-demand refilling of pseudonym in VANET," *Int. J. Commun. Syst.*, vol. 33, no. 10, pp. e4087, 2020, doi: 10.1002/dac.4087.

[50] L. Benarous, seS. Bitam, and A. Mellouk, "CSLPPS: Concerted Silence-Based Location Privacy Preserving Scheme for Internet of Vehicles," *IEEE Trans. Veh. Technol.*, vol. 70, no. 7, pp. 7153–7160, 2021, doi: 10.1109/TVT.2021.3088762.

[51] K. Emara, W. Woerndl, and J. Schlichter, "Context-based Pseudonym Changing Scheme for Vehicular Adhoc Networks," pp. 13, 2016, [Online]. Available: http://arxiv.org/abs/1607.07656

[52] H. Mistareehi, T. Islam, and D. Manivannan, "A secure and distributed architecture for vehicular cloud," *Internet of Things (Netherlands)*, vol. 13, no. 100355, pp. 100355, 2021, doi: 10.1016/j.iot.2020.100355.

[53] M. Yang, Y. Feng, X. Fu, and Q. Qian, "Location privacy preserving scheme based on dynamic pseudonym swap zone for Internet of Vehicles," *Int. J. Distrib. Sens. Networks*, vol. 15, no. 7, pp. 1550147719865508, 2019, doi: 10.1177/1550147719865508.

[54] Z. Zhang, T. Feng, B. Sikdar, and W. C. Wong, "A Flickering Context-based Mix Strategy for Privacy Protection in VANETs," *IEEE Int. Conf. Commun.*, pp. 6, 2021, doi: 10.1109/ICC42927.2021.9500880.

[55] I. Ullah, M. A. Shah, and A. Khan, "Adaptive Grouping and Pseudonym Changing Policy for Protection of Vehicles Location Information in VANETs," *Proc. 2021 IEEE Symp. Ser. Comput. Intell. SSCI 2021* , pp. 1–7, 2021, doi: 10.1109/SSCI50451.2021.9659852.

[56] K. Emara, W. Woerndl, and J. Schlichter, "CAPS: Context-aware privacy scheme for

VANET safety applications," *Proc. 8th ACM Conf. Secur. Priv. Wirel. Mob. Networks, WiSec 2015*, pp. 12, 2015, doi: 10.1145/2766498.2766500.

[57] B. Ying and D. Makrakis, "Reputation-based Pseudonym Change for Location Privacy in vehicular networks," *IEEE Int. Conf. Commun.*, vol. 10, pp. 7041–7046, 2015, doi: 10.1109/ICC.2015.7249449.

[58] I. Shaleesh, A. Almohammedi, N. Mohammad, A. Ahmad, and V. Shepelev, "Cooperation and radio silence strategy in Mix Zone to Protect Location Privacy of Vehicle in VANET," *Tikrit J. Eng. Sci.*, vol. 28, no. 1, pp. 31–39, 2021, doi: 10.25130/tjes.28.1.04.

[59] K. Emara, "Poster: PREXT: Privacy extension for Veins VANET simulator," *IEEE Veh. Netw. Conf. VNC*, December 2016, pp. 1–2, 2016, doi: 10.1109/VNC.2016.7835979.