LOCATION PRIVACY AND HIDING USING PSEUDONYM SWAPPING ZONE

By

AYESHA FARID

NATIONAL UNIVERSITY OF MODERN LANGUAGES

ISLAMABAD

9 October, 2024

LOCATION PRIVACY AND HIDING USING PSEUDONYM SWAPPING ZONE

By

AYESHA FARID

MCS, Fatima Jinnah Women University, 2016

A THESIS SUBMITTED IN PARTIAL FULFILMENT OF
THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE

In **Computer Science**

To

FACULTY OF ENGINEERING & COMPUTING

NATIONAL UNIVERSITY OF MODERN LANGUAGES ISLAMABAD

THESIS AND DEFENSE APPROVAL FORM

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

Thesis Title: Location Privacy And Hiding Using Pseudonym Swapping Zone

Submitted By: Ayesha Farid **Registration #:** 69 MS/CS/S22

Master of Science in Computer Science (MSCS)
Degree Name in Full

Computer Science
Name of Discipline

Dr. Ata Ullah
Research Supervisor — Signature of Research Supervisor

Research Co-Supervisor — Signature of Research Co-Supervisor

Dr. Fazli Subhan
Head of Department (CS) — Signature of HoD (CS)

Dr. M. Noman Malik
Name of Dean (FEC) — Signature of Dean (FEC)

October 9th, 2024

AUTHOR'S DECLARATION

I Ayesha Farid

Daughter of Ghulam Farid

Registration # 69 MS/CS/S22

Discipline Computer Science

Candidate of **Master of Science in Computer Science (MSCS)** at the National University of Modern Languages do hereby declare that the **Location Privacy and Hiding Using Pseudonym Swapping Zone** 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 canceled and the degree revoked.

Signature of Candidate

Ayesha Farid

Name of Candidate

October 9th, 2024

Date

ABSTRACT

Title: Location Privacy and Hiding Using Pseudonym Swapping Zone

The Internet of Vehicles (IoV) is a growing technology that enables seamless communication among vehicles, pedestrians, On-Board Units (OBU), cloud platforms, and Road Side Units (RSU) as vehicles travels. This Intelligent Transport System (ITS) has significantly bolstered road safety, resulting in a marked reduction in road accidents. On one side it offers various advantages but at the same time security issues affects its utility. The proposed Mutual Reporting based Pseudonym Swapping Zone protocol (MR-PSZ) addresses critical challenges in the Internet of Vehicles (IoV), focusing on securing data privacy and efficient pseudonym swap. MR-PSZ introduces an approach where vehicles can exchange pseudonyms in designated zones, enhancing location privacy and minimizing the risk of information exposure to potential attackers. This protocol's main phases include Vehicle Registration, Pseudonym Update, and Pseudonym Swapping, each contributing to the overall goal of improving security and privacy in vehicular communication. The pseudonym swapping phase involves a carefully orchestrated process, ensuring that vehicles can exchange pseudonyms securely in specified areas called pseudonym swapping zones and maintain location privacy. The protocol also considers conditions for successful pseudonym swapping, such as continuous connected time between vehicles and dimension of the pseudonym exchange region. Additionally, proposed scheme emphasizes importance of uploading pseudonym swap logs to the CA after each exchange, enabling the CA to update mappings between real identities and pseudonyms. The proposed scheme is simulated by using SUMO and PREXT tools, the results shows high improvement in terms of anonymity and lowers chances of tracking. The proposed scheme has attained lower attack probability of 10%, followed by 25% by Slotswap, 17% by DPSZ, 55% by PSNV and 62% by DMLP. Similarly during high speed, the traceability factor is reduced to 11.11%, 42.8%, 38.4% and 69.2% than DPSZ, PSNV, SlotSwap and DMLP. During sparse traffic the traceability by adversary is reduced to 23%, 44.4%, 64.28% and 60% than DPSZ, PSNV, SlotSwap and DMLP. Overall, the MR-PSZ protocol contributes in enhancing vehicular network security ensuring data privacy through continuous pseudonym updates, and maintaining data integrity with secure communication and reliable logging. It effectively prevents long-term tracking and unauthorized data tampering, fostering a trustworthy and private vehicular communication environment. This contributes to the advancement of secure, anonymous, and accountable vehicular networks.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

VANET	-	Vehicular Ad-hoc Network
ITS	-	Intelligent Transport System
V2V	-	Vehicle to Vehicle
IoV	-	Internet of Vehicles
RSU	-	Road Side Unit
QoS	-	Quality of Service
CA	-	Central Authority
TA	-	Trusted Authority
PID	-	Pseudonym Identity
BSM	-	Basic Safety Message
VS	-	Vehicle Subnet
SI	-	Service Infrastructure
TCP	-	Transmission Control Protocol
RFID	-	Radio Frequency Identification
GH	-	Group Head
SUMO	-	Simulation of Urban Mobility
CAM	-	Cooperation Awareness Mechanism
ITS	-	Intelligent Transport System
WAVE	-	Wireless Access in Vehicular Environments

LIST OF SYMBOLS

ϕ_1	-	A set of vehicles currently in the swap zone.
Ψ_1	-	The collection of vehicles that are eligible for pseudonym swapping
$\in$	-	For every vehicle v_n in the swap zone ϕ_1
ε	-	Attack strength of the attacker
T_S	-	A size threshold
T_t	-	A time threshold
Cert	-	Used for Certification Authority

ACKNOWLEDGMENT

In the name of Allah, the most Gracious, the most Merciful and the most Beneficent. I am thankful to Almighty Allah for giving me strength and blessed me with all kind of needs to complete my thesis. I would love to offer my heartiest praises to the Prophet Muhammad (PBH), 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 am thankful, from the depth of my heart for his supervision, continuous support and precious pieces of advice, without his efforts, this dissertation would not even be anywhere near to possible. I believe he put his best to make my efforts into a success. It is only because of his insight, enthusiasm, and continuous encouragement which helped me to complete this task. I express my deepest gratitude to all the faculty member and administration of Department of Computer Science. For all whom I did not mention but I shall not neglect their significant contribution, thanks for everything.

I would also like to thanks my parents, Mr. Ghulam Farid and Mrs. Shafqat Bibi, because without them I am nothing, both of them are very important part of my life and a driving force for me to find positive ways for existence and to achieve goals. They are the reason behind all of my success and learning.My parents are my mentors. I would like to special thanks to my husband Qazi Ali Raza, my daughter Fatima Bint-e-Ali. I would also like to thanks to my all brothers and sisters Mr. Nauman Tabassum, Mr. Adnan Farid, Miss. Aqsa Farid, Mrs. Haleema Sadia, Mr. Muhammad Usman Farid, and Mr. Muhammad Ateeq-ur-Rehman for having belief in me and showing their presence at the time of need and making my family the best family and keeping my home a sweet home.

Finally, I would like to thanks to my in-laws especially my mother-in-law Miss Khateb-un-Nisa and sister-in-law Mrs. Ghosia yaqoob, Mrs. Nabila Yaqoob, Mrs.Tehmina Touseef, Mrs. Amna Majeed and brother in laws Mr.M.Junaid Ali and Mr.M.Jamshed Ali. There are lots of names of friends and relatives that I want to count but cannot point them all, so compositely I am thankful to all for being a beautiful part of my life.

DEDICATION

I would like to dedicate this thesis to my parents, my beloved daughter Fatima Bint-e-Ali, my elder brother Nauman Tabassum and Sister in law Nabila Yaqoob. They have been a source of encouragement and inspiration to me throughout my life and actively supported me in my determination to find and realize my potential, and to make this effort possible.

CHAPTER 1

INTRODUCTION

1.1 Overview

In the very first chapter, description of VANET and its all communication types are briefly discussed. Then, working of internet of vehicles (IoV) with its architecture is given. After this, IoV applications and its limitations are described. Then, background of the problem, its negative impact on IoV privacy and security is described. Research objectives, its aim with questions related to research stated. The Scope along with research goals also listed. And lastly, detail of each chapter explained in detail.

The word VANET was firstly introduced as a Mobile Ad-hoc Network application in 2001. Vehicular Ad-hoc Networks (VANETs) are a base technology for modernized transportation systems that goal to be efficient, secure, informative, and entertaining [1]. VANETs play a vital role in formulating modern intelligent transportation system (ITS) architecture [2]. VANETs interlink to wide area networks (WANs) through Road Side Units (RSUs) to allow authorized access and data downloads for different social media applications in vehicle [3]. VANETs supports Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), and Vehicle-to-Roadside Unit (V2R) communication [4][5]. In V2V communication, vehicles directly transmit beacon messages among each other to exchange real-time information of traffic density and road conditions. This enables vehicles to be aware of the surrounding traffic situation. In V2I communication, vehicles communicate to the internet and get access various services driving on the road by linking to roadside units. Through V2R communication, vehicles connect with roadside units to get updates about conditions of roads and different situations ahead.

If an accident occurs at any place on the road, the roadside unit can promptly notify vehicles in its range so they can take alternate routes. This communication and information sharing between vehicles, and between vehicles and roadside units, allows VANETs to give more reliable and optimized driving services and safety for drivers [6][7]. Wireless Access in Vehicular Environments (WAVE) protocol is used in communication of Vehicles of VANETs. This enables communication saves between vehicles (V2V), and between vehicles and roadside infrastructure (V2I). Generally in V2V communication, the influence of gravity is very little and mostly neglect. V2V communication primarily depends on wireless signals that are affected by atmospheric conditions, distance and obstacles slightly than gravitational forces.OBU and sensors are embedded in every vehicle to observe obstacles and road condition. The OBU enables a vehicle to communicate when it is turn on. Therefore, for both inter-vehicle and intra-vehicle communication OBU is crucial for enabling this communication in the VANET. Vehicles have also a device called Application Unit (AU) that helps to keep the network smooth during communication. Roadside Units (RSUs) are infrastructure located on roads, and buildings to send wider awareness of traffic and roads conditions. In any emergency RSUs alert vehicles so they can choose alternative routes to keep away from congestion. This roadside infrastructure also monitors network vehicles. If any vehicle acts skeptically, the RSU notify the Trusted Authority (TA) to take any action by canceling the vehicle's credentials. RSUs also notify other vehicles to stop sharing information with such dubious vehicle [8]. The communication scenario of VANET is shown in in figure 1.1.

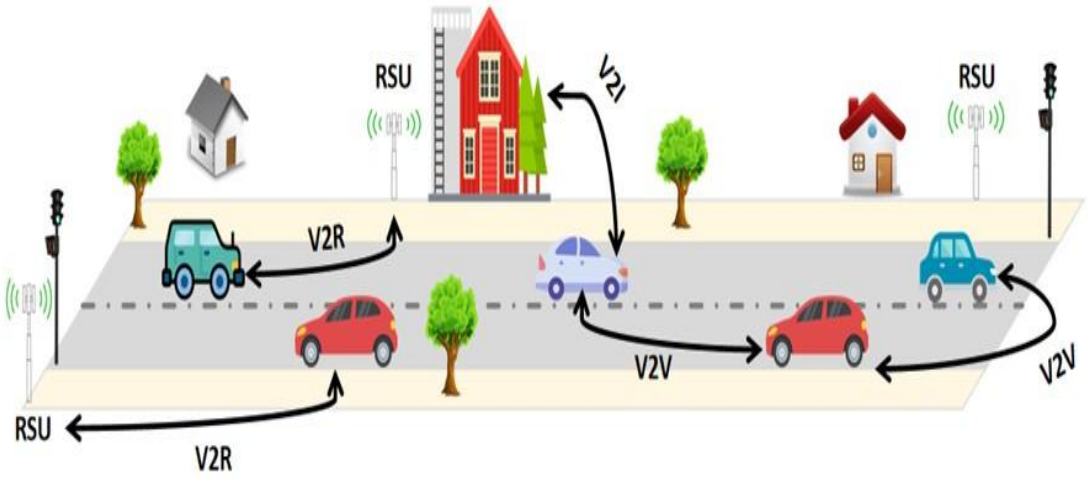

Figure 1.1: Communication Scenario of VANET [8]

VANETs allow vehicles to connect with each other and RSUs through beacon safety messages but, VANETs have limitations in performance of vehicles, compatibility with systems, dealing with large data from Vehicles, and network connection in urban areas [9]. To overcome these limitations, the idea of the IoV developed. The aims of IoV is to optimize VANET capabilities and resolve issues like insufficient data capacity, systems compatibility, erratic network connections, and bad performance in complicated urban environments with continuous traffic jams. The IoV provide optimal connectivity, scalability and good performance for vehicle communication networks in dense urban areas [10].

The IoV helps on VANETs by assimilates ideas from VANETs and the Internet of Things (IoT) to establish an improved network for connected vehicles [11]. In the IoV, vehicles disperse messages about their position and location status to allow communication. Information included in it is called BSM or heartbeat information. All communication is done through BSM in US, Cooperation Awareness Procedure in other countries [12][13]. The elements of a Beacon are presented within figure 1.2.

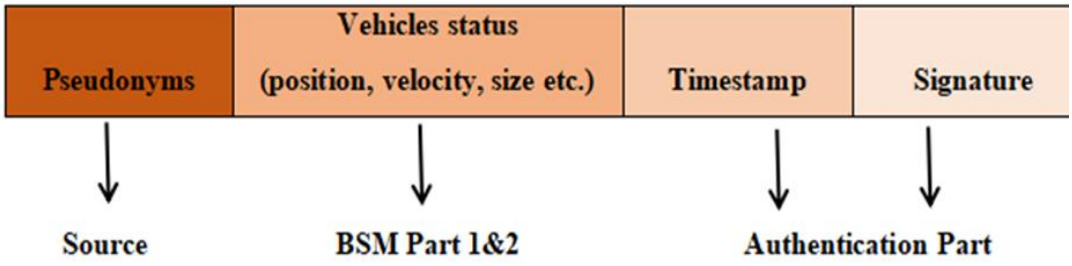

Figure 1.2: Elements of Beacon [13]

This enables broader data assemblage and network capabilities as compared to VANETs alone. Vehicles broadcast BSMs having sensitive data and information which could be catch by opponents. Opponents could misuse this information to trace vehicle's location, learning traffic patterns and compromising privacy [14]. To protect their privacy, vehicles use pseudonyms that are frequently changed pseudonyms, but tenacious opponents can try to link these pseudonyms [15]. Establishing distinct dimensional zones can enable to prevent pseudonym linking by maximizing confusion for opponents trying to track vehicles over

zones [16][17]. Research has focused on maintaining vehicle anonymity and preventing attacks through careful pseudonym changing and creation of distinct zones.The IoV provide an advanced network for vehicle-to-infrastructure and vehicle-to-vehicle communication. IoT assigns to the connection of physical devices and systems to the internet. IoT allows these devices to gather data by using sensors and broadcast it over the internet through wireless network [18]. The development of IoT enables for more connectivity and automation in various industries of healthcare, manufacturing, transportation and etc. The applications of IoT utilize different technologies such as cloud computing, RFID, sensors, and more to interlink devices and data transmission [19]. IoT shows a vital role in enhancing security and privacy measures in various aspects. Sensors and wireless networking in IoT monitor and detection potential hazards real-time and earlier. IoT have many applications, some of them are shown in figure 1.3.

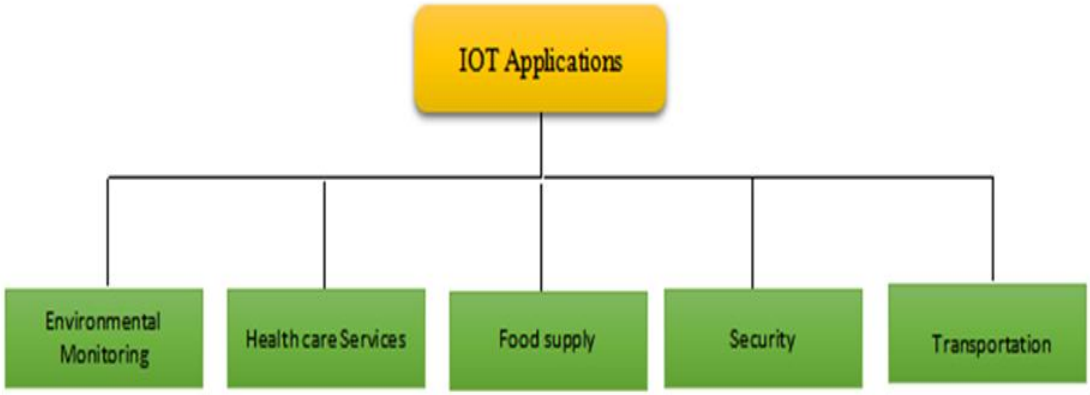

Figure 1.3: Applications of IoT [19]

1.2 Motivation

Location privacy is main principal in the internet of vehicles (IoV). Vehicles utilize pseudonyms and send basic safety messages (BSMs) to nearby vehicles to remain anonymous. When intruders get access the pseudonyms then they can target vehicles and trace their information. Attackers can physically or financially harm passengers and drivers by using this data. Various privacy and security techniques have been proposed to solve this problem. But existing schemes have some limitations and cannot keep save vehicle privacy. Therefore,

more research is required to get affordable solutions that optimize privacy and confidentiality. The requirement to keep save vehicle anonymity motivates continued research in IoV field.

1.2.1 Architecture of IoV

The Internet of Vehicles (IoV) allows all connected vehicles to communicate with different entities like vehicles, mobile devices, pedestrians, road side units, infrastructure, cloud services etc.[20]. V2V(Vehicle-to-Vehicle) communication allows vehicles to share information like location, direction and speed of vehicles to the neighbouring vehicles. This help to prevent in collision. V2M communication enable vehicles to interact with smart phones and devices having of pedestrians, passengers and drivers. V2P (Vehicle-to-Pedestrian) communication share alerts to pedestrians about proceeding vehicles to stop accidents. .V2R(Vehicle-to-Road side unit) communication allows vehicles to interlink with roadside units to share information that can increase traffic efficiency, protection, and access service.V2I (Vehicle-to-Infrastructure) communication provide the vehicle to receive safety warnings, traffic alerts, and signals from infrastructure.V2C (Vehicle-to-Cloud) communication connects vehicles to cloud services for entertainment, navigation and other application. All these different types of communication are collectively known as V2X [21]. The V2X message setup presented within figure 1.4.

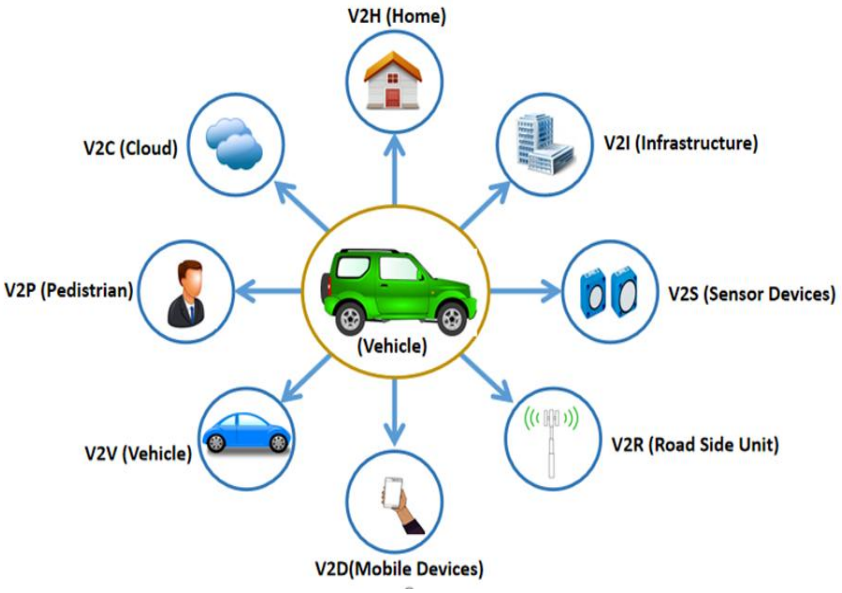

Figure 1.4: Setup of V2X communication [21]

Trusted Authority (TA) registers the vehicles on network and allots pseudonyms to these vehicles. If a vehicle behaves suspiciously RSU have access to inform this to TA, which can then call off the vehicle's credentials [22]. The goal of IoV is to allow vehicles to communicate for better, safer driving and to avoid accidents through sharing of information between vehicles, pedestrians, and infrastructure and cloud services. The architecture of IoV consists on seven different layers. This architecture in Figure 1.5 shows seamless connectivity among all network components and information sharing in an Internet of Vehicles (IoV) environment [23].

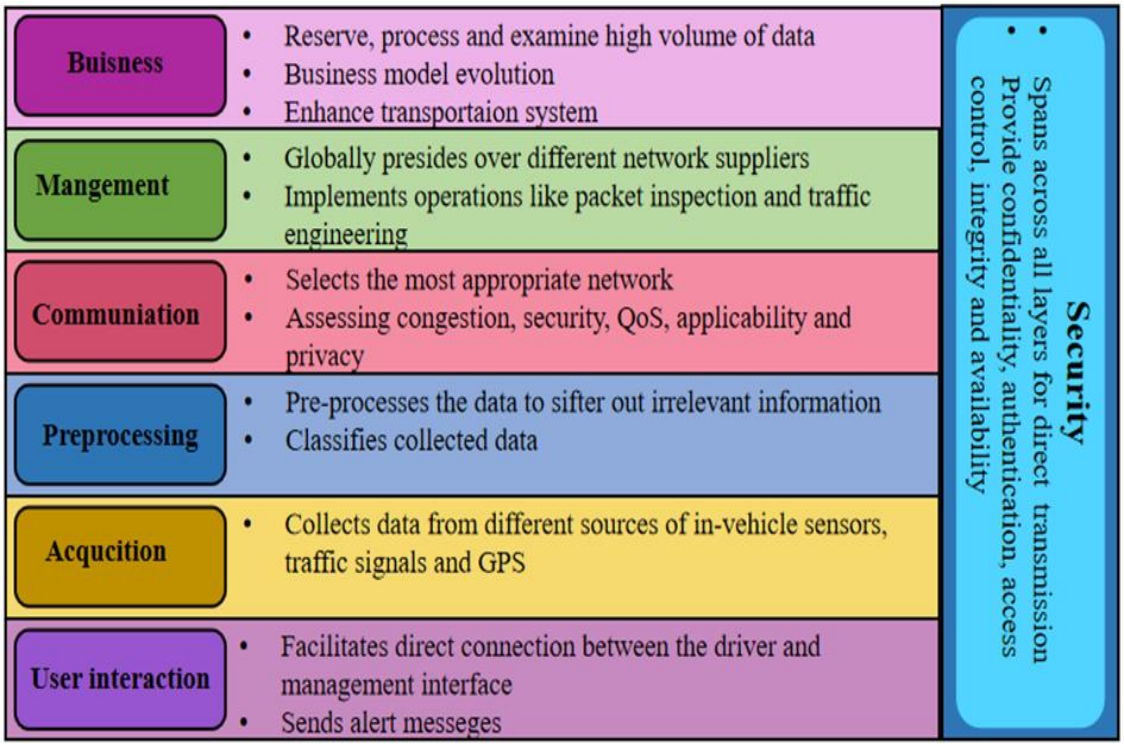

Figure 1.5: Architecture of IoV [23]

The very first layer is known as user interaction layer that facilitates direct connection between the driver and management interface to coordinate alerts and choose best displays to minimize distractions. The second layer is called data acquisition layer which aims to collects data from different sources such as in-vehicle sensors, traffic signals and GPS etc. The third layer is data filtering and pre-processing layer use to pre-processes the data to sifter out irrelevant information before Communication on the basis of subscribed services profiles created for the vehicles. The fourth layer is communication layer which selects the most

appropriate network for sharing information by assessing congestion, security, QoS, applicability and privacy. The control and management layer is the fifth layer to globally presides over different network suppliers in the IoV environment and implements operations like packet inspection and traffic engineering. The sixth layer is business layer that uses cloud infrastructure to reserve, process and examine the very high volume of data, allowing statistical examination and business model evolution based on data utilization and applications. The seventh and last layer is security layer that spans across all layers for direct transmission and allow various functions like confidentiality, authentication, access control, integrity and availability to mitigate privacy attacks [24].

1.2.2 Applications of IoV

IoV provides various advantages to its users. These benefits fall into two main categories which are safety oriented and non-safety applications that are described below:

i) Safety-oriented Applications providers

Vehicle safety applications send alert messages to inform drivers of hazards and stop accidents. When a vehicle is too close to avoid a rear-end collision then danger location alerts inform drivers of hazardous conditions of road like potholes. Vehicles communicate this information among selves to know conditions of road, which is very helpful in rural areas [3] Pre-crash alerts ready the driver for unavoidable accidents to avoid injuries [24]. Post-crash alerts share messages to other vehicles of an accident so they can choose alternate path or themselves Emergency vehicle signals inform drivers that accidental vehicle is coming so it can go securely through red lights [2]. These various notifications and alerts help to make the journey of vehicles more secure by alerting the driver of dangers. Overall, the timely notifications enable both emergency vehicles and drivers to give timely response to hazards [15].The Amber Alert notify vehicles about offender or dubious vehicles in the surrounding area leaving out for that vehicle itself. Pedestrian vicinity alert warns drivers when a pedestrian is nearby the vehicle to prevent hitting them. Vehicles are also notified about

nearby vehicle's speed and distance to prevent accidents in foggy conditions. Lane change alerts notify the driver about traffic density in the deliberate lane previous to exchange lanes to be safe from danger. If a vehicle crosses a red light illegally, infrastructure gives a warning about the vehicle to avoid accidents [25].

ii) Increase Scalability

Non-safety applications aim to provide entertainment, convenience and comfort to passengers and drivers. These services might be needing high bandwidth to operate properly. Navigation services facilitate drivers to choose the best hotels in unknown cities and find the nearest open parking area [27]. Showing updates passengers about the most recent sales and products at nearby stores and shopping malls as they drive by. E-toll payment scans vehicles located at toll plazas which automatically produce payment receipts to prevent annoyance and time waiting in long toll lines. Many entertainment services allow media streaming and internet access and to passengers. Non-safety applications enhance the overall travel experience by improving comforts on long journey. These applications give convenience and make travel more enjoyable by real-time information and entertainment access, while not critical for avoiding accidents such as safety applications [26]

iii) Non-safety applications

It improves the travel experience by providing entertainment and convenience. Online gaming and video streaming provide entertainment but need high bandwidth to stop buffering. Traffic congestion is prevented by smart intersection. Navigation services show directions to the nearby hospital in a situation of a medical emergency. Passengers can use the internet to send emails, messages and entertain by music [24]. Drivers get weather updates, location map and online directions for unknown location area [2][10]. These non-safety services provide lavishness not feasible in standard travel, removing boredom. while enjoying entertainment access users stay connected and up-to-date. These non-standard-safety applications optimized comfort on long journeys, while less critical than safety warnings [12].

1.2.3 Constraints in Adhoc Networks

IoV has many advantages but also have limitations needs more research. Main constraints are privacy vulnerabilities and lack of full exploration of adeptness. More research can help IoV meet its potential

i) Privacy Issue

Vehicles transmit location data in plain text which can be traced and hacked if approached by intruders, effecting user privacy. Many prior strategies like silent periods, mix contexts and mix zones cannot completely protect active, passive, active, masqueraded, Sybil and DDOS attacks. More research is necessary to develop more techniques that completely solve this security and privacy problem which is very important and cannot be ignored [21][10].

ii) Fixed Message Dissemination Frequency

Vehicles frequently communicate BSMs having pseudonyms, up to 10 per second [14]. This high frequency communication makes vehicles more attack able to attackers by tracking target vehicles through linking pseudonyms [17]. Most anonymity strategies still utilize maximum BSM frequencies which allowing attackers to scheme and perform pseudonym linking attacks.

iii) High Dynamic Network Structure

Vehicles have varying and undetermined speeds in the internet of vehicles (IoV), which creating the network topology highly dynamic. There are limitations in existing routing protocols to handling the changing topology. A perfect protocol is required to route data from node(source) to node(destination) with minimum delay and packet loss, good QoS and maximum road safety. No any recent robust protocol attains these goals [21] [28].

iv) Lack of Location Precision

GPS localization separately does not give the good precision accuracy required for IoV, which needs less than 5m error. In urban areas performance of GPS declines due to complicated buildings, long underpasses and tunnels. Depending only on GPS increases susceptibility in systems of IoV systems. More research is required beyond GPS to enhance location accuracy and hardiness [8].

v) Enormous Rebroadcast BSM

Vehicles transmit safety beacons to nearby vehicles in communication range. These neighbors then re-transmit the beacons, establishing a storm of repeated same messages. This BSM storm devalues QoS, maximizing packet loss and delay as the same beacons are got numerous times [19] [29].

vi) Computation Overhead

The enormous data produced from vehicle-to-vehicle transmission in dense IoV traffic is difficult to save and examine. This massive data needs makes the technology more composite and costly to execute. Improving devices to control the additional memory require add complexity [1].

1.3 Applications of the proposed scheme in terms of data privacy and integrity

The proposed Mutual Reporting-based Pseudonym Swapping Zone (MR-PSZ) scheme has significant applications that are presented here.

i) Location Privacy

The MR-PSZ scheme ensures that the real identities of vehicles are not exposed during communication. By using pseudonyms instead of actual identities and swapping these pseudonyms, it becomes significantly harder for malicious entities to track the movements of individual vehicles. This prevents the disclosure of the vehicle's location history, thus safeguarding drivers' privacy.

ii) Anonymity

The use of pseudonyms provided by a trusted CA ensures that vehicles remain anonymous while communicating. This anonymity is crucial in scenarios where vehicles share sensitive information such as accident reports or hazardous road conditions.

iii) Secure Communication

The MR-PSZ scheme uses cryptographic methods to ensure data integrity during communication. Vehicles use public and private key pairs to encrypt messages, ensuring that only intended recipients can decrypt and read the messages. This prevents unauthorized access and tampering of data during transmission.

iv) Mutual Authentication

The pseudonym-swapping process involves mutual authentication between vehicles before exchanging data. This ensures that both parties are authentic and have been verified by the CA, preventing impersonation attacks and ensuring the validity of the communicating entities.

v) Tamper-Proof Logging

After each pseudonym swap, vehicles upload a pseudonym swap log to the CA. This log includes encrypted details of the swap, ensuring that any attempt to alter the log can be detected. The CA can use these logs to trace back and verify the history of pseudonym swaps, ensuring accountability and integrity within the network.

vi) Detection of Misbehavior

The scheme's logging mechanism allows the CA to detect and handle misbehaving vehicles. If a vehicle does not receive the log upload confirmation or detects an inconsistency, it can report the issue to the CA. The CA can then investigate and take appropriate actions, such as revoking certificates or blacklisting vehicles, to maintain the integrity of the system.

1.3.1 Ideal Scenario

In an ideal scenario, the MR-PSZ protocol operates in a well-managed, secure, and resource-rich environment:

i) Efficient Infrastructure

The communication infrastructure is robust, with low latency and high bandwidth, allowing seamless and better pseudonym exchanges.

ii) Strong CA Management

The CA is secure, reliable, and capable of handling the volume of pseudonym management tasks without becoming a bottleneck.

iii) Resource Availability

Vehicles are equipped with sufficient computational resources to handle the cryptographic operations involved in the MR-PSZ protocol without impacting other critical functionalities.

iv) Effective Adversary Management

The system can effectively detect and mitigate any adversarial attempts to compromise the pseudonym-swapping process.

1.3.2. Worst-Case Scenario

In a worst-case scenario, several challenges and limitations come to the fore, which are described below:

i) Resource Constraints

Vehicles may lack the computational power or storage capacity to efficiently manage cryptographic operations, leading to delays and potential failures in the pseudonym-swapping process.

ii) CA Compromise or Failure

If the CA is compromised or becomes unavailable, the entire pseudonym management system could be interrupted, leaving vehicles susceptible to tracking and data breaches.

iii) High Communication Latency

In environments with high latency or limited bandwidth, the communication overhead of the MR-PSZ protocol can cause significant delays, reducing the effectiveness of privacy protection measures.

iv) Sparse Vehicle Density

In scenarios with low vehicle density, finding sufficient nearby vehicles to form a pseudonym-swapping zone becomes difficult, potentially leaving vehicles exposed for extended periods.

1.4 Problem Statement

IoV ensures secure and reliable communication between vehicles for a safe journey. However, maintaining the privacy and integrity of exchanged information is paramount. If the sensitive information of vehicles is exposed it results in severe consequences, reducing the reliability of the network.

The primary issue in the base scheme is twofold. First, after pseudonym swapping occurs within a designated zone, both vehicles involved upload their swap log data to the CA after successful swapping. The CA then waits for an accusing message for a specified duration. The main challenge arises when the log upload message sent by one vehicle is not received by neighboring vehicles as the vehicle moves out of communication range. This situation may result in the CA not receiving false accusing messages from neighboring nodes. Second, it does not ensure message integrity, which further complicates the reliability and security of the system [27].

1.5 Research Questions

This study address the following research questions:

i. How can pseudonym swap and continuous privacy protection be managed?
ii. How can the risks of location and profiling be mitigated?

1.6 Aim of Research

The aim of the research is to provide a solution for which traceability can be reduced while sharing track information and also protect against the identity of exposure attacks. This also includes the protection of anonymity while updating at central authority by upload the swap maximum throughput.

1.7 Research objectives

The objectives of this research study are as follows:

i. To reduce the traceability of vehicle to protect against the identity of exposure attacks.
ii. To upload the swap log by providing anonymity

1.8 Scope of Research

The primary focus of research is on addressing the challenges related to data security and privacy during wireless communication among vehicles in the IoV. This includes the protection of sensitive information such as location, speed, and other vehicle-related data.

1.9 Thesis organization

The structure of the whole thesis provided below: In chapter 2 outlines previous techniques centered at Pseudonym Changing mechanism, compares them, and highlights major issues in this domain. Chapter 3 elucidates the methodology of the proposed techniques. Chapter 4 provides a detailed explanation of the proposed scheme. Chapter 5 presents the results of MR-PSZ, while in Chapter 6 includes the summary and suggestions for work in future. Finally, the references provided. in the end

CHAPTER 2

LITERATURE REVIEW

2.1 Overview

This chapter includes VANET is elucidated with main issues related vehicle anonymity. It then describes existing prior studies on pseudonym changing to prevent vehicle privacy with relevant schemes. The section analyzes these schemes by discussing the strengths and limitations. It also points out research gaps before concluding with a summary.

2.2 Security Issues in Vehicular Ad-hoc Network

BSMs contain detailed information about vehicles. Adversaries monitoring these beacons can learn drivers' locations, routines, social circles, beliefs, and endanger them. Frequent trips reveal patterns. This private data could enable abuse by third parties. Thus it poses serious security threats to driver and passenger lives.

2.2.1 Lack of privacy

The continual observing and data assembling of user personal information and affairs online without command or control. Vehicles share BSMs contains sensitive information about vehicles. Many adversaries monitor these beacons and if they get driver’s personal identity, social circles locations and routines the they can create any danger for them [28]. Continuous travel trips show patterns. This private information could allow abuse by third parties like intruders or adversaries. Thus it leads to serious privacy threats to driver as well as passenger lives [29].

2.2.2 The Syntactic Linking Attack

Syntactic attacks utilize feebleness in network protocols and software to obtain uncertified access or through services into confusion by sending distorted input. Vehicles regularly exchange their pseudonyms to elude adversaries, but remain unsafe after changing [30]. If there are three vehicles running on a road and a vehicle A on a road exchanges its pseudonym with another Vehicle B from A to B in time t in the presence of these 3 vehicles, then an intruder can draw the interference vehicle B was formerly A at time t. At time t+ Δt, B again exchange pseudonyms [31]. This attack attempt successful when vehicles do not interrelate pseudonym changes.

2.2.3 The Semantic Linking Attacks

Semantic linking attacks include correlating information from different origin to infer private and personal sensitive information about persons that was meant to be hold separate [31]. As compared to a syntactic attack, semantic attack is considered more powerful attack because the opponent can know the location of vehicles and related information even though vehicles exchange pseudonyms with working together [32]. The rivals when accessing messages of other vehicles interrelate by the novel pseudonym allotted to vehicles utilizing tracking procedures likelihoods and tracing procedures in this attack [33].

2.2.4 Presence of Malicious nodes in Network Topology

Within IoV network, vehicles get information about neighbor nodes. If a vehicle is make a deal an adversary, it becomes a fraudulent, malicious node. These malicious nodes can disclose information about the network [34]. Adversaries can learn about neighboring vehicles and locations, while listening to BSMs received by fraudulent nodes, adversaries can learn about nearby vehicles and locations. They can also change malicious vehicle information in BSMs, broadcasting wrong location data that could lead to accidents [35].

2.2.5 Increasing of Accidents during Silent Mode

Vehicles broadcast BSMs using regularly change pseudonyms in travelling to escape from adversaries. Some techniques go on silent mode for slots after pseudonym changes to increase security [36]. This silent mode can enhance privacy; it protects vehicles at explicate areas like intersections from receiving critical safety messages about neighbor vehicle's speeds. Vehicles in silence mode miss these warnings, risking accidents [37].

2.2.6 High Pseudonym Consumption

CA assigns pseudonyms to vehicles, a neutral entity allowing verified certificates. However, vehicles have finite memory for pseudonyms and communication [38]. Regular changing in pseudonym maximize consumption, too early consuming pseudonym pools. Then vehicles must request to re allot pseudonyms from the CA, needing more memory and communication [39]. The usage of pseudonyms should be efficient to preserve resources [40].

2.2.7 Compromise on Quality of Service (QoS)

QoS is essential for evaluating the efficacy of proposed technique. The vehicle memory is filled with unneeded messages, protecting receiving of essential road safety data from other vehicles and RSUs [14]. This packet misplacement chance accident by not sending critical safety information in time. Effective memory handling is required to categorize explicate road safety transmissions [17].

2.3 Pseudonym changing scheme for VANETs

Privacy and anonymity are essential but make concession in the technology era. In VANETs, vehicles transmit and share sensitive information that can be accessed by any

malicious person or third parties, regarding drivers. So it is a serious issue [12]. For Privacy, vehicles require to change pseudonyms - private/public key pairs from a CA to authenticate vehicles [14]. Regularly change pseudonyms keep alive vehicle anonymity and reduce traceability by intruders [29] Various studies take a look at optimal pseudonym changing to successfully balance anonymity and privacy in VANETs. The existing pseudonyms-changing schemes are divided into two main groups Mix Context Based pseudonym changing technique and Mix zone based techniques

2.3.1 Mix Context-Based Pseudonym changing Techniques

Mix context-based schemes involve changing pseudonyms based on specific conditions. If these conditions are not met, vehicles retain their current pseudonyms until the maximum stable time is reached. Yang et al. [27] presented the Swapping Zone technique that focus to give vehicles to swap pseudonyms with nearby vehicles in order to enhance privacy. In this strategy, vehicles get pseudonyms from a trusted Certificate Authority (CA) which behaves as an honest entity. The vehicles contain an OBU for communication which can be made a deal by an adversary to attempt attacks. At here RSUs behaves as a semi-honest entity. Vehicles send pseudonyms and information with neighbors. An initial vehicle vi examines two situations before establishing a swap zone as in Figure 2.1 [27] the communication time threshold and very low neighbor vehicle threshold.

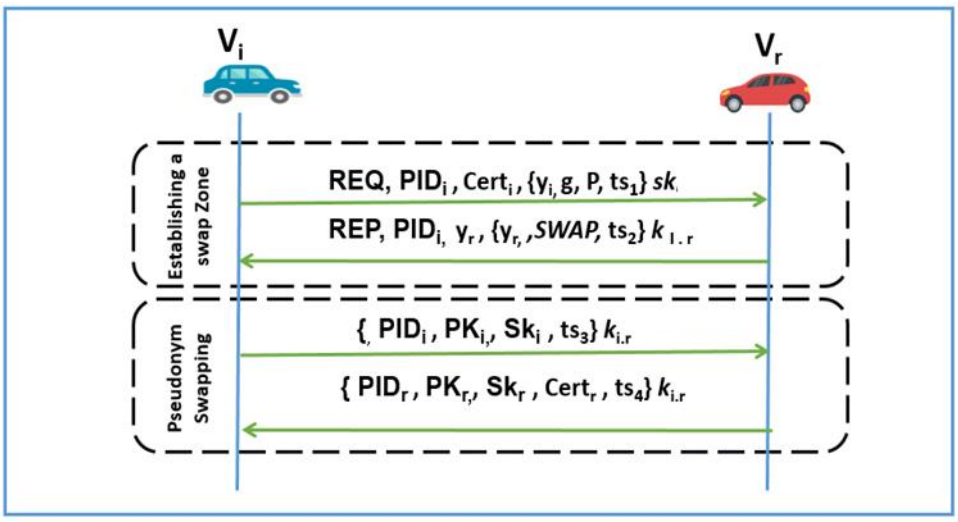

Figure 2.1: Establishing Pseudonym Swapping Zone [27]

If both conditions meet, vi shares a swap request to vehicle and receives acceptance in replies. It finds a vehicle vr randomly to swap pseudonyms after encrypting all informative data. Any kind of misbehavior is monitored by CA. If it is detected, CA expels and blacklists fraudulent vehicles. Then it revokes certificates and stop swapping. It also notifies to victim vehicles and then allots new pseudonyms. This allows security against interior attacks. When vi is at a busy intersection, transmitting with all vehicles conducts to maximum figuring and resource costs. To minimize it, vi only communicates with permitted vehicles where communication is foremost. Response probability of permitted vehicles is evaluated by using an Equation 2.1. *d* signifies the degree of anonymity, *k* symbolizes the capacity of the vehicular region and |*AS*| is the occupancy of the region. As vehicles increases reply probability decreases. This prevents maximum communication costs.

$$d = \frac{\log_2 (|AS|)}{\log_2 (K)} \qquad (2.1)$$

The scheme provides high security against internal attacks. However, a limitation is pseudonym swapping relies on reaching the neighbor vehicle threshold which may not be consistently achieved. So the scheme is dependent on vehicle density to function effectively. The proposed Dynamic Pseudonym Swap Zone (DPSZ) approach address better location privacy protection compared to prior existing approaches because DPSZ showed maximum anonymity entity with minimum likelihood for traced vehicles across various simulation environments including various vehicle densities, speeds, attack capabilities, etc. The self-adaptive transmission method in DPSZ also improves costs in high density situations. Comprehensively the performance evaluation highlights the progress privacy protection given by the DPSZ scheme.

Mehreen et al. [30] presented the efficient pseudonym consumption protocol (EPCP) to address the challenge of protecting person anonymity in IoV. The purpose of the studies is to compose a unique pseudonym consumption scheme that manage the usage of pseudonyms efficiently by vehicles and preserve then security from unauthorized users and intruders' attacks. The goals of the scheme are to contribute to the evolution of vigorous and privacy – bluff solutions for IoV operations, maintaining user trust and acceptance. The main problem identified is that consumption and wastage of pseudonym at higher rate due to unneeded pseudonym changes to irrelevant vehicles. Before pseudonym exchange less consideration of

relevant context also increases traceability for vehicles. Moreover, the maximum dynamic network topology begins faraway vehicles to still receive pseudonym change message and alert. Various approaches also describe a swap between privacy and safety by utilizing silence periods for pseudonym change. Ultimately filling up buffers with irrelevant messages conducts to increase BSM loss rate. The EPCP uses mix content base strategy for effective pseudonym usage in IoV. EPCP includes vehicles V that estimate the next step by checking it neighbors by using Kalman filter before appearing pseudonym change message. Only those vehicles are considered relevant which are near in range and with similar estimated directions. The Equation 2.2 is used to calculate probability ∞ of vehicles that five responses to initiator vehicles for pseudonym change where |Þì| is neighbors' vehicle, µ threshold number of vehicles needed to established swap zone, e Euler's constant.

$$\alpha = \begin{cases} 1, |\,Þi| \;=\; \mu \\ e^{1\frac{|\,Þi|}{\mu}}, |\,Þi| \;\geq \mu \end{cases} \qquad (2.2)$$

Equation 2.3 is used for calculating degree of anonymity d where |AS| is occupied area of vehicular zone and k is vehicular zone capacity. These given equations help in the calculation of important parameters that are included pseudonym changing process and calculation of anonymity.

$$d = log_2|AS|log_2(k) - (2) \qquad (2.3)$$

To ignore faraway vehicles speeds of neighbors are counted against the thresholds. Vehicles change pseudonyms to avoid wastage in spouse traffic and cooperative pseudonyms exchange will be happen in dense traffic EPCP prevent linking attacks by minimizing pseudonym life time to 50 seconds and focus on relevant selected vehicles. The methodology includes simulation using veins frame work comprising OMNet + + and SUMO to evaluate and compare against existing technique such as DGVP, WHISPER and CPN. The metrics such as utilization of pseudonym, tracking probability, BSM loss rate, and confusion ratio used to analyze its performance.

Nabil Kerkacha et al. [31] proposed a Probalistic Pseudonym Change (PPC) new privacy scheme is to prevent some desired vehicles from approaching silent periods to lead as

a communication pillar, while others endure assassinating pseudonym change. Most of the existing schemes either focus on minimizing cost of QoS at the privacy or maximizing privacy at the cost of QoS. The elected vehicles that work as a back bone in the network to stop in silent period because some privacy is offered by these vehicles. Where some other vehicles continuously perform pseudonym change to protect privacy. Neighborhood Density Quotient (NDQ) is calculated by the Vehicles on the basis number of neighbors within a radius R. The probability of a vehicles enters in silent period is determined by the estimated NDQ. If the NDQ is higher than it means the chance of pseudonym change is higher too. Outsider vehicles those are not included in silent periods are revolved gradually for impartially. NDQ to calculate the probability of pseudonym change by using given Equation 2.4. *n* is number of neighbor's vehicles included in radius *R*.

$$NDQ = 1 - \frac{1}{n+1} \qquad (2.4)$$

Author have used open source VEINS framework for vehicular network simulations to evaluate their proposed PPC scheme. It merges two simulators a road traffic simulator SUMO and a network simulator OMNeT++. SUMO is used to cause vehicle movability tracks. OpenStreetMap -is used to cause the road topology for the simulation schemes on the basis of a map of Munich city. PREXT is a privacy extension that built on top of VEINS to allow the evaluation of privacy strategies in VANETs. The authors performed PPC on PREXT [32].

Leila et al. [33] proposed and analyzed a location privacy scheme in vehicular ad – hoc networks VANETS by using a pseudonym change strategy. The objective of the given strategy is to maintain unlink ability between new and old pseudonyms to prevent from taking vehicles by intruders on basis of their cyber activity. The approach merges "location obfuscation" and "hiding within the crowd" schemes together. The pseudonym changes cooperatively in high densities area, but it uses altered location data and speed in low density areas before updating to confuse attackers. The strategy acts by changing pseudonyms during their expiration or exit ion of geo – spatial boundaries. Methodology of this approach includes a global passive adverse model to perform semantic and syntactic linking attacks. The given Figure 2.2 shows the process of pseudonym changing in presented scheme. When vehicles enter a region and their number is greater than k, they are allowed to update their pseudonym. The expiry date of a pseudonym is also stated which presents that afterward

pseudonym is updated again. It demonstrates different scenarios during updates caused by validity time expiration or exiting geo -spatial range Scenario I shows cooperation by pseudonym changing of vehicle during high density areas.

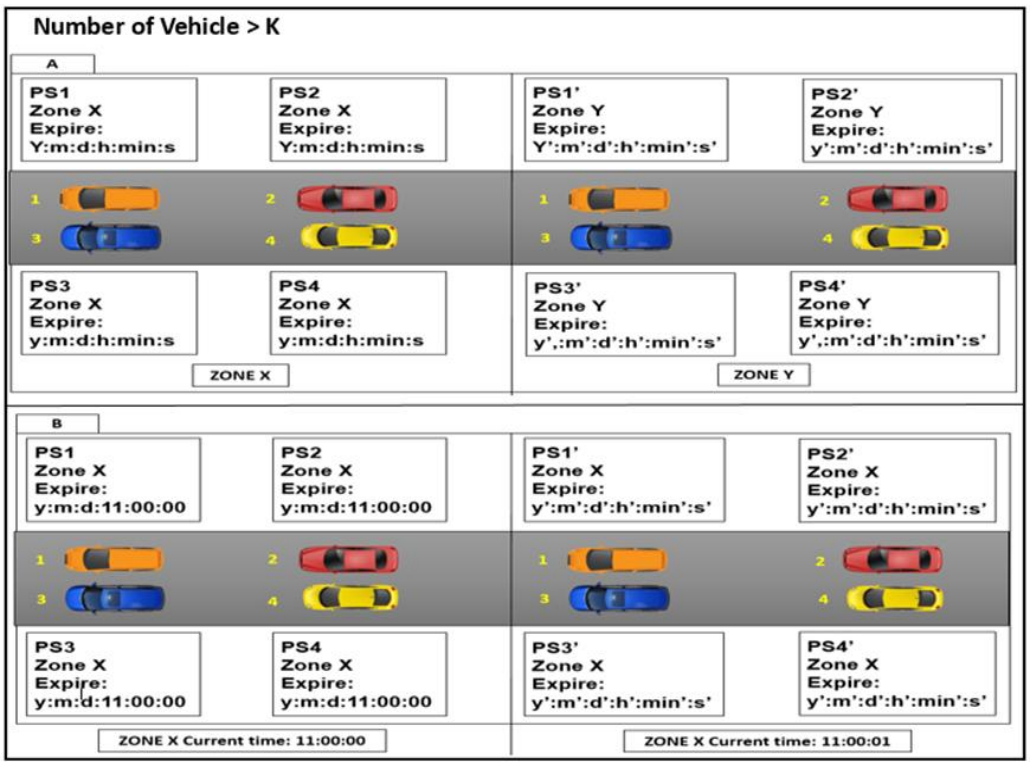

Figure 2.2: Process of Pseudonym Changing [33]

In Scenario II a vehicle nous it is alone before updating during its low density. Then it changes its speed and sets its location in beacons for some time before pseudonyms changes. Attackers are confused by this obfuscation. The real data is resumed after the updates. This whole procedure protects to link of new and old pseudonyms and ensure privacy even in low density. The performance of this scheme is evaluated by Ns – 2 simulators to produce mobility models. Simulations are conducted in high, medium, and low traffic densities for 900 seconds performance is calculated using linked pseudonyms ration and tracked vehicles. The given scheme's results are showing improved after compared to a periodic changing scheme.

Saini et al. [34] proposed two new smart and efficient schemes for placing attacking terminal to trace vehicles in VANETs. It demonstrates different pseudonym changing strategy utilizing these schemes compared to random induction. The aim is to evaluate the impact of informed terminal induction on tracing achievement. This spotlight the need to test schemes

against targeted attacks utilizing traffic knowledge when establishing hefty pseudonym techniques. The author's evolved two astute attacker induction schemes to choose best locations for terminals to trace vehicles in VANETs. The distance-based approach (DBAP) focuses recurrent pseudonym changes by spacing terminals with maximum traffic paths. The spacing is measured on the basis of connection range and frequency of pseudonym alteration so terminals can detect consecutive changes from a vehicle. Paths are choosing from potential initiating points to a maximum-traffic target. Full coverage is needed for more terminals; the spacing is shortening. The spacing is increased if there are fewer terminals, unless all terminals can be settled. The speed-based approach (SBAP) focuses pseudonym schemes that change at minimum speeds. It finds terminals at cross way with traffic lights or stop marks and along crowded road sectors where speed will be reduced. Stations are placed sequentially at intersections along selected paths in an urban area. A terminal is placed at the middle of cross way. If the distance between cross ways exceeds twice of the range of communication. It remains until the urban road is fully covered. Rest of the terminals is spaced uniformly along selected highway sectors estimated to have more congestion. In both approaches, the placement drags knowledge of traffic arrangement and road topology to increase the number of vehicles observed and probable pseudonym change events monitored.

A privacy preserving scheme is proposed by Jianwen et al. to address privacy problems in fog computing internet of vehicles (F–IoV). They showed a hierarchical structure in pseudonym fogs at the corner for disperse pseudonym management. Some communication protocols for secure and effective pseudonym management are also presented by the authors. The authors formulate a pseudonym change game to give access vehicles to change pseudonyms at hotspot on the basis of other numbers of changing vehicles. This optimizes the location privacy of vehicles in IoV. Basically objective of the scheme is to give an effective and secure pseudonym management that improves the location privacy in F–IoV using fog computing and contact aware pseudonym change. To manage pseudonyms for vehicles this strategy used geo – distributed pseudonym fogs at the edge of network, each with local authority. The vehicles send request to it near- by neighbor vehicles where the vehicles are verified by the local authority to generates new pseudonyms and then divide them [35].

In context –aware pseudonym changing game, vehicles can participate hotspots evaluate their security level and decide whether to change pseudonyms on basis of the number

of other vehicles [36]. More changing vehicles contains more privacy changing vehicles updates their records by informing the local authority [37]. The given figure 2.3 shows the architecture for pseudonym management presented by authors which contains three layers the first layer is called cloud layer, has central authority and data base. The second layer consists multiple pseudonyms fogs, along with local authority, RSU, etc. The third and last layer has vehicles.

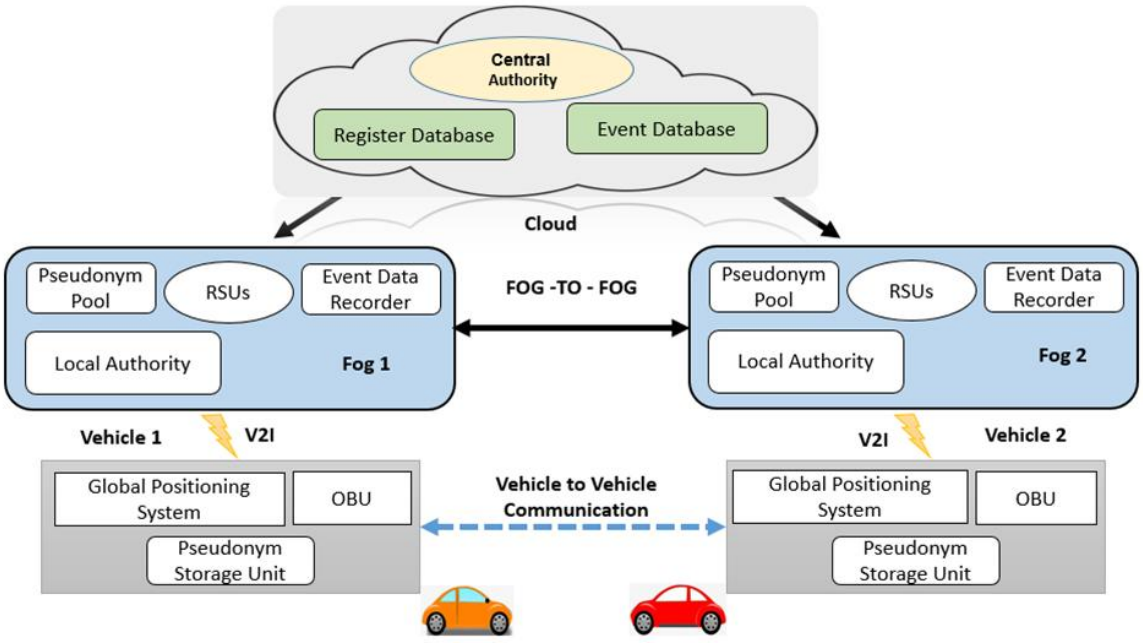

Figure 2.3: Security model of pseudonym management [35]

To address problem pseudonym linkage, Xinghua et al. introduced a method called Pseudonym Swap with Provable Unlinkability Based on Differential Privacy. In PAPU, vehicles exchange their pseudonyms with other vehicles within their vicinity (vehicle Vi). The infrastructure includes vehicles, Roadside Units (RSU), and a Registration Authority (RA). RA assigns legal pseudonyms to vehicles and maintains a record of their true identities and the pseudonyms assigned to them in a data center. A pseudonym mapping database ensures the connection between vehicles before and after pseudonym swaps to ensure liability. In case, a Vi wishes to exchange the pseudonym, then broadcasts a notification Reqi then sends the Vehicle ID and current pseudonym at the RSU. Upon receiving the request, a nearby vehicle sends an assist reply with its information to the RSU, indicating its willingness to participate in the pseudonym swap. These participating vehicles, denoted as Vswap, have their

pseudonyms collected by the RSU and then undergo pseudonym swaps based on the similarity of their driving characteristics, which include factors like speed, position, and location similarity, with the addition of random weights. The aim of this process is to make the vehicles indistinguishable and confuse potential adversaries. Various techniques, such as identical function, exponent function, usefulness function standardization, likelihood sample, and the application of disparity, are utilized to choose pseudonyms by the pseudonym store (ppseu). The primary advantage of the approach is to deliver a great level of low traceability among the old along new pseudonyms [35].

When there is high pseudonym consumption, it negatively impacts the Quality of Service (QoS) and can result in delayed packet delivery. To mitigate this issue, Zidani et al. proposed a method that Estimate Neighbors Position using an Adaptive Beaconing method. In this approach, vehicles are permitted to modify pseudonyms in case there are changes in velocity and the total nearby vehicles. In case, a vehicle which intends to modify the pseudonym, firstly verify the total neighboring vehicles and synchronously considers them for pseudonym changes. Every allotted pseudonym having a specified lifetime, and in case it terminates, the vehicle is allowed to use new pseudonym [36].

For enhanced confidentiality as well as reduced tracing probability, the Context-based Privacy technique is offered. This scheme assesses a vehicle's eligibility for a pseudonym change based on traffic density and the number of neighboring vehicles. Vehicles can enter a "silent mode", but time span remained low to prevent compromising safety BSM. The mechanism of this scheme uses security of drivers as preferences and adapts its security measures accordingly. When drivers enter sensitive areas, where privacy preferences are high, the scheme detects specific parameters (b values) to provide better security. An advantage of this scheme is a significant reduction in traceability [37].

In the Dynamic Grouping based technique proposed by Ullah et al. groups of vehicles are formed, with one vehicle designated as the Group Head (GH). Each vehicle in a group is assigned a Group ID (GID), and vehicles wishing to join a group are vetted by the GH to ensure their credentials are valid. Communication within a group is protected and cannot be intercepted by vehicles outside the group. Vehicles change their pseudonyms by assessing their neighbors. If the assessed value exceeds a threshold, vehicles simply change their

pseudonyms. Otherwise, a virtual approach for exchanging pseudonym is utilized, where every participant has two BSM having changed speeds that are swapped at random. This process involves selecting distant vehicles for the exchange, or if all distances are the same, nominating a vehicle at random. The advantage of this scheme is the secure communication within a group, but a drawback is the increased computational cost due to the creation of two additional beacons, which adds to the overhead [38].

The Traffic-Aware Pseudonym Changing Strategy (TAPCS) scheme aims to optimize resource consumption and enhance vehicle anonymity by utilizing a "silence mode." When a vehicle's speed falls below a specified threshold (vc) for a set time (tc), it assumes that traffic congestion has occurred. This assumption is confirmed by other vehicles that send congestion messages. The vehicle must select an initiator to create a "silence zone" for pseudonym changes. If no initiator message is received, the vehicle waits for a defined time (dmax) and then checks for the initiator message. The vehicle with the lowest position becomes the initiator (T_0). The initiator stops broadcasting safety messages and sends a notification to other vehicles, including speed thresholds, location, and the initiator's position. Vehicles with speeds below the threshold change their pseudonyms, while those with speeds above the threshold continue broadcasting safety messages to prevent accidents. As the silent zone may fill over time and new vehicles may be out of range of the initiator, a new initiator is selected. The previous initiator informs vehicles when traffic congestion ends, and vehicles return to normal communication. This scheme is effective primarily during periods of traffic congestion [32].

2.3.2 Mix Zone-Based Pseudonym changing Techniques

In Mix zone pseudonym changing techniques, specific locations are predetermined where vehicles move in and change their pseudonyms. Tao Jiang et al. proposed three mechanisms to optimize privacy location. The objective of this studies to examine the issue of wireless network security and location privacy. The key aim of the studies is to disrupt different types of privacy understanding information which leaked through wireless communication containing sender identity, time of communication and signal strength. The main goal is to provide user command over the location privacy while using of wireless

network's services. As the author present three mechanisms to get location privacy and searching first is utilizing of coating changing pseudonyms to hide and protect user identity. The second one is addressing expedient silent periods to separate pseudonyms. The final is Lessing area precision by commanding and controlling communication power to put the number of accessing points in limit. In these studies, the author used analysis, simulations, and real system estimation to perform their location privacy techniques. The authors demonstrate a module to measure to estimate the silent period on basis of pattern. Bus mobility data from Seattle is used to perform the simulations of this model. They experiment calculating channel asymmetry and variations are performed for silent communication power command. On the basis of their estimations the authors applied and check their power command techniques using wireless customized cards. To validate the feasibility and quantify the security benefits for these schemes the authors merge analytical modeling with extensive simulation and experiments on wireless systems.

Al-Marshoud et. al [39] proposed an improved Chaff-based CMIX scheme to enhance location privacy and security in VANETs. It identifies vulnerabilities in a previous given scheme and directed them through mutual authentication, adaptive cuckoo filters, and preventing symmetric key leakage. The proposed strategy focuses to attain unlinkability, unfeasibility, authentication, and robustness contrary to low density traffic conditions. Low density means the areas with fewer vehicles or less traffic volumes, which can affect travel patterns and congestion levels.Specifically, the studies state that transmission and duplicate certificates during authentication activate linking attacks outer side of the mix-zone. Moreover, malevolent injections can smash Cuckoo Filter legality and disrupt protective applications. In the end, authors record that symmetric key leakage outer side of the mix-zones let unauthorized approach that accommodates system protection. In improved Chaff-based CMIX scheme authors used a modified identity-based signature protocol for mutual authentication without disclosing personal identities. Adaptive Cuckoo Filters are used at the replacement of standard Cuckoo Filters to reduce false positive's crash. RSUs completely give out signed filter updates to finish variations. To prevent leakage Diffie-Hellman key exchange leads to fresh mix-zone keys at each communication to avoid from leakage. Digital Signatures are used to filter updates and sign messages to give non-rejection and protect malicious injections. Pseudo-Identities are created by using a cryptographic scheme on the basis of Cramer-Shoup encryption technique to provide unlinkability. The aim of the given scheme is to achieve robust unlinkability, unfeasibility, and authentication. The study does not present

experimental results from a simulation because authors demonstrate a security analysis of the strategy conceptually and mathematically.

To buoy up more vehicles to be a participant in pseudonym changing, a reputation-based proposed scheme is proposed [40] vehicles should register with a trusted authority before connecting to the network. RPCLP motivates selfish vehicles to change pseudonyms through mix zones utilizing a reward based system. In case, a vehicle needs to alter its pseudonym, it develops two zones, and checks how many other vehicles are present. The vehicle transmits a Request message at the control server, which sends a COMMAND to other vehicles in the zone asking them to cooperate in changing pseudonyms. The control server monitors which vehicles respond to the COMMAND with an RNP, tracking who changed pseudonyms versus who did not. Vehicles that cooperate are assigned an incentive value, starting at zero and increasing with continual cooperation. A threshold ε determines if a vehicle is selfish. If the reputation value of a vehicle is ≥ ε, all vehicles in the zone must change pseudonyms; otherwise vehicles can independently decide based on remaining pseudonym lifetime and incentive value. Results show RPCLP provides better energy consumption. The main advantage is increased anonymity size, which confuses adversaries and improves privacy.

Vehicular location privacy (VLPZs) [34] scheme is presented to enhance Security of vehicles by enabling suitable changing of pseudonym. The given scheme is based on an infrastructure. In this infrastructure the vehicular network is distributed into grids. In which each grid is having VLPZ. The vehicles which start entering in the VLPZ are galvanize to synchronize changes of pseudonym with other nearby vehicles in the zone. Area wise trusted authorities (TARs) behave as mediator among the VLPZs and generally TA allowing protective communication. Each VLPZ contain RSU that notify about nearer vehicles. The Vehicles which are entered through routers change pseudonyms to prevent FIFO attacks after a random time period then pass out through aggregators.

Xanmei Li et al. proposed broadcast and silence period (BSP) pseudonym change scheme to secure vehicle location privacy attack in IoV. The idea of proposed scheme is to protect the vehicles location against semantic and syntactic linking attack. The scheme analyzed vehicle trajectory data to search vehicle’s location of their start and stop trips, by

choosing mix zones approach. Vehicles dwell on these probable spots. According to preset silence and broad cast slots, vehicles change their pseudonym in silent period. This pseudonym change protects syntactic links of new and old pseudonyms BSP maximize privacy against security attacks. To keep each silent slot in limited range, the impact of not communicating BSM on driving is minimized as compare to silence approaches. Results analyzed the group density coefficient demonstrates the number of taken mix zones minimize the coefficient maximizes for both rest and work day. The presented BSP scheme shows optimal privacy protection when comparing with two other privacy protection schemes for new and old adversaries. The results show location privacy scheme BSP increases protection against linking attacks [41].

The Pseudonym Changing at Social Spots (PCS) [42] scheme is introduced as an additional mix-zone based stratagem aimed at thwarting adversary attacks. This scheme operates in two distinct scenarios: Firstly, vehicles that come to a halt at red traffic signals, and secondly, vehicles stationed outside shopping malls. In the former case, pseudonym adjustments are facilitated at small-scale 'social spots,' coinciding with the transition from red to green signals. In the latter case, where vehicles congregate in larger numbers, this process transpires at expansive 'social spots.' Notably, vehicles departing from shopping mall parking lots occur randomly, inducing a heightened level of confusion for potential adversaries seeking to trace target vehicles. The utilization of a discrete model based on C++ underpins simulation efforts. While this scheme significantly diminishes traceability within dense traffic scenarios, it bears the limitation of potential pseudonym stagnation in the absence of traffic congestion, thereby inadvertently facilitating adversarial pseudonym linking attacks.

The Urban Pseudonym Changing Strategy for Location Privacy (UPCS) scheme is introduced [43] as a measure to curtail pseudonym consumption and augment location privacy. Within this framework, vehicles are afforded the opportunity to update their pseudonyms exclusively in proximity to red traffic signals at signalized intersection junctures. A red traffic signal denotes a "silent zone," wherein any entering vehicle receives notification from the Road Side Unit for Silent Mode (RSUSM). This prompts the vehicle to cease the broadcast of BSM and relay pertinent lane and pseudonym identification information to the RSU. Within the confines of the red zone, all vehicles maintain a state of silence, either exchanging or altering their pseudonyms as necessitated. If opting for pseudonym exchange, a protocol for

swapping is engaged. Vehicles expressing intent to exchange pseudonyms transmit their private key and pseudo ID to the RSU, eliciting a randomized pseudonym exchange in return. The silent zone remains in effect until the transition to a green or yellow traffic signal. Upon cessation of the silent phase, the vehicle reverts to broadcasting a beacon incorporating the updated pseudonym. Noteworthy benefits of pseudonym exchange encompass a reduction in computational costs and pseudonym utilization.

In the Concerted Silence-based Location Privacy Preserving Scheme (CSLPPS) [44], when a vehicle opts to alter its pseudonym, it issues a "Ready-to-change" directive to other vehicles. Those vehicles electing to participate in the pseudonym modification process respond with a "Do change" communication. Subsequently, all designated vehicles transition to a silent state and deactivate their OBUs. During this silent phase, no inter-vehicle or infrastructure communication ensues. The collective cohort of muted vehicles synchronously updates their pseudonyms on their respective OBUs, subsequently vacating the dynamic silent zone and resuming normal operations. It is pertinent to note that the predictability of target vehicles diminishes post-silent mode, as vehicles forego communication during this phase, potentially forgoing vital safety beacons.

In the pursuit of bolstering vehicular privacy and safeguarding confidentiality [31] initiative posits the creation of a Cryptographic Mix Zone when pseudonym alterations are necessitated. The architecture of this scheme encompasses a Roadside entity named as (RSU), Control Servers, and TA. In case, a vehicle changes its pseudonym, then dispatches an appeal to the CS, which, in turn, issues a COMMAND message to the nearest vehicles, mandating the establishment of a fundamental cryptographic based region. In it, vehicles refrain from entering silent mode, perpetually transmitting encrypted safety messages. Vehicles within this zone collectively effect pseudonym adjustments prior to exiting the dynamic zone, each bearing a renewed pseudonym. It is important to note that this scheme does entail additional time for the decryption of safety beacons. Vehicles within the same velocity band are grouped within a transmission range (TX), where 'r' represents the radius of the transmission range, 'Dt' signifies the distance threshold, 'α' denotes a constant, and 'v' signifies the velocity of vehicle 'v' at time 't'. Eligibility for pseudonym change is contingent upon 'Dt $\leq$1', thereby regulating the pseudonym adjustment process. Grouping of vehicles in VBPC is shown in Figure 2.4

[31]. However, vehicles are not obligated to modify their pseudonyms if 'Dt > 1', facilitating a dynamic response to vehicle velocities. An intrinsic limitation of this scheme resides in its applicability chiefly to vehicles engaged in prolonged journeys, rendering it less suitable for shorter distance travel scenarios [45].

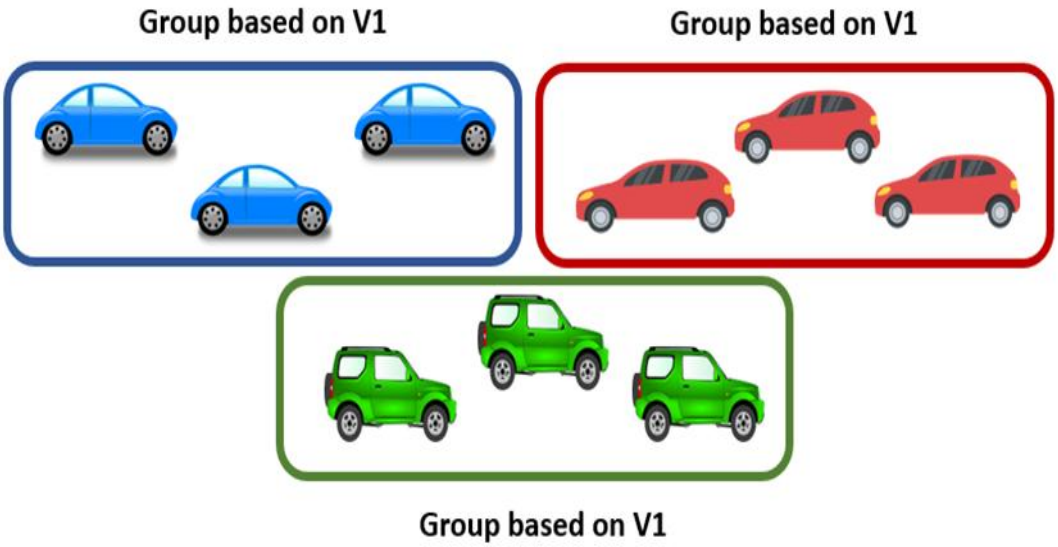

Figure 2.4: Groups of vehicles based on velocities [31]

To enhance the efficiency of utilizing memory and pseudonyms, a Privacy Conserves Pseudonym Acquisition scheme (PCPA) is introduced [46]. In this approach, vehicles receive a single pseudonym from the Certification Administration. When additional aliases are needed, the Gao procedure generates multiple pseudonyms randomly based on the initially assigned one. Notably, RSU and PSA are not involved in this process. All communications are encrypted, and unlike other methods, the Gao algorithm-generated pseudonyms suffice for a period of ten days, offering a robust defense against syntactic attacks and confusing adversaries. This results in less burden on RSUs and significantly improves pseudonym usage efficiency.

To address concerns related to location privacy and driver information confidentiality, an alternative strategy involves the concept of a mix-zone, allowing for intersections, tolls, and traffic signals as silence regions. In the Cooperation and Silence based approach, vehicle speeds are taken into account when entering these mixed zones. Depending on the vehicle's speed, different treatments are applied. Vehicles at low speeds (20 to 40 km/h) go into quiet

method and change pseudonyms simultaneously by neighboring vehicles. For medium speeds (>40 km/h to 60 km/h), the existence of k neighbors is checked, and if present, the Readyflag is set to 1, leading to cooperative pseudonym changes with surrounding neighbors. Finally, for vehicles exceeding 60 km/h, the Readyflag bit is set to 0, and a pseudonym change occurs. This strategy effectively confuses adversaries and minimizes traceability, especially in scenarios with high neighbors in a mixing zone [47]. Similarly, techniques [48] [49] work in the same way.

2.4 Analysis of Pseudonym Utilization Strategies in Vehicular Ad-hoc Networks

Pseudonym-changing schemes are discussed earlier and categorized into Mix-Zone and Mix-Context schemes. In Mix-Zone strategies, pseudonyms change upon entering a predetermined geographic zone, while Mix-Context strategies involve pseudonym changes based on contextual factors. The earlier schemes were delineated in relation to their fundamental concepts, procedures, advantages, and limitations. This section provides a summary of prior pseudonym-changing schemes, including their conceptual ideas, operation, strengths, and weaknesses

Table 2.1: Comparison of Pseudonym-based strategies in Vehicular Ad-hoc Network

Scheme	Basic idea	Mechanism	Advantages	Limitations
DPSZ [27]	Enhance location privacy protection in IoV by forming pseudonym swap zones between vehicles.	Vehicles establish temporary zones dynamically with nearby vehicles to secretly change pseudonyms to enhance privacy.	Enhances location privacy by to secretly swap pseudonyms within dynamically formed zones with neighbor's vehicles.	The communication needed to dynamically form pseudonym exchange region, especially in huge traffic.

EPCP [30]	Efficiently use pseudonyms and maximize vehicle anonymity in iov	Vehicle's estimated next condition, direction, and speed thresholds to decide suitable nearby vehicles before sharing pseudonym swap alerts to reduce unnecessary pseudonym consumption and maximize anonymity.	Less pseudonym consumption, reduce BSM loss rate, maximize confusion for adversaries, and make better anonymity with lower traceability	Encouragement procedure is not founded to buoy up selfish entities to take part in pseudonym swapping procedure.
DMLP [31]	To change pseudonym a Virtual CMIX zone is created.	Vehicles send request to CS for pseudonym changing by Sending a message RNP in response sends a COMMAND message to RSU to establish a CMIX zone and change the pseudonym.	Vehicles do not goes in silent mode in duration of CMIX zone to prevent compromise on security.	May be take more time in decryption of BSM.
PPC [46]	Offers a smart implementation for vehicles to balance quality and security by selectively preserving nodes during pseudonym swapping to serve as a transmission backbone.	Utilizes Nearby Density Quotient to determine which vehicles should sacrifice privacy, remaining available for message relaying instead of entering silent periods.	Optimizes QoS while safeguarding privacy by adjusting trade-offs based on density and application requirements.	In case of sparse traffic, the anonymity of vehicles can be compromised.
F-iov [37]	Disseminate management of pseudonym in vehicular	Generate and distribute pseudonym through localized	Reduced overhead, timely pseudonym distribution, and	When vehicles enter in silence mode, no mechanism is

	networks through computing fog for vehicle's efficiency and privacy.	authorities at the network edge for good management and optimize location privacy.	context-aware pseudonym changing allowed by localized authorities in fog computing.	introduced to develop anonymity set.
PAPU [35]	Exchange pseudonyms with same matrices in range vehicles.	V_i send request to nearby vehicle, give their id to RSU and considered vehicles reply back with a message to be part of swapping by provide their own real id to RSU.	Lesser consumption of pseudonym and greater vehicle's unlinkability.	No procedure is mentioned to tackle internal adversary attack.
EneP-AB[36]	Adaptive beacon intervals are used for privacy protection.	Alteration of pseudonyms with variation of speed, position, and neighbors.	Enhance privacy protection against pseudonym linking attacks upto 65% as compared to other approaches.	Not better for sparse traffic conditions.
CADS [37]	Utilization of Silent Period for pseudonym changing	In silent mode duration drivers can select high and low privacy level Pseudonym along with nearby vehicle changes.	Minimize large extent traceability.	If silent zone is not developed for extended period, it results in revealing information.
DGVP [38]	Make dynamic groups on the basis of context information.	Speed grouping on the basis of vehicle's position. If number of vehicles are more than threshold value, then pseudonyms are swapped otherwise virtual pseudonym swap is selected.	Adversary can get access to information in case vehicles are moving in high pace.	Low secure to implement for sparse traffic conditions.

TAPCS [32]	Utilization of silent mode for pseudonym swap.	When vehicle's speed is lowest for certain time, this shows vehicle exist in crowd then it do not transmit BSM and update its pseudonym. Vehicles with maximum velocity share beacon.	Protect from linking attacks.	Have low anonymity during dense traffic.
RPRep [35]	A robust and privacy-preserving reputation management strategy for pseudonym-allowed VANET.	Setup service and feedback reputations to recognize and highlight malicious behaviors, working with hidden-zone and k-anonymity approaches to secure from reputation link attacks during pseudonyms modification.	Robust against self-promoting and bad-mouthing attacks and protects location privacy against reputation link attacks during pseudonyms modification.	When intruders connive to reveal target vehicles then not fully deals the warning of fraud in the k-anonymity scheme.
VLPZ [34]	Give reward to utilized silent mode.	Vehicles use router for zone entrance to become silent, modify their pseudonyms and escape route through aggregator.	Enhance anonymity in case of vehicle's cooperation.	Implementation is costly especially when RSU's bring into service.

CMIX [39]	Optimize location privacy and security in (VANETs).	Reduce linkability attacks, preserve cuckoo filter injection, and save mix-zone key leakage as compared to existing research.	Give mutual authentication unlinkability, unforgeability.	Performance evaluation results are not efficient.
RRCLP [40]	Advise selfish Nodes to be participant in the process of Pseudonym Changing.	An award is given to Vehicles that modify their pseudonyms in a dynamic zone.	Maximize the size of anonymity and protect from adversary attacks.	Maximum pseudonym consumption.
BSP [41]	Enhance vehicle's location, security and protection for in IoV.	Proposed broadcast and silence period pseudonym change strategy is that vehicles intermittently broadcast or silence BSMs and change pseudonyms in mix zones selected by analyzing vehicle trajectory data.	While minimize the negative influence by utilizing radio silence on vehicle protection, allow better security protection against linking attacks like syntactic and semantic 51% as compared to prior strategies.	Might not completely express the complexity of real-world vehicle trajectories because simulated data is used in experimental evaluation.
PCS [42]	Modification of pseudonym at social spots.	During modification of pseudonyms those traffic signals and shopping malls are considered whose change red into green.	Enhance privacy upto 65% in more dense traffic scenarios.	Not good in sparse traffic scenarios.
UPCS [43]	At signalized convergence a silent zone is	A silent zone contain red traffic light vehicles	Minimum consumption of pseudonym	Not useful in condition of sparse traffic.

	established.	decide to modify or swap pseudonyms in the zone.	because of exchange mode.	As vehicles modify pseudonyms only for the red signal. Therefore, on other signals traceability can occur.
CSLPPS [44]	Considering a Silence mode While changing pseudonyms.	Vehicles are shifted to silent mode when life span of pseudonym expires for changing pseudonym.	Very difficult for attacker to trace the desired vehicle after escaping from the silent zone.	During silence mood safety messages get overlooked.
PCPA [41]	Gao algorithm is utilized for replication of pseudonym	After encryption only one pseudonym is given by PCA after encryption, Then this Pseudonym is converted into many pseudonym by the Gao algorithm for 10 days usage.	Memory efficient approach that do not rely on RSU.	Pseudonyms randomization is a challenge. If an entity becomes malicious, no method is available to identify it.
CRSM Z[46]	Traffic stuck and highways are think to be as mixzone.	Speed in the mixed region checked, whichever lowermost, average, or uppermost, treated as per speed.	Provides high anonymity in zones and reduces 55% traceability as compared to previous techniques.	Vehicle with lowest velocity moved to silence therefore, not much effective for safety purpose.

As various schemes are presented, each has its merits and drawbacks, comprising of two major categories. Mix-context techniques and Mix-Zone strategies. Both categories offer

high security, they also exhibit high pseudonym consumption, resulting in increased computation overhead and additional memory requirements, making them costly to implement.

2.5 Research Gap and Directions

While VANETs greatly enhance over transportation systems and minimize road accidents, but the security of vehicle's location, vehicle information, driver and passenger personal data remains a serious concern. Intelligent Transportation Systems (ITS) have improved the quality of life but still have vulnerabilities which must be considerable. A main issue is securing vehicle anonymity among these networked vehicles. Substantial research purposes to give a boost to security and anonymity, up till now attaining robust anonymity still an open challenge. Existing methods vehicles fail to account for real distances between vehicles when broadcasting BSMs along sensitive information. More work is needed to allow precise distance-based Messaging while protecting privacy.

2.6 Summary

The development of IoV and ITS has brought many advantages like easier transportation and reduced road accidents. However, security and data privacy in the IoV and ITS remains a serious concern. Vehicles recently use pseudonyms approach generated by CA to maintain anonymity. A lot of researches have explored to exchange these pseudonyms to secure privacy but no existing technique fully safeguards against active or passive attacks from attackers. All prior schemes still have some limitations that leaks vehicle's information, as focused in comparative assessments. While progress has been made towards privacy protection, vulnerabilities persist. Vehicles employing formulaic patterns of pseudonym changes can still risk of identification and location tracking. More comprehensive solutions for these problems are required to enable truly secure and protect IoV and ITS transmission resistant to both observation and manipulation.

CHAPTER 3

METHODOLOGY

3.1 Overview

This chapter includes the research methodology used in this study. It gives a detail description of the literature review conducted to spot this research problem and give proposed solution which is on novelty based. The simulation environment is used for the evaluation of given proposed solution. Then proposed solution explained the proposed strategy to resolve the problem find in base scheme paper with the system model, flowchart, and algorithm in this chapter. A detail explanation of each step of the algorithm is given. Finally, all the key points of the research methodology are summarized at the end of this chapter.

3.2 Operational Framework

The internet of vehicles (IoV) has brought conveniences but it also have privacy and security issues that could harm drivers and vehicles. Although it reduces accidents, but different security issues are still remaining. The communication between vehicles is through BSMs to share information for security, but malevolent vehicles may monitor to extract data for tracing vehicles. Intruders could also bring into service antennas to spy on BSMs for targeting interested vehicles. There is an interpretative need to maximize IoV privacy and security to avoid such attacks. Many researches and schemes are proposed for security issue but limitations are still there. Furthermore, studies and necessary researches of IoV security are required to strengthen protections against intruders exploiting BSMs and other weaknesses to destroy vehicles. The operational framework of the research work consists of three main phases: Analysis Phase, Design and Development Phase and Performance Evaluation Phase as shown in the below figure 3.1.

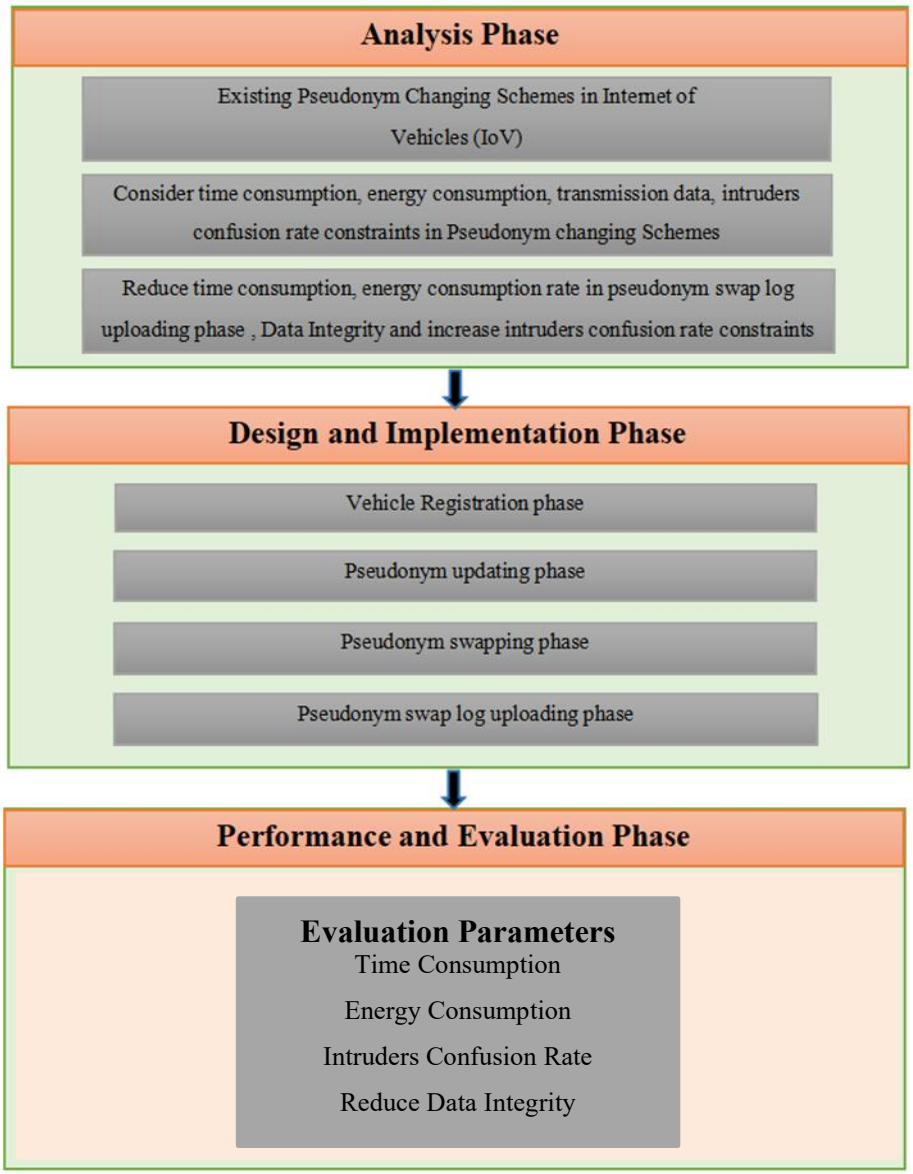

Figure 3.1: Working framework of MR-PSZ

3.3 Research Design and Development

Mutual Reporting based Pseudonym swapping zone protocol (MR-PSZ), is a secure communication protocol designed for the context of the Internet of Vehicles (IoV). The primary focus of MR-PSZ is to address challenges related to data privacy and integrity during wireless communication among vehicles. In IoV, vehicles transmit information through BSMs, containing data such as speed, location, and pseudonyms generated by a CA during vehicle registration. Instead of using real identities, vehicles employ pseudonyms to communicate safely with other vehicles and infrastructure. The Research roadmap is shown in figure 3.2.

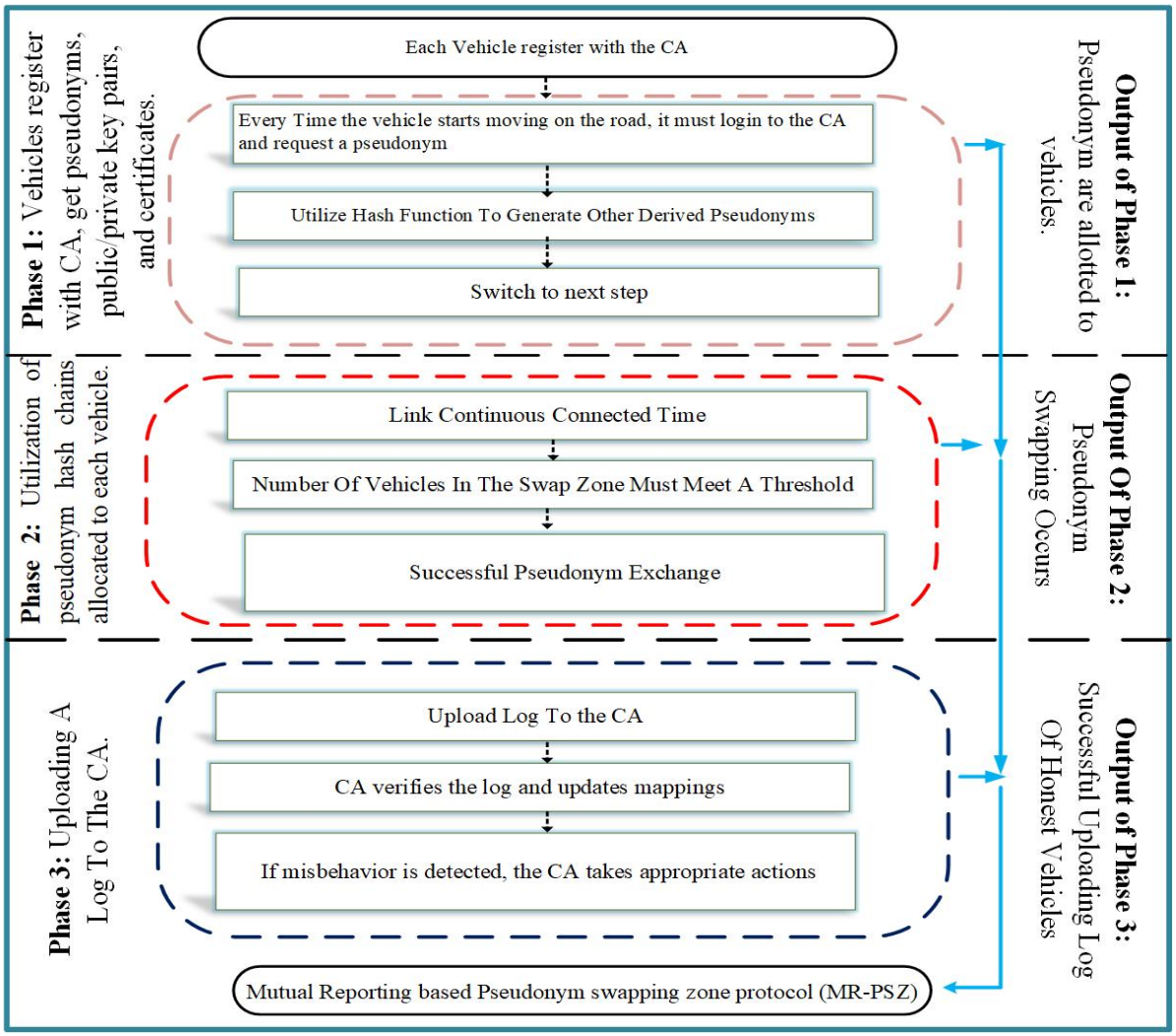

Figure 3.2: Roadmap of Research

The MRPSZ protocol introduces a systematic approach to increase security in IoV through exchange of pseudonyms when vehicles are in proximity. The model comprises of two major entities: the Vehicle Subset (VS) and the Service Organization (SO). The VS is a network of OBUs mounted within vehicles, enabling direct communication between vehicles without infrastructure support. The SI includes the CA, responsible for identity and credential management, and Road Side Units (RSUs) serving as gateways between the CA and vehicles.

The protocol functions in distinct phases, including the Vehicle Registration Phase, where vehicles register with the CA to obtain pseudonyms and credentials, and the Pseudonym Update Phase, where vehicles periodically update pseudonyms to ensure location privacy. The key innovation lies in the Pseudonym Swapping Phase, where vehicles exchange pseudonyms securely within a designated swapping zone. This swapping introduces an

additional layer of privacy and security by making it computationally challenging for intruders to link derived pseudonyms back to the original ones.

The four steps involved in a complete pseudonym swap include building a swapping zone, creating a session key using an enhanced key exchange protocol, broadcasting pseudonym swap data, and completing the pseudonym swap with encrypted messages. After a successful swap, vehicles upload a pseudonym swap log to the CA, allowing it to update the mappings between real identities and pseudonyms. The protocol considers ethical considerations, simulation and modeling for evaluation, and emphasizes the importance of disseminating research findings to contribute to the advancement of secure vehicular communication in IoV.

3.3.1 Broad Review of Literature

Around about 50 recent security related research papers were chosen and reviewed, then 20 most relevant are selected after study. The titles, abstracts, methodologies, and summaries of these research papers were studied to conduct the research problem. keyword searches and reference tracing are used to found papers. After reviewing all papers, an overview paragraph of the existing schemes and highlighted problems was written. After that a table of this review is given that analyzed idea, mechanism, strength, and limitations. A paragraph of analytical descriptions of existing approaches is given with advantages, disadvantages, and references of the strategies.

3.4 Summary

In this section, a detailed description of the research methodology, outlining the sequential steps undertaken throughout the research is discussed. Starting from the operational framework and extending to the selection of simulation tools, each stage is meticulously described.

CHAPTER 4

MUTUAL REPORTING BASED PSEUDONYM SWAPPING ZONE PROTOCOL

4.1 Overview

In this chapter, we explain the proposed technique designed to address the challenge of privacy and security. Subsequently, the system model incorporating all pertinent entities is delineated. An algorithm is then presented, with clearly defined steps aimed at enhancing readability. In conclusion, the entirety of the chapter is summarized. Finally, the whole chapter is concluded.

4.2 Mutual Reporting based Pseudonym swapping zone protocol

In IoV, the most important challenge is to secure data privacy and integrity during wireless communication. Data must be secured between both nodes from source to destination because there is always a third party that can hack and steal information and data. Vehicles transmit information and data through BSMs with other vehicles to optimized security and privacy. BSMs consist on vehicle data like speed, location area of vehicle, and pseudonyms generated by a honest party called CA through vehicle's registration. Instead of real identities Vehicles utilize issued aliases for privacy and transmit information to other vehicles and infrastructure. Prior schemes that work to provide anonymity are not ensure data integrity during communication and in base scheme CA have to wait for any excuse message to decide for further process of vehicle security and privacy. To resolve these issue, the scheme is proposed, In Location Privacy and Hiding Using Pseudonym Swapping Zone (MR-PSZ) vehicles allow to exchange pseudonyms when vehicle has many nearby vehicles.

4.3 System Model

The detail of all components of proposed scheme Mutual Reporting based Pseudonym swapping zone protocol (MR-PSZ) is given. The proposed model system in figure 4.1 consists of two main components: first one is the vehicle subnet and other one is the service setup. The vehicle subset is an adhoc of OBUs installed in vehicles that allow V2V and V2I communication. The service infrastructure includes a CA and RSUs.

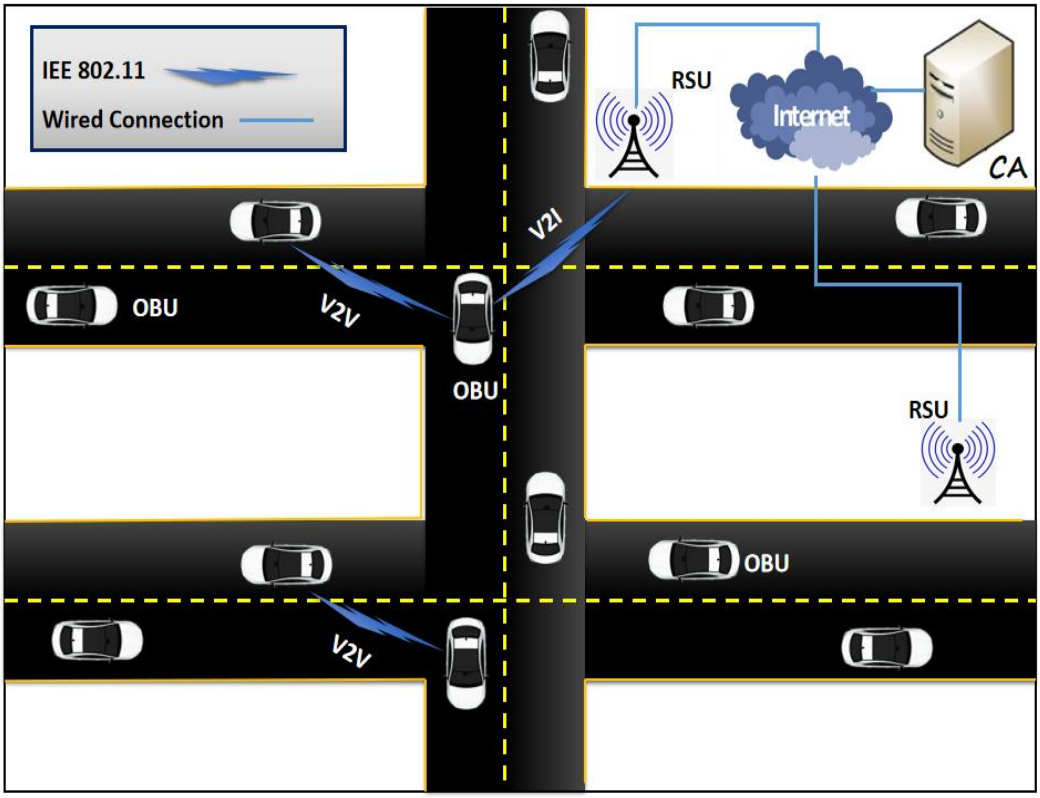

Figure 4.1: System Model of MR-PSZ Scheme

4.3.1 Vehicle Subnet (VS)

The vehicle subnet is a main component that allows direct communication between vehicles in the secure vehicular network. It be formed of an ad hoc network made by OBUs that installed on each vehicle. The vehicle subnet allows the connection that allows vehicles to communicate each other without infrastructure support.

4.3.1 OBUs

The OBUs enables vehicles to communicate in both way V2V and V2I. Through V2V communication, vehicles can directly communicate with each other and share information such as warning notification about accidents to get better road safety. V2I enables vehicles to put requests to and get information from RSUs and the broader network infrastructure.

4.3.2 The Service Infrastructure (SI)

The service infrastructure includes a CA and RSUs. he services infrastructure is a critical constituent of the secure vehicular communication system that allow coordination centralized management. It consists primarily of two elements CA and RSUs.

4.3.2.1 Certification Authority (CA)

The CA is the trusted party that is responsible for identity and credential management. It gives pseudonyms and certificates to vehicles to allow their privacy protection. If needed, then CA can revoke credentials. The CA allows communication by issuing credentials, within the vehicular network.

4.3.2.2 Road Side Units (RSUs)

The RSUs behave as the gateways among the CA and vehicles. RSUs receive request messages from OBUs. They pass on these requests messages to the CA to get the necessary credentials or other information requested. RSUs also send messages from the CA back to vehicles.

4.4 Phases of MR-PSZ

The main phases of proposed scheme are presented in Figure 4.2. Each step is explained within detail also.

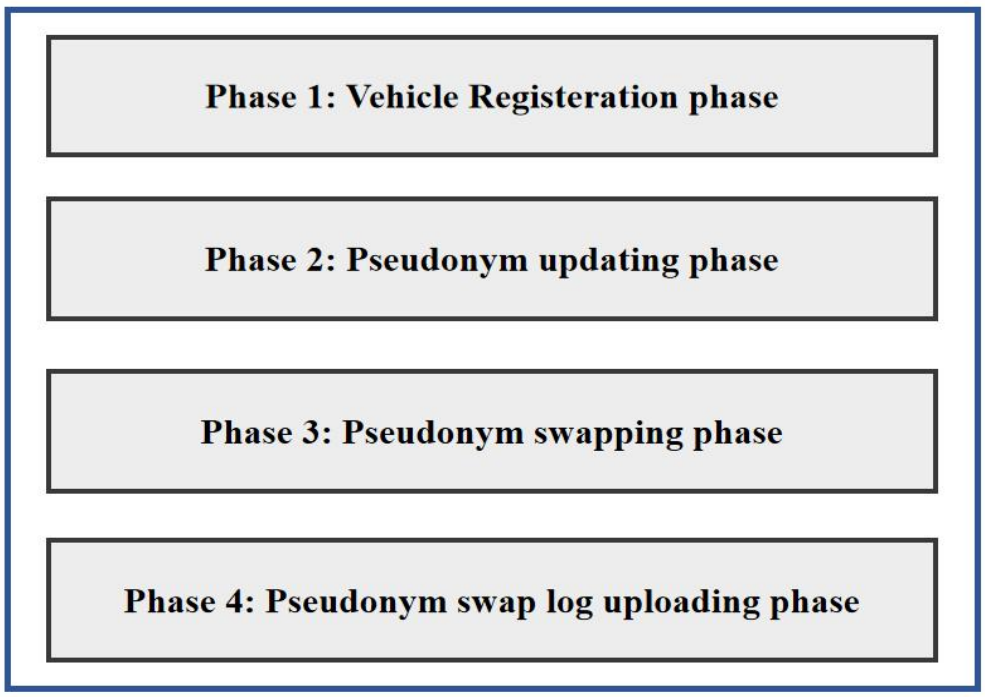

Figure 4.2: Phases of MR-PSZ scheme

4.4.1 Vehicle Registration Phase

During communication while connecting to the network, each vehicle (e.g. C_1) must register with the CA. After registering, every time the vehicle starts moving on the road, it must login to the CA and ask for a pseudonym (PID_1), with public and private key pair (PK_1, SK_1), and with this C_1 also need corresponding certificate $Cert_1$. Additionally, C_1 requires to get a secret key (K_1) from the CA to produce derived pseudonyms. Public key used encrypt messages or pseudonyms. Private key kept secret by the vehicle and used to decrypt incoming messages. This strategy may involve a secure key exchange mechanism, allowing vehicles to setup shared keys for secure communication without exposing their identities.Using K_1, C_1 can utilize a hash function to generate other derived pseudonyms as given, the first derived

pseudonym is $PID_{1,1}$ = Hash (PID_1, K_1), The second is $PID_{1,2}$ = Hash ($PID_{1,1}$, K_1)…… The k_{th} pseudonym is $PID_{1,k}$ = Hash ($PID_{1,k-1}$, K_1). It is computationally not possible for an intruder to link the derived pseudonyms back to the original PID_1 without K_1.

4.4.2 Pseudonym Update Phase

Periodic BSM by vehicles are very necessary for many applications in the IoV. To provide and maintain location privacy, vehicles use pseudonyms instead of their personal original IDs in these BSM and then communicate with RSUs and Vehicles. The proposed MR-PSZ scheme allows privacy protection by using pseudonym hash chains allocated to each vehicle. For example, vehicle C_1 starts with the last pseudonym PID_1, k from its hash chain and change it over time with its most previous ones like PID_1, k-1. By Updating pseudonyms in this way save tracking and help to maintain location privacy of vehicles. If vehicles are in sparse traffic with a very few vehicles exist in an area, so in such scenario if vehicles not swapped their pseudonyms But in case of an unchanged pseudonym in a long time period have risks to the exposure of location by attackers and leak privacy. The threshold considered for swapping pseudonyms is 60 seconds. By setting this threshold time, the system minimizes the likelihood of prolonged tracking of a vehicle by an attacker. This interval is enough to disrupt tracking attempts while still being practical for real-time implementation within the network and more effective in case of sparse traffic. Moreover, the storage capacity of hash chain is fixed, it means the availability of pseudonyms deplete is only for after some utilization. Hence, MR-PSZ approach directives pseudonym swapping upon utilizing above half the hash chain to refill pseudonyms while build up privacy.This swapping A window signaling C_1 by this swapping can start up a swap. Imperatively, the timing of this swap is unpredictable to rest of vehicles since they cannot exert a influence on C_1's pseudonym utilization history. The given scheme does not specify an accurate duration for the swapping process because it depends and based on different factors such as number of vehicles, time to generate pseudonyms. Eventually, continuous rotation and and confidentially pseudonyms swapping as managed in MR-PSZ significantly enhance location privacy in IoV.

4.5 Algorithm for Pseudonym Swapping

There are four steps that are involved to complete a complete pseudonym swap

shown earlier. Step 1 and 2 are used to build a swapping zone, and at same time utilized to create a session key, where session key is generated via enhanced Diffie-Hellman key swapping procedure. The session based key utilized for keeping the complete mechanism of pseudonym swapping. In Step 3, 4 the mechanism and handling of pseudonym swapping is presented. To overcome the chances of tracking and for efficient utilization, considering suitable context is an important factor. The Algorithm in Figure 4.3 is presented in which each step of swapping pseudonym is presented.O (n) is the complexity of the algorithm as per the number of iterations in the while loop.

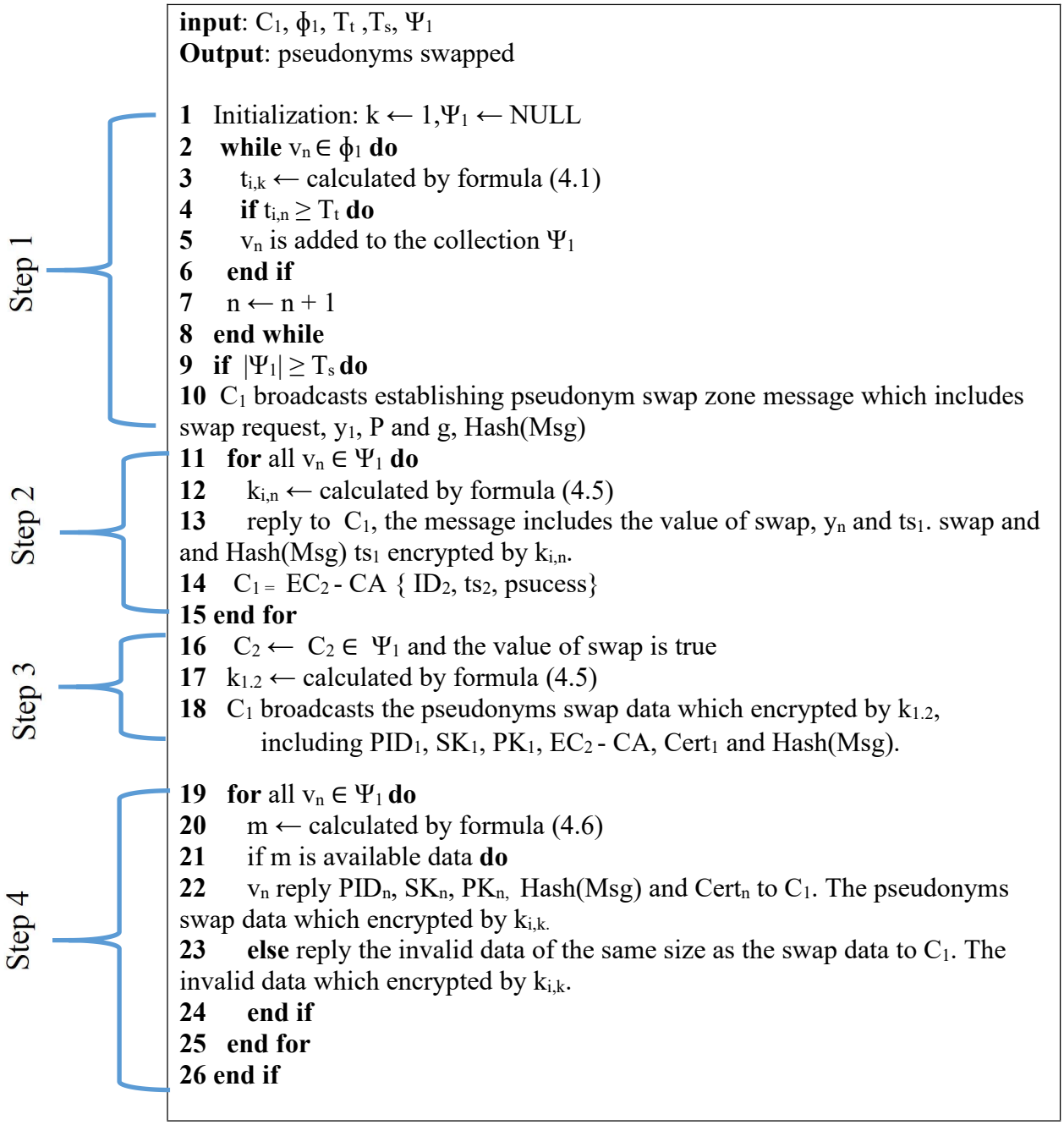

Figure 4.3: Algorithm for Pseudonym Swapping

The Set of notations used in algorithm is presented in Table 4.1.

Table 4.1: Set of Notations

Notations	Description
ID_1	Real identity of vehicle C_1
K_1	Secret key shared by C_1 and CA
PID_1,PK_1,SK_1, $Cert_1$	Pseudonym, public, private key and certificate that C_1 obtains form CA
Hash()	Hash functions of generating pseudonyms
$PID_{1,k}$	Kth pseudonym that C_1 generates by Hash(), PID_1 and K_1
ε	Attack strength of the attacker
p	Probability that a vehicle being tracked by the attacker
T_s	Threshold of vehicle number to create a pseudonym exchange region
$t_{i,K}$	Link expiration between the two vehicles
T_t	T_t Threshold of time to complete a pseudonym swap
x_1, x_n, g, P	Used to generate a secret key common parameters between C_1 and C_n
$K_{1,n}$	Session key shared by C_1 and C_n to encrypt pseudonym swap data
p_t	Probability that the eligible vehicles respond an appeal to establish pseudonym swap zone
Ψ_1	The set of nearby vehicles of C_1
REQ	Pseudonym swap request
REP	Pseudonym swap request reply
ts_1	Timestamp of step 1

4.5.1 State 1: linkage between frequent connection time

Vehicles frequently move in IoV networks, directing to dynamic, unsteady, and irregular connections between them. Before exchange pseudonyms of any two vehicles, it is necessary to compute and determine the total uninterrupted linkage time for each vehicle pair. A vehicle C_1 can get speed, direction, and location to broadcast data in BSM by any neighbor vehicle C_2. This provides C_1 to calculate its connectivity with C_2 over time as their direction and motions relate. In equation (4.1), the values of a, b, c, and d are presented as: $a = s_1\cos\theta_1 - s_2\cos\theta_2$, $b = x_1 - x_2$, $c = s_1\sin\theta_1 - s_2\sin\theta_2$, and $d = y_1 - y_2$. Here, (x_1, y_1) and (x_2, y_2), s_1 and s_2, θ_1 and θ_2, are the coordinates, speeds and directions of vehicle C_1 and C_2, correspondingly. The distance between two vehicles is r.

$$t_{1,2} = \frac{-(ab+cd)+\sqrt{(a^2+c^2)\,r^2-(ad+bc)^2}}{(a^2+b^2)} \qquad (4.1)$$

A threshold time (T_s) is required to indicate if there is sufficient continuous connected time between vehicles to get involve in the swapping zone as given in equation (4.2) where T_s is express as follow:

$$T_s = t_b + 2T_s t_r \;\; T_s \qquad (4.2)$$

T_s consists of two times t_b the broadcast time (time to send and receive a message between neighbor vehicles) t_r the reply time (time to send and receive a reply message from Gs neighbor vehicles). Considering that the exchange region composed T_s nodes, C_1 has T_s t_r for gaining the rerun notification by its adjacent nodes by every replay mechanism. To assess either there exists a connection among nodes C_x and C_y that help to finish a mechanism of exchanging pseudonyms, there is required to calculate the frequent linkage connection time $t_{x,y}$ as started by the BSM, then see either $t_{x,y}$ is not lower to T_s. In case, it is less, the connection among C_x and C_y will assure the sccaerio for linkage of frequent connection.

The calculations of continuous linkage time between vehicles C1 and C2 can be performed by both vehicles rather than exclusively by C1. This distributed approach ensures that both vehicles independently calculate the uninterrupted linkage time using the

broadcasted speed, direction, and location data. Each vehicle utilizes the same formula and parameters to compute the linkage time and checks if the calculated time meets the threshold for pseudonym swapping. If both vehicles determine that the conditions are satisfied, they proceed with the swapping process.

This distributed calculation method offers several advantages. Firstly, it provides reliability as both vehicles independently verify the conditions, reducing the risk of errors and increasing the reliability of the process. Secondly, it enhances security by ensuring mutual agreement between the vehicles before proceeding with the pseudonym swap, thereby preventing potential manipulation or errors by a single vehicle. Thirdly, it balances the computational load, distributing the processing effort between both vehicles and preventing any single vehicle from being overwhelmed by the calculations.

4.5.2 State 2: Size of exchanging region for pseudonym

The region of the MP-PSZ pseudonym swap zone indicates the total number of vehicles which are taking part, crucially impacts the trouble of tracing vehicles while exchanges pseudonyms. Clearly, a larger swap zone means lower probability of tracking individual vehicles. However, a vehicle needing exchange in pseudonym might not have more nearby to develop a properly sized swap zone because of the robust division of vehicles that are moving on the road. So that, require a minimum threshold size T_s to ensure privacy and of the pseudonym exchange when the accessible swap zone contains at least T_s candidates. By utilizing equation (4.3), the T_s value can intent by the likelihood for tracing p by adversaries with various attack ε. The relationship of likelihood of tracing p, the variable T_s, by adversary attack range ε is shown in figure 3. As this figure shows, the greater T_t requires to be, when the greater the probability of being traced is, and the stronger attack strengths is. Where the principles of p and ε already given for instance, p = 0.2, j =0.5, the extent of T_s can be computed, which is T_s= 5. When a vehicle C_1 requires pseudonym, initially it is verified that its nearby fulfills above both situations. Assume ϕ_1 is close vehicles set of C_1, so the set contains vehicles having sufficient uninterrupted connection to C_1 is stipulated as

$$\Psi_1 = \{C_2 | \forall C_2 \in \phi_1, t_{1,2} \geq T_s\} \qquad (4.3)$$

Where, if $|\Psi_1| \geq T_s$ that shows C_1 can form a exchange region along safe scope and C_1 start sending request of forming pseudonym swapping zone by using following steps.

Stage 1: Appeal of founding pseudonym swapping region

The introducing vehicle C_1 arbitrarily choose a greater prime number P, an element g, with a arbitrary value x_1, then computes y_1 by the equation (4.4).

$$y_1 = g x_1 \ mod \ P \qquad (4.4)$$

Next, C_1 broadcasts a request for pseudonym swap consisting its current pseudonym (PID_1, k), along with y_1, P, g, and a timestamp (ts_1). C_1 must encode the notification by its private key (SK_1), digitally signature the encoded messaging ($Sign_c$), then add its public key (PK_1) before broadcasting. Receiving vehicles can confirm the messages beginning inception by signature and public key.

Stage 2: Answer of establishing pseudonym swapping region

Afterward getting C_1's broadcast, a nearby vehicle C_2 confirm that C_1 is not spiteful by checking its digital signature $Sign_c$. If C_1 is secure, C_2 then checks if its continuous linkage time with C_1 assures the certain conditions. If so, C_2 randomly choose a number as x_2 and calculates a shared secret key ($K_{1,2}$) with C_1 in equation (4.5).

$$K_{1,2} = y_1 x_2 \ mod \ P = g^x 1^x mod \ P \qquad (4.5)$$

The nearby vehicle C_2 replies to vehicle with the recent swap value, the value y_2 and timestamp. If the requirements for exchanging pseudonyms are not fulfilled, C_2 will not send a reply. If C_2 replies with swap set to true, then C_2 can do a pseudonym swap now. On the other hand, a reply from C_2 with swap set to false be a sign that C_2 cannot currently contain a pseudonym exchange, for different feasible causes. To protect the privacy of data, C_2 encrypts the answer notification utilizing shared secret key $K_{1,2}$.To protect data privacy it is necessary to encrypt this data with session key at every time before sharing.

Step 3: Pseudonym based data exchange broadcasting:

Afterwards getting replies, early vehicle C_1 match the responses from vehicles in the swap zone, specifies whether they can do a swap or not. C_1 generate discrete secret keys $K_{1,2}$ with every vehicle in region by using y_2 from every vehicle. Then, C_1 arbitrarily take and choose a vehicle C_2 by those that replies and are able to swap pseudonyms. C_1 shares a pseudonym swap message to C_2 with current pseudonym PID_1, key pair SK_1 and PK_1, and timestamp ts_3. The broadcast is encrypted by C_1 utilizing the shared secret $K_{1,2}$ among C_1 and C_2. This make sure that only C_2 can decrypt the message, while remaining vehicles in the zone cannot get important information from the encrypted data. C_1 digitally signs the encrypted information therefore receiving vehicles can verify the message from C_1 before broadcasting.
Step 4: Pseudonym swap data reply: The existing vehicles in the region first confirm the digital signature that the notification is from vehicle C_1 afterward getting the broadcasted encoded pseudonym exchanging data from C_1. If the verification done, then try to decrypt the data by given formula (4.6).

$$m = c(y1^x2)^{-1} mod\ P \qquad (4.6)$$

Only C_2 can successfully decrypt the data because only it has the shared secret key $K_{1,2}$ with C_1. Then C_2 then encrypts its own swap data included current pseudonym PID_2, key pair SK_2 and PK_2, certificate $Cert_2$ and timestamp ts_4 using the secret key $K_{1,2}$, and sends this encrypted data back to the vehicle C_1. So rest of the vehicles cannot decrypt C_1's real broadcast data, both of them encrypt useless dummy data of the same size as C_2, using their separate session keys with C_1. To put all nodes in the exchange region return messages of equal extent to C_1, which make it tough for an adversary to locate which specific vehicle swapped original pseudonyms with C_1, on the basis of the number and sequence of communications.

4.5.3 Pseudonym Swap Log Uploading

After a successful pseudonym swap by vehicles CA no longer have the ability to link original identities to pseudonyms. This conflicts with the CA's role in finding and handling

misbehaving vehicles. So, it is necessary to vehicle C_1 must upload a pseudonym swap log to the CA after each exchange. The log provides the CA to remodel the mapping between actual identities and new pseudonyms. When pseudonym swap completes in MR-PSZ, C_1 transfer this log to CA. It comprises of the swapped pseudonyms PID_1 and PID_2 and timestamp ts_5 encoded by the session key $K_{1,2}$ distributed among C_1 and C_2. Moreover, C_1 encrypts this whole log entry with the key K_1 it shares with the CA and involves it in the upload. The uploaded log format and updates procedure details is shown in Figure 4.3.

As it is a wireless communication so, C_2 can receive the log message from C_1 and confirm that C_1 uploaded true swap data. If C_2 moves far from C_1's communication range without getting a log message, it considers something went wrong.

After waiting a random time, C_2 will send an accuse message about the failed pseudonym swap uploaded log to the CA it will also send the acceptance message to CA if it receives this log to save time and ensuring CA that C_2 received log that is uploaded by C_1. Upon receiving the log from C_1, the CA first checks that the encrypted $\{PID_1, PID_2, ts_1\}K_{1,2}$ matches the separately encrypted portion under K_1, and that ts_5 is recent. The CA then waits a preset time to see if an accusation about C_1 arrives from C_2 then CA will upload this log to C_2.

If all goes smoothly, the CA updates the real identity to pseudonym mappings for C_1 and C_2. Otherwise, the CA investigates if C_1 or C_2 misbehaved. If the CA confirms misbehavior by any one of these vehicle then: (1) it expel that vehicle from the system (2) blacklist it (3) revoke its public certificate (4) undo the pseudonym swap. It will also inform any victim vehicle to re-login and get a new pseudonym, certificate and shared CA key. CA can also resolve contradictions when vehicle C2 shares an accusation message by cross-verifying the log details provided by C1 with the accusation from C2. The CA first verifies whether it received the log from C1, checking that it contains the correct pseudonym swap data, timestamp, and encryption with the session key shared between C1 and C2. If discrepancies arise, the CA investigates further by requesting additional information from both vehicles and reviewing network logs to trace the sequence of events. The CA determines whether C1 or C2 engaged in any malicious activity or failed to follow the protocol correctly, and then takes appropriate actions such as revoking credentials or blacklisting the misbehaving vehicle. The victim vehicle would then re-initiate its pseudonym update and swap using the new credential. SHA-3 Hash Function is used to ensured message integrity

before sending message, creating a special fixed-size representation of the message content. The hash value can be sent parallel to the message, allowing recipients to verify its integrity by comparing the hash of the new received message to the actual value of hash.

This approach enhances the overall security and trust within the vehicular network by ensuring that pseudonym swaps are conducted correctly and securely. By holding vehicles accountable for their actions and promptly addressing any discrepancies, the CA maintains the integrity of the pseudonym swapping protocol. This not only protects the privacy of vehicles but also reinforces adherence to security measures, thereby maintaining the robustness of the network's privacy and security framework.

4.6 Summary

In this chapter, our objective in-depth understanding of the proposed scheme is presented. A complete description of the entire technique is provided. Subsequently, the proposed model is presented, elucidating the functionalities of all objects. Following this, algorithm for the MR-PSZ is incorporated, accompanied by a detailed description of each step.

CHAPTER 5

RESULT AND ANALYSIS

5.1 Overview

This chapter includes a comparative analysis is conducted between the proposed (MR-PSZ) technique and several existing schemes. The results are formulated, and an in-depth analysis is carried out through simulation methods. In the evaluation process, essential metrics are taken into account from the perspective of anonymity.

5.2 Tools used for Simulation

To assess the effectiveness of the proposed (MR-PSZ) protocol, a thorough simulation was conducted by utilizing the OMNet++, SUMO, and PREXT software, which are developed upon the Veins framework. OMNet++ served as the system construction simulator, a stable and open-source tool built on the C++ library and framework for constructing network models. In order to emulate real-world vehicle mobility scenarios, the Simulation of Urban Mobility (SUMO) simulator was employed. SUMO is recognized as a traffic mobility simulator, facilitating the observation of large-scale traffic models.

For evaluating privacy metrics, the Privacy Extension-PREXT was employed. The PREXT is only works with the Ubuntu operating system developed by Emara et al. [50], PREXT serves as an extension of Veins and supports various scenarios employing the swapping of pseudonyms. It familiarizes the concept of a Global Adversary trying to get access on BSM to ascertain vehicle identities.

The co-simulation of SUMO was made possible through communication via TCP protocol. SUMO ran concurrently, with data exchanged through the TCP socket using port 9999. The simulation employed a map downloaded from OpenStreetMap (OSM), converted into a network file. Additionally, a polygon file was generated to depict buildings and other infrastructure realistically. To define the routes of vehicle trips, file was constructed and configured.The network topology was created by including .net, .h, and .cc extension files. Privacy metrics were incorporated using PREXT, establishing communication in SUMO through TCP socket communication on port 9999.

The specified simulation parameters for the proposed schemes and their associated values are shown in Table 5.1.

Table 5.1: Parameter with values

Parameter	**Value**
Simulation duration	1900s
Area allotted for Simulation	3200m * 3200m
Total Roads	50
No. of Vehicles	50-950
Interval for BSM dissemination	10s
Radius for communication	350m
Size of BSM	80 bytes
Acknowledgment packet	40 bytes
Speed	15 km/h-95km/h
Adversary ability of attack	0.49-0.94
Total Road Side units	150

5.3 Communication Cost

The self-adaptive communication environment is devised to mitigate communication costs in regions with high vehicle density. The communication cost is described as the size of

packets generated during vehicle communication scenario. Figure 5.1 illustrates a contrast of communication costs in both cases with and without the self-adaptive communication environment. In environments with sparse vehicle density, the communication costs in both scenarios are comparatively similar. Though, as the number of vehicles rises, a visible difference arises. When the number of vehicle reaches to 500, the communication costs in the self-adaptive scheme become stable, while those in the non-self-adaptive scheme continuously increasing.

The simulation results demonstrate the effectiveness of the self-adaptive scheme in controlling communication costs in high vehicle density environments. Given the substantial computational requirements for producing, sending, receiving, and processing extensive communication data, proposed scheme effectively lessens the communication overhead that ultimately reduces computation cost. When there are 600 vehicles on road, in case of self-adaptive mode, the communication cost is 170 Bytes while for non-self-adaptive approach the communication cost is 220 Bytes.

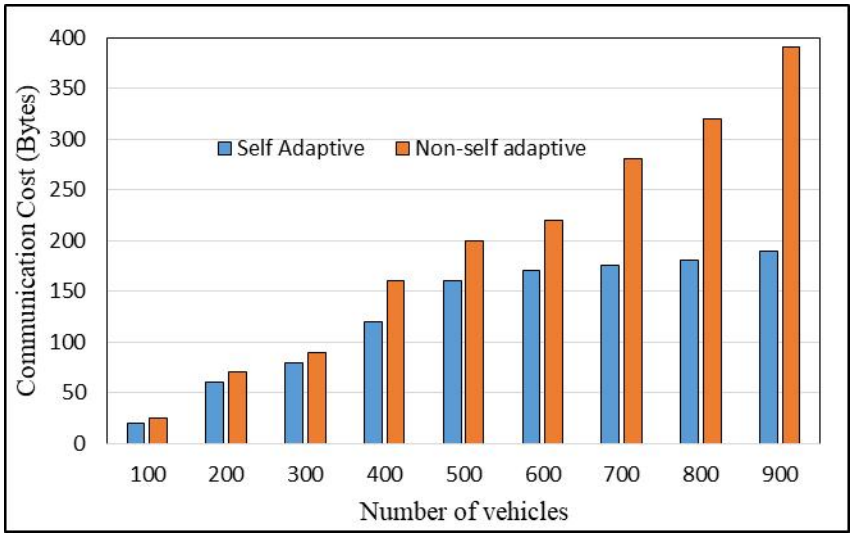

Figure 5.1: Communication Cost

5.4 Impact on Average anonymity Entropy by participant vehicles

The simulation results show that T_s values have high influence on the regular anonymity entropy of vehicles.In this scheme, entropy refers to the measure of

unpredictability correlated with the pseudonym changes. Maximum entropy refers higher unpredictability in pseudonym utilization by vehicles and vice versa, which improving vehicle's privacy by making it difficult for intruders to track vehicle paths. In figure 5.2 it can be observed that that an increase in T_s results in gradual decrement on the regular entropy of anonymous for vehicles. This decrement in anonymity is because when T_s increases, the frequency of pseudonym swaps per unit distance decreases for vehicles.

As T_s values increase, vehicles execute pseudonym swaps less frequently for the period of the same distance traveled. So, the average entropy for anonymity displays a constant decline. Notably, Figure 5.2 represents a substantial drop in anonymity entropy when T_s exceeds 8. Adjusting T_s values directly impacts the frequency of pseudonym swaps and, consequently, the overall entropy of vehicles. When T_s equal to 11, the attained entropy is 9.

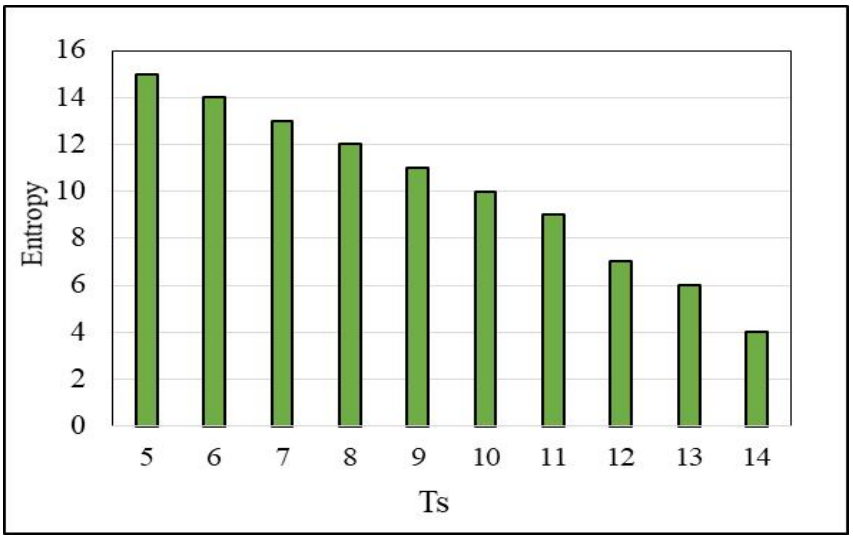

Figure 5.2: Average anonymity Entropy under varying value of T_s

5.5 Average attained Anonymity

Figure 5.4 shows an analysis of entropy of anonymity and the likelihood of vehicles traced in varying density of vehicle. Figure 5.3 represents the average attained anonymity entropy under sparse to dense traffic. The graph indicates that when vehicles increase in number, the anonymity of the all techniques shows a rises in upward fashion. When the average entropy of anonymity increases, it increases the privacy of vehicles ultimately lessens

the likelihood for vehicles being traced. The average anonymity in the MR-PSZ scheme is high due to its innovative approach to pseudonym swapping and location privacy maintenance. By introducing a dynamic pseudonym swapping mechanism, vehicles continuously update their pseudonyms, making it challenging for potential attackers to trace and identify them over time. In the SlotSwap technique, exchange of pseudonym is performed at least for 2 vehicles results in minimum effectiveness which ultimately results in lower anonymity, The PSNV and DPSZ has better anonymity due to suitable partition of zones for swapping.

The x-axis represents number of vehicles while y-axis represents attained entropy. When there are 500 vehicles, DPSZ achieves entropy of 23, while PSNV has entropy of 18, slotswap has entropy of 9, DMLP has entropy of 12,and proposed scheme has entropy of 30.

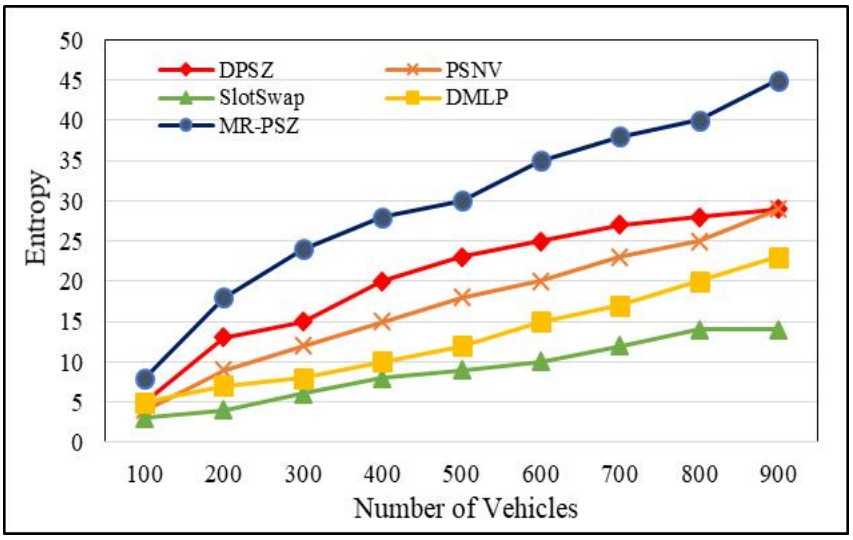

Figure 5.3: Average attained anonymity

5.6 Attained Traceability

When anonymity is high, chances of being traced is reduced. So, the anonymity is inversely proportion to traceability. The chance of being traced lessens as the vehicles increases in number. When vehicle density surges, many vehicles fulfill the exchange conditions, thus improving anonymity and dropping the likelihood of being chased. The traceability is low in the MR-PSZ scheme due to its strategic use of pseudonym swapping and the dynamic nature of the pseudonym update process. The scheme employs a continuous

rotation of pseudonyms through hash chains, ensuring that a vehicle's real identity remains concealed during communication. Pseudonym swapping is initiated unpredictably, making it difficult for potential attackers to anticipate or influence the timing of these swaps. The conditions for establishing pseudonym swap zones, including link continuity and a minimum threshold size, add an additional layer of complexity for anyone attempting to trace vehicles. DPSZ and PSNV maintains lower tracking probability because of higher anonymity while DMLP and slotswap has not selected context wisely to change pseudonym that results in increasing tracking probability as illustrated in figure 5.4. When number of vehicles is 600, the tracking probability of adversary remains 3, 7, 15, 10 and 2 in DPSZ, PSNV, Slotswap, DMLP and MR-PSZ respectively.

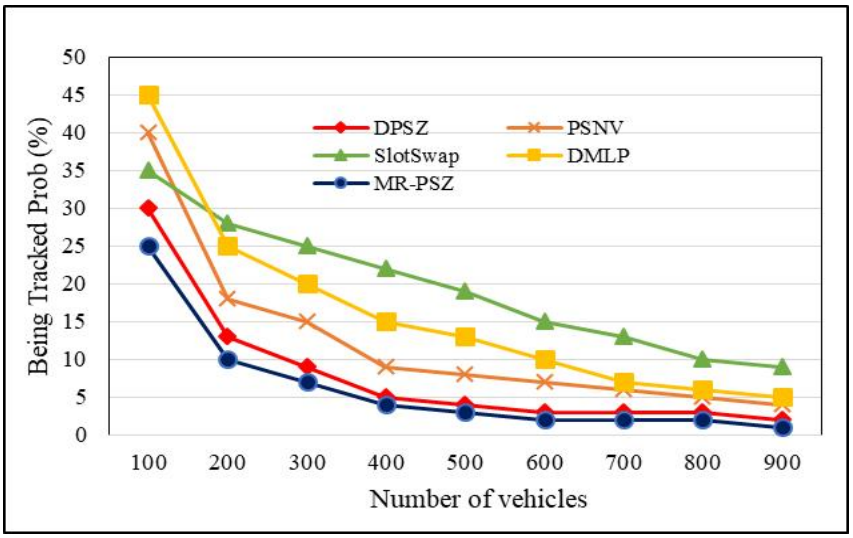

Figure 5.4: Average attained traceability

5.7 Effect of vehicles speed at anonymity

The vehicles speed has high impact on attained anonymity. In figure 5.5, the trend shows an initial decline and then rise. At stable speed, vehicles achieve higher level of anonymity. As speed of vehicle increase, the dynamics of nearby vehicles change rapidly, leading to a higher number of neighboring vehicles needed for pseudonym swap. All scheme touches its highest anonymity at different vehicle speeds: 51 km/h for DPSZ, 59 km/h for the PSNV, 29 km/h for DMLP, and 39 km/h for SlotSwap and 50 km/h for MR-PSZ. The proposed scheme MR-PSZ shows high constancy in anonymous entropy and tracing

likelihood through different speeds as compared to the other techniques.The effect of vehicles speed on anonymity fluctuates from scheme to scheme. MR-PSZ displays little sensitivity to speed of vehicles. PSNV's simplistic conditional restrictions on swap members overlook the impact of high-speed operations. DMLP and SlotSwap, designed for pseudonym swap between two vehicles, are minimally affected by speed variations. In our proposed technique, the number of nodes is increased for alleviating effect of speed at exchange of pseudonyms. The formation of MR-PSZ shows a distinct pattern: an earlier surge in anonymous entropy, topping at 50 km/h speed, showed a minute decline with speeds fluctuating by 15 to 80 km/h. This configuration rises because he frequent connection time among vehicles in locality and their direction has an important role to the prerequisites for establishing a zone. Both extremely slow and fast speed overcomes the anonymity entropy as the speed of vehicles has significantly influences anonymity. When the speed of vehicles is 50km/h, the DPSZ achieves an anonymity of 26, PSNV attains entropy of 15, while slotswap has entropy of 7, DMLP has entropy of 8 and proposed technique has an entropy of 28.

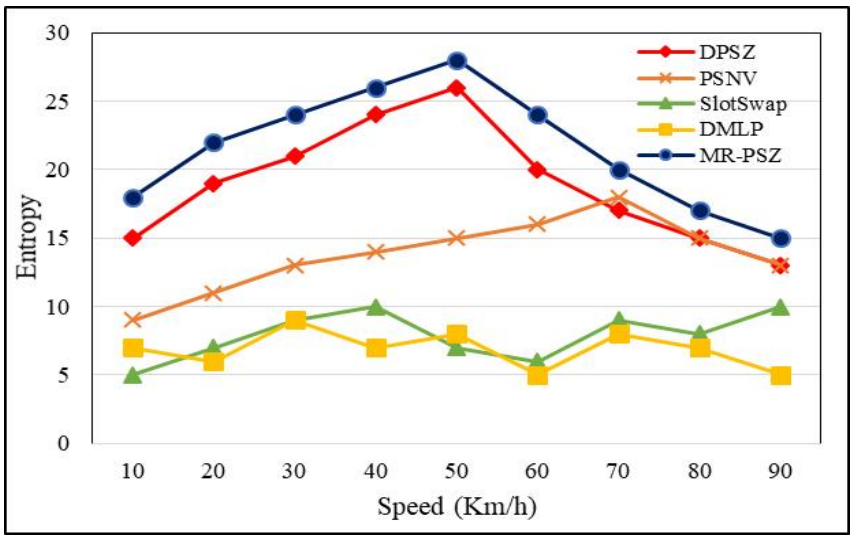

Figure 5.5: Effect of vehicles speed at anonymity

The level of anonymity has deep influence on vehicles tracking. When the level of anonymity entropy is high it overcomes the probability of being tracked. The simulation results demonstrate that when the entropy is high, the tracking probability is low and vice versa. Therefore, when the speed of vehicles is 50 km/h, the probability of traceability is lower as it is shown in figure 5.6. As the vehicle speed is 40km/h, the DPSZ achieves probability of 6, the PSNV attains likelihood of 15, SlotSwap achieves probability of 20, DMLP also maintained probability of 20 and MR-PSZ lower the chances of tracking to 5.

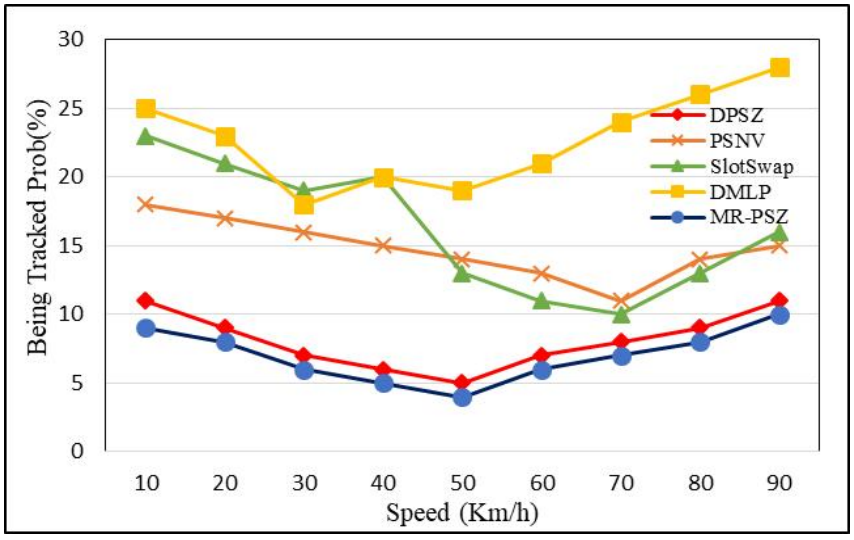

Figure 5.6: Tracking likelihood on the basis of Speed

5.8 Influence of simulation duration

Under varying duration of execution, figure 5.7 determines the mean anonymity of vehicles against likelihood of tracking. The mean anonymity of nodes escalates by prolonged runtime. The greater the anonymity level of the vehicles, diminished the likelihood of tracking. When the simulation time reaches to 1000 seconds, the attained entropy remains 13.4, 10.1, 5.5, 7.5 and 16.5 in DPSZ, PSNV, Slotswap, DMLP and MR-PSZ respectively.

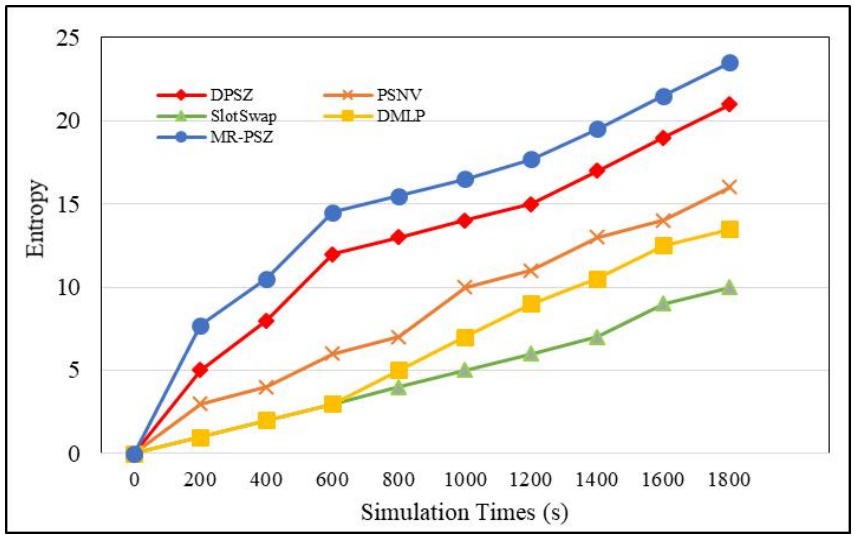

Figure 5.7: Impact on Entropy by Simulation

Through extended runtime, the likelihood of vehicle tracing gradually decreasing, and our proposed technique tracking probability is much lower comparatively to that of the other techniques. At the onset of the simulation, a greater number of vehicles necessitate pseudonym exchange, thus leading to a more rapid increase in mean anonymous entropy. Figure 5.8 shows that when simulation time is 200 s, the attained tracking probability remains 200, 20, 39, 30,45 and 15 in DPSZ, PSNV, SlotSwap, DMLP and MR-PSZ. The rate of mean anonymous entropy growth for vehicles tends to stabilize after a 450s of simulation run. Similarly, the likelihood of vehicles being tracked gradually decreases after the 450 s. The simulation runtime reveal that MR-PSZ outperforms the other techniques in terms of tracking likelihood. It shows that the proposed scheme offers high anonymity.

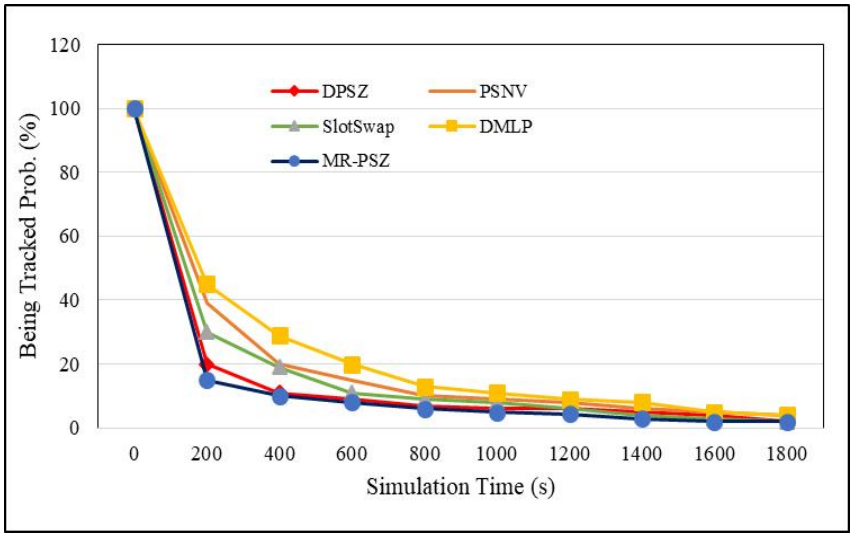

Figure 5.8: Impact of Simulation duration at tracking probability

5.9 Execution Time

Execution time refers to the duration required to complete various operations involved in pseudonym swapping, including verifying log uploads and resolving any issues such as false accusations. The execution time is slightly high in the proposed technique as CA needs additional time to verify that both vehicles, the initiating vehicle (Va) and neighboring vehicles (Vb) have received the log information message. This verification step ensures that both parties have acknowledged the swap and prevents potential disputes. If Vb sends a negative reply indicating that it did not receive the log message, the CA must spend extra time resolving this issue. This involves cross-checking the logs and potentially re-initiating

communication to confirm the swap details. The DPSZ technique has attained lower execution time as it leverages parallel processing, allowing tasks to be handled concurrently. DMLP has a high execution time because it involves complex processes for pseudonym swapping and log verification. PSNV has a high execution time due to its detailed zone partitioning and pseudonym-swapping mechanisms. The scheme requires significant processing to ensure suitable partitioning of zones and to manage the conditions for swapping pseudonyms effectively. This complexity in managing zone configurations and swap conditions increases the computational load, leading to longer execution times. Additionally, ensuring the accuracy and security of pseudonym swaps further adds to the overall execution time. SlotSwap has high execution time primarily because it involves frequent pseudonym swaps between pairs of vehicles. This constant swapping requires careful coordination and synchronization between vehicles, which increases computational overhead. Additionally, it needs to manage the timing and conditions for these swaps accurately, adding to the complexity and execution time. Moreover, ensuring the integrity and security of pseudonym exchanges during high-frequency swaps further contributes to the overall execution time of the SlotSwap scheme. The performance of all techniques is presented in figure 5.9.

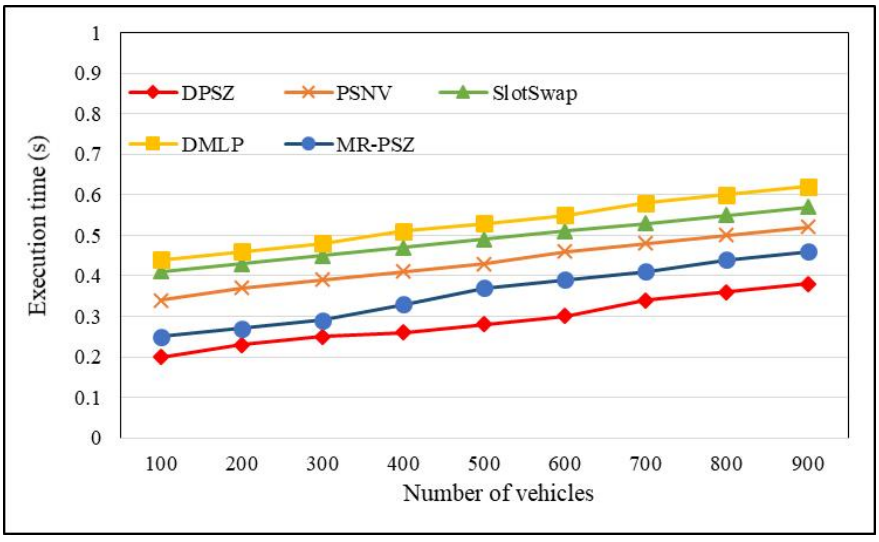

Figure 5.9: Execution Time

When surrounding vehicles are 600 in number, the execution time is 0.3s, 0.46s, 0.51s, 0.55s, and 0.39s for DPSZ, PSNV, SlotSwap, DMLP, and proposed technique MR-PSZ. The proposed technique performance is slightly down for this metric as the value of vehicles increases, it takes more time for processing.

5.10 Influence of Attack Capacity

As the efficiency of maintaining anonymity varies within a given range, there is an observable decline in average anonymous entropy as the competency for attacks upsurges. Higher attack abilities correspond to a great likelihood, denoted as "*R*" of vehicles being traced, consequently leading to a reduction in mean anonymous entropy. The likelihood of vehicles being tracked is directly associated with the value of "*R*" hence, as attackers' capabilities improve, there is an escalated likelihood of vehicles being traced. There is a substantial reduction in the anonymous entropy of vehicles when adversary's capabilities range between 0.71 and 0.76. This implies that vehicles exhibit better anonymity when attackers' capabilities remain below 0.70. Figure 5.10 shows that when attack capability reaches to 0.8, the entropy of all schemes remains 13, 8, 6, 6, and 14 in DPSZ, PSNV, Slotswap, DMLP, and MR-PSZ respectively.

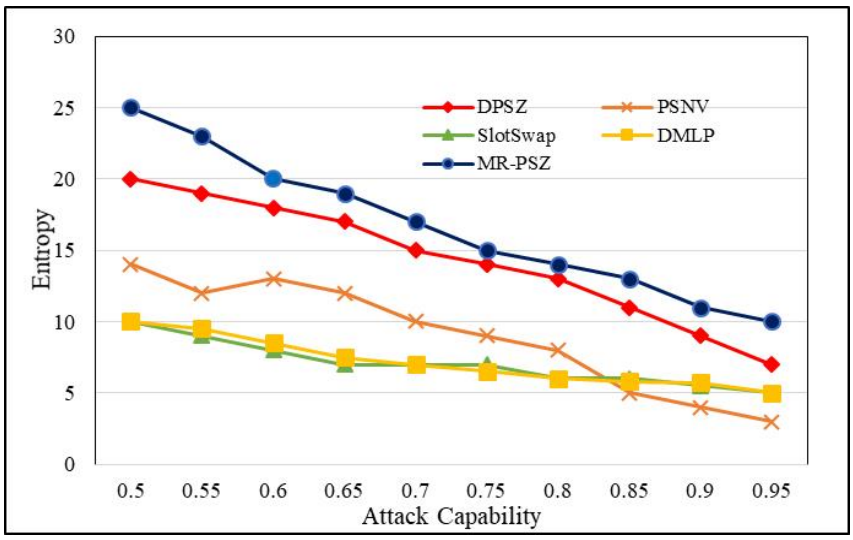

Figure 5.10: Influence of Attack Capacity

The techniques including DMLP and SlotSwap designed to facilitate pseudonym swaps among 2 vehicles, resulting in comparable average anonymous entropy values for both schemes. In the MR-PSZ scheme, during exchanging, all contributing vehicles transmit information of uniform form. This uniformity thwarts attackers' attempts to discern the introducing vehicle by examining frequency and nature of communications among vehicles, thus ensuring robust confidentiality protection. Figure 5.11 shows when the attack value = 0.75, the DPSZ, PSNV, Slotswap, DMLP and MR-PSZ maintains 9, 10, 24, 25, 8 respectively.

Across varying levels of attack capabilities, experimental findings consistently demonstrate that the MR-PSZ scheme outperforms the all other approaches for usual anonymity entropy and the likelihood of vehicles for traced, underscoring its superior confidentiality defense capabilities.

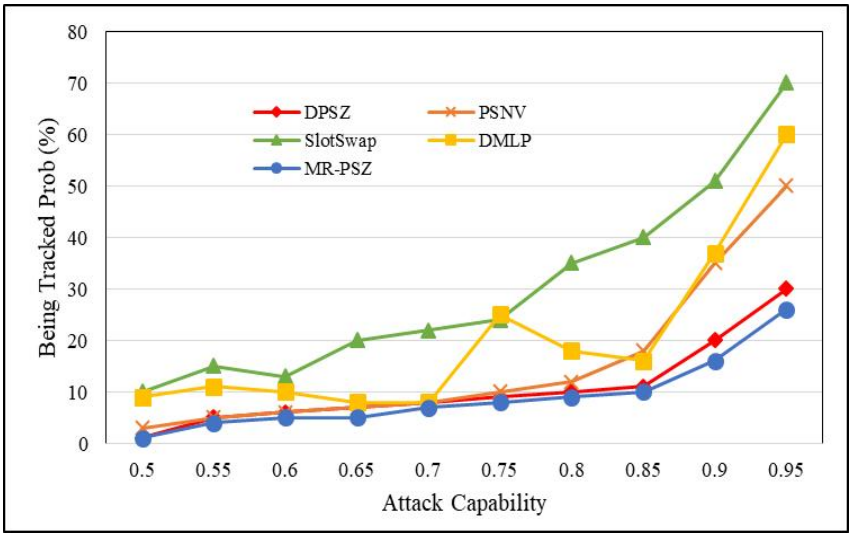

Figure 5.11: Impact of Attack Capacity on Tracking

5.11 Summary

The MR-PSZ is presented to address the critical challenges of data privacy and integrity within the Internet of Vehicles (IoV) framework. By implementing a protocol that allows vehicles to exchange pseudonyms securely while ensuring continuous connectivity and maintaining a sufficient number of participating vehicles in the exchange region, MR-PSZ aims to enhance the privacy of vehicle communication. The simulation results reveal that proposed scheme performs better in most of the evaluation metrics. So, MR-PSZ aims to establish a secure and privacy-preserving environment for vehicular communication, ultimately contributing to safer and more efficient transportation system.

CHAPTER 6

CONCLUSION AND FUTURE WORK

6.1 Overview

This chapter presents the conclusion of the research undertaken and outlines the work expected to be done in future. The primary objective of this study is to mitigate tracking planned by attacker and enhance anonymity entropy. To assess the efficacy of the proposed technique MR-PSZ, extensive simulations were conducted. The evaluation of the proposed scheme was conducted by utilizing SUMO, OMNET++, and PREXT, considering important metrics. Comparative analysis with existing schemes revealed that MR-PSZ demonstrated superior performance.

6.2 Summary of Research

The Mutual Reporting based Pseudonym swapping zone protocol (MR-PSZ) addresses critical challenges in securing data privacy and integrity within the Internet of Vehicles (IoV). It introduces an enhancement in security and privacy by allowing vehicles to exchange pseudonyms within designated swapping zones. The scheme involves two main components: the Vehicle Subnet (VS), which comprises OBUs enabling V2V and V2I communication, and the Service Infrastructure (SI), consisting of a CA and Road Side Units (RSUs).

In MR-PSZ, vehicles register with CA to obtain pseudonyms, public and private keys, and certificates for privacy protection. The protocol operates in phases, including Vehicle Registration and Pseudonym Update, facilitated by OBUs and RSUs. The core of the scheme is the pseudonym swapping phase, where vehicles exchange pseudonyms to enhance location

Privacy. The process involves establishing a swapping zone, generating session keys, and securely exchanging pseudonym swap data.

To ensure the effectiveness of pseudonym swapping, MR-PSZ incorporates conditions such as continuous link connectivity and the size of the pseudonym swap zone. These conditions prevent tracking and enhance privacy by regulating the exchange process based on connectivity and the number of participating vehicles. Additionally, the protocol includes mechanisms for uploading pseudonym swap logs to the CA for monitoring and managing misbehavior.

In summary, MR-PSZ offers a comprehensive solution to safeguard data privacy and integrity in IoV. By allowing vehicles to exchange pseudonyms securely within designated swapping zones and incorporating robust conditions and mechanisms, the protocol significantly enhances location privacy and strengthens the overall security of vehicular communication networks.

This thesis has some limitations. The proposed technique relies heavily on the timely exchange of pseudonym swap logs between vehicles and the CA, which may be hindered by communication range limitations or network disruptions. Secondly, managing dynamic pseudonym swapping within designated zones takes high execution time and it remains increasing as number of vehicles surges.

6.3 Future Work

In future, optimizing resource utilization and minimize communication overhead will be considered. Beyond this, some more latest cryptographic techniques are explored to make swapping process even more secured. Also the impact of cryptography is examined on network performance, such as latency and throughput, for ensuring efficient communication in real-world scenarios.

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.

[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.

[3] W. Afifi, H. A. Hefny, and N. R. Darwish, “A Cooperative Localization Method based on V2I Communication and Distance Information in Vehicular Networks,” International Journal of Computer Networks and Communications, vol. 13, no. 6, pp. 53–70, 2021.

[4] M. L. Bouchouia et al., “A survey on misbehavior detection for connected and autonomous vehicles,” Vehicular Communications, vol. 41, p. 100586, 2023.

[5] 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. 1–22, 2021.

[6] G N. Tabassum and C. R. K. Reddyy, “Review on QoS and security challenges associated with the internet of vehicles in cloud computing,” Measurement: Sensors, vol. 27, August 2022, p. 100562, 2023.

[7] A. Hayat, Z. Iftikhar, M. I. Khan, A. Mehbodniya, J. L. Webber, and S. Hanif, “A novel pseudonym changing scheme for location privacy preservation in sparse traffic areas,” *IEEE Access*, vol. 11, pp. 1234-1245, 2023.

[8] S. Sharma and B. Kaushik, “A survey on internet of vehicles: Applications, security issues & solutions,” Veh. Commun., vol. 20, p. 100182, 2019.

[9] Z. Afzal and M. Kumar, “Security of Vehicular Ad-Hoc Networks (VANET): A survey,” J. Phys. Conf. Ser., vol. 1427, no. 1, p. 012019, 2020.

[10] A. Abd Razak, S. Shukor, N. H. Mohd Nazari, and A. Al-Dhaqm, "Data anonymization using pseudonym system to preserve data privacy," *IEEE Access*, vol. 8, pp. 43256-

43264, 2020.

[11] Z. Zhang, T. Feng, W.-C. Wong, and B. Sikdar, “A geo-indistinguishable context-based mix strategy for trajectory protection in VANETs,” *IEEE Trans. Veh. Technol.*, 2023.

[12] 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.

[13] M. Babaghayou, M. Chaib, N. Lagraa, N. A. Ferrag, and L. Maglaras, “A safety-aware location privacy-preserving IoV scheme with road congestion-estimation in mobile edge computing,” *Sensors*, vol. 23, no. 531, 2023.

[14] 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.

[15] B. Chaudhary and K. Singh, “A dummy location generation model for location privacy in vehicular ad hoc networks,” in *Advances in Intelligent Systems and Computing*, vol. 1166, Springer, Berlin/Heidelberg, Germany, 2021, pp. 1–10.

[16] B. Moussaoui, N. Chikouche, and H. Fouchal, "An efficient privacy scheme for C-ITS stations," *Comput. Electr. Eng.*, vol. 107, p. 108613, 2023.

[17] Al-ani, R. Baker, T. Zhou, B. Shi, Q. “Privacy and Safety Improvement of VANET Data via a Safety-Related Privacy Scheme,”,Int. J. Inf. Secur. 2023, 22, 763–783.

[18] R. Al-Ani, T. Baker, B. Zhou, and Q. Shi, “ Privacy and safety improvement of VANET data via a safety-related privacy scheme,” Int. J. Inf. Security, vol. 22, no. 4, pp. 763–783, 2023.

[19] E. Alalwany and I. Mahgoub, “Security and trust management in the internet of vehicles (IoV): Challenges and machine learning solutions,” *Sensors*, vol. 24, no. 2, p. 368, 2024.

[20] B. Günay, E. Öztürk, T. Çavdar, Y. S. Hanay, and A. U. R. Khan, “Vehicular ad hoc network (VANET) localization techniques: a survey,” *Arch. Comput. Methods Eng.*,

vol. 28, pp. 3001–3033, 2021.

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

[22] H. Mistareehi, T. Islam, and D. Manivannan, “A secure and distributed architecture for vehicular cloud,” *Internet of Things (Netherlands)*, vol. 13, p. 100355, 2021.

[23] 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 Special Issue, pp. 2065–2074, 2018.

[24] D. Koutras, G. Stergiopoulos, T. Dasaklis, P. Kotzanikolaou, D. Glynos, and C. Douligeris, “Security in iomt communications: A survey,”*Sensors (Switzerland)*, vol. 20, no. 17, pp. 1–49, 2020.

[25] A. Hozouri, A. Mirzaei, S. RazaghZadeh, and D. Yousefi, “An overview of VANET vehicular networks,” *arXiv preprint arXiv:2309.06555*, 2023.

[26] J. Zeng, Laurence, T. Yang, M. Lin, H. Ning, and J. Ma, “A survey: Cyber-physical-social systems and their system-level design methodology,” *Futur. Gener. Comput. Syst.*, vol. 105, pp. 1028–1042, 2020.

[27] 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. 1–16, 2019.

[28] T. A. Butt, R. Iqbal, K. Salah, M. Aloqaily, and Y. Jararweh, “Privacy Management in Social Internet of Vehicles: Review, Challenges and Blockchain Based Solutions,” *IEEE Access*, vol. 7, pp. 79694–79713, 2019.

[29] M. Babaghayou, N. Chaib, N. Lagraa, M. A. Ferrag, and L. Maglaras, “A Safety-Aware Location Privacy-Preserving IoV Scheme with Road Congestion-Estimation in Mobile Edge Computing,” *Sensors*, vol. 23, no. 1, pp. 1–38, 2023.

[30] M. Mushtaq *et al.*, “Anonymity Assurance Using Efficient Pseudonym Consumption in Internet of Vehicles,” *Sensors*, vol. 23, no. 11, pp. 1–17, 2023.

[31] 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.

[32] S. M. A. Mohamed and Y. Wang, “A survey on novel classification of deduplication storage systems,” *Distrib. Parallel Databases*, vol. 39, no. 4, pp. 201–230, 2021.

[33] 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.

[34] A. Boualouache, S. M. Senouci, and S. Moussaoui, “Towards an efficient pseudonym management and changing scheme for vehicular ad-hoc networks,” *2016 IEEE Glob. Commun. Conf. GLOBECOM 2016 - Proc.*, pp. 0–7, 2016.

[35] J. S. L. N. Bin, “PAPU: Pseudonym Swap with Provable Unlinkability Based on Differential Privacy in VANETs,” *IEEE Internet Things*, vol. 7, no. 12, pp. 11789–11802, 2020.

[36] 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. July, pp. 359–371, 2018.

[37] K. Emara, W. Woerndl, and J. Schlichter, “POSTER: Context-adaptive user-centric privacy scheme for VANET,” *Lect. Notes Inst. Comput. Sci. Soc. Telecommun. Eng. LNICST*, vol. 164, pp. 590–593, 2015.

[38] 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. 1–41, 2021.

[39] M. S. Al-Marshoud, A. H. Al-Bayatti, and M. S. Kiraz, “Improved chaff-based cmix for solving location privacy issues in vanets,” *Electron.*, vol. 10, no. 11, 2021.

[40] 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.

[41] A. Goel and C. Prabha, “A Detailed Review of Data Deduplication Approaches in the Cloud and Key Challenges,” *2023 4th Int. Conf. Smart Electron. Commun.*, vol. 19,

2023.

[42] 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.

[43] 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.

[44] R. Rani, N. Kumar, and Meenu Khurana., “Redundancy elimination in IoT oriented big data: a survey, schemes, open challenges and future applications,” *Cluster Comput.*, pp. 1–25, 2024, .

[45] I. Ullah, A. Wahid, M. A. Shah, and A. Waheed, “VBP C : Velocity Based Pseudonym Changing Strategy to Protect Location Privacy of Vehicles in VANET,” *2017 Int. Conf. Commun. Technol.*, pp. 132–137, 2017.

[46] 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. 1–19, 2020.

[47] Babaghayou, Messaoud, et al. “A safety-aware location privacy-preserving iov scheme with road congestion-estimation in mobile edge computing,” Sensors 23.1 (2023): 531..

[48] I. Ullah and M. A. Shah, “SGO: Semantic group obfuscation for location-based services in VANETS,” *Sensors*, vol. 24, no. 4, p. 1145, 2024.

[49] Babaghayou, Messaoud, et al. “SAMA: Security-aware monitoring approach for location abusing and UAV GPS-spoofing attacks on Internet of Vehicles,” International Conference on Cognitive Radio Oriented Wireless Networks. Cham: Springer International Publishing, 2021.

[50] K. Emara, “Poster: PREXT: Privacy extension for Veins VANET simulator,” IEEE Vehicular Network Conf. VNC, vol. 1, no. 3, 2016, pp. 3–5, 2016.