A Pseudonym-based Solution for Efficient Security and Enhanced Privacy in VANET Safety Applications

Ruqayah Ayad Abduljabbar Al-Ani

A Thesis Submitted in Partial Fulfilment of the Requirements of Liverpool John Moores University for the Degree of Doctor of Philosophy

May 2020

Abstract

In Vehicle Ad-hoc NETworks (VANET) safety applications, vehicles are required to exchange messages periodically at 1-10 Hz with nearby vehicles (within 300 meters) wirelessly and in plain format. The exchanged message usually contains the state of vehicle such as its current location, speed, and direction, as well as the state of roads such as icy road, closed road, traffic jams, an accident on the road, etc. With such support, the contextual awareness of the drivers about their surrounding environment would be improved. Thus, the road safety would be significantly improved because of a potential accident can be prevented in advance.

The security of the exchanged messages is a paramount requirement because an accident, injury, or even loss of life could be a direct consequence of malicious notification. Moreover, eavesdroppers can collect the exchanged messages and track the individual driver's whereabouts by linking subsequent messages for a period of time. Thus, the location privacy of the driver must be properly protected to obtain the public acceptance of these applications.

Current standardisations and research efforts have mainly nominated the use of pseudonyms, rather than real-identities, based on Public Key Cryptographic (PKC) to provide an acceptable balance between security and privacy. The public key is excluded from any identification information and used as a pseudonym. This pseudonym must be certified by a trusted authority who can verify it later in the case of a dispute. Moreover, with the amount of information that a vehicle is required to broadcast in these applications, the pseudonym must be changed over time to avoid the long-term linkability of the vehicle via its locations. A simple pseudonym changing scheme is ineffective to prevent tracking the vehicle based on its locations. Thus,

many researchers have been working on designing more effective schemes but very few of them have considered the impact of such schemes on safety applications.

Therefore, in this thesis, we aim to design a novel scheme for VANET safety applications that can achieve efficient security and enhance the privacy level without compromising safety. First, the main requirements of these applications were specified, and the state-of-the-art schemes were reviewed. Then, two schemes have been proposed: 1) the Safety-related Privacy Scheme (SRPS) was mainly aimed to reduce the impact of enhancing privacy level on safety, and 2) the Hybrid-based Pseudonym Changing Scheme (HBPCS) was mainly aimed to reduce the impact of security overheads on safety.

To evaluate the efficiency of the designed schemes, we implemented these schemes using a combination of four simulators and then compared them quantitatively with the other five selective schemes from the literature (CAPS, PPC, RSP, CSP, and SLOW). The experiment results have shown that the SRPS can achieve the best balance between the three key issues (security, privacy, and safety) but its efficiency decreased in traffic jams, which has been addressed by the HBPCS.

Acknowledgment

In the name of Allah, the Most Gracious and the Most Merciful

All praises and thanks are due to Allah for enabling me to stay strong, patient and courageous to undertake this thesis and reach the stage of accomplishment.

I would like to express my sincere gratitude to my supervisors, Dr Bo Zhou, Prof Qi Shi, and Dr Thar Baker Shamsa for their enthusiasm for the topic, their support, encouragements, recommendations, and patience. I would also like to thank Prof Ali for his support at the early stages of my PhD.

I am also thankful to the Iraqi government represented by the Ministry of Higher Education and Scientific Research and its representative in the UK, the Iraqi cultural attaché through the University of Anbar in Iraq for granting me a scholarship to pursue my PhD.

Special thanks are also owed to the staff at the Department of Computer Science at Liverpool John Moores University for their support and courage during the period of my study. Many thanks are to our administration officers, especially Tricia Waterson. I am also thankful to the CS-techs, especially Paul Cartwright and Ian Fitzpatrick, for their assistance and patience in setting up, maintaining and troubleshooting the software.

I would like to express my profound gratitude to my parents for their love and support to keep me strong and persistent. I also wish to express my gratitude to my sisters, Fatima and Aisha, and brothers, Yousif, Omar, and Abdul-Jabbar. I would also like to thank my brother-in-law, Fadhil, as well as my friends, Rokayah, Sawsan, and Ruba, who provided me with everlasting inspiration. Finally, my special thanks are to my lovely husband, Riyadh and daughters, Hanan and Rawan, for being always supportive and helpful throughout my PhD journey.

Publications and contributions

- Ruqayah Al-ani, Bo Zhou, Qi Shi, Thar Baker, and Mohamed Abdlhamed (2020), "Adjusted Location Privacy Scheme in VANET Safety Applications", accepted in the NOMS-ITCVT 2020.
- Ruqayah Al-ani, Bo Zhou, Qi Shi, Thar Baker, Yue Gao (2020), “Privacy and Safety Improvement of VANET Data via Safety-related Privacy Scheme”, IEEE Internet of Things Journal, under correction.
- Ruqayah Al-ani, Bo Zhou, Qi Shi, and Ali Sagheer (2019), “Privacy Preserving Scheme for Safety Applications in VANET”, Faculty Research Conference 2019 in LJMU.
- Ruqayah Al-ani, Bo Zhou, Qi Shi, and Ali Sagheer (2018), “A Survey on Secure Safety Applications in VANET”, 2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th Intl. Conference on Data Science and Systems
- Ruqayah Al-ani, Bo Zhou, Qi Shi, and Ali Sagheer (2018), “An Improved Elliptic Curve Digital Signature Algorithm for Vehicular Ad Hoc Networks”, IEEE UK & Ireland YP Postgraduate STEM Research Symposium, 2018.
- Ruqayah Al-ani, Bo Zhou, Qi Shi, and Ali Sagheer (2017), “Authenticated Real-time Privacy Preserving in VANETs”, Faculty Research Conference 2017 in LJMU.
- Ruqayah Al-ani, Bo Zhou, Qi Shi, and Ali Sagheer (2018), “Secure Real-time communication for VANET”, Faculty Research Conference 2018 in LJMU.

Table of Contents

CHAPTER 1 : INTRODUCTION *1*

1.1 Overview **1**

1.2 Motivations **3**

1.3 Research Aims and Objectives **6**

1.4 Contributions **8**

1.5 Thesis Structure **9**

CHAPTER 2 : VEHICULAR AD HOC NETWORKS BACKGROUND *10*

2.1 Overview **10**

2.2 VANET Architecture **11**

2.3 VANET Safety Applications **13**

2.4 VANET Safety Applications Requirements **14**

2.5 Attacks on VANET **17**

2.5.1 Attacker Models 17

2.5.2 Basic Attacks 18

2.6 Security Requirements in VANET **18**

2.7 Privacy Requirements in VANET **20**

2.8 Problem definition **21**

2.9 VANET supportive characteristics **22**

2.10 Summary **23**

CHAPTER 3 : LITERATURE REVIEW OF SECURITY AND PRIVACY-PRESERVING SCHEMES FOR VANET APPLICATIONS *25*

3.1 Overview **25**

3.2 Categories of Cryptographic Mechanism Schemes **26**

3.2.1 Public Key Cryptography 27

3.2.2 Identity-based Cryptography 28

3.2.3 Group-based Cryptography 29

3.2.4 Symmetric Cryptography 29
3.3 Cryptographic Schemes for VANET Safety Applications 30
3.4 Communication and Computation Overheads in PKC using ECDSA . 31
3.5 Pseudonym Management Schemes 33
3.6 Pseudonym Changing Schemes 36
3.7 Privacy Metrics 39
3.8 Vehicle Tracker 40
3.9 Summary 44
CHAPTER 4 : PRIVACY SCHEME FOR VANET SAFETY APPLICATIONS 45
4.1 Overview 45
4.2 Motivation 46
4.3 Proposed Safety-related Privacy Scheme 48
4.3.1 Algorithm1: SRPS-Active 52
4.3.2 Algorithm2: SRPS-Silent 53
4.4 Implementation 56
4.4.1 System overview and assumptions 56
4.4.2 VANET Simulation 57
4.5 Evaluations 61
4.5.1 Comparison 61
4.5.2 Setting up Parameters 62
4.5.3 Results and Discussion 64
4.6 Schemes' shortcomings 77
4.7 Summary 79
CHAPTER 5 : PSEUDONYM CHANGING SCHEME 80
5.1 Overview 80
5.2 Motivation 82
5.3 The complexity of ECDSA 83
5.4 Proposed Hybrid-based Pseudonym Changing Scheme 86

5.5 Evaluation 89
5.5.1 Comparison 89
5.5.2 Setting up parameters 89
5.5.3 Results and Discussion 89
5.6 Summary 93
CHAPTER 6 : CONCLUSIONS AND FUTURE WORK 95
6.1 Conclusions 95
6.2 Future Works 101

List of Figures

Figure 1.1 VANET Communications 3
Figure 1.2 Linking attacks 5
Figure 2.1 The Future Smart Vehicle 12
Figure 2.2 The VANET system model 13
Figure 3.1 Pseudonym management system 35
Figure 3.2 Kalman filter process 42
Figure 3.3 Gating phase 43
Figure 4.1 Vehicle's traces with noteworthy positions 48
Figure 4.2 OSM road network 58
Figure 4.3 The confusing road section 58
Figure 4.4 Disconnected trips 60
Figure 4.5 SUMO screenshot of the road network's subsection 60
Figure 4.6 Density of vehicles during simulation in three arrival rates 64
Figure 4.7 Average changed pseudonyms per second 66
Figure 4.8 Average traceability percentage 69
Figure 4.9 Traceability in the Adjusted minimum silent period in CAPS (ACAPS) ... 70
Figure 4.10 Average number of sending beacon messages per second 72
Figure 4.11 SBMs in Adjusted minimum silent period in CAPS 73
Figure 4.12 Number of predicted accidents in SRPS 73
Figure 4.13 The average confusion level percentage 76
Figure 4.14 Number of vehicles wasted pseudonyms 77
Figure 5.1 Average changed pseudonyms per second 90
Figure 5.2 Average traceability percentages 91

Figure 5.3 Average number of sending beacon messages per second 92
Figure 5.4 The average confusion level percentage 93
Figure 5.5 Number of vehicles wasted pseudonyms 93
Figure 6.1 Average number of sending beacon messages per second 100
Figure 6.2 Average traceability percentage 100
Figure 6.3 Average changed pseudonyms per second 101

List of Tables

Table 4.1 Notations 50

Table 4.2 Parameters of each Scheme 63

Table 4.3 Number of Vehicles 63

Table 4.4 Average values of the three arrival rates 78

Table 4.5 Comparison between the schemes 78

Table 5.1 Communication overheads [142] 80

Table 5.2 Computation overheads based on 400 MHz [146] 81

Table 5.3 Sent safety message format 81

List of Abbreviations

ACAPS	Amended Context Adaptive Privacy Scheme
BM	Beacon Message
CA	Certificate Authority
CAPS	Context Adaptive Privacy Scheme
CSP	Coordinate Silent Period
DSRC	Dedicated Short-range Communication
ECDSA	Elliptic Curve Digital Signature Algorithm
EDR	Event Data Recorder
FCC	Federal Communication Commission
GBC	Group-based Cryptography
GM	Group Manager
GPA	Global Positioning System
HBPCS	Hybrid-based Pseudonym Changing Scheme
IBC	Identity-based Cryptography
LID	Long-term IDentity
MAC	Message Authentication Code
MANET	Mobile Ad hoc NETwork
MTT	Multi Target Tracker
OBU	On Board Unit
OMNET	Object-oriented Modular NETwork
OSM	Open Street Map
PKC	Public Key Cryptography
PPC	Periodical Pseudonym Changing
PREXT	PRivacy EXTension for Veins
RSP	Random Silent Period
RSU	Road Side Unit
SBM	Sent Beacon Message
SID	Short-term IDentity
SLOW	Speed LOWer
SRPS	Safety-related Privacy Scheme
SUMO	Simulation of Urban MObility
TA	Trusted Authority
TPD	Tamper Proof Device
V2R	Vehicle to Roadside
V2V	Vehicle to Vehicle
VANET	Vehicular Ad hoc NETwork
Veins	VEhicles In Network Simulation
VSC	Vehicle Safety Communication
WAVE	Wireless Access in Vehicular Environment

Chapter 1 : Introduction

1.1 Overview

Population growth has played a crucial role in increasing the number of vehicles, which is expected to reach two billion by 2040 [1]. Thus, the increase in traffic jams is directly related to the increase in the number of road traffic accidents. According to the World Health Organization (WHO), nearly 1.35 million people are killed yearly and more than 20 million suffer from non-fatal injuries due to road traffic accidents [2].

The development of wireless communications and sensing technologies has encouraged car manufacturers and telecommunication industries to equip vehicles with wireless devices, embedded sensors, and processing capabilities. Therefore, vehicles are enabled to collect data about themselves and their surrounding environment and exchange the collected data via a so-called Vehicular Ad-hoc NETwork (VANET). Accordingly, VANET has been attracting the attention of many researchers and vehicle manufacturers mainly for its ability to improve road safety and traffic efficiency [3].

VANET safety-related applications require vehicles to broadcast messages periodically at 1-10 Hz in so-called Beacon Messages (BMs) that can be received by anyone within the communication range to improve the level of awareness between vehicles such as blind-spot warning, cooperative collision warning, and lane change warning [4]. Moreover, these applications are non-tolerant to any delay and require real-time decision making and thus any delay through transmission and processing must be minimized.

A Dedicated Short-range Communication (DSRC), which has been known also as Vehicle Safety Communication (VSC), based on IEEE 802.11p technology has been chosen over other wireless technology, such as Cellular and Satellite, for its easy deployment, low cost, and low latency (i.e., only several milliseconds in most situations) [5, 6]. The first generation of the DSRC system operates at 915 MHz and has a transmission rate of 0.5 Mb/s that was mainly used for electronic toll collection and automatic vehicle identification [6, 7]. The second generation of DSRC was in 1999 when the Federal Communication Commission (FCC) allocated an additional 75 MHz of bandwidth in the 5.9 GHz band due to the request of the Intelligent Transportation Society of America in 1997 for safety communications. Following this, the standardization organizations have been working on the implementation of the 5.9 GHz DSRC as it is open-source which was the main reason for its success upon 915 MHz DSRC. For example, there is the North America standards program which aims to reduce traffic accidents by enabling the vehicle to communicate and exchange up-to-date information on their surrounding environment with nearby entities [6].

There are two main DSRC wireless communications in VANET: Vehicle to Vehicle (V2V) communications and Vehicle to Roadside (V2R) communications. A vehicle can exchange messages with its neighbouring vehicles through V2V communications (either directly “one-hop” or through intermediary vehicles “multi-hop”) or with Road Side Units (RSUs) located near arterial road intersections or highway on-ramps through V2R communications. In Figure 1.1, a VANET communication model is illustrated in which the vehicle sends messages to other vehicles within its communication range via V2V or it can communicate with neighbouring RSUs via V2R. RSUs can further communicate with the service provider via Cellular technology but it is out of the scope of this thesis.

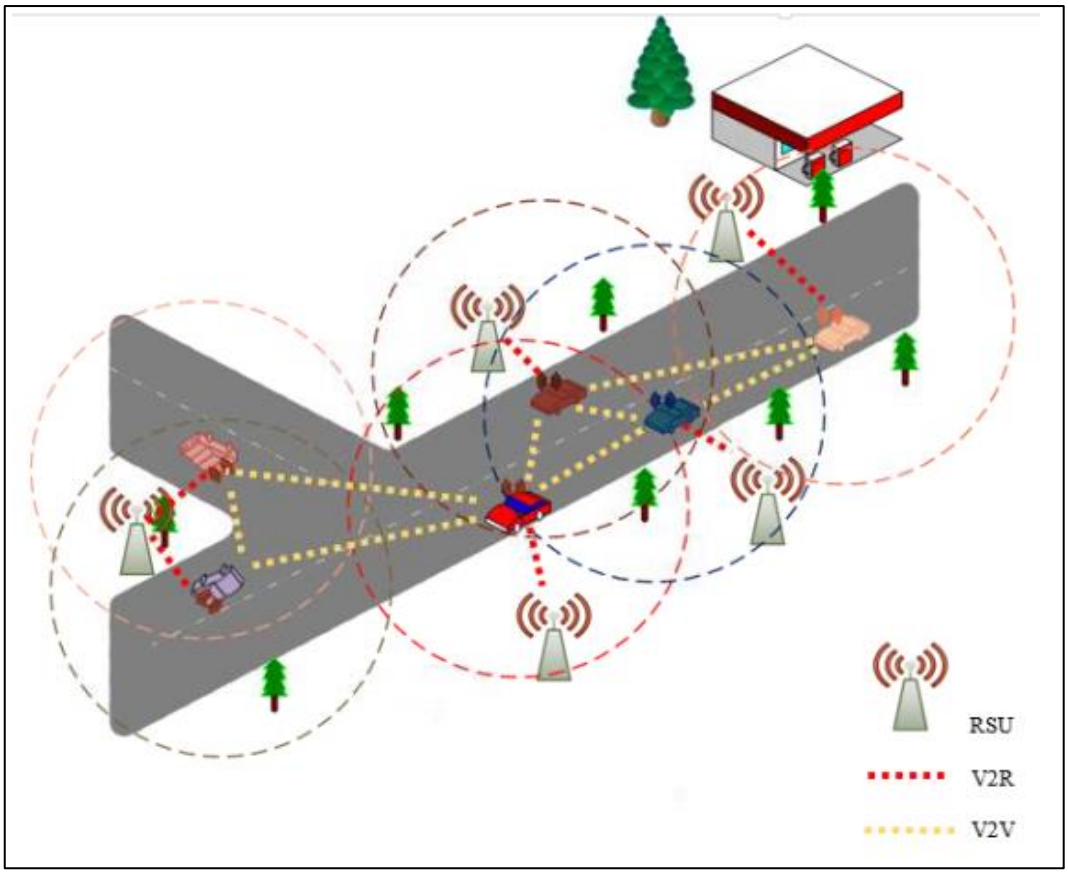

Figure 1.1 VANET Communications

1.2 Motivations

With all the advantages associated with the use of VANET, secure communication [8] of the exchanged data is identified as a paramount requirement as its applications are related directly to people's life (i.e., any dispute may cause disasters, accidents, injuries and loss of life). Moreover, as a BM usually contains a vehicle's location, speed, and heading, as well as being broadcasted in plaintext format [4, 9, 10], it could threaten the privacy of the driver. Some eavesdroppers can collect and analyse the broadcasted BMs to track the individual driver's whereabouts by linking subsequent BMs. Therefore, the location privacy of the driver must be protected well before the deployment of any VANET applications.

Secure communications in VANET could be achieved via authentication which potentially endangers the privacy of the drivers [11]. Messages are exchanged

periodically (1-10Hz) and publicly within its communication range of 300m. Preserving location privacy is a critical issue; that is because eavesdroppers can easily track vehicles and breach the privacy of the driver via detecting whereabouts information included in the broadcasted messages. The use of pseudonyms as short-term public keys, which excluded from the identification information, has been considered as the most reasonable proposed solution for securing the communications and preserving the privacy of vehicles/drivers [12] so that it is adopted by many researchers and standardization efforts. In order to achieve the accountability of the dispute vehicle such as a vehicle sent the false alert, these pseudonyms must be issued by a Trusted Authority (TA) who stores a map linked between each real identity and its pseudonym to be able to resolve it later [13].

Current standardization follows mainly the traditional Public Key cryptography (PKC) to manage these pseudonyms in which the TA issues a digital certificate for each pseudonym. Then, vehicles send this certificate along with the exchanged messages and receivers would only accept and interact upon messages with valid certificates.

However, with the amount of information that a vehicle broadcasts and exchanges, it will still be vulnerable to linkable attack, even if it is not using its real identity, from its spatio-temporal information. Accordingly, each vehicle is provided with a pool of pseudonyms where each pseudonym is used over a period of time. However, privacy is still an issue even after changing the pseudonym of the vehicle because it could still be vulnerable to syntactic attack (i.e., it is the only vehicle to have changed its pseudonym) or to semantic attack (i.e., its route is different from other neighbours' routes), as illustrated in Figure 1.2 [14]. Therefore, pseudonyms should only be changed in unobserved situations by allowing vehicles to change their pseudonyms in a mix-zone area [15] or after being silent for a period [16].

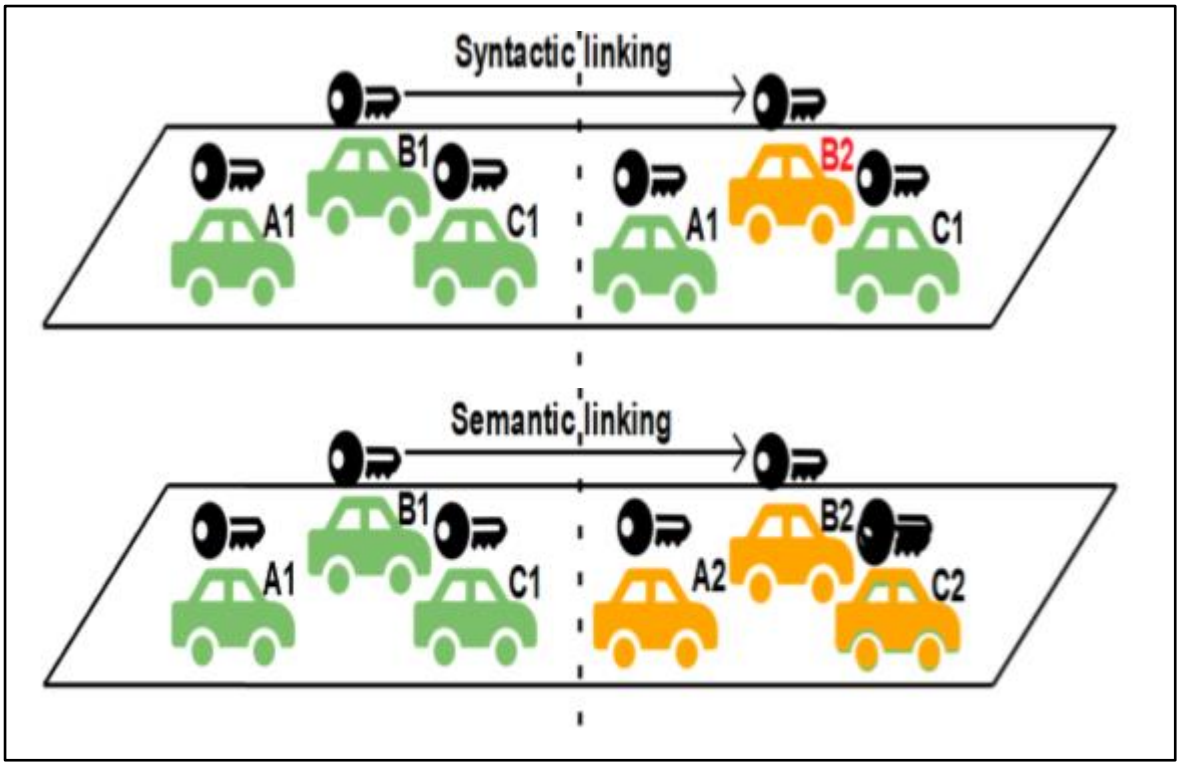

Figure 1.2 Linking attacks

In mix-zone based strategies, vehicles change their pseudonyms inside predefined road areas such as road intersections [15, 17-19], social spots [20-22]. Infrastructure is required to be installed to inform vehicles of the boundary (enter and exit points) of the mix-zone area and thus all vehicles inside this area will stop sharing messages and change their pseudonyms. Then, when the vehicle exits this area, it will start sharing messages again but using the new pseudonyms. On the other hand, in silent-period based strategy, the is no need for infrastructures because the vehicle decides locally when to stop and start sharing messages either depending on time [16, 23] and/or on context (i.e., state of the vehicle itself or its neighbours) [24-28].

Most researchers and standardization efforts nominated silent period over mix-zone because there is no need for infrastructure and thus it is more likely to facilitate the deployment of VANET applications in the near future. Moreover, the semantic attack is difficult to prevent in mix-zone based strategies because the vehicle could still be

trackable. In silent period based strategies, the vehicle should synchronize this period with its neighbours and only start sharing its state if the attacker is probably to be confused (i.e., its state is probably to be mixed with its neighbour (s)) [24-28].

Moreover, changing pseudonym more frequently and having longer silent periods are intended to enhance privacy but have a negative impact on safety applications for the following reasons:

- Increase security overheads and thus more messages could be lost via increasing communication and computation overheads.
- An accident could have happened during silent periods as a vehicle stops sharing its positions.

In the last decade, a wide range of pseudonym changing schemes have emerged to achieve an adequate balance between security and privacy but only a few of them consider the impact on safety applications (i.e., an accident could be unrecognizable due to being silent or lost critical messages via security overheads). Yet, it is still a scientific challenge to design a pseudonym scheme that effectively addresses the three key issues: security, privacy, and safety.

1.3 Research Aims and Objectives

The main aim of this thesis is to efficiently secure VANET communications and preserve the privacy of vehicles/drivers without compromising the other requirements of safety applications. In order to achieve this aim, the following objectives are formulated:

1. Specify the main requirements of VANET safety applications that derived from VANET characteristics, safety functionality needs, and users' demands.

2. Investigate the well-known schemes from the literature and specify the main key points that challenge the existing schemes to be applied to the VANET safety applications.
3. Design and implement a scheme that can minimize the impact of privacy on safety applications.
4. Design and implement a scheme that can address the scalability (i.e., when the number of vehicles increases in urban areas) via reducing the security overheads.
5. Evaluate the effectiveness of the new schemes via comparing them with the existing state-of-the-art schemes in terms of achieving an adequate balance between the three key issues: privacy, security, and safety.

According to the above-mentioned objectives, this thesis tries to answer the following research questions:

1. What are VANET safety applications and what are their most important requirements?
2. How can security overheads and preserving privacy impact on safety applications? And how this impact can be measured?
3. What is the existing designed security and privacy schemes in VANET and which are the most appropriate schemes that can be integrated into its safety applications?
4. How can we measure security overheads and privacy levels? What are the most suitable metrics? Why?
5. How can we measure the impact of the schemes on safety applications? What are the best metrics?

6. Depending on the selected metrics, how effective are the existing schemes in achieving the adequate balance between security overheads, privacy-preserving, and the operation of safety applications compared with the proposed schemes?

1.4 Contributions

The main contributions of this thesis are as follows:

1. Propose a novel Safety-related Privacy scheme (SRPS) that not only preserves the privacy but also enhances the efficiency of safety in VANET applications.
2. Propose a Hybrid-based Pseudonym Changing Scheme (HBPCS) which restricts changing pseudonyms to time-driven and distance-driven to decrease the security overheads due to traffic jams.
3. Reduce the impact of privacy scheme on safety by integrating a Multi-Target Tracker (MTT) algorithm [21] to the proposed scheme.
4. Use a combination of four different tools to simulate the proposed scheme efficiently. These tools are OSM [2] to download a real map, OMNeT++ [3] to build wireless network communication, SUMO [4] to build road traffic, Veins [29] to simulate vehicular network, and PREXT [5] to implement the privacy scheme.
5. The real map is selected upon specific criteria to successfully demonstrate the effectiveness of any schemes in a short time.
6. Evaluate and compare the security overheads, privacy level, and safety level of the proposed schemes with other related works.
7. Propose new metrics to facilitate the comparisons in addition to other selected metrics from the previous studies.

1.5 Thesis Structure

Chapter 2 is dedicated to understand the background of VANET in which its architecture, applications, and the requirements of its main applications i.e. safety applications, and the main attacks are explained first. Then, followed by the security and privacy requirements that contributed to demonstrate the problem definitions. At the end of Chapter 2, the supportive characteristics that can facilitate the disseminating of its applications and facilitate achieving its requirements are explained.

Chapter 3 discusses the existing research efforts to achieve security and/or privacy in VANET and how the existing works challenge the achievement of the other requirements of VANET safety applications (i.e. communication and computation overheads). Moreover, because certified pseudonyms have been widely accepted as a nominated method to achieve both security and privacy, we illustrates the managements of these pseudonyms and reviewed the existing pseudonym changing schemes and their impact on safety. The security overheads of the existing schemes can be compared in regards to the computation and communication overheads in addition to the frequent pseudonym changes while the privacy level is compared using different metrics that are illustrated in Chapter 3. At the end of this chapter the vehicle tracker is illustrated for its importance to design the new proposed schemes.

Chapter 4 and Chapter 5 present the new designed schemes along with their motivation, implementation, and evolution. The first one aims to reduce the impact of privacy-preserving on safety. Then, because we noticed the security overheads during the traffic jams increased in the first designed scheme, the second scheme is designed to overcome this issue.

Finally, **Chapter 6** lists the conclusions and outlines some directions for future work.

Chapter 2 : Vehicular Ad Hoc Networks Background

2.1 Overview

Drivers are responsible for most hazardous road accidents [30] that could account for 50% of global deaths and injuries [2]. These accidents are usually because of the inability of the drivers to monitor the surrounding vehicles and decide quickly the correct driving manoeuvres. Vehicular Ad Hoc NETwork (VANET), which is a subset of Mobile Ad hoc NETwork (MANET), has mainly been developed to improve road safety and reduce the number of accidents via enabling real-time wireless communications between its entities that are mainly the mobile vehicles in the road or roadside infrastructure alongside the road. In VANET, vehicles are required to sense and broadcast messages - which include traffic relevant information such as position, speed, and heading, in addition to traffic situations - to their neighbour vehicles. Thus, each vehicle can monitor the behaviour of itself and its neighbouring vehicles. Then, a vehicle might automatically react or alert the driver if detecting a proximate danger helping the driver to react faster, thus accidents can be prevented in advance. Another scenario is that when there are accidents or traffic jams, vehicles can be warned even before they see the situations so that they can slow-down or change route.

To facilitate the successful deployment of VANET, different technologies are integrated into vehicles such as communication, computation, storage, and sensor devices, which would facilitate designing a wide range of applications. VANET applications are mainly divided into three main categories: safety, traffic efficiency, and infotainment applications. Each category has different requirements and characteristics such as communication range, data rates, security level, and latency. Yet, the most important applications in VANET and the primary focus of researchers

are those related to safety, which raise the most challenging issues. Thus, this chapter is dedicated to discussing first the VANET architecture and then illustrate a number of safety applications, their requirements, and the main challenges.

2.2 VANET Architecture

In VANET, vehicles are equipped with different kinds of sensors, application units, electronic systems, etc. to sense and collect information about themselves and their surrounding environment. Figure 2.1 shows an example of the future smart vehicle [31] that can be equipped with devices to enable VANET applications. Some of the installed devices are illustrated below:

- On-Board Units (OBUs) that can store, process, and communicate with other VANET entities [10].
- A Global Positioning System (GPS) receiver for detecting the position of vehicles and navigation services. Moreover, the timestamps obtained from GPS could be added to the message to prevent a replay attack.
- A Tamper Proof Device (TPD) to store sensitive data such as cryptographic material; it also has the capability to process the cryptographic operations such as hashing, signature generation/verification, etc. [32].
- An Event Data Recorder (EDR) to store the information related to emergency events (such as the position, speed, time, etc.) similar to the black box in airplanes [32].
- Forward and rear sensors to alert the driver of obstacles typically for parking.
- A speed sensor to collect information on how fast the vehicle is travelling.
- An ice sensor for warning of a slippery road, which could help other vehicles to change their routes.

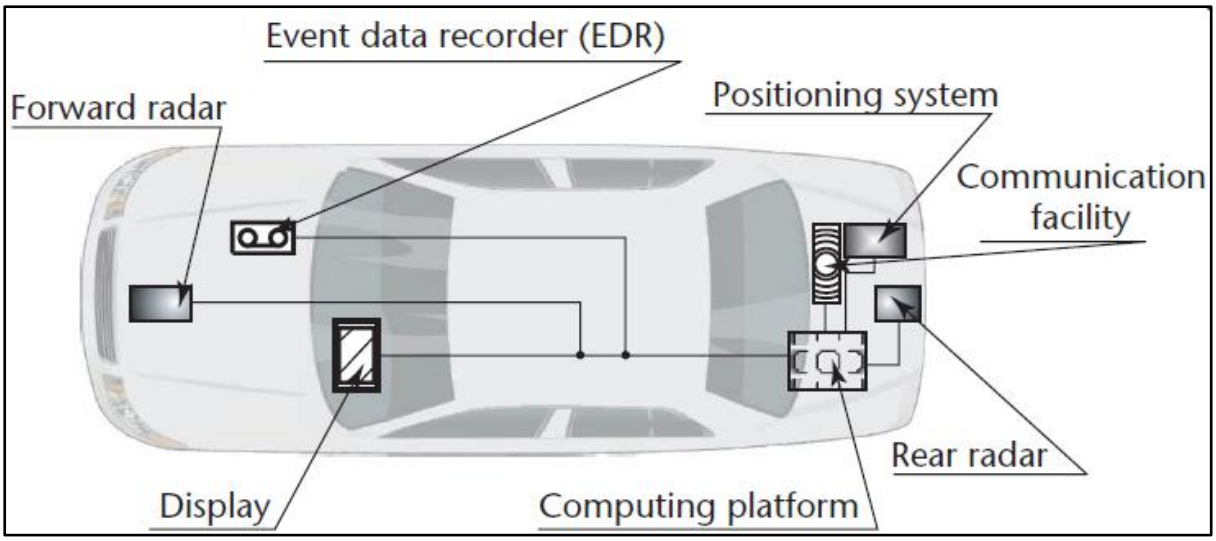

Figure 2.1 The Future Smart Vehicle

The collected information could be used by a vehicle itself (e.g., to warn the driver of the current speed) and/or broadcasted to other VANET entities to make an informed decision (e.g., divert the traffic in case of a traffic jam ahead in the current route).

The VANET is not a pure ad hoc network but it also needs to integrate other entities, to facilitate its requirements and improve its functionality, such as the following:

- Trusted authorities that are responsible for registration of vehicles, providing secure communications, and resolving any disputes.
- Physical devices called Road Side Units (RSUs) that are located at fixed positions along the roadside or highway and have communication, storage, and computation devices similar to OBUs in vehicles, but they should be more powerful. The RSUs are responsible for routing messages to extend the communication range, providing internet connectivity to the vehicles on the roads, serving as a proxy between vehicles and trusted authorities, etc.

The communication between RSUs, or between RSUs and authorities are usually via wired communication. On the other hand, OBUs (or vehicles) communicate with other OBUs and RSUs wirelessly through Vehicle-to-Vehicle (V2V) and Vehicle-to-

Roadside (V2R) communications, respectively. Figure 2.2 illustrates the VANET system model [33].

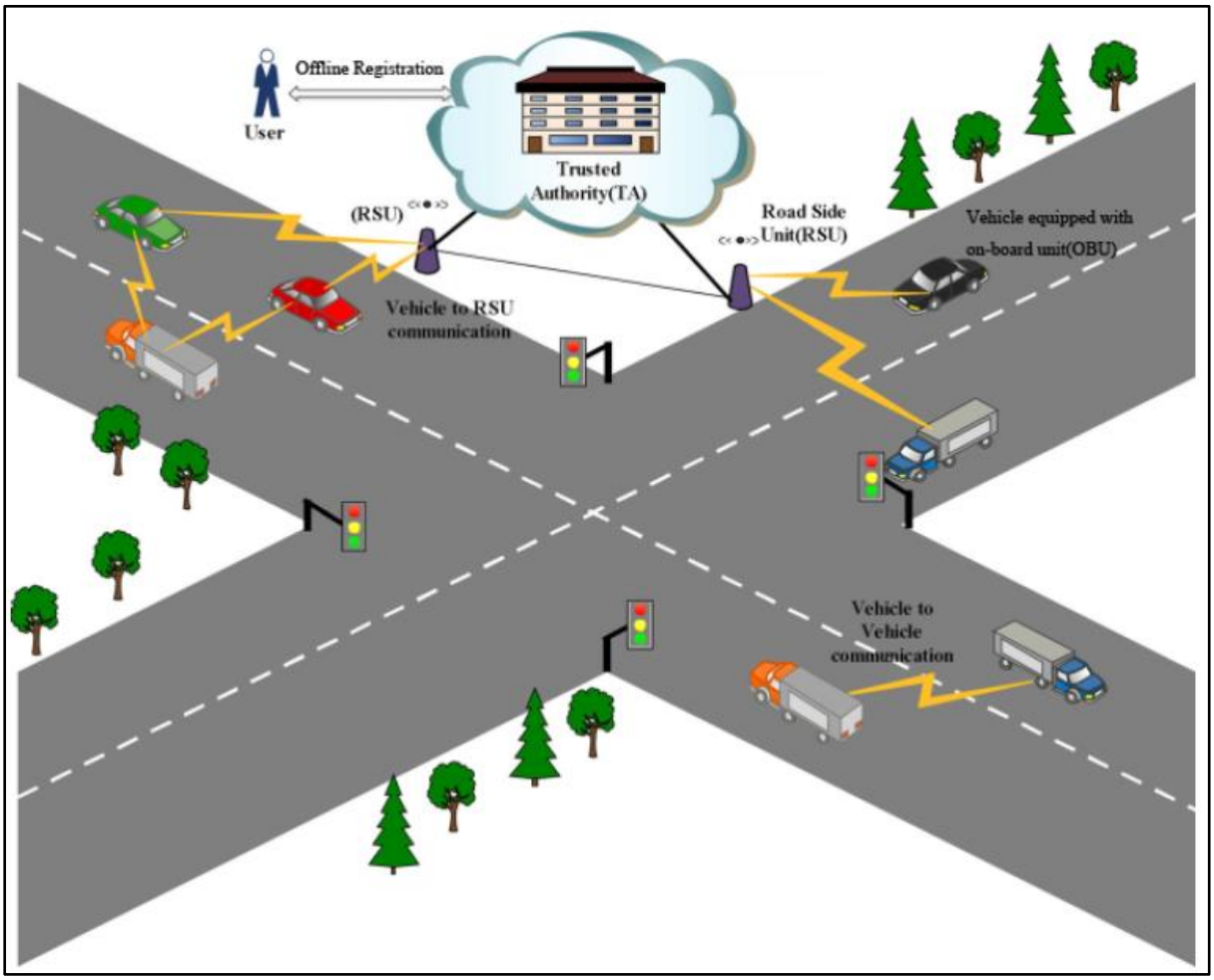

Figure 2.2 The VANET system model

2.3 VANET Safety Applications

In this section, a number of the most popular under investigation safety applications, which aim to reduce the probability of traffic accidents due to human error or obstacles, are explained briefly below [9, 10, 34-37].

- Lane change assistance [36]: this application monitors the surrounding vehicles and calculates the distances between the vehicle and its neighbours. Then, it warns the driver if the lane change could cause an accident or vehicles could

become too close to each other. This would potentially reduce crashes during lane change in blind spot areas.

- Forward collision warnings [36, 37]: this application warns the driver of an expected rear-end collision with a heading vehicle driving in the same lane and direction, due to, for example, slowdowns or the road curvature.
- Head-on collision warnings [38]: this application provides early warnings that are sent to vehicles that are travelling in opposite directions.
- Intersection collision warnings [37]: this application warns the driver when approaching road intersections if there is a high collision probability with other vehicles.
- Cooperative collision warnings: in this application, a stopped or slowed-down vehicle due to the curve or downhill would inform the following vehicles of the upcoming road environment and thus others can react in time.
- Post-crash notification: in this application, a vehicle that involved in the accident would send warning messages to nearby vehicles so that they can apply the brakes quickly, or to distant vehicles so that they can change their directions/routes.

2.4 VANET Safety Applications Requirements

The requirements of safety applications could be derived from the functionality need, the characteristics of VANET, or the need for obtaining public acceptance and facilitating the dissemination of these applications.

In the following, the essential requirements, which facilitate safety functionality to work properly, are illustrated:

- Safety messages usually contain the current states of vehicles (position, speed, and heading) as well as traffic-related information (accidents, traffic jams, icy roads, etc.).
- Safety messages are broadcasted periodically with high frequency (1-10 Hz) in so-called beacons or they are generated when detecting safety events in so-called event-driven messages.
- The vehicle could broadcast messages directly to its neighboring vehicles within its communication range (such as within 300m) in single-hop communications. However, in some cases, multi-hop communications are required when there is a need to broadcast messages to other vehicles beyond the communication range.
- Secure Communications of the related-safety applications is highly important to be implemented well. Malicious messages sent out by attackers could cause a severe damage or a fatal consequence [39].
- Short-term linkability is important for most of the safety applications in which the receiver should be able to recognize that messages over a short period issued by the same sender. Otherwise, it becomes harder and error prone to indicate an accident risk based on unlinkable messages [40]. For example, in lane change warning alert application, the receiver builds a map of nearby vehicles upon receiving the subsequent beacons and then decides if changing lane is safe or not [41].

The special characteristics of VANET, which are the high mobility, rapidly changing topology, and a large number of vehicles, would introduce some special requirements, as illustrated below:

- Real-time Constraints: Vehicles can travel up to 112 km/h, which means connectivity between them is very short. This emphasizes the need for real-time

decision-making (i.e., most safety applications require strict deadlines 100ms - 1000ms) and thus any communication and computation overheads should be minimized [6].

- Overheads: The number of vehicles can be increased to a very large scale especially in large cities which requires reducing both communication and computation overheads of any embedded schemes such as security schemes.
- Distributed and Non-Cooperative Scheme: Scalability would challenge any centralized scheme and the speed of vehicles would challenge any cooperation between them i.e. communication between vehicles would last for a short period.

Finally, there are two other requirements that are highly important to meet the public acceptance and successful deployment of any VANET applications [32], which are illustrated below.

- Cost Constraints: the embedded devices in vehicles, communication media, storage media, infrastructure dependency should be kept at low cost to facilitate the deployment of such networks [6, 42].
- Privacy-preserving of the driver/vehicle: the amount of broadcasted location information could enable an adversary to track a location of vehicle and breach the privacy of the driver as there is a strong correlation between a vehicle and its driver i.e. most vehicles are driven by their owner only [43].

Despite the above-mentioned requirements, security and privacy [8] of the exchanged messages are identified as the main concerns of any application especially if the applications are related directly to people's life (i.e. any dispute could cause disasters, accidents, injuries, or loss of life). Thus, we will elaborate further at the end of this chapter the main requirements of security and privacy in VANET safety applications and what are the main challenges and the supportive characteristics.

2.5 Attacks on VANET

VANET exchange messages wirelessly and publicly which makes this networks to be vulnerable to different types of attacks. Thus, in this section, we will describe first the attackers' models in VANET followed by the most well-known classification of its basic attacks.

2.5.1 Attacker Models

Raya and Hubaux [44] divided the attackers into four main categories:

- Insider vs. Outsider: an insider attacker is an authenticated VANET entity who is legitimate to communicate with other entities (i.e., an authenticated entity has a pool of the certified public keys as it will be explained later). An outsider attacker is an intruder who is not allowed to exchange information with another VANET entity (i.e., not certified to use its services/applications) and does not have direct access to the system. Thus, the outsider attack is less harmful than the insider, as the latter can cause more damage to the system by tampering with OBU or sending false information.
- Malicious vs. Rational: a malicious attacker's main aim is to harm other VANET entities or to damage the functionality of VANET applications while a rational attacker's main aim is to seek for personal benefit.
- Active vs. Passive: An active attacker can generate and broadcast false messages or does not forward the received messages whereas a passive attacker would only breach the wireless channel and collect the exchanged messages.
- Local vs Global: a local attacker has a limited scope on roads such as controlling several vehicles or installing receivers over several sections of road networks. A Global attacker has potential to have control over the whole road network.

2.5.2 Basic Attacks

In this section, the main attacks against the exchanged messages are illustrated as follows:

- Sybil attack [45]: a malicious vehicle could forge identities and pretend to be another vehicle such as fabricating a traffic jam or masquerading a police car.
- Denial of service attack [6]: this attack is aimed to consume the VANET resources by flooding the networks with dummy messages. This could result in an accident in which an important message will not be arrived or processed.
- Bogus information [45]: a malicious vehicle could send wrong information such as a closed road or an accident, which could affect the behaviour of other vehicles such as changing routes, stopping or slowing down, etc.
- Replay attack [6]: a malicious or unauthorized vehicle could replay a legitimate message at a later time and different place. For example, if an ambulance sends a message to evacuate the road or a vehicle sends a warning of an accident, the selfish driver could replay sending these messages later to prevent other vehicles from being in its route.
- Eavesdropping attack [46]: in this attack, the eavesdropper aims to collect the exchanged messages over a long-period and link between them to find the trajectory of the driver.

2.6 Security Requirements in VANET

In this section, the basic VANET security requirements are summarized based on Raya and Hubaux [47] in which they outlined the security requirements of wireless communications. Thus, it would be compatible to provide secure communications in VANET, as illustrated below.

- Authentication: entities have to be authenticated first to be able to exchange messages in VANET. A receiver reaction should be only upon messages generated by a legitimated entity. This is a major security requirement because it ensures that the received message is sent by an actual node and not by a malicious node who impersonates another identity or represents multiple identities. For example, a selfish driver would represent multiple vehicles to free his route.
- Message integrity: receivers must ensure that the message, which sent by a legitimate entity, has not been altered during transmission.
- Accountability and non-repudiation: the misbehaving entity must be accountable for its activities, such as sending a false alarm message, and unable to deny sending that message.
- Revocation: the misbehaving/compromised entity must be excluded from the network through revocation of its credentials.
- Freshness: the received messages should be generated recently and have expiration time to prevent replaying of the authenticated message later. For example, a vehicle should not be able to resend the received messages from the ambulance after a while to free the road.
- Confidentiality: VANET safety applications may differ from other wireless applications in which messages are usually sent in a plain format while others may require rendering confidentiality of the exchanged data. However, confidentiality can still be utilized when certain messages require to be exchanged privately between certain nodes such as between the road authority and a vehicle to issue the speed ticket or to inform certain vehicles of the suspected criminal locations [12].

2.7 Privacy Requirements in VANET

In VANET, it is essential to protect the privacy of the driver/vehicle, rather than RSUs and public vehicles, such as ambulances. However, road users are encouraged to share as much information as possible in order to enhance the accuracy and timeliness of road-safety applications. The privacy of drivers/users could be threatened in VANET through the huge amount of shared data. Attackers actually could identify and extract useful information, such as the whereabouts of a particular user, simply based on the message he/she periodically broadcasts. This might put the user off if their privacy cannot be protected. Thus, preserving privacy is highly important to obtain public acceptance of VANET applications. In [11], Schaub et al. discussed the privacy requirements in detail. However, we will only discuss the main privacy requirements of real-time communication in safety applications as follows:

- Conditional anonymity: The sender of the messages should not be identifiable by other VANET entities in innocent situations. However, in case of dispute, the authority should be able to identify the real identity of the sender for accountability purpose.
- Unlinkability: To prevent location tracking, messages generated by the same sender should be unlikable for a long-time. Thus, an eavesdropper cannot identify the points of interest such as home or a work address that identify the driver's whereabouts information.
- Minimum disclosure: The driver should disclose only the required information for the functionality of safety applications such as its position. However, the identity of the driver should be kept secret, as it is not required by these applications.
- Distributed resolution authorities: it is preferable that identity resolution can only be achieved by the cooperation of several authorities.

- Perfect forward privacy: the resolution of a specific event to its identity should not reveal further information that decreases the unlinkability of more events.

2.8 Problem definition

The special behaviour and characteristics of VANET leads to particular challenges, which impact the future deployments of its applications, as discussed below.

- Security vs. privacy: to provide secure communication, it is necessary to authenticate all exchanged messages. However, this leads to identifying and tracking vehicles from these messages [48] and breach the privacy of the driver.
- Quality of services vs. privacy: to enhance the quality of safety applications, vehicle are required to share its location continuously that would breach the privacy and challenge any privacy-preserving scheme.
- Real-time constraints vs. overheads: in safety-related applications, the broadcasted messages are time-critical and have expiration time of 100-1000 ms [10]. Thus, it is necessary to minimizing the processing and communication overheads of the security scheme. Moreover, the cooperative authentication protocols [49-51] and RSU-aided authentication protocols [52-54] are not feasible due to the speed of vehicles, especially on highways [55].

Researchers and standardizations have reached a consensus to use certified pseudonyms to balance between security and privacy requirements. They suggested that a vehicle is required to change its pseudonym after being silent for a period to prevent long-term linkability. Moreover, they assumed that changing pseudonyms more frequently and having longer silent period would enhance the privacy level.

However, this would increase the security overheads and have an impact on safety applications such as the probability of accidents could be increased. Although most

researchers are working to enhance the balance between the security overheads and the privacy level but only few of them consider the impact on safety applications. Accordingly, in this thesis, the state-of-the-art security and privacy schemes in VANET will be investigated thoroughly in related to their impact on other requirements of VANET safety applications. Then, design a scheme that can be integrated to these applications. The designed scheme would be adhere to the requirements of security and privacy in sections 2.6 and 2.7 as well as reduce the impact on safety. The impact on safety would be achieved as follows:

- Increase the number of exchanged messages as 10 Hz is recommended and reduce the impact of silent period on safety.
- Reduce the security overheads both the communication and computation overheads.
- Depend on technology that does not require the vehicle to communicate with any other entities in real-time i.e. vehicle can locally verify the authenticity of the other vehicles and the integrity of the received messages without the need for a third party.

2.9 VANET supportive characteristics

VANET special characteristics such as high mobility and scalable network have introduced unique requirements and challenges in comparison to other ad hoc networks, as discussed above. However, VANET has other supportive characteristics [56-58] that could be promising for its success, as discussed below.

- High energy supply and sufficient processing power: a major aspect in VANET is that its nodes are vehicles that have their own power supply in the form of batteries.

Moreover, the computation resource is sufficient to allow for vehicles performing complex calculations.

- Constrained mobility and prediction: the mobility of vehicles is usually constrained by the pattern of roads and streets, speed limit, traffic lights, traffic conditions, etc. Therefore, the future position of vehicle is feasible to be predicted given the current mobility state.
- Law enforcement infrastructure: there is an agency that is responsible for monitoring and tracking back the disputed vehicle and thus the driver would be accountable for their behaviour. This would encourage most participants of VANET to become honest.
- Known position and time: as a vehicle would be equipped with a GPS receiver, the position of vehicles with time would be available, which could facilitate designing security and privacy schemes.
- Limited physical access: access to a vehicle is usually limited to driver or authorized person and thus it is difficult to physically compromise the vehicle.

2.10 Summary

In this chapter, first, the design of vehicles that can participate in VANET applications is demonstrated followed by the main entities and communications that can be integrated to form the VANET system. Then, a number of VANET applications, specifically those related to safety, are explained followed by their requirements, which mainly derived from three perspectives: functionality of safety, characteristics of VANET, and compliance with public need. Moreover, the well-known attacks in VANET are presented to understand how to achieve the most important VANET safety requirements (security and privacy). Finally, VANET characteristics that could facilitate designing a scheme are detailed.

Despite the advantages that can be achieved from sharing information between vehicles, any dispute could put people's lives in danger. Thus, secure comminution of the exchanged messages is important to prevent broadcasting false messages. Moreover, in VANET safety applications, a vehicle is required to send its exact locations and at a high rate (10 Hz) in plain text so that attacker can link these messages and identify the whereabouts of the driver. Long-term linkability between these messages would reveal the identity of the driver that must be well protected to meet public acceptance of such applications. Next, a survey on the different research directions for providing security and/or privacy is explained and what are the main consequences on the functionality of safety are illustrated.

Chapter 3 : Literature Review of Security and Privacy-Preserving Schemes for VANET Applications

3.1 Overview

In the past decade, researchers have proposed numerous schemes to secure VANET communications and protect the privacy of the driver. However, it is still a challenge to meet other requirements of VANET safety applications as well as to find an effective balance between security and privacy, as we will explain in this chapter.

To achieve security in VANET, authentication of a vehicle is important which would endanger the privacy of a driver. Pseudonym schemes have emerged to provide an acceptable balance between security and privacy. Pseudonym schemes are mainly implemented using traditional cryptography mechanisms. In the last decade, a large body of literature has been dedicated to facilitate the design of the pseudonym schemes, which can efficiently address VANET requirements such as how to generate these pseudonyms, who is responsible for traceability, what are the overheads of the underlying cryptography, when and where pseudonyms should be changed, etc.

The underlying cryptography mechanism schemes, which can facilitate secure communication, will be discussed first followed by the well-suited mechanism for VANET safety applications and its main issues (overheads). Then, the management of these pseudonyms from issuing to revocation process will be demonstrated in details. As the frequency of pseudonym change challenge the achievement of the requirements and impact on the efficiency of safety applications, the state-of-the-art pseudonym changing schemes are discussed.

Accordingly, how these schemes can achieve both security and privacy without compromising safety is critically analysed (i.e. how these schemes can balance between the requirements of safety applications). Security overheads should be minimized to meet real-time decision making in VANET safety applications and thus it should be considered when designing a pseudonym changing scheme. Moreover, in the literature, different metrics have been designed to quantify privacy as illustrated in section (3.7).

Finally, a prediction of the vehicle's next position is an important feature, not only to measure the achieved privacy level, but also to effectively changing pseudonym. Accordingly, the main required phases to track the vehicle through predicting its next position is illustrated in section (3.8) i.e., vehicle tracker.

3.2 Categories of Cryptographic Mechanism Schemes

Security and privacy in VANET are mainly achieved by using pseudonyms coupled with traditional cryptographic techniques: public-key cryptography, identity-based cryptography, group-based signature cryptography, and symmetric cryptography. Accordingly, the cryptographic keys are stripped from any identifying information and used as pseudonyms [59].

These pseudonyms must be issued and certified by a Trusted Authority (TA), which stores the links between the real identity and pseudonyms to ensure traceability of misbehaving vehicles. To enhance privacy against authority, resolution of the real identity should only be fulfilled through multi-authorities. For example, the US Department of Transportation [60] proposed role separation of duties between authorities (issuing, linking, and revocation authorities) while other researchers employed cryptographic primitives (blind signature and secret sharing) between multi-

authorities [61]. Accordingly, they enforce that linking pseudonym to its real-identity is only achievable upon the agreement of all authorities.

In VANET safety applications, the delay in issuing, resolution, and revocation of these pseudonyms is not an issue and can be done via a wired network. However, the main concerns are the authentication of vehicles and the integrity of messages in which they are time-critical and must be accomplished locally inside vehicles. Thus, we will elaborate more on how to verify both vehicles and messages in each cryptographic scheme and then surmise the most suitable one for VANET safety applications.

3.2.1 Public Key Cryptography

Public key cryptography (PKC) is asymmetric cryptography in which each vehicle requires a pair of keys (public and private) to authenticate the message. One key is used to sign the sent message, which is the private key, while the other key is used to verify the received message, which is the public key. To ensure privacy, the public key must be excluded from any identification details and used as a pseudonym. A Certificate Authority (CA) is required to issue a certificate for each pseudonym to ensure the legitimacy of the vehicle.

A static pseudonym is insufficient to protect the privacy of the driver because an adversary is still able to track a vehicle for a long-time via its spatio-temporal information included in safety messages and identify its trajectory. Moreover, the vehicle is usually driven by one person, its trajectory will reveal the owner's home and/or work address, and even his activities [62]. Raya and Hubax [44] suggested that each vehicle is equipped with a set of certified pseudonyms, which must be securely stored inside vehicle (i.e., TPD). Each pseudonym has a validity period, which can be

ensured by the signed certificate, and messages are signed using the private key of the current valid pseudonym.

Distributed authentication is important to enable real-time decision making which could be hindered in the case of a centralized entity being needed. Thus, the required information to verify the authenticity of the vehicle and the integrity of messages should be available locally i.e. messages should be signed and sent along with the signature and the certificate for the current valid pseudonym.

Each certificate usually contains the public key of the CA, the pseudonym, its validity period, which is digitally signed by the CA using its private key, and the signature of the CA [63]. The size of the certificate depends on the security strength as illustrated later in Chapter 5.

3.2.2 Identity-based Cryptography

Certificates would result in storage and communication overheads that can be addressed by using Identity-based Cryptography (IBC). The IBC, which was first proposed by Shamir (1984) [64], is asymmetric cryptography in which the public key is derived from the identity of the node, such as, their name, email address, telephone number, etc. [65]. The key generation centre (KGC), which is assumed to be trusted and owns a master private key, is responsible for generating the private keys for all vehicles. Thus, a vehicle's legitimacy is implicitly certified and communication and storage overheads are considerably reduced over the PKC (i.e., there is no need to exchange or store the certificates) [66]. Moreover, in VANET, to achieve pseudonymity, these public keys should be extracted from arbitrary strings and used as pseudonyms.

However, IBC is similar to PKC, because they both require periodically changing pseudonyms to protect the individuals' privacy.

3.2.3 Group-based Cryptography

In [16], authors applied the Group-based Cryptography (GBC) concept, which was first introduced by Chaun and Van Heyst in 1991 [67]. In GBS, a group manager (GM), which is assumed to be trusted, is responsible for issuing a shared public key for each group to be used as a pseudonym to verify the exchanged messages, while each group member has it is own private key to generate the signature. The GM, using its secret key, is the only member who is able to trace a signature to the individual signer.

In GBC, preserving individuals' privacy is achieved without the need to change pseudonyms as the sender cannot be recognized from other group members (two messages signed by the same vehicles cannot be linked). This leads to eliminating the need for issuing and storing thousands of pseudonyms in PKC and IBC [68].

3.2.4 Symmetric Cryptography

In symmetric schemes, a single key, which is also called a secret key, is used to sign and verify the exchanged messages differ from the previous cryptography schemes (i.e., asymmetric cryptography). A sender hashes the messages and the secret key to generate a Message Authentication Code (MAC) and then send this MAC along with the message. A receiver must know the secret key to verify the MAC by using the same operation on the received message.

The main advantage of applying symmetric over asymmetric schemes is that they are highly efficient in terms of computation and communication overheads. However, the symmetric key can only be released when it is expired as the knowledge of this key will enable impersonation attacks. Moreover, similar to PKC and IBC, its key needs to

be changed over time to avoid tracking via the spatio-temporal information and thus each key has a validity period. The sender generates the MAC for each broadcasted message using the current valid key and only sends this key when it is expired [69].

3.3 Cryptographic Schemes for VANET Safety Applications

Instead of the diversity of the applied cryptography schemes in VANET, safety applications have strict requirements as illustrated in the previous chapter. Accordingly, the consequences of the cryptographic schemes on safety applications are illustrated below:

- Safety applications are non-tolerant to any delay and have expiration time usually 100-1,000 milliseconds which could present a challenge to apply IBC or GBC. The IBC and GBC are mainly dominated by bilinear pairing operations which are not affordable for a typical OBU with 400 MHz processor [70].
- The computation overheads of the symmetric cryptographic are highly efficient but the delay in releasing the key would hinder real-time decision making [71, 72].
- In GBC, short-term linkability (i.e., messages are unlinkable) is not supported because the receiver can only verify that messages are sent by a group member but not the exact one. Moreover, this would impact safety applications that require the exact number of surrounding vehicles along with their positions.
- IBC and GBC schemes require the dense deployment of RSUs that is not possible in the near future as a result of their cost, and the communication delay would hinder real-time decision making. The need for RSUs could be to manage the group in GBC and/or to verify messages in IBC and GBC (i.e., pairing operations are not affordable to be accomplished by vehicles) [66]. Moreover, instead of the wide use of batch verification (i.e., multiple signatures verified at the same time

simultaneously instead of sequentially) to improve the efficiency of pairing in IBC and GBC [66, 73-82], verification is still not affordable for vehicles.

According to the previous points, current research and standardization efforts mainly utilized PKC to secure communication in VANET. The most time-consuming operation in the PKC is the scalar multiplication which is nearly twenty times lower than the pairing operation [83]. Thus, verification can be done locally inside the vehicle without the need for RSU (i.e., omit V2R communication overheads), which is required in IBC and GBC. Moreover, as the vehicle sends the key certificate along with the message, it allows timely verification of these messages, unlike in symmetric schemes.

PKC can work perfectly in sparse traffic but the issue arises in dense traffic as the number of received messages which need to be verified is increased. Researchers have been working to enhance the communication and computation overheads of PKC to improve its efficiency in dense traffic.

3.4 Communication and Computation Overheads in PKC using ECDSA

In the mid-eighties, ECC was proposed independently by Miller [84] and Koblitz [85]. Since then, it has acquired wide acceptance as an alternative to the conventional cryptosystems, such as Rivest Shamir Aldeman (RSA) [86], Digital Signature Algorithm (DSA) [87] and Diffie Hellman DH [88]. This is due to the highest security capability per bit, faster computation as well as memory and bandwidth utilization [89]. Therefore, IEEE 1609.2 standards address the issues of securing Wireless Access in Vehicular Environment (WAVE)by nominating the Elliptic Curve Digital Signature Algorithm (ECDSA) for the key pairs of the PKC [90].

ECDSA was first introduced in 1992 by Vanstone in response to the NIST request [91]. The key length of the digital signature provides a fundamental trade-off between

processing overheads and the security level. Two variants of ECDSA are defined in the IEEE 1609.2 standard:1) The first variant, which uses a key length of 224 bits, is used for messages that have short validity time, such as safety messages, 2) The second one, which uses a key length of 256, is used for messages that have a long validity period. This is because the 256-bit key requires more communication and computation overheads [10]. The security level of ECDSA depends on the elliptic curve discrete logarithm problem (ECDLP) complexity which is the difficulty to find an integer d for the given two points (G, Q) belonging to the same elliptic curve, where $Q = d * G$ [92]. Thus, the longer key length takes more time to be compromised.

However, ECDSA has difficulties in providing real-time verification when the number of vehicles is increased, and safety-related messages have between 100-1000 ms as the upper bound on delivery and process delay. To rectify this problem, a vast amount of research has been done to enhance its communication and computation overheads efficiency. To reduce the computation overheads of the scalar multiplication, different methods are given in [93],for example, Shamir proposed a method to compute the addition of two scalar multiplications simultaneously to reduce the computation overhead when calculating them individually [94]. Moreover, authors in [95, 96] have proposed a cryptographic acceleration via an integrated hardware security model which is not practical due to VANET cost limitation.

Other researchers have devoted efforts to design an efficient scheme to improve the efficiency of PKC in VANET. In [44], Raya and Hubaux suggested verifying only relevant messages. Similarly, Grover and Lim [71] designed a probabilistic verification scheme based on ECDSA to maximize the number of relevant verifications in which messages from a closer vehicle will be assigned a higher probability. The Batch Verification (BV) scheme is also employed to eliminate some time-consuming

operations via verifying a large number of signatures simultaneously instead of sequentially [77]. However, the efficiency of BV decreases when the number of invalid messages increases. Researchers in [50, 66, 97] have applied a co-operative authentication scheme by allowing neighbouring vehicles to participate in the verification process. In this scheme, each vehicle will verify a small number of messages and share its results with its nearby vehicles. However, this method is difficult to implement because vehicles exhibit a high degree of mobility [6, 48] and also it is a challenge to form trustworthiness among them because of VANET scalability [48].

One of the most promising suggestions was by Raya and Hubaux in [44] to reduce the verification overheads in which as pseudonyms are usually used to sign several messages, there is no need to verify the already verified pseudonym. The other promising suggestion was proposed in [98, 99] to reduce the communication overheads in which they suggested to attach a certificate to a message one time and then attach it again only when a new vehicle enters the communication range. To avoid the issue of discarding messages when a certificate packet is lost, the authors in [100, 101] suggested a periodic omission scheme. Omission schemes motivated other researchers, such as, in [102-104] the authors have studied the omission schemes in more detail and proposed an omission scheme based on channel loads in which there is no need for omitting certificates in sparse traffic i.e. in a free channel.

3.5 Pseudonym Management Schemes

Pfitzmann and Hansen have characterized a pseudonym as a digital unique identifier used instead of the real identity [105]. Moreover, a pseudonym must excluded from any identifiable information to avoid any linkability to the holder's real identity [62]. However, a trusted authority has to be able to link between the pseudonym and real

identity, which allows accountability of the dispute entity [11]. To be a part of VANET, each vehicle needs to register through a trusted authority such as the government organization or a vehicle manufacturer who issue a Long-term IDentity (LID). The LID is coupled with a pair of keys and an attribute of the vehicle such as an electronic licence plate or a chassis number. Moreover, the LID has to be certified by the authority and stored in the TPD inside the vehicle at the time of registration and only changed if the owner of the vehicle changed. The LIDs are used in V2R communications in which vehicles can use them to obtain a pool of pseudonyms, which is a Short-term Identity (SID) to be used in V2V communications. A pseudonym is used to authenticate several messages and then the vehicle should switch to another one to avoid long-term linkability. The pseudonyms pool should be periodically renewed for the reason that all have been used or expired.

The authority should retain the escrow information for each pseudonym [62] to enable resolution of the misbehaving entity in which the authority could issue a fine; and revoke the LID, or the SID depending on the consequences of the dispute. Authority could be a single party but to preserve the privacy of honest drivers from being trackable, multi-parties is recommended [106] and only the cooperation between all parties would enable revealing the misbehaving real-identity. In [13], the authors have suggested the participation of at least three parties which are one to issue LID and retain the map between LID and real-identity, another one to issue SIDs and retain the map between LID and SIDs, and the last one is responsible for resolution and/or revocation of misbehaving vehicle. However, in [13], the vehicle is still trackable by the SIDs issuing authority as they can link different pseudonyms and reveal the whole vehicle trajectory. In [41], a GBC scheme was applied in which the LID’s authority will group a number of vehicles during registration and thus the SID’s authority can verify

authenticity of the vehicle using the group's public key. Fescher et al. [61] suggested applying cryptographic primitives to enforce the need for cooperation between parties for resolution. In their protocol, the blind signature and secret sharing cryptographic were applied.

It is worth mentioning that LID and SID are both supposed to be pseudonyms but to avoid confusion we will only use pseudonym terminology for the SID in this thesis as we are only interested in improving the secure communication between vehicles in safety-related applications. In Figure 3.1, a simple pseudonym management system is depicted.

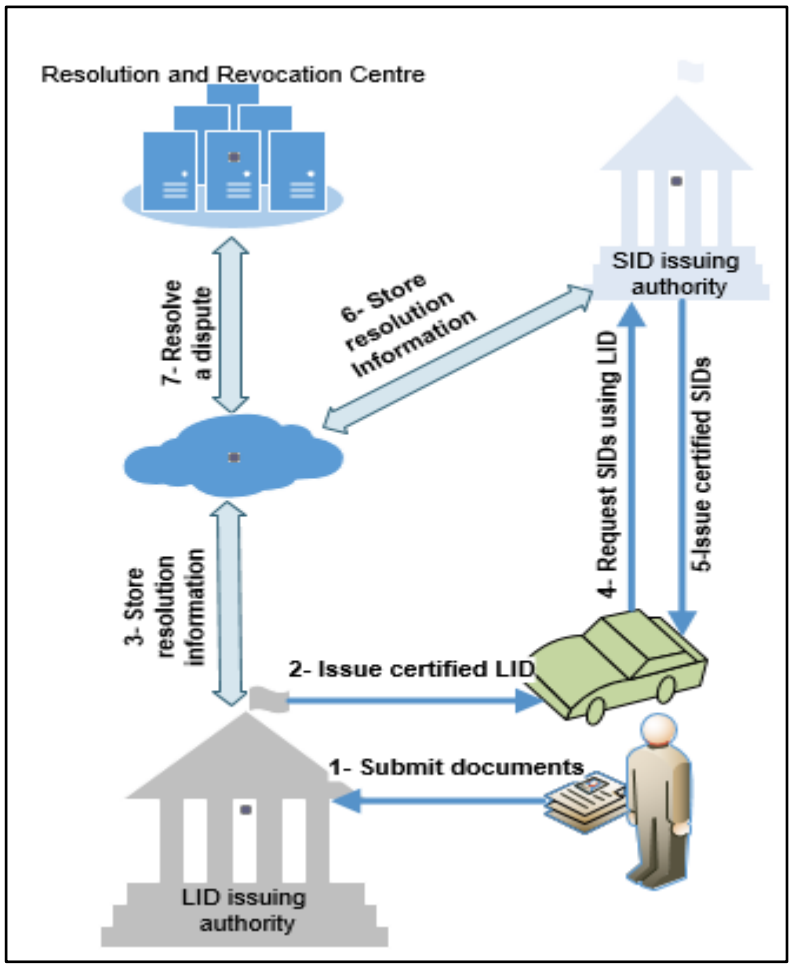

Figure 3.1 Pseudonym management system

3.6 Pseudonym Changing Schemes

The frequency of pseudonym change is directly related to computation, communication, and storage overheads as the TA needs to generate, deliver, and store these pseudonyms. Moreover, storage overhead due to the need for more pseudonyms; communication overheads due to attaching new ones to safety messages; computation overheads as the receiver might already have verified the pseudonym and only need to verify the integrity of messages. Finally, if message routing to other distant vehicles using a position-based routing scheme, it will be dropped if it is routed to already expired pseudonyms. Thus, we will give details of the current research and standardizations trend to design an efficient scheme.

The current VANET standards recommended vehicles to change their pseudonyms frequently such as every five minutes in ETSI TS 102 867 standards [107] and every 120 seconds or 1 km whichever comes first in the SAE J2735 standard [108]. The author in [41] suggested that each pseudonym should be used to sign two or more messages in a short time frame to allow short-term linkability by the receiver and meet applications' requirements.

However, pseudonym changing strategies with a repetitive pattern is not enough to preserve the privacy of the driver from continuous tracking. A service provider or a global adversary is able to collect messages over a long period and then analyse them using the spatio-temporal information in each message to discover the pattern. Researchers proved that even if messages were fully anonymous, a global adversary can effectively track vehicles [109-111] which means it is even easier in periodical pseudonym change at fix [112] or random [113] periods.

A repetitive pattern could be in time such as in periodical pseudonym change at fix-time [112] or in transition such as in mix-zone areas where a pseudonym changes at

a predefined area such as at intersections or petrol station [15, 114]. Buttyán et al. [115] conducted a comprehensive analysis to deliberate the inefficiency of changing pseudonyms in a mix-zone area. They concluded that if the adversary only controls half of the road intersections, the adversary is still able to identify vehicles with successful tracking reaching 90%.

Thus, the need for stopping sharing locations is highlighted to avoid long-term linkability in which the vehicle is forced to enter a silent period before changing the pseudonym, in which the vehicle stops sharing its location for a predefined period [16, 23, 112]. In the SAE J2735 standard [108], the vehicle was recommended to enter a random silent period, which could be within a period of 50-250m or 3-13s whichever comes first, before changing its pseudonym. Accordingly, an adversary cannot predict the next pseudonym change, which could improve privacy, but the vehicle could be still identifiable if it is the only one that has changed its pseudonym. In [116], Tomandl et al. suggested to increase the anonymity set size through synchronizing the silent period and pseudonym change between all vehicles in the network. This is still insufficient as the vehicle could be still identifiable in sparse traffic or being alone in the road.

To overcome the aforementioned issues, Gerlach and Guttler [24] proposed a mix-context approach in which the vehicle holds its pseudonym for a stable time. Then, it only changes its pseudonym if it is surrounded by k-neighbour vehicles who have the same direction and speed, or the maximum pseudonym lifetime is passed. After changing the pseudonym, the system will consider the change was successful only if there are other vehicles within the same speed and direction also changing their pseudonym simultaneously and then holding the pseudonym for a minimum stable time. Otherwise, the vehicle directly starts looking for another opportunity to change

its pseudonyms. Similarly, Liao and Li in [25] proposed a context-based scheme but the velocity of vehicles is also included in the context comparison. Moreover, to ensure simultaneous change a ready flag is added to the message, which is set to 1 after the vehicle holds its pseudonym for a stable time. The ready flag had already been proposed in the conclusion by Gerlach and Guttler [24] but implemented in [25].

Although silent periods can address the issue related to continuous tracking, only a few schemes consider their impact on safety applications. For example, if there is a potential accident during a silent period, the scheme could prevent safety applications from sending a timely alert. Buttyán et al. propose the SLOW scheme [14] in which vehicles enter silent periods at low speed (less than 30 km/h) to decrease the opportunity of having accidents. A state-of-the-art scheme in 2015 was designed by Emara et al. [28] to improve safety by increasing message updating rates by reducing silent periods. They proposed a Context Adaptive Privacy Scheme (CAPS), which also synchronizes silent periods between the nearby vehicle(s). The ability of the vehicle to be trackable is employed in CAPS to exit silent and resume sending a message as soon as predicting that eavesdropper is confused. Accordingly, vehicle tracker is assumed to be installed in each vehicle to be used in its silent period in which the vehicle keeps tracking itself and its silent neighbours. Then, when the vehicle finds itself in unpredicted locations or its predicted silent neighbour, it exits the silent period. The CAPS scheme seems to be a promising scheme as it improves the balance between the three key issues (security, privacy, and safety). However, in CAPS, if the context of the vehicle is expected to be mixed with any other silent vehicles, the vehicle randomly exits a silent period to prevent the local attacker who might be able to predict when the vehicle would probably to exit the silent period. However, when the context of vehicles is expected to be mixed, it would indicate a probability of accidents.

Moreover, in CAPS, the probability of accident during this period is high which we aim to reduce it in this thesis.

3.7 Privacy Metrics

To evaluate the achieved level of privacy when applying different pseudonym changing schemes, a variety of metrics have been applied or designed. In the following, we present the most popular privacy metrics.

- Anonymity set size: the Anonymity Set (AS) of a target vehicle (i) is defined as the set of all vehicles whose trajectory may be equivalent to the trajectory of the target vehicle T_i [117]. The number of vehicles included in AS is denoted as $|AS|$ and represents the achieved level of privacy protection. Given a vehicle $i \in ID$ and its trajectory T_i, AS is calculated using the following formula:

$$AS_i = \{j | j \in ID, \exists\, T_i, T_j \in T, p(i,j) \neq 0\} \qquad (1)$$

- The entropy of AS: AS metric does not take into consideration the prior knowledge of the adversary which makes some vehicles more likely to be the target vehicle. This can be achieved using the entropy metric [118] which is denoted as H. Thus, $H = 0$ when the same pseudonym is used to authenticate several messages. Given p_i as the probability assigned by the adversary for a vehicle i being the target, H can be calculated using the following formula:

$$H = -\sum_{i=1}^{|AS|} p_i \times \log_2 p_i \qquad (2)$$

- Degree of anonymity: The maximum entropy is achieved when the probabilities are uniformly distributed over the anonymity set i.e. if the probability of all vehicles having the same value, the $H_{max} = \log_2 |AS|$. Accordingly, Diaz in [119] proposed an extended metric to calculate the degree of the anonymity (d) as given in the following formula:

$$d = \frac{H}{H_{max}} \qquad (3)$$

- Tracking probability metrics: the ability of an adversary to track a vehicle and re-identify its trajectory is important to evaluate the location privacy [120]. As a result, several metrics are designed to calculate this probability. Huang et al. [121] measured how long a vehicle could be tracked continuously by an adversary. In [23], the maximum cumulative time of $|AS_i| = 1$, which means vehicle i has no anonymity, is defined as a probability tracking metric. Hoh et al. [120, 122] have defined two metrics (time-to-confusion and distance-to-confusion) in which the tracking time/distance until the adversary reaches a specific confusion level (i.e. using uncertainty or Entropy) is calculated. Moreover, the percentage of vehicles that can be tracked from their departure to their destinations [14, 123] is used to measure the tracking success rate.
- Distortion/confusion metrics: the difference between the real and the reconstructed tracks is used to design distortion-based metrics. In [124, 125], the authors calculated the accuracy of an adversary as the distance error between the actual position and the estimated position. In [126], the average number of confused tracks per vehicle is used to measure the location privacy. This confusion could have happened when the adversary does not sign a track to its originated vehicle due to changing its pseudonym or missing a beacon.

3.8 Vehicle Tracker

A vehicle movement is predictable as it is limited to road structure, speed regulation, traffic density, etc. Thus, in VANET, an adversary is able to track vehicles not only by linking safety messages having the same pseudonym but also using the spatio-temporal information in case of pseudonyms being changed. That is because the

adversary can utilize a multi-target tracking algorithm [109-111, 115] to track vehicles through their beacon messages. As discussed in the previous section, a number of privacy metrics [23, 24, 109, 127] have been designed based on tracking ability, to evaluate and compare the achieved privacy level when applying different pseudonym schemes.

In [123], Emara et al. have designed a vehicle tracker model that is considered as a typical multi-target tracking problem because beacon messages were assumed to be fully anonymous. The vehicle tracker collects the broadcasted messages from vehicles within its coverage area and tries to reconstruct the full route of each vehicle via linking between these messages using the spatio-temporal information. They assumed that the attacker controls the whole road network via distributing receivers such as RSUs installed along the road and receive the exchanged messages that can be sent later to the service provider. The service provider can apply the vehicle tracker to reconstruct the full journey of each vehicle; which breaches privacy. The vehicle tracker has adjusted to include silent periods [128] to compare the efficiency of different pseudonym changing schemes; which mainly consists of four iterative phases as illustrated below:

- State estimation phase: its goal is to find the best estimation of the target vehicle's state in the next time step k+1. The most common state estimation filter is Kalman filter [129], which is an iterative process including the prediction and updating phases, as illustrated in Figure 3.2. In the prediction phase, the next estimated state at k+1 is generated depending on the current state at k and a predefined kinematic model. Then, in the updating phase, the vehicle state is updated either from the broadcasted message (i.e. GPS inside vehicle detects its location) or using the estimated state (k+1) in case of missing the broadcasted messages due

to a communication fault or the vehicle being silent. More details about the Kalman filter and its mathematical equations can be found in [130].

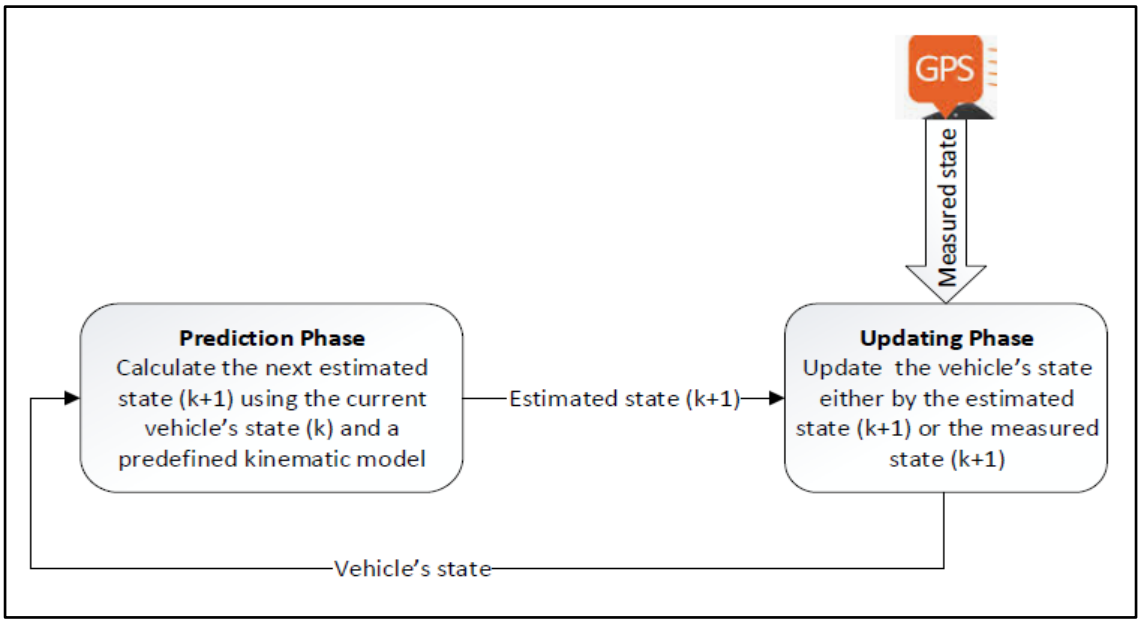

Figure 3.2 Kalman filter process

- Data association phase: the broadcasted messages are linked to their originating vehicle via matching pseudonyms. However, when a vehicle changes its pseudonym, a probabilistic association approach is required to link between messages. In [128], the nearest neighbour probabilistic data association (NNPDA) algorithm [131] is used in which the probability for each beacon message to be associated with its originating vehicle is calculated. Then, the optimal assignment is selected in which its accuracy is improved when vehicles are far away from each other and/or the beaconing rate is increased [132].
- Gating phase: to improve the efficiency of NNPDA, the gating process is required to narrow the association scope by excluding the unlikely beacon messages that are outside the validation area. The most common gating technique is the ellipsoidal [133] gating in which the association is only allowed if the location in the estimated state is within a predefined gate. In Figure 3.3, three vehicles are given

with their estimated state in which the estimated state of vehicles is represented in a dark colour while the actual state is in a lighter colour. Then, the ellipsoidal shape is generated around each estimated state to reduce comparison in which vehicles 1 and 2 have only one option (1~ and 2~) but vehicle 3 will compare two values 2~ and 3~.

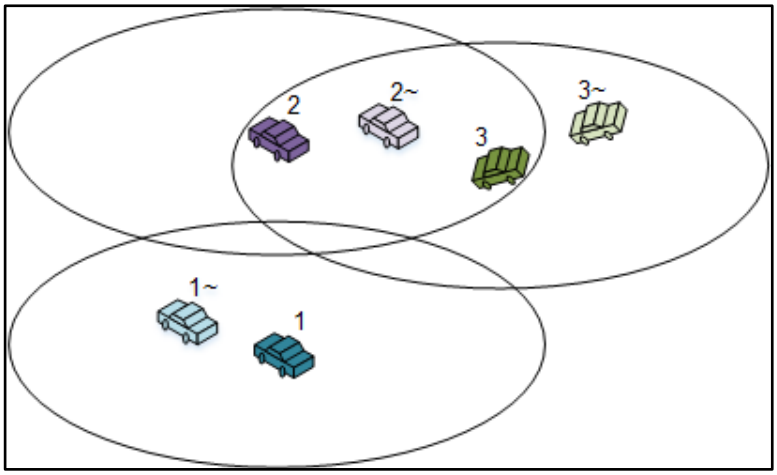

Figure 3.3 Gating phase

- Maintenance phases: as the number of vehicles in the road is dynamic, this phase is important to stop tracking vehicles outside the road networks or the communication range (i.e. having arrived at their destination) and start tracking new vehicles entering the road network (i.e. starting their journey). The vehicle tracker can recognize a vehicle enters/exits the road when it starts/stops sharing safety messages. Thus, this phase was adjusted to deal with silent periods in [123] in which the vehicle tracker will continue tracking vehicles up to its maximum silent period.

In CAPS [28], the above vehicle tracker is also assumed to be installed in each vehicle to enhance the efficiency of the pseudonym changing scheme in which in each time step vehicle can decide locally to stop sharing messages or change pseudonyms

depending on its state and their neighbours' states. Similar to CAPS, we need the vehicle tracker in designing our schemes as we will demonstrate in the next chapter.

3.9 Summary

Using pseudonyms has been widely accepted as the underlying strategy to achieve both security and privacy in VANET safety applications. Thus, in this chapter, different cryptographic schemes, which are used to implement pseudonyms, are illustrated along with the nominated one for safety applications i.e. the cryptographic scheme depending on PKC. Then, the overheads of PKC are explained along with the possible solutions. Moreover, to achieve the balance between security and privacy, state-of-the-art pseudonym management and changing schemes are illustrated followed by the most popular privacy metrics. Finally, a vehicle tracker has been illustrated in detail because it can be used to measure the achieved privacy level and/or to reduce wasting pseudonyms.

So far, in VANET, there is still a need to design a scheme that efficiently balance between the three key issues: security, privacy, and safety. Thus, next, we aim to design a pseudonym changing scheme in which security overheads are reduced by avoiding changing pseudonym in observed situation, privacy is preserved by applying the same CAPS technique i.e. vehicle tracker to investigate the mix-context, and finally, the functionality of safety applications is improved via avoiding potential accidents during the silent period and reducing pseudonym change resulting in the reduction of the number of lost messages.

Chapter 4 : Privacy Scheme for VANET Safety Applications

4.1 Overview

In the previous two chapters, we presented a review of VANET safety applications, their requirements, and the existing research effort to achieve an acceptable balance between the conflicts in their requirements. In this chapter, the possible promising solutions and challenges of using pseudonyms in VANET safety applications are explained first and followed by the reasons that motivated us to design the new scheme. Then, the design and implementation of the proposed Safety-related privacy scheme (SRPS) are presented. To compare the performance of the new scheme, it is compared with five other schemes from literature. The best scheme is defined by achieving the three key issues: security, privacy, and safety (i.e., it balances between them without compromising one key as a result of achieving another key).

Standardization organizations have nominated a Dedicated Short-range Communication (DSRC) [4, 108, 134, 135] over satellite or cellular wireless technologies; that is because it has the minimal delay (latency) less than 200ms and it is free [6] which facilitate both real-time and cost constraints. The DSRC is a short to medium range (100 to 1,000m) wireless communication medium, which is used for the communication between V2V and V2R but it is typically 300m to promote higher frequency reuse [5]. IEEE 802.11p is considered as the de facto DSRC in which Wireless Access for the Vehicular Environment (WAVE) is integrated to facilitate implementing VANET applications [5]. VANET has attracted attention from governments, industries, and researchers. The Federal Communications Commission (FCC) in the US has dedicated a new spectrum for VANET, which is 75 MHz in the 5.9 GHz band. The European Telecommunications Standards Institute (IETS) has

allocated a radio spectrum of 30 MHz at a 5.9 GHz band. Subsequently, many projects devoted to VANET, such as the Car-to-Car communication consortium [136] in Europe, and The Research and Innovative Technology Administration in the United States [137].

To secure communication and protecting privacy in VANET, standardizations [138-140] and researchers' effort [32, 141] have adopted pseudonym-based schemes based on public-key cryptography (PKC). In PKC, a pair of key (public and private) is required in which the public key must be certified by a trusted third party to ensure the authenticity of the driver/vehicle. Then, a vehicle digitally signs the sent message using the private key to prove its integrity and attach the signature and the certificate of the current valid public key to the broadcasted messages. Moreover, a timestamp is required to be attached to the message to avoid replaying messages later.

As the vehicle can still be identifiable via its locations included in the broadcasted safety messages, standardization organizations and academia have recommended changing these pseudonyms frequently after being silent for a period, as detailed in section 3.6, to preserve the privacy of vehicles/drivers.

4.2 Motivation

Although the research efforts to design a pseudonym changing scheme, an efficient scheme, is still an open issue. The frequent pseudonym changes and the length of the silent period could have an impact on the following aspects:

- Pseudonym needs to be issued and certified by authorities so that if pseudonyms are changed more frequently, the need for communicating with these authorities is increased.

- Pseudonym and its certification must be stored securely inside the vehicle (TPD) so that if pseudonyms are changed more frequently, vehicles require to store a large number of pseudonyms (i.e. increasing the storage overheads).
- The new pseudonym must be sent along with safety messages and needs to be verified by the receiver so that the frequent change would impact the communication and computation overheads.
- A simple pseudonym changing strategy cannot efficiently preserve the privacy of the driver [109, 111]. In [14], Buttyán et al. have highlighted the two pseudonym linking attacks which are either: pseudonyms could be linked to each other syntactically when a vehicle changes its pseudonyms individually; or they could be linked semantically using the spatio-temporal information in beacon messages.
    - The syntactic attack could be avoided by synchronizing pseudonym changes between vehicles.
    - The semantic attack could be avoided by stopping sharing the location for a period i.e. silent period.
- The longer silent period could improve privacy but there is an impact on safety as an accident could happen during this period i.e. safety applications need a continuous updating of vehicles' locations.
- Using each pseudonym for a short period will prevent long-term linkability (i.e. enhance privacy). Yet, the overheads are increased, and the efficiency of safety applications will be decreased (i.e. the number of lost messages is increased due to both communication and computation overheads), as illustrated below:
    - Communication overheads could be reduced if the certificate is only sent when a new neighbour is recognized in the communication range [44]. However, when a pseudonym is changed, it needs to be sent.

- Computation overheads could be decreased by storing the already certified pseudonym, thereby omitting the need to verify it again [44]. Thus, when a pseudonym is changed, it needs to be verified (i.e. increase the verification overheads).

Thus, we aim to design an efficient scheme that could achieve the best balance between the three key issues: security overheads, privacy level, and safety level.

4.3 Proposed Safety-related Privacy Scheme

The main aim of the Safety-related Privacy Scheme (SRPS) is to reduce the impact of the existing privacy schemes, which applied silent periods, on VANET safety applications. This could be achieved by determining the appropriate context for a vehicle to update its pseudonyms or enter/exit a silent period [28] and by avoiding any predicted accidents through this period. Figure 4.1 shows an example of three vehicles' traces and four states which represent the noteworthy positions. In these four states, two vehicles are expected to be at the same time in the same positions that may confuse the attacker or cause an accident.

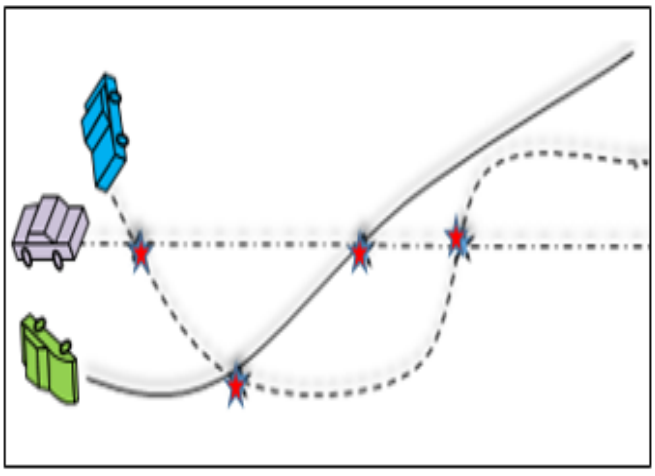

Figure 4.1 Vehicle's traces with noteworthy positions

Accordingly, the main contribution of SRPS is to find the above noteworthy positions which could achieve the following:

1. Reducing accidents during silent periods as each vehicle (silent/active) in each time step calculates in advance its predicted next positions and its predicted neighbours' (silent/active) positions using Kalman filter. Then, if a silent vehicle predicted any accident in the next time step, it exits the silent period and starts sharing its state.
2. Reducing the need for pseudonyms, that need to be issued, stored, verified, and sent, because of reducing the change of pseudonyms in an observed situation i.e. wasting pseudonyms in an observed situation.
3. Enhancing the functionality of safety applications via reducing silent periods in which a vehicle can successfully change its pseudonym without entering a silent period. That is because the vehicle calculates the next predicted position of itself and neighbours' (silent/active) positions using Kalman filter and then if its position is probably to be mixed with others, it will broadcast its new state using a new pseudonym.
4. Increasing the chance of mixing context because vehicles cooperatively enter a silent period and directly start looking for the mix-context with their silent neighbours before being far away from each other. Unlike other cooperative schemes as they force a minimum silent period to ensure protecting the privacy, for example, in CAPS [28], vehicles cooperatively enter a silent period and after 3s starts looking for the mix-context but as the vehicle can travel [142] up to 60m within the 3s, it would have less chance to find mix context i.e. they will be far away from each other.

The SRPS consists of two main algorithms: SRPS-Active to guide each vehicle in its *active* status, as illustrated in Algorithm1, and SRPS-Silent to guide each vehicle in its *silent* status, as shown in Algorithm2. Each vehicle needs to use the Kalman filter illustrated in section 3.8, which can help the vehicle to predict the states of itself and its neighbours. Then, depending on the prediction states, a vehicle can decide locally to change its status such as in case the adversary is probably to be confused or an accident will probably happen if continue ceasing messages. The notations used in these algorithms an in the thesis are illustrated in Table 4.1. In SRPS-Active, a vehicle tries to synchronize silent periods or finds a mix-context to change its pseudonym while in SRPS-Silent, the vehicle keeps tracking its neighbours to avoid any potential accidents and looking to exit the silent state when the attacker is probably to be confused, as illustrated next.

Table 4.1 Notations

Symbol	Stand for	Notation
$\boldsymbol{vL}$	Vehicle Lifetime	The vehicle enters and exits the road at different times. Thus, the lifetime for each vehicle is the difference between exits and enter time.
BR	Beacons Rate	The number of sent BMs per second.
VS	Vehicle State	The current vehicle state (position, speed, and heading) sensed by GPS
EVS	Estimated Vehicle State	The estimated vehicle state at the next step using the Kalman filter.
$\boldsymbol{P'_v}$	next Position of Vehicle itself	The expected position of the vehicle itself using the Kalman filter.
SBM	Sent Beacon Message	Which is either 1 when a vehicle shared its state or 0 when the vehicle is silent.
RBMs	Received Beacon Messages	The received current states of nearby vehicles within a predefined communication range.
ERBMs	Estimated Received Beacon Messages	Estimate the new state of neighbours (RBMs) for the next step using an in-vehicle tracker.
$\boldsymbol{P'_n}$	next neighbour Position	The expected position of neighbour vehicles using the in-vehicle tracker.
nV	number of Vehicles	Total number of vehicles

Symbol	Stand for	Notation
nN	number of Neighbours	Number of neighbours within a specific communication range
MinPL	Minimum Pseudonym Lifetime	It is recommended to be 60 s upon safety application requirements.
MaxPL	Maximum Pseudonym Lifetime	A longer lifetime would decrease privacy but enhance safety.
MinPD	Minimum Pseudonym Distance	It is the minimum distance that a vehicle should drive before changing its pseudonym. It is specified depending on MinPL as we will explain later.
MaxPD	Maximum Pseudonym Distance	It is the maximum distance that a vehicle should drive and then change its pseudonym. It is specified depending on MaxPL as we will explain later.
Dist	Distance	Distance has driven which is calculated upon the previous and current position
MinSP	Minimum Silent Period	The vehicle has to stop sharing its states for a minimum period.
MaxSP	Maximum Silent Period	The vehicle has to resume sharing its states after this period
CT	Current Time	The current real-time
PL	Pseudonym Lifetime	It is initiated when pseudonym is changed
SP	Silent Period	Ceasing safety messages started time and it is initiated when a vehicle enters a silent period.
MTs	Missed Tracks	Check if there is any vehicle within 50 or 100 m enter silent period then store its state in MTs.
PAA	Potentially Avoided Accidents	The number of potential accidents if the vehicle keeps silent.
SBMs/s	Sent Beacon Messages per Second	The average number of sent messages per second.
m/s	meter per second	Measure the speed of vehicles
m	meter	Measure the distant.
ms	millisecond	Measure the time.
$\boldsymbol{T_i}$	Tracking Vehicle	The maximum tracking period of vehicle i.
$\boldsymbol{nPseud}$	Number of Pseudonyms	The total number of pseudonyms used in the whole scenario.
$\boldsymbol{ChPseud}$	Change Pseudonym	The average number of pseudonym changes in the whole scenario.
$\boldsymbol{nV_{ch}}$	Number of Vehicles	The total number of vehicles who changed their pseudonym during the simulator

4.3.1 Algorithm1: SRPS-Active

- Algorithm1 takes as input the status of the vehicle, the Received Beacon Messages (RBMs) from its neighbour, its current Vehicle's State (VS), the Expected Vehicle State (EVS) of the current state from the previous step, the predefined MINimum and MAXimum Pseudonym Lifetime (MinPL, MaxPL), and the current Pseudonym Lifetime (PL).
- A vehicle will continue broadcasting messages with the current valid pseudonym until the PL passed MinPL, as demonstrated from steps 2 to 5.
- Then, when the MinPL is passed, the vehicle starts searching for an opportunity, as shown in Algorithm1 step 6 to 34, to change its pseudonym or its status depending on the following:
  - Changing pseudonym: the EVS from the previous time step (i.e. expected current state), which was predicted by the installed vehicle tracker using Kalman-filter in section 3.8, is compared with the actual current VS. The comparison is achieved by calculating the distance between EVS and VS. Accordingly, if the distance is sufficient to confuse the adversary, the vehicle will broadcast its state with a new pseudonym. That is because the state of the vehicle is different from the state that could be predicted by the adversary, such as if the vehicle is intending to go ahead but under specific circumstances (i.e. accidents or traffic jam warning), it might change its direction (i.e. turn right, stop, etc.).
  - Changing pseudonym: if the above condition has not met, the EVS and the expected neighbour states ERBMs are predicted for the next time step using the vehicle tracker in section 3.8. The EBRMs are calculated for all vehicles (i.e. silent and active neighbours) within the communication range. Then, the

distance between EVS and ERBMs is calculated and if the distance between the EVS and any of the ERBMs is small enough (i.e. the state of the vehicle could be mixed with another neighbour in the next time step), the vehicle broadcasts its current state and changes its pseudonym for broadcasting the next state, as shown in steps 13 to 23.

  - Change status: if the above two conditions have not met, the vehicle would check if any of its neighbour are being silent to cooperatively enter a silent period, as shown in steps 25 to 30. A silent vehicle can be recognized by the vehicle tracker when two consecutive messages from a neighbour are missed (i.e. if just one beacon message is missed, it could be due to communication overheads) [28]. Moreover, even if the neighbour vehicle enters its silent period, its next states can still be expected by the vehicle tracker for a period of time using the state maintenance phase in the vehicle tracker (i.e. the period of time meant that vehicle keep predicting its silent neighbours up to the Maximum Silent Period (MaxSP)).

- Otherwise, if the above three conditions have not met, the vehicle will keep broadcasting safety messages using the same pseudonym until the PL has passed its MaxPL, as shown in steps 32 to 34. Then, when PL has passed MaxPL, the vehicle will be forced to stop sharing messages to avoid long-term linkability.
- The outputs from this algorithm are the vehicle's status, EVS, RBM, SP, and PL.

4.3.2 Algorithm2: SRPS-Silent

- Algorithm2 is run when the vehicle starts its silent period and it takes as input the status of the vehicle, the Received Beacon Messages (RBMs) from its neighbour, its current Vehicle's State (VS), and its expected current state from the previous

time step (EVS), the predefined MAXimum Silent Period (MaxSP), and the total Silent Period (SP).

- A silent vehicle will directly start searching for an opportunity to resume sending messages according to the following conditions.
  - Unexpected state: if the state of vehicle from the previous time step (EVS) is not equal to the current actual state (VS), i.e. the position of the vehicle becomes unexpected, it will change its status and resume sending messages, as illustrated in step 3 to 7.
  - Mixed-context/ Predicted-accident: in every time step, the vehicle predicts its next state EVS and its next silent/active neighbour states ERBMs using Kalman filter in section 3.8. Then, calculating the distance between EVS and ERBMs and if the state of the vehicle could be mixed with another neighbour in the next time step (i.e. if the distance between EVS and any ERBM is small, the adversary is probably to be confused between them). Accordingly, the vehicle will change its pseudonym and start sharing its state, as shown in steps 13 to 23. Moreover, when the context of two vehicles is probably to be mixed, it means they probably will be in the same position or very near to each other which could cause an accident if the vehicle continues ceasing its state.
- Otherwise, if the above conditions have not met, the vehicle will keep ceasing safety messages until the SP has passed its MaxSP. Then, the vehicle will be enforced to start sharing its states to avoid the negative impact on the efficiency of safety application.
- The outputs from this algorithm are the status of the vehicle itself, EVS, SP, PL, RBM, and the total number of the Potential Avoided Accidents (PAA).

Algorithm1: SRPS-Active

Input (Status, RBMs, VS, EVS, MinPL, MaxPL, PL)

1. If (Status=Active)
2. If (**PL** <= **MinPL**)
3. *Broadcast* (**VS**)
4. **PL = PL + BR**
5. *GoTo step 1*
6. Else If (**PL** >= **MinPL**) and (**PL** <= **MaxPL)**
7. If (**VS**<>**EVS**)
8. *Change Pseudonym* ( )
9. **PL** = **BR**
10. *Broadcast* (**VS**)
11. *GoTo step 1*
12. Else
13. *Kalman_update* (**ERBMs**, **RBMs**)
14. *Kalman_predict* (**ERBRs**)
15. **nN** = *size of* (**ERBMs**)
16. *Kalman-update* (**EVS**, **VS**)
17. *Kalman-Predict* (**EVS)**
18. for i = 0 to **nN**
19. if (**ERBMs**[i]) ≈ **EVS**)
20. *Broadcast* (**VS**)
21. *Change Pseudonym* ( )
22. **PL** = **0**
23. *GoTo step 1*
24. Else
25. **MTs** = *MissedTracks* (**ERBMs**)
26. **mN**=*size of* (**MTs**)
27. If (**mN** > 0)
28. Status=Silent
29. **SP** = 0
30. *Call (SRPS-Silent)*
31. Else
32. *Broadcast* (**VS**)
33. **PL = PL + BR**
34. *GoTo step 1*
35. Else If (**PL** >= **MaxPL**)
36. Status=Silent
37. **SP** = 0
38. *Call (SRPS-Silent)*

Output (Status, RBMs, EVS, SP, PL)

Algorithm2: SRPS-Silent

Input (Status, RBMs, VS, EVS, MaxSP, SP)

1. If (Status=Silent)
2. If (**SP** <= **MaxSP**)
3. If (**EVS**<>**VS**)
4. Status=Active
5. *Change Pseudonym* ( )
6. **PL** = 0
7. *Call (SRPS-Active)*
8. Else
9. *Kalman_update* (**ERBMs**, **RBMs**)
10. *Kalman_predict* (**ERBRs**)
11. **nN** = *size of* (**ERBMs**)
12. *Kalman-update* (**EVS**, **VS**)
13. *Kalman-Predict* (**EVS**)
14. for i = 0 to **nN**
15. if (**ERBMs**[i] ≈ **EVS**)
16. **PAA** = **PAA** + 1
17. *Change Pseudonym* ( )
18. **PL** = 0
19. *Call (SRPS-Active)*
20. Else If (**PL** >= **MaxSP**)
21. Status=Active
22. *Change Pseudonym* ( )
23. **PL** = 0
24. *Call (SRPS-Active)*
25. Else
26. *Ceasing* (**VS**)
27. **SP** = **SP** + **BR**;
28. *GoTo step 1*

Output (Status, EVS, RBMs, SP, PL, PAA)

4.4 Implementation

4.4.1 System overview and assumptions

In our work, the security scheme will not be implemented and thus messages will not be signed or verified. However, the pseudonym is assumed to be a concatenation of the identity of the vehicle and a local counter which is increased by one if a changing pseudonym is required [143]. We would follow the assumption in [47] to evaluate the overheads of security schemes in which they assumed that the sender will only include the pseudonym when a new vehicle is entering its communication range or changing its pseudonym while the receiver will store the already verified pseudonyms to reduce computation overheads i.e. when pseudonym is received, it will be checked if it has been verified to omit its verification overheads. This assumption would be used to compare the security overheads of our designed scheme against other schemes in which the frequency of pseudonyms change would result in increasing the overheads. Moreover, the more frequent pseudonyms change means more pseudonyms need to be issued by the TA and to be stored in the vehicle.

According to the requirement of safety applications, a vehicle can exchange messages wirelessly with its neighbours within 300m based on DSRC/WAVE. These messages mainly include the state of the vehicle i.e. its current position, speed, and direction in addition to the security-related information such as its pseudonym, certificate, and timestamp. Moreover, the movements of a vehicle are restricted to road rules such as direction, speed limits, etc.; so that the vehicle tracker in section 3.8 is assumed to be installed on each vehicle that could predict the next state of the vehicle itself and maintain the states of its neighbour vehicles even if they are silent.

The vehicle tracker is used in CAPS [28] to predict the mix-context which shortens the silent period and reduces wasting pseudonyms in observed situations. In SRPS, it is

used for the same purposes in addition to avoiding accidents during silent periods by maintaining the silent neighbour states. Moreover, in CAPS, the silent vehicle only maintains the states of other silent vehicles but in SRPS, silent and active vehicles maintain the states of each other which could increase the opportunity of finding the mix-context as well as avoiding accidents.

Finally, we assume a global adversary model to test the worst case in which receivers would be installed alongside the whole road networks. Then, they can eavesdrop all exchanged messages between vehicles and send them to the central vehicle tracker to reconstruct each journey i.e. full route.

4.4.2 VANET Simulation

A real geographical road map is downloaded using the Open Street Map (OSM) database [144], which is a free editable map of the entire world. The road network map of (3.8 km*2.8 km) has been chosen in the city of Liverpool/UK, as shown in Figure 4.2, according to the two specific criteria illustrated in Figure 4.3. The first criterion is achieved by having two or more vehicles with the same probability to be in the same position. The other criterion is met by having vehicles with two or more directions having the same probability. These criteria would increase the confusion level of the attacker and prove the efficiency of any scheme in short-time (i.e. if the road is one way and one direction, the probability of the context between vehicles to be mixed is rarely and also the effect of silent period on privacy level cannot be measured as the vehicle would still be trackable from its location). The downloaded data of the road network from OSM will be saved in a file (*.osm.xml).

Due to the lack of real traffic data for hundreds of vehicles, the researcher depends on simulators to implement VANET environment. Accordingly, to apply SRPS to VANET, different simulation frameworks are used as well, as illustrated below:

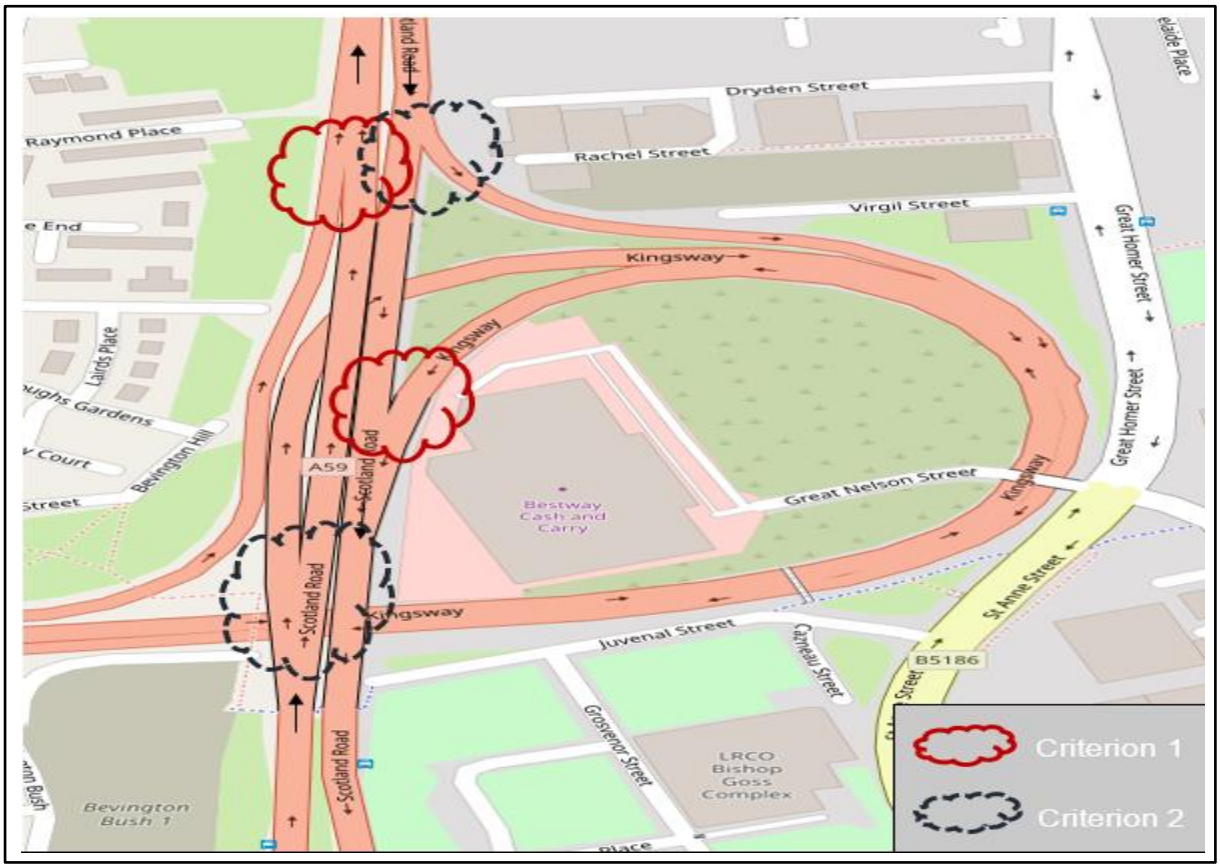

Figure 4.2 OSM road network

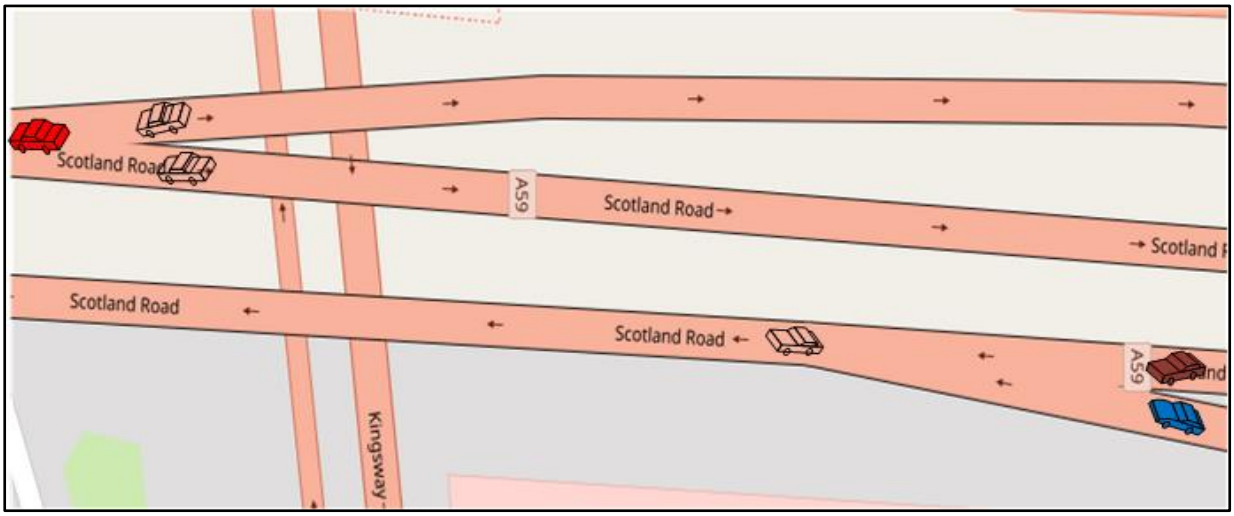

Figure 4.3 The confusing road section

- Mobility Simulator: SUMO [145] version 0.25.0 (Simulation of Urban MObility) is a time-driven discrete simulator used to generate large road traffic networks.
  - Imports the road network from *(*.osm.xml)* and stores it into the SUMO network file *(*.net.xml)* using *netconvert* script.
  - The visualization of the simulation is enhanced by importing the polygons, such as buildings, and rivers are imported from *(*.osm.xml)* and stored into the SUMO polygon file *(*.poly.xml)*. Importing the additional polygons file is needed, which is already downloaded with SUMO *(osmPolyconvert.typ.xml)*.
  - A set of random trips is generated via the script *"randomTrips.py"* which randomly choose the source and destination for each trip in a given network *(*.net.xml)* and store it in *(trip.trips.xml)*.
  - The full route for each trip in *(trip.trips.xml)* is also generated by script *"randomTrips.py"* and stored in *(*.rou.xml)*. When the type of the output file is a route, *"randomTrips.py"* will automatically execute the *"DUAROUTER"* script to discard the disconnected trips and specify the route for other connected trips. Examples of disconnected trips are given in Figure 4.4 and a screenshot of SUMO is shown in Figure 4.5 that represents the subsection of the downloaded OSM road network including the generated vehicles. Moreover, the arrival rate of vehicles is one per second (v/s) by default but we also increased that rate (one vehicle per 0.5s and 0.3s) to investigate the performance of each scheme in different traffic scenarios (i.e., when the density of vehicles increases)
- Network Simulator: OMNeT++ [29] version 5.0 (Object-oriented Modular NETwork) is a discrete event simulator used to build the wireless communication networks between vehicles.

- Vehicular Simulator: the framework Veins [29] version 4.4 (VEhicles In Network Simulation) is used to simulate the vehicular network which is a combination of OMNeT++ and SUMO. To provide a bidirectional connection between OMNeT++ and SUMO, a standard communication protocol - Traffic Control Interface (TraCI) - is used.
- Privacy Simulator: PREXT [143] (PRivacy EXTension for Veins), which supports several privacy metrics and schemes, is used to implement and evaluate the proposed privacy scheme. That is because, it facilitates the implementation as some modules are already implemented such as the vehicle tracker, safety messages, etc.

```
Error: No connection between edge '-217908398' and edge '31290438#4' found.
Error: Mandatory edge '31290438#4' not reachable by vehicle '0'.
Error: The vehicle '0' has no valid route.
Error: No connection between edge '5036087' and edge '-60198091#2' found.
Error: Mandatory edge '-60198091#2' not reachable by vehicle '10'.
Error: The vehicle '10' has no valid route.
```

Figure 4.4 Disconnected trips

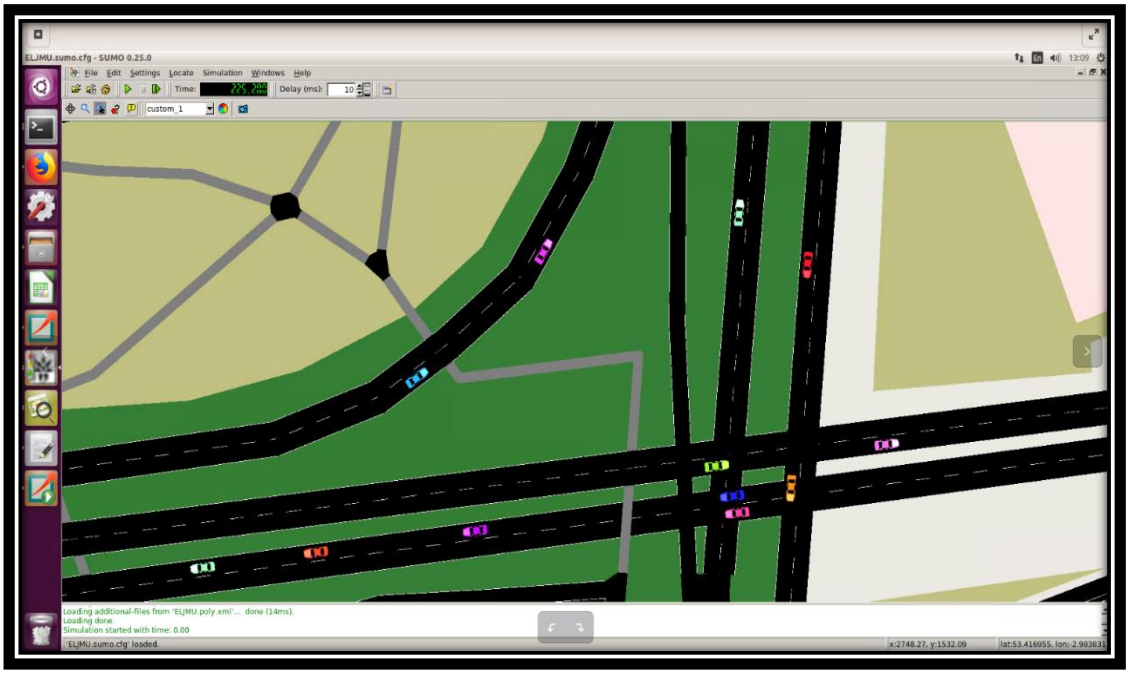

Figure 4.5 SUMO screenshot of the road network's subsection

4.5 Evaluations

4.5.1 Comparison

SRPS is compared against five state-of-the-art schemes (CAPS [28], PPC [113], RSP [16], CSP [116], and SLOW [14]) which adopt the same cryptography scheme (i.e., Public Key Cryptography (PKC)) to secure VANET communications and public keys are chosen randomly to anonymize the communications (i.e. certified pseudonyms are used instead of real identities). However, each scheme has applied different strategies to change these pseudonyms and avoid long-term tracking via the spatio-temporal data of the exchanged messages (i.e. privacy preserving). Moreover, to prove the hypothesis of SRPS, which is the privacy will be improved if there is no minimum silent period, we adjusted the minimum silent period in CAPS (ACAPS). The other five schemes are summarised briefly as follows:

- Context Adaptive Pseudonym Scheme (CAPS) [28]: It is a decentralized scheme in which the vehicle decides locally to change its pseudonym based on its state or its neighbours' states.
- Periodical Pseudonym Changing (PPC) [113]: It changes pseudonyms at random periods, which are selected within a predefined range.
- Random Silent Period (RSP) [16]: It is applying random silent periods which are selected within a predefined range.
- Coordinate Silent Period (CSP) [116]: It is a centralized scheme in which all vehicles in the networks will enter silent and change their pseudonym at the same time.
- Speed LOWer (SLOW) [14]: In this scheme, the silent status will depend on the context of the vehicle itself (i.e. when its speed is slow), and then it changes its pseudonym only if the silent period would be greater than a predefined value.

4.5.2 Setting up Parameters

In this section, the experimental comparison of SRPS against the above-selected schemes are provided. To compare the schemes fairly, their parameters are assigned equally whenever it is possible, such as pseudonym lifetime and silent periods. However, each scheme has its own aims, e.g., SRPS aims to avoid any accidents and thus does not have a minimum silent period, whereas SLOW and CSP do not have a silent period range, instead having only one value so that we assign 7s to the silent period (i.e. nearly the average of min and max silent periods of other schemes). In general, longer silent periods increase privacy but decrease safety because it decreases the number of exchanged safety messages [63]. Moreover, a shorter pseudonym lifetime will improve privacy as fewer messages can be linked continuously to the same pseudonym, but this would decrease the efficiency of safety applications (i.e. the new pseudonym is required to be sent and verified which could increase the lost messages as a result of increasing communication and computation overheads). In SRPS and CAPS, vehicles keep track of their neighbours within a specific radius which is set up at 50 m in these experiments. However, if we try to increase the radius value in order to increase the probability of finding more vehicles with the mix-context, the computation overheads will also be increased which could affect real-time decision making. In the future, we aim to adjust this value depending on the traffic status (i.e., number of neighbours). The parameters of each scheme and their values are given in Table 4.2.

To allow vehicles enough time to change their pseudonyms, each test runs for 360s which is 5 times the value of the minimum pseudonyms' lifetime. A random trip generation function in SUMO is used to generate three different trips databases for each arrival rate (v/s, v/0.5s, and v/0.3s) to test the efficiency of each scheme in a

sparse and dense traffic scenario. The evaluation depends on the average values of the three trips databases (Test1, Test2, and Test3) for each arrival rate, as shown in Table 4.3. Moreover, in Table 4.3, the number of vehicles with a minimum lifetime of 60 or 120 is calculated as it affects the final results (i.e., the higher number of vehicles having the opportunity to change their pseudonyms means more vehicles would be included to evaluate the scheme). Moreover, this table and the density of vehicles over time in Figure 4.6 would help to understand the cause of some results in the next section. Finally, we selected the highest beaconing rate for exchanging safety beacon messages, which is 10 Hz to show the worst possible tracking ratio.

Table 4.2 Parameters of each Scheme

Scheme	parameters
SRPS	MinPL=60 s MaxPL=120 s MinSP=0 s MaxSP=13 s Neighbour Radius=50 m
CAPS	MinPL=60 s MaxPL=120 s MinSP=3 s MaxSP=13 s Neighbour Radius=50 m
ACAPS	MinPL=60 s MaxPL=120 s MinSP=0 s MaxSP=13 s Neighbour Radius=50 m
RSP	PL=60 s MinSP=3 s MaxSP=13 s
CSP	MaxPL=120 s SP=7 s
SLOW	Speed Thresold=8 m/s Silent Threshold=7 s
PPC	MinPL=60 s MaxPL=120 s

Table 4.3 Number of Vehicles

Arrival Rates	Test1	Test2	Test3	Average	vL>=60s	vL>=120
v/1s	162	146	173	160	133	87
v/0.5s	281	308	262	283	230	148
v/0.3s	474	504	468	482	397	272

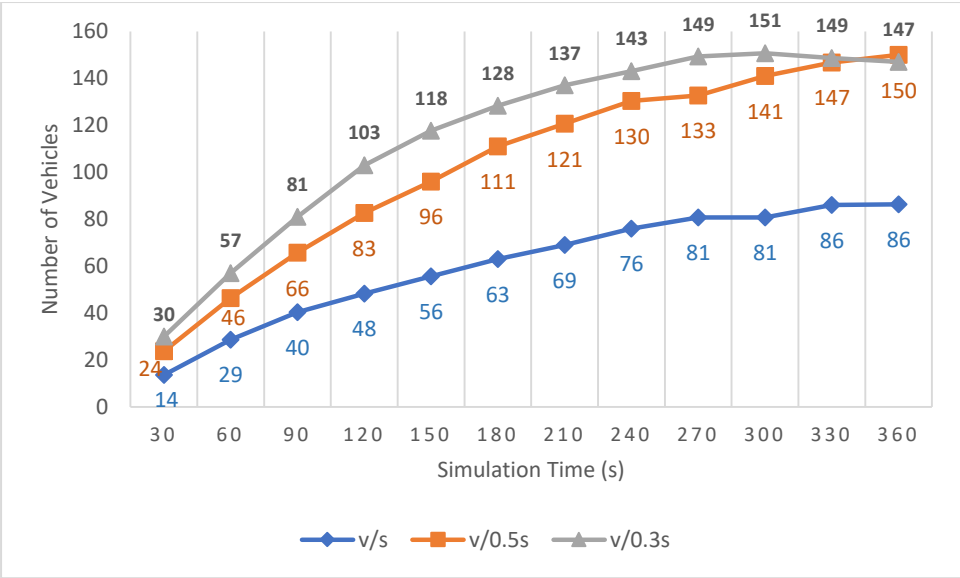

Figure 4.6 Density of vehicles during simulation in three arrival rates

4.5.3 Results and Discussion

The performance of SRPS against other selected schemes is evaluated using quantitative measurements. The statistics obtained from OMNeT++ and PREXT are discussed below, along with the newly designed metrics, for comparison purposes.

1. ***Security overheads*** are compared depending on the average number of changed pseudonyms (ChPseud), as calculated in equation (4), in which the total number of pseudonyms changed is divided by the number of vehicles that changed their pseudonyms at least one time during the simulation time. Then, to obtain the average number of changed pseudonyms per second, the result is divided by the average vehicle lifetime $\overline{vL}$. The security overheads should be kept as low as possible to enhance the efficiency of the applications.

$$ChPseud/s = \frac{nPseud}{nV_{ch} * \overline{vL}} \qquad (4)$$

where:

$$\overline{vL} = \frac{\sum_{i=1}^{nV} vL_i}{nV}$$

The average number of changed pseudonyms during the simulation time for each scheme in different traffic densities are presented in Figure 4.7.

Overall, the frequent of changing pseudonyms in the schemes that allow for a vehicle to decide locally depending on its state or its neighbours' states to enter a silent period and/or changing pseudonyms, is increased when the number of vehicles increases, as illustrated below:

- In SRPS and CAPS, each vehicle monitors its neighbours, which increases in dense traffic, to cooperatively start its silent period and/or change pseudonyms. The correlation between traffic density and pseudonym change in SRPS is consistent (i.e., 0.62/s, 0.66/s, and 0.73/s). However, in CAPS, it is inconsistent (i.e., 0.61/s, 0.61/s, and 0.65/s) which may be because a vehicle randomly exits silent and changes its pseudonym when finding a cooperative neighbour.
- In SLOW, the speed of vehicles is usually low in dense traffic. Thus, vehicles enter longer silent periods more frequently (i.e., pseudonyms change only if silent period above a predefined threshold) that increases the average pseudonym change (i.e., 0.59/s, 0.66/s, and 0.69/s).

However, traffic density does not affect the frequency of pseudonym change in the centralized schemes that depend only on time to enter silent periods and/or change pseudonyms. In Figure 4.7, the three centralized schemes RSP, PPC, and CSP, are illustrated as follow.

- In RSP and CSP, they suggested to enable vehicles entering silent period before changing pseudonyms but in different strategies (in RSP, each vehicle decides locally to enter a random silent period after holding pseudonym for 60 s while in CSP all vehicles in the network enter a fixed silent period every 60 s depending on system time such as GPS). The average number of pseudonyms

change per second of both schemes in all arrival rates is between 0.59/s and 0.63/s.

- In PPC, the traffic density does not have an effect on changing pseudonyms as well. That is because it enables the vehicle to change its pseudonym periodically after a random period chosen within a predefined range (60s – 120s) without considering other factors (such as its speed or its neighbours' states/number).

Overall, PPC has the highest number of pseudonyms (up to 0.74) which is probably because the vehicle does not enter a silent period (i.e., after changing pseudonyms, it will directly calculate the pseudonym lifetime to change it again while other schemes start calculating after the silent period has passed).

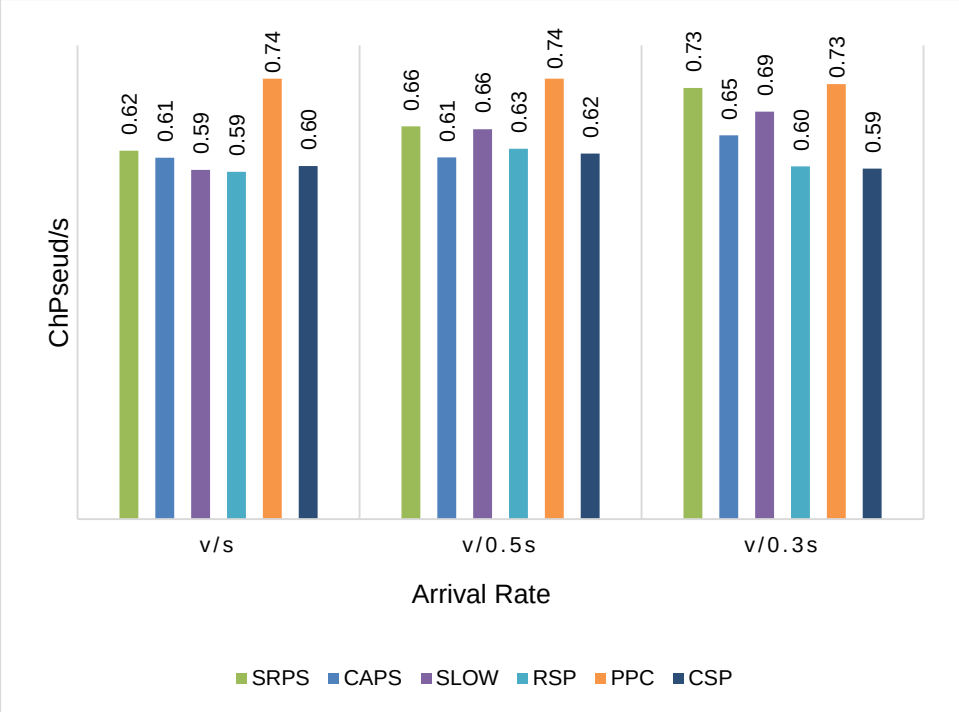

Figure 4.7 Average changed pseudonyms per second

2. ***Privacy-preserving level*** is compared depending on the traceability metrics in [128] which represent the ability of the adversary (i.e. using vehicle tracker in section 3.8) to reconstruct the original vehicle's trace T_i for more than 90%

using the broadcasted SBMs or the estimated locations. The continuous tracking is important to breach the privacy of the driver and de-anonymize the original identity such as using its home or work address. The adversary is able to link the broadcasted messages either by matching pseudonyms or using the spatio-temporal information in the messages in case of changing pseudonyms. However, the traceability decreases when the adversary fails to link the SBM to its originated vehicle (i.e., the SBM is assigned to different vehicles or cannot be linked to any vehicles which happens when pseudonym changes successfully). The average traceability percentage ($Trac_{ch}$) for vehicles, which change their pseudonyms at least once during the simulator, is given in equation (5) [128]. If the adversary can reconstruct over 90% of the vehicle's route, it is assumed to succeed and thus λ_i will be assigned 1. Otherwise; $\lambda_i = 0$, then the total summation will be divided on the total number of vehicles that participate in the calculation.

$$Trac_{ch}\% = \frac{1}{nV_{ch}} \sum_{i=1}^{nV_{ch}} \lambda_i \times 100\%, \qquad (5)$$

where:

$$\lambda_i = \begin{cases} 1, & \frac{T_i}{vL_i} \geq 90\% \\ 0, & Otherwise \end{cases}$$

Figure 4.8 shows the comparisons of the average traceability percentage that are calculated for each scheme using equation (5) for the three different traffic densities. The general trend is that the traceability percentages decrease when the number of vehicles increases except in CSP where it has fluctuated around 5. Moreover, in Figure 4.8, the cooperative pseudonym changes and applying silent periods have shown their effectiveness to reduce traceability, as illustrated below.

- In CSP, all vehicles in the road have cooperatively synchronized silent periods between all vehicles in the road network and therefore the lowest traceability percentages are achieved when applying CSP. This might be because the chosen road network always has a high number of vehicles as shown in Figure 4.6. Moreover, the properties of the chosen road network shown in Figure 4.3 would increase the difficulties for the adversary to link messages after the silent period. However, in reality, a vehicle could be alone in the road or could have different route from its neighbours so that it would waste pseudonyms (i.e. still trackable even if it changes its pseudonym).
- In SRPS and CAPS, a vehicle cooperatively enters a silent period if it recognizes any other nearby silent vehicles. Then, the vehicle starts looking for a mix-context with its neighbour or be in an unexpected position to start broadcasting SBM with its new pseudonym. However, SRPS reduces the traceability percentage nearly by 30%, as shown in Figure 4.8. In CAPS, silent vehicles only monitor each other to find the mix-context while in SRPS, all vehicles monitor each other which increases the probability of finding the mix-context. Moreover, in CAPS, the hypothesis is that the silent vehicle has to stop sending messages for at least 3s to ensure its privacy but in SRPS, the hypothesis is that the silent vehicle has to start looking for the mix-context with another silent vehicle directly before being far away from each other (i.e., increase the probability of finding the mix-context). Thus, we amended the parameters in CAPS by omitting the minimum silent period and therefore the traceability is decreased up to 12% as shown in Figure 4.9, where ACAPS refers to amended CAPS.

- In SLOW, a vehicle is being silent when its speed is low and the vehicle's speed decreases with the increasing number of vehicles so that more vehicles will cooperatively enter a silent period. Thus, it achieves low traceability percentages specifically when the number of vehicles increases (the traceability percentage reduces up to 14%). However, this reduction is not only from the cooperative silent period but also from the length of this period as will be illustrated later at the end of this section (4. Efficiency).
- In RSP, a vehicle individually enters the silent period and thus it is easier to be tracked (up to 83%) using its spatio-temporal information. However, the adversary could be confused if by chance there are other nearby vehicles being silent as well or vehicle being in unrecognized location. However, the lowest privacy level was in PPC because the vehicle continuously sends messages and is being tracked most of the time even if their pseudonyms change via its spatio-temporal information. Thus, PPC has recorded the highest traceability percentage (it is up to 94%).

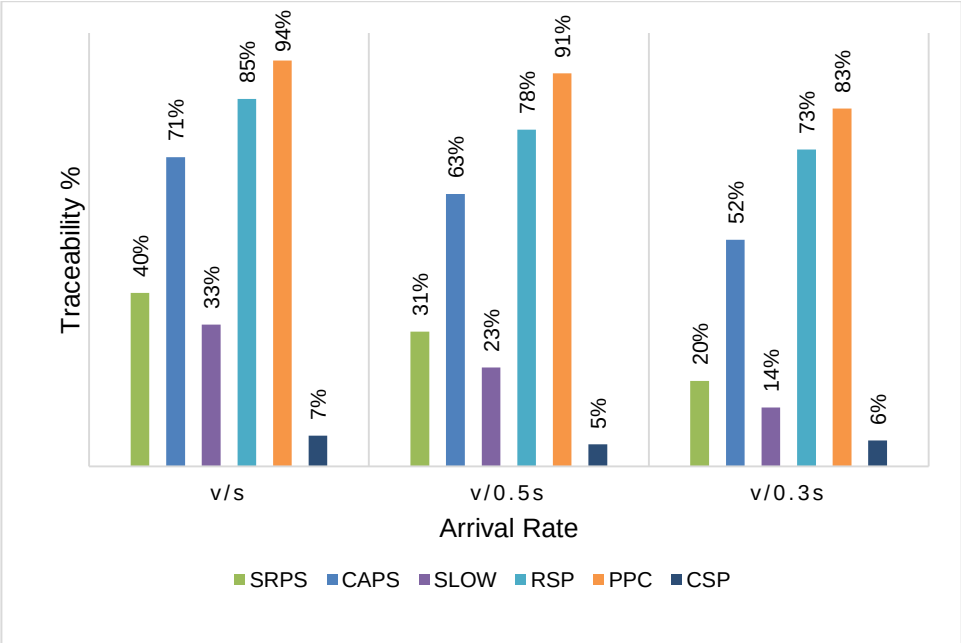

Figure 4.8 Average traceability percentage

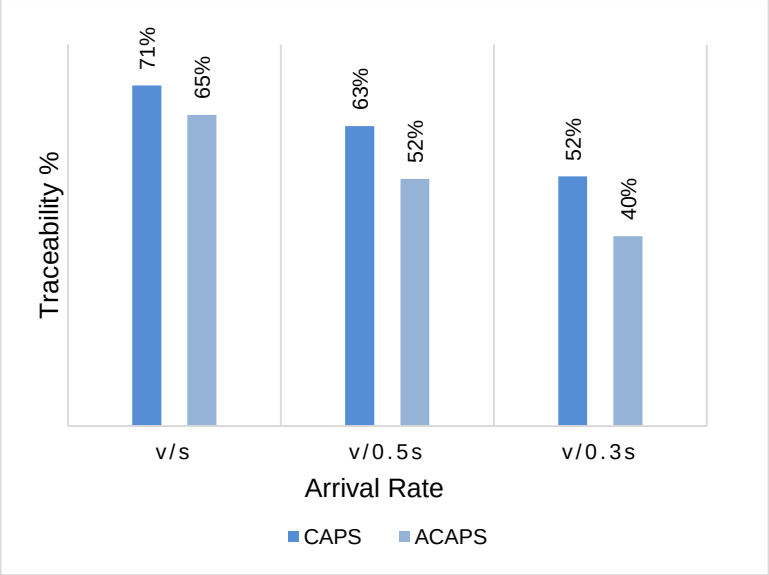

Figure 4.9 Traceability in the Adjusted minimum silent period in CAPS (ACAPS)

3. ***Safety level*** is mainly illustrated by calculating the average number of sent beacon messages SBM rate per second (SBM/s) as given in equation (6). The highest number would indicate shorter silent periods and thus enhance safety. Moreover, in SRPS, a silent vehicle keeps monitoring nearby vehicles and exits the silence if an accident is expected in the next step. Thus, the total number of potential accidents is calculated as given in equation (7).

$$SBMs/s = \frac{1}{nV}\sum_{i=1}^{nV}\frac{1}{vL_i}\left(\sum_{j=1}^{vL_i}\sum_{k=1}^{br} S\right), \qquad (6)$$

$$PAA = \sum_{i=1}^{nV}\left(\sum_{j=1}^{vL_i}\sum_{k=1}^{br}\sum_{l=1}^{nN} Z\right), \qquad (7)$$

where:

$$Z = \begin{cases} 1 & if\ P_s'(X_i, Y_i) = P_n'(X_k, Y_k) \\ 0 & otherwise \end{cases}$$

$$S = \begin{cases} 1 & if\ Status = Active \\ 0 & if\ Status = Silent \end{cases}$$

Figure 4.10 shows the average number of SBMs per second, which is initialized by 10 Hz but it is decreased depending on the silent period. As there is no silent period in PPC, the SBMs are 10 per second, which is compatible with the requirement of safety applications. However, SLOW has the lowest updating states (i.e. SBMs/s) that are always less than 6.50 (i.e., it means on average 3.5 messages missed every second). RSP has scored the second lowest value in which it is less than 7.65 messages every second. Accordingly, SLOW and RSP have the highest negative impact on safety.

The cooperative silent period schemes can improve safety by reducing the length of silent periods such as in SRPS, CSP and CAPS, the value of SBMs is always higher than 9 per second (i.e., if SBMs/s is 9.82, it means vehicles with a journey of 100s will broadcast 982 messages and cease only 18 messages). In CSP all vehicles synchronize their fixed-silent periods while in CAPS, a vehicle synchronizes its silent period with another silent neighbour (s) and exits this period as soon as the adversary could be confused. Similar to CAPS, in SRPS, the vehicle also synchronizes its silent period but is different from CAPS because of the following:

- It is allowed for the silent vehicle to broadcast its state once there is a forward potential accident. In the previous point (privacy level), we discuss the improvement in the privacy level in case of omitting the minimum silent period and it is applied to CAPS (ACAPS). This would also improve safety level as it increases the chance of finding the mix-context as soon as possible which decreases the silent period, as shown in Figure 4.11, the number of exchanged messages increased nearly by 0.20,0.30, and 0.60 along with the arrival rate.

- SRPS has increased SBMs/s over CAPS also because not only the silent vehicle is looking for a mix-context with its neighbours but also active vehicles. Thus, an active vehicle can change its pseudonym without being silent if its state is probably to be mixed with other nearby vehicles (silent/active), which increased the SBMs/s. Moreover, when the number of vehicles increased, the possibility of accidents increased, and the silent period minimized (i.e., SBMs/s is increased by 0.40 in sparse traffic then 0.49 and up to 0.60 in dense traffic).
- Finally, the number of predicted accidents that could be prevented in SRPS is illustrated in Figure 4.12 in which it is increased with the increase in the number of vehicles.

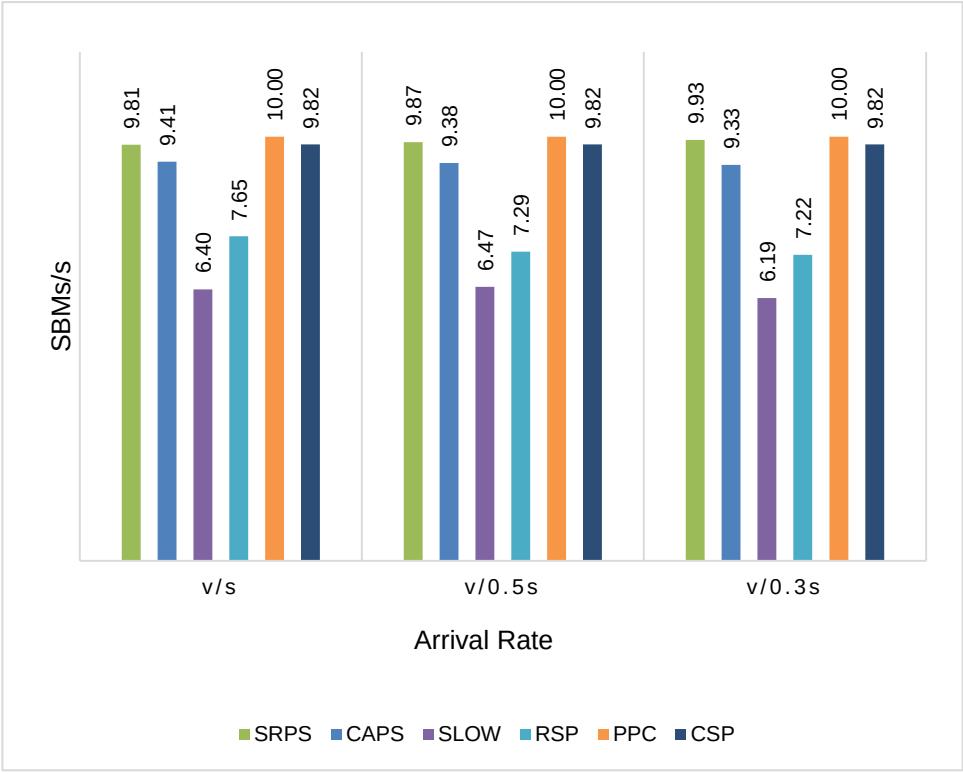

Figure 4.10 Average number of sending beacon messages per second

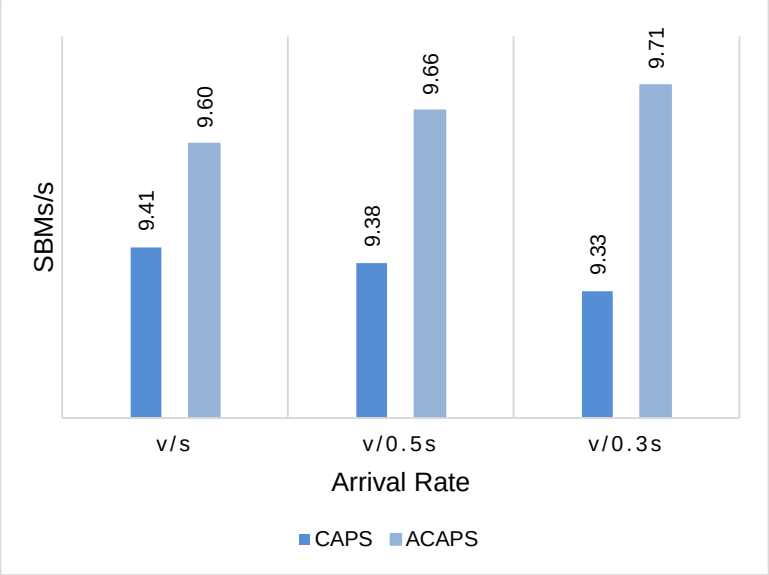

Figure 4.11 SBMs in Adjusted minimum silent period in CAPS

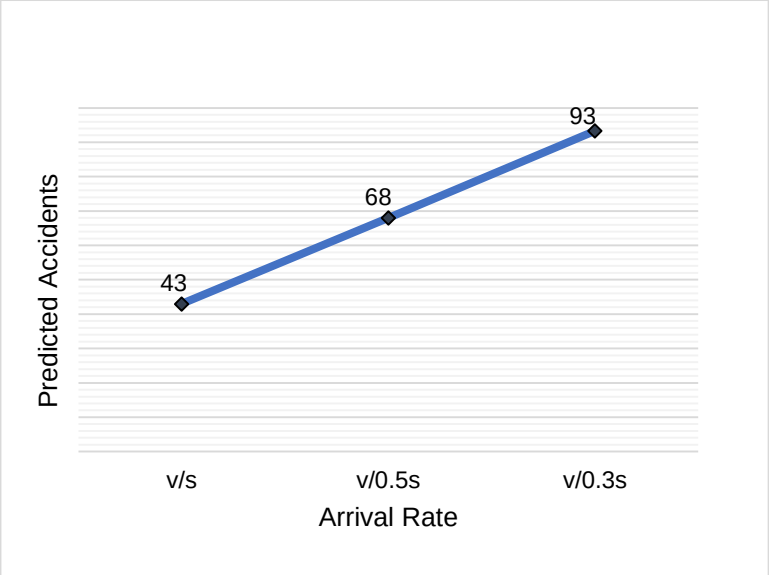

Figure 4.12 Number of predicted accidents in SRPS

4. **Efficiency** can be demonstrated by achieving the best balance between the three key issues: security overheads, privacy level, and safety, as illustrated below:

- Privacy levels can be enhanced in three approaches that are either by stopping the broadcast of a vehicle's locations, using pseudonyms for short period,

and/or changing pseudonyms only when the adversary is probably to be confused (i.e., the two consecutive messages cannot be linked probably).

- Safety level would be negatively affected if a vehicle stops broadcasting its states in which it is difficult to avoid accidents. Thus, SBMs/s should be kept as high as possible. Moreover, when the number of vehicles that synchronized silent period is increased, the traceability will be decreased. However, safety would be affected as it is also difficult to get knowledge of other neighbours' positions which increased the possibility of accidents
- Changing pseudonyms more frequently will increase security overheads. Thus, the number of lost messages increases, and safety functionality would be worsening.
- The best way to balance between the three key issues is to increase the confusion level during pseudonym changes and try to reduce pseudonyms change and silent periods.

Accordingly, we calculate the average of confusion level percentage (conf%) for each scheme in equation (8) and calculate the number of traceable vehicles (nV_{trac}) despite their pseudonyms are changed in equation (9).

$$Conf\ \% = \frac{1}{nV} \sum_{i}^{nV} \sum_{j}^{vL} \sum_{k}^{br} \beta_{i,j,k} \times 100\%, \qquad (8)$$

where:

$$\beta_{i,j,k} = \begin{cases} 1, & SBM_{i,j,k}\ cannot\ link\ correctly\ to\ the\ previous\ SBM_{i,j-1/br,k-1} \\ 0, & Otherwise \end{cases}$$

$$nV_{trac} = Trac_{ch}\% * nV_{ch} \qquad (9)$$

Figure 4.13 demonstrates the average confusion level and Figure 4.14 demonstrates the number of vehicles that are unable to protect their privacy instead of changing pseudonyms. The results observed from these two figures are summarized next.

- It is obvious from these two figures that the higher confusion level would reduce the number of traceable vehicles and vice versa.
- The confusion level is increased when the density of vehicles increases (i.e., the arrival rates increase).
- The silent period is highly important to prevent long-term linkability and maintain privacy, otherwise, vehicles would be traceable most of the time via their spatio-temporal information. Accordingly, PPC has the lowest confusion level in which the highest is only 10% and thus changing pseudonyms has usually failed (i.e., scored the highest nV_{trac} which is up to 250 vehicles wasted pseudonyms).
- The random silent period is insufficient as well because if the vehicle changes its pseudonym alone, it will remain traceable, as shown in Figure 4.13. Thus, RSP is similar to PPC, it is inefficient in which the highest conf% is only 22% and nV_{trac} is up to 141.
- CSP has achieved the best confusion level of 100% and the lowest wasting pseudonyms (less than 19 vehicles). Despite CSP can achieve the best confusion level, it compromises safety during its silent periods as all vehicle will stop broadcasting their states. Moreover, wasting pseudonym are most probably to be happened if vehicle have different route from its neighbour or being alone in the road.
- SLOW is able to confuse the adversary due to its long silent period, as demonstrated in Figure 4.7 nearly 4 messages are missed every second, which

has a negative impact on safety. Moreover, the conf% is high because vehicles in dense traffic would be driven in slow speed and thus more vehicles are staring their silent period cooperatively with its neighbours.

- Finally, CAPS and SRPS have employed the in-vehicle tracker to reduce the silent period by monitoring the confusion level and as soon as it is expected that the adversary could be confused, the vehicle will exit the silence. We enhance the confusion level, in SRPS, significantly (more than 39%) and reduce wasting pseudonyms specifically when the number of vehicles increased. That is because in our scheme, the silent vehicle starts looking for the confusing content with all nearby vehicles (silent/active) as soon as being silent. In contrast with CAPS as the silent vehicle will wait for 3s before starting looking to be confused with another silent vehicle.

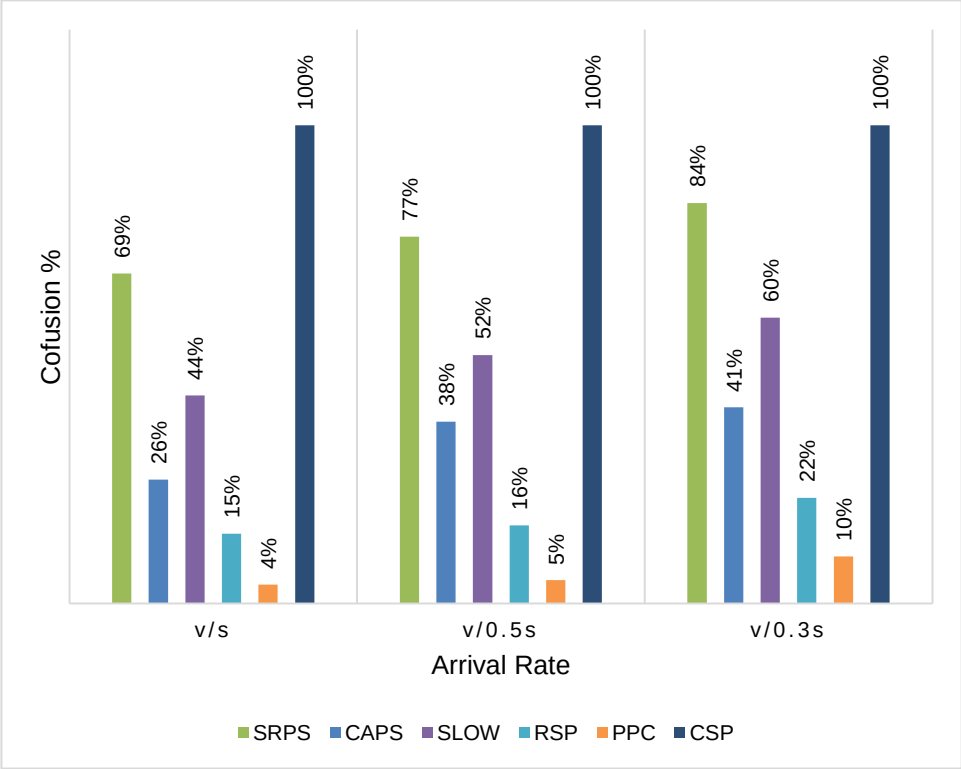

Figure 4.13 The average confusion level percentage

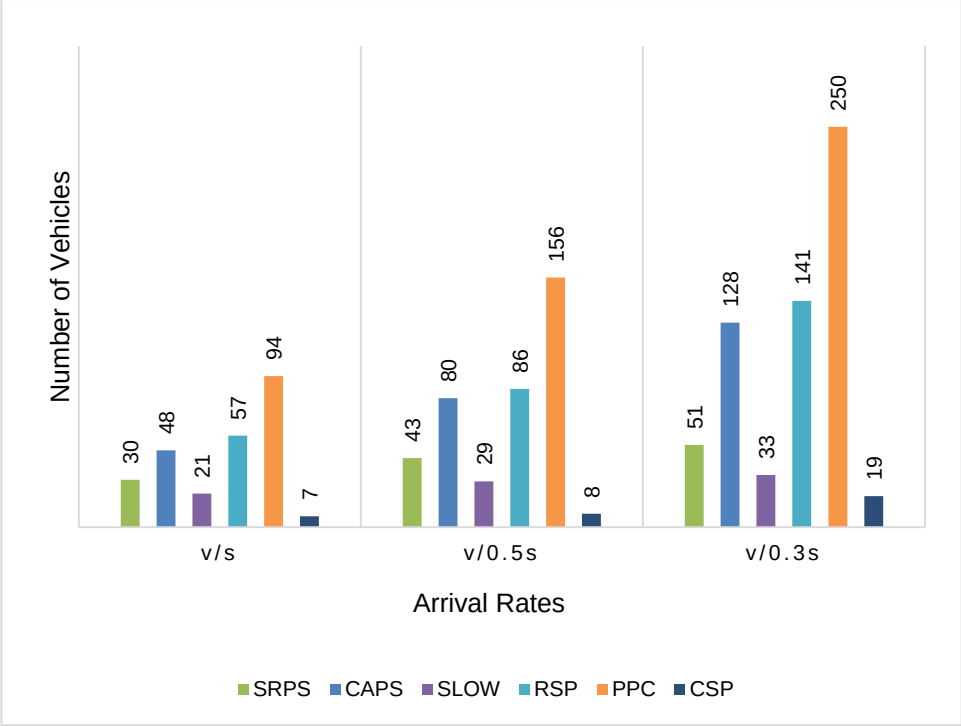

Figure 4.14 Number of vehicles wasted pseudonyms

4.6 Schemes' shortcomings

The challenge in pseudonym changing schemes is how to achieve an efficient balance between the three keys issue. To conclude the shortcoming of each scheme, we calculate the average of the three arrival rates in figures (4.7 to 4.14), as illustrated in Table 4.4. Then, as shown in Table 4.5, each scheme's result in Table 4.4 will allocate a distinct number between 1 and 6 in which 1 is allocated for the best scheme and 6 for the worst upon.

The safety level is allocated according to SBMs/s because safety applications require vehicles continuously sending their states to enhance their functionality such as avoiding accidents. Moreover, CSP and SRPS are affected by other features in which CSP is supposed to be the worst as all vehicles enter the silent period at the same time which would increase accidents and SRPS is supposed to be the second-best scheme after PPC as silent vehicles are always monitoring the expectation of having accidents, as shown in Figure 4.12, and exit silent to avoid it. Other schemes depend

totally on SBMs/s in which the highest is PPC (allocated 1) and the lowest is SLOW (allocated 5).

Privacy level and security overheads depend totally on $Trac_{Ch}$% and PseudCh/s, respectively. In the privacy column, the best scheme which allocated 1 is the scheme with the lowest traceability percentage. In the security overheads' column, the best scheme which allocated 1 is the scheme with the fewest pseudonyms changed.

The least efficient pseudonym changing scheme is the scheme that has the lowest confusion level which in turn would increase wasted pseudonyms such as PPC which is 6 followed by RSP which is 5. However, as the confusion level can be increased either by being silent for a long period such as in SLOW or by changing pseudonyms cooperatively such as in CSP, CAPS, and SRPS, SLOW is considered as inefficient for safety applications in comparison to a cooperative changing scheme. Then, the other cooperative schemes are allocated numbers depending on Conf%, and the number of a vehicle's wasted pseudonyms.

Table 4.4 Average values of the three arrival rates

	SRPS	**CAPS**	**SLOW**	**RSP**	**PPC**	**CSP**
SBMs/s	9.87	9.38	6.35	7.39	10.00	9.82
$Trac_{Ch}$%	30%	62%	23%	79%	89%	6%
PseudCh/s	0.671	0.625	0.644	0.603	0.742	0.602
Conf%	77%	35%	52%	18%	6%	100%
Wasted Pseud	41.45	85.34	27.43	94.84	166.57	11.60

Table 4.5 Comparison between the schemes

	Safety Level	**Privacy Level**	**Security Overheads**	**Efficiency**
SRPS	2	3	5	2
CAPS	3	4	3	3
SLOW	5	2	4	4
RSP	4	5	2	5
PPC	1	6	6	6
CSP	6	1	1	1

4.7 Summary

In this chapter, we proposed a Safety-related Privacy Scheme (SRPS) that significantly improves the balance between privacy and safety. It utilizes the ability of a vehicle to predict its next position and its neighbours' positions. This would assist vehicle 1) to change its pseudonyms effectively when its next position is more likely to be mixed with its neighbours and 2) to avoid a predictable accident when the vehicle is silent. The SRPS is compared with the other five privacy schemes in terms of reducing security overheads, achieving an adequate privacy level, and not compromising safety.

To summarize the comparison's results illustrated in Table 4.5, CSP and SLOW have compromised safety for privacy, and PPC has compromised privacy for safety. RSP has failed to achieve satisfactory safety or privacy level. Accordingly, SRPS and CAPS are the most promising schemes in which SRPS is better safety, privacy, and efficiency than CAPS but SRPS has higher security overheads. This could also impact safety applications due to increasing the lost messages (i.e., routing, verification overhead, and communication overhead). For this reason, we propose another scheme in Chapter 5 to reduce the security overheads specifically during the traffic jams when the verification and communication overheads are already high.

Chapter 5 : Pseudonym Changing Scheme

5.1 Overview

Pseudonym changing schemes have to support a challenging environment with high vehicle densities that generate communication and computation overheads especially via security overheads material (i.e., a digital signature and a corresponding certificate are attached to the exchanged safety beacon messages). The IEEE 1609.2 standards address the issues of securing Wireless Access in Vehicular Environment (WAVE) by applying the ECDSA [90] as a result of the security level per bit in comparison to other digital signature algorithms such as RSA [86]. For example, ECDSA with keys of 256 bits (32 bytes) and signature size of 64 bytes, resulting in a security level of approximately equal to RSA 3072 bits (384 bytes) and signature size of 384 bytes.

IEEE 1609.2 standard uses two variants of ECDSA, which are 224 bits for safety messages with short validity time and 256 bits for certificates with a long validity period. That is because of the trade-off between key size and communication, computation, and storage overheads in which longer key size takes a longer time to be attacked but increases the overheads. In tables 5.1 and 5.2, the comparisons of the communication and computation overheads between (ECDSA 224 bits (28 bytes) vs. ECDSA 256 (32 bytes)) and (ECDSA 256 bits (32 bits) vs. RSA 3072 bits (384 bytes)) are demonstrated. Moreover, the storage overheads can be extracted from the communication overheads in Table 5.1 because it is the addition of the public key, private key, and certificate.

Table 5.1 Communication overheads [142]

Algorithm	**Security strength**	**Size (Bytes)**			
		Public key	private Key	Signature	Certificate
ECDSA	112	28	28	56	113
ECDSA	128	32	32	64	117
RSA	128	384	384	384	788

Table 5.2 Computation overheads based on 400 MHz [146]

Algorithm	Time (ms)		
	Security Strength	Signature Generation	Signature Verification
ECDSA	112	≈4	≈16
ECDSA	128	≈6	≈23
RSA	128	≈240	≈8

In VANET, a public key is stripped from any identification details and used as a pseudonym which needs to be certified by a TA. Accordingly, before a vehicle sends a safety message, it adds a timestamp (i.e., to ensure message freshness) and signs it with its private key associated with the current valid pseudonym (i.e., validate via a certificate), as illustrated in Table 5.3. The receiver first has to verify the certificate, which contains the pseudonym and the signature generated by the TA's private key, using the TA's public key assumed to be provided in advance to all vehicles. Then, it has to verify the integrity of the message using the embedded pseudonym in the certificate [44].

Table 5.3 Sent safety message format

Safety message				Security		
Position	Speed	Direction	Road Status	Vehicle's pseudonym	Vehicle's signature (Safety message | Timestamp)	TA's certificated of the pseudonym

Attaching a certificate and verifying it would not be an issue in sparse traffic, but the issue is worsening when the number of vehicles increases. That is because the number of exchanged messages will be increased which would increase the lost messages via communication overheads, and also the number of received messages will be increased which would increase the number of lost messages via verification overheads (i.e., messages expired before verification). Moreover, vehicles with OBU of 400 MHz need nearly 39 ms to verify a certificate (ECDSA 256 bits) and messages (ECDSA 224 bits), as shown in Table 5.2, which is time-consuming and will challenge the real-time decision making.

In VANET, to reduce communication overheads, in [98], the authors suggested that a vehicle only need to attach its certificate when recognizing a new neighbour vehicle. In [101, 147], it is suggested to only attach a certificate on a periodic schedule. Omitting certificates will require a vehicle only to attach the pseudonym in which the communication overheads are significantly reduced (i.e., pseudonym size is 28 bytes while its certificate is 117 bytes). However, omitting a certificate needs more investigation such as testing the average number of packets lost in different traffic scenarios so that the certificate could be dropped, and the consequence messages cannot be verified. Moreover, to reduce computational overheads of certificate verifications in VANET, researchers [99, 101, 147] proposed to store the verified certificates in a local database. Thus, because the same pseudonym can be used to sign a number of messages, the certificate only needs to be verified for the first signed message along with its integrity and the following messages need to verify only their integrity.

5.2 Motivation

Omitting certificate and certificate verification schemes is a promising solution to reduce the security overheads during traffic jams because when the speed of vehicles decreases, it allows vehicles to stay with their neighbour for a longer time. Therefore, the need for verifying the received pseudonyms is decreased as the already verified pseudonyms from old neighbours are omitted. Moreover, the probability of having new neighbours is decreased as vehicles in a congested road move slowly.

However, changing pseudonyms more frequently would reduce the efficiency of such schemes. A vehicle in a traffic jam would change its pseudonym but this change could fail to confuse the attacker because its location has not been changed. Moreover, the

computation and communication overheads would be increased as the certificate for the new pseudonyms needs to be sent and the receiver needs to verify it.

Thus, the main aim of our Hybrid Based Pseudonym Changing Scheme (HBPCS) is to reduce changing pseudonyms during the traffic jams by binding this change to time and distance driven in which the vehicle would use the same pseudonym to sign more messages. To the best of my knowledge, the only hybrid scheme was suggested in [108] in which the pseudonym is changed frequently after being used over 120 seconds or 1 km whichever comes first. However, the frequent change could lead to wasting pseudonyms and only the cooperation between neighbours could achieve successful change and reduce wasting pseudonyms such as in SRPS. Thus, in HBPCS, we apply the hybrid changing on the SRPS, and then we compare HBPCS and SRPS with the state-of-the-art scheme CAPS.

5.3 The complexity of ECDSA

In ECDSA, verification of the signature is the most time-consuming in comparison to the key and signature generation. In VANET safety applications, the generation of the key is not an issue as it is not necessary to be in real-time (i.e., the vehicle has obtained its keys and stored them inside a vehicle during registration before starting sharing messages). Moreover, while the vehicle signs a message, it needs to verify (n) messages (i.e., n is the number of its neighbours inside its communication range) and (n) certificates.

To illustrate more the overheads of each phase, Johnson's ECDSA, which is the first accepted algorithm by the IEEE Security Standards [89], is explained in detail.

The generation of the domain parameters is defined first, and the three phases of key generation, signature generation, and verification are given later.

- **Elliptic curve domain parameters:**

  q: denotes the size of the underlying field F_q which can be a large prime p or a prime to a power (pm).

  $a, b \in F_q$: two field elements which define the equation of the elliptic curve E over F_q

  i.e.:

  $y^2 = x^3 + ax + b$ in the case $p > 3$;

  or

  $y^2 + xy = x^3 + ax^2 + b$ in case of $p = 2^m$

  $G \in E(F_q)$: two field elements x_G and y_G in F_q which define a finite point

  $G = (x_G, y_G)$ of prime order in $E(F_q)$.

  n: the order of point G and it is a prime.

- **Key generation phase:**

  Select a random number $d \in [1, n-1]$ as the private key.

  Compute the corresponding public key $Q = d * G$.

- **Signature generation phase:**

  Input parameters: message m and (d, Q).

  Select a random number $k \in [1, n]$

  Compute $k * G = (x1, y1)$

  Compute $r = x_1 \ mod \ n$, if $r = 0$, then goes to step 1.

  Compute $s = k^{-1}(e + d * r) \ mod \ n$,

  $where \ e = Hash\ (m)$.

  If s=0, then go to step 1.

  Output: the signature on message m is (s, r).

- **Signature verification phase:**

  Input parameters: (m, r, s, and Q).

  Verify $r, s \in [1, n]$

  Compute $w = s^{-1} \ mod \ n$.

  Compute u1 and u2

  $u_1 = e * w \ mod \ n$,

  $u_2 = r * w \ mod \ n$,

  $where \ e = Hash\ (m)$.

Compute $(X_1, Y_1) = u_1 * G + u_2 * Q$

Compute $V = X_1 \, mod \, n$.

Output: the signature is accepted if V=r.

The complexity of each ECDSA phase is detailed below:

- **Key generation phase includes:**

  One scalar multiplication:

  $Q = d * G$

- **Signature generation phase includes:**

  One scalar multiplication:

  $k * G = (x1, y1)$.

  Two modular multiplications:

  $x_1 \, mod \, n$ and $k^{-1}(e + d * r) \, mod \, n$

  One modular inversion:

  $k^{-1} mod \, n$

  One hash operation:

  $e = Hash\,(m)$

- **Signature verification phase includes:**

  Two scalar multiplications:

  $u_1 * G + u_2 * Q$

  Two modular multiplications:

  $e * w \, mod \, n$ and $r * w \, mod \, n$

  One modular inversion:

  $s^{-1} \, mod \, n$

  One hash operation:

  $e = Hash\,(m)$

The most time-consuming operation in ECC is the scalar multiplication [148], which is included twice in the verification process and once in the key and signature generation processes. This would emphasize the need to reduce signature verification overheads.

5.4 Proposed Hybrid-based Pseudonym Changing Scheme

The proposed Safety-related Privacy Scheme (SRPS) can achieve the best balance between privacy and safety but increase the security overheads especially when the number of vehicles increases as shown in Figure 4.7. Thus, we design the Hybrid-based Pseudonym Changing Scheme (HBPCS) in which each pseudonym is used to sign the exchanged messages for a predefined time and distance. Then, before using the new pseudonym, the vehicle has to enter a silent period to avoid long-term linkability via its spatio-temporal information. HBPCS consists of two algorithms, one to be run when the vehicle is active (HBPCS-Active) and the other run when the vehicle is silent (HBPCS-Silent). As we apply HBPCS to SRPS, we can use the same algorithm of SRPS-Silent for HBPCS-Silent and only need to adjust a few steps in SRPS-Active for HBPCS-Active, as given below and illustrated in Algorithm3:

- Algorithm3 takes as input the status of the vehicle, the Received Beacon Messages from its neighbour (RBMs), its current vehicle's state (VS), the Expected Vehicle State (EVS) of the current state from the previous step, the predefined MINimum and MAXimum Pseudonym Lifetime/Distance (MinPL, MaxPL, MinPD, and MaxPD), and the current Pseudonym Lifetime/Distance (PL, PD). Moreover, in this algorithm, Dist ( ) function is required to calculate the distance between the previous and current position to find the total distance driven since started using the current pseudonym.
- A vehicle will continue broadcasting messages with the current valid pseudonym until the PL passed MinPL and PD passed MinPD, as demonstrated in step 2 to 6 in Algorithm3.

- Then, when the MinPL and MinPD are passed, the vehicle starts searching for an opportunity, as shown in Algorithm3 step 7 to 34, to change its pseudonym or its status depending on the following:
  - Changing pseudonym: the EVS from the previous time step (i.e. expected current state) which was predicted by the installed vehicle tracker using Kalman-filter is compared with the actual current VS. The comparison is achieved by calculating the distance between EVS and VS. Accordingly, if the distance is sufficient to confuse the adversary, the vehicle will broadcast its state with a new pseudonym in step 12. That is because the state of the vehicle is different from the state that could be predicted by the adversary.
  - Changing pseudonym: if the above condition has not met, the EVS and the expected neighbour states ERBMs are predicted for the next time step using the vehicle tracker in section 3.8. The EBRMs are calculated for all vehicles (i.e. silent and active neighbours) within the communication range. Then, the distance between EVS and ERBMs is calculated and if the distance between the EVS and any of the ERBMs is small enough (i.e. the state of the vehicle could be mixed with another neighbour in the next time step), then, the vehicle broadcasts its current state and changes its pseudonym for broadcasting the next state, as shown in steps 15 to 25.
  - Change status: if the above two conditions have not met, the vehicle would check if any of its neighbour are being silent to cooperatively enter a silent period, as shown in steps 28 to 33. A silent vehicle can be recognized by the vehicle tracker when two consecutive messages from a neighbour are missed [28]. Moreover, even if the neighbour vehicle enters its silent period, its next states can still be expected by the vehicle tracker for a period of time using the

state maintenance phase (i.e. the period of time meant that vehicle keep predicting its silent neighbours up to the Maximum Silent Period (MaxSP)).

- Otherwise, if the above three conditions have not met, the vehicle will keep broadcasting safety messages using the same pseudonym until the PL has passed MaxPL and PD has passed MaxPD, as shown in steps 35 to 37. Then, when PL and PD has passed MaxPL and MaxPDin step 39, the vehicle will be forced to stop sharing messages to avoid long-term linkability.
- The outputs from this algorithm are the vehicle's status, EVS, RBM, SP, PL, and PD.

Finally, HBPCS is simulated and implemented in the same way as SRPS, given in section 4.4.

Algorithm3: HBPCS-Active

Input (Status, RBMs, VS, EVS, MinPL, MaxPL, MinPD, MaxPD, PL, PD)

1. If (Status = Active)
2. If (**PL** <= **MinPL** and **PD** <= **MinPD**)
3. *Broadcast* (**VS**)
4. **PL** = **PL** + **BR**
5. **PD** = **PD** + Dist ( )
6. *GoTo step 1*
7. Else If (**PL** >= **MinPL** and **PD** >= **MinPD**) and (**PL** <= **MaxPL and PD** <= **MaxPD)**
8. If (**VS**<>**EVS**)
9. *Change Pseudonym* ( )
10. **PL**= **BR**
11. **PD**= 0
12. *Broadcast* (**VS**)
13. *GoTo step 1*
14. Else
15. *Kalman_update* (**ERBMs**, **RBMs**)
16. *Kalman_predict* (**ERBRs**)
17. **nN**=*size of* (**ERBMs**)
18. *Kalman-update* (**EVS**, **VS**)
19. *Kalman-Predict* (**EVS)z**
20. for i=0 to **nN**
21. if (**ERBMs**[i]) ≈ **EVS**)
22. *Broadcast* (**VS**)
23. *Change Pseudonym* ( )
24. **PL**= 0
25. **PD**= 0
26. *GoTo step 1*
27. Else
28. **MTs**= *MissedTracks* (**ERBMs**)
29. **mN**=*size of* (**MTs**)
30. If (**mN** >0)
31. Status=Silent
32. **SP**= 0
33. *Call (HBPCS-Silent)*
34. Else
35. *Broadcast* (**VS**)
36. **PL** = **PL** + **BR**
37. **PD** = **PD** + Dist ()
38. *GoTo step 1*
39. Else If (**PL** >= **MaxPL** and **PD** >= **MaxPD**)
40. Status=Silent
41. **SP** = 0
42. *Call (HBPCS-Silent)*

Output (Status, RBMs, EVS, SP, PL, PD)

5.5 Evaluation

5.5.1 Comparison

To evaluate the performance of HBPCS, it is compared only to SRPS and CAPS [28] as the other schemes were already discussed in the previous chapter and showed their failure to achieve an adequate balance between privacy and safety.

5.5.2 Setting up parameters

The same parameters and metrics in subsections 4.5.2 and 4.5.3 are used. Moreover, HBPCS require extra parameters related to distance (MinPD and MaxPD) which are calculated using the average distance driven per vehicle in sparse traffic, as given in Equation (9). In this equation, the total distance driven for each vehicle is divided by the vehicle lifetime to obtain the average metres driven per second (i.e. m/s).

$$m/s = \frac{1}{nV}\sum_{i=1}^{nV}\frac{Distance}{vL_i} \qquad (9)$$

The result from the above equation was nearly 10m/s. Then, we multiply it by MinPL and MaxPL. We did not use the exact value that we obtain from the above step (i.e., MinPD=600 and MaxPD=1200) instead we decrease them (i.e., MinPD=500 and MaxPD=1000) to enhance the privacy in case the arrival rates increase and distance-driven is probably going to decrease.

5.5.3 Results and Discussion

The performance of HBPCS against SRPS and CAPS is evaluated using quantitative measurements in section 4.5.3. HBPCS are applied to sparse and dense traffic (i.e., v/s and v/0.3s) in which the same generated trips and routing files for schemes in the previous chapter are used.

1. **Security overheads** of the three schemes are compared depending on the average number of changed pseudonyms per second (ChPseud/s) in equation (4), as illustrated in Figure 5.1. From this figure, it is clear that the new scheme, HBPCS, can achieve the lowest security overheads up to 0.59. Overall, it can be seen that the frequency of changing pseudonyms increases along with increasing the density of vehicles in which HBPCS, SRPS, and CAPS from 0.55, 0.62, and 0.61 in sparse traffic to 0.59, 0.73, and 0.65 in dense traffic, respectively. The substantial increase was in SRPS in which ChPseud/s is increased by 0.11, but it is softened by HBPCS in which it is only increased by 0.4 (i.e., overheads nearly decreased to a third).

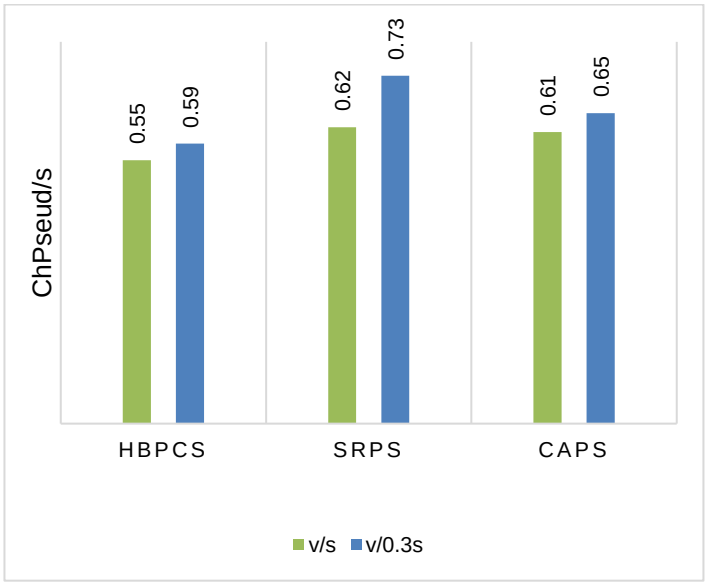

Figure 5.1 Average changed pseudonyms per second

2. **Privacy-preserving level** is compared depending on the average traceability percentage ($Trac_{ch}$%) for vehicles changing their pseudonyms at least once during the simulation which is calculated using equation (5) and illustrated in Figure 5.3. Overall, the privacy level enhances when the number of vehicles increases, and the best scheme that reduces the traceability is SRPS. In terms of the improvement percentages between v/s and v/0.3s, the HBPCS achieve

the highest rate of traceability reduction by 27% (53% to 26%) as opposed to nearly 20% in SRPS and CAPS (40% to 20% and 71% to 52% respectively).

Figure 5.2 Average traceability percentages

3. **Safety level** is demonstrated by calculating the average number of sent beacon messages SBMs rate per second using equation (6), as shown in Figure 5.3. In terms of increasing the density of vehicles, both HBPCS and SRPS increase the number of broadcasted messages while in CAPS it is reduced. Moreover, the SBMs/s in HBPCS and SRPS are significantly increased compared to CAPS (it is up to 9.42 in CAPS as opposite to 9.93 in the other two schemes).

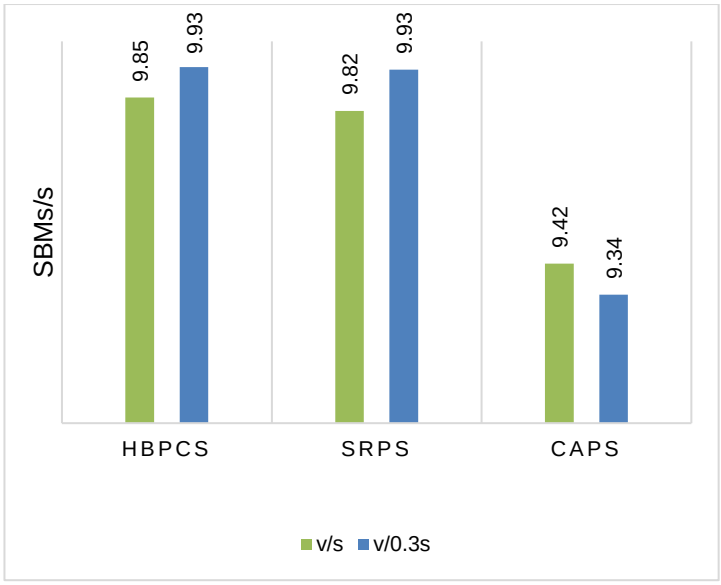

Figure 5.3 Average number of sending beacon messages per second

4. **Efficiency of scheme** can be improved by achieving an acceptable balance between the three keys issues: security overheads, privacy level, and safety that would be satisfied by reducing changing pseudonyms, increasing the confusion level during the change, and reducing the silent periods, as demonstrated at the end of section 4.5.3. Accordingly, we calculate the average of confusion level percentage (conf%) for each scheme using equation (8) and calculate the number of traceable vehicles (nVtrac) despite their pseudonyms being changed using equation (9), as demonstrated in Figure 5.4 and Figure 5.5, respectively. Overall, the increase in vehicles' density results in a higher confusion level for the three schemes (55% to 81% in HBPCS, 69% to 84% in SRPS, and 26% to 41% in CAPS). HBPCS has achieved significant confusion differences between sparse and dense traffic (confusion increased by 26%) opposite to SRPS and CAPS (it is increased by 15%). Moreover, as shown in Figure 5.5, CAPS has the highest number of wasted pseudonyms as it has the lowest confusion level (128 vehicles being traceable instead of changing its pseudonym). The two other schemes are different from CAPS for

the reason that HBPCS has the lowest number of wasted pseudonyms, instead its confusion level is less than SRPS. That is because HBPCS avoids changing pseudonyms more frequently.

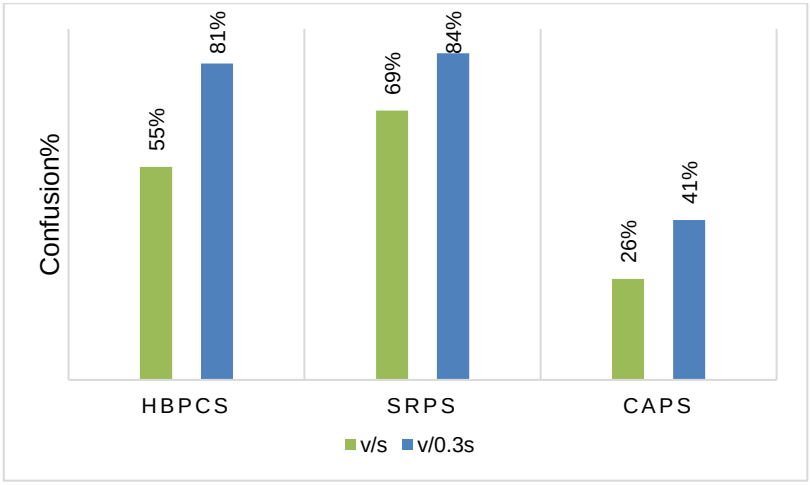

Figure 5.4 The average confusion level percentage

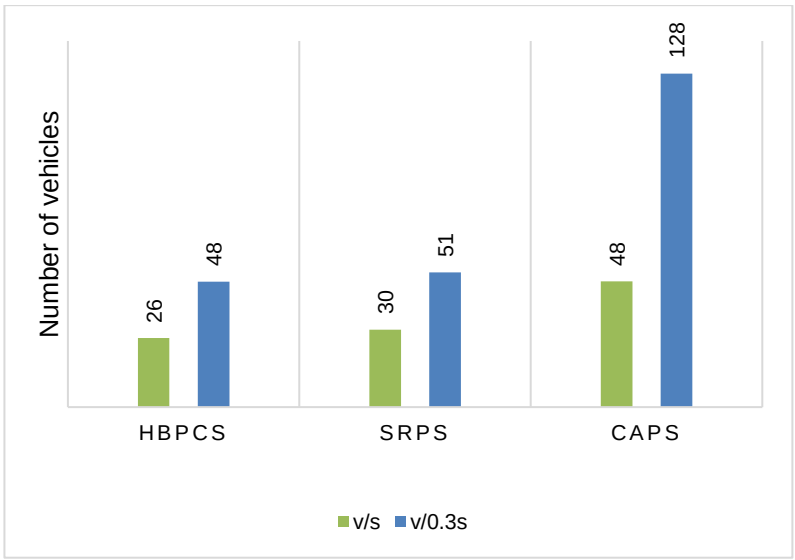

Figure 5.5 Number of vehicles wasted pseudonyms

5.6 Summary

To minimize the security overheads of the proposed scheme (SRPS) in Chapter 4, in this chapter we proposed a Hybrid-based Pseudonym Changing Scheme (HBPCS). In HBPCS, changing pseudonyms is linked to both time and distance driven unlike other cooperative schemes discussed in the previous chapter (CSP, CAPS, and

SRPS) in which changing pseudonyms is only linked to time-driven. Based on the experiment's results that compare the new scheme with the best two pseudonym changing schemes (SRPS and CAPS) as concluded from the previous chapter, HBPCS can reduce the security overheads significantly during traffic jams without compromising privacy. However, HBPCS is not suitable to be applied in sparse traffic as it reduces the security overheads slightly and at the same time, it impacts the privacy level. That is because, it is less likely for a vehicle to find the mix-context with its neighbours and thus once this is met, the vehicle should directly change its pseudonym without taking into its consideration the distance driven as in SRPS. To conclude, the two designed schemes have achieved better balance than others and the combination between them would improve the efficiency (i.e., using SRPS in sparse traffic and HBPCS in dense traffic).

Chapter 6 : Conclusions and Future Work

6.1 Conclusions

This thesis aimed to design a scheme to efficiently address the three key issues: security overheads, privacy, and safety of VANET safety applications based on the investigation of the main requirements of these applications and the impact of the existing schemes. Despite the consensus to use certified pseudonyms to achieve both security and privacy in VANET, the impact of changing these pseudonyms, on safety applications still needs to be studied carefully and addressed efficiently.

In this thesis, two schemes have been proposed: Safety Related Privacy Scheme (SRPS) and Hybrid-based Pseudonym Changing Scheme (HBPCS). The first scheme, SRPS, the aim is to protect privacy without compromising safety by integrating a Multi-Target Tracking (MTT) algorithm to the privacy scheme. The MTT predicts the location of the vehicle itself and its neighbour vehicles to prevent an expected accident in advance. Moreover, the MTT can help neighbour vehicles to investigate if their context in the next time step is likely to be mixed. If so, they will cooperatively change their pseudonyms. In our literature review, researchers suggested that vehicles must have a minimum silent period to protect their privacy, in contrast to SRPS as this period was omitted, to increase the probability of finding mix-context when vehicles synchronized silent periods with other silent neighbour(s). The second scheme, HBPCS, aims to reduce the change of pseudonyms in dense traffic that could minimize both communication and computation overheads. In HBPCS, the overheads were minimized by correlating pseudonym changes to both distance and time driven.

The proposed schemes were implemented using a combination of four simulators that are SUMO, OMNET++, Veins, and PREXT. Then, a quantitative evaluation was achieved via metrics from literature and the newly designed metrics. The traceability percentage and confusion metrics were nominated from previous studies, but the other metrics have been designed upon the requirements of VANET safety applications as illustrated below:

- These applications require messages to be exchanged more frequently so that the average number of exchanged messages per second was calculated.
- Safety messages are life-critical and thus lost messages via communication and computation overheads should be minimized. This could be achieved via reducing pseudonym changes and thus the average number of changing pseudonyms per second was calculated.

The major advantages of SRPS are concluded as follows:

- Enabling silent vehicles to monitor and anticipate its neighbour's next position can reduce the impact of preserving privacy on safety as shown in Figure 4.12 in which up to 93 accidents were expected and can be prevented.
- Enabling vehicles to exit silent periods in case of accident expectation would increase the number of exchanged messages and thus enhance the efficiency of safety applications (i.e., these applications require continuous updating of vehicles' locations).
- Enabling all vehicles (silent and active) to search for the mix-context with other neighbours would increase the efficiency of changing pseudonyms (i.e., confusion level increased when pseudonym changed) as illustrated in Figure 4.13 in which the average confusion level reached up to 84% in dense traffic in comparison to

CAPS in which it is just 41%. This would significantly enhance the privacy because the probability of linking messages via spatio-temporal information is decreased.

- Starting the search for a mix-context directly after synchronizing the silent period between neighbours enhanced the privacy and safety, as shown in figure (4.9 and 4.11) in which the traceability increased from 6% in sparse traffic up to 12% in dense traffic and the exchanged messages increased from 0.20 in sparse traffic up to 0.60 in dense traffic.

Although SRPS has the above advantages, its security overheads increase in dense traffic because the opportunity of finding a mix-context between neighbours is increased. Moreover, the pseudonym lifetime could be passed even before the vehicle changes its location as a result of the traffic jam. Accordingly, we designed the HBPCS in which pseudonym life is coupled to both time and distance-driven. This reduces the pseudonym changes per second by 0.07 in sparse traffic and by 0.14 in dense traffic as shown in Figure 5.1.

What is interesting in HBPCS is that the reduction in the pseudonym changes, as illustrated in Figure 5.2, has a higher impact on privacy in sparse traffic (traceability increased by 13%) but less impact in dense traffic (traceability increased only by 6%). Because a vehicle has less chance to find a mix-context in sparse traffic, it should change its pseudonym once this context is expected without taking into consideration the distance-driven.

A combination of the two schemes (SRPS in rural areas and HBPCS in urban areas) would achieve the best balance between security, privacy, and safety in comparison to other state-of-the-art schemes. The most recent privacy scheme for safety applications is CAPS, which we believe is the most applicable scheme in comparison to other schemes in the literature (excluding SRPS and HBPCS) as it reduces wasting

pseudonyms (security overheads), changes pseudonyms when finding mix-context (privacy level) and reduces silent periods (safety level). However, in comparison to SRPS, as shown in Figure 4.14, the number of a vehicle's wasted pseudonyms is decreased by 18 when v/s, 37 when v/0.5s, and 77 when v/0.3, that is because the confusion level increased by nearly 40% as shown in Figure 4.13. Moreover, the silent period decreased further compared to CAPS especially in dense traffic (illustrated in Figure 4.10)) in which SBMs increased by 0.60 per second. However, the security overheads of SRPS are slightly higher than CAPS by 0.03/s in sparse traffic but increase significantly by 0.08/s in dense traffic. The overheads in sparse traffic is not an issue but the issue arises in dense traffic so that HBPCS was designed to address this issue without affecting the privacy level (as shown in figures (5.1 and 5.2), the ChPseud/s in dense traffic is 0.65 with traceability 52% in CAPS and ChPseud/s is 0.59 with 26% in HBPCS).

In conclusion, our schemes met the VANET safety applications' requirements listed in Chapter 2.4 as below:

- Safety: as shown in Figure 6.1 the exchanged safety messages of both schemes are always at a high rate (i.e., greater than 9 Hz) and even when the vehicle stops sharing messages, it continues to monitor its surrounding vehicles to avoid accidents. Thus, SRPS and HBPCS are the most suitable schemes (that can achieve security and privacy) for VANET safety applications. PPC is the only scheme that exchanged safety messages higher than our schemes, but it has the lowest privacy level as shown in Figure 6.2 (always higher than 83%).
- Privacy: the traceability ratio of both schemes is between 20% and 53% which can be decreased over time (the maximum vehicle's trip in our simulation is 360 which is probably higher in real life). The only two schemes that have achieved a lower

traceability ratio than our schemes are SLOW and CSP. However, these two schemes would impact safety as in SLOW nearly 4m/s are missed as shown in Figure 6.1, and in CSP the silent period is synchronized between all vehicles that could increase the probability of accidents (i.e., VANET is turned off).

- Security overheads: security overheads are not an issue in sparse traffic, but they increase the number of lost messages in dense traffic (due to the increase in the communication and computation overheads as new pseudonyms need to be sent along with the messages and verified by the receiver) that would impact safety. HBPCS and CSP achieved the lowest security level as shown in Figure 6.3 (PseudCh/s is 0.59) but as it is discussed in the previous point, CSP is not suitable for safety applications. Thus, HBPCS can achieve the best security overheads for VANET safety applications. However, we nominated SRPS for sparse traffic because its security overheads are higher than the security overheads of HBPCS (which is not an issue in sparse traffic) but the traceability percentage is increased (40% in SRPS and 53% in HBPCS).
- Distributed and non-cooperative scheme: safety messages are exchanged directly between vehicles and there is no need for infrastructure in real-time or cooperation with other entities to authenticate messages (depend on public-key cryptography where verification is affordable for a vehicle with a processor of 400 MHz and our schemes decreased the verification overhead in dense traffic that would challenge the processor of 400 MHz).
- Real-time constraints: as HBPCS decreases changing pseudonyms in dense traffic, it would increase the number of verified messages in real-time (the number of the new certificates that require to be verified is decreased thus increasing the chance of verifying more messages).

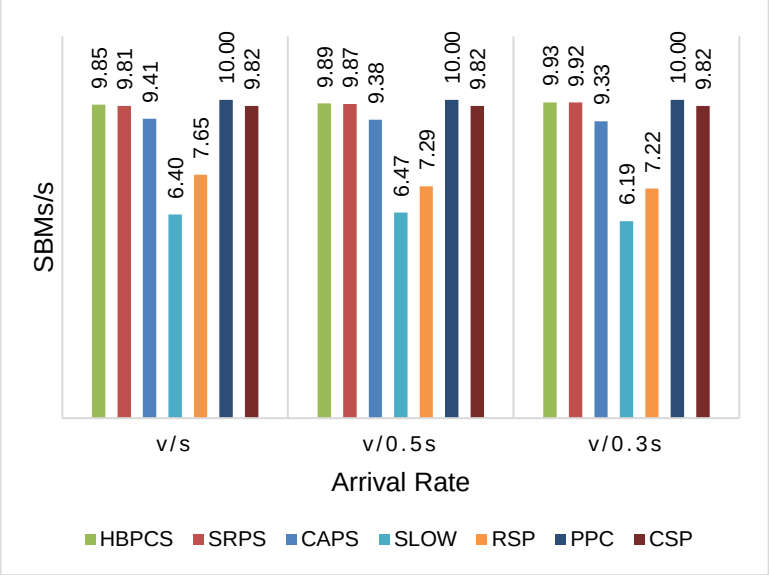

Figure 6.1 Average number of sending beacon messages per second

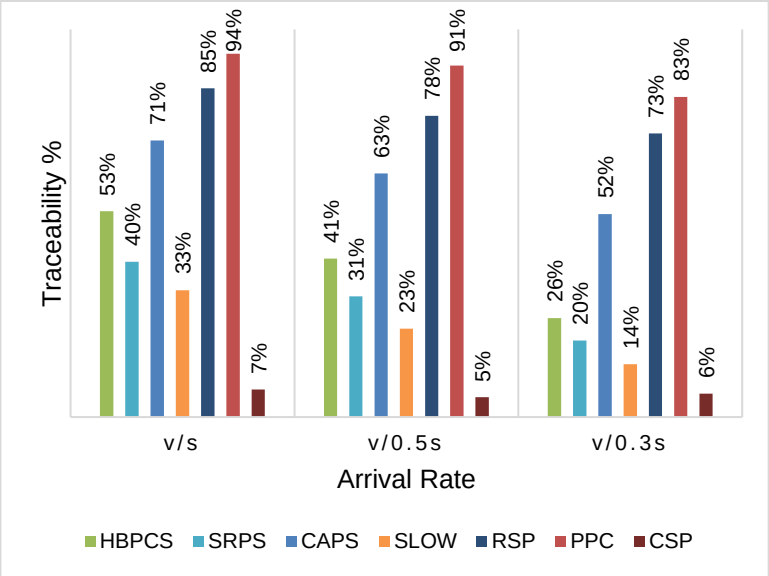

Figure 6.2 Average traceability percentage

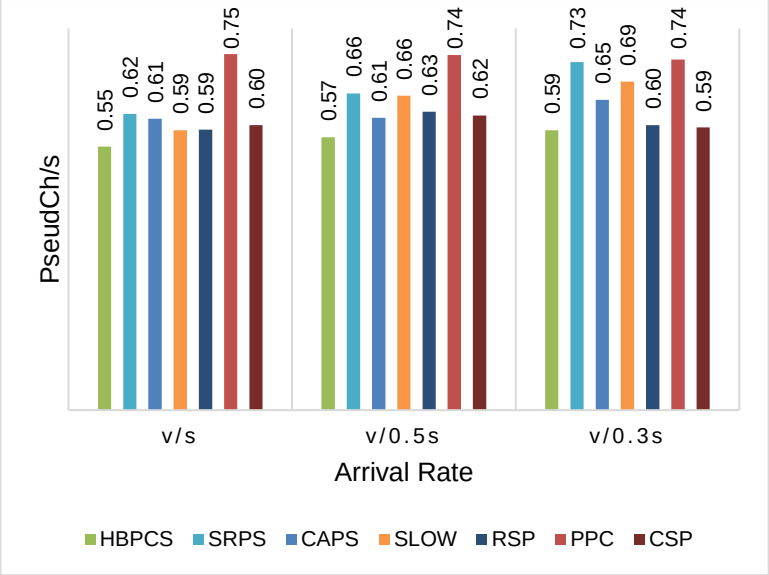

Figure 6.3 Average changed pseudonyms per second

6.2 Future Works

The results of the designed schemes can provide a good starting point for future work to improve the efficiency of the designed schemes further. Accordingly, future research should investigate the following points:

- Consider different traffic scenarios (urban, rural, or highway) as we only depend on the dense traffic on the same road map.
- Measure the success of achieving the privacy level after changing pseudonyms and then the vehicle can decide to reduce the frequent silent period.
- Apply the newly designed schemes on specific safety applications such as a change lane warning application to measure the impact on safety as we only depend on achieving the requirements of these applications.
- Measure the privacy level against a global adversary, which is very strong, is impractical in real-world scenarios except for the service provider. Thus, the schemes should be examined against the local adversary and adjust the

pseudonym lifetime to reduce the overheads (i.e., a longer lifetime would reduce storage, computation, and communication overheads).

- Lost messages via routing to already expired pseudonym would be reduced when pseudonym changes reduced. Thus, the efficiency of the designed schemes on routing should be compared with other schemes in the literature.
- Implement security scheme (ECDSA) and integrate it to the existing schemes (DBPCS, SRPS, CAPS, etc.). Then, when pseudonyms are received for the first time, vehicle will verify and store the authenticated pseudonyms in a table. Thus, when vehicle receives these pseudonyms in the future, it will not verify them again. Moreover, vehicle will only send the certificate for the current pseudonym if it is new or there is a new neighbour. Thus, lost messages via computation and communication overheads can be calculated and compared between the schemes.

References

[1] M. N. Smith, "The number of cars worldwide is set to double by 2040," in "World Economic Forum, Geneva," 2016, Available: https://www.weforum.org/agenda/2016/04/the-number-of-cars-worldwide-is-set-to-double-by-2040, Accessed on: 11/22/2019.

[2] W. H. O. (WHO), "Road traffic injuries," United Nations4 th, 2018, Available: https://www.who.int/news-room/fact-sheets/detail/road-traffic-injuries, Accessed on: 13/2/2019.

[3] A. Vaibhav, D. Shukla, S. Das, S. Sahana, and P. Johri, "Security challenges, authentication, application and trust models for vehicular ad hoc network-a survey," *International Journal of Wireless and Microwave Technologies (IJWMT)*, vol. 7, no. 3, pp. 36-48, 2017.

[4] D. SAE, "J2735 dedicated short range communications (dsrc) message set dictionary," *Society of Automotive Engineers, DSRC Committee*, 2009.

[5] Z. H. Mir and F. Filali, "LTE and IEEE 802.11 p for vehicular networking: a performance evaluation," *EURASIP Journal on Wireless Communications and Networking*, vol. 2014, no. 1, p. 89, 2014.

[6] J. Guo and N. Balon, "Vehicular ad hoc networks and dedicated short-range communication," *University of Michigan*, 2006.

[7] A. K. K. Aboobaker, "Performance analysis of authentication protocols in vehicular ad hoc networks (VANET)," *Master of Science Thesis, Department of Mathematics, University of London, September*, vol. 2, 2010.

[8] (2016, 02/02/2020). *What are your main concerns about IoT adoption?* . Available: https://www.statista.com/statistics/690190/iot-adoption-hurdles-and-obstacles/

[9] T. ETSI, "Intelligent transport systems (ITS); vehicular communications; basic set of applications; definitions," Tech. Rep. ETSI TR 102 6382009.

[10] F. Ahmed-Zaid *et al.*, "Vehicle Safety Communications–Applications (VSC-A) Final Report: Appendix Volume 3 Security," 2011.

[11] F. Schaub, Z. Ma, and F. Kargl, "Privacy requirements in vehicular communication systems," in *Computational Science and Engineering, 2009. CSE'09. International Conference on*, 2009, vol. 3, pp. 139-145: IEEE.

[12] V. S. Yadav, S. Misra, and M. Afaque, "Security in vehicular ad hoc networks," *Security of Self-Organizing Networks: MANET, WSN, WMN, VANET*, vol. 227, 2010.

[13] F. Kargl and J. Petit, "Security and privacy in vehicular networks," in *Vehicular Communications and Networks*: Elsevier, 2015, pp. 171-190.

[14] L. Buttyán, T. Holczer, A. Weimerskirch, and W. Whyte, "Slow: A practical pseudonym changing scheme for location privacy in vanets," in *Vehicular Networking Conference (VNC), 2009 IEEE*, 2009, pp. 1-8: IEEE.

[15] J. Freudiger, M. Raya, M. Félegyházi, P. Papadimitratos, and J.-P. Hubaux, "Mix-zones for location privacy in vehicular networks," in *ACM Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS)*, 2007, no. LCA-CONF-2007-016.

[16] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki, "CARAVAN: Providing location privacy for VANET," Washington Univ Seattle Dept Of Electrical Engineering2005.

[17] B. Palanisamy and L. Liu, "Mobimix: Protecting location privacy with mix-zones over road networks," in *Data Engineering (ICDE), 2011 IEEE 27th International Conference on*, 2011, pp. 494-505: IEEE.

[18] X. Liu and X. Li, "Privacy preservation using multiple mix zones," in *Location Privacy Protection in Mobile Networks*: Springer, 2013, pp. 5-30.
[19] X. Liu, H. Zhao, M. Pan, H. Yue, X. Li, and Y. Fang, "Traffic-aware multiple mix zone placement for protecting location privacy," in *2012 Proceedings IEEE INFOCOM*, 2012, pp. 972-980: IEEE.
[20] 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 Transactions on Vehicular Technology*, vol. 61, no. 1, pp. 86-96, 2012.
[21] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen, "Anonymity analysis on social spot based pseudonym changing for location privacy in VANETs," in *2011 IEEE International Conference on Communications (ICC)*, 2011, pp. 1-5: IEEE.
[22] A. Boualouache, S.-M. Senouci, and S. Moussaoui, "Vlpz: The vehicular location privacy zone," *Procedia Computer Science*, vol. 83, pp. 369-376, 2016.
[23] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, "AMOEBA: Robust location privacy scheme for VANET," *IEEE Journal on Selected Areas in communications*, vol. 25, no. 8, 2007.
[24] M. Gerlach and F. Guttler, "Privacy in VANETs using changing pseudonyms-ideal and real," in *Vehicular Technology Conference, 2007. VTC2007-Spring. IEEE 65th*, 2007, pp. 2521-2525: IEEE.
[25] J. Liao and J. Li, "Effectively changing pseudonyms for privacy protection in vanets," in *Pervasive Systems, Algorithms, and Networks (ISPAN), 2009 10th International Symposium on*, 2009, pp. 648-652: IEEE.
[26] Y. Pan and J. Li, "Cooperative pseudonym change scheme based on the number of neighbors in VANETs," *Journal of Network and Computer Applications*, vol. 36, no. 6, pp. 1599-1609, 2013.
[27] Y. Pan, Y. Shi, and J. Li, "A novel and practical pseudonym change scheme in VANETs," in *International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, 2017, pp. 413-422: Springer.
[28] K. Emara, W. Woerndl, and J. Schlichter, "CAPS: Context-aware privacy scheme for VANET safety applications," in *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, 2015, p. 21: ACM.
[29] C. Sommer, R. German, and F. Dressler, "Bidirectionally Coupled Network and Road Traffic Simulation for Improved IVC Analysis," *IEEE Transactions on Mobile Computing*, vol. 10, no. 1, pp. 3-15, 2011.
[30] K. Kowalenko, "Keeping cars from crashing," *IEEE The Institute*, vol. 9, no. 1, 2010.
[31] J.-P. Hubaux, S. Capkun, and J. Luo, "The security and privacy of smart vehicles," *IEEE Security & Privacy*, vol. 2, no. 3, pp. 49-55, 2004.
[32] W. Yang, "Security in vehicular ad hoc networks (vanets)," in *Wireless network security*: Springer, 2013, pp. 95-128.
[33] T. Wang and X. Tang, "A more efficient conditional private preservation scheme in Vehicular Ad Hoc Networks," *Applied Sciences*, vol. 8, no. 12, p. 2546, 2018.
[34] R. Brignolo, G. Vivo, V. Visintainer, F. Belarbi, and M. Dozza, "Use cases, functional specifications and safety margin applications for the SAFESPOT project," *SAFESPOT deliverable SF_D8*, vol. 4, 2008.
[35] G. Karagiannis *et al.*, "Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions," *IEEE communications surveys & tutorials*, vol. 13, no. 4, pp. 584-616, 2011.
[36] R. Sengupta, S. Rezaei, S. E. Shladover, D. Cody, S. Dickey, and H. Krishnan, "Cooperative collision warning systems: Concept definition and experimental

implementation," *Journal of Intelligent Transportation Systems,* vol. 11, no. 3, pp. 143-155, 2007.
[37] J. A. Misener, R. Sengupta, and H. Krishnan, "Cooperative collision warning: Enabling crash avoidance with wireless technology," in *12th World Congress on ITS*, 2005, vol. 3.
[38] E. C. Eze, S. Zhang, and E. Liu, "Vehicular ad hoc networks (VANETs): Current state, challenges, potentials and way forward," in *2014 20th International Conference on Automation and Computing*, 2014, pp. 176-181: IEEE.
[39] A. Studer, M. Luk, and A. Perrig, "Efficient mechanisms to provide convoy member and vehicle sequence authentication in VANETs," in *2007 Third International Conference on Security and Privacy in Communications Networks and the Workshops-SecureComm 2007*, 2007, pp. 422-432: IEEE.
[40] M. Khodaei and P. Papadimitratos, "Evaluating on-demand pseudonym acquisition policies in vehicular communication systems," in *Proceedings of the First International Workshop on Internet of Vehicles and Vehicles of Internet*, 2016, pp. 7-12: ACM.
[41] A. Studer, E. Shi, F. Bai, and A. Perrig, "TACKing together efficient authentication, revocation, and privacy in VANETs," in *Sensor, Mesh and Ad Hoc Communications and Networks, 2009. SECON'09. 6th Annual IEEE Communications Society Conference on*, 2009, pp. 1-9: IEEE.
[42] T. Leinmüller *et al.*, "Sevecom-secure vehicle communication," in *IST Mobile and Wireless Communication Summit*, 2006, no. POST_TALK.
[43] M. Gruteser and B. Hoh, "On the anonymity of periodic location samples," in *International Conference on Security in Pervasive Computing*, 2005, pp. 179-192: Springer.
[44] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of computer security,* vol. 15, no. 1, pp. 39-68, 2007.
[45] K. Amirtahmasebi and S. R. Jalalinia, "Vehicular Networks–Security, Vulnerabilities and Countermeasures," 2010.
[46] A. Aijaz *et al.*, "Attacks on inter vehicle communication systems-an analysis," *Proc. WIT,* pp. 189-194, 2006.
[47] M. Raya and J.-P. Hubaux, "The security of vehicular ad hoc networks," presented at the Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks, Alexandria, VA, USA, 2005.
[48] K. Zaidi and M. Rajarajan, "Vehicular Internet: Security & privacy challenges and opportunities," *Future Internet,* vol. 7, no. 3, pp. 257-275, 2015.
[49] X. Lin and X. Li, "Achieving efficient cooperative message authentication in vehicular ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 7, pp. 3339-3348, 2013.
[50] Y. Hao, Y. Cheng, C. Zhou, and W. Song, "A distributed key management framework with cooperative message authentication in VANETs," *IEEE Journal on selected areas in communications,* vol. 29, no. 3, pp. 616-629, 2011.
[51] X. Zhu, S. Jiang, L. Wang, and H. Li, "Efficient privacy-preserving authentication for vehicular ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 2, pp. 907-919, 2014.
[52] C. Zhang, X. Lin, R. Lu, and P.-H. Ho, "RAISE: An efficient RSU-aided message authentication scheme in vehicular communication networks," in *Communications, 2008. ICC'08. IEEE International Conference on*, 2008, pp. 1451-1457: IEEE.
[53] Y. Jiang, M. Shi, X. Shen, and C. Lin, "BAT: A robust signature scheme for vehicular networks using binary authentication tree," *IEEE Transactions on Wireless Communications,* vol. 8, no. 4, pp. 1974-1983, 2009.

[54] J. Shao, X. Lin, R. Lu, and C. Zuo, "A threshold anonymous authentication protocol for VANETs," *IEEE Transactions on vehicular technology*, vol. 65, no. 3, pp. 1711-1720, 2016.
[55] W. Yang, "Security in Vehicular Ad Hoc Networks (VANETs)," in *Wireless Network Security: Theories and Applications*, L. Chen, J. Ji, and Z. Zhang, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 95-128.
[56] A.-S. K. Pathan, Security of self-organizing networks: MANET, WSN, WMN, VANET. CRC press, 2016.
[57] F. Cunha *et al.*, "Data communication in VANETs: Protocols, applications and challenges," *Ad Hoc Networks*, vol. 44, pp. 90-103, 2016.
[58] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "VANet security challenges and solutions: A survey," *Vehicular Communications*, vol. 7, pp. 7-20, 2017.
[59] M. Gerlach, "Assessing and improving privacy in VANETs," *ESCAR, Embedded Security in Cars*, 2006.
[60] (DraftReport —April 13, 2012). Security system design for cooperative vehicle-to-vehicle crash avoidance applications using 5.9 GHz Dedicated Short Range Communications (DSRC) wireless communications. Available: https://docplayer.net/11118742-Www-its-dot-gov-index-htm-draft-report-april-13-2012-publication-number.html
[61] L. Fischer, A. Aijaz, C. Eckert, and D. Vogt, "Secure revocable anonymous authenticated inter-vehicle communication (SRAAC)," in *4th Conference on Embedded Security in Cars (ESCAR 2006), Berlin, Germany*, 2006: Citeseer.
[62] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym schemes in vehicular networks: A survey," *IEEE communications surveys & tutorials*, vol. 17, no. 1, pp. 228-255, 2015.
[63] K. A. A. E.-S. Emara, "Safety-aware location privacy in vehicular ad-hoc networks," Technische Universität München, 2016.
[64] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Workshop on the theory and application of cryptographic techniques*, 1984, pp. 47-53: Springer.
[65] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: A secure and privacy-preserving protocol for vehicular communications," *IEEE Transactions on vehicular technology*, vol. 56, no. 6, pp. 3442-3456, 2007.
[66] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*, 2008, pp. 246-250: IEEE.
[67] D. Chaum and E. Van Heyst, "Group signatures," in *Workshop on the Theory and Application of of Cryptographic Techniques*, 1991, pp. 257-265: Springer.
[68] X. Chen, G. Lenzini, S. Mauw, and J. Pang, "A group signature based electronic toll pricing system," in *Availability, Reliability and Security (ARES), 2012 Seventh International Conference on*, 2012, pp. 85-93: IEEE.
[69] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "The TESLA broadcast authentication protocol," *Rsa Cryptobytes*, vol. 5, 2005.
[70] H.-C. Hsiao *et al.*, "Flooding-resilient broadcast authentication for vanets," in *Proceedings of the 17th annual international conference on Mobile computing and networking*, 2011, pp. 193-204: ACM.
[71] K. Grover and A. Lim, "Performance Comparison between Broadcast Authentication Methods for Vehicular Networks," presented at the Proceedings of the 4th International Conference on Information and Network Security, Kuala Lumpur, Malaysia, 2016.
[72] K. Grover and A. Lim, "A survey of broadcast authentication schemes for wireless networks," *Ad Hoc Networks*, vol. 24, pp. 288-316, 2015.

[73] J. Camenisch, S. Hohenberger, and M. O. Pedersen, "Batch verification of short signatures," in *Eurocrypt*, 2007, vol. 4515, pp. 246-263: Springer.
[74] Y. Wang, H. Zhong, Y. Xu, and J. Cui, "ECPB: Efficient Conditional Privacy-Preserving Authentication Scheme Supporting Batch Verification for VANETs," *IJ Network Security,* vol. 18, no. 2, pp. 374-382, 2016.
[75] Y. Liu, Z. He, S. Zhao, and L. Wang, "An efficient anonymous authentication protocol using batch operations for VANETs," *Multimedia Tools and Applications,* vol. 75, no. 24, pp. 17689-17709, 2016.
[76] A. Wasef and X. Shen, "Efficient group signature scheme supporting batch verification for securing vehicular networks," in *Communications (ICC), 2010 IEEE International Conference on*, 2010, pp. 1-5: IEEE.
[77] J. H. Cheon and J. H. Yi, "Fast batch verification of multiple signatures," in *International Workshop on Public Key Cryptography*, 2007, pp. 442-457: Springer.
[78] C. Zhang, P.-H. Ho, and J. Tapolcai, "On batch verification with group testing for vehicular communications," *Wireless Networks,* vol. 17, no. 8, p. 1851, 2011.
[79] Z. Jianhong, X. Min, and L. Liying, "On the security of a secure batch verification with group testing for VANET," *International Journal of Network Security,* vol. 16, no. 5, pp. 351-358, 2014.
[80] M. Bayat, M. Barmshoory, M. Rahimi, and M. R. Aref, "A secure authentication scheme for VANETs with batch verification," *Wireless networks,* vol. 21, no. 5, pp. 1733-1743, 2015.
[81] L. Malina, J. Castellà-Roca, A. Vives-Guasch, and J. Hajny, "Short-term linkable group signatures with categorized batch verification," in *International Symposium on Foundations and Practice of Security*, 2012, pp. 244-260: Springer.
[82] C.-C. Lee and Y.-M. Lai, "Toward a secure batch verification with group testing for VANET," *Wireless networks,* vol. 19, no. 6, pp. 1441-1449, 2013.
[83] L. Chen, Z. Cheng, and N. P. Smart, "Identity-based key agreement protocols from pairings," *International Journal of Information Security,* vol. 6, no. 4, pp. 213-241, 2007.
[84] V. S. Miller, "Use of elliptic curves in cryptography," in *Conference on the Theory and Application of Cryptographic Techniques*, 1985, pp. 417-426: Springer.
[85] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of computation,* vol. 48, no. 177, pp. 203-209, 1987.
[86] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM,* vol. 21, no. 2, pp. 120-126, 1978.
[87] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE transactions on information theory,* vol. 31, no. 4, pp. 469-472, 1985.
[88] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE transactions on Information Theory,* vol. 22, no. 6, pp. 644-654, 1976.
[89] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," *International Journal of Information Security,* vol. 1, no. 1, pp. 36-63, 2001.
[90] I. T. S. Committee, "Ieee standard for wireless access in vehicular environments–security services for applications and management messages," *IEEE Std,* pp. 1609.2-2013, 2013.
[91] C. NIST, "The digital signature standard," *Communications of the ACM,* vol. 35, no. 7, pp. 36-40, 1992.
[92] J. Mikulski, Activities of Transport Telematics: 13th International Conference on Transport Systems Telematics, TST 2013, Katowice-Ustron, Poland, October 23--26, 2013. Proceedings. Springer, 2013.
[93] E. Karthikeyan, "Survey of elliptic curve scalar multiplication algorithms," *International Journal of Advanced Networking and Applications,* vol. 4, no. 2, p. 1581, 2012.

[94] J. A. Solinas, "Low-weight binary representations for pairs of integers," 2001.
[95] G. Nabil, K. Naziha, F. Lamia, and K. Lotfi, "Hardware implementation of elliptic curve digital signature algorithm (ECDSA) on Koblitz curves," in *Communication Systems, Networks & Digital Signal Processing (CSNDSP), 2012 8th International Symposium on*, 2012, pp. 1-6: IEEE.
[96] M. Knežević, V. Nikov, and P. Rombouts, "Low-Latency ECDSA Signature Verification—A Road Toward Safer Traffic," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 24, no. 11, pp. 3257-3267, 2016.
[97] X. Zhu, S. Jiang, L. Wang, H. Li, W. Zhang, and Z. Li, "Privacy-preserving authentication based on group signature for VANETs," in *Globecom Workshops (GC Wkshps), 2013 IEEE*, 2013, pp. 4609-4614: IEEE.
[98] E. Schoch and F. Kargl, "On the efficiency of secure beaconing in vanets," in *Proceedings of the third ACM conference on Wireless network security*, 2010, pp. 111-116: ACM.
[99] F. Kargl, E. Schoch, B. Wiedersheim, and T. Leinmüller, "Secure and efficient beaconing for vehicular networks," in *Proceedings of the fifth ACM international workshop on VehiculAr Inter-NETworking*, 2008, pp. 82-83: ACM.
[100] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "On the performance of secure vehicular communication systems," *IEEE transactions on dependable and secure computing*, vol. 8, no. 6, pp. 898-912, 2011.
[101] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficient and robust pseudonymous authentication in VANET," in *Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks*, 2007, pp. 19-28: ACM.
[102] M. Feiri, J. Petit, and F. Kargl, "Congestion-based certificate omission in VANETs," in *Proceedings of the ninth ACM international workshop on Vehicular inter-networking, systems, and applications*, 2012, pp. 135-138: ACM.
[103] M. Feiri, J. Petit, and F. Kargl, "Evaluation of congestion-based certificate omission in vanets," in *Vehicular Networking Conference (VNC), 2012 IEEE*, 2012, pp. 101-108: IEEE.
[104] M. Feiri, J. Petit, R. K. Schmidt, and F. Kargl, "The impact of security on cooperative awareness in VANET," in *Vehicular Networking Conference (VNC), 2013 IEEE*, 2013, pp. 127-134: IEEE.
[105] A. Pfitzmann and M. Hansen, "A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management," 2010.
[106] K. Zaidi, Y. Rahulamathavan, and M. Rajarajan, "Diva-digital identity in vanets: A multi-authority framework for vanets," in *2013 19th IEEE International Conference on Networks (ICON)*, 2013, pp. 1-6: IEEE.
[107] T. ETSI, "102 941-v1. 1.1 (2012-06)-Intelligent Transport Systems; Security; Trust and Privacy Management," ed.
[108] D. Committee, "Dedicated short range communications (DSRC) message set dictionary," *Soc. Automotive Eng., Warrendale, PA, USA, Tech. Rep. J2735_200911*, 2009.
[109] B. Wiedersheim, Z. Ma, F. Kargl, and P. Papadimitratos, "Privacy in inter-vehicular networks: Why simple pseudonym change is not enough," in *Wireless On-demand Network Systems and Services (WONS), 2010 Seventh International Conference on*, 2010, pp. 176-183: IEEE.
[110] J. Petit, D. Broekhuis, M. Feiri, and F. Kargl, "Connected vehicles: Surveillance threat and mitigation," *Black Hat Europe*, vol. 11, p. 2015, 2015.
[111] K. Emara, W. Woerndl, and J. Schlichter, "Vehicle tracking using vehicular network beacons," in *2013 IEEE 14th International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM)*, 2013, pp. 1-6: IEEE.

[112] D. Eckhoff, R. German, C. Sommer, F. Dressler, and T. Gansen, "Slotswap: Strong and affordable location privacy in intelligent transportation systems," *IEEE Communications Magazine*, vol. 49, no. 11, pp. 126-133, 2011.
[113] Y. Pan, J. Li, L. Feng, and B. Xu, "An analytical model for random changing pseudonyms scheme in VANETs," in *Network Computing and Information Security (NCIS), 2011 International Conference on*, 2011, vol. 2, pp. 141-145: IEEE.
[114] A. Boualouache, S.-M. Senouci, and S. Moussaoui, "PRIVANET: An efficient pseudonym changing and management framework for vehicular ad-hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, 2019.
[115] L. Buttyán, T. Holczer, and I. Vajda, "On the effectiveness of changing pseudonyms to provide location privacy in VANETs," in *European Workshop on Security in Ad-hoc and Sensor Networks*, 2007, pp. 129-141: Springer.
[116] A. Tomandl, F. Scheuer, and H. Federrath, "Simulation-based evaluation of techniques for privacy protection in VANETs," in *2012 IEEE 8th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, 2012, pp. 165-172: IEEE.
[117] L. Huang, H. Yamane, K. Matsuura, and K. Sezaki, "Towards modeling wireless location privacy," in *International Workshop on Privacy Enhancing Technologies*, 2005, pp. 59-77: Springer.
[118] A. Serjantov and G. Danezis, "Towards an information theoretic metric for anonymity," in *International Workshop on Privacy Enhancing Technologies*, 2002, pp. 41-53: Springer.
[119] C. Diaz, "Anonymity metrics revisited," in *Dagstuhl Seminar Proceedings*, 2006: Schloss Dagstuhl-Leibniz-Zentrum für Informatik.
[120] B. Hoh, M. Gruteser, H. Xiong, and A. Alrabady, "Preserving privacy in gps traces via uncertainty-aware path cloaking," in *Proceedings of the 14th ACM conference on Computer and communications security*, 2007, pp. 161-171.
[121] L. Huang, H. Yamane, K. Matsuura, and K. Sezaki, "Silent cascade: Enhancing location privacy without communication QoS degradation," in *International Conference on Security in Pervasive Computing*, 2006, pp. 165-180: Springer.
[122] B. Hoh *et al.*, "Virtual trip lines for distributed privacy-preserving traffic monitoring," in *Proceedings of the 6th international conference on Mobile systems, applications, and services*, 2008, pp. 15-28.
[123] K. Emara, W. Woerndl, and J. Schlichter, "Beacon-based vehicle tracking in vehicular ad-hoc networks," 2013.
[124] B. Hoh and M. Gruteser, "Protecting location privacy through path confusion," in First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05), 2005, pp. 194-205: IEEE.
[125] R. Shokri, J. Freudiger, M. Jadliwala, and J.-P. Hubaux, "A distortion-based metric for location privacy," in *Proceedings of the 8th ACM workshop on Privacy in the electronic society*, 2009, pp. 21-30.
[126] R. Shokri, G. Theodorakopoulos, J.-Y. Le Boudec, and J.-P. Hubaux, "Quantifying location privacy," in *2011 IEEE symposium on security and privacy*, 2011, pp. 247-262: IEEE.
[127] K. Emara, W. Woerndl, and J. Schlichter, "Context-based pseudonym changing scheme for vehicular adhoc networks," *arXiv preprint arXiv:1607.07656*, 2016.
[128] K. Emara, W. Woerndl, and J. Schlichter, "On evaluation of location privacy preserving schemes for VANET safety applications," *Computer Communications*, vol. 63, pp. 11-23, 2015.

[129] R. E. Kalman, "A new approach to linear filtering and prediction problems," *Journal of basic Engineering*, vol. 82, no. 1, pp. 35-45, 1960.
[130] G. Bishop and G. Welch, "An introduction to the kalman filter," *Proc of SIGGRAPH, Course*, vol. 8, no. 27599-23175, p. 41, 2001.
[131] R. J. Fitzgerald, "Development of practical PDA logic for multitarget tracking by microprocessor," in *1986 American Control Conference*, 1986, pp. 889-898: IEEE.
[132] S. Blackman and R. Popoli, "Design and Analysis of Modern Tracking Systems (Artech House Radar Library)," *Artech house*, 1999.
[133] Y. Bar-Shalom, F. Daum, and J. Huang, "The probabilistic data association filter," *IEEE Control Systems Magazine*, vol. 29, no. 6, pp. 82-100, 2009.
[134] J. B. Kenney, "Dedicated short-range communications (DSRC) standards in the United States," *Proceedings of the IEEE*, vol. 99, no. 7, pp. 1162-1182, 2011.
[135] D. Jiang, V. Taliwal, A. Meier, W. Holfelder, and R. Herrtwich, "Design of 5.9 GHz DSRC-based vehicular safety communication," *IEEE Wireless Communications*, vol. 13, no. 5, 2006.
[136] N. P. S. Andersen and D. K.-O. Proskawetz, "CO-OPERATIVE ROAD TRAFFIC: FORESIGHT, SAFETY, AND COMFORT," ed. Torino, Italy: CAR 2 CAR Communication Consortium, 30 October 2019.
[137] "the research and innovative technology administration," ed. United States.
[138] T. ETSI, "Intelligent Transport Systems (ITS); Security; Trust and Privacy Management," 2018, Available: https://www.etsi.org/deliver/etsi_ts/102900_102999/102941/01.02.01_60/ts_102941v010201p.pdf, Accessed on: 12/6/2019.
[139] T. ETSI, "103 097 v1. 3.1-Intelligent Transport Systems (ITS); Security; Security header and certificate formats," *Technical specification, European Telecommunications Standards Institute*, 2017.
[140] I. S. Association, "IEEE guide for wireless Access in vehicular environments (WAVE) architecture," *IEEE Std*, pp. 1609.0-2013, 2013.
[141] S. S. Manvi and S. Tangade, "A survey on authentication schemes in VANETs for secured communication," *Vehicular Communications*, vol. 9, pp. 19-30, 2017.
[142] GOV.UK. (01/01/2020). *Speed limits* Available: https://www.gov.uk/speed-limits
[143] K. Emara, "PREXT: Privacy Extension for Veins VANET Simulator," presented at the in Vehicular Networking Conference (VNC), 2016.
[144] M. Haklay and P. Weber, "Openstreetmap: User-generated street maps," *Ieee Pervas Comput*, vol. 7, no. 4, pp. 12-18, 2008.
[145] P. A. Lopez *et al.*, "Microscopic Traffic Simulation using SUMO," in *2018 21st International Conference on Intelligent Transportation Systems (ITSC)*, 2018, pp. 2575-2582: IEEE.
[146] M. Brown, D. Hankerson, J. López, and A. Menezes, "Software implementation of the NIST elliptic curves over prime fields," in *Cryptographers' Track at the RSA Conference*, 2001, pp. 250-265: Springer.
[147] P. Papadimitratos, G. Calandriello, J.-P. Hubaux, and A. Lioy, "Impact of vehicular communications security on transportation safety," in *INFOCOM Workshops 2008, IEEE*, 2008, pp. 1-6: IEEE.
[148] H. Rifa-Pous and J. Herrera-Joancomartí, "Computational and energy costs of cryptographic algorithms on handheld devices," *Future internet*, vol. 3, no. 1, pp. 31-48, 2011.