الجمهورية الديمقراطية الشعبية الجزائرية
PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA
وزارة التعليم العالي والبحث العلمي
MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH
جامعة عمار ثليجي بالأغواط
AMAR TELIDJI UNIVERSITY OF LAGHOUAT

كلية العلوم
FACULTY OF SCIENCES
قسم الإعلام الآلي
DEPARTMENT OF COMPUTER SCIENCE

Privacy Preservation in Vehicular Ad Hoc Networks

Thesis submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Computer Science (LMD)

Thesis defended on

Ines Khacheba

Jury Members

Ms. Hadda CHERROUN	Professor	UATL	President
Mr. Mohamed BENMOHAMMED	Professor	U. Constantine 2	Examiner
Mr. Azeddine BILAMI	Professor	U. Batna 2	Examiner
Mr. Mustapha BOUAKKAZ	MCA	UATL	Examiner
Mr. Mohamed Bachir YAGOUBI	Professor	UATL	Supervisor
Mr. Nasreddine LAGRAA	Professor	UATL	Co-Supervisor
Mr. Abderrahmane LAKAS	Professor	UAEU	Invited

Laghouat, June 2019

Dedication

This thesis is dedicated to my mother, my father, my two sisters Hajer and Ihcen, my two little nephews Mohamed Amine and Mohamed Islam, and my three little nieces Hana, Basma and Khadidja Yasmine.

Acknowledgments

Above all, I thank God the Almighty for giving me the courage and patience to do this work.

Having reached the end of the writing of this thesis, I am particularly pleased to express my gratitude and my thanks to all those who, by their encouragement, their support and their advice, helped me in its realization.

I express my gratitude and thanks to the members of the jury for agreeing to judge this work and for devoting some of their valuable time to the examination of this thesis.

I thank Ms. Hadda CHERROUN, Professor at Amar Telidji University of Laghouat, for having accepted the presidency of this jury.

I would like to express my thanks to the examiners, Mr. Mohamed BENMOHAMMED, Professor at Constantine University 2, Mr. Azeddine BILAMI, Professor at the University of Batna 2, Mr. Mustapha BOUAKKAZ, MCA at Amar Telidji University of Laghouat, who have accepted to evaluate this work.

I would like to thank my thesis supervisor, Mr. Mohamed Bachir YAGOUBI, Professor at Amar Telidji University of Laghouat, and my thesis co-supervisor, Mr. Nasreddine LAGRAA, Professor at Amar Telidji University of Laghouat, who welcomed me in the research team of the Laboratory of Computer Science and Mathematics at the University of Laghouat during this project. I thank them for their help, their advice and their availability throughout the duration of this thesis.

I express my gratitude to Mr. Abderrahmane LAKAS, Professor at the United Arab Emirates University for his welcome and for his availability every time I asked for his help. I also thank him for his many encouragements, his relevant advice, and his guidance that came at the most difficult times of the PhD.

I would like to express a special thanks to Mr. Mohamed YOUSFI, Professor at Amar Telidji University of Laghouat for his availability, his many encouragements, and his precious help. I also thank him for his great wisdom and for teaching me to be persevering, to fight relentlessly and to believe constantly that the efforts made are always worthwhile. Thank you again for simply helping me with all that this word means.

My gratitude goes to those who have particularly provided emotional support for this doctoral work: my family.

I thank my mother. She knew how to show empathy, comprehension, patience and love. She knew how to find the right words to help me. This thesis is dedicated to her. Thank you mom for the motivations, the help and the moral support you always gave me. Thank you Dad for the relevant advice and the interesting discussions during this PhD. I would also like to tell him how much I appreciate his great availability and precious help at each solicitation from me. The presence and encouragement of my parents are for me the founding pillars of what I am and what I do. Thank you for always being by my side by your devoted love and your tenderness. Thank you for giving taste and meaning to our family life.

I thank my two adorable sisters Hajer and Ihcen who have always been there and continue to be there to make me happy.

I kindly thank all the people who have contributed and participated from far or near to the realization of this work.

Finally, I hope from the bottom of my heart that all this little world, my world, finds here a word of gratitude and thanks.

Thank you all! You helped build the person I am today.

ملخص

توفر أنظمة النقل الذكية إلى المجال العام رحلات آمنة ومريحة. ينعكس ظهورهم في تحريك الحكومات ومصنعي السيارات والباحثين والعمالقة الرقمية. تعتبر اليوم الاتصالات بين المركبات أهم عنصر في أنظمة النقل الذكية. في الواقع، الاتصالات بين المركبات تعمل على زيادة الامن والسلامة على الطرق وتعزيز راحة السائقين والركاب. تشكل هذه الاتصالات شبكة تُسمى شبكة الفانيت.

تعتمد معظم التطبيقات التي تم تطويرها في مجال الفانيت على التبادل الدوري للرسائل التي تحتوي على معلومات شخصية عن مرسلها مثل موقع السيارة. ومع ذلك، يمكن اعتراض هذه المعلومات وجمعها بواسطة خصم لتحديد المركبات وتعقبها. يسمح هذا الهجوم للخصم برسم مسارات السائقين، وبالتالي معرفة أنشطتهم. ونتيجة لذلك، يؤدي هذا الهجوم إلى تهديدات على خصوصية موقع المستخدم في شبكات المركبات. وبالتالي، فإن أمن هذه البيانات في شبكات المركبات يشكل تحديا للباحثين. في هذا السياق، طريقة تغيير اسم مستعار مقبولة على نطاق واسع كحل لحماية خصوصية المستخدمين في شبكة الفانيت. تم اقتراح بروتوكولات مختلفة تعتمد على الاسم المستعار لحماية الخصوصية في الأدب.

في هذه الاطروحة، نحن مهتمون بالحفاظ على خصوصية المستخدمين في شبكة الفانيت. في الجزء الأول من هذه الأطروحة، نقدم معلومات عن شبكة الفانيت وأمنها وكذلك أنظمة حماية الخصوصية. في الجزء الثاني، نبحث عن كيفية إنشاء أسماء مستعارة، وتقديم بروتوكول إنشاء أسماء مستعارة فعال، من أجل تحقيق التتبع الشرطي، وبالتالي تحقيق متطلبات الحفاظ على الخصوصية الشرطي. أخيرًا، نقدم بروتوكول خصوصية الموقع المستند إلى السياق للحفاظ على خصوصية المستخدمين في شبكة الفانيت. المساهمة الأولى هي استراتيجية تغيير أسماء مستعارة تعتمد على السياق، وتتميز بمنع ضد قابلية ربط الأسماء المستعارة مع مراعاة خصائص الفانيت (تنقلية عالية، كثافة، إلخ). المساهمة الثانية هي إعداد نموذج الخصم، يسمى هجوم الغش الذي يمكن تطبيقه على استراتيجية تغيير الاسم المستعار المقترحة. أخيرا، تم تطوير آلية الكشف عن الغش القائمة على السياق لمواجهة هذا الهجوم.

الكلمات المفتاحية: شبكة الفانيت، الأمن، الخصوصية، إخفاء الهوية، المصادقة، الاسم المستعار.

Résumé

Les Systèmes de Transport Intelligents (STI) fournissent à la sphère publique des trajets sécurisés et confortables. Leur apparition se reflète dans la mobilisation des gouvernements, des constructeurs automobiles, des chercheurs et des géants du numérique. Les communications inter véhiculaires sont aujourd'hui considérées comme l'élément le plus important des STIs. En effet, elles permettent d'accroître la sécurité routière et d'améliorer le confort des conducteurs et des passagers. Ces communications constituent un réseau appelé réseau ad hoc de véhicules (en anglais, Vehicular Ad Hoc Network ou VANET).

La plupart des applications développées dans le domaine des VANETs sont basées sur l'échange périodique de messages beacon qui contiennent des informations personnelles sur leur expéditeur, telles que la localisation du véhicule. Cependant, ces informations peuvent être interceptées et collectées par un adversaire pour identifier et traquer les véhicules. Cette attaque permet à l'adversaire de tracer les chemins des conducteurs et de connaître ainsi leurs activités. En conséquence, cette attaque entraîne des menaces pour la vie privée de l'utilisateur dans les réseaux véhiculaires. Par conséquent, la sécurité de ces données dans les réseaux véhiculaires constitue un défi pour les chercheurs. Dans ce contexte, l'approche du changement de pseudonyme est largement acceptée en tant que solution pour protéger la vie privée des utilisateurs dans les VANETs. Différents protocoles basés sur les pseudonymes pour la protection de la vie privée ont été proposés dans la littérature.

Dans cette thèse, nous nous intéressons à la protection de la vie privée des utilisateurs dans les VANETs. Dans la première partie de cette thèse, nous présentons l'état de l'art des VANETs et leur sécurité ainsi que les protocoles de protection de la vie privée. Dans la deuxième partie, nous cherchons comment générer les pseudonymes et nous introduisons un protocole de génération de pseudonymes (en anglais, Pseudonyms Generation Protocol (PGP)) efficace, afin de réaliser le suivi conditionnel et de satisfaire ainsi la condition de la préservation de la vie privée conditionnelle. Enfin, nous présentons un protocole de la vie privée basé sur le contexte (en anglais, Context-based Pseudonym Changing Strategy (CLPS)) pour la préservation de la vie privée des utilisateurs dans les VANETs. La première contribution de CLPS est une stratégie de changement de pseudonyme basée sur la contexte (en anglais, Context-based Pseudonym Changing Strategy (CPCS)) basée sur le contexte, qui se caractérise par une prévention contre la liaison des pseudonymes en tenant compte des caractéristiques du VANET (forte mobilité, densité, etc.). La deuxième contribution de CLPS

est l'élaboration d'un modèle d'adversaire, appelé attaque de tricherie, qui peut être appliqué contre la stratégie de changement de pseudonyme proposée CPCS. Ensuite, un mécanisme de détection de tricherie basé sur le contexte (en anglais, Context-based Cheating Detection Mechanism (CCDM)) est développé afin de faire face à cette attaque.

Mots-Clés : Réseau Ad Hoc Véhiculaire, Sécurité, Vie Privée, Anonymat, Authentification, Pseudonyme.

Abstract

Intelligent Transport Systems (ITSs) provide to the public sphere safe and comfortable journeys. Their advent is reflected in the mobilization of governments, car manufacturers, researchers and digital giants. Inter-vehicular communications are today considered to be the most important element in ITSs. In fact, they permit to increase the road safety and enhance the comfort of drivers and passengers. These communications constitute a network called Vehicular Ad Hoc Network (VANET).

Most of the applications developed in the field of VANETs are based on the periodic exchange of beacon messages that contain personal information about their sender such as the location of the vehicle. However, this information can be intercepted and collected by an adversary to identify and track vehicles. This attack allows the adversary to draw the paths of the drivers, and thus know their activities. As a result, this attack leads to threats on the user's location privacy in vehicular networks. Hence, the security of this data in vehicular networks is a challenge for researchers. In this context, the pseudonym change approach is widely accepted as a solution to protect the privacy of users in VANETs. Different pseudonym-based schemes and protocols for the protection of privacy have been proposed in the literature.

In this thesis, we are interested in preserving the privacy of users in VANETs. In the first part of this thesis, we introduce the state of the art of VANETs and their security as well as privacy protection schemes. In the second part, we look for how to generate pseudonyms, and introduce an effective Pseudonyms Generation Protocol (PGP), in order to support the conditional tracking, and thus to achieve the requirement of conditional privacy preservation. Finally, we present the Context-based Location Privacy Scheme (CLPS) for the preservation of users' privacy in VANETs. The first contribution of CLPS is a Context-based Pseudonym Changing Strategy (CPCS), which is characterized by a prevention against the linkability of pseudonyms while taking into account the characteristics of the VANET (high mobility, density, etc.). The second contribution of CLPS is the elaboration of an adversary model, called cheating attack that can be applied against the proposed pseudonym changing strategy CPCS. Then, a Context-based Cheating Detection Mechanism (CCDM) is developed in order to confront this attack.

Keywords: Vehicular Ad Hoc Network, Security, Privacy, Anonymity, Authentication, Pseudonym.

Table of Contents

List of Tables

List of Figures

List of Abbreviations

4G	4th Generation
5G	5th Generation
AES	Advanced Encryption Standard
AS	Anonymity Set
ASS	Anonymity Set Size
BSM	Basic Safety Message
CA	Certification Authority
CAM	Cooperative Awareness Message
CAPS	Context-Aware Privacy Scheme
CCA	Cooperative Collision Avoidance
CCDM	Context-based Cheating Detection Mechanism
CDM	Cheating Detector Module
CLPS	Context-based Location Privacy Scheme
CM	Context Module
CMIX	Cryptographic MIX-zone
CPCS	Context-based Pseudonym Changing Strategy
CPN	Cooperative Pseudonym change scheme based on the number of Neighbors
CRL	Certificate Revocation List
DMM	Decision Maker Module
DoS	Denial of Service
DOT	Department of Transportation in United States
DSRC	Dedicated Short Range Communication
EEBL	Electronic Emergency Brake Light
ETC	Electronic Toll Collection
ETSI	European Telecommunication Standards Institute
FL	Facilities Layer
FREP	Failure Reply
GPA	Global Passive Adversary
GPS	Global Positioning System
ICW	Intersection Collision Warning

IP	Internet Protocol
ITS	Intelligent Transportation System
IVC	Inter-Vehicle Communication
LBS	Location-Based Service
LDW	Local Danger Warning
MAC	Medium Access Control
MANET	Mobile Ad Hoc Network
MZM	Mix Zone Module
NHTSA	National Highway Traffic Safety Administration
NT	Neighbors Table
OBU	On-Board Unit
OppNet	Opportunistic Network
PCS	Pseudonyms Changing at Social spots
PDA	Personal Digital Assistant
PGP	Pseudonyms Generation Protocol
PKI	Public Key Infrastructure
PREXT	Privacy Extension
RSP	Random Silent Period
RSU	Road-Side Unit
SAE	Society of Automotive Engineers
SPCA	Synchronous Pseudonym Change Algorithm
SREP	Success Reply
SUMO	Simulation of Urban MObility
SV	Subject Vehicle
SVA	Slow Vehicle Alert
TA	Trusted Authority
TNCP	Total Number of Changed Pseudonyms
TPD	Tamper-Proof Device
TTP	Trusted Third Party
V2I	Vehicle-to-Infrastructure
V2R	Vehicle-to-RSU
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Anything

VANET	Vehicular Ad Hoc Network
Veins	Vehicles in Network Simulation
VREQ	Verification Request
Wi-Fi	Wireless Fidelity

1 Introduction

With the advent of wireless technologies such as 4G, 5G, Wi-Fi, or Bluetooth, wireless communications have become ubiquitous and inexpensive. Currently, users access the Internet anywhere and anytime. Researchers began to exploit this technology for multiple purposes. We cite the example of ad hoc networks, one of the wireless technologies where nodes self-organize and collaborate with each other to achieve a large number of applications (e.g., wireless sensor networks, rescue operations).

Governments and automakers have thought about the idea of using ad hoc networks at the scale of the vehicles to minimize and prevent road accidents and traffic fatalities, support self-driving cars, and comfort drivers and passengers [1]. In fact, current vehicles already generate and analyze a large amount of data, but do not broadcast anything. With wireless communications, the vehicle environment and the driver's field of vision are increased. This innovative idea of making vehicles and roads smarter through wireless communications was considered a major priority and was quickly supported by several organizations and research projects. Thus, thanks to connected and cooperative intelligent vehicles that are attentive to their environment, there are many possible applications to be implemented, some of which are intended for safety, and others are intended for the optimization of road traffic, and the comfort of drivers and passengers [2]. In order to deploy these applications, a type of network has emerged: the Vehicular Ad Hoc Network (VANET).

The VANET is a promising vehicular communication system, which enables inter-vehicle communications to increase road safety, and enhance driving experience and comfort. Inter-vehicle communication is characterized by the periodic exchange of messages between vehicles in order to realize the copious applications and services that the VANET must provide. These messages contain personal information directly related to the vehicle such as the location of the vehicle [3]. Thus, a periodic broadcast of this private data allows an adversary, through the eavesdropping; to collect this data and use it for malicious purposes such as the location tracking of the vehicle, and the monitoring of the driver's activities. This type of attack breaches the privacy of users. As a result, the deployment of VANETs will be jeopardized if the users' privacy is not protected. Therefore, the research work done to make VANETs flourish is likely to fall apart.

To protect vehicles' privacy, the VANET should use privacy preservation schemes. However, a malicious vehicle cannot be tracked and identified if a complete privacy preservation scheme is used. Therefore, a conditional privacy preservation scheme should be

employed to secure VANET systems, where a Trusted Authority (TA) has the ability to reveal and revoke a malicious vehicle's real identity. This is known as conditional tracking. Unlinkable pseudonyms schemes can build conditional privacy preservation.

The privacy of users appears as the cornerstone of the security of VANETs. So, the addition of security mechanisms that guarantee privacy becomes indispensable and essential so that VANETs recognize success in the future. Since the users' privacy is highly dependent on the messages exchanged between the vehicles, the content of these messages must be protected against eavesdropping of communications. Thus, researchers have thought of using a pseudonym instead of the real identity of the vehicle. The broadcast of a message with a pseudonym permits to hide the real identity of the message's sender and anonymize its location. However, the use of the same pseudonym by a vehicle allows an adversary to easily trace the path of the driver through the different points he visited and whose locations are associated with the same pseudonym. This method is therefore not practical since it also threatens the privacy of users. To solve this problem, the researchers think that it is necessary to use several pseudonyms (i.e., temporary identities) in order to confuse the adversary. In this approach, a vehicle holds a set of pseudonyms, and selects a single pseudonym to communicate its messages with its environment. After a certain period, the vehicle changes its pseudonym so that the adversary is confused and loses its target. Therefore, the pseudonym change approach is widely accepted by the research community as a solution to protect the privacy of VANETs' users.

In this thesis, we present the concept of VANET and its characteristics, and develop a set of security and privacy-preserving solutions to permit and facilitate the deployment of VANETs in the future.

The objective of our research work is to establish a general framework to secure the VANET against eavesdropping of communications, and thus protect the privacy of its users. Specifically, the main contributions in this thesis lie in the following aspects:

- We propose a Pseudonym Generation Protocol (PGP) [4], which aims to effectively generate the pseudonyms of an individual vehicle, and prevent unauthorized entities to use the pseudonyms in case of theft of the vehicle by storing the pseudonyms in a connection card, and using it inside the vehicle to connect to the VANET system.

- We propose a Context-based Location Privacy Scheme (CLPS) [5] for the protection of privacy in VANETs. CLPS consists in two parts: (1) A Context-based Pseudonym Changing Strategy (CPCS) and (2) A Context-based Cheating Detection Mechanism (CCDM).
- We present a global framework that focus on the privacy preservation in VANETs, and shows the operation of the proposed scheme CLPS for better understanding and clarifying our research contributions. The framework is structured in the form of modules that interact with each other, and with other entities via V2X communications.
- We use the location privacy extension PREXT for Veins VANET simulator to implement the proposed scheme CLPS, and then we compare CLPS with different privacy schemes implemented in PREXT.

The organization of the remainder of the thesis is as follows. Chapter 2 presents the context of VANETs and the security in VANETs. Chapter 3 focuses on the privacy preservation of users in VANETs. We first describe the set of attacks that threaten the users' privacy in VANETs. In particular, we explain the linkability attack that negatively affects the effectiveness of the pseudonym change approach. Then, we define the privacy and give the privacy requirements. Next, we present the principle of the pseudonym change approach and the different stages of the pseudonym lifecycle. Most of this chapter is devoted to the presentation and comparison of the pseudonym change schemes. Finally, we present the privacy metrics used to evaluate the performance of pseudonym change schemes. Chapter 4 addresses the problem of achieving location privacy to secure VANETs. We look for how to generate pseudonyms, and propose an effective Pseudonyms Generation Protocol (PGP) for VANETs, which supports the conditional tracking, and thus permits to achieve the requirement of conditional privacy preservation. Chapter 5 presents the Context-based Location Privacy Scheme (CLPS). We first define the system and privacy models. Next, we present the first contribution of CLPS, which consists of an effective Context-based Pseudonym Changing Strategy (CPCS). Then, we present the second contribution of CLPS where we describe a novel linkability threat, called cheating attack, and we show its negative impact on the performance of the proposed CPCS. In order to confront the cheating attack, we develop a Context-based Cheating Detection Mechanism (CCDM), which assesses whether the pseudonym change was successful or not, and additionally detects the cheating vehicles. Chapter 6 presents an overall framework that summarizes our research contributions on privacy preservation in VANETs. We first start by presenting and describing the framework's

modules. Then, we show the role of each module of the framework. We give an algorithm that determines the functionality provided by each module of the framework at the end of this chapter. Finally, we conclude this thesis by presenting our contributions in summary form, and the perspectives we plan to study in the future in Chapter 7.

2 Vehicular Ad Hoc Networks

2.1. Introduction

The communication between the devices (computer, laptop, PDA, tablet, smartphone, etc.) has been possible since the advent of the wireless technology. This communication forms a wireless network.

The deployment of wireless networks has quickly spread, and given rise to two main categories of these networks. The first category of wireless networks works with the help of an infrastructure (e.g., access point). The nodes in this category can communicate through an access point. On the other hand, in the second category, the nodes can exchange messages without the help of an infrastructure using the multi-hop communication. This type of communication constitutes an ad hoc network.

In general, in an ad hoc network, the nodes are mobile and move randomly. In this case, the network is called Mobile Ad Hoc Network (MANET). The MANET had a great success in offering the possibility of communication in hostile places where the deployment of an infrastructure is almost impossible. Thus, their deployment has generated several types of networks that differ depending on the desired application. The permanent need to increase road safety and to reduce road crashes has motivated governments, car manufacturers, researchers, and the industry consortium to develop a vehicular network that links vehicles together through wireless communication for the purpose of exchanging safety messages, and preventing road hazards [6]. The vehicular network is a particular type of the MANET where the mobile nodes are substituted by vehicles that communicate with each other to constitute a Vehicular Ad Hoc Network (VANET). The VANET is nowadays experiencing rising popularity, and representing a promising technology of the near future whose main objective is to increase the road safety, and enhance the comfort of drivers and passengers.

This chapter aims to define the context of this dissertation by apprehending the notion of VANET and the security of VANET.

2.2. Vehicular Ad Hoc Networks

In this section, we present the VANETs, their characteristics and their architecture. We also see the different applications of VANETs, and the importance of the role that they play in road safety and comfort of drivers and passengers.

2.2.1. Vehicular Ad Hoc Network

Over the last decade, VANET has gained a lot of interest in both research and industry fields. Today, we can see the emergence of many activities in the field of VANETs such as research projects and standards.

Examples of research projects include (but are not limited to): Network on Wheels (NoW) [7], PRESERVE [8], and Car 2 Car Communication (C2CC) Consortium [9].

Also, several standards for vehicular communications exist, including IEEE 802.11p [10], IEEE 1609 working group [11], the work of the ETSI Technical Committee on ITS [12], and the ISO Technical Committee 204 [13].

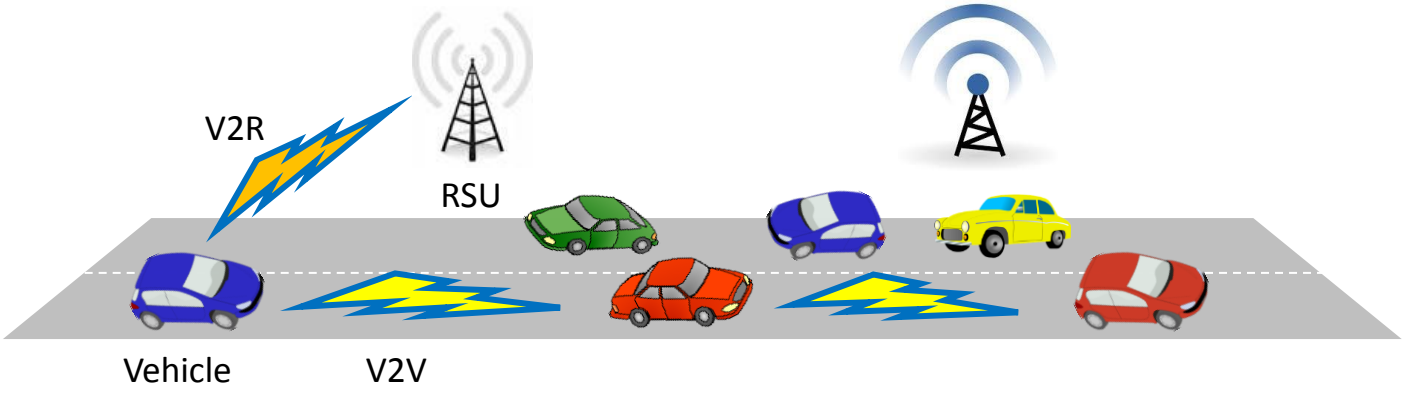

Figure 2.1: Vehicular Ad Hoc Network

A Vehicular Ad Hoc Network (VANET) is a hybrid ad hoc network that consists of smart vehicles moving on the road (i.e., mobile nodes), and Road-Side Units (RSUs) (i.e., static nodes) situated at the roadside, like a traffic light at a road intersection. These nodes are equipped with radio transceivers that allow them to send and receive messages. The vehicles move on the road and communicate with each other through multi-hop Inter-Vehicle Communication (IVC) or Vehicle-to-Vehicle (V2V) communication, and communicate with RSUs through Vehicle-to-Infrastructure (V2I) communication or Vehicle-to-RSU (V2R) communication (globally called V2X) [14]. The V2V communication has the advantage to offer more comprehensive awareness than other detection systems (e.g., radar, camera) [15]. The back-end infrastructure, which is accessible via RSUs, provides a multitude of network services to drivers and passengers, such as Internet access that supports diversified services (e.g., real-time multimedia streaming applications). Fig. 2.1 shows an illustration of a VANET.

Table 2.1 shows a comparison between VANET and MANET.

	VANET	MANET
Topology	Freeway, Manhattan, streets in real world	Random waypoint
Mobility	High	Medium
Architecture	V2V, V2R	Node-to-node
Connectivity	Random and intermittent	Random
Resource	Unlimited	Limited hardware
Scalability	Huge	Medium (50-100 nodes)
Application	Road safety, traffic, comfort	Military, disaster, rescue

Table 2.1: Comparison between VANET and MANET

2.2.2. Characteristics

VANETs are a special case of MANETs [16], [17], where the mobile nodes are instantiated with vehicles. Therefore, VANETs have the same characteristics as MANETs, but they are distinguished from MANETs due to their own unique characteristics that we quote below [18], [19].

1. *High mobility:* The nodes of the vehicle network are characterized by a high mobility especially in motorways. The velocity of vehicles in cities ranges from 0 to 60 km/h, and the average velocity can reach up to 100 km/h on a highway. VANETs are distinguished from MANETs by the high mobility of mobile nodes.
2. *Highly dynamic topology:* The topology of the vehicular network changes frequently and rapidly due to the permanent and high-speed movement of vehicles. Also, the topology usually follows the freeway, Manhattan, and streets in real world.
3. *Variable density:* Some times of the day or places on the road are characterized by a high density of vehicles, such as rush hours, or road intersections in the urban environment where vehicles stop and wait for the green light to turn on to be able to cross the intersection. The vehicle density can have an impact on vehicle communications. For example, a high vehicle density can increase interferences, and thus decrease the throughput, and increase the transmission delay. Contrariwise, if the density of vehicles is low, the connectivity between vehicles could be unavailable or sporadic, which may result in a network disconnection, and may have a negative effect on vehicular communication.
4. *No power constraint:* The batteries of the vehicles are self-charging. So, vehicles in VANETs do not have the conventional power constraints of the mobile nodes in MANETs.

5. *Large scale:* VANETs is the largest instance of MANETs, which is formed by a huge number of vehicles.
6. *Security:* The security of VANETs is very indispensable and the circulating data must be reliable and secure in order to keep the proper functioning of the protocols and applications of VANETs, particularly the applications related to road safety.

2.2.3. Architecture

The VANET is composed of mobile nodes that are vehicles, and static nodes located at the edge of the road called Road-Side Units (RSUs) equipped with radio transceivers. These nodes are organized according to a communication architecture and exchange messages between them via the V2V and V2R communications. In addition, these nodes can meet different environments (urban, suburban, highway) having their own constraints. In this section, we present the communicating entities in a VANET and the types of messages exchanged between these entities.

2.2.3.1. Communicating Entities

The communicating entities in a VANET constitute the nodes and form the topology of the network. There are four communicating entities in a VANET: personal entity, intelligent vehicle, RSU, and central entity.

A. Personal Entity

A personal entity is an entity that can be brought by the user into the vehicle. It can be a mobile phone, a laptop, a Personal Digital Assistant (PDA) or a standalone Global Positioning System (GPS) device. These entities can interact with the vehicle.

B. Intelligent Vehicle

An intelligent vehicle is a vehicle equipped with an On-Board Unit (OBU), which is used to perform V2X communications, and a Global Positioning System (GPS) device to provide the accurate location information of the vehicle. The OBU can record, calculate, locate and send messages over a network interface. A Hardware Security Module (HSM) is used in the intelligent vehicle to assure the storage and non-disclosure of cryptographic credentials, e.g., private keys, and the correct execution of cryptographic operations. The vehicle uses a pseudonym in the V2X communications to sign/verify the exchanged messages. The pseudonym is used instead of the real identity to anonymize the beacon and protect the holder's privacy. The intelligent vehicle maintains a neighbors table or a location table that

contains the states of neighboring vehicles located in its communication range (e.g., 300 m). In general, the neighbors table is updated every time the vehicle receives any packet from some neighbor. The intelligent vehicle is able to expect or detect dangerous situations that can cause serious damages such as collisions and accidents. Fig. 2.2 illustrates an intelligent vehicle and the equipment constituting it. This equipment forms a system named Dedicated Short Range Communication (DSRC).

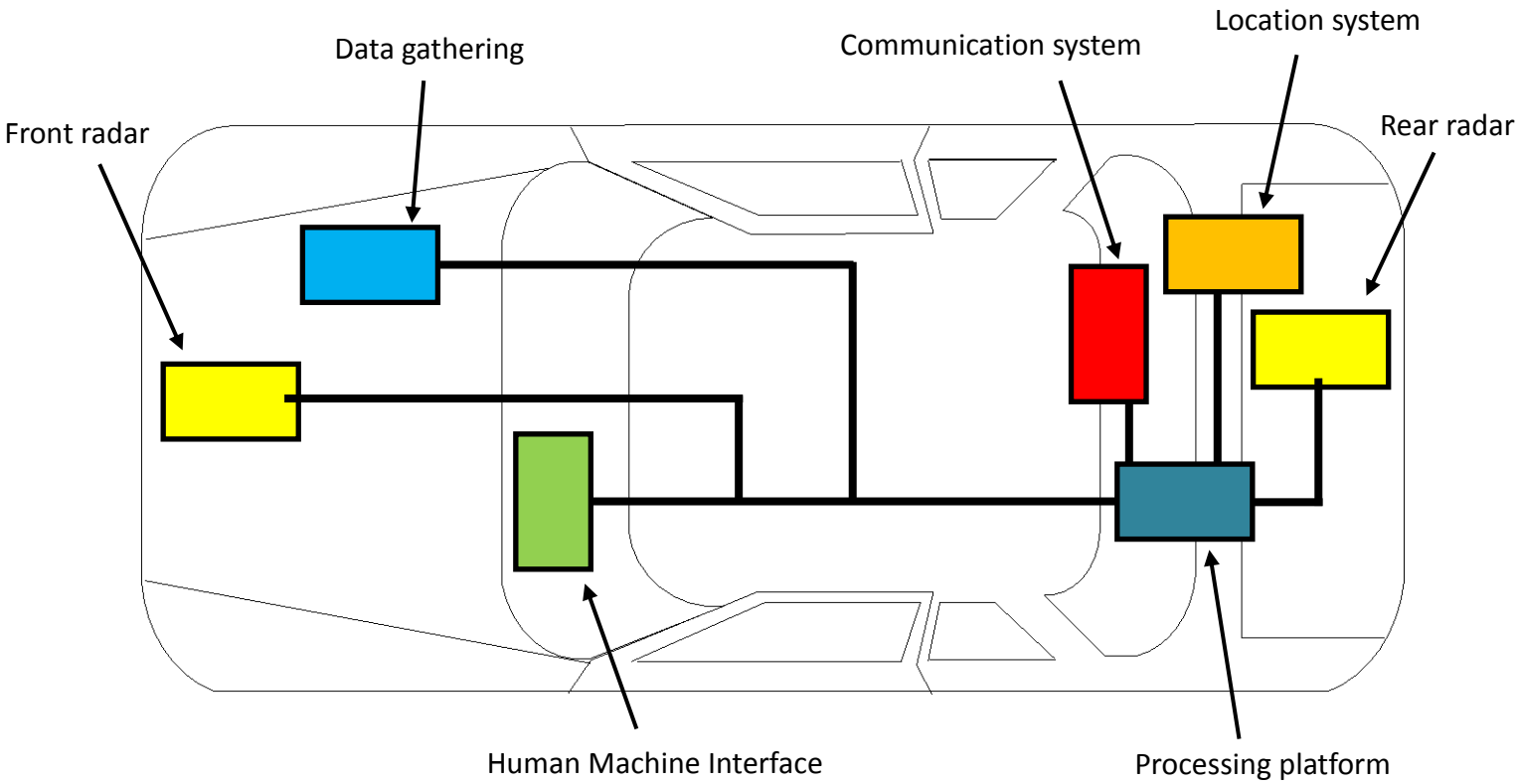

Figure 2.2: Intelligent vehicle [20]

C. Road-Side Unit

A Road-Side Unit (RSU) is an access point located by the side of the road. Its role is to enable passing vehicles to communicate with the back-end infrastructure, including the Trusted Authority (TA) and multiple network services, such as Location-Based Services (LBS), traffic monitoring, and Internet access. Also, the RSUs can provide information to nearby vehicles about traffic, meteorological or road-specific conditions (e.g., maximum speed).

D. Central Entity

A central entity is transparent to the user. It can be a storage server, an entry point to a wired network (e.g., Internet), a transaction server (e.g., Electronic Toll Collection (ETC)), a location-based service provider or a Trusted Authority (TA).

The TA is a fully trustable central entity that is responsible for the initialization of the security system of the VANET, and the issuance and management of the pseudonym credentials for each registered vehicle. The pseudonym credentials consist of a set of pseudonyms, i.e., public keys, and their corresponding private keys and public key certificates. The TA must keep the relation of the pseudonyms to the driver's real identity secret. If a broadcasted message is in dispute, the TA can disclose the real identity of the vehicle that broadcasted the disputed message in order to revoke it. This operation is called conditional tracking.

2.2.3.2. Types of messages

In order to ensure the operation of the protocols and applications of the VANET, the communicating entities (vehicles and RSUs) must exchange messages with each other. In the context of the VANET, we distinguish usually two types of messages exchanged according to the desired application.

A. Beacons

A beacon or hello message is a message sent periodically and unencryptedly by a vehicle to announce its presence to its neighboring environment, and exchange information about local traffic situation with nearby vehicles. The beacon enable a 360-degree awareness of surrounding vehicle states and possible threats. The beacon is called Cooperative Awareness Message (CAM) in Europe [21] and Basic Safety Message (BSM) in US [22], [23], and it is broadcasted with a high frequency ranging from 1 to 10 Hz as proposed by standardization bodies such as IEEE, ETSI, and SAE.

The beacon contains a pseudonym, a timestamp, and the current vehicle state (i.e., position, velocity and direction) [3], [24]. With the beacons received, a vehicle can build its own neighbors table, which includes all the vehicles within its transmission range. The beacon is useful for the operation of several VANET protocols and applications such as geographic routing and location-based services (e.g., point of interest notification).

B. Event-Based Message

An event-based message, also called event-triggered message is a message sent occasionally by a vehicle or a RSU when an event occurs, or is about to occur. The event-based message can be re-broadcast by receiving vehicles with multi-hop communication over a larger area of the road network for a particular purpose (e.g., warning vehicles of accidents). An example of an event-based message is the safety-related message, which is sent when a danger appears on the road (e.g., ice, risk of collision).

2.2.4. Applications

The VANET comes with a very wide range of applications ranging from road safety to comfort of drivers and passengers. A consortium of automobile manufacturers and industrialists (General Motors, Daimler Chrysler, Toyota, Nissan, Volkswagen, Ford, BMW) has established in 2005 a report [25] that lists 75 applications for VANETs. In general, the applications of VANETs are classified into two major categories: (1) safety-related applications and (2) comfort-related applications [14]. Safety-related applications allow vehicles to exchange safety-related information in order to increase vehicle safety on the roads. Comfort-related applications are developed to provide value-added services (e.g., entertainment) [14], [26], [27].

2.2.4.1. Safety-Related Applications

Safety-related applications are the most important kind of applications for VANETs, since they relate directly to the drivers and passengers' lives. They are intended for the improvement of road safety, and reduction of road crashes and hazardous situations (e.g., pothole, obstacle, speeding, construction site). They consist of providing vehicles and roads with capacities that allow to make driving safer. Some examples of important safety-related applications are given below [28], [29].

- Electronic Emergency Brake Light (EEBL).
- Slow Vehicle Alert (SVA).
- Intersection Collision Warning (ICW).
- Pre-Crash Detection System.
- Lane Change Alert.
- Lane Departure Alert System (e.g., trajectory deviation and sway warning).
- Lane Change Assistance.

- Real-Time Traffic.
- Cooperative Collision Avoidance (CCA).
- Dangerous Area Alert.
- Forward Collision Warning.
- Work Zone Warning.
- Road Condition Warning.
- Post-Crash Warning.
- Intersection Management.
- Weather Warning.
- Collision Warning/Avoidance.
- Road Traffic Information.
- Longitudinal Control: See through obstacles to increase the line of sight of the driver.
- Speed control system.
- Remote diagnostics.
- Driving assistance system.
- Local Danger Warning (LDW).
- Road hazard or accident warning.
- Meteorological information.

2.2.4.2. Comfort-Related Applications

The comfort-related applications focus on the comfort, convenience and entertainment of drivers and passengers, and assure them a comfortable and pleasant ride. They make the time spent on the road more enjoyable.

The comfort applications offer a wide range of services provided to the drivers and passengers. Among the applications of comfort, we mainly find the Internet access, which offers a multitude of services (e.g., news, music, video games, social media). Listed below are some examples of comfort-related applications.

- Internet access.
- Infotainment.
- Network games.
- Instant messaging.
- Discussion group in a traffic jam.

- Advertisement.
- Point of interest notification (restaurants, hotels, parking lots, gas stations, rest areas, etc.) according to the driver's choice.
- Point-to-point communications between two drivers traveling together.
- Electronic remote control of the vehicle (verification of the driving license, technical control, license plate) for the competent services (police, customs, gendarmerie) [30].
- Media download.
- Road maps download.
- Electronic Toll Collection (ETC).
- Remote diagnosis.
- Meteorological information.

2.3. Security of Vehicular Ad Hoc Networks

The wireless networks are very vulnerable to attacks and threats from adversaries. In fact, the open nature of the wireless environment exposes the communications to adversaries and offers them an opportunity to launch a multitude of various attacks. Therefore, the security of wireless networks becomes indispensable to ensure their deployment and the reliability of wireless communications.

Like any wireless network, the deployment of VANET is difficult to achieve, because the open nature of its wireless environment makes it very vulnerable to attacks of adversaries that can disrupt vehicular communications, and thus ruin the proper functioning of the VANET. In addition, these malicious attacks represent a serious danger to road safety, and threaten the lives of drivers and passengers. Therefore, it is essential to hamper the malicious attacks by the development of security mechanisms to ensure secure vehicular communications in order to successfully deploy the VANETs. Consequently, the security of VANETs is indispensable and mandatory as their deployment relates to human life-threatening situations.

In this section, we first discuss the security of wireless networks. We present the vulnerabilities of a wireless network, and the different types of attacks and threats that can occur in a wireless network. Next, we provide the security objectives, and then we present the security tools and mechanisms designed for the protection of wireless networks against attacks. In the second part of this section, we decide to present the security of VANETs, and how to deal with malicious attacks. We start by presenting the different attacks and possible

adversary models in VANETs. Then, we give the security objectives. Finally, we present the existing work in the literature on security in VANETs.

2.3.1. Security of Wireless Networks

The globalization of wireless networks is obviously a phenomenon that gives people the opportunity to communicate, work and build a single unit that contributes to the development and evolution of the entire world. However, this globalization also brings its batch of threats and attacks that can disrupt the communications, and ruin the proper operation of wireless networks. These malicious actions must be hampered by the development of security mechanisms to protect wireless communications. In this section, we present the vulnerabilities of wireless networks and the various malicious attacks against these networks, and then we provide the security objectives, and the countermeasures to be respected and implemented in order to avoid or counter these attacks.

2.3.1.1. Vulnerabilities of Wireless Networks

The communications in a wireless environment are exposed to a multitude of attacks. In what follows, we list the vulnerabilities of wireless networks.

- Unencrypted wireless data.
- Easy to eavesdrop.
- Physically insecure locations.
- Lack of network monitoring.
- Insufficient network performance.

2.3.1.2. Attacks and Threats

The wireless network is exposed to a multitude of malicious attacks and threats that can ruin its proper functioning due to the open nature of the wireless environment. In the following, we give a simple definition of an attack, and present the different categories of the existing attacks.

- Attack

  An attack is any action that compromises the security of information in a wireless network.

- Categorization of Attacks

Here, the attacks are categorized according to the objective that an adversary wants to achieve.

A. Information Search

The search for information can be done by eavesdropping in the wireless network (e.g., installation of sniffer, backdoor), or by unauthorized access to servers and routers. Fig. 2.3 shows an example of eavesdropping messages in a public Wi-Fi.

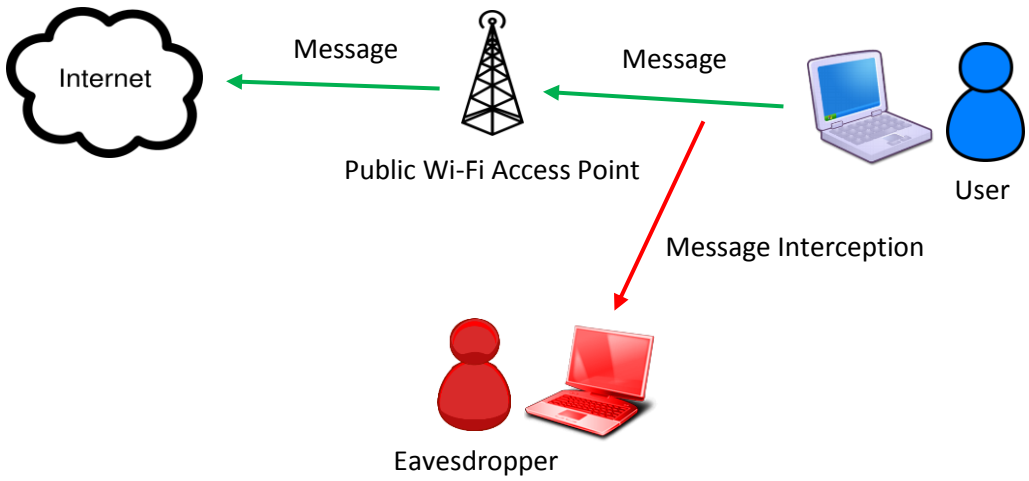

Figure 2.3: Eavesdropping communications in a public Wi-Fi

B. Injection of fake messages

The adversary is able to inject fake messages into the wireless channel to disrupt the proper functioning of the wireless network (*c.f.*, Fig. 2.4).

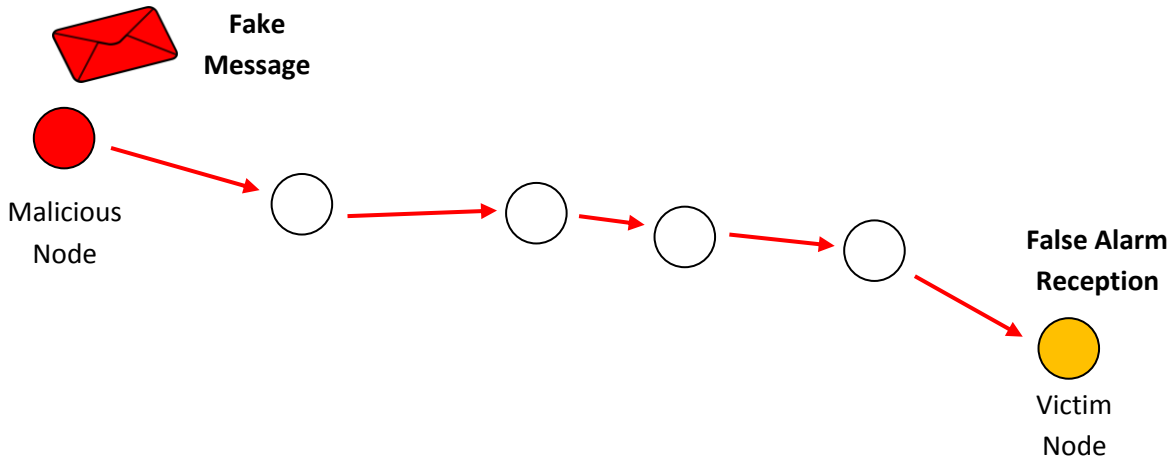

Figure 2.4: Injection of a fake message in an ad hoc network

C. Vulnerability Search

The adversary can search for vulnerabilities on operating systems and application servers to attempt to gain access to launch its attack.

D. Attempt to Exploit Vulnerabilities

When an adversary encounters a vulnerability in a system, he/she can attempt to exploit the vulnerability for malicious purposes. The attempt to exploit vulnerabilities can be done remotely (buffer overflow), and then locally.

E. System Non-Availability

An adversary can compromise the wireless network by launching the denial of service attack (*c.f.*, Fig. 2.5).

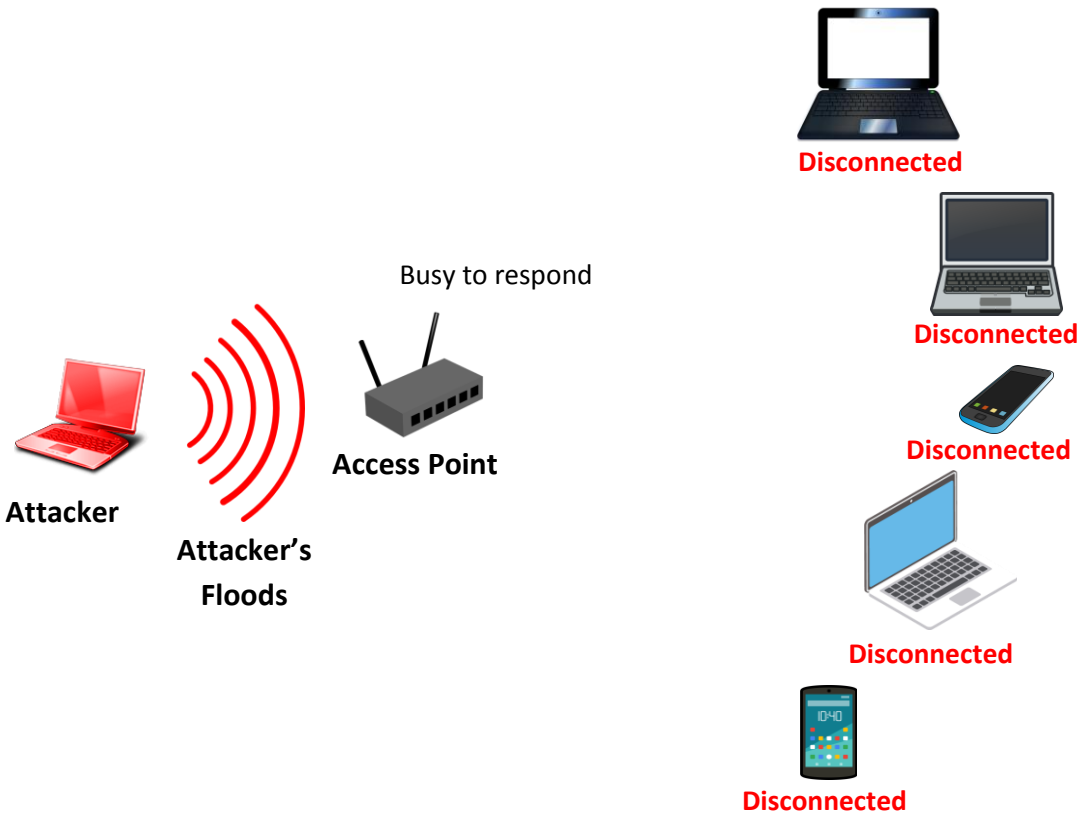

Figure 2.5: Denial of service attack on a wireless network

2.3.1.3. Security Objectives

Given the increasing and continuing number of attacks against the wireless networks, the researchers have thought to secure these networks. In what follows, we enumerate the objectives of security.

- **Privacy**

The privacy concerns the protection of information directly related to the privacy of users.

a. Attacks

- Eavesdropping communications.
- Interception of transmitted data on the wireless channel.
- Unauthorized access to servers and theft of personal data.

b. Countermeasures

- Use of pseudonyms.
- Cryptography (data encryption).

- **Data Confidentiality**

The confidentiality of the data is the process of making the data confidential and allowing access to this data only to authorized persons.

a. Attacks

- Eavesdropping communications.
- Interception of transmitted data on the wireless channel.
- Unauthorized access to servers and theft of personal data.

b. Countermeasures

- Cryptography (data encryption).

- **Data Integrity**

The integrity of the data is the guarantee that the data arriving at destination has not been tampered or modified whether intentionally or unintentionally.

a. Attacks

- Data modification.
- Replay attack.

b. Countermeasures

- Cryptography.

- **Data Availability**

The availability of data is the guarantee that the data is available and accessible at all times.

a. Attacks

- Denial of Service (DoS).
- Channel jamming.

b. Countermeasures

- Identification of the adversary's IP address.

- **Authentication**

The authentication is the process that consists in verifying the identity of the sender of a message. The authentication consists of two phases: the digital signature and the verification.

a. Attacks

- Identity impersonation (spoofing).
- Data fabrication (masquerade).

b. Countermeasures

- Cryptography (digital signature).

- **Non-repudiation**

The non-repudiation is the means that prevents a malicious entity from denying that it has executed a transaction.

a. Attacks

- Identity impersonation (spoofing).
- Purchase on the Internet.

b. Countermeasures

- Cryptography (digital signature).

- **Access Control**

The access control is the permission to access data to authorized persons only.

a. Attacks

- Unauthorized access to servers.
- Theft of passwords.
- Access to users' personal accounts (bank accounts and e-mails).

b. Countermeasures

- Encryption of passwords.
- Sensitization of users.

2.3.1.4. Security Mechanisms and Tools

Different security mechanisms and tools have been developed and used to secure the wireless networks. The cryptography comes with multiple solutions to achieve the different security requirements. This section presents some important security mechanisms based on cryptography for wireless networks.

- Encryption and Decryption of Data

There are two popular encryption schemes that can be used to encrypt and decrypt data in a wireless network.

1. Symmetric Encryption

In the symmetric encryption, a sender encrypts a readable data (plaintext) with a symmetric key (i.e., secret key) to produce an unreadable data (ciphertext), and then sends the obtained ciphertext on the wireless channel to the receiver. The receiver uses the same symmetric key to decrypt the ciphertext and obtain the plaintext, as shown in Fig. 2.6.

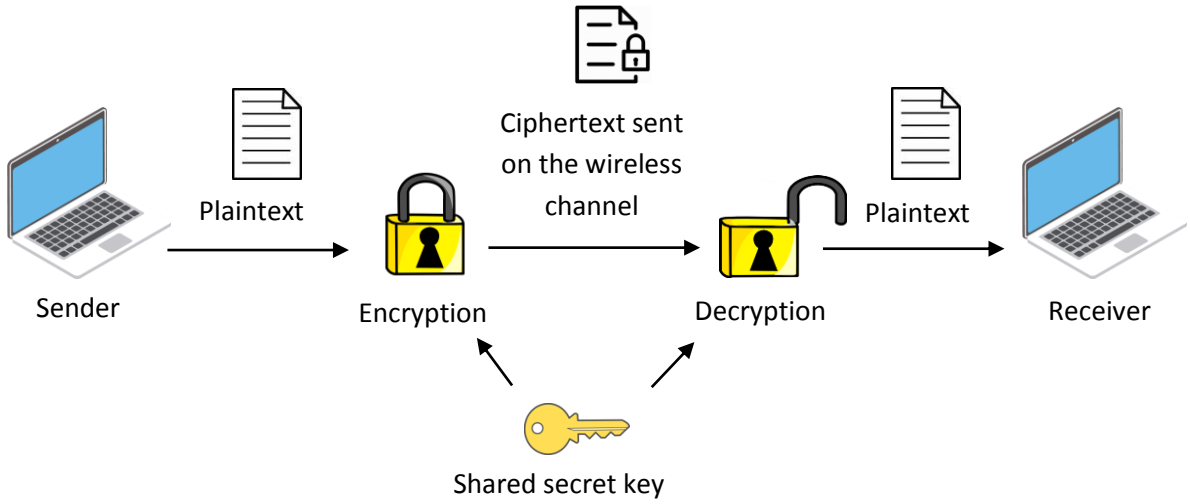

Figure 2.6: Symmetric encryption in a wireless network

2. Asymmetric Encryption

In the asymmetric encryption, a sender encrypts the plaintext with the public key of the receiver to produce the ciphertext, and then sends the obtained ciphertext on the wireless channel to the receiver. The receiver uses its private key (i.e., secret key) to decrypt the ciphertext and obtain the plaintext, as shown in Fig. 2.7.

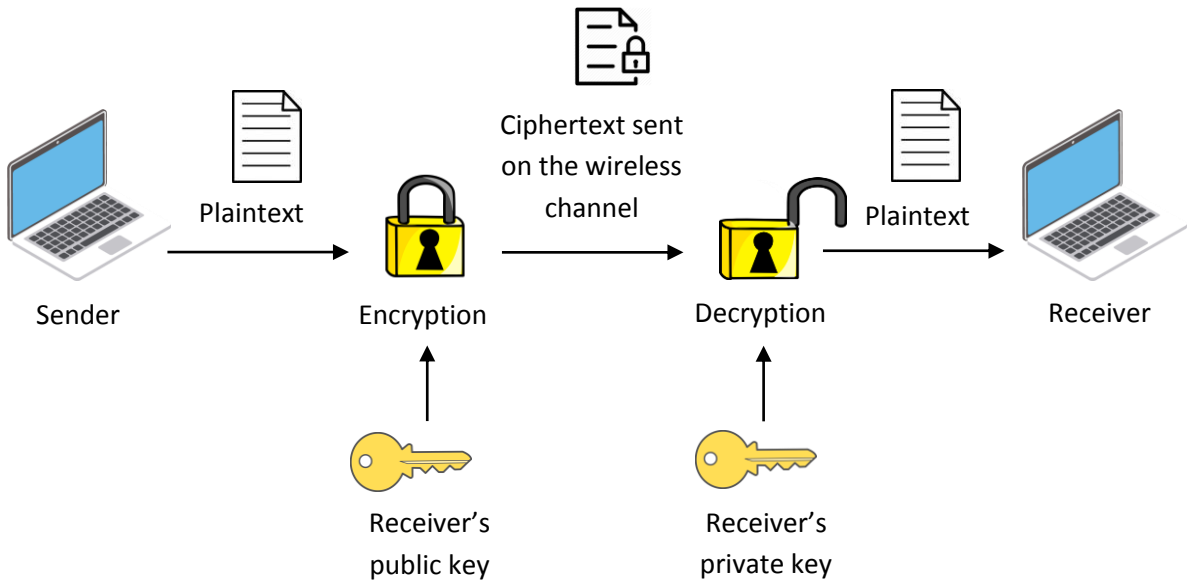

Figure 2.7: Asymmetric encryption in a wireless network

- Digital Signature

The digital signature is a mathematical scheme used for the authenticity of a transmitted message. The digital signature allows the sender to digitally sign a message. Upon receipt of

the signed message, the recipient verifies its validity. The digital signature and the verification constitute the fundamental steps of the authentication. The digital signature uses the hash and asymmetric encryption mechanisms, as shown in Fig. 2.8.

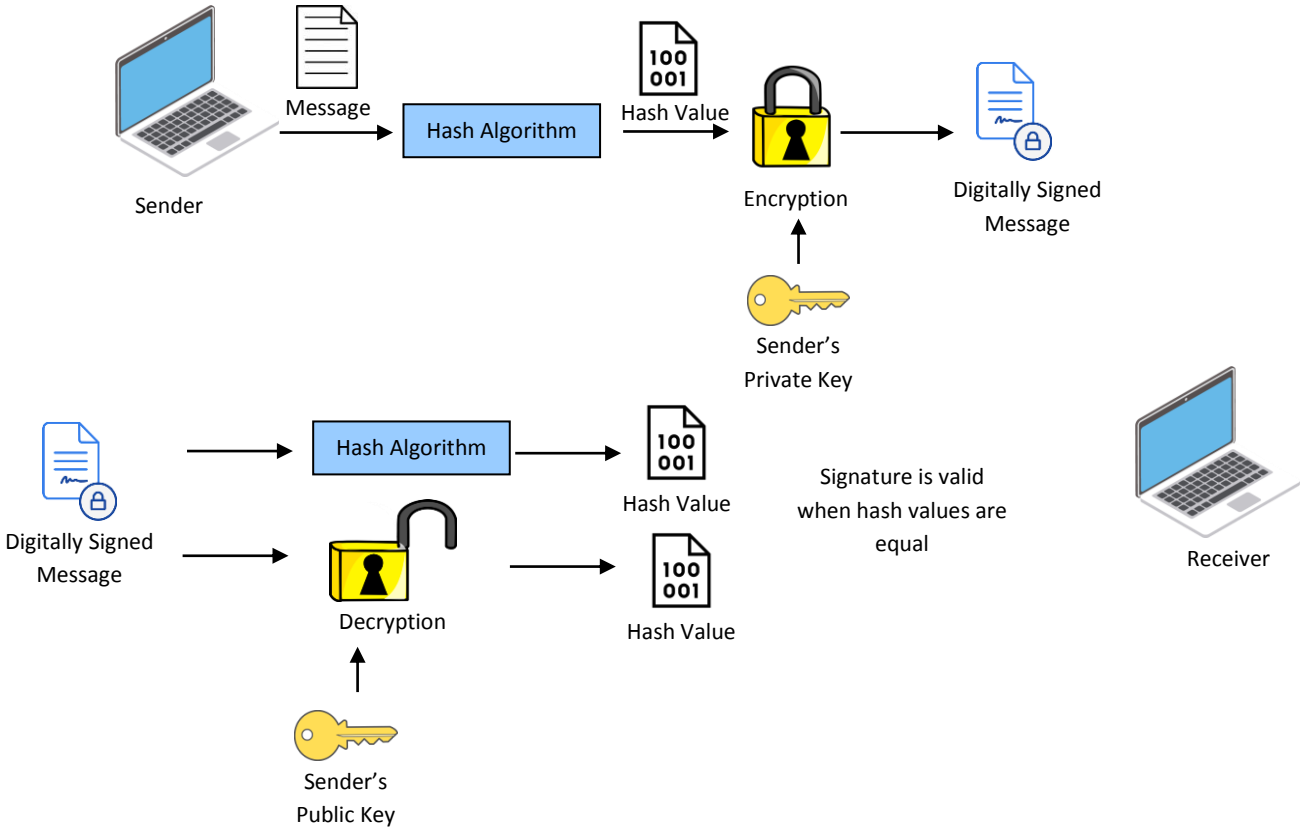

Figure 2.8: Digital signature

- Public Key Infrastructure

A Public Key Infrastructure (PKI) is a set of procedures needed to create, manage, distribute, use, and revoke digital certificates and public/private key pairs. The PKI enables a user to secure exchanged data over the wireless network, confirm the identity of the sender, and validate the received data.

2.3.2. Security of Vehicular Ad Hoc Networks

Like any wireless network, the VANETs need to be secured and protected against the malicious attacks of the adversaries. Indeed, adversaries could send out spoofed or forged information that may result in incorrect warnings to drivers, and cause road accidents. Hence, these attacks can disrupt the vehicular communications, and put the lives of drivers and passengers in danger. Therefore, security schemes for VANETs are of paramount importance to enable normal V2X communications. In this section, we provide the categories of the

different malicious attacks that threaten the VANETs, and the possible adversary models in these networks. Then, we present the security objectives. Finally, we mention the main existing work on security in VANETs.

2.3.2.1. Attacks and Threats

In the same way as wireless networks, the VANETs are vulnerable to attacks of adversaries, and face many security and privacy issues. In general, the attacks in VANETs can be classified into the following categories [31], [32], [33], [34], [35], [36], [37].

1. *Channel jamming:* An adversary deliberately generates a huge number of false messages to jam the wireless channel to prevent other vehicles from normal communications.
2. *Forgery:* The forgery attack could potentially cause the road accidents. Therefore, the correctness of the transmitted messages in the VANET is very important to ensure that the received messages are not forged.
3. *In-transit traffic tampering:* In this attack, an adversary deliberately delays, drops, corrupts, or modifies messages to disrupt the normal communications.
4. *Identity impersonation:* In this attack, an adversary aims to convince others that he/she is a legitimate vehicle for his/her own benefits.
5. *Privacy violation:* An adversary can collect the transmitted messages (e.g., beacons) from overheard vehicular communications, launch inference attacks on the drivers' personal data to identify drivers, and then launch location tracking attack to track the drivers and follow their activities. This set of attacks violates drivers' privacy.
6. *On-board tampering:* Beyond abuse of the communication protocols, an adversary may select to tinker with data (e.g., velocity, location, status of vehicle parts) at their source, tampering with the on-board sensing and other hardware.

2.3.2.2. Adversary Models

To classify the capacities of an adversary, four dimensions are defined in the literature [18], [38].

- *Internal or External:* In a VANET, an adversary can be internal or external. The internal adversary has wireless interfaces that are legitimate members of the network. On the contrary, the external adversary is considered by the members of the network as an intruder.

- *Malicious or Rational:* The malicious adversary has malicious intentions, and aims to disrupt the vehicular communications, while the rational adversary only looks for personal profit.
- *Active or Passive:* The active adversary broadcasts messages to launch his attack, while the passive adversary only listens to the communications on the wireless channel.
- *Local or Global:* The local adversary performs his attack in a limited area. So, only the vehicles in this area can be affected by this attack. The global adversary is able to carry out his attack on the entire VANET.

2.3.2.3. Security Objectives

The security mechanisms in VANETs must achieve the following security objectives [3], [14], [36], [39], [40], [41], [42], [43].

- *Authentication:* The message authentication ensures that a received message is really sent from a legitimate and authorized entity (e.g., vehicle) in the network.
- *Integrity:* The integrity ensures that all messages sent by vehicles have not been modified or deleted, and should be delivered unaltered.
- *Non-repudiation:* The non-repudiation can prevent an adversary from denying the attacks that he/she has launched.
- *Access control:* Any misbehaving entity should be revoked from the VANET to protect the normal communications. Moreover, any actions taken by that misbehaving entity should be canceled.
- *Privacy:* The privacy ensures the protection of private information from an unauthorized party. In VANETs, the real identity of any vehicle should be hidden from other vehicles and RSUs, but should be transparent to a trusted authority (TA). This security requirement is also called "conditional privacy preservation".

2.3.2.4. Related Work on Securing VANETs

The security and privacy issues in VANETs have motivated and encouraged researchers and industrialists to design and develop protocols and mechanisms for security and privacy preservation since 2004. In this section, we present some existing research work on security and privacy preservation in VANETs [18], [20], [34], [38], [44], [45], [46], [47], [48], [49].

The IEEE 1609.2 standard [44] defines the security services for vehicular communications. This standard can be used to protect messages against attacks such as spoofing, eavesdropping

and alteration. Also, with this standard, vehicles can send encrypted messages to each other or to RSUs.

J.-P. Hubaux *et al.* [20], [34] discuss security and privacy issues arising in VANETs. To address the privacy issue, they propose to use temporary pseudonyms instead of the real identity for each vehicle. The concept of changing pseudonyms permits to achieve anonymity and prevents tracking vehicles.

M. Raya *et al.* [17], [38] discuss the security of VANETs. They define the possible adversary models, and provide a set of security and privacy protocols. To achieve authentication and privacy, they propose that each vehicle should be preloaded with a large number of anonymous public and private key pairs with the corresponding public key certificates. For authentication, each outgoing message is digitally signed using a public key based scheme. For privacy, each public and private key pair is used for a short life period.

X. Lin *et al.* [50] propose a group signature based scheme. In this scheme, all vehicles within the same group share the same public key, and each vehicle in the group has its own private key. When a vehicle receives a signed message from a group member, the vehicle verifies it with the group public key. The verifier only knows whether the signer is a legitimate group member or not, but the verifier does not know who the signer exactly is. In this way, the identity privacy is well protected. In case of dispute, a Trusted Authority (TA) working as the group manager is capable to trace the real identity of the sender by using the TA's secret key.

G. Calandriello *et al.* [47] propose a hybrid scheme that uses the traditional PKI based scheme and the group signature based scheme. Similar to the above group signature based scheme of X. Lin *et al.* [50], each vehicle (i.e., group member) holds a distinct private key and a group public key (i.e., the same key for all group members). Unlike the above scheme [50], the private key is not used for signing messages. Instead, a vehicle uses the private key to generate temporary private and public key pairs. Each pair has a public key certificate, which mainly contains a pseudo identity and a lifetime, as well as a signature. The signature in the certificate is signed using the group private key of the vehicle instead of the trust authority TA.

2.4. Summary

In this chapter, we have presented the context of VANETs and the security of VANETs. We have first presented the characteristics of VANETs, and then we have given the architecture of VANETs. In the VANET architecture, we have shown the different communicating entities and the types of messages exchanged between these entities. Next, we have seen the applications offered by VANETs. In the rest of the chapter, we have presented the security of wireless networks, and then we have presented the security of VANETs. In this part, we have shown the malicious attacks of adversaries that represent a serious danger to road safety and threaten the lives of drivers and passengers. Next, we have provided the possible adversary models. Finally, we have presented the security objectives and the research work carried out in the context of securing VANETs at the end of the chapter.

3 Privacy Preservation in Vehicular Ad Hoc Networks

3.1. Introduction

The privacy preservation in VANETs constitute a challenge for researchers. In fact, if the privacy of the users is not protected, they will not participate in the VANET.

Frequent changing pseudonyms are accepted as a solution for the protection of users' privacy in VANETs. The basic idea of this approach is that each vehicle has a large set of pseudonyms. A single pseudonym is used instead of the real identity of the vehicle to send messages, and then changed by a new pseudonym after a certain short period.

In the literature, the researchers have proposed numerous schemes for the realization of the pseudonym change approach [51], [52], [53]. These schemes regroup several pseudonym management mechanisms such as generation of pseudonyms, change of pseudonyms or revocation of pseudonyms.

In the context of VANETs, the messages (e.g., beacons) exchanged between vehicles contain sensitive personal information (e.g., position). Since this information is broadcast publicly [54], a serious privacy threat arises. In fact, an adversary can use this information to link between pseudonyms and reconstruct the vehicles' anonymous trajectories [31], [55], [56]. Then, the adversary launches inference attacks to identify the vehicles and find out the drivers' real identities [57], [58], [59]. The adversary can after track the vehicles remotely and continuously, and follow the activities of the drivers. This malicious attack is called location tracking. The set of attacks (i.e., linkability attack, inference attack, location tracking attack) directly affects the privacy of the VANET users. In the literature, many authors have proposed and designed pseudonym change schemes that aim to effectively change a pseudonym in the right context in order to avoid the linkability attack. In the literature, many authors have proposed and designed pseudonym change schemes that aim to effectively change a pseudonym in the right context in order to avoid the linkability attack.

In this chapter, we first begin by describing attacks on privacy in VANETs. Then, we present the concept of privacy, and we give the privacy requirements. We present after the principle of the pseudonym change approach, and the different stages of the lifecycle of a pseudonym. Then, the largest section of this chapter is devoted to the presentation of an overview on the state-of-art pseudonym change schemes, and a comparative study of the most popular pseudonym change schemes in VANETs. Finally, we provide privacy metrics that are

used to evaluate the performance of pseudonym change schemes, and the effectiveness of the adversary.

3.2. Attacks on Privacy in VANETs

Like any wireless network, VANETs need to be secured and protected against malicious attacks of adversaries. In fact, these attacks can disrupt vehicular communications, and put the lives of drivers and passengers in danger. In this section, we provide the set of attacks that affect the users' privacy in VANETs (*c.f.*, Fig. 3.1).

3.2.1. Location Tracking Attack

In a VANET, if a vehicle broadcasts its messages with its real identity, an adversary can easily eavesdrop and collect these messages, and then use the location information inserted in these messages to track the vehicle's path, and follow the driver's activities. This attack is called location tracking attack.

3.2.2. Inference Attack

To avoid the location tracking attack, a vehicle can use a single pseudonym instead of the real identity to send its messages. In this way, the adversary cannot recognize the driver and track his activities. However, the adversary is able to launch the inference attack on the vehicle's anonymous trace, which is drawn from the different locations associated with the same pseudonym in beacons. In the inference attack, the adversary collects and analyzes the information (e.g., location, timestamp) contained in the vehicle's beacons, and tries to recognize the places visited by the driver (e.g., house, workplace, university, shopping mall, amusement park). These places permit to the adversary to find the driver's real identity [57], [58], [59]. Then, the adversary can launch the location tracking attack and track the driver as mentioned above.

3.2.3. Linkability Attack

To overcome the problem of inference attack, researchers propose the pseudonym change approach, where a vehicle holds a large set of pseudonyms, and selects only one pseudonym to communicate with other entities in the VANET. After a certain short duration, the vehicle changes its pseudonym. This approach has the advantage to hide the real identity of the vehicle, and cause the adversary to lose the target vehicle's trace to avoid being tracked for an extremely long period. However, this solution may become invalid if a vehicle changes its pseudonym in an improper occasion, because an adversary is able to eavesdrop and collect

continuous periodical broadcast beacons from vehicles, and then use the spatiotemporal information contained in beacons to link between pseudonyms, and reconstruct anonymous vehicle traces [31], [55], [56]. Then, the adversary can launch the inference attack on the drivers' personal data (e.g., location) to de-anonymize the reconstructed vehicles' traces, and find out the drivers' real identities [57], [58], [59], and then track their activities.

In [60], M. Wernke *et al.* classify privacy attacks as single position attack, multiple position attack, context linking attack, multiple position and context linking attack, and compromised Trusted Third Party (TTP). The multiple position attack is also known as location tracking attack, in which the adversary uses the various locations of a vehicle to link its pseudonyms, and reconstruct its path [61], [62]. This attack jeopardizes the unlinkability of pseudonyms. The adversary can then run an inference attack or identity revealing attack (called context linking attack in [60]), in which he/she identify the driver from the visited locations (e.g., home, workplace, shopping mall) that constitute the reconstructed anonymized trace.

Therefore, to break the privacy of users, the adversary has two objectives to realize:

1. Launch the linkability attack to link the pseudonyms of the target vehicle and determine its trajectory;
2. Start an inference attack to link the reconstructed trajectory to the identity of the target vehicle to break driver's privacy.

Therefore, due to the linkability attack, simply changing pseudonyms in an improper occasion could be ineffective, since an adversary could link a new pseudonym with the old one [55]. In fact, an adversary has two possibilities for linking pseudonyms:

(i) Individual Pseudonym Change Behavior. If a vehicle individually changes pseudonym without taking into account the surrounding environment, then it can, in certain cases, change its pseudonym alone among its neighbors, which makes it linkable. This behavior helps the adversary to easily link the new pseudonym with the old one, and track the vehicle since no other vehicle changed its pseudonym with it. As a solution, a vehicle should cooperate with a certain number of vehicles nearby to change its pseudonym simultaneously with them to disrupt the adversary.

(ii) Spatiotemporal Information in Beacons. Even if vehicles change their pseudonyms simultaneously, an adversary still has the possibility to link between pseudonyms, and track

vehicle movements using the spatiotemporal information contained in beacon messages [31], [55], [56]. To overcome this problem, a vehicle should dissimulate the content of beacon messages to change the pseudonym.

Therefore, a successful change of pseudonym is only possible if the following two unlinkability requirements are met:

R-1. Pseudonym Changing Simultaneity. A vehicle should cooperate with a certain number of vehicles in its vicinity to change the current pseudonym simultaneously (i.e., in the same time slot) with them.

R-2. Concealment of Messages Information. The purpose of this requirement is to prevent an adversary from obtaining the messages information at the time of the pseudonym change. This requirement can be achieved with three different approaches:

- Using a silence period before a pseudonym change [63].
- Changing pseudonyms in mix-zones where the adversary cannot eavesdrop the exchanged messages, which makes the vehicle trajectory unpredictable [64].
- Encrypting the exchanged messages for changing pseudonym [48].

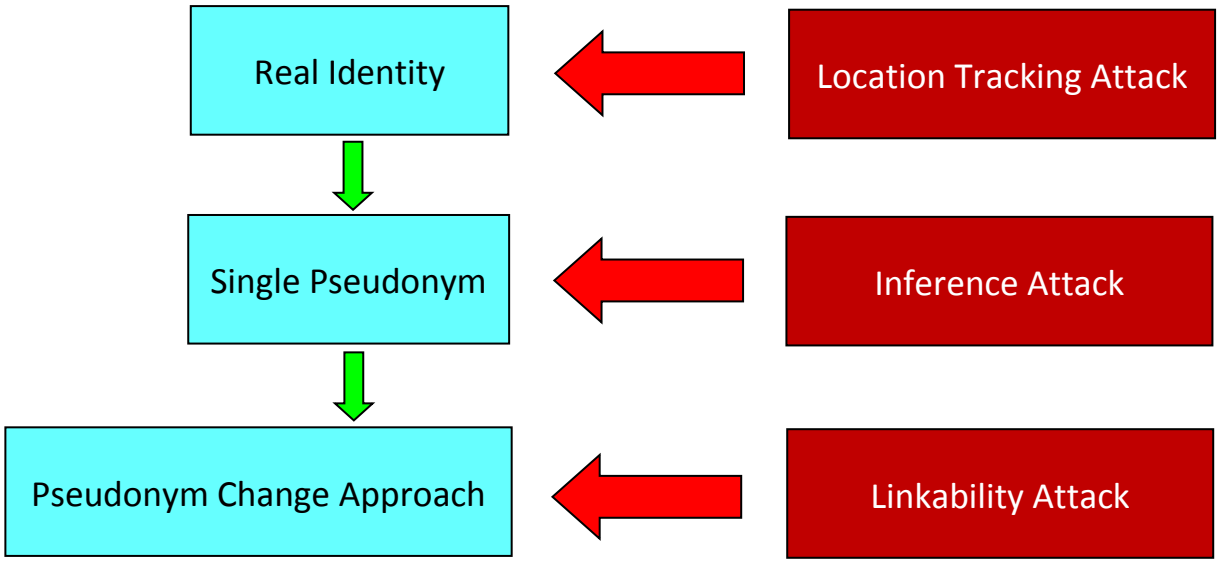

Figure 3.1: Attacks on privacy in VANETs

3.3. Privacy

The privacy of an individual must be respected and protected in any situation. For this reason, many countries recognize privacy as a right and have attempted to codify it in law [64]. For example, en 1890, US Supreme Court Justice Louis Brandeis stated that “the right to be left alone” is one of the fundamental rights of a democracy [65]. Several research projects

consider privacy risks and countermeasures such as the Privacy Flag project [66], which aims to protect citizen privacy when visiting websites, using smartphone applications, or living in a smart city. Furthermore, numerous research works address security and privacy issues in a smart city that deploys VANET [53], [67].

In this section, we give the definition of privacy, and present the privacy requirements.

3.3.1. Definition of Privacy

In this thesis, we give the definition of privacy come from Dr. Standler. He defined privacy as *"the expectation that confidential personal information disclosed in a private place will not be disclosed to third parties, when that disclosure would cause either embarrassment or emotional distress to a person of reasonable sensitivities [68]."*

Another definition of privacy is given by A. F. Westin in [69]. He defined privacy as an individual's right *"to control, edit, manage, and delete information about them[selves] and decide when, how, and to what extent information is communicated to others."*

A. Pfitzmann *et al.* [70] define anonymity as *"the state of being not identifiable within a set of subjects."*

The privacy and anonymity can be provided in VANETs by the use of pseudonyms. Pseudonyms were originally introduced by D. L. Chaum to provide anonymity for electronic transactions [71]. A. Pfitzmann *et al.* [72] define a pseudonym as *"a bit string which [. . .] is unique as identifier (at least with very high probability) and suitable to be used to authenticate the holder's items of interest relatively to his/her digital pseudonym, e.g., to authenticate his/her messages sent."*

According to these definitions, a pseudonym can be used for authentication, but must not contain any personal identifiable information. Thus, a pseudonym is effective in ensuring both the privacy and authentication requirements.

3.3.2. Privacy Requirements

The Global Internet Liberty Campaign [73] has produced an extensive report that discusses personal privacy at length and identifies four broad categories of privacy: information privacy, bodily privacy, privacy of communications, and territorial privacy.

In the context of VANETs, the first category, i.e., the information privacy, concerns three types of information:

- *Data Privacy:* the data privacy prevents others from obtaining communication data.
- *Identity Privacy:* the real identity of each vehicle should be kept secret to any entity except for TA. This privacy requirement is called conditional privacy preservation.
- *Location Privacy:* the exact movement trajectory of any vehicle should not be determined.

This thesis concentrates on how to preserve identity privacy and location privacy. A. R. Beresford *et al.* define the location privacy as the ability to prevent other parties from learning one's current or past location [64].

The attacks on pseudonym changes permit to define the privacy requirements that need to be taken into account by pseudonym change schemes. F. Schaub *et al.* [74] identify the following privacy requirements:

- Minimum disclosure: The amount of information that a vehicle discloses in the V2X communication should be kept to the minimum, i.e., there is no need to disclose more information than required for proper functioning of VANET applications.
- Conditional Anonymity: A malicious vehicle cannot be tracked and identified if a complete privacy scheme is used. Therefore, a conditional privacy scheme must be used to achieve anonymity for vehicles, and guarantee that the real identity of a malicious vehicle can be disclosed for revocation in case of dispute (i.e., pseudonym resolution). The conditional anonymity is then required for the good functionality of the VANET.
- Unlinkability: Unlinkability requires that the pseudonyms of an individual vehicle should not be linked.
- Distributed resolution authority: The pseudonym resolution should be distributed between multiple distinct authorities, because the cooperation of authorities is required to link a pseudonym to a user's identity.
- Perfect forward privacy: Resolution of one pseudonym to a user's identity should not reveal any information that allows to link other pseudonyms of the same user.

3.4. Privacy Preservation Schemes in VANETs

The privacy preservation in VANETs is a very challenging issue for researchers. In fact, if the privacy of users cannot be protected, they will not participate in the VANET. The

protection of privacy is therefore mandatory to allow the acceptance of VANETs by users. The privacy preservation schemes are then indispensable; in fact, they represent a prerequisite for the deployment of the VANET. In this section, we provide the principle of the pseudonym change approach, and then we show the different stages of the pseudonym lifecycle. Finally, we present a taxonomy of the state-of-the-art pseudonym change schemes, and then we present a comparative table that summarizes the characteristics of some important pseudonym change schemes proposed for VANETs. Finally, we detail the privacy metrics used to evaluate pseudonym change schemes.

3.4.1. Pseudonym Approach

The preservation of the users' privacy in VANETs concerns the protection of information that may reveal the real identity of each vehicle in the VANET (e.g., identity, position) in order to avoid the tracking of the vehicle by the adversary. Many authors consider the pseudonym change approach as a solution to preserve the privacy of VANET users [53]. The pseudonyms are a set of certified public keys (anonymous certificates) stored in the vehicle's OBU [3]. The purpose of this approach is to hide the real identity of vehicles, and also to decorrelate the identity of vehicles from their locations [48]. The basic idea of this approach is as follows. Prior to joining the network, each vehicle must detain a set of pseudonyms. Then, a single pseudonym is selected and used instead of the real identity of the vehicle to sign outgoing messages, and then changed to a new pseudonym after a certain short duration (e.g., one minute), so that the vehicle cannot be tracked by an adversary, and thus remains anonymous throughout the communication [75].

We should notice that the adversary can use the addresses of the different layers of the protocol stack (e.g., IP address, MAC address) to link pseudonyms. This open issue was addressed by E. Fonseca *et al.* in [76]. As a solution, they propose a multi-layer addressing scheme with support for pseudonymity enabling user privacy across layers of the protocol stack. Therefore, to protect the vehicle's privacy, the change of pseudonym should be accompanied by the change of all the identifiers of the protocol stack layers such as the MAC and IP addresses [77].

3.4.2. Pseudonym Lifecycle

The pseudonym lifecycle begins with the pseudonym generation process and ends with the pseudonym change or the pseudonym revocation in case a malicious attack is launched. Fig. 3.2 shows the pseudonym lifecycle for VANETs.

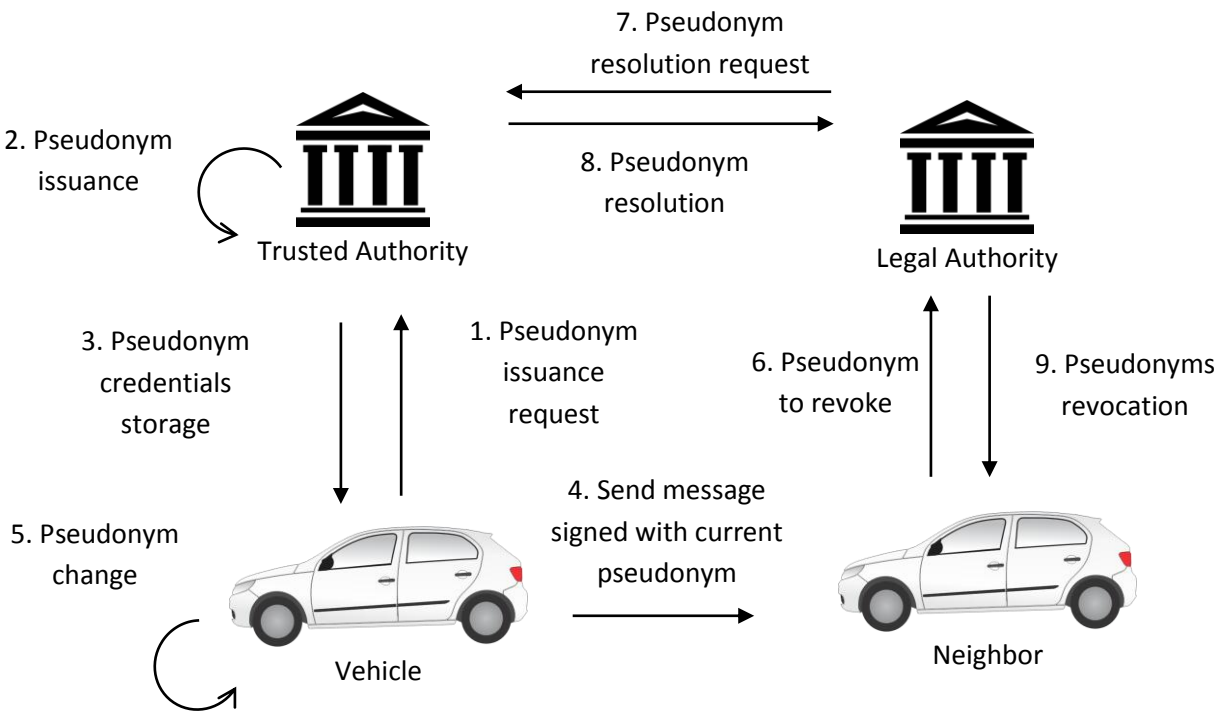

Figure 3.2: Pseudonym lifecycle in VANETs

A. Pseudonym Generation

The pseudonym generation, also called pseudonym issuance, is the initial stage of the pseudonym lifecycle. A trusted authority TA is responsible for the registration of each vehicle wishing to join the VANET, and the issuance of its pseudonyms using a pseudonym acquisition policy [78].

The issuance of pseudonyms requires the use of cryptography. Each issued pseudonym consists of a public key and has its corresponding private key. The TA also creates a public key certificate for each public/private key pair to verify the validity of the pseudonym at the beacon's receiver level.

The pseudonym generation must respect the two following rules:

- The content of a pseudonym must not reveal the true identity of the vehicle.
- A pseudonym is a unique temporary identifier. In other words, a pseudonym must belong to only one vehicle in the network.

B. Pseudonym Storage

In this step, the trusted authority TA stores the issued set of pseudonyms into a Hardware Security Module (HSM) or Tamper-Proof Device (TPD) in the OBU of the vehicle to ensure their protection against malicious attacks. The HSM or TPD is a safe and secure hardware encryption device used to store the vehicle's credentials, and run the cryptographic operations.

C. Pseudonym Use

When a vehicle joins the network, it selects one pseudonym and uses it to authenticate the outgoing messages to ensure the integrity and authenticity of the exchanged information. The pseudonym and its corresponding certificate are attached to the signed message to allow any receiver verify it.

D. Pseudonym Change

A pseudonym has a minimum short validity period of time during which it must be kept unchanged to ensure stable communication. After this period, the vehicle changes the pseudonym to a new one according to a privacy (i.e., pseudonym change) scheme. The European standard ETSI TS 102 867 recommends changing a pseudonym every 5 min [79] while the American standard SAE J2735 recommends changing it every 120 s or 1 km [22].

E. Pseudonym Refill

The pseudonym refill process becomes mandatory when the number of remaining pseudonyms (not yet used) reaches a certain predefined threshold. In this case, the vehicle must request new pseudonyms from the TA.

F. Pseudonym Resolution

The pseudonym resolution, also called conditional tracking is performed when a problem occurs in the network (e.g., sending a malicious message). Therefore, in case of liability issues, the TA has to be able to resolve a pseudonym to a malevolent vehicle's real identity in order to revoke it from the VANET.

G. Pseudonym Revocation

The pseudonym revocation is a step performed by the TA against the malicious attacks of the adversaries. It consists in revoking the pseudonyms of the malicious vehicle from the VANET system. The revocation of pseudonyms is accomplished by adding the certificates of the malicious vehicle to a Certificate Revocation List (CRL).

3.4.3. Pseudonym Change Schemes in VANETs

Many pseudonym change schemes have been proposed in the literature for VANETs. They aim primarily at ensuring an effective pseudonym change, and preventing the linkability of pseudonyms by confusing the adversary [51], [52], [53]. S. Zakhary *et al.* [51] present a survey of privacy-protection solutions proposed for Opportunistic Networks (OppNets). They present the privacy-related attacks, and the contemporary research efforts aiming to protect users' privacy. Also, the authors provide a taxonomy of privacy-preserving approaches showing the major trends in addressing the privacy problem. In [52], A. Boualouache *et al.* develop a survey on pseudonym change schemes in VANETs. In this survey, they present a classification of the different pseudonym change schemes, and make a comparison of these schemes. J. Petit *el al.* [53] present a survey on pseudonym schemes in VANETs, which regroups and presents many pseudonym management schemes.

In this section, we present a taxonomy and a description of the state-of-art pseudonym change schemes, and we determine their level of effectiveness to prevent the linkability of pseudonyms. Then, we perform a comparative study of some pseudonym change schemes proposed for VANETs with respect to some relevant criteria.

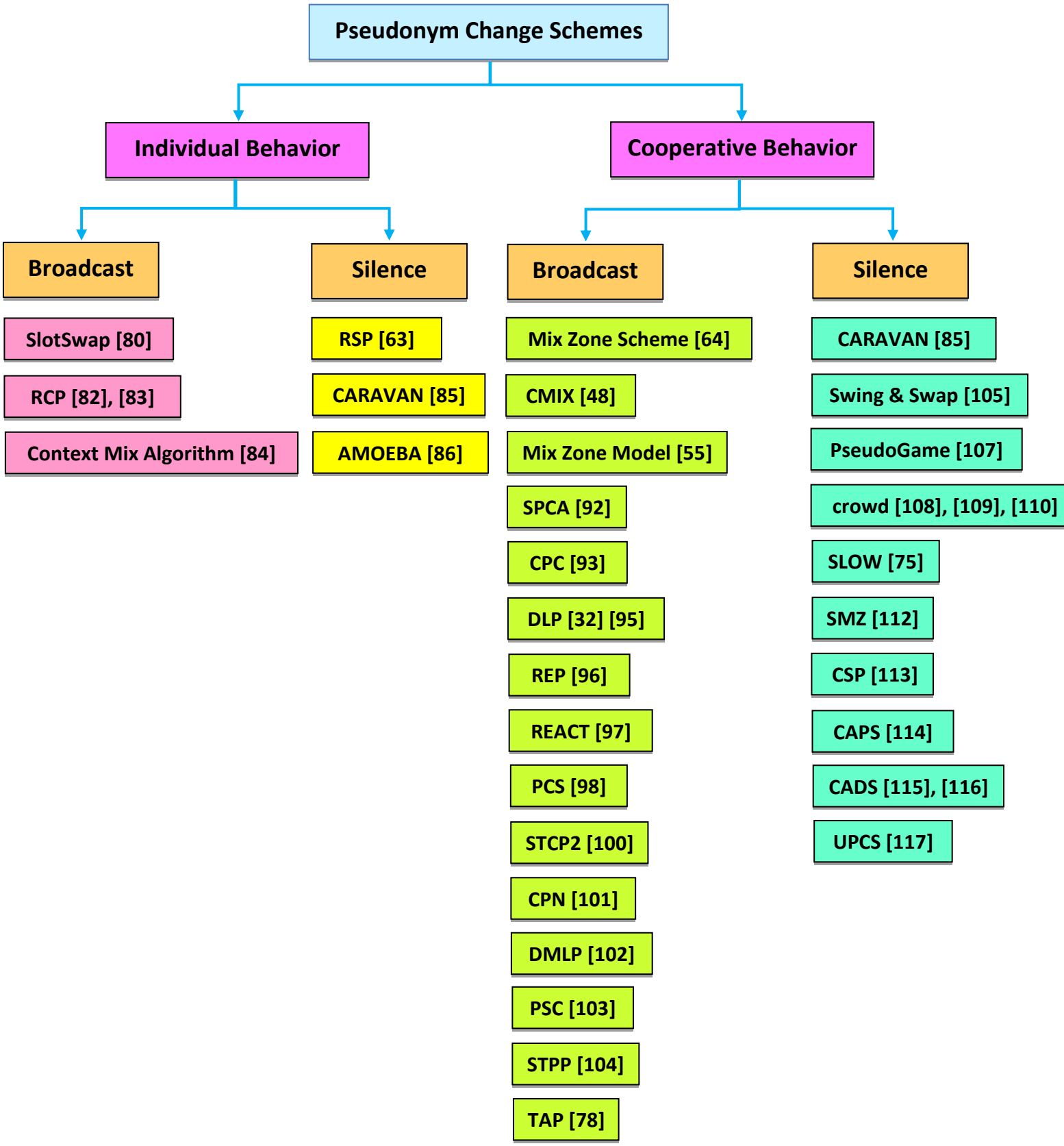

Figure 3.3: Taxonomy of pseudonym change schemes

Basically, the taxonomy of the state-of-art pseudonym change schemes has to be made according to the behavior of changing pseudonym to show the performance of each scheme against the linkability attack. In this thesis, we review the existing pseudonym change schemes, which we have classified into two main categories based on their properties related to the behavior of changing pseudonym, as shown in Fig. 3.3.

A. Individual Behavior

An individual behavior-based pseudonym change scheme lets a vehicle individually change its pseudonym without taking into consideration the neighboring environment. In this category, a pseudonym change scheme can either use silent period technique or not.

- *Broadcast Approach*

1) Periodical Pseudonym Change Scheme: In this scheme, the vehicle periodically changes pseudonym at fixed or random times. The fixed time periodical scheme [80] uses a fixed period to change pseudonyms. However, this rhythm of pseudonym change helps the adversary to predict the time and location of the next change of pseudonym. D. Eckhoff *et al.* [81] extend the fixed time periodical scheme with that of a time-slotted pseudonym pool to reduce the storage and computation needs. In the proposed scheme, every vehicle maintains a time-slotted pseudonym pool. Each pseudonym is used at a specific time slot. The time slot length determines the period in which one single pseudonym is used. When a time-slot has passed, the vehicle will change its pseudonym. In addition, the proposed scheme allows the exchange of pseudonyms between vehicles to eliminate the mapping between vehicles and pseudonyms. In the random time periodical scheme [82], [83], the vehicle keeps the current pseudonym for a random period of time.

2) Context Mix Algorithm: M. Gerlach *et al.* propose the context mix algorithm in [84]. The mix context means a vehicle finds several neighbors with similar status. The principle of the context mix algorithm is as follows. After using the pseudonym for a stable time, the vehicle assesses its context (i.e., neighborhood information) in search for a mix context. If the mix context is found, the vehicle changes its pseudonym. After each change of pseudonym, the vehicle assesses whether it was successful or not by measuring if other vehicles changed their pseudonyms in the same time step. If not so, it restarts the pseudonym change cycle again. However, this algorithm discusses an individual behavior, and it is a low probability that at least two vehicles with similar status change their pseudonyms simultaneously. In

addition, the mix context represents all the information that an adversary may use to link pseudonyms.

- *Silence Approach*

1) Random Silent Period Scheme: The random silent period (RSP) scheme is proposed by L. Huang *et al.* in [63] to prevent linking a new pseudonym with the old one. A silent period is defined by authors as a transition period between the use of new and old pseudonyms, when a node is not allowed to disclose either the old or the new address. In RSP, a vehicle keeps the current pseudonym for a fixed pseudonym period, and then enters silence for a random period within a range to change the pseudonym (see Fig. 3.4). However, in RSP scheme, a vehicle individually enters silence and changes pseudonym, which is not so effective in preserving privacy.

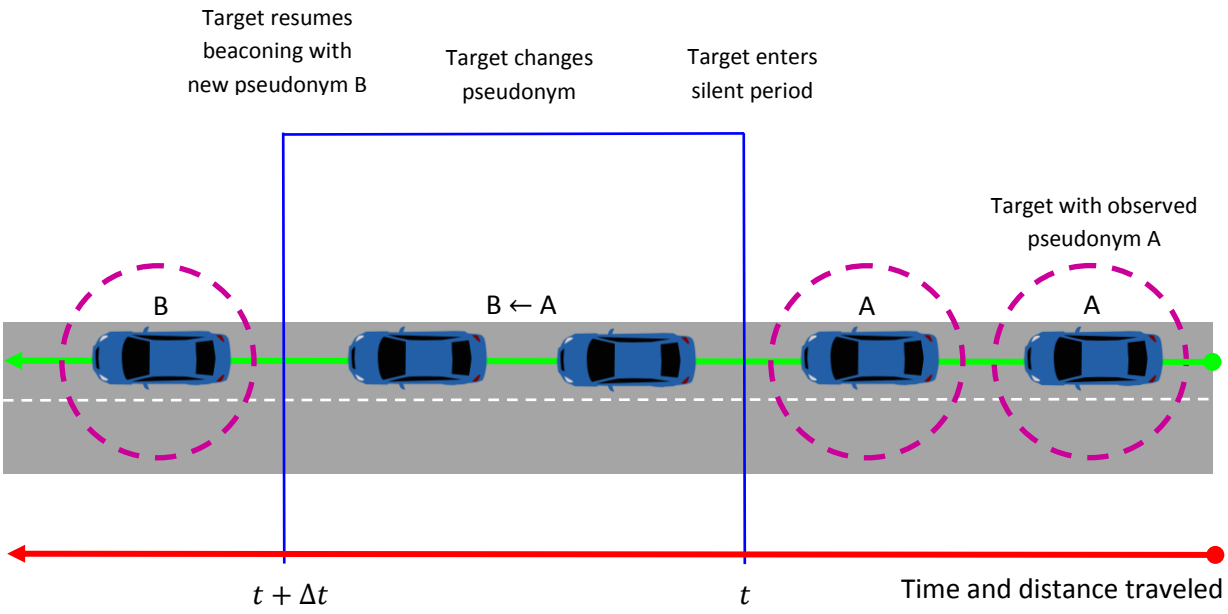

Figure 3.4: Illustration of the silent period scheme

2) CARAVAN: K. Sampigethaya *et al.* introduce a location privacy enhancing scheme for VANETs, called CARAVAN [85]. For V2V communications, CARAVAN uses the random silent period [63] to provide unlinkability to a vehicle entering the network. However, this solution suffers from the individual pseudonym change behavior. Indeed, if the entering vehicle enters silence and changes its pseudonym alone, it still remains linkable.

3) AMOEBA: In [86], K. Sampigethaya *et al.* propose the successor of CARAVAN [85], called AMOEBA. As in CARAVAN, AMOEBA enables a vehicle entering the network to enter random silent period to ensure unlinkability between the old and new pseudonyms.

B. Cooperative Behavior

In this category of pseudonym change schemes, a vehicle cooperates with the surrounding vehicles to change its pseudonym with them at the same time slot. As in the first category, a cooperative-based pseudonym change scheme can either apply the silent period scheme or not. Most of the proposed pseudonym change schemes fall within this category.

- *Broadcast Approach*

1) Mix Zone Scheme: In order to achieve location privacy in a pervasive computing environment, A. R. Beresford *et al.* propose the concept of mix zone [64]. Mix zones are anonymous regions of the network where mobile nodes change their identifiers to obfuscate the relation between entering and exiting events. Numerous proposals have since followed to allow the creation of mix zones, and the measurement of their effectiveness. In [87], B. Palanisamy *et al.* provide an overview of various known attacks (e.g., timing attack, transition attack, continual query (CQ) attack, CQ-timing attack, CQ-transition attack) that make basic mix zones and road network mix zones vulnerable. Then, they present a set of attack-resilient mix zone techniques, and analyze the privacy strength of these attack-resilient mix zones against the described attacks through experimental evaluation. In [88], B. Palanisamy *et al.* propose a MobiMix framework, which is a mix zone model to confront timing and transition attacks. R. Yu *et al.* [89] propose MixGroup, which uses group signature to construct extended pseudonym change regions (i.e., large mix zones), in which vehicles can exchange their pseudonyms. Fig. 3.5 illustrates a mix zone at a signalized road intersection. The vehicles inside the mix zone change their pseudonyms simultaneously.

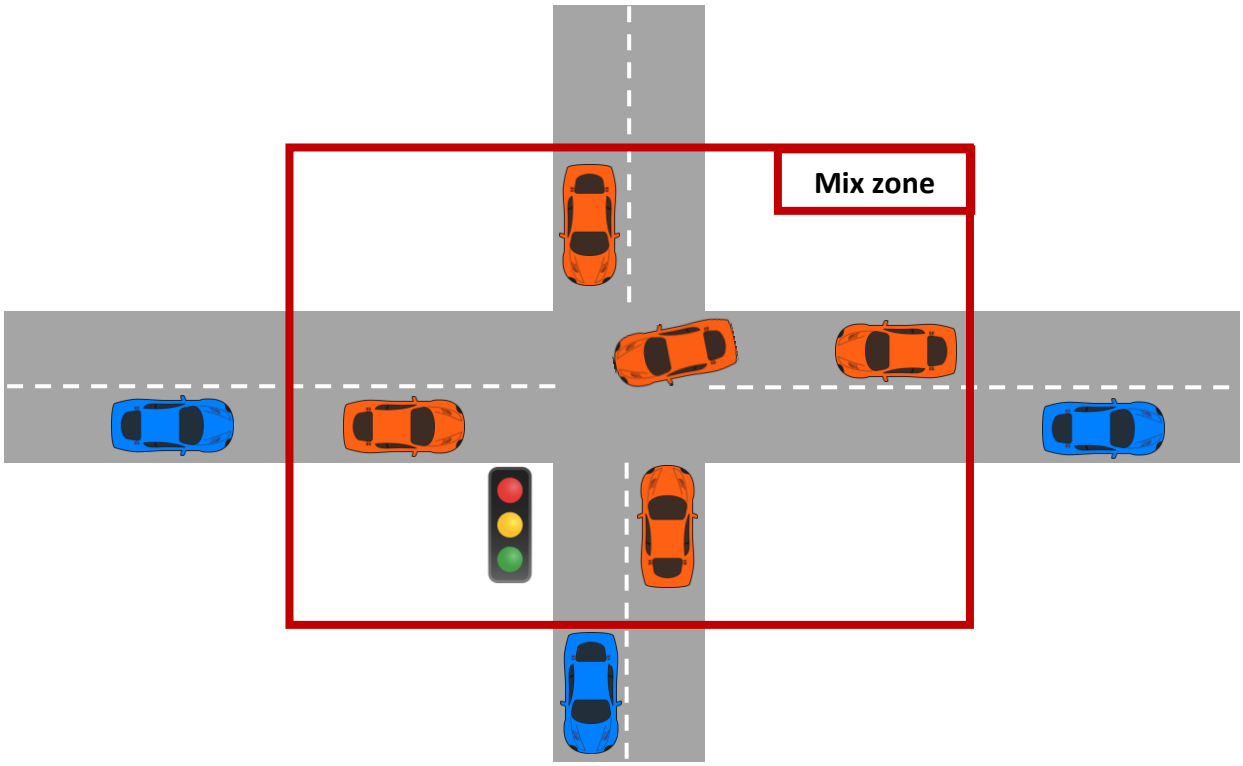

Figure 3.5: Example of a mix zone at a road intersection

2) CMIX: To achieve location privacy in VANETs, J. Freudiger *et al.* propose the cryptographic mix zone (CMIX) protocol against an external adversary [48]. CMIX places mix zones at road intersections, where vehicles change their pseudonyms. When a vehicle enters a mix zone, it uses a symmetric key to encrypt safety messages to prevent the external adversary from reading the content of the exchanged safety messages inside the mix zone. The symmetric key is obtained from the RSU of the mix zone. Then, the authors propose to combine several mix zones to create a vehicular mix network. CMIX protocol achieves the simultaneity of changing pseudonyms, and encrypts safety messages inside mix zones to prevent the external adversary from linking pseudonyms from safety messages. However, CMIX requires the presence of a RSU at each road intersection for encryption of safety messages. This requirement could lead to a hard deployment of the network due to administrative and installation costs [38]. Moreover, the cryptographic processing can slow the transmission of safety messages and so the reflex of drivers, as safety messages are real time in nature. Further, if an accident occurs at a road intersection, only the vehicles inside the intersection can be aware about the accident, because they detain the symmetric key to decrypt safety messages. Following CMIX proposal, M. Dahl *et al.* [90] describe a formal

analysis of mix-zones to investigate the effectiveness of vehicular mix-zone proposals. They analyze, using the protocol analysis tool ProVerif [91], the CMIX protocol. They show that in many scenarios CMIX protocol does not preserve privacy, and they propose a fix to the protocol.

3) Mix Zone Model: L. Buttyán *et al.* [55] define a model based on the concept of the mix zone (i.e., unobserved area on the road), a tracking strategy, and a privacy metric to study the effectiveness of changing pseudonyms in this mix zone model. They show that the frequency of pseudonym changes depends on the type of the mix zone (location, size) and the number of mix zones present in the network.

4) SPCA: In [92], J. Liao *et al.* propose a synchronous pseudonym change algorithm (SPCA), where both simultaneity of changing pseudonyms and vehicular status information are taken into consideration. The status of a vehicle i is defined as $\{Pi,\ Vi,\ Di\}$, $Pi, Vi,$ and Di denote its position, velocity and heading direction, respectively. In SPCA, a vehicle v changes its pseudonym if it finds at least k neighbors that want to change their pseudonyms, and have the same status as v. However, the adversary can use the disclosed vehicular status information (e.g., position) to link pseudonyms. Further, some neighbors may not find the trigger, and thus they will not change their pseudonyms with v. This behavior decreases the confusions of the adversary, and augments the chance of matching pseudonyms.

5) CPC: J. Liao *et al.* propose a cooperative pseudonym change (CPC) scheme [93] where cooperation between neighboring vehicles is performed to make more neighbors changing their pseudonyms synchronously to prevent linking pseudonyms and strengthen privacy. Numerical simulations were conducted to discuss the effectiveness of CPC scheme. In [94], Y. Pan *et al.* develop an approximate analysis model for CPC scheme to measure the level of achieved anonymity in one-dimensional VANETs where vehicles are uniformly distributed on the road. Analytical and simulation results indicate that several parameters have an impact on the level of anonymity provided by CPC scheme, and the performance of CPC scheme is better than that of non-cooperative pseudonym change (NCPC) scheme.

6) DLP: J.-H. Song *et al.* present a vehicle density-based location privacy (DLP) scheme [32], [95]. In DLP scheme, a vehicle monitors the neighboring vehicle density, and triggers a pseudonym change only when the number of neighboring vehicles reaches a certain threshold $k-1$. The area where the vehicle changes its pseudonym is called a k-density zone, which is

defined by authors as the area where at least k−1 distinct neighboring vehicles always exist around the vehicle.

7) REP: A. Wasef *et al.* [96] propose to use a random encryption period (REP) to prevent the spatiotemporal information in beacons from being stolen by an adversary to link the old and new pseudonyms. When a vehicle wants to change its pseudonym, it requests its neighbors to enter a REP with it, when the beacons are encrypted with a shared group key, and then it changes its pseudonym. The pseudonym change is considered successful if at least one neighbor has changed its pseudonym and its speed or its direction.

8) REACT: K. Mershad *et al.* [97] propose a secure and efficient data acquisition (REACT) scheme for VANETs to secure the exchanged data messages between users and RSUs. In REACT, the authors address the location privacy of users by enabling a RSU to assign a pseudonym (i.e., virtual ID) to each connected user. Then, the RSU changes the user's pseudonym per packet to prevent user movement tracking and jeopardizing his location privacy. In the city environment, a vehicle is usually surrounded by several neighbors. Thus, if each vehicle changes its pseudonym each time it sends a new packet, an adversary will not be able to know if the vehicle or a neighbor sent the new packet.

9) PCS: R. Lu *et al.* propose a pseudonym changing at social spots strategy, called PCS [98], [99]. A social spot is the place where many vehicles temporarily gather, e.g., a road intersection when the traffic light turns red, or a free parking lot near a shopping mall. PCS enables a vehicle to change its pseudonym before leaving a social spot to create a mix zone. However, PCS creates observed mix zones, where the spatiotemporal information embedded in beacons is visible, and permits to the adversary to link pseudonyms.

10) STCP2: Z. Li *et al.* [100] propose a short-time certificate-based privacy protection (STCP2) scheme to address privacy implications in VANETs. In STCP2, the authors propose a secure and privacy-preserving pseudonym change procedure that enables each vehicle to protect its privacy against both external and internal adversaries. In the pseudonym change procedure, each vehicle needs to confidentially change its pseudonym assisted by a RSU with three important tasks:

- *Location cloaking:* location cloaking conceals the vehicle's mobility trace nearby a RSU (i.e., cloaking region(CR)) from global passive adversary (GPA) and local passive adversary (LPA) using symmetric encryption for beacons.

- *Synchronized pseudonym update:* synchronized pseudonym update enables a vehicle to change its pseudonym and its corresponding IP/MAC addresses with the neighboring vehicles, and become a new vehicle to GPA and LPA.
- *Random mobility trace auditing:* random mobility trace auditing can detect local active adversaries (LAAs) that can obtain the symmetric key used for encrypting beacons inside the CR, and monitor the pseudonym changes in the CR.

11) CPN: In [101], Y. Pan *et al.* propose a cooperative pseudonym change scheme based on the number of neighbors (CPN). CPN lets a vehicle monitor its neighbors within a range R, and wait until they reach a threshold *k*. When this trigger occurs, the vehicle broadcasts a set flag with its beacon to inform its neighbors that the trigger is met, and then changes its pseudonym. When a neighbor receives a beacon with a set flag, it changes pseudonym immediately. CPN offers the advantage of changing pseudonyms simultaneously. However, the problem encountered is that vehicles continue to broadcast plain messages when changing pseudonyms, which facilitates linking pseudonyms. Further, a vehicle may excessively change its pseudonyms, if it receives a lot of pseudonym change requests from its neighbors in the long run. Excessively changing pseudonyms gives clearly an advantage to improve anonymity and prevent tracking, but makes the communication unstable and has a negative impact on communication protocols (e.g., routing task), and long-term communication applications (e.g., file transfer or interactive chat sessions).

12) DMLP: In [102], B. Ying *et al.* propose dynamic mix-zone for location privacy (DMLP) scheme for VANETs. DMLP allows vehicles to dynamically create cryptographic mix zones where and when it is needed.

13) PSC: S. Xingjun *et al.* [103] propose a pseudonyms synchronously change (PSC) scheme to optimize pseudonym update process and maximize the level of anonymity in VANETs. PSC scheme lets *k* neighbors synchronously change pseudonyms, such that $k > 1$. In PSC scheme, if a vehicle has more than or equal to *k* neighbors, it sends a requested message to request its neighbors to change their pseudonyms together with it, and then it changes its pseudonym. Therefore, the size of the anonymity set becomes sufficiently large to hide the vehicle within a large crowd. We note that the pseudonym change procedure in PSC scheme is similar to that proposed in CPN scheme [101]. In PSC, each RSU periodically broadcasts the number of transmitting vehicles in its vicinity. Thus, a vehicle can utilize the broadcast to obtain the number of neighbors.

14) STPP: In [104], D. Eckhof *et al.* propose a holistic solution for location privacy protection in VANETs. This solution is based on synchronized time-slotted pseudonym pools (STPP). Each vehicle maintains a pool of chronologically ordered pseudonyms. Only one pseudonym is valid at a specific time slot. The pseudonyms of the pool have the same validity duration for all vehicles (e.g., 10 minutes). Assuming synchronized clocks (e.g., via GPS), all vehicles change their pseudonym at exactly the same time (e.g., at 0:10 AM). Therefore, the benefit of using the STPP is to limit the storage overhead and maximize the adversary's confusions.

15) TAP: M. Khodaei *et al.* propose a time-aligned pseudonym (TAP) scheme for protecting privacy in VANETs [78]. In TAP scheme, the certification authority (CA) issues pseudonyms for a predetermined universally fixed interval Γ. These pseudonyms have the same pseudonym lifetime τ_P and are timely aligned with the rest; as a result, all vehicles change their pseudonyms at the same time and there is no distinction among vehicle sets.

- *Silence Approach*

1) CARAVAN: K. Sampigethaya *et al.* [85] present the second contribution of CARAVAN, where they combine the group navigation with the random silent period technique to ensure the simultaneity of changing pseudonyms. For most of the V2I communications based applications, CARAVAN uses the group navigation to enable vehicles to form a group that is represented by a single vehicle (the group leader), which communicates on behalf of the group. Hence, the remaining vehicles in the group can stay silent for an extended period of time that is bounded by the time they stay in the group. However, the group leader sacrifices its privacy for other vehicles in the group, since it does not enter silent period, and so it remains monitored and tracked by the adversary. Further, the silent period could be extended as long as silent vehicles are in the group, which may cause a network disconnection issue.

2) Swing & Swap: In [105], M. Li *et al.* propose a user-centric scheme called Swing & Swap to increase the location privacy of users in wireless networks. Swing is an approach that enables the nodes to independently initiate and loosely synchronize updates of their identifiers when changing their velocity (i.e., speed, direction) to overcome the limitations posed by the asynchronous identifier updates and tracking based on movement predictability. Swap is an extension of Swing that enables the nodes to exchange their identifiers to maximize the location privacy provided by each update, hence reducing the number of updates to new identifiers. The proposed scheme builds on the random silent period technique of [106].

3) PseudoGame: In [107], J. Freudiger *et al.* use a game-theoretic model that takes into account the gained payoff and the cost generated by each mobile node when changing pseudonym at a silent mix zone. Based on the results of their analysis and simulations, they proposed PseudoGame protocols for optimizing pseudonym changing at silent mix zones.

4) crowd: B. K. Chaurasia *et al.* [108], [109], [110] propose a strategy called crowd that allows a vehicle to change its pseudonym at a time and place where the anonymity can be enhanced. The proposed strategy aims to increase the cardinality of the anonymity set to hide the vehicle in the crowd of its neighboring vehicles by entering silent period and changing its pseudonym. The change is effective if the number of the neighboring vehicles becomes more than k. Simulation and analysis results show that updating pseudonyms in accordance to the proposed strategy enhances the anonymity of a vehicle.

5) SLOW: L. Buttyán *et al.* propose SLOW scheme for location privacy in VANETs in [75]. In SLOW, a vehicle continuously checks its current speed and broadcasts beacons only when its speed is higher than a preset threshold SP. The vehicle stops broadcasting beacons (i.e., enters silent period) when its speed becomes lower than SP. If the vehicle does not send beacons for ST seconds, it changes its pseudonym. The advantage offered by SLOW is that it allows to a group of neighboring vehicles to enter silence and change their pseudonyms simultaneously, which confuses the adversary and prevents linking pseudonyms. However, SLOW makes a vehicle silent during almost the whole trip, particularly in high-density urban areas (e.g., road intersections, rush hours, traffic jam). This silence may negatively impact the proper functionality of safety applications as shown in [111].

6) SMZ: In [112], H. Dok *et al.* propose to combine a set of published privacy-preserving solutions, namely: mix zone concept, silent period technique, and group signature mechanism to create a silent mix zone (SMZ) scheme in order to improve the privacy of users in VANETs. In this scheme, a vehicles enters a region where vehicles change their pseudonyms as well as network addresses (i.e., mix zone); next enters the silent period, and then uses one group key for communication.

7) CSP: In [113], A. Tomandl *et al.* propose a coordinated silent period (CSP) scheme, which coordinates all vehicles in the network to enter silent period and change their pseudonyms synchronously. CSP has the advantage to increase the privacy level significantly because it maximizes the size of the anonymity set at every pseudonym change. However,

CSP seems to be theoretical, since the coordination overhead in real world situations is very large.

8) CAPS: The context-aware privacy scheme (CAPS) is proposed by K. Emara *et al.* in [114]. In CAPS, a vehicle selects the effective context to enter silent period and change its pseudonym, and when to resume beaconing with a high probability of confusion to a global adversary. For this, a vehicle monitors the surrounding vehicles and enters silent period when it finds one or more neighbors silent. It resumes beaconing with a new pseudonym when its actual state is likely to be mixed with the state of a silent neighbor.

9) CADS: K. Emara *et al.* propose in [115], [116] a context-adaptive and user-centric privacy scheme (CADS), which is a significant improvement of CAPS. In CADS, a vehicle determines the effective context to enter silent period and change its pseudonym, and the right period of silence to provide unlinkability of subsequent pseudonyms. Moreover, in CADS, the driver has the possibility to choose his privacy preference whether low, normal or high levels.

10) UPCS: A. Boualouache *et al.* suggest in [117] a urban pseudonym changing strategy (UPCS) for the urban environment. UPCS constructs silent mix zones at signaled intersections, where vehicles can use either pseudonyms changing technique or pseudonyms exchanging technique. The pseudonyms exchanging technique uses a RSU-based swapping protocol.

An overview of the characteristics of some important pseudonym change schemes for VANETs is shown in Table 3.1.

Table 3.1: Comparison of VANET pseudonym change schemes

	Attacker Model[1]	Pseudonym Generation[2]	Behavior of Changing Pseudonym[3]	Messages Information Protection[4]	Pseudonym Change Area[5]	Pseudonym Change Success Check	Neighbors Table	Traffic Light	Infrastructure (RSU)	Evaluation Privacy Metrics[6]	Mobility[7]	Simulation Tool
CARAVAN [85]	GPA	RA	I C	SP	S F	No	Yes	No	Yes	ASS TT	IMPORTANT C-F-M C-L-M	-
Context Mix Algorithm [84]	GPA	-	I	None	S	Yes	Yes	No	No	T TT	STRAW	JIST/SWANS
CMIX [48]	GPA	CA	C	E	RI	No	No	No	Yes	E ASR	MATLAB	-
SPCA [92]	GPA	-	C	None	S	No	Yes	No	No	PST	STRAW	-
PCS [98]	GPA	User (KPSD)	C	None	RI PL	No	No	Yes	Yes	ASS LPG	-	-
CPN [101]	GPA	-	C	None	S	No	Yes	No	No	ASS	MATLAB	MATLAB
CAPS [114]	GPA	CA	C	SP	S	No	Yes	No	No	T NT	STRAW SUMO	-
CADS [115]	GPA LAA	-	C	SP	S	No	Yes	No	No	T NT	SUMO	MATLAB
UPCS [117]	GPA LPA	CA	C	SP	RI	No	No	Yes	Yes	E PST	SUMO	Veins

[1]**Attacker Model:** GPA: Global Passive Adversary, LAA: Local Active Adversary, LPA: Local Passive Adversary.

[2]**Pseudonym Generation:** RA: Registration Authority, CA: Certification Authority, KPSD: Key-insulated Pseudonym Self-Delegation.

[3]**Behavior of Changing Pseudonym:** I: Individual, C: Cooperative.

[4]**Messages Information Protection:** SP: Silent Period, E: Encryption.

[5]**Pseudonym Change Area:** S: Street, F: Freeway, RI: Road Intersection, PL: Parking Lot.

[6]**Evaluation Privacy Metrics:** ASS: Anonymity Set Size, TT: Tracking Time, T: Traceability, E: Entropy, ASR: Adversary Success Ratio, PST: Pseudonyms Statistics, LPG: Location Privacy Gain, NT: Normalized Traceability.

[7]**Mobility:** C-F-M: Car Following Model, C-L-M: Changing Lane Model.

3.4.4. Privacy Metrics

Several privacy metrics have been proposed in the literature for performance evaluation of pseudonym change schemes in VANETs [118], [119], [120], [121], [122]. In the following, we give a definition to each privacy metric.

1. Pseudonyms Statistics

The pseudonyms statistics are used as a privacy metric to do statistics and calculations on the pseudonyms used in a pseudonym change scheme. The pseudonyms statistics include, for example, the total number of changed pseudonyms and the total number of successfully changed pseudonyms.

2. Anonymity Set Size

The Anonymity Set Size (ASS) is a privacy metric introduced by D. Chaum in [123]. The Anonymity Set (AS) of a vehicle includes the vehicle and its neighbors that change pseudonyms together with it in the same slot [101]. The ASS represents the cardinality of the AS. The achieved location privacy level is obtained by computing the average anonymity set size $\overline{ASS}$. The average ASS $\overline{ASS}$ was calculated in [124] using the following formula:

$$\overline{ASS} = \frac{\sum_{i=1}^{N} \sum_{k=1}^{max} ASS_{i,k}}{TNCP}$$

where N and max stand for the number of vehicles and the maximum number of pseudonym changes by each vehicle in the network, respectively. $ASS_{i,k}$ is the ASS obtained by the vehicle i at the kth pseudonym change. $TNCP$ is the total number of changed pseudonyms.

As a privacy metric, the ASS can only show how a proposed pseudonym change scheme can affect the simultaneous pseudonym change. However, the ASS does not consider the ability of an adversary of distinguishing a target vehicle among members in the AS using the spatiotemporal information included in beacons. For this reason, R. Shokri *et al.* show that the ASS is not a suitable privacy metric [125], because an adversary can exclude unlikely hypotheses using tracking algorithms.

3. Entropy

To overcome the limitations of the anonymity set size, Serjantov *et al.* [126] and Diaz *et al.* [127] propose the entropy to measure the achieved level of anonymity. In Information Theory, entropy is a measure of the uncertainty in a random variable. The entropy of the

anonymity set is the measure of the anonymity of a vehicle in the set [108]. It allows expressing the adversary's knowledge about each vehicle of the anonymity set. Formally, the entropy of the anonymity set, denoted by $H(p)$, is calculated as follows:

$$H(p) = -\sum_{i=1}^{V} p_i \log_2 p_i$$

where p_i is the probability that the vehicle i is the target, and V is the number of the vehicles in the anonymity set, such that $V = |AS|$.

4. Traceability

The traceability of vehicles, denoted as Π, is a quantitative measurement calculated by counting the percentage of tracked vehicles. Formally, the traceability Π is defined in [115] as follows:

$$\Pi = \frac{1}{N}\sum_{v \in V} \lambda_v \times 100, \lambda_v = \begin{cases} 1, & \frac{\tau_v}{L(v)} \geq 0.90 \\ 0, & otherwise \end{cases}$$

where V represents the set of vehicles in the network and N is the total number of vehicles in the network. τ_v and $L(v)$ stand for the tracking period and the lifetime of the vehicle v, respectively.

5. Normalized Traceability

The normalized traceability Π_n excludes the vehicles that never change their pseudonyms during their lifetime, since they are easily tracked by the adversary and reflected in the original traceability metric. Π_n is introduced and defined in [115], [116] as:

$$\Pi_n = \frac{1}{N}\sum_{v \in V} \lambda_v^{norm} \times 100,\ \lambda_v^{norm} = \begin{cases} 1, & \frac{\tau_v}{L(v)} \geq 0.90 \wedge psd(v, k_0) \neq psd(v, k_0 + L(v)) \\ 0, & otherwise \end{cases}$$

where $psd(v, k_0)$ and $psd(v, k_0 + L(v))$ are the pseudonyms of the vehicle v at the first and last time steps in its lifetime, respectively.

6. Traceability- and Distortion-based Privacy Metric

In [128], K. Emara propose a combined privacy metric that is based on traceability and distortion metrics. The proposed metric can be used to measure both aspects to determine how

long the adversary can track a vehicle, and how accurate the reconstructed tracks are related to the original traces of vehicles.

Several efforts have been made to realize a simulation framework dedicated to the evaluation of the pseudonym change schemes in VANETs. In [129], K. Emara propose a location privacy extension (PREXT) for Veins VANET simulator [130], [131]. PREXT implements seven pseudonym change schemes of different approaches including silent period, context-based and mix-zone, and can be easily extended to include more schemes. For the evaluation of the pseudonym change schemes, PREXT includes adversary modules that can eavesdrop vehicle messages and track their movements. This adversary is used in measuring the protection level of a privacy scheme in terms of several popular privacy metrics such as ASS, entropy, traceability and pseudonym statistics.

3.5. Summary

In this chapter, we have discussed about the preservation of privacy in VANETs. We have first presented the different attacks that arise a serious privacy threat in VANETs. We have seen that the continuous periodical broadcast of spatiotemporal information contained in beacons facilitates to the adversary to link between pseudonyms of the same vehicle, and rebuild its anonymous trace. Then, the adversary can launch the inference attack to de-anonymize the reconstructed vehicle's trace, and find the driver's real identity. Hence, the adversary can easily track the driver's activities. In the rest of the chapter, we have given a definition of privacy, and the privacy requirements. We have then presented the pseudonym change approach that is widely accepted as a solution to protect the users' privacy in VANETs. Next, we have mentioned the different stages of the pseudonym lifecycle. Finally, we have presented the research work carried out in the context of changing pseudonyms in order to achieve the preservation of privacy, and we have compared between some pseudonym change schemes proposed for VANETs according to different criteria. We have given the privacy metrics used for performance evaluation of pseudonym change schemes in VANETs at the end of the chapter.

4 Conditional Privacy Preservation for VANET Safety Applications

4.1. Introduction

Nowadays, VANETs become an emerging wireless technology that promises to improve road safety and traffic management. In general, the VANET applications are divided into two major categories: (1) safety applications and (2) non-safety applications [14]. Safety applications aim to ensure road safety in order to prevent accidents and hazardous situations. Examples of such applications include cooperative driving, work zone warning, road condition warning, post-crash warning, etc. Non-safety applications, such as Internet access and infotainment offer convenience and entertainment to drivers and passengers.

The greatest motivation of the development of VANETs is the safety applications, since they play a very important role in reducing road accidents and problems. According to the analysis conducted by the U.S. Department of Transportation's (DOT) National Highway Traffic Safety Administration (NHTSA), crashes, injuries, and fatalities could be reduced by 50% on average using two potential safety applications, intersection movement assist and left turn assist [15]. Unfortunately, safety applications may lose their effectiveness due to misbehaving vehicles, which causes the unacceptance of VANETs. Therefore, security and privacy enhancing schemes are indispensable for the success of VANETs, and represent a prerequisite for their deployment. The location privacy preservation makes drivers reassured and more attracted to use VANETs. Thus, how to ensure the users' location privacy is a challenge, and is only guaranteed by the development of an efficient privacy preservation scheme. However, a malicious vehicle cannot be tracked and identified if a *complete* privacy preservation scheme is used [49]. Therefore, a *conditional* privacy preservation scheme must be used to achieve location privacy, and guarantee that the real identity of a malicious vehicle can be disclosed for revocation in case of dispute. In this scheme, a central Trusted Authority (TA) is responsible for revealing and revoking the malicious vehicle's real identity, that is, the conditional tracking.

Group signatures are capable of building conditional privacy preservation scheme; however, the computation costs are relatively high [46], [49]. Unlinkable pseudonyms schemes are considered as an effective solution to achieve conditional privacy preservation. However, unlinkable pseudonyms schemes, which propose to preload pseudonyms inside the vehicle [48], become ineffective in case of vehicle theft. In fact, the preloaded pseudonyms could be abused by the thieves, once the vehicle is stolen [98]. Therefore, to prevent the use of pseudonyms by an unauthorized entity, we introduce the use of a *connection card*, where

pseudonyms are stored. The role of the connection card is to allow a vehicle to connect to the VANET system, and communicate with other entities (since it contains the pseudonyms). The use of the connection card is similar to the use of the car keys that allow the ignition and start-up of the vehicle. Thus, without the connection card, the vehicle is not able to connect to the VANET, and therefore can not be part of the network members.

In this chapter, we address the problem of achieving location privacy to secure VANETs. We look for how to generate pseudonyms, and develop an efficient Pseudonyms Generation Protocol (PGP), in order to support real identity tracking by a TA, and thus to achieve the requirements of location privacy, conditional privacy preservation, and pseudonyms protection in secure VANET safety applications.

4.2. Pseudonyms Generation Protocol

In this section, we propose our efficient pseudonym generation protocol for securing VANET safety applications, which consists of two parts: (1) system settings and (2) conditional tracking.

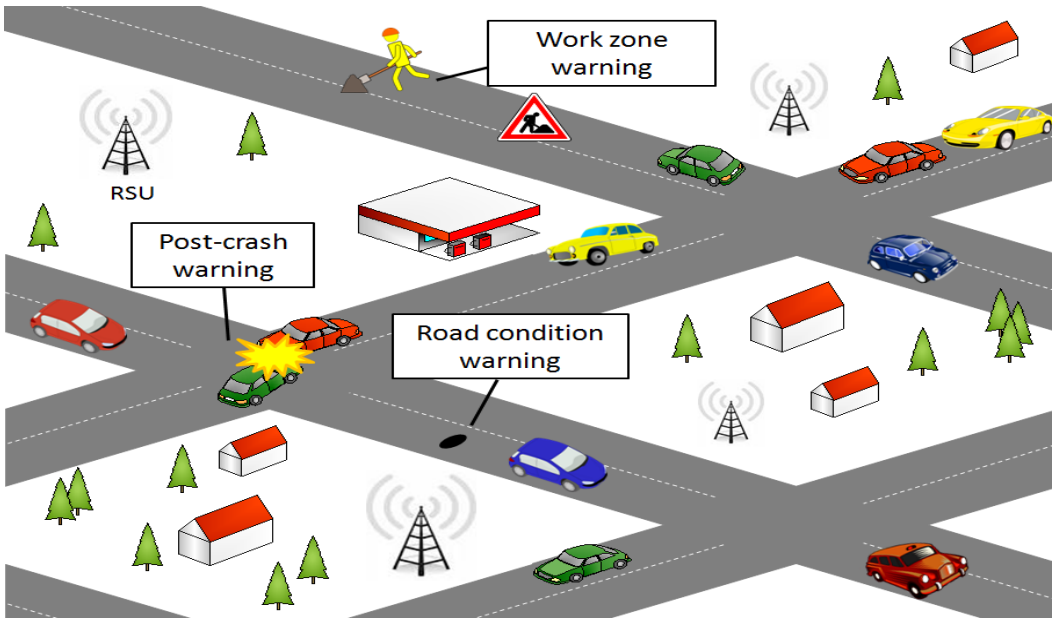

Figure 4.1: Illustration of a VANET system in an urban area. Examples of safety applications include work zone warning, road condition warning, and post-crash warning. If used effectively, this could help drivers avoid road construction sites, potholes and traffic jams due to cars collisions

4.2.1. System Settings

The VANET system considered consists of vehicles $V = \{V_1, V_2, \dots\}$ moving on the road, RSUs, and a TA accessible via the RSUs. The Fig. 4.1 illustrates a VANET system in an urban area. The TA is a fully trusted entity, which is responsible for initializing the whole system, assigning pseudonyms to vehicles as well as tracking and revoking malicious vehicles. Each vehicle $V_i \in V$ is equipped with an OBU to guarantee V2V and V2R communications. In addition, vehicles are required to exchange safety messages to achieve the VANET safety applications. Each safety message is signed with the current used pseudonym for authentication. RSUs are deployed roadside for the purpose to allow and provide passing vehicles access to the TA, and other network services.

To establish a secure VANET system, the TA first sets up the system parameters as follows: given a security parameter κ, the TA issues the bilinear parameters (q, g, G, G_T, e), where q is a κ-bit large prime number, G, G_T are two additive cyclic groups of the same order q, $g \in G$ is a generator, and $e: G \times G \to G_T$ is a non-degenerated and efficiently computable bilinear map [132], [133]. Then, the TA chooses two random numbers $u, v \in Z_q^*$ as the master key, and computes $P = ug$ as the public key. Moreover, the TA selects a secure symmetric encryption algorithm E (e.g., the Advanced Encryption Standard (AES)), and three collision-resistant hash functions H_1, H_2, H, where $H_i: \{0,1\}^* \to Z_q^*$ with $i \in \{1,2\}$ and $H: \{0,1\}^* \to G$. Finally, the TA keeps the master key secret, and publishes the system parameters: $(q, g, G, G_T, e, P, E, H_1, H_2, H)$.

To join the VANET system, a vehicle $V_i \in V$ has to register with the TA. First, the TA chooses a random number $R_i \in Z_q^*$, and stores (V_i, R_i) in a Tracking List (TL). Then, the TA divides a long time interval into small and continuous time periods $T_1, T_2, \dots, T_n$, and generates two auxiliary keys (a_j^i, b_j^i) at each time period T_j for V_i, where $a_1^i = R_i$, $a_j^i = H_1(a_{j-1}^i)$ with $j = 2, \dots, n$, and $b_j^i = H_2(a_j^i)$ with $j = 1, \dots, n$ [134]. At each time period T_j, the TA creates a set of pseudonyms PSD_k^{ij} for the vehicle V_i, so that V_i can regularly change its pseudonyms for location privacy. Each pseudonym PSD_k^{ij} consists of a public/private key pair (pk_k^{ij}, sk_k^{ij}), and the corresponding public key certificate $Cert_k^{ij}(pk_k^{ij})$. To generate a public key pk_k^{ij} for V_i at time period T_j, the TA chooses two random numbers r_{k1}^{ij}, r_{k2}^{ij}, and uses the master key v and b_j^i to calculate the public key $pk_k^{ij} = E_v(V_i \parallel r_{k1}^{ij}) \parallel E_{b_j^i}(T_j \parallel r_{k2}^{ij}) \parallel$

T_j, and then uses the master key v to compute the corresponding private key $sk_k^{ij} = vH(pk_k^{ij})$. In addition, the TA generates the corresponding public key certificate $Cert_k^{ij}(pk_k^{ij})$. Finally, the TA stores the issued pseudonyms PSD_k^{ij} into a connection card cc_j^i, and then gives the connection card cc_j^i to the owner of the vehicle V_i.

Once the owner of the vehicle V_i gets the connection card cc_j^i, he/she will be able to use it to connect to the VANET when he/she gets inside the vehicle V_i, and plugs it into the (connection card) dedicated port. To communicate with other network entities, the in-car communication system selects and loads from the connection card cc_j^i one pseudonym PSD_k^{ij} to generate a signature [135] for anonymous authentication. Then, the pseudonym is discarded and changed by a new one to achieve location unlinkability. Each pseudonym has a short validity period and is not reused.

Before the time period T_j elapses and the connection card cc_j^i is exhausted totally, the vehicle V_i must warn the driver about that. To do that, if the number of the residual pseudonyms in the connection card cc_j^i reaches a predetermined threshold, the vehicle notifies the driver on the in-vehicle display monitor that the threshold is reached, and that it is time to get a new connection card cc_{j+1}^i from the TA for the next time period T_{j+1} before residual pseudonyms exhaust all. This alert is very analogous to fuel gauge with low fuel alert.

4.2.2. Conditional Tracking

In case of dispute, the conditional tracking is required, which consists in revealing the real identity of the rogue vehicle by the TA in order to be revoked.

If a message M signed by the pseudonym PSD_k^{ij} is in dispute, the real identity V_i of the message source should be tracked and disclosed by the TA. Once the TA receives the disputed message M, along with its signature with respect to the pseudonym PSD_k^{ij}, it uses the public key $pk_k^{ij} = E_v(V_i \parallel r_{k1}^{ij}) \parallel E_{b_j^i}(T_j \parallel r_{k2}^{ij}) \parallel T_j$ to simply extract $E_v(V_i \parallel r_{k1}^{ij})$, and uses the master key v to get $V_i \parallel r_{k1}^{ij}$. In this way, the TA can disclose the real identity V_i.

To support revocation, the TA uses the real identity V_i to search the entry (V_i, R_i) in the TL, then it computes the auxiliary key a_j^i at time period T_j from the retrieved R_i, and updates a_j^i in the Revocation List (RL). Finally, the TA disseminates the latest RL to vehicles on the

road through RSUs. If V_i was revoked in a past time period T_p where $p < j$, other vehicles can perform the local revocation using the auxiliary key a_j^i that is stored in the RL. For example, if a vehicle V wants to verify whether the vehicle V_i was revoked or not, it computes a_j^i at time period T_j from a_p^i using the hash function H_1, computes the corresponding auxiliary key $b_j^i = H_2(a_j^i)$, and then uses b_j^i to decrypt $E_{b_j^i}(T_j \parallel r_{k2}^{ij})$. If the recovered time period T_j is correct, the vehicle V locally revokes the message M sent by PSD_k^{ij} as well as the real identity V_i.

4.3. Privacy Preservation Verification

In this section, the privacy preservation of the proposed protocol PGP is verified in terms of location privacy, conditional privacy preservation, and pseudonyms protection.

4.3.1. Location Tracking

To achieve location privacy in the VANET system, each vehicle $V_i \in V$ should detain a large number of unlinkable pseudonyms. In PGP, each public key $pk_k^{ij} = E_v(V_i \parallel r_{k1}^{ij}) \parallel E_{b_j^i}(T_j \parallel r_{k2}^{ij}) \parallel T_j$ is calculated with two random numbers r_{k1}^{ij} and r_{k2}^{ij}. As a result, all pseudonyms of the vehicle V_i are unlinkable. In addition, for pseudonyms unlinkability, the vehicle V_i should change its pseudonyms at the proper time and occasion [48], [92], [98].

4.3.2. Conditional Privacy Preservation

To achieve conditional privacy preservation, no other vehicles except the TA should be able to identify the real identity V_i from any pseudonym PSD_k^{ij}. From the public key $pk_k^{ij} = E_v(V_i \parallel r_{k1}^{ij}) \parallel E_{b_j^i}(T_j \parallel r_{k2}^{ij}) \parallel T_j$, only the TA is able to use the master key v to recover V_i from $E_v(V_i \parallel r_{k1}^{ij})$. Hence, PGP preserves conditional privacy.

4.3.3. Pseudonyms Protection

The most important objective that incited us to propose the use of connection cards is to protect the pseudonyms from abuse by vehicles thieves. In fact, the use of connection cards permits to the owner of the vehicle to always have the pseudonyms in his company, which prevents, in case of vehicle theft, the use of pseudonyms by an unauthorized entity as well as the impersonation attack. In this way, the vehicle thieves can not connect to the VANET, and communicate by means of the vehicles pseudonyms.

4.4. Summary

In this chapter, to secure VANET safety applications, we proposed an efficient pseudonym generation protocol, called PGP, which ensures the conditional privacy preservation requirement. In future work, we plan to design more efficient pseudonym generation protocols for VANETs.

5 Context-based Location Privacy Scheme for VANETs

5.1. Introduction

VANETs are a promising wireless communication system, which enables copious applications to enhance road traffic safety and offer entertainment to drivers and passengers. These applications need the design and implementation of reliable and efficient communication protocols and services to work properly [136]. The state-of-art presents a multitude of variant research works to meet different applications needs in the VANET research field [137], [138].

Security and privacy in VANETs are crucial as vehicular communications are subjected to critical life-threatening attacks. The continuous periodical broadcast of beacon messages containing the spatiotemporal information of the vehicle permits to a global passive adversary to correlate messages of old and new pseudonyms, and reconstruct vehicle traces [31], [56]. This attack threatens the driver's privacy. Also, the adversary can perform inference attacks to de-anonymize the reconstructed traces and find out the driver's identity [57], [58].

If a vehicle individually changes pseudonym without taking into account the surrounding environment, it may in some cases be forced to change its pseudonym alone. This behavior helps the adversary to easily link the new pseudonym with the old one, and track the vehicle since no other vehicle changed its pseudonym with it. Thus, to confuse the adversary, a vehicle should cooperate with a certain number of vehicles nearby to simultaneously change its pseudonym with them. However, even if vehicles change their pseudonym simultaneously, the adversary still has the possibility to link pseudonyms, and track vehicle movements owing to the spatiotemporal information contained in beacon messages. To prevent this attack, the messages information should be kept secret during pseudonym change. Therefore, a successful change of pseudonym is only possible if the following unlinkability requirements are met:

R-1. Pseudonym Changing Simultaneity: a vehicle should change its pseudonym simultaneously with a certain number of vehicles in its vicinity.

R-2. Concealment of Messages Information: the purpose of this condition is to prevent the adversary from obtaining the messages information during pseudonym changing process. This condition can be achieved with three different approaches:

- Using a silence period before a pseudonym change [63].

- Changing pseudonyms in mix-zones where the adversary cannot eavesdrop the exchanged messages, which makes the vehicle trajectory unpredictable [64].
- Encrypting the exchanged messages for changing pseudonym [48].

In the literature, there are several pseudonym change schemes that try to efficiently change pseudonyms, and prevent their linkability [53]. In this thesis, to achieve high-level location privacy in VANETs, we propose a Context-based Location Privacy Scheme, called CLPS. Our proposal CLPS is based on the context of a vehicle. A. K. Dey *et al.* [139] define context as "any information that can be used to characterize the situation of an entity". We define the context of a vehicle as the information regarding the vehicle's neighborhood such as the number of neighbors, their position, direction and speed. The context information is used for initiating a pseudonym change. In fact, it permits to a vehicle to identify the good situation to blend in a number of vehicles and change its pseudonym in an anonymous manner [84]. There are several existing works that include the use of context information [84], [92], [101], [114], [115]. The CLPS offers the contributions that can be summarized as follows:

- Propose an effective pseudonym changing strategy, where a vehicle must be able to determine the suitable context to change the current pseudonym in order to achieve unlinkability of pseudonyms, and maintain its privacy.
- Give a detailed description of a novel linkability attack, called cheating attack, and show its negative effect when applicable on the proposed pseudonym changing strategy.
- Propose a context-based cheating detection mechanism to confront the cheating attack. The cheating detection mechanism is responsible for efficiently detecting the malicious vehicles that launch the cheating attack, and checking the success of the pseudonym change. We show the impact of the mobility of vehicles on the performance of the cheating detection mechanism, and we present the solutions that counter the effect of mobility and increase the efficiency of the cheating detection mechanism.

The remainder of the chapter is organized as follows. In Section 5.2, we present the network and attacker models. The pseudonym changing strategy of CLPS is presented in Section 5.3. Section 5.4 presents the second contribution of CLPS in which we explain how the cheating attack works, and we introduce the cheating detection mechanism. Section 5.5 presents the security analysis of CLPS. The evaluation of CLPS performance along with a comparison of CLPS against different privacy schemes using the privacy extension, PREXT,

are discussed in Section 5.6. We conclude this chapter and point out future work in Section 5.7.

5.2. System and Privacy Models

In this section, we present the vehicular network, and formalize the privacy model.

5.2.1. Vehicular Network

We consider a typical VANET in a city environment, which consists of vehicles moving on the road, a Certification Authority (CA), and Road-Side Units (RSUs), as shown in Fig. 5.1.

- Vehicles: We assume each vehicle is equipped with an On-Board Unit (OBU) device, which is used to perform the V2X communications, and periodically broadcast beacons (e.g., 1-10 Hz). A beacon comprises a pseudonym, a timestamp, and the current vehicle state (i.e., position, velocity, and direction). We assume each vehicle is fitted with a Global Positioning System (GPS) receiver to provide the accurate position information, and a Tamper-Proof Device (TPD), which is used to store the vehicle's credentials, and run the cryptographic operations. We also assume each vehicle maintains a neighbors table that contains the states of vehicles located in its communication range (e.g., 300 m).
- Certification Authority (CA): CA is a fully trustable entity that is responsible of the initialization of the system, and the registration of vehicles by issuing and granting the vehicles' credentials, which consist of a family of pseudonyms and the corresponding key materials. For the purpose of preserving privacy, the CA must keep the relation of the pseudonyms to the driver's real identity secret. In case of dispute, the CA discloses this relation in order to revoke the mischievous vehicle.
- Road-Side Unit (RSU): RSU is deployed along the road to allow passing-by vehicles access to the CA and the back-end infrastructure.

In the following, we present the lifecycle of a vehicle in the VANET.

1. Vehicle Registration: Before joining the VANET, a vehicle v_i must register with the CA. To accomplish the vehicle registration, the CA runs the following steps.

Step 1. CA issues for v_i a large set of n pseudonyms $\{P_{i,k}\}_{k=1}^{n}$. Each pseudonym $P_{i,k}$ consists of a public key $K_{i,k}$.

Step 2. CA generates a private key $K_{i,k}^{-1}$ for each public key $K_{i,k}$.

Step 3. CA creates a public key certificate $Cert_{i,k}(K_{i,k})$ for each public/private key pair $(K_{i,k}, K_{i,k}^{-1})$.

Step 4. CA preloads the issued credentials into the pseudonyms pool that is stored in the TPD of v_i.

2. Use of Pseudonyms: When v_i joins the VANET, it selects a pseudonym from the pseudonyms pool, and uses it in the V2X communications to sign/verify the exchanged messages for a short period, and then changes it by a new pseudonym. The European standard ETSI TS 102 867 recommends changing a pseudonym every 5 min [79], and the American standard SAE J2735 recommends changing it every 120 s or 1 km [22]. We notice that pseudonyms have a short validity period and cannot be reused [48].

3. Pseudonyms Revocation: In case of liability issues, the conditional tracking is required, where the CA reveals the misbehaving vehicle's real identity in order to revoke it from the VANET system.

5.2.2. Privacy Model

In our privacy model, we consider how to protect a vehicle's location privacy against a Global Passive Adversary (GPA), where the GPA deploys low-cost radio receivers over the road network to passively eavesdrop and gather all exchanged messages in VANET. In addition, the GPA can use the spatiotemporal information contained in beacons to link subsequent pseudonyms, and reconstruct all vehicle traces. The GPA achieves this goal by using a multi-target tracker algorithm, such as NNPDA [140]. The GPA can then de-anonymize the reconstructed traces to breach the driver's location privacy. Note that, the GPA could be either internal or external.

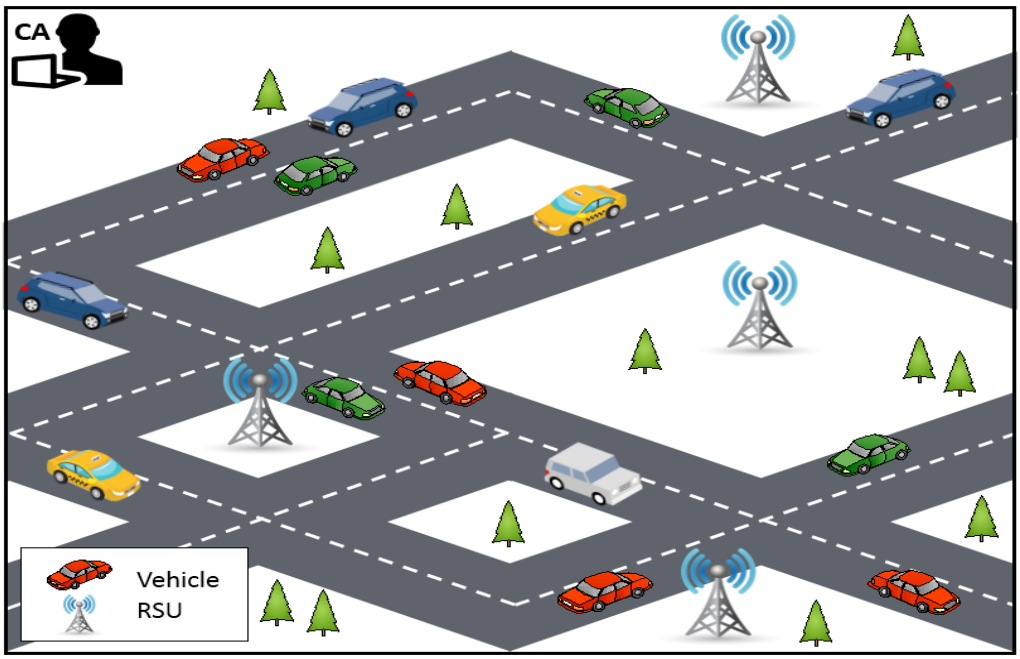

Figure 5.1: Vehicular network under consideration for CLPS

5.3. Context-based Pseudonym Changing Strategy

In this section, we present the first part of the proposed scheme CLPS, which consist of an effective Context-based Pseudonym Changing Strategy (CPCS), where a vehicle selects the appropriate context to enter silence and change its pseudonym in order to prevent linking the new pseudonym with the old one.

In order to successfully change the current pseudonym, the Subject Vehicle (SV) must fulfill the unlinkability requirements we outlined earlier in this thesis.

R-1. Simultaneity of Changing Pseudonym: to achieve this requirement, we propose that the SV should change its pseudonym along with at least k surrounding vehicles. The constant k is defined as the anonymity threshold, which is set in advance.

R-2. Concealment of Messages Information: in order to conceal the messages information from the adversary, we propose using the silent period technique before the change of pseudonym to ensure the discontinuity in the spatiotemporal information contained in beacons, and accordingly, confuse the adversary. Thus, it will have difficulties to match two pseudonyms, used successively by the same vehicle.

Fig. 5.2 presents the state diagram of the pseudonym lifecycle. When the SV joins the network, it fires a timer, called pseudonym timer (ptimer), to keep the current pseudonym for a minimum period of time, which is the requirement of position-based routing [141], such as

one minute. In fact, the use of changing pseudonyms has an impact on the position-based routing, which is an important task to achieve V2V communication needs, and keep the proper functioning of VANET applications. This issue has been addressed and discussed in [142]. When the ptimer expires, the SV must inform the neighboring environment that it is willing to change the current pseudonym. For this, the SV uses a flag, called change flag, which consists in a bit that indicates whether the SV is willing to change its pseudonym or not. This bit is sent with the beacon. Then, the SV starts a wait timer (wtimer), which defines the maximum age of the current pseudonym. In the meantime, the SV starts searching for the trigger by checking whether there are at least k neighbors of which change flags are all set to 1. Let N_{cf} denotes the set of neighbors of which change flags are set to 1. If the SV meets the trigger, it sends another flag, called ready flag, which consists in a bit that indicates that the SV has met the trigger, and requests the neighbors that did not meet the trigger to enter silent period and change their pseudonyms with the SV. Similarly, the ready flag like the change flag is sent with the beacon. Then, the SV enters silence to change the current pseudonym. The SV and the set of neighbors that change their pseudonyms with it form the Anonymity Set, which is denoted by AS, and the cardinality of the AS is called the Anonymity Set Size, which is denoted by ASS. In general, the anonymity of a vehicle is limited by the anonymity set size [143]. In fact, the larger the anonymity set size, the higher the anonymity achieved [55], [144]. If the SV does not meet the trigger before the wtimer expires, and receives a ready flag set to 1 from at least one of its neighbors in N_{cf}, it enters silent period to change pseudonym. If a vehicle with change flag set to 1 sends or receives a ready flag set to 1, it enters silence and changes pseudonym. In this way, an anonymity set of at least k silent vehicles (the anonymity threshold is reached) that change pseudonyms simultaneously is created to confuse the adversary, and achieve a high level of anonymity. When the silent period expires, the SV restarts the ptimer and resumes beaconing with a new pseudonym and change and ready flags set to 0 to restart the pseudonym change cycle from the beginning. If the wtimer expires and the SV does not meet the trigger and does not receive any ready flag during wtimer, it switches to silence and changes its pseudonym to avoid being tracked for an extremely long period.

In CPCS, a vehicle enters the silent mode and changes pseudonym in one of the following cases:

1. When it finds at least k neighbors with change flags set to 1 and sends ready flag set to 1.
2. When it receives a ready flag set to 1 from at least one of its neighbors with change flag set to 1.

This approach engenders an anonymity set AS of vehicles that enter silent period and change pseudonyms simultaneously. The entrance in silence mode is performed simultaneously by all the AS members. The period of silence can be the same for all vehicles (e.g., 11 s) or fixed for each vehicle or chosen randomly for each pseudonym change (using RSP scheme).

We can notice that, in CPCS, a vehicle does not announce that it is entering silent period to its neighbors. It immediately enters silent period after sending or receiving a ready flag set 1.

The advantage of using silent period is to increase the confusion of the adversary and improve the anonymity of the silent vehicle, because silent period does not allow the adversary to link old and new pseudonyms from the spatiotemporal information since no beacon is broadcasted during silence. We will discuss later the impact of using silent period on the scheme security and safety applications in Section 5.5.

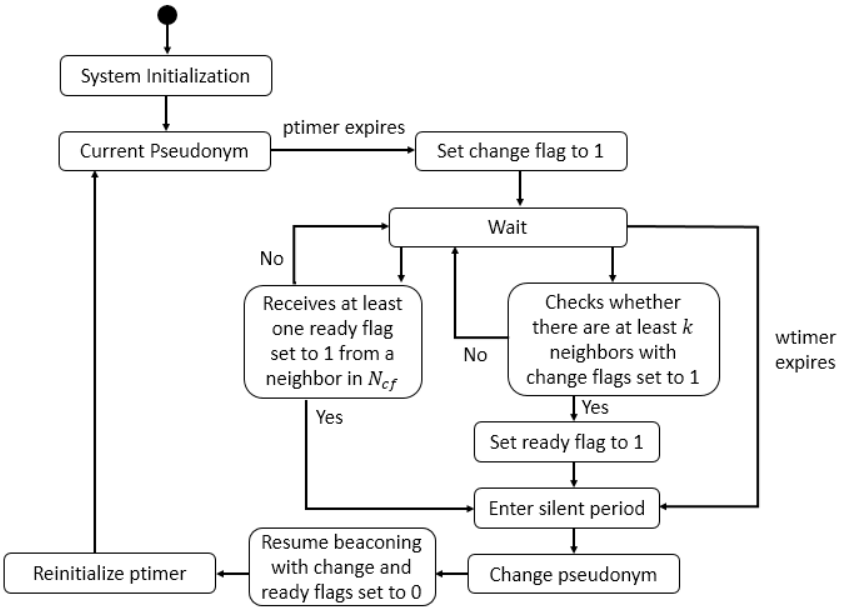

Figure 5.2: Pseudonym lifecycle state diagram for CLPS

5.4. Context-based Cheating Detection Mechanism

In this section, we present the second part of the proposed scheme CLPS in which we describe a novel linkability attack, called cheating attack, and we show its negative impact on the size of the anonymity set ASS, and how it degrades the performance of the proposed CPCS. In order to confront the cheating attack, we proposed developing a Context-based Cheating Detection Mechanism (CCDM), which assesses whether the pseudonym change was successful or not, and additionally detects the cheating vehicles in order to be locally blacklisted, and then evicted by the CA from the VANET system.

5.4.1. Cheating Attack

In the cheating attack, we assume that the adversary (i.e., compromised vehicle) deliberately generates beacons of which the change flag is constantly set to 1, in order to compel other vehicles to believe that it wants to change its pseudonym, whereas it does not intend to do so. Consequently, a vehicle that is looking for the trigger (k vehicles) considers the adversary among the k found neighbors, and will change the pseudonym.

The Table 5.1 shows the behavior of honest and malicious vehicles regarding the change of pseudonym. The honest vehicle is one that enters silence period and changes pseudonym, while the malicious vehicle (cheater) does the opposite, which makes it linkable all the time.

Table 5.1: Behavior of honest and malicious vehicles

Vehicle (Change Flag = 1)	Silent Period	Pseudonym Change
Honest	1	1
Malicious (Cheater)	1	0
	0	1
	0	0

The primary aim of the cheating attack is to reduce the ASS in order to decrease the confusions of the GPA, and facilitate matching subsequent pseudonyms, and thus decrease the location privacy level.

We consider that the pseudonym change fails when the ASS diminishes under the anonymity threshold k. Further, the more there are malicious vehicles (namely cheaters) in the network, the more the ASS decreases.

5.4.2. Cheating Detection Mechanism

After entering silent period, the SV initiates the cheating detection mechanism, which consists in two main parts:

1. Pseudonym Change Success Verification: since the change of pseudonym is exhibited to the cheating attack, the expected ASS, which should be worth the size of N_{cf}, may decrease under the specified anonymity threshold k, making the pseudonym change fail. Hence, the SV should verify (the success of the pseudonym change) if the change of pseudonym is successful or not, and might launch another change of pseudonym in case of failure. After each change of pseudonym, if the SV finds that the ASS is greater or equal to k, it considers that the pseudonym change has been accomplished with success, and then restarts the whole pseudonym change process from the beginning with the new pseudonym. Otherwise, if the ASS value is strictly less than k, the SV considers that the pseudonym change has failed and resets the change flag to 1 for resuming the pseudonym change cycle again. The Table 5.2 shows the different values that can take the ASS. In the presence of the cheating attack, the number of honest neighbors represents the ASS.

Table 5.2: Different values of the anonymity set size

Cheating Attack	ASS	Pseudonym Change
NO	$\lvert N_{cf} \rvert$	Successful
YES	$k \leq ASS \leq \lvert N_{cf} \rvert$	Successful
	$0 \leq ASS < k$	Failed

2. Malicious Vehicles Detection: the malicious vehicles detection process consists of differentiating between honest and malicious vehicles, and then adding the malicious vehicles into the local blacklist.

For cheating detection, we consider two types of neighbors:

1. Static Neighbors: in this case, we assume that a neighbor does not leave the communication range of the SV during the period of silence. We call this neighbor a *static neighbor*.

2. Changing Neighbors: here, we consider that a neighbor can leave the communication range of the SV during the period of silence. This neighbor is called a *changing neighbor*. Consequently, the frequent change of neighbors may negatively affect the performance of the cheating detection mechanism, especially in high mobility environments (e.g., freeway). In

fact, the vehicles that were part of the AS are not in range anymore and thus the cheating detection mechanism fails.

1. Static-aware CCDM (S-CCDM): In the following, we describe the different steps of the cheating detection mechanism by considering the existence of static neighbors.

According to the functional block diagram depicted in the Fig. 5.3, the cheating detection mechanism occurs in three steps.

1. Silent Period Check (SPC): after entering silent period, the SV starts the SPC procedure. Clearly, the neighbors whose change flags are set to 0 are not taken into consideration by the SV, while those which have change flags set to 1 could be honest or malicious. Rationally, all the neighbors belonging to N_{cf} should switch to silence to change their pseudonyms with the SV except for malicious neighbors (see Table 5.1). To distinguish malicious neighbors, the SV first checks if each neighbor $n_{cf} \in N_{cf}$ has entered silent period or not. For this, the SV monitors during the whole period of silence if each neighbor $n_{cf} \in N_{cf}$ is still broadcasting beacons or not. The neighbors that are still broadcasting beacons are considered as malicious since they did not enter silent period (see Table 5.1). The SV includes them in a List of Broadcasting neighbors (ListB), and then puts the content of this list into the local blacklist at the end of the SPC procedure (see Algorithm 1).

Algorithm 1

```
1:  procedure DumpList(List)
2:  begin
3:  if (List ≠ ∅) then
4:      PutBlacklist(List);
5:      List ← ∅;
6:  end if
7:  end procedure
```

The set of neighbors that have not sent beacons have entered silent period. The SV puts them in the List of Silent neighbors (ListS). In the following, we present the algorithm of the SPC procedure.

Algorithm 2

1: **procedure** SilentPeriodCheck(N_{cf})
2: **var**
3: n_{cf}: neighbor;
4: sp: silent period;
5: **begin**
6: **foreach** $n_{cf} \in N_{cf}$ **in parallel**
7: **if** (n_{cf} is broadcasting beacons during sp) **then**
8: $ListB \leftarrow ListB \cup \{n_{cf}\}$;
9: **else**
10: $ListS \leftarrow ListS \cup \{n_{cf}\}$;
11: **end if**
12: **end for**
13: DumpList($ListB$);
14: **end procedure**

2. Pseudonym Change Check (PCC): when the SV leaves silent period, it waits for an extra time t_{extra}, in such a way that the silent neighbors in ListS are all out of silent period. Then, the SV verifies whether those silent neighbors have changed their pseudonyms or not. For this, it has to check if they are still broadcasting beacons with their old pseudonyms or not. If a neighbor from ListS is still broadcasting beacons, which means that it did not change pseudonym after exiting silent period, the SV includes it in the list of Silent neighbors that keep the same pseudonym ListSsame. At the end of the PCC procedure, the ListSsame content is blacklisted. Otherwise, if a neighbor from ListS has disappeared, which means that it has changed its pseudonym, thus, it is considered by the SV as honest, and puts it into the List of Honest neighbors ListH, which composes with the SV the anonymity set AS.

Algorithm 3

1: After the extra time t_{extra} expires
2: **procedure** PseudonymChangeCheck($ListS$)
3: **var**
4: n_{silent}: neighbor;
5: **begin**
6: **foreach** $n_{silent} \in ListS$ **do**
7: **if** (n_{silent} is broadcasting beacons) **then**
8: $ListS_{same} \leftarrow ListS_{same} \cup \{n_{silent}\}$;
9: **else**
10: $ListH \leftarrow ListH \cup \{n_{silent}\}$;
11: **end if**
12: **end for**
13: DumpList($ListS_{same}$);
14: **end procedure**

3. Success Check (SC): the SV computes the number of honest neighbors, which represents the ASS, and compares it to the anonymity threshold k. The algorithm below shows the SC procedure.

Algorithm 4

```
1:  procedure SuccessCheck(ListH)
2:  begin
3:      if (|ListH| < k) then
4:          Call the pseudonym change procedure;
5:      end if
6:  end procedure
```

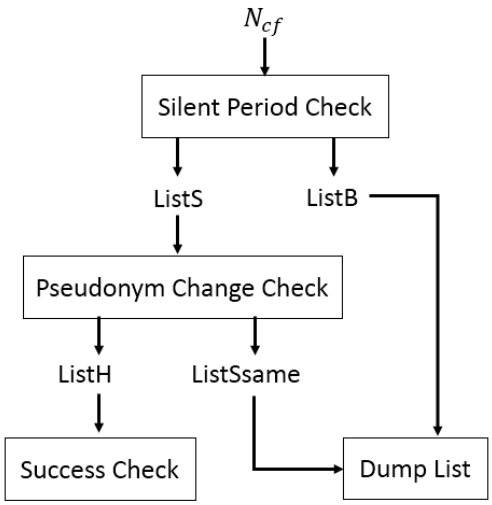

Figure 5.3: Cheating detection mechanism

2. Changing-aware CCDM (C-CCDM): Here, we consider the handling of the case where the neighbors of the SV may vary during the period of silence.

To ensure unlinkability of pseudonyms, the SV and the neighbors from the set N_{cf} enter silence at the same time to change pseudonyms, and constitute the anonymous set AS. However, some malicious neighbors in the set N_{cf} do not respect the rule, and skip entering silence or changing their pseudonyms.

When the SV enters silence, it checks whether neighbors from the set N_{cf} entered silence with it or not.

Clearly, the neighbors in the set N_{cf} that are still broadcasting beacons are considered as malicious (see Table 5.1).

Let $n_{cf} \in N_{cf}$ be a neighbor that stopped broadcasting beacons at the same time that the SV. At this time, stopping the broadcast of beacons by n_{cf} may be due to one of the two following cases:

- n_{cf} entered silent period.
- n_{cf} left the communication range of the SV.

It is possible, for example, to distinguish between these two cases from the last status of n_{cf} before it stops transmitting. The last status of n_{cf} indicates the position, velocity, and direction in the last beacon broadcasted by n_{cf}.

If the neighbor n_{cf} had approximately the same velocity as the SV, which means that n_{cf} did not leave its communication range, then the SV considers that n_{cf} has entered silent period.

Otherwise, if the velocity of n_{cf} is different from the velocity of the SV (with a large gap), the risk that n_{cf} has left the communication range of the SV becomes possible. The SV considers that n_{cf} has left the communication range in one of the three following cases:

First case:
- n_{cf} has the same direction as the SV.
- n_{cf} is located in the end of the communication range of the SV.
- The velocity of n_{cf} is greater than the velocity of the SV.

Second case:
- n_{cf} has the same direction as the SV.
- n_{cf} is located in the end of the communication range of the SV.
- The velocity of n_{cf} is less than the velocity of the SV.

Third case:
- n_{cf} is traveling in the opposite direction to the current traveling direction of the SV.
- n_{cf} is located in the end of the communication range of the SV.

The neighbors that left the communication range when the SV entered silence are not considered by the SV anymore; thus, the exclusion of these neighbors, and the malicious neighbors that did not enter silence diminishes the size of N_{cf}, which contains now only the

silent neighbors. Let $n_{cf}^{s} \in N_{cf}$ be a silent neighbor. During the period of silence, the SV changes the pseudonym. In the meantime, the silent neighbor n_{cf}^{s} could leave the communication range, change pseudonym or does not change pseudonym.

After period of silence, the SV resumes beaconing with a new pseudonym. Now, the SV has to make the difference between honest and malicious silent neighbors.

If the neighbor n_{cf}^{s} resumes beaconing with the same old pseudonym, the SV considers it as malicious. However, if n_{cf}^{s} disappeared, this means that it has left communication range or changed pseudonym. It is impossible to distinguish between these two cases from the last status of n_{cf}^{s}, since it could change during the period of silence. As a solution, we thought to attribute a unique number, called *pseudonym change number* to the SV and the group of neighbors from N_{cf}. When the SV and the neighbors from N_{cf} are formed, they have to cooperate to exchange, and agree on the pseudonym change number before they all enter silence. After exiting silence, each vehicle in the AS inserts the pseudonym change number in the beacon to announce that the pseudonym has been changed.

After exiting silence, the neighbors that did not leave communication range, and changed pseudonyms are visible to the SV owing to the pseudonym change number, and constitute with the SV the AS. We can see here that several neighbors have been excluded by the SV. The SV then computes the ASS, and announces a successful change of pseudonym if the ASS is greater than the anonymity threshold k, or requests another pseudonym change if the ASS is less than k.

If we use the pseudonym change number, it is possible to ignore the process of checking whether neighbors from the set N_{cf} that stopped broadcasting beacons have entered silence or left communication range. The SV first starts by excluding neighbors that did not stop broadcasting beacons (i.e, malicious neighbors). Then, it waits until the expiration of silent period to exclude the neighbors that keep their old pseudonyms (i.e., malicious neighbors), and compute the number of neighbors that resume beaconing with their new pseudonyms and the agreed pseudonym change number, which represents the ASS.

5.5. Security Analysis of the CLPS

The proposed CPCS permits to effectively change pseudonyms by achieving the unlinkability requirements that aim to augment the confusions of the GPA, and hardens linking pseudonyms.

The CPCS requires the cooperation between vehicles to ensure the simultaneity of changing pseudonyms. The cooperation needs the exchange of two flags inserted in beacons. The change flag permits to the SV to inform neighbors about pseudonym change, and assess its context to find the trigger (i.e., at least k vehicles with change flags set to 1). The ready flag is used to request the neighbors that did not meet the trigger to enter silence and change pseudonyms with the SV. The advantage of using ready flag is to prevent the reduction of the ASS, and to form an anonymous set $AS = \{SV\} \cup N_{cf}$, such that $|AS| = ASS \geq k + 1$, and of which all the elements enter silence and change pseudonyms simultaneously.

The concealment of messages information is achieved in CPCS by the use of silent period. Hence, the adversary cannot eavesdrop any information to link between the old and new pseudonyms of the same vehicle. However, in some cases, the risk of linkability of pseudonyms could be possible, and that depends on many factors such as road topology, velocity, duration of silent period, ASS, k, vehicle status before and after pseudonym change, adversary strength of tracking, etc. For example, the duration of silent period may have a negative impact on the pseudonym change.

In fact, if we choose a short silent period, an adversary may still locate the position of the target vehicle among the elements of the AS, because the probability that the target vehicle changes its position regarding the neighboring vehicles during a short silent period is very low. Therefore, the straight road structure and the shortness of silent period facilitate the detection of the target vehicle's position regarding other vehicles around. Otherwise, if the vehicles stay silent for a long time, an adversary can lose its target, because vehicles might be mixed during long silence, and can change their positions regarding each other. However, a long silent period may result in a network disconnection, and disrupt the communication.

As a solution, the SV can use a short silent period, and inform the driver about pseudonym change before it enters silence so that the driver makes the choice to change velocity or lane during silence to confuse the adversary, and avoid linkability of pseudonyms. However, this solution cannot be put in practice, since it requires sending many pseudonym change

notifications, and thus it annoys the driver. Another solution is to choose a long silent period to prevent linkability of pseudonyms, and break silence if any important event or situation that requires resuming communication happens or is about to happen such as road accident, collision, and pothole. Further, if the ASS is great enough, the CPCS can exclude some vehicles from the pseudonym change procedure. The CPCS would exclude $|AS| - k$ vehicles from the procedure. Those vehicles can be selected either randomly or based upon some characteristics like the distance separating them from the SV. The exclusion of the previous vehicles aims to alleviate the degradation of the network performance due to disconnection caused by long silent period. The last two solutions seem practical, and transparent to the driver compared to the first given solution. In addition, they ensure that the adversary get confused, and make linkabiliy of pseudonyms difficult, and also prevent the network disconnection problem.

Furthermore, we assume that a compromised vehicle can act as an internal adversary, and launch the cheating attack in order to reduce the ASS, and facilitate to the GPA to link pseudonyms. This attack mainly degrades the effectiveness of the proposed CPCS.

The objective of the adversary that launches the cheating attack is to decrease the ASS to facilitate the linkability of pseudonyms. The cheating attack is then considered as a linkability attack that threatens the pseudonym change approach proposed in CPCS. In [51], S. Zakhary *et al.* present several categories of privacy-related attacks. The proposed CPCS can also be subjected to the Sybil attack, especially since we assume that the pseudonyms are short lived with overlapping lifetimes. In the Sybil attack, when the minimum lifetime expires, the SV sends change flag, and starts waiting for the trigger. Here, a Sybil attacker can easily fool the SV into believing that there are multiple vehicles that are willing to change pseudonyms around its vicinity, whereas they do not exist at all. When the SV finds the trigger, it enters silence and changes pseudonym with the honest real neighbors. On the contrary, the Sybil fake vehicles controlled by the Sybil attacker do not do any action. Hence, the resulting ASS is reduced, which makes linkability of pseudonyms easier. The Sybil attacker can use valid pseudonyms to create fake vehicles, so that any receiver validates that the pseudonym is certified by the CA. We can see here that both Sybil and cheating attacks have a common goal, which is to fool the SV that the trigger is met so that the SV enters silence and changes pseudonym. This behavior reduces the ASS and the confusions of the adversary, and thus facilitates linking of pseudonyms. If the adversary can draw an anonymous trace of the target

vehicle by linking its pseudonyms, it can then launch social contact inference attacks to deanonymize the target vehicle's trace and find out the driver's identity. Then, the adversary can launch a location tracking attack against a particular vehicle to track the driver's path and compromise its privacy. The linkability attack (e.g., cheating attack, Sybil attack), the social contact inference attack and the location tracking attack are the main attacks that threaten directly the pseudonym change and users' privacy in VANETs. Considering the Sybil attack against CPCS, when the SV finds the trigger, it won't enter silence and change pseudonym as usual, because the trigger may include fake Sybil neighbors that cause a reduction in the ASS. So, at this stage, the SV keeps the current pseudonym, and tries to detect Sybil neighbors to eliminate them. To perform the Sybil detection, the SV needs connectivity to the back end infrastructure (i.e., CA) to detect if two different pseudonyms belong to the same vehicle or not. After Sybil detection, the SV eliminates Sybil neighbors and computes the cardinality of real neighbors set. If the cardinality of real neighbors set is greater or equal to k, the SV sends ready flag and then enters silence to change the current pseudonym with the real neighbors to constitute the AS. Otherwise, if the size of real neighbors set does not attain k, the pseudonym change is locked and the SV resumes the process of waiting for the trigger again.

As a solution to confront the cheating attack, we propose the CCDM, which lies on the vehicle's context to detect the malicious vehicles, and assess whether the change of pseudonym was successful or not.

For cheating detection, we have considered two different cases.

In the first case, the CCDM assumes that a neighbor stays in the communication range of the SV during silence period. Here, the detection of malicious vehicles can be performed in an efficient way, because it is simple to detect whether a neighbor has entered into a silent period or not, and whether it has changed pseudonym or not.

The second case takes into account the mobility of vehicles, and their speed variation, so a neighbor is able to leave the communication range of the SV at any moment. This case corresponds to the reality compared to the first one. Therefore, the high mobility of vehicles in VANET has an impact on the performance of the CCDM. In fact, the frequent changing of neighbors can degrade the performance of the CCDM, and thus it can fail. It is possible to avoid the problem of mobility by using the pseudonym change number as we explained in our contribution. In addition, to avoid the exclusion of neighbors that can leave communication

range, the SV can, for example, select only the neighbors which are in a radius of 100 m around it (with a communication range set to 300 m), and look for the trigger among this set of neighbors. In this way, the problem of leaving the communication range can be solved, and the SV can easily detect if a neighbor entered silence or not, since this neighbor will not leave the communication range during the whole silent period. For example, if the silent period is set to 5 s, and the velocity of the neighbor is 40 m/s, the distance traveled by the neighbor during silent period is 200 m; thus, a neighbor cannot leave the communication range, and will be detectable by the SV.

In Table 5.3, we carry out a comparison between the proposed scheme CLPS and other known pseudonym change schemes such as mix zones and *k*-anonymity obfuscation based approaches [51], [52], [53].

Regarding the SCP, the context mix algorithm [84], the RSP scheme [63], and the first proposal in CARAVAN [85] follow an individual pseudonym change behavior, and do not take into account the SCP, which does not prevent linkability of pseudonyms in the case where a vehicle changes its pseudonym alone. CLPS and most of the pseudonym change schemes in the literature propose a cooperative pseudonym change to allow changing pseudonyms simultaneously.

The OVCP feature considers that a vehicle that changed its pseudonym has previously intended to change it, and has not been forced to do it. For example, in SPCA [92], CAPS [114], CADS [115], and CLPS schemes, a vehicle uses a minimum pseudonym lifetime, and then starts searching for a trigger to change pseudonym in the right context. However, in CMIX [48], PCS [98], and UPCS [117] schemes, a vehicle is forced to change its pseudonym at a predetermined location (i.e., road intersection) even if it does not intend to change it. Also, in CPN [101], a vehicle that finds at least *k* neighbors request them to change their pseudonyms with it even if probably some of them have no intention to change their pseudonyms. This approach involves a lot of pseudonym changes and increases the number of changed pseudonyms, which negatively affects the proper functioning of communication protocols (e.g., routing), and long-term communication applications (e.g., file transfer or chat sessions).

The schemes that achieve the AVCP has the advantage to make all the vehicles that want to change their pseudonyms to be part of the anonymous set AS. CLPS and CPN schemes can

achieve this feature by using a ready flag to request the appropriate neighbors to change pseudonyms with the subject vehicle. The individual schemes cannot achieve this feature because there is no cooperation between vehicles to change pseudonyms simultaneously. Also, in SPCA, not all the k vehicles can find the trigger and change their pseudonyms with the subject vehicle. In mix zone schemes (e.g., CMIX and PCS), all the vehicles that enter the mix zone must change their pseudonyms, thus, they can achieve AVCP feature.

Most of the pseudonym change schemes including CLPS achieve the CMI unlinkability requirement. The schemes that does not consider this requirement cannot prevent the adversary from linking pseudonyms using the spatiotemporal information contained in beacons. The CMI requirement can be achieved either by silent period SP or encryption of messages information EMI. We can see from Table 5.3 that only the CMIX protocol uses symmetric encryption to hide messages information from the external adversary. The rest of the schemes use the silent period to prevent both external and internal adversaries from linking old and new pseudonyms.

The MWT mechanism was introduced in SPCA. The advantage of using the maximum wait time is to avoid being tracked for an extremely long period through the same pseudonym in the case where a vehicle cannot find the trigger to change pseudonym. CAPS, CADS and CLPS schemes have also used the MWT. The rest of schemes do not use it. Thus, some schemes (e.g., context mix algorithm and CPN) cannot handle the extreme case where a vehicle cannot find the trigger to change pseudonym for an extremely long time, consequently an adversary has more time to track the vehicle.

Only the context mix algorithm and the CLPS assess whether the change of pseudonym is successful after a pseudonym is changed. If the change of pseudonym is successful, the vehicle keeps the new pseudonym. Otherwise, it tries to change pseudonym again. The difference between CLPS and context mix algorithm in using the PCSC is that PCSC considers the change of pseudonym fails if a vehicle solely changes pseudonym in context mix algorithm, and if the ASS decreases below the specified anonymity threshold k in the presence of the cheating attack in CLPS.

Table 5.3: Comparative study between CLPS and pseudonym change schemes

Features and Functionalities	Context Mix Algorithm [84]	RSP [63]	CARAVAN [85]	CMIX [48]	SPCA [92]	PCS [98]	CPN [101]	CARAVAN [85]	CAPS [114]	CADS [115]	UPCS [117]	CLPS
SCP[1]	✗	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓
OVCP[2]	✓	✓	✗	✗	✓	✗	✗	✓	✓	✓	✗	✓
AVCP[3]	✗	✗	✗	✓	✗	✓	✓	✓	✓	✓	✓	✓
CMI[4]	✗	✓	✓	✓	✗	✗	✗	✓	✓	✓	✓	✓
SP[5]	✗	✓	✓	✗	✗	✗	✗	✓	✓	✓	✓	✓
EMI[6]	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗
MWT[7]	✗	✗	✗	✗	✓	✗	✗	✗	✓	✓	✗	✓
PCSC[8]	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓

[1]SCP: Simultaneity of Changing Pseudonyms.

[2]OVCP: Only the Vehicles that want to Change their Pseudonyms are considered for pseudonym change.

[3]AVCP: All the Vehicles that want to Change their Pseudonyms are part of the AS.

[4]CMI: Concealment of Messages Information.

[5]SP: Silent Period.

[6]EMI: Encryption of Messages Information.

[7]MWT: Maximum Wait Time.

[8]PCSC: Pseudonym Change Success Check.

5.6. Performance Evaluation

5.6.1. Simulation Setup

We created a road map of Laghouat university campus whose size of 1×1 km^2 (c.f., Fig. 5.4) using SUMO traffic simulator [145]. This road map is downloaded from OpenStreetMap [146], [147], and converted into a SUMO network using netconvert and polyconvert tools included in the SUMO 0.25.0 [148]. To generate the trips of vehicles, we used the randomTrips Python script [149]. The vehicle trips are generated with different arrival rates of 1, 1.6, and 2 vehicles per second, and the maximum speed is set to 50 km/h. We used the privacy extension, PREXT [129], for Veins simulator [130], [131] to implement our proposed scheme CLPS, and compare results with several privacy schemes implemented in PREXT: periodical pseudonym change [80], [82], random silent period (RSP) [63], CPN [101], and CAPS [114]. The Table 5.4 summarizes the simulation parameters.

Table 5.4: Parameters default values

	Parameter	Default Value
Simulation Environment	Road Traffic Simulator Network Simulator	SUMO Veins
Road Model	Map Size	Laghouat University Campus 1×1 km^2
Mobility Model	Vehicles Arrival Rate Speed Range	1 veh/s 1.6 veh/s 2 veh/s 0~50 km/h
VANET	Transmission Power Beacon Generation Interval	20 mW 1 s
CLPS Periodical RSP CPN CAPS	Minimum Pseudonym Lifetime Maximum Pseudonym Lifetime Anonymity Threshold Silent Period Radius Pseudonym Lifetime Pseudonym Lifetime Silent Period Radius Neighbors Threshold Minimum Pseudonym Lifetime Maximum Pseudonym Lifetime Silent Period Missed beacons silence threshold Neighborhood radius	60 s 120 s 2 11 s 100 m 60 s 60 s (3, 11) s 100 m 2 60 s 120 s (3, 13) s 2 beacons 50 m
Adversary	Eavesdropper Range Eavesdropper Overlap Track Interval	300 m 30 m 1 s
Simulation Run	Simulation Time	300 s

Figure 5.4: Laghouat university campus map

To evaluate the performance of CLPS, we consider the following privacy metrics supported by PREXT:

1. Mean Maximum Anonymity Set Size (meanMaxASS): the ASS represents the cardinality of the anonymity set AS. The AS of the SV is formed by the SV and its neighbors that change their pseudonyms together with the SV [101]. For the evaluation of our scheme, we take the maximum anonymity set size for each vehicle, and calculate the mean maximum anonymity set size $meanMaxASS$ as follows:

$$meanMaxASS = \frac{\sum_{i=1}^{|V|} maxASS_i}{|V|}$$

where $|V|$ stands for the number of vehicles in the network, and $maxASS_i$ represents the maximum ASS obtained by each vehicle appearing in the simulation.

2. Traceability (Π): the traceability of vehicles is calculated by counting the percentage of tracked vehicles. Formally, the traceability Π is defined in [115] as follows:

$$\Pi = \frac{1}{N}\sum_{v \in V} \lambda_v \times 100, \lambda_v = \begin{cases} 1, & \frac{\tau_v}{L(v)} \geq 0.90 \\ 0, & otherwise \end{cases}$$

where V represents the set of vehicles in the network and N is the total number of vehicles in the network. τ_v and $L(v)$ stand for the tracking period and the lifetime of the vehicle v, respectively.

3. Normalized Traceability (Π_n): the normalized traceability Π_n excludes the vehicles that never change their pseudonyms during their lifetime, since they are easily tracked by the adversary and reflected in the original traceability metric. Π_n is introduced and defined in [115] as:

$$\Pi_n = \frac{1}{N}\sum_{v \in V} \lambda_v^{norm} \times 100,\ \lambda_v^{norm} = \begin{cases} 1, & \frac{\tau_v}{L(v)} \geq 0.90 \wedge psd(v, k_0) \neq psd(v, k_0 + L(v)) \\ 0, & otherwise \end{cases}$$

where $psd(v, k_0)$ and $psd(v, k_0 + L(v))$ are the pseudonyms of the vehicle v at the first and last time steps in its lifetime, respectively.

4. Mean Maximum Entropy (meanMaxEntropy): the entropy is a privacy metric used to measure the anonymity of a vehicle in the anonymity set. It allows expressing the adversary's

knowledge about each vehicle in the anonymity set. Formally, the entropy, denoted by H, is calculated as follows:

$$H = -\sum_{i=1}^{V} p_i . \log p_i$$

where V is the number of the vehicles in the anonymity set, such that $V = |AS|$, and p_i is the probability assigned by the adversary for each vehicle i in the anonymity set AS to be the target such that $\sum_{i=1}^{V} p_i = 1$.

In our experiments, we choose to measure the maximum entropy H_{max}^{i} for each vehicle i, and determine the mean maximum entropy $meanMaxEntropy$ as follows:

$$meanMaxEntropy = \frac{\sum_{i=1}^{V} H_{max}^{i}}{V}$$

5.6.2. Results

To study the impact of the proposed scheme CLPS on the simultaneous pseudonym change, we calculate the mean maximum anonymity set size obtained for CLPS, Periodical, RSP, CPN, and CAPS schemes by varying the arrival rate. We generate three arrival rates of 1, 1.6 and 2 vehicles per second. We ran multiple simulations, and we obtained the simulation results shown in Fig. 5.5.

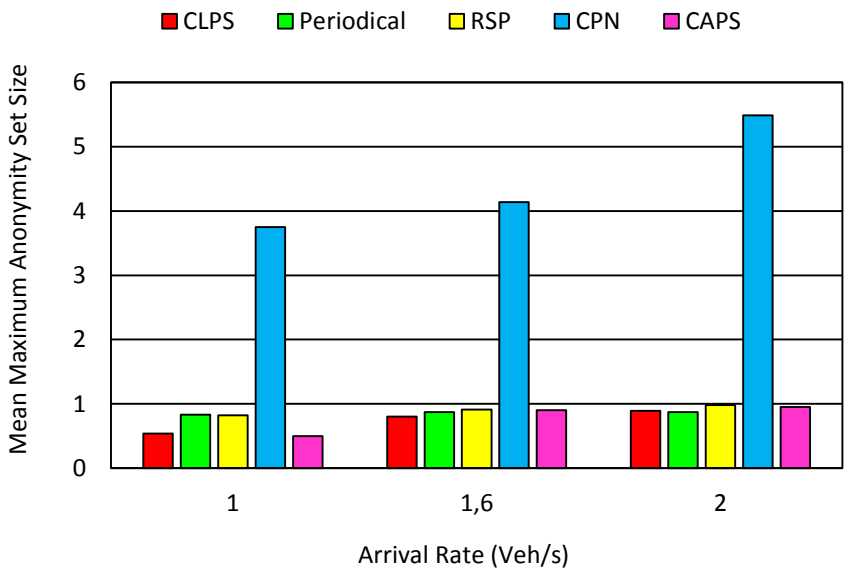

Figure 5.5: Mean maximum anonymity set size of the privacy schemes in various arrival rates

Fig. 5.5 presents the mean maximum anonymity set size versus the arrival rate. We can see from the figure that the mean maximum ASS is reduced in CLPS, Periodical, RSP and CAPS schemes compared to CPN scheme. The reason is that Periodical and RSP schemes adapt an individual behavior to change pseudonym, thus it's rare where a vehicle changes its pseudonym with at least one neighbor. CLPS and CAPS schemes cannot increase the mean maximum ASS compared to CPN scheme, which represents good results by completing a mean maximum ASS exceeding the specified neighbors' threshold 2. The reason is that, in CLPS and CAPS, a vehicle has always to keep its pseudonym for a minimum pseudonym lifetime before it starts searching for the trigger to change pseudonym. However, in CPN, a vehicle changes pseudonym as soon as it finds at least two neighbors in its entourage. Therefore, CLPS and CAPS do not look for the trigger during the whole minimum pseudonym lifetime, thereby reduce the period the vehicle searches for the trigger in the simulation scenario. On the contrary, CPN continuously searches for the trigger during the whole simulation, and thus, there are more simultaneous pseudonym changes compared to CLPS and CAPS. Moreover, in CPN, a vehicle always changes its pseudonym with at least two neighbors whereas, in CLPS, the trigger is more difficult to find compared to CPN because it consists in finding at least two neighbors that broadcast change flags set to 1 (i.e., one more condition) in order to change the pseudonym with them. Also, in CAPS, a vehicle should find at least one silent neighbor to be able to enter silence and change its pseudonym. Thus, in the simulated scenario for CLPS and CAPS, it was probably difficult to find the trigger for the majority of vehicles, which leads them most of the time to change their pseudonyms individually at the expiration of the maximum pseudonym lifetime. Furthermore, we can see that the mean maximum ASS increases by increasing the arrival rate for all five privacy schemes, because when the number of neighbors increases, the ASS increases for each vehicle.

To evaluate the performance of the proposed scheme CLPS in reducing traceability, we measure the traceability of vehicles for CLPS, Periodical, RSP, CPN, and CAPS schemes by varying the arrival rate. We generate three arrival rates of 1, 1.6 and 2 vehicles per second. We ran multiple simulations, and we obtained the simulation results as shown in Fig. 5.6.

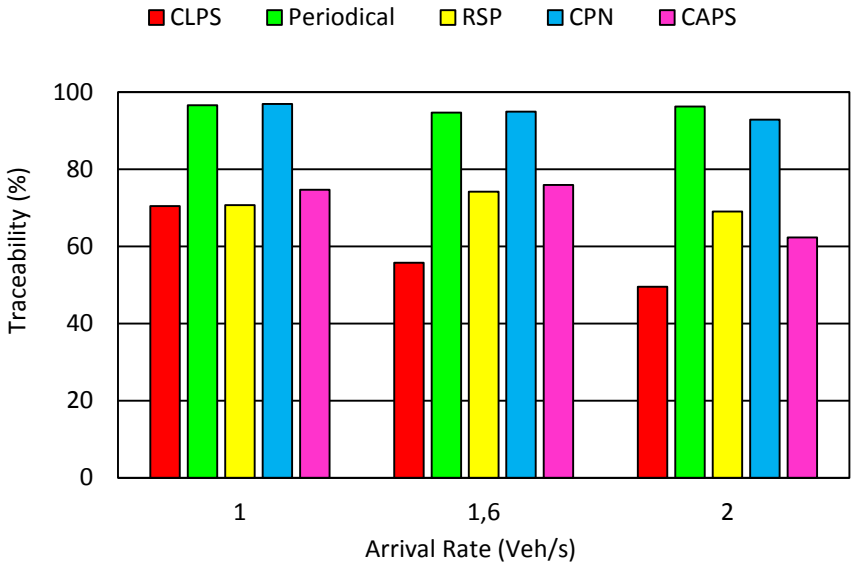

Figure 5.6: Traceability of the privacy schemes in various arrival rates

Fig. 5.6 shows the traceability level for CLPS, Periodical, RSP, CPN, and CAPS schemes in various arrival rates. From the figure, we can see that the periodical and CPN schemes cannot reduce the level of traceability regardless the arrival rate, because they do not use the silent period technique. The tracker can then use the spatiotemporal information broadcast in beacons to link pseudonyms, and reconstruct the vehicles' traces. The silent period-based schemes CLPS, RSP, and CAPS can reduce traceability due to the silent periods, but with different levels. RSP and CAPS schemes reduce traceability a little bit compared to CLPS. The reason is that RSP scheme adapts an individual pseudonym change behavior, and it is a low probability that at least two vehicles change pseudonyms simultaneously. CAPS takes into account the simultaneity of changing pseudonyms, but cannot reduce traceability as CLPS. This is because CAPS varies the length of the silent period according to the context while in CLPS it is fixed to 11 s. CLPS reasonably reduces the traceability, since it takes into consideration the simultaneity of changing pseudonyms and a reasonable value for silent period to confuse the adversary. Thus, the reduction in traceability is closely related to the duration of the silent period. In fact, the traceability is significantly reduced with the increase of the silent period. From the figure, we can also see that with increasing the arrival rate, the traceability reduces for all five schemes, because a larger arrival rate augments the chance of changing pseudonym with more vehicles, which makes linkability of pseudonyms more difficult for the tracker, and thus results in a reduction in traceability. Moreover, we can see from the figure that the traceability level is significantly reduced by increasing the arrival rate in CLPS compared to other privacy schemes. That is because CLPS selects the effective

context to enter silence and change pseudonym. Also, compared to RSP and CAPS schemes, the silent period in CLPS is set to 11 s, which is apparently of sufficient value to confuse the tracker, and reduce the level of traceability.

To show the effectiveness of the proposed scheme CLPS, we choose to compare it with Periodical, RSP, CPN, and CAPS schemes in terms of normalized traceability. Here, we choose three different arrival rates of 1, 1.6 and 2 vehicles per second. We conducted a set of simulations, and obtained the results as presented in Fig. 5.7.

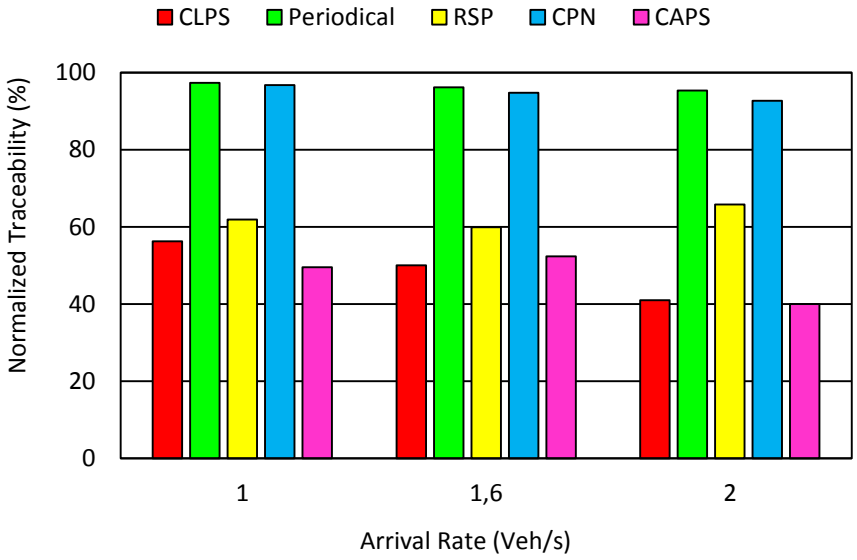

Figure 5.7: Normalized traceability of different privacy schemes in three different arrival rates

In Fig. 5.7, CLPS, Periodical, RSP, CPN, and CAPS privacy schemes are evaluated in terms of the normalized traceability by varying the arrival rate. Recall that the normalized traceability neglects the vehicles that have not changed their pseudonyms during their lifetime, and were tracked by the adversary. So effectively, the results in Fig. 5.7 show that the normalized traceability is reduced for all five privacy schemes compared to the results obtained for the traceability metric (see Fig. 5.6). Moreover, we can see that the silent period-based schemes CLPS, RSP, and CAPS show good results in reducing the normalized traceability compared to Periodical and CPN regardless the arrival rate due to the silent periods. The proposed scheme CLPS and CAPS show better results compared to RSP scheme by remarkably reducing the normalized traceability for all arrival rates. That is because CLPS and CAPS take into account the simultaneity of changing pseudonyms, and choose the right context to cause tracker confusions, whereas the RSP scheme has individual pseudonym change behavior, and uses a random silent period. Also, we can see that CLPS scheme

reduces normalized traceability significantly up to 40% with an arrival rate of 2 vehicles per second. Therefore, a larger vehicle density and a longer silence period can reduce the traceability level, and improve the privacy of vehicles.

In order to see if the proposed scheme CLPS affects the simultaneous pseudonym change, we choose to vary the anonymity threshold k to measure the mean maximum ASS in different arrival rates 1, 1.6, and 2 vehicles per second. We performed multiple simulations of CLPS, and obtained the results presented in Fig. 5.8.

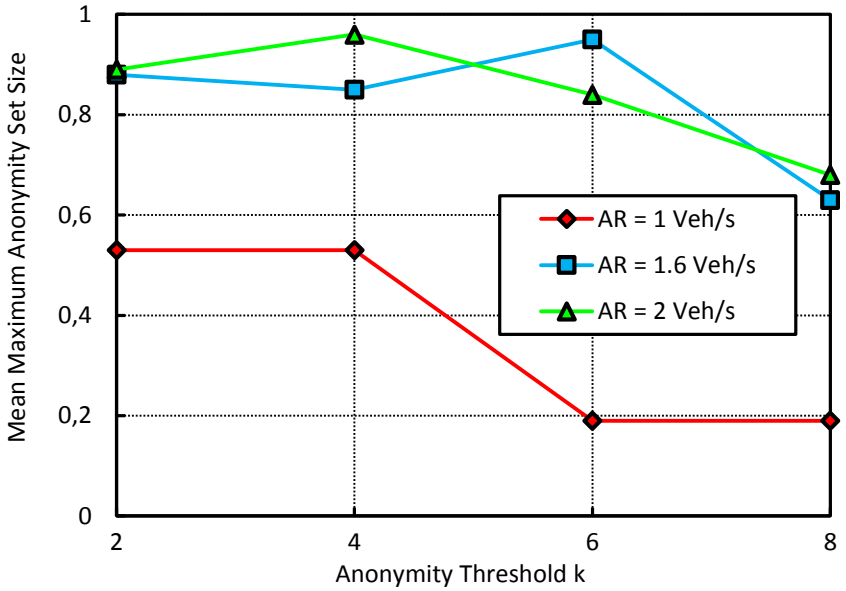

Figure 5.8: Mean maximum anonymity set size for various values of the anonymity threshold k with different arrival rates

Fig. 5.8 presents the mean maximum anonymity set size for the proposed scheme CLPS by varying the anonymity threshold k for different arrival rates. We can see from the figure that the mean maximum ASS reduces by increasing the anonymity threshold k regardless the arrival rate, because with a large k, it is more difficult for a vehicle to find the trigger in its vicinity. Thus, most of the vehicles in the simulation may change their pseudonyms individually at the end of the maximum pseudonym lifetime, which obviously reduces the mean maximum ASS. In addition, we can see that the increase in the arrival rate contributes to increase the mean maximum ASS. The reason is that with a large number of vehicles, a vehicle has more chance to meet the trigger in its neighborhood and thus it performs more simultaneous pseudonym changes, which augments the mean maximum ASS.

To show the impact of the period of silence on the traceability level for the proposed scheme CLPS, we decide to calculate the traceability by varying the silent period from 5 to 11

with increase of 2 in various arrival rates 1, 1.6, and 2 vehicles per second. We carried out multiple simulations of CLPS, and got the simulation results that can be seen in Fig. 5.9.

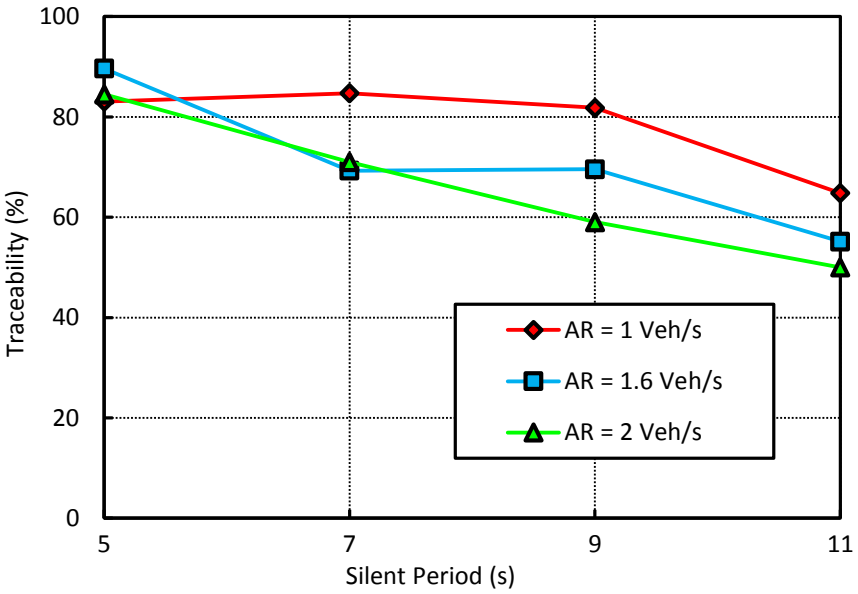

Figure 5.9: Traceability of CLPS versus silent period with different arrival rates

Fig. 5.9 presents the traceability of vehicles under different silent periods for the proposed scheme CLPS in different arrival rates. The figure shows that the traceability decreases as the silent period increases regardless the arrival rate, this is because the prolongation in the period of silence augments tracker confusions, and thus reduces the traceability level. Also, in the variation of the arrival rates, we can see that the CLPS significantly reduces the traceability level by increasing the arrival rate especially in longer silence periods thanks to the huge amount of traces that work on confusing the tracker. Consequently, the increase in silent period and vehicles density result in a reduced traceability, and permit to achieve better anonymity.

To investigate the level of entropy achieved by the proposed scheme CLPS, we evaluate the mean maximum entropy for CLPS, Periodical, RSP, CPN, and CAPS schemes in various arrival rates. We run multiple experiments, and obtain results shown in Fig. 5.10.

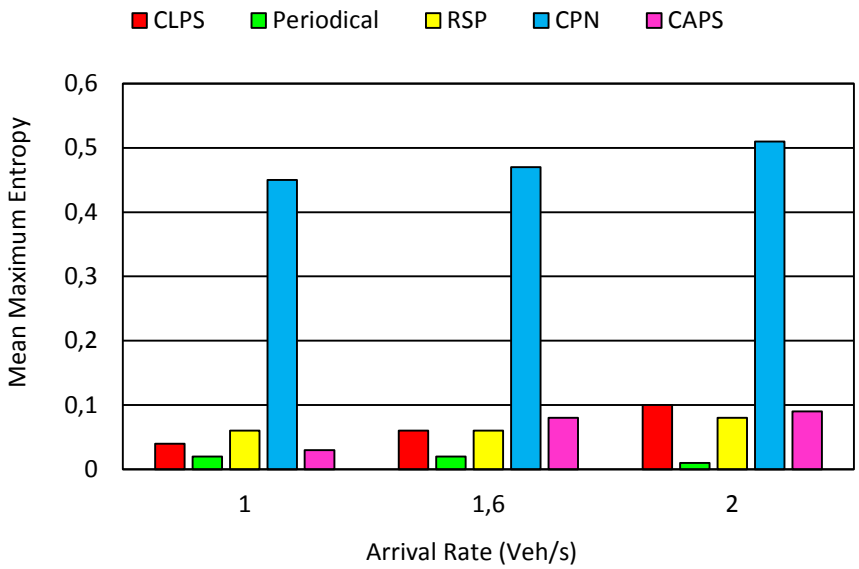

Figure 5.10: Mean maximum entropy of the privacy schemes in various arrival rates

Fig. 5.10 shows the results of the mean maximum entropy obtained for CLPS, Periodical, RSP, CPN, and CAPS schemes in various arrival rates. It can be seen from the figure that CPN scheme significantly increases the mean maximum entropy compared to other schemes regardless the arrival rate. The reason is that, in CPN, there is no individual pseudonym change. Thus, a vehicle always changes its pseudonym with at least k neighbors, which leads to large entropy values. On the contrary, RSP and Periodical schemes are individual schemes, and CLPS and CAPS schemes adapt most of the time an individual behavior as explained in the results of Fig. 5.5. Therefore, we conclude that the individual behavior lowers the entropy. Moreover, CLPS, RSP and CAPS schemes slightly increase the mean maximum entropy compared to Periodical scheme for all arrival rate scenarios, because of using silent periods. Also, from the figure, we can observe that the mean maximum entropy increases with the increase of the arrival rate for all five schemes. The reason is that, with a big arrival rate, a large number of vehicles moves on the map, which increases the chance of changing the pseudonym with more vehicles, and thus increases entropy.

To study the impact of the minimum and maximum pseudonym lifetimes on the traceability level, we calculate the traceability obtained for the proposed scheme CLPS by varying the minimum and maximum pseudonyms lifetimes. Here, the arrival rate is set to 1 vehicle per second. We run multiple experiments, and obtain the results shown in Fig. 5.11.

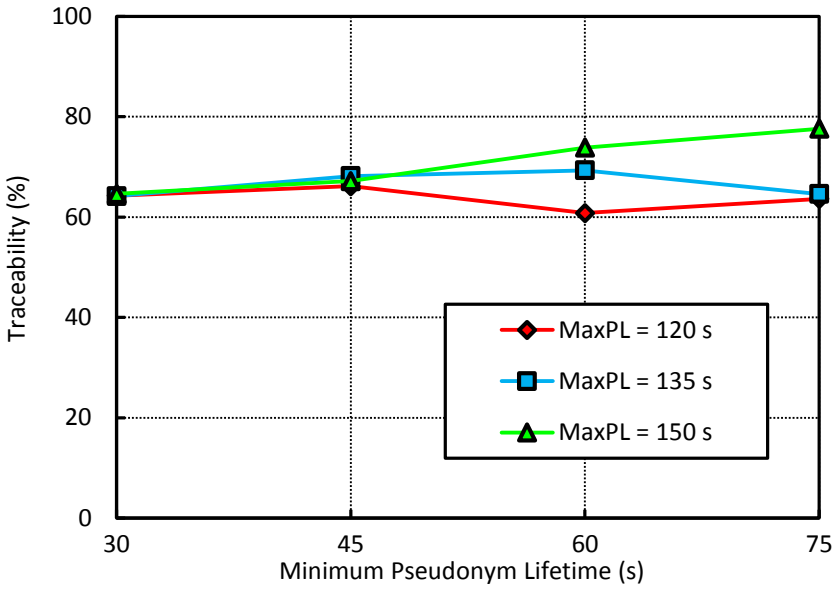

Figure 5.11: Traceability of CLPS in different pseudonym lifetimes

Fig. 5.11 shows the achieved traceability level of the proposed scheme CLPS in variant pseudonym lifetimes. We can see that the increase in the minimum pseudonym lifetime slightly increases the traceability level. Also, the increase in the maximum pseudonym lifetime increases a little bit the traceability level. The reason is that with large pseudonym lifetimes, a vehicle tends to keep the current pseudonym for a longer period of time as long as it does not find the trigger. This behavior causes a reduction in the number of pseudonym changes, and thus reduces the adversary confusions, which augments the traceability level.

5.7. Summary

In this chapter, we presented CLPS to protect the privacy of users in VANETs. CLPS consists of two main parts: (1) CPCS lets the vehicle select the effective context to enter silent period and change pseudonym. In this way, the vehicle achieves the unlinkability requirements, which permit to confuse the adversary, and avoid the linkability of pseudonyms. (2) CCDM checks the success of the pseudonym change, and detects the compromised vehicles that launch the cheating attack to degrade the performance of the proposed pseudonym changing strategy CPCS. We evaluate the performance of the proposed scheme CLPS by simulation study and compare it with Periodical, RSP, CPN, and CAPS schemes. The results show that CLPS is significantly more efficient than other schemes in terms of traceability and normalized traceability privacy metrics. However, CLPS cannot increase the mean maximum ASS compared to CPN. Thus, the ASS is not a suitable privacy metric, and cannot show whether the adversary succeeded in tracking a vehicle during its

lifetime or not. In addition, the results show that a high density and the achievement of the unlinkability requirements with a relatively long silent period permit to reduce traceability, and enhance the privacy of users in VANETs. In future work, we will carry out more experiments by testing other parameters to see their impact on the effectiveness and robustness of CLPS in improving the location privacy of users in VANETs. We also plan to study the impact of using silent period on the network connectivity (e.g., safety applications).

6 Framework for Privacy Preservation in VANETs

6.1. Introduction

In the previous chapter of this PhD thesis, we have presented the Context-based Location Privacy Scheme (CLPS), which provides two major contributions: (1) a pseudonym changing strategy CPCS and (2) a cheating detection mechanism CCDM. These two contributions need to be structured in the form of modules that interact with each other, and with other entities via V2X communications. This structure constitute an overall framework for better understanding and clarifying our contributions. Therefore, the main goal of this chapter is to propose a general framework that focus on the privacy preservation in VANETs. The remainder of the chapter is organized as follows. In Section 6.2, we present the architecture of the framework that contains different inputs and modules. Then, we give a detailed description of each module of the framework, and its interactions with other modules and other entities in the VANET, and following that, we provide the algorithm run by each module in the framework. Finally, we conclude this chapter in Section 6.3.

6.2. Framework for Privacy Preservation

In this section, we present the framework of our contributions in CLPS.

6.2.1. Framework Design

Here, we provide the framework design, as shown in Fig. 6.1.

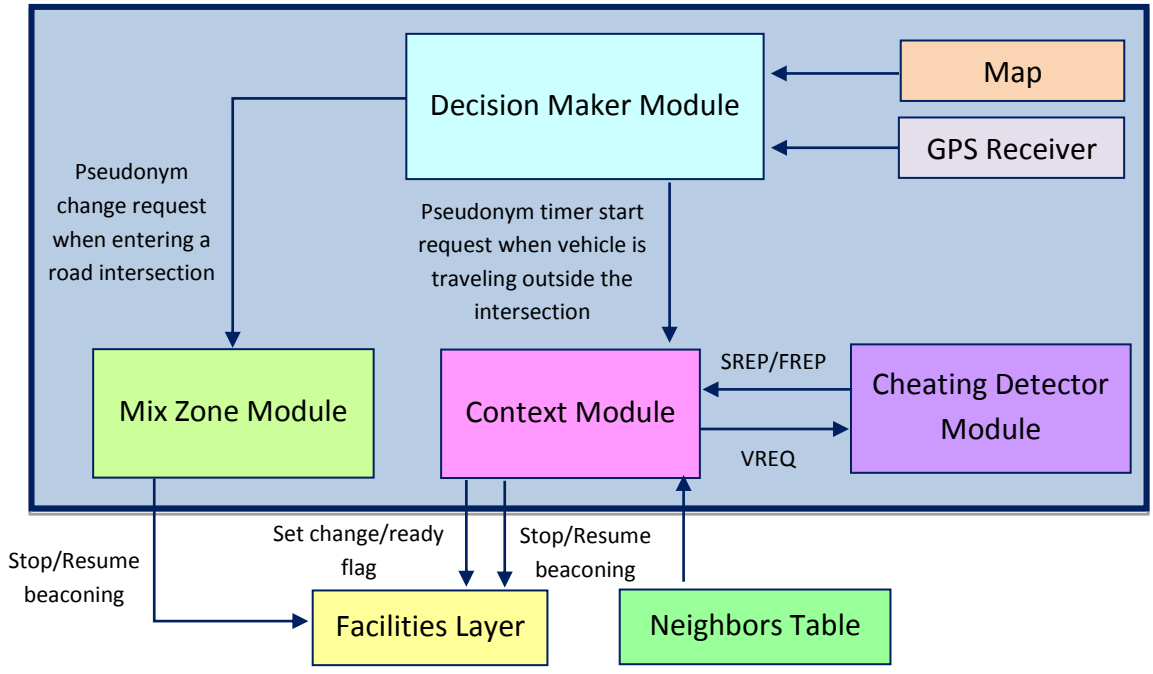

Figure 6.1: Framework design for privacy preservation in VANETs

The framework design for our scheme requires the insertion of four main modules in the security layer of the ITS communication architecture.

- Context Module (CM): the CM runs a context-based pseudonym changing algorithm when needed.
- Mix Zone Module (MZM): the MZM runs a mix zone pseudonym changing algorithm when needed.
- Cheating Detector Module (CDM): this module validates or cancels the pseudonym change operation.
- Decision Maker Module (DMM): the DMM gives the order based on many factors (maps, GPS, etc.) to change the pseudonym to the CM or MZM.

The CM needs to know the context of the vehicle (i.e., the neighborhood information). Thus, the framework has as an input the neighbors table to collect the necessary information for changing the pseudonym. The neighbors table is constructed from the beacons received from other vehicles, nearby RSUs, and the CA.

6.2.2. Framework Description

Our proposed framework consists of four main modules. Here, we give the functionalities of each module in the framework.

- Context Module: the CM is responsible for identifying the appropriate times for changing pseudonyms, and ensures the cooperation between vehicles to successfully change the pseudonym. The DMM first sends a pseudonym timer start request to the CM when the vehicle is moving outside the intersection. Upon the receipt of the request, the CM fires the pseudonym timer ptimer to keep the current pseudonym for a minimum pseudonym lifetime. When the ptimer expires, the CM requests the facilities layer to set the change flag to 1 in the issued beacons to inform other vehicles that the vehicle wants to change its pseudonym. Meanwhile, the CM looks for the trigger (i.e., at least k vehicles with change flag set to 1) from the neighborhood information (i.e., change flag) obtained from the neighbors table. The CM sends a request to the facilities layer to stop beaconing for a certain period (i.e., enter silent period), and changes the pseudonym in one of the following cases:
  1. If the CM finds the trigger and requests the facilities layer to set the ready flag to 1 in the issued beacons.

2. If the CM does not find the trigger and receives at least a ready flag from one of the vehicles with change flag set to 1.

After expiry of the silent period, the CM sends a request to the facilities layer to resume beaconing with the new pseudonym.

For each change of pseudonym, the CM solicits the CDM by sending a Verification Request (VREQ) after entering silent period so that the CDM initiates the pseudonym change success verification, and the malicious vehicles detection. When the CDM accomplishes its task, it replies the CM by sending a Success Reply (SREP) if the pseudonym change is successful or a Failure Reply (FREP) in the case where the pseudonym change fails.

- Mix Zone Module: the MZM receives a pseudonym change request from the DMM when the vehicle enters a road intersection. For the pseudonym change, the MZM should send a request to the facilities layer to stop beaconing for a certain period (i.e., enter silent period). The duration of the silent period can be fixed or varied according to the road intersection structure (e.g., delay characteristics, trajectory of the vehicle in the intersection). After sending the silent period request, the MZM changes the current pseudonym to a new pseudonym. Then, when the silent period expires, the MZM sends a new request to the facilities layer asking it to resume beaconing. In this way, the road intersection becomes then a silent mix zone where vehicles enter silent period and change their pseudonyms simultaneously.
- Cheating Detector Module: the CDM checks the success of the pseudonym change procedure, and might request another pseudonym change in case of failure. The CDM also can detect the malicious vehicles that are responsible for launching the cheating attack.
- Decision Maker Module: the DMM sends a pseudonym change request to the MZM if the vehicle enters a road intersection or a pseudonym timer start request to the CM if the vehicle is traveling outside the intersection. The DMM makes this decision based on the current position of the vehicle on the road map.
- Map: the Map module stores the road map, which is used to locate the vehicle according to its current position.
- GPS Receiver: the GPS Receiver module provides the accurate position of the vehicle to the DMM.

- Facilities Layer (FL): the facilities layer is responsible for generating/receiving beacons that are used for changing pseudonyms.
- Neighbors Table (NT): the neighbors table contains the state information about each neighboring vehicle (e.g., pseudonym, position, speed, change flag, ready flag, etc.). The neighbors table must be updated as vehicles move out of range of each other.

6.2.3. Framework Operation

In this section, we provide the implementation details for each component in the framework.

1. Decision Maker Module

Algorithm 1 shows the procedure of the DMM. Note that the SV uses this algorithm every time step in order to decide on the next pseudonym change whether mix zone or context.

Algorithm 1

```
1:  procedure decision_maker()
2:  begin
3:  i ← intersection(current_position);
4:  if (i) and (not lock) then
5:      send_psd_change_req();
6:      lock ← true;
7:  else
8:      if (not lock) then
9:          send_ptimer_start_req();
10:         lock ← true;
11:     end if
12: end if
13: end procedure
```

2. Mix Zone Module

Algorithm 2 provides the procedures of the MZM, which are run upon the receipt of the pseudonym change request from the DMM.

Algorithm 2

```
1:  procedure mix_zone()
2:  begin
3:  send_stop_beacon_req();
4:  schedule_at(sim_time() + silent_period, exit_silent_evt);
5:  set_current_psd(get_new_psd());
6:  end procedure

1:  procedure handle_self_msg(msg)
2:  begin
3:  send_resume_beacon_req();
4:  while (i)
5:      i ← intersection(current_position);
6:  end while
7:  lock ← false;
8:  end procedure
```

3. Context Module

Algorithm 3 provides the procedures of the CM, which are run upon the receipt of the pseudonym timer start request from the DMM.

Algorithm 3

```
1:  procedure context_psd_change()
2:  begin
3:  schedule_at(sim_time() + min_psd_time, change_psd_evt);
4:  schedule_at(sim_time() + max_psd_time, time_out_evt);
5:  while (i)
6:      i ← intersection(current_position);
7:  end while
8:  lock ← false;
9:  end procedure

1:  procedure handle_self_msg(msg)
2:  begin
3:  switch (msg → get_kind())
4:      case CHG_PSD:          change_flag ← true;
5:                             break;
6:      case ENTER_SILENT:     send_stop_beacon_req();
7:                             schedule_at(sim_time() + silent_period, exit_silent_evt);
8:                             set_current_psd(get_new_psd());
9:                             change_flag ← false;
10:                            ready_flag ← false;
11:                            set_ready_flag_received ← false;
12:                            break;
13:     case EXIT_SILENT:      send_resume_beacon_req();
```

```
14:                          if (lock) then
15:                             schedule_at(sim_time() + min_psd_time, change_psd_evt);
16:                             schedule_at(sim_time() + max_psd_time, time_out_evt);
17:                          end if
18:                          break;
19:     case TIME_OUT:       schedule_at(sim_time(), enter_silent_evt);
20:                          break;
21:   end procedure

1:    procedure send_beacon(bcn)
2:    if (change_flag) then
3:       if (ready_flag or set_ready_flag_received) then
4:          time_out_evt ← cancel_evt(time_out_evt);
5:          schedule_at(sim_time(), enter_silent_evt);
6:       else
7:          if (nneighbors_set_chg_flag ≥ k) then
8:             ready_flag ← true;
9:             nneighbors_set_chg_flag ← 0;
10:         end if
11:      end if
12:   end if
13:   bcn → set_change_flag(change_flag);
14:   bcn → set_ready_flag(ready_flag);
15:   end procedure

1:    procedure receive_beacon(bcn)
2:    if (bcn → get_ready_flag()) then
3:       set_ready_flag_received ← true;
4:    end if
5:    if (change_flag) then
6:       if (bcn → get_change_flag()) then
7:             nneighbors_set_chg_flag ← nneighbors_set_chg_flag + 1;
8:       end if
9:    end if
10:   end procedure
```

4. Cheating Detector Module

Algorithm 4 provides the procedures of the CDM, which are run upon the receipt of a VREQ from the CM.

Algorithm 4

```
1:    procedure dump_list(list)
2:    begin
3:    if (list ≠ ∅) then
4:       put_blacklist(list);
5:       list ← ∅;
6:    end if
7:    end procedure

1:    procedure silent_period_check(N_cf)
2:    var
```

```
    n_cf: neighbor;
    sp: silent period;
begin
foreach n_cf ∈ N_cf in parallel
    if (n_cf is broadcasting beacons during sp) then
        listB ← listB ∪ {n_cf};
    else
        listS ← listS ∪ {n_cf};
    end if
end for
dump_list(listB);
end procedure
```

```
After the extra time t_extra expires
procedure pseudonym_change_check(listS)
var
    n_silent: neighbor;
begin
foreach n_silent ∈ listS do
    if (n_silent is broadcasting beacons) then
        listS_same ← listS_same ∪ {n_silent};
    else
        listH ← listH ∪ {n_silent};
    end if
end for
dump_list(listS_same);
end procedure
```

```
procedure success_check(listH)
begin
    if (|listH| < k) then
        Call the pseudonym change procedure;
    end if
end procedure
```

6.3. Summary

The last chapter of the thesis is devoted to the development of a complete framework for the privacy preservation in VANETs. This framework represents a global architecture of the contributions of this thesis and concludes the research work of this PhD. In addition, the framework contains and regroups several entries and modules. Each module has a specific task to run when it is needed at the right time and in the right place, and can interact with other modules of the same architecture as well as with other entities of the VANET (e.g., vehicle, RSU) through inter-vehicular communications (sending and receiving messages).

7 Conclusions and Future Work

In this last chapter, we recapitulate our contributions in this thesis and reveal our future work.

7.1. Contributions

The major contributions of this thesis can be summarized as follows:

- First, we proposed a pseudonyms generation protocol, called PGP, for VANETs. This protocol permits to ensure pseudonymous protection against the damage caused by vehicle theft by the use of a connection card, which always accompanies the driver and in which the generated pseudonyms are stored. The driver uses the connection card to connect to the VANET system.
- Second, we proposed a Context-based Pseudonym Changing Strategy (CPCS) for the privacy protection in VANETs. In this strategy, a vehicle cooperates with the neighboring vehicles to change its pseudonym simultaneously with them. In addition, to protect the information contained in beacons, we used the silent period technique to change pseudonyms. Therefore, our pseudonym change contribution permits to guarantee the pseudonym changing simultaneity and the concealment of messages information. These two requirements ensure the unlinkability of pseudonyms. We used the ASS, entropy and traceability as the privacy metrics to evaluate the performance of our pseudonym change strategy CPCS by simulations in different network scenarios.
- Third, we introduced a novel adversary model, called a cheating attack that we applied on the proposed pseudonym change strategy CPCS. In this attack, the adversary tries to decrease the ASS in order to be able to link between the pseudonyms more easily. To thwart this attack, we built a Context-based Cheating Detection Mechanism (CCDM) that allows a vehicle to verify if the change of pseudonym is successful or not, and detect the malicious vehicles that are responsible for launching the cheating attack.
- Finally, we conclude the thesis by the development of a global framework for the privacy preservation in VANETs. The architectural framework provides the functionalities of the proposed scheme CLPS for better understanding and clarifying our research contributions.

7.2. Future Work

The contributions of this thesis have provided answers to some problems, but there are still some ways to explore. Each of these ways is a possible perspective in the continuity of this thesis.

- In future work, we plan to improve our pseudonym changing strategy CPCS. We also plan to study the impact of the use of the silent period on the capacity of the adversary in terms of traceability, and on the V2X communication (e.g., safety-related applications), and choose the optimal duration of the silent period that balances the tradeoff between privacy and network connectivity.
- Different types of attacks that can be added in addition to the cheating attack to ruin the good operation of the proposed pseudonym change strategy CPCS will be studied. We intend to apply the replay attack and the Sybil attack on CPCS, and we see how to confront these attacks in detail, so that the operation of this strategy is not disrupted.
- Finally, to combat these attacks, we plan to study, detail and enhance the proposed cheating detection mechanism CCDM in this thesis, so that it can be more efficient in the realistic network scenario (i.e., the case where a neighbor leaves the transmission range of the subject vehicle).

Appendices

Appendix

Author’s Publications

1. Journal Papers

[J1] **Ines Khacheba**, Mohamed Bachir Yagoubi, Nasreddine Lagraa, and Abderrahmane Lakas, “CLPS: Context-based Location Privacy Scheme for VANETs”, *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 29, no. 1-2, pp. 141-159, 2018.

Attached is the first page of the paper. The full-text paper can be found in the second document "Summary of PhD Thesis and Published Articles".

CLPS: context-based location privacy scheme for VANETs

Ines Khacheba*, Mohamed B. Yagoubi and Nasreddine Lagraa

Laboratory of Computer Science and Mathematics,
University of Laghouat,
BP 37G, Ghardaïa Road, Laghouat, Algeria
Email: in.khacheba@lagh-univ.dz
Email: m.yagoubi@lagh-univ.dz
Email: n.lagraa@lagh-univ.dz
*Corresponding author

Abderrahmane Lakas

College of Information Technology,
United Arab Emirates University,
P.O. Box 17551, Al Ain, UAE
Email: alakas@uaeu.ac.ae

Abstract: Location privacy preservation is considered as a challenge for deploying vehicular ad hoc networks (VANETs). In fact, the continuous periodical broadcast of spatiotemporal information in beacons allows a global passive adversary (GPA) to link pseudonyms and reconstruct vehicle traces. Consequently, it is imperative that a vehicle selects the right context to change pseudonym to confuse the adversary and ensure pseudonyms unlinkability. In this paper, we propose a context-based location privacy scheme (CLPS) that makes the following contributions: i) a pseudonym changing strategy that allows a vehicle to change pseudonyms based on its context; ii) a linkability threat, called cheating attack that negatively affects the proposed pseudonym changing strategy. A cheating detection mechanism is developed to allow a vehicle to detect misbehaving vehicles that launch the cheating attack, and assess the success of the pseudonym change. Finally, we evaluate CLPS against GPA by simulations using privacy extension, PREXT, in Veins, and we compare it against different existing privacy schemes.

Keywords: VANET; security; location privacy; changing pseudonyms; linkability; cooperation; cheating detection.

Reference to this paper should be made as follows: Khacheba, I., Yagoubi, M.B., Lagraa, N. and Lakas, A. (2018) 'CLPS: context-based location privacy scheme for VANETs', *Int. J. Ad Hoc and Ubiquitous Computing*, Vol. 29, Nos. 1/2, pp.141–159.

Biographical notes: Ines Khacheba is currently a PhD student in Computer Science. She received the degree of License in Computer Science (2010), and the degree of Master in Computer Science (2012) from the University of Laghouat, Algeria. She is currently working as a Research Assistant in the Laboratory of Computer Science and Mathematics at the University of Laghouat, Algeria. Her research interests include computer networks, wireless networking, vehicular networks, and networks security and privacy.

Mohamed B. Yagoubi is currently a Professor at the University of Laghouat, Algeria. He received his MSc in 1992 from Paris 13 University, Paris, France and the PhD in Computer Science in 1997 from Evry-val-d'Essonne University, France. His research interests include distributed systems, fault tolerance, security, and vehicular networks.

Nasreddine Lagraa received his PhD in Automation from the Ecole Nationale Polytechnique, Algeria (2008). He is currently the Director of the Computer Science and Mathematics Laboratory, University of Laghouat, Algeria. He is teaching various courses on computer architecture, multimedia, mobile networks, and network security. His research interests are vehicular networks, network security, decentralised control, fuzzy, and artificial neural networks. He is serving in the technical program committees of many international conferences, Wireless and Mobile Computing, Networking and Communications (WiMob), and Innovations in Information Technology (IIT).

2. Conference Papers

[C1] **Ines Khacheba** and Mohamed Bachir Yagoubi, “Conditional Privacy Preservation for VANET Safety Applications”, *The International Workshop on Cryptography and its Applications* (IWCA 2016), Oran, Algeria, April 26-27, 2016.

Attached is the first page of the paper. The full-text paper can be found in the second document "Summary of PhD Thesis and Published Articles".

Conditional Privacy Preservation for VANET Safety Applications

Ines Khacheba, Mohamed Bachir Yagoubi
Laboratory of Computer Science and Mathematics University of Laghouat,
Laghouat, Algeria

Abstract
Vehicular Ad Hoc Network (VANET) is a promising vehicular communication system, which offers a wide range of applications and services for the purpose of improving road safety, and traffic management. However, it faces many security and privacy issues, especially for location privacy. Indeed, if the vehicles' location privacy can't be protected, drivers won't accept the VANET. To protect vehicles' location privacy, the VANET should use privacy preservation schemes. However, a malicious vehicle can't be tracked and identified if a complete privacy preservation scheme is used. Therefore, a conditional privacy preservation scheme should be employed to secure VANET systems, where a Trusted Authority (TA) has the ability to reveal and revoke a malicious vehicle's real identity. This is known as conditional tracking. Unlinkable pseudonyms schemes can build conditional privacy preservation. In this study, we address the problem of achieving location privacy to secure VANET systems. We look for how to generate pseudonyms, and introduce an effective Pseudonyms Generation Protocol (PGP), in order to support the conditional tracking, and thus to achieve the requirement of conditional privacy preservation.

Keywords: Vehicular Ad Hoc Networks, Location Privacy, Conditional Privacy Preservation, Pseudonyms Generation, Connection Card, Conditional Tracking

Réf :42_23

[C2] **Ines Khacheba**, Mohamed Bachir Yagoubi, Nasreddine Lagraa, and Abderrahmane Lakas, “Location Privacy Scheme for VANETs”, *2017 IEEE International Conference on Selected Topics in Mobile and Wireless Networking* (MoWNet'17), Avignon, France, May 17-18, 2017.

Attached is the first page of the paper. The full-text paper can be found in the second document "Summary of PhD Thesis and Published Articles".

Location Privacy Scheme for VANETs

Ines Khacheba, Mohamed B. Yagoubi,
Nasreddine Lagraa
Laboratory of Computer Science and Mathematics
University of Laghouat
BP 37G, Ghardaïa Road, Laghouat, Algeria
{in.khacheba, m.yagoubi, n.lagraa}@lagh-univ.dz

Abderrahmane Lakas
College of Information Technology
United Arab Emirates University
PO Box 17551, Al Ain, UAE
alakas@uaeu.ac.ae

***Abstract*-In Vehicular Ad Hoc Networks (VANETs), a vehicle could be identified and tracked by eavesdropping its messages (e.g., beacons) by an adversary, since these messages contain personal information such as the location of the vehicle. This attack leads to threats on the user's location privacy. Frequent changing pseudonyms are accepted as a solution to protect the location privacy of users in VANETs. In this paper, we propose an efficient pseudonym changing strategy to provide location privacy in VANETs. In addition, we describe a novel tracking attack, that is, the cheating attack. To confront this attack, we develop a cheating detection mechanism. Finally, we show by simulations that the proposed scheme is effective.**

***Keywords*-Vehicular Ad Hoc Network, Location Privacy, Changing Pseudonyms, Cheating Detection**

I. INTRODUCTION

Vehicular Ad Hoc Networks (VANETs) allow vehicles to communicate among themselves using Vehicle-to-Vehicle (V2V) communications, and with road-side infrastructure using Vehicle-to-Infrastructure (V2I) communications [1]. VANETs promise of safer driving conditions and more comfort to drivers and passengers by presenting a wide range of applications that focus on providing road safety, convenience and entertainment to drivers and passengers.

To achieve VANET applications, vehicles broadcast periodically beacons, and occasionally event-based messages (e.g., safety messages). These messages contain personal information such as the location of the vehicle [2], which allows the adversary to eavesdrop it to identify and track vehicles. This attack affects the users' location privacy. Consequently, drivers won't participate in the VANET if the vehicles' location privacy can't be protected. To prevent such attack, location privacy enhancing schemes are vital; in fact, they are a prerequisite for deployment of the VANET.

In this paper, we propose a location privacy scheme for VANETs, which makes the following contributions. (i) We look for how the change of pseudonym can be performed in a successful way, and propose an effective pseudonym changing strategy to strengthen the location privacy of users in VANETs. (ii) We describe a novel tracking attack, called cheating attack, which aims to degrade the performance of the proposed pseudonym changing strategy. To confront this attack, we propose a cheating detection mechanism, which permits to detect the malicious cheating vehicles.

The rest of the paper is organized as follows. In Section II, we review the related work. In Section III, we present the problem definition. Section IV describes the network and adversary models considered in the paper. Section V introduces the proposed location privacy scheme. In Section VI, we present the performance evaluation of the proposed scheme. In Section VII, we draw our conclusion and future work.

II. RELATED WORK

In this section, we briefly review some existing location privacy enhancing schemes.

In [3], the authors introduces the concept of mix zone. Mix zones are anonymous regions of the network where mobile nodes change their identifiers to obfuscate the relation between entering and exiting events.

In [4], the authors propose a Cryptographic MIX-zone (CMIX) protocol for vehicular networks, where mix zones are situated at road intersections. At each mix zone, safety messages are encrypted with a symmetric key given by the RSU to each vehicle entering the mix zone. The advantage of CMIX is the simultaneity of changing pseudonyms, and the encryption of safety messages that prevents the external adversary from linking pseudonyms through safety messages. However, CMIX requires a RSU at each road intersection, which could cause a hard deployment of the network due to installation costs. In addition, cryptographic operations can slow the transmission of safety messages and so the reflex of drivers, as safety messages are real time in nature. Further, if an accident happens at a road intersection, only the vehicles that are in the intersection can be aware about the accident, because they detain the symmetric key to decrypt safety messages.

In [5], the authors propose the concept of silent period. However, this scheme adapts an individual pseudonym change behavior, which facilitates linking pseudonyms.

In [6], the authors. introduce CARAVAN that combines the group navigation with the random silent period. For V2V communications, the authors use random silent period to provide unlinkability to a vehicle entering the network. Then for most of the V2I communications based applications, the authors use the group navigation concept to enable vehicles to form a group that can be represented by a single vehicle (the group leader), which communicates on behalf of the group. Hence, the remaining vehicles in the group can remain silent for an extended period that is bounded by the time they stay in the group. However, the group leader sacrifices its privacy, since it does not enter silence, and so it remains tracked by the adversary. Further, the silent period could be extended as long

978-1-5090-4977-6/17/$31.00 ©2017 IEEE

References

References

[1] N. H. T. S. A. (NHTSA), "Advance notice of proposed rulemaking (ANPRM) (Docket No. NHTSA-2014-0022)," http://www.regulations.gov/#!documentDetail;D=NHTSA-2014-0022-0002, Aug. 2014, [Online; accessed Mar-2018].

[2] G. Karagiannis, O. Altintas, E. Ekici, G. Heijenk, B. Jarupan, K. Lin, and T. Weil, "Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions," *Communications Surveys Tutorials, IEEE*, vol. 13, no. 4, pp. 584-616, Fourth 2011.

[3] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, "Secure vehicular communication systems: design and architecture," *IEEE Communications Magazine*, vol. 46, no. 11, pp. 100-109, 2008.

[4] I. Khacheba and M. B. Yagoubi, "Conditional Privacy Preservation for VANET Safety Applications", *The International Workshop on Cryptography and its Applications* (IWCA 2016), Oran, Algeria, April 26-27, 2016.

[5] I. Khacheba, M. B. Yagoubi, N. Lagraa, and A. Lakas, "CLPS: Context-based Location Privacy Scheme for VANETs", *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 29, no. 1-2, pp. 141-159, 2018.

[6] Blincoe L., Seay A., Zaloshnja E., Miller T., Romano E., Luchter S., Spicer R., "The Economic Impact of Motor Vehicle Crashes", U.S. Department of Transportation National Highway Traffic Safety Administration, Technical Report, 2002.

[7] Project NoW - Network on Wheels. http://www.network-on-wheels.de.

[8] Project PRESERVE - Preparing Secure Vehicle-to-X Communication Systems. https://www.preserve-project.eu.

[9] Car 2 Car Communication (C2CC) Consortium. http://www.car2car.org.

[10] *Wireless Access in Vehicular Environments*, IEEE 802.11p-2010, 2010, IEEE.

[11] http://standards.ieee.org/develop/wg/1609_WG.html.

[12] http://www.etsi.org/website/technologies/intelligenttransportsystems.aspx.

[13] http://www.iso.org/iso/iso_technical_committee?commid=54706.

[14] X. Lin, R. Lu, C. Zhang, H. Zhu, P.-H. Ho, and X. Shen, "Security in vehicular ad hoc networks," *IEEE Communications Magazine*, vol. 46, no. 4, pp. 88–95, 2008.

[15] J. Harding, G. Powell, R. Yoon, J. Fikentscher, C. Doyle, D. Sade, M. Lukuc, J. Simons, and J. Wang. Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application. Technical report, National Highway Traffic Safety Administration, Washington, DC, August 2014.

References

[16] K. Hoeper and G. Gong, “Preventing or utilising key escrow in identity-based schemes employed in mobile ad hoc networks,” *IJSN*, vol. 2, no. 3/4, pp. 239–250, 2007.

[17] X. Fan and G. Gong, “Key revocation based on dirichlet multinomial model for mobile ad hoc networks,” in *LCN*, 2008, pp. 958–965.

[18] M. Raya and J.-P. Hubaux, “Securing vehicular ad hoc networks,” *Journal of Computer Security, Special Issue on Security of Ad Hoc and Sensor Networks*, vol. 15, no. 1, pp. 39-68, 2007.

[19] F. Li and Y. Wang, “Routing in vehicular ad hoc networks: A survey,” *IEEE Vehicular Technology Magazine*, vol. 2, no. 2, pp. 12–22, 2007.

[20] J.-P. Hubaux, S. Capkun, and J. Luo, “The security and privacy of smart vehicles,” *IEEE Security and Privacy Magazine*, vol. 2, no. 3, pp. 49-55, 2004.

[21] *Intelligent Transport Systems (ITS); Security; Security Header and Certificate Formats*, ETSI TS 103 097 v1.1.1, 2013, TC ITS.

[22] SAE J2735 V1.1.1 - Dedicated Short Range Communications (DSRC) Message Set Dictionary. *SAE Standard*, 2009.

[23] C. Sommer, D. Eckhoff, and F. Dressler, “Ivc in cities: signal attenuation by buildings and how parked cars can improve the situation,” *Mobile Computing, IEEE Transactions on*, vol. 13, no. 8, pp. 1733-1745, 2014.

[24] *Intelligent Transport Systems (ITS); Communications Architecture*, EN 302 665, 2010, ETSI TC ITS.

[25] Vehicle Safety Consortium, “Task 3 Final Report - Identify Intelligent Vehicle Safety Applications Enabled by DSRC”, Vehicle Safety Communications Project, 2005.

[26] Y. Toor, P. M¨uhlethaler, A. Laouiti, and A. de La Fortelle, “Vehicle ad hoc networks: Applications and related technical issues,” *IEEE Communications Surveys and Tutorials*, vol. 10, no. 1-4, pp. 74–88, 2008.

[27] H. Zhu, R. Lu, X. Lin, and X. Shen, “Security in service-oriented vehicular networks,” *IEEE Wireless Communications*, vol. 16, no. 4, pp. 16-22, 2009.

[28] P. Papadimitratos, A. La Fortelle, K. Evenssen, R. Brignolo, S. Cosenza, “Vehicular communication systems: Enabling technologies, applications, and future outlook on intelligent transportation”, *IEEE Communications Magazine*, vol. 47, no. 11, pp. 84-95, November 2009.

[29] *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 1 to 3*, ETSI EN 302 637-1-3, 2010, ETSI.

[30] J. Petit, “Surcoût de l’authentification et du consensus dans la sécurité des réseaux sans fil véhiculaires”, Université de Toulouse, Thèse de Doctorat, 2011.

[31] B. Wiedersheim, Z. Ma, F. Kargl, and P. Papadimitratos, “Privacy in inter-vehicular networks: why simple pseudonym change is not enough,” in *Proceedings of the Seventh International Conference on Wireless On-demand Network Systems and Services (WONS 2010)*, Kranjska Gora, Slovenia, February 2010.

[32] J.-H. Song, V. Wong, and V. Leung, “Wireless location privacy protection in vehicular ad-hoc networks,” *Mobile Networks and Applications*, vol. 15, no. 1, pp. 160-171, 2010.

[33] M. Feiri, J. Petit, and F. Kargl, “Efficient and secure storage of private keys for pseudonymous vehicular communication,” in *Proceedings of the 2013 ACM Workshop on Security, Privacy & Dependability for Cyber Vehicles*, Berlin, Germany, November 2013.

[34] M. Raya and J.-P. Hubaux, “Security aspects of inter-vehicle communications,” in *Swiss Transport Research Conference (STRC)*, 2005.

[35] C. Laurendeau and M. Barbeau, “Threats to security in dsrc/wave,” in *Ad-Hoc, Mobile, and Wireless Networks*, 2006, pp. 266-279.

[36] M. Raya, P. Papadimitratos, and J.-P. Hubaux, “Securing vehicular communications,” *IEEE Communications Magazine*, vol. 44, no. 10, pp. 8-15, 2006.

[37] B. Parno and A. Perrig, “Challenges in securing vehicular networks,” in *Proc. HotNets-IV, 2005*, 2005.

[38] M. Raya and J.-P. Hubaux, “The security of vehicular ad hoc networks,” in *Proceedings of the 3rd ACM Workshop on Security of Ad hoc and Sensor Networks (SASN)*, Alexandria, USA, November 2005.

[39] X. Lin, X. Sun, X. Wang, C. Zhang, P.-H. Ho, and X. Shen, “TSVC: timed efficient and secure vehicular communications with privacy preserving,” *IEEE Transactions on Wireless Communications*, vol. 7, no. 12, pp. 4987-4998, December 2008.

[40] H. Hartenstein and K. P. Laberteaux, “A tutorial survey on vehicular ad hoc networks,” *IEEE Communications Magazine*, vol. 46, no. 6, pp. 164-171, June 2008.

[41] C. Zhang, X. Lin, R. Lu, P.-H. Ho, and X. Shen, “An efficient message authentication scheme for vehicular communications,” *IEEE Transactions on Vehicular Technology*, vol. 57, no. 6, pp. 3357-3368, 2008.

[42] R. Brooks, S. Sander, J. Deng, and J. Taiber, “Automobile security concerns,” *IEEE Vehicular Technology Magazine*, vol. 4, no. 2, pp. 52-64, June 2009.

References

[43] F. Kargl, P. Papadimitratos, L. Buttyan, M. Muter, E. Schoch, B. Wiedersheim, T.-V. Thong, G. Calandriello, A. Held, A. Kung, and J.-P. Hubaux, "Secure vehicular communication systems: implementation, performance, and research challenges," *IEEE Communications Magazine*, vol. 46, no. 11, pp. 110-118, November 2008.

[44] "IEEE standard 1609.2 - ieee trial-use standard for wireless access in vehicular environments - security services for applications and management messages," July 2006.

[45] X. Sun, X. Lin, and P.-H. Ho, "Secure vehicular communications based on group signature and id-based signature scheme," in *Proceedings of IEEE International Conference on Communications (ICC'07)*, 2007, pp. 1539-1545.

[46] 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.

[47] G. Calandriello, P. Papadimitratos, A. Lioy, and J.-P. Hubaux, "Efficient and robust pseudonymous authentication in vanet," in *Proceedings of the International Workshop on Vehicular ad hoc networks (VANET'07)*, 2007, pp. 19-28.

[48] J. Freudiger, M. Raya, M. Félegyházi, P. Papadimitratos, and J.-P. Hubaux, "Mix-zones for location privacy in vehicular networks," in *Proceedings of WiN-ITS 2007*, Vancouver, British Columbia, Canada, August 2007.

[49] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in *The 27th Conference on Computer Communications (INFOCOM 2008)*, Phoenix, Arizona, USA, April 2008, pp. 1229-1237.

[50] 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.

[51] S. Zakhary and A. Benslimane, "On location-privacy in opportunistic mobile networks, a survey," *Journal of Network and Computer Applications*, 2017. https://doi.org/10.1016/j.jnca.2017.10.022.

[52] A. Boualouache, S. M. Senouci, and S. Moussaoui, "A survey on pseudonym changing strategies for vehicular ad-hoc networks," *IEEE Communications Surveys & Tutorials*, 2017. doi: 10.1109/COMST.2017.2771522.

[53] 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.

[54] European Telecommunications Standards Institute, "ETSI TS 102 940 V1.1.1," Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management, Jun 2012.

[55] L. Buttyan, T. Holczer, and I. Vajda, "On the effectiveness of changing pseudonyms to provide location privacy in vanets," in *Proceedings of the Fourth European Workshop on Security and Privacy in Ad hoc and Sensor Networks (ESAS)*, Cambridge, UK, July 2007.

[56] K. Emara, W. Woerndl, and J. Schlichter, "Vehicle tracking using vehicular network beacons," in *Fourth International Workshop on Data Security and PrivAcy in wireless Networks (D-SPAN)*, Madrid, Spain, June 2013.

[57] P. Golle and K. Partridge, "On the anonymity of home/work location pairs," in *Proceedings of the 7th International Conference on Pervasive Computing*, Nara, Japan, May 2009.

[58] H. Zang and J. Bolot, "Anonymization of location data does not work: A large-scale measurement study," in *Proceedings of the 17th Annual International Conference on Mobile Computing and Networking*, Las Vegas, NV, USA, September 2011.

[59] A. Cecaj, M. Mamei, and N. Bicocchi, "Re-identification of anonymized CDR datasets using social network data," in *The Third IEEE International Workshop on the Impact of Human Mobility in Pervasive Systems and Applications*, Budapest, Hungary, March 2014.

[60] M. Wernke, P. Skvortsov, F. Dürr, and K. Rothermel, "A classification of location privacy attacks and approaches," *Personal and Ubiquitous Computing*, vol. 18, no. 1, pp. 163–175, January 2014.

[61] A. Aijaz, B. Bochow, F. Dotzer, A. Festag, M. Gerlach, R. Kroh, and T. Leinmuller, "Attacks on inter-vehicle communication systems—An analysis," in *Proc. 3rd Int. WIT*, March 2006.

[62] Z. Ma, F. Kargl, and M. Weber, "Measuring location privacy in V2X communication systems with accumulated information," in *Proc. 6th IEEE Int. Conf. MASS*, October 2009.

[63] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki, "Enhancing wireless location privacy using silent period," in *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC)*, New Orleans, USA, March 2005.

[64] A. R. Beresford and F. Stajano, "Location privacy in pervasive computing," *IEEE Pervasive Computing*, vol. 2, no. 1, pp. 46–55, 2003.

[65] S. Warren and L. Brandeis, "The Right to Privacy," *Harvard Law Rev.*, vol. 4, no. 5, pp. 193–200, December 1890.

[66] Privacy Flag, "Enabling Crowd-sourcing based privacy protection for smartphone applications, websites and Internet of Things deployments, PN: 653426," http://privacyflag.eu, [Online; accessed Mar-2018].

[67] A. Boualouache, S. M. Senouci, and S. Moussaoui, “Towards an efficient pseudonym management and changing scheme for vehicular ad-hoc networks,” in *2016 IEEE Global Communications Conference (GLOBECOM)*, Dec 2016, pp. 1–7.

[68] R. B. Standler, “Privacy Laws in the US,” http://www.rbs2.com/privacy.html, Massachusetts, 1997.

[69] A. F. Westin, “Privacy and freedom,” *Washington Lee Law Rev.*, vol. 25, no. 1, p. 166, 1968.

[70] A. Pfitzmann and M. Köhntropp, “Anonymity, unobservability, and pseudonymity—A proposal for terminology,” *Designing Privacy Enhancing Technol.*, vol. 2009, pp. 1–9, 2001.

[71] D. L. Chaum, “Untraceable electronic mail, return addresses, and digital pseudonyms,” *Commun. ACM*, vol. 24, no. 2, pp. 84–90, Feb. 1981.

[72] A. Pfitzmann and M. Hansen, A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management, TU Dresden. [Online]. Available: http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf

[73] D. Banisar and S. Davies, Privacy and Human Rights, www.gilc.org/privacy/survey.

[74] F. Schaub, Z. Ma, and F. Kargl, “Privacy requirements in vehicular communication systems,” in *Proc. IEEE Int. Conf. PASSAT*, Vancouver, BC, Canada, August 2009.

[75] L. Buttyan, T. Holczer, A. Weimerskirch, and W. Whyte, “SLOW: A practical pseudonym changing scheme for location privacy in vanets,” in *Proceedings of the IEEE Vehicular Networking Conference (IEEE VNC)*, Tokyo, Japan, October 2009.

[76] E. Fonseca, A. Festag, R. Baldessari, and R. Aguiar, “Support of anonymity in VANETs—Putting pseudonymity into practice,” in *Proc. IEEE WCNC*, Mar. 2007, pp. 3400–3405.

[77] P. Papadimitratos, L. Buttyan, J.-P. Hubaux, F. Kargl, A. Kung, and M. Raya, “Architecture for secure and private vehicular communications,” in *Telecommunications, 2007. ITST'07. 7th International Conference on ITS*. IEEE, 2007, pp. 1-6.

[78] 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 (IoV-VoI 2016)*, Paderborn, Germany, July 2016.

[79] ETSI TS 102 867 v1.1.1. *Intelligent Transport Systems (ITS); Security; Stage 3 mapping for IEEE 1609.2*, June 2012.

[80] D. Eckhoff, R. German, C. Sommer, F. Dressler, and T. Gansen, “Slotswap: strong and affordable location privacy in intelligent transportation systems,” *Communications Magazine, IEEE*, vol. 49, no. 11, pp. 126 –133, Nov. 2011.

[81] D. Eckhoff, C. Sommer, T. Gansen, R. German, and F. Dressler, “Strong and affordable location privacy in VANETs: Identity diffusion using time-slots and swapping,” in *Proc. 2nd IEEE VNC*, Dec. 2010, pp. 174–181.

[82] Y. Pan, J. Li, L. Feng, and B. Xu, “An analytical model for random pseudonym change scheme in vanets,” *Cluster Computing*, vol. 17, no. 2, pp. 413–421, 2014. [Online]. Available: http://dx.doi.org/10.1007/s10586-012-0242-7

[83] Y. Pan, J. Li, L. Feng, and B. Xu, “An analytical model for random changing pseudonyms scheme in VANETs,” in *Proc. Int. Conf. NCIS*, May 2011, pp. 141–145.

[84] M. Gerlach and F. Guttler, “Privacy in vanets using changing pseudonyms - ideal and real,” in *Proceedings of the 65th Vehicular Technology Conference (VTC)*, Dublin, Ireland, April 2007.

[85] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki, “CARAVAN: Providing location privacy for vanet,” in *Proceedings of the Workshop on Embedded Security in Cars (ESCAR)*, Cologne, Germany, November 2005.

[86] 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, pp. 1569–1589, 2007.

[87] B. Palanisamy, L. Liu, K. Lee, A. Singh, and Y. Tang, “Location privacy with road network mix-zones,” in *IEEE 2012 Eighth International Conference on Mobile Ad-hoc and Sensor Networks (MSN)*, Chengdu, China, December, 2012.

[88] B. Palanisamy and L. Liu, “Attack-resilient Mix-zones over Road Networks: Architecture and Algorithms,” *IEEE Transactions on Mobile Computing*, vol. 14, no. 3, pp. 495–508, 2015.

[89] R. Yu, J. Kang, X. Huang, S. Xie, Y. Zhang, and S. Gjessing, “MixGroup: Accumulative Pseudonym Exchanging for Location Privacy Enhancement in Vehicular Social Networks,” *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 1, pp. 93–105, January 2016.

[90] M. Dahl, S. Delaune, and G. Steel, “Formal analysis of privacy for vehicular mix-zones,” in *European Symposium on Research in Computer Security*, Springer, Berlin, Heidelberg, 2010.

[91] B. Blanchet, M. Abadi, and C. Fournet, “Automated verification of selected equivalences for security protocols,” *The Journal of Logic and Algebraic Programming*, vol. 75, no. 1, pp. 3–51, 2008.

[92] J. Liao and J. Li, "Effectively changing pseudonyms for privacy protection in vanets," in *Proceedings of the 10th International Symposium on Pervasive Systems, Algorithms, and Networks*, December 2009.

[93] J. Liao, J. Li, and Y. Pan, "Cooperatively changing pseudonyms for privacy protection in vanets," in *Proc. the 2nd IEEE International Conference on Wireless Access in Vehicular Environments (WAVE)*, Shanghai, China, Dec. 2009, pp. 13-18.

[94] Y. Pan and J. Li, "An analysis of anonymity for cooperative pseudonym change scheme in one-dimensional VANETs," in *Proc. IEEE 16th Int. Conf. CSCWD*, May 2012, pp. 251–257.

[95] J.-H. Song, V. Wong, and V. Leung, "Wireless location privacy protection in vehicular ad-hoc networks", *IEEE International Conference on Communications (IEEE ICC'09)*, Dresden, Germany, June 2009.

[96] A. Wasef and X. Shen, "Rep: location privacy for vanets using random encryption periods", *Mobile Networks and Applications*, vol. 15, no. 1, pp. 172–185, 2010.

[97] K. Mershad and H. Artail, "REACT: Secure and efficient data acquisition in VANETs," *2011 IEEE 7th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, Wuhan, China, October 2011.

[98] 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.

[99] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. S. Shen, "Anonymity analysis on social spot based pseudonym changing for location privacy in vanets," in *Proceedings of 2011 IEEE International Conference on Communications (ICC)*, Kyoto, Japan, June 2011.

[100] Z. Li, C. Chigan, and C. Gao, "STCP2: Short-time certificate-based privacy protection for vehicular ad hoc networks," *2013 IEEE Wireless Communications and Networking Conference (WCNC)*, Shanghai, China, April 2013.

[101] 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.

[102] B. Ying, D. Makrakis, and H. Mouftah, "Dynamic mix-zone for location privacy in vehicular networks", *IEEE Communications Letters*, vol. 17, no. 8, pp.1524–1527, 2013.

[103] S. Xingjun and X. Huibin, "An effective scheme for location privacy in VANETs," *Journal of Networks*, vol. 9, no 8, pp. 2239-2244, 2014.

[104] D. Eckhoff, and C. Sommer, "Marrying safety with privacy: A holistic solution for location privacy in VANETs," in *IEEE Vehicular Networking Conference (VNC)*, Columbus, Ohio, USA, December 2016.

[105] M. Li, K. Sampigethaya, L. Huang, and R. Poovendran, "Swing & swap: user-centric approaches towards maximizing location privacy," in *5th ACM workshop on Privacy in electronic society (WPES '06)*, Oct. 2006.

[106] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki, "Towards modeling wireless location privacy," in *Proceedings of Privacy Enhancing Technologies (PET)*, pages 59–77, 2005.

[107] J. Freudiger, M. H. Manshaei, J. P. Hubaux, and D. C. Parkes, "Non-cooperative location privacy," *IEEE Transactions on Dependable and Secure Computing*, vol. 10, no. 2, pp. 84-98, March 2013.

[108] B. Chaurasia and S. Verma, "Optimizing pseudonym updation for anonymity in VANETs," in *Proceedings of the 2008 IEEE Asia-Pacific Services Computing Conference*, Yilan, Taiwan, December 2008.

[109] B. Chaurasia, S. Verma, G. Tomar, and A. Abraham, "Optimizing pseudonym updation in vehicular ad hoc networks," in *Trans. Comput. Sci. IV*, 2009, pp. 136–148.

[110] B. Chaurasia, S. Verma, G. Tomar, and S. Bhaskar, "Pseudonym based mechanism for sustaining privacy in VANETs," in *Proc. 1st Int. Conf. CICSYN*, Jul. 2009, pp. 420–425.

[111] K. Emara, "Safety-aware location privacy in vehicular ad-hoc networks," Ph.D. dissertation, Munchen, Technische Universitat Munchen, 2016.

[112] H. Dok, H. Fu, R. Echevarria, and H. Weerasinghe, "Privacy issues of vehicular ad-hoc networks," *International Journal of Future Generation Communication and Networking*, vol. 3, no. 1, pp. 17-32, march 2010.

[113] A. Tomandl, F. Scheuer, and H. Federrath, "Simulation-based evaluation of techniques for privacy protection in vanets," in *Wireless and Mobile Computing, Networking and Communications (WiMob)*, Barcelona, Spain, October 2012.

[114] 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*, New York, USA, June 2015.

[115] K. Emara, W. Woerndl, and J. Schlichter, "Context-based pseudonym changing scheme for vehicular adhoc networks," *arXiv preprint arXiv:1607.07656*, 2016.

[116] K. Emara, W. Woerndl, and J. Schlichter, "POSTER: Context-Adaptive User-Centric Privacy Scheme for VANET," in *International Conference on Security and Privacy in Communication Systems*, Dallas, TX, USA, October 2015.

[117] A. Boualouache and S. Moussaoui, "Urban pseudonym changing strategy for location privacy in vanets," *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 24, no. 1-2, pp. 49-64, 2017.

[118] 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.

[119] I. Wagner and D. Eckhoff, “Privacy assessment in vehicular networks using simulation,” *Simulation Conference (WSC), 2014 Winter*, Savanah, GA, USA, December 2014.

[120] G. P. Corser, H. Fu, and A. Banihani, “Evaluating location privacy in vehicular communications and applications,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 9, pp. 2658-2667, 2016.

[121] Z. Ma, F. Kargl, and M. Weber, “A location privacy metric for v2x communication systems,” in *Sarnoff Symposium, 2009. SARNOFF '09. IEEE*, March 2009, pp. 1-6.

[122] Z. Ma, “Location privacy in vehicular communication systems: a measurement approach,” Ph.D. dissertation, University Ulm, 2011.

[123] D. Chaum, “The dining cryptographers problem: Unconditional sender and recipient untraceability,” *J. Cryptol.*, vol. 1, no. 1, pp. 65–75, 1988.

[124] I. Khacheba, M. B. Yagoubi, N. Lagraa, and A. Lakas, “Location privacy scheme for vanets,” in *Proceedings of the Sixth International Conference on Selected Topics in Mobile & Wireless Networking (MoWNet'17)*, Avignon, France, May 2017.

[125] R. Shokri, G. Theodorakopoulos, J.-Y. Le Boudec, and J.-P. Hubaux, “Quantifying Location Privacy,” in *Proceedings of the 2011 IEEE Symposium on Security and Privacy*, Oakland, CA, USA, May 2011.

[126] A. Serjantov and G. Danezis, “Towards an information theoretic metric for anonymity,” in *Proceedings of the 2Nd International Conference on Privacy Enhancing Technologies*, ser. PET’02. Berlin, Heidelberg: Springer-Verlag, 2003, pp. 41–53.

[127] C. Diaz, S. Seys, J. Claessens, and B. Preneel, “Towards measuring anonymity,” in *Proceedings of the 2Nd International Conference on Privacy Enhancing Technologies*, ser. PET’02. Berlin, Heidelberg: Springer-Verlag, 2003, pp. 54–68.

[128] K. Emara, “Safety-aware Location Privacy in VANET: Evaluation and Comparison,” *IEEE Transactions on Vehicular Technology*, vol. 66, no. 12, pp. 10718-10731, 2017.

[129] K. Emara, “Poster: PREXT: Privacy Extension for Veins VANET Simulator,” in *IEEE Vehicular Networking Conference (VNC)*, Columbus, Ohio, USA, December 2016.

[130] Project Veins. http://veins.car2x.org.

[131] 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.

[132] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," *Journal of Cryptology*, vol. 17, no. 4, pp. 297–319, 2004.

[133] D. Boneh and M.K. Franklin, "Identity-Based Encryption from the Weil Pairing," *Advances in Cryptology*, LNCS 2139, Springer, 2001, pp. 213–229.

[134] R. Lu, X. Lin, Z. Shi, and X. S. Shen, "A Lightweight Conditional Privacy-Preservation Protocol for Vehicular Traffic-Monitoring Systems," *IEEE Intelligent Systems*, vol. 28, no. 3, pp. 62-65, 2013.

[135] P.S.L.M. Barreto, B. Libert, N. McCullagh, and J.-J. Quisquater, "Efficient and Provably-Secure Identity-Based Signatures and Signcryption from Bilinear Maps," in *International Conference on the Theory and Application of Cryptology and Information Security*, LNCS 3788, Springer, Berlin, Heidelberg, pp. 515–532, December 2005.

[136] T. Umer, M. H. Rehmani, Z. G. Ding, B.-S. Kim, S. U. Khan, "Resource management in vehicular adhoc networks: energy management, communication protocol and future Applications," *IEEE Access Special Section Editorial, IEEE Access*, vol. 5, pp. 7839-7842, 2017.

[137] M. Rehan, H. Hasbullah, I. Faye, W. Rehan, O. Chughtai, M. H. Rehmani, "ZGLS: a novel flat quorum-based and reliable location management protocol for VANETs," *Wireless Networks*, pp. 1-19, 2017.

[138] F. Jamil, A. Javaid, T. Umer, and M. H. Rehmani, "A comprehensive survey of network coding in vehicular ad-hoc networks," *Wireless Networks*, vol. 23, no. 8, pp. 2395-2414, 2017.

[139] A. K. Dey and G. D. Abowd, "Towards a better understanding of context and context-awareness," in *Proceedings of 1st International Symposium on Handheld and Ubiquitous Computing*, 1999, pp. 304–307.

[140] K. Emara, W. Woerndl, and J. Schlichter, "Beacon-based vehicle tracking in vehicular ad-hoc networks," Technical report, TECHNISCHE UNIVERSITAT MUNCHEN, April 2013.

[141] Z. Ma, "Location privacy in vehicular communication systems: a measurement approach," Ph.D. dissertation, University Ulm, 2011.

[142] E. Schoch, F. Kargl, T. Leinmüller, S. Schlott, and P. Papadimitratos, "Impact of pseudonym changes on geographic routing in vanets," in *Proc. 3rd ESAS*, Sep. 2006, pp. 43–57.

[143] J. Sun, C. Zhang, and Y. Fang, "An id-based framework achieving privacy and non-repudiation in vehicular ad hoc networks," in *Proceedings of the IEEE Military Communications Conference*, Orlando, USA, October 2007.

[144] A. Pfitzmann and M. Kohntopp, “Anonymity, unobservability, and pseudonymity – a proposal for terminology,” in *Workshop on Design Issues in Anonymity and Unobservability*, Berkeley, California, July 2000.

[145] D. Krajzewicz, J. Erdmann, M. Behrisch, and L. Bieker, “Recent development and applications of sumo–simulation of urban mobility,” *International Journal On Advances in Systems and Measurements*, vol. 5, no. 3&4, 2012.

[146] OpenStreetMap. https://www.openstreetmap.org.

[147] SUMO Wiki Page. http://sumo.dlr.de/wiki/Networks/Import/OpenStreetMapDownload.

[148] SUMO Wiki Page. http://sumo.dlr.de/wiki/Networks/Import/OpenStreetMap.

[149] SUMO Wiki Page. http://sumo.dlr.de/wiki/Tools/Trip.