PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA
MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH

**UNIVERSITY OF ABOUBAKR BELKAÏD – TLEMCEN –**

# LMD Thesis

Presented to:

FACULTY OF SCIENCES–COMPUTER SCIENCE DEPARTMENT

Thesis submitted in partial fulfilment of the requirements for the degree of:

DOCTORATE

Specialty: Networks and Distributed Systems

By:

**Leila BENAROUS**

Theme

---

# Security and Privacy in Vehicular Networks

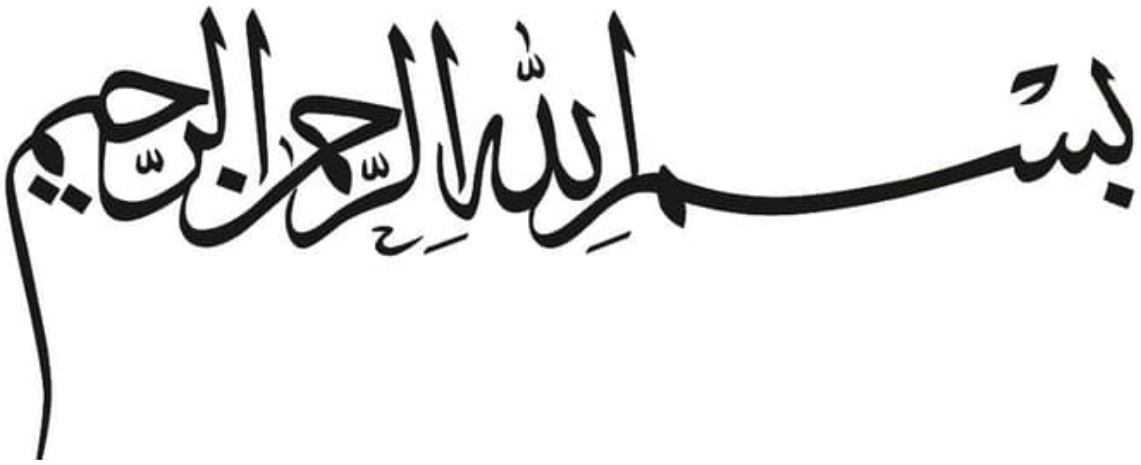
---

Thesis defended publicly on February 20th, 2020 at Tlemcen.

Jury members

| | | | |
|---|---|---|---|
| Mr Abdelkarim Benamar | Associate Professor | Univ. Tlemcen | President |
| Mr Benamar Kadri | Associate Professor | Univ. Tlemcen | Supervisor |
| Mr Sofiane Boukli Hacene | Associate Professor | Univ SBA | Examiner |
| Mr Badr Benmammar | Associate Professor | Univ. Tlemcen | Examiner |
| Mr Nassim Denouni | Associate Professor | Univ Chlef | Examiner |
| Mr Fethallah Hadjilla | Associate Professor | Univ. Tlemcen | Invited |

2019-2020



**...نَرْفَعُ دَرَجَاتٍ مَّن نَّشَاءُ ۗ وَفَوْقَ كُلِّ ذِي عِلْمٍ عَلِيمٌ.**

سورة يوسف – الآية 76

# *Dedication*

*To my beloved parents,*
*My cherished brothers,*
*My dear sisters,*
*My lovely nieces and nephews*

# Acknowledgments

*First and foremost, I would like to thank Allah the great for blessing me, helping me and for giving me the ability to elaborate this work.*

*I deliver my utmost gratefulness to my parents. I am thankful for everything you have done, without you I would not be where I am, I would not be who I am. Thank you so much for your great support and love, for your immense care, for your continuous support, encouragements and patience.*

*I also thank my brothers and sisters for their continuous encouragements, support and understanding.*

*I would like to show my appreciation to my supervisor for proposing this interesting topic. Thank you for your understanding and support, for your availability, for the fruitful discussions, for your encouragements and support, for your open mind and flexibility.*

*I am thankful to Pr. Lehsaini Mohamed the head of STIC laboratory for his kind understanding, encouragement, advice and support. I also thank Mr Benamar Albdelkrim, Mr Matallah Hocine the head of the computer science department and Pr Arrar Zoheir for their availability, understanding and encouragement.*

*A special thanks to Mrs Nouria Khelif and my colleagues and friends at STIC laboratory for the friendly atmosphere, for their brightness and help. Thank you all, you made me feel home.*

*I would like to thank Pr. Bouridane Ahmed from the University of Northumbria, UK, for his great help and support. Thank you so much for your availability, for your valuable advice and continuous encouragements, for your trust and for the provision of various rare scientific opportunities.*

*I am very grateful to Pr. Bitam Salim from the University of Biskra and Pr. Mellouk Abdelhamid from the University of Paris-Est Créteil for their trust and cooperation, for their continuous help and support, for the efforts they made, for their availability and valuable advice.*

*A special thanks to Dr. Saadi Boudjit from the University of Paris 13 for his availability, meaningful advice and support. I appreciate your great help, efforts and encouragements.*

*I thank Dr. Saidi Yazid Mohand from University of Paris 13 and Pr. ZERHOUNI Noureddine from ENSMM for their encouragements support, and advice.*

*I deeply thank Dr. Yamani Ahmed the head of Yamani Institute of Technology and his humble family for their continuous support, help, advice, encouragements and prayers.*

*I thank Mr Djoudi Mohamed for his continuous encouragements, advice, and support.*

*I am thankful to researchers and professors at LIM laboratory of the University of Laghouat. Particular thanks for Pr. Belabbaci Youcef, Pr. Ouinten Youcef, Pr. Yagoubi Mohamed Bachir, Pr. Lagraa Nasereddine, Dr. Bensaad Lahcen, Dr. Oubbati Omar Sami and Dr. Kerrache Chaker Abdelaziz for their availability, advice, encouragement and support.*

*I thank Pr. Mohsen Guizani from Qatar University for his availability, kind help, advice and encouragements.*

*I thank Mr Ullah Irfan from the University of Kent, UK, and Dr. Emara Karim from Ain Shams University, Egypt for their availability and help whenever needed.*

*I thank the anonymous reviewers for their valuable comments, for their objectiveness and for their efforts.*

*I specially thank the honorable jury members for the time and efforts they spent reading the thesis, for their constructive comments aiming to improve its quality, for their recommendations, advice and enlightenment regarding my future research perspectives.*

*I am thankful to all the great persons who have helped me so far, your existence made a difference. I am grateful to your positivity, your continuous support, your encouragements and help.*

# *Abstract*

The vehicular networks are formed by connected vehicle. They were initially developed to ensure safe driving and to extend the internet to the road edge. They provide various types of services and applications to the road users rendering their trips more enjoyable and comfortable. However, the vehicle's cyber-activity may expose it to new types of risks, such as blackmailing, data trading, and profiling. Even worst, it may impact the onboard user's safety and cause road causalities. The risks come from the tracking and privacy violation through the interception of exchanged messaged needed in the participation in the network. The privacy and security are the major issues that need to be resolved for the vehicular networks to be realized in a real-world implementation.

In this thesis, we aim to propose privacy-preserving solutions that protect the user's identity and location on roads to prevent tracking from occurring. Our solutions were tested to evaluate their performance against a strong attacker model. The thesis facilitates the understanding of the vehicular networks and their used technologies as well as their various types. It highlights the importance of privacy and security issues and their direct impact on the safety of their users. It includes two anonymous authentication methods that preserve the identity privacy and a total of five schemes that preserve the location privacy in the vehicular ad hoc networks (VANET) and the cloud-enabled internet of vehicles (CE-IoV) respectively. Moreover, it provides the design of a new privacy-aware blockchain-based pseudonym management framework. The framework is secure, distributed and public. It ensures the revocation, non-repudiation, authenticity and integrity which are fundamental security requirements. The proposal was developed as a potential replacement for the vehicular public key infrastructure (VPKI).

**Keywords:** privacy, vehicular networks, VANET, CE-IoV, security, anonymous authentication, location, identity, tracking, blockchain, VPKI.

# *Résumé*

Les réseaux véhiculaires sont formés par des véhicules connectés. Ils ont été initialement développés pour assurer la sécurité routière et pour étendre l'Internet aux routes. Ils fournissent des différents types de services et d'applications aux utilisateurs de route, rendant leurs trajets plus agréables et plus confortables. Cependant, la cyber-activité du véhicule peut l'exposer à de nouveaux types de risques tels que: le chantage, le commerce de données et le profilage. Pire encore, cela pourrait avoir un impact sur la sécurité de l'utilisateur du véhicule et causer des accidents routiers. Les risques proviennent du suivi et de la violation de la confidentialité via l'interception des messages échangés nécessaires au bon fonctionnement du réseau. La protection de la vie privée et la sécurité sont les principaux problèmes à résoudre pour que les réseaux de véhicules puissent être réalisés dans le monde réel.

Dans cette thèse, nous visons à proposer des solutions en préservant la confidentialité, en protégeant l'identité de l'utilisateur et sa position sur la route afin d'empêcher qu'une poursuite se produise. Nos solutions ont été testées pour évaluer leurs performances contre un modèle d'attaquant puissant. La thèse facilite la compréhension des réseaux de véhicules et leurs technologies utilisées, ainsi que leurs divers types. On développe l'importance de la confidentialité (la vie privée) et de la sécurité et leurs impacts directs sur la sécurité de leurs utilisateurs. Nous incluons deux méthodes d'authentification anonyme qui préservent la confidentialité de l'identité et un total de cinq solutions qui préservent la confidentialité de la localisation dans les réseaux ad hoc de véhicules (VANET) et l'internet de véhicules avec cloud (CE-IoV) respectivement. En outre, nous développons la conception d'un nouveau système de gestion des pseudonymes, basé sur la technologie de blockchain respectant la confidentialité. Ce système est sécurisé, distribué et public. Il garantit la révocation, la non-répudiation, l'authenticité et l'intégrité, qui constituent les exigences fondamentales de la sécurité. La proposition a été élaborée pour remplacer potentiellement l'infrastructure à clés publiques pour les réseaux véhiculaires (VPKI).

**Mots clés :** la vie privée, réseaux de véhicules, VANET, CE-IoV, sécurité, authentification anonyme, localisation, identité, suivi, blockchain, VPKI.

# ملخص

تتكون شبكة المركبات الذكية من سيارات متصلة. لقد تم تطويرها في البداية لضمان القيادة الآمنة و تمديد شبكة الانترنت إلى الطرقات. تقدم هذه الشبكات أنواع متعددة من الخدمات و التطبيقات لمستعملي الطرقات لجعل رحلاتهم أكثر راحة و متعة. إلا أن النشاط الافتراضي للسيارة عند استعمالها لخدمات الشبكة قد يعرضها لأنواع جديدة من المخاطر كالابتزاز، المتاجرة بالمعلومات الشخصية للمستخدم والتنميط. الأسوأ من ذلك أنها قد توثر على سلامة المستخدم و تتسبب في حوادث المرور. تحدث مثل هذه الأخطار إذا تم تعقب السيارات على الطرقات و خرق خصوصيات راكبيها من خلال التصنت و تتبع الرسائل المتبادلة على الشبكة. تعد الخصوصية و أمن الشبكات من أهم الخصائص التي يجب توفيرها في شبكة المركبات الذكية حتى يتم تنفيذها و تداول استعمالها في الواقع.

في هذه الأطروحة نهدف إلى إيجاد حلول للمحافظة على خصوصية المستخدمين و حمايتها من خلال حماية هوية و موقع المستخدم وذلك بتجنب السماح بحدوث التعقب. لقد تم اختبار حلولنا لتقييم أدائها في مواجهة نموذج تعقب قوي. الأطروحة تسهل فهم شبكة السيارات و تقنياتها المستعملة، إضافة الى تمكينها من تمييز بين أنواع شبكات السيارات. لقد قمنا فيها ايضا بتوضيح مخاطر اختراق الخصوصية و أمن المعلومات على سلامة مستخدمي الطرقات. تقدم هذه الاطروحة نظامين للتعرف على الهوية(authentication) من دون فضح الخصوصية أي من دون استعمال الهوية. كما تعرض أيضا خمسة حلول للحفاظ على خصوصية المستخدم من التعقب و التتبع، اي حلول لحماية سرية المواقع. الحلول تم تطويرها لكل من شبكة السيارات VANET و انترنت السيارات CE-IoV. كما تقدم هذه الأطروحة أيضا تصميم نظام يعتمد على سلسلة الكتل (Blockchain) لتوليد مفاتيح التشفير العامة المؤقتة للسيارة (pseudonyms) مع الحفاظ على خصوصية المستخدمين. النظام يتميز بأنه آمن، موزع و علني (عام). كما أنه يضمن أهم خصائص أمن الشبكات كإمكانية إلغاء المفاتيح، عدم إنكار استعمالها، صحتها و سلامتها من التغيير. يمكن لهذا النظام أن يكون بديل محتمل لنظام البنية تحتية للمفاتيح العامة VPKI المستعمل حاليا في شبكة المركبات الذكية لتزويد السيارات بالمفاتيح العامة.

**الكلمات المفتاحية**: الخصوصية، شبكة المركبات الذكية، VANET،CE-IoV ، الامن، أنظمة التعريف بدون استعمال الهوية، الموقع، الهوية، تعقب، blockchain، VPKI.

# Table of Contents

# GENERAL INTRODUCTION

# I. Introduction

The vehicles are continuously evolving, from a mere mean of transportation to a computer on wheels. The researchers and industrials are concentrating on developing smart vehicles that are safer and eco-friendlier. They are also aiming to extend the internet and networking concepts to the road. This led to the appearance of the vehicular networks' concept. These networks are formed by vehicles and road infrastructures. They were initially created to ensure the user's safety on roads and reduces accidents. The accurate timely update of road conditions helps the road takers plan their trips to be smooth and secure. Therefore, the traffic management was also ensured by these networks. Their applications are various, among which is the autonomous driving by relying on the data exchanged over the network to make driving decisions. The vision of researchers and industrials was not limited to the safety-related applications but also to the infotainment applications as well. Enabling its users to enjoy internet access and its services while on roads. One of the implicit fundamental consequences of the vehicular networks is the environment preservation. It results from reducing fuel consumption and its emitted toxins and gazes. The reduction is due to the smooth traffic management.

However, although the vehicular networks may save the users lives and offer them various services on the road, they may violate their privacy in the process. Security and privacy are two fundamental issues to resolve, in order to safely use these networks.

# II. Motivation

The risks that come from violating the security of cyber-systems, in general, are disastrous in terms of moral, financial and human-life related damages. The technology news report annual security violations with extreme causalities recorded against top high-level IT corporations. The vehicular networks are of no exception as the extension of the computers and cyber-world on roads. The fatalities resulting from security violation on road are even worst. They are directly related to users' safety. Among the important security issues to preserve is privacy.

The vehicle shall not be tracked by its cyber-activity on roads. Its user shall not be known, nor his/her identity extracted from the vehicle's emitted messages. If the vehicle is to be tracked on roads by an attacker, s/he may learn its driver's routines, parsed trajectories, hideouts and frequented places. The attacker may trade this data for profit, out of personal interest (stalking) or may blackmail the vehicle owner with collected secrets. The consequences may be more severe such as causing traffic congestion or accidents in frequented routes. Even worst, the attacker may execute on-road assassination. To avoid these severe consequences and ensure safe usage of vehicular networks, we concentrate our research on developing security and privacy solutions.

# III. Objectives

The main purpose of our research is to preserve the privacy and security of vehicular network users. We are interested in the identity and location privacy types as they can be correlated with each other. Exposing one of them leads to the violation of the other resulting in

one or more of the previously mentioned fatalities. The privacy is threatened in the vehicular network by the state messages required by the safety applications. These messages are exchanged wirelessly in clear with high frequency. Moreover, they contain accurate real-time identity and spatiotemporal information. This facilitates their interception and results in the vehicle trajectory tracking. The vehicular network also necessitates the insurance of the authentication, the non-repudiation (accountability) and the revocation of misbehaving nodes to maintain its correct functionality. In a matter of facts, these requirements contradict with privacy. Thus, when developing a solution both the privacy and the security requirements shall be ensured in a balanced way. The existing solutions to preserve location privacy rely on the use of temporal identities known as pseudonyms. These pseudonyms are frequently updated using change strategies that aim to reduce their linkability. The unlinkability between the updated pseudonyms preserve the trajectory (location) privacy. The use of pseudonym ensures anonymity. Therefore, most of the existing solutions aim to ensure anonymity and reduce linkability to prevent tracking.

The identity privacy may further be risked if repetitively used in authentication to infrastructures, authorities and service providers. Therefore, we concentrate on developing privacy-preserving authentication solutions also known as the anonymous authentication methods. While developing these solutions, we aim to make them resilient to security attacks targeting vehicular networks in particular such as Sybil attack and the authentication systems in general.

Noting that the current vehicular networks are authority-based which means that the vehicle registration and the issuance of the certificate are done by the authority. This authority is responsible for keeping the correct functionality of the network by being able to revoke misbehaving nodes and tracing honest nodes. This means that privacy is conditional in vehicular networks. It is preserved from other vehicles and nodes but not from the authority. Besides, it is preserved as long as the vehicle is not misbehaving. The authority is responsible for providing the vehicle with its security parameters, keys, certificates and algorithms. This authority-based central system is known as the vehicular public key infrastructure (VPKI). The VPKI is favored over the self-generated keys system because it ensures the main requirements needed in vehicular networks such as preventing Sybil attack, ensuring conditional privacy, guaranteeing the non-repudiation and revocation, … etc. Therefore, most of the existing solutions are built over the VPKI.

In the following, we explain the objectives we tried to achieve in our thesis. Also, the key security problematics we resolved:

- One of our earliest objectives is to understand the vehicular networks' characteristics and types. Besides surveying their security issues and their causes. Among the security issues we studied, we concentrate on the authentication and privacy issues.
- Our second objective is to ensure the authentication without violating the identity privacy. However, privacy-preserving authentication methods also known as anonymous authentication methods may cause other security breaches. Being anonymous may allow untraceable network abuse. It may even disrupt the correct functionality of the network. It also contradicts with the non-repudiation and the revocation needs. Therefore, when developing the anonymous authentication methods, we ought to think of how to resolve the highlighted issues first.

- Our third objective is to develop crowd, infrastructure and road-map independent location privacy-preserving schemes for vehicular ad hoc networks. The proposed solutions are pseudonym change strategies which reduces the linkability while maintaining the network functionality. The solutions were developed to preserve the location privacy even within low-density roads where the tracking is sure to occur.
- Our fourth objective is to develop location privacy-preserving schemes for the internet of vehicles (IoV) on-road users. The objective is to reduce the linkability that may result from matching location-based service IoV queries with safety applications frequent beacons. Reducing the linkability results in reducing the tracking. Taking into consideration that the developed solutions shall not interfere negatively with the network functionality nor disrupt service usage.
- Our last objective is to propose a potential replacement for the central-based VPKI. The VPKI is secure and most of the existing solutions discuss its robustness from the researcher's perspectives. However, the certificate provision is most likely to be a paid service. Furthermore, the fact that it is centralized, makes it a single point of failure and the target of attacks. Finally, the cost of VPKI deployments to cover and satisfy all of the network vehicles pseudonym needs is extremely high. Therefore, we suggest elaborating a distributed blockchain-based cost-free pseudonym management framework as a replacement to the VPKI. This framework ensures the security requirements of privacy, authenticity, integrity, non-repudiation and revocation. It relies on the network nodes (vehicles and infrastructures) to self-generate the pseudonyms and insert them in the blockchain. The aim is to reduce the cost of the VPKI, prevent the single point of failure issue and provide a distributed secure pseudonym management framework.

## IV. Thesis Structure

The thesis is organized into a total of five chapters. The first two chapters are a literature review. The following three chapters are our contributions. The chapters' brief descriptions are given in what follows:

- **Chapter 1: Vehicular Networks**

This chapter aims to clarify the basic concepts related to vehicular networks. Their evolution, technology, architecture, characteristics and challenges. It also lists their standards, applications and real-world implementations. The chapter also includes public opinions about these networks. Most importantly, it enumerates the various types of vehicular networks and highlights the key differences between them.

- **Chapter 2: Privacy and Security in Vehicular Networks**

This chapter introduces the reader to the privacy and security issues in vehicular networks. We particularly focus on identity and location privacy and on the authentication as a security issue. The chapter explains the privacy issue and sheds light on its importance and the potential consequences of its violation. It also answers questions about why the privacy is threatened, when, by whom and how. It resumes prominent security issues in vehicular networks and defines our attacker model. Similarly, the authentication issue is explained and its contradiction with privacy requirements is highlighted. The chapter also surveys prominent existing solutions

for each issue separately. Moreover, it included the security and privacy evaluation metrics and tools.

- **Chapter 3: Privacy-preserving Authentication Methods.**

In this chapter, two anonymous authentication methods for two types of applications are proposed. The first is a mutual authentication method between the vehicles to share their resources and form the Cloud-enabled Vehicle Named Data Networks dynamically on roads. The proposed anonymous reputation-based mutual authentication method is proved to achieve its underlined aims using BAN Logic. The second application is the on-road on-demand pseudonym refilling requests preceded by the anonymous challenge-based authentication method. The proposed authentication method ensures the authenticity, integrity, non-repudiation and revocation. Furthermore, it is resilient to man-in-the-middle attack, replay attack, impersonation, brute-force and Sybil attacks. We used BAN logic to prove its correctness and SPAN and AVISPA to prove that it is safe, it ensures the authentication aims and it is resilient to well-known attacks.

- **Chapter 4: Preserving the location privacy for Vehicular Networks Users**

The location privacy issue in vehicular networks is a critical issue. Trajectory tracking is risky. It results from accurate linkability between updated pseudonyms. The consequences of tracking may vary from stalking, blackmailing to assassination. Various solutions exist in literature aiming to reduce the linkability and tracking ratio. In this chapter, we propose two solutions to protect the location privacy for VANET users. The solutions are road, crowd and infrastructure independent. Both aim to reduce the linkability ratio even when the vehicle is within low-density roads. They were analyzed by simulation against the attacker model defined in Chapter 2. The first proposal reduced the tracking ratio to an average of 27%. The second proposal was even better with an average tracking ratio of 10.4%.

The chapter also includes the proposition of three location privacy-preserving solutions for IoV users. The solutions are also tested through simulation against the attacker model defined in Chapter 2. Each solution is the amelioration of its predecessor. These ameliorations aimed to reduce the tracking ratio. Noting that the lower is this ratio, the higher is the level of privacy provided by the solution. The obtained ratios are 30%, 16% and 10% on average for the three proposals respectively.

- **Chapter 5: Blockchain-Based Privacy-Aware Pseudonym Management Framework for Vehicular Network**

In this chapter, we propose a potential replacement framework to the vehicular PKI which suffers from a single point of failure and is costly to deploy. The framework is a blockchain-based. It preserves the privacy even though it is public. It ensures the authentication, revocation, non-repudiation and integrity. It inherits the security strength of the blockchains, prevents the alterations and ensures the availability. The framework is a blockchain of two public blockchains. The first blockchain is permission-less and it contains the vehicles generated pseudonyms. The second is permissioned and it contains the revoked pseudonyms. Our framework proved to provide the same requirements ensured by the VPKI while ensuring a higher level of security.

# List of Figures

# List of Tables

# List of Algorithms

# List of Acronyms

**A**

AASS : Average Anonymity Set Size
ASS : Anonymity Set Size
AVISPA : Automated Validation of Internet Security Protocols and Applications

**B**

BAN: BURROWS, ABADI and NEEDHAM
BC: Blockchain
BCN: Beacon

**C**

CA : Certifying Authority
CAAS : Cooperation-As-A-Service
CE-IoV : Cloud Enabled Internet of Vehicles
CIoV : Cognitive-IoV
CLPPS : Cooperative-based Location Privacy-preserving Scheme for Internet of Vehicles
CM : Cloud Manager
COO : Cooperation
CPS : Certified Pseudonyms
CS : Content Store
CSLPPS : Concerted Silence-based Location Privacy-preserving Scheme for Internet of Vehicles
CVD : Change VMID
CVNDN : Cloud-enabled Vehicle Named Data Networks

**D**

DataPk : Data Packet
DC : Do the change
DRL : Data Reliability
DSRC : Dedicated Short-Range Communications

**E**

EDGE : Enhanced Data rates for GSM Evolution
ERGS : Electronic Route Guidance System

**F**

FCC : Federal Communications Commission

FIB : Forwarding Information Base

**G**

GPA : Global Passive Attacker
GPRS : General Packet Radio Service
GPS : Global Positioning System
GSM : Global System for Mobile

**H**

HLPSL : High Level Protocol Specification Language
HMI : Human Machine Interface
HSDPA : High-Speed Downlink Packet Access
HVC : Hybrid Vehicular Cloud

**I**

IC-NOW : Information Centric Network on Wheels
INAAS : Information-As-A-Service
IntPk : Interest Packet
IoT : Internet of Things
IoV : Internet of Vehicle
ITS : Intelligent Transport System

**L**

LTCA : Long-Term Certification Authority

**M**

MITM : Man In The Middle
MSC : Message Sequence Chart

**N**

NAAS : Network-As-A-Service
NDN : Named Data Networks
NOW : Network On Wheel
NRV : New Reputation Value

**O**

OBU : On-Board Units
ORV : Old Reputation Value

**P**

PCA : Pseudonym Certification Authority
PIT : Pending Interest Table
PKI : Public Key Infrastructure
PoS : Proof of Stake
PoW : Proof of Work
PRA : Pseudonym Resolution Authority
PROMETHEUS : Program for European Traffic with Highest Efficiency and Unprecedented Safety
Psd : Pseudonym
PUF : Physically Unclonable Functions

**Q**

QoS : Quality of Service

**R**

RA : Regional Authority
RCA : Root Certifying Authority
RCP : Resource Command Processor
RDC : Ready To Do The Change
RFID : Radio Frequency Identification
RS : Registration Server
RSU : Road Side Units

**S**

SC : Service Continuity
SDN : Software Defined Networks
SDVN : Software Defined Vehicular Networks
SF : Selfishness
SIG :Signature
SPAN : Security Protocol Animator
STAAS : Storage-As-A-Service

**T**

TA : Trusted Authority
TMN : Testimony
TPD : Tamper Proof Device
Tx : Transaction

**U**

UMTS : Universal Mobile Telecommunication System

**V**

V2H : Vehicle-to-Human
V2I : Vehicle-to-Infrastructure
V2N : Vehicle-to-Network
V2S : Vehicle-to-Sensors
V2V : Vehicle-to-Vehicle
V2X :Vehicle-to-Everything
VC : Vehicular Cloud
VIN : Vehicle Identification Number
VM : Virtual Machine
VN : Vehicular Networks
VS : Verification Server
VuC : Vehicle Using the Cloud

# PART I: LITERATURE REVIEW

# CHAPTER 1

# VEHICULAR NETWORKS

## 1.1. Introduction

The vehicular networks have been the core of the Intelligent Transport System (ITS). The interest toward these networks has been growing bigger because of the necessity to reduce road fatalities which cause huge yearly losses in terms of human lives, mental and physical health after-effects, property damages and financial losses. They were initially developed to ensure the safety of road users by having accurate prior knowledge about the traffic, the shortcuts and the road condition. Also, by allowing the users to have comfortable safe trips in their self-driven vehicles. Moreover, vehicle networks may allow smooth driving and reduce traffic jam which helps in reducing fuel consumption.

In this type of networks, the vehicles are the main nodes regardless of their type. They are often referred to as computers on wheels. The vehicles are equipped with sensors for various internal and external purposes such as sensing engine heat or closeness distance. The Global Positioning System (GPS) for localizing the vehicle. Cameras, lidar and radar to sense the surroundings, detect road condition and obstacles. The Onboard Unit (OBU) which is the vehicle brain and computer that controls it, processes the sensed data and ensures its correct functioning. It is what gives the vehicle the smartness trait which is the reason they are called smart vehicles. They are also equipped with network interfaces to communicate together, besides a storage space to store the sensed data, received messages and other security programs.

The vehicular networks englobe various types in which the vehicle is the main participant. It includes the autonomous vehicles, the Vehicular Ad Hoc Networks (VANETs), the vehicular cloud computing, the internet of vehicles and vehicular named data networks. These types could be considered as the extensions or the evolution of the vehicle networks as its applications evolved. Its earliest applications were safety related, focusing on how to assist the driver. Then, later the infotainment applications became necessary. Finally, the internet and cloud computing were extended to provide road users with their services.

In this chapter, we give a review on the vehicular networks, their evolution and their applications. It will be organized on thirteen parts:

Part 2 highlights in digits the fatalities caused by vehicle accidents yearly and the estimations of the benefits of the vehicular networks in ensuring safety besides the evaluation of their market value.

Part 3 describes the evolution of the vehicular networks which is part of the intelligent transportation systems and road automation projects.

Part 4 explains the intelligent vehicles components and the vehicular networks architectures.

Part 5 briefs the vehicular networks main distinguishable characteristics.

Part 6 enumerates the technical challenges and issues facing the real implementations of the vehicular networks.

Part 7 lists the potential wireless technologies used in the vehicular networks.

Part 8 outlines the standards that regulate these networks.

Part 9 explains the different existing types of vehicular networks.

Part 10 lists some real-world implementations projects and test-beds.

Part 11 illustrates various examples of the vehicular networks offered services and applications.

Part 12 surveys the public opinion and acceptance of the technology.
Part 13 concludes the chapter.

## 1.2. Motivation by numbers

To highlight the importance of the vehicular networks, we give a few statistics [1]:

- Yearly, approximately 1.3 million people die,
- More than 7 million people are injured, and,
- Around 8 million traffic accidents are recorded.
- People waste over 90 billion hours because of accidents and traffic jams.
- Vehicles generate 220 million metric tons of carbon.
- The estimations of the Internet of Everything global market are said to reach 14.4 trillion Dollars by 2022 [2] and the Internet of Vehicle value alone would reach 129.33 billion Dollars (115.26 billion Euros) by 2020 [1].
- More importantly, the use of autonomous vehicles could eliminate 80-90% of the vehicle's crashes and accidents [3].
- A rough estimation states that it would take from 14-15 years to reach 100% of Market penetration of vehicular networks starting from the initial deployment date [4].

With these digits and statistics, it is daylight clear that the vehicular networks would serve the purposes they were made for in reducing car accidents, injuries, deaths, pollutions…etc. The academics and industrials are playing their parts in bringing this technology to life and seeing it in markets. What is left is to shift the attention of the public opinion to convince them about the benefits of this solution and draw their attention to it.

## 1.3. Evolution

Automation of roads and creating self-driving vehicles have been the dream of many researchers and industrial forces. General Motors was the first to exhibit the basic concepts of road automation as "Futurama" at the 1939 World Fair. Followed by, the USA proposition of the Electronic Route Guidance System (ERGS) in 1970. It guides the drivers to their destination which is transmitted to the roadside unit at each intersection to be decoded and the roadside infrastructure transmits back the routing instructions. In Japan, the Comprehensive Automobile Traffic Control System was carried out from 1973 to 1979. The project has the objectives to reduce traffic congestion, air pollution and to prevent accidents. Also, to guide the driver along the appropriate route by providing him/her with accurate information and warnings [5]. In Europe, the PROMETHEUS (Program for European Traffic with Highest Efficiency and Unprecedented Safety) framework was initiated in 1986 and launched in 1988.

The term vehicular networks as we know it today was first coined by Ken Laberteaux in the first International Workshop on Vehicular Ad hoc Networks which was held in 2004 in Philadelphia [6]. It was considered as the first commercial version of Mobile Ad-hoc Networks and one of its most promising applications that would automate the roads and ensure its user's safety and comfort. It approached the community from realizing the vision of self-driving vehicles [5].

Ever since, the VANET has become a topic of interest and many projects and consortium were launched every year few of them are the FleeNET, the Car2Car consortium, the CarTalk2000, Network On Wheel (NOW), PReVENT, MobiVip…etc. [7]

Starting of 2010, a new type of vehicular networks appeared, it merges the cloud computing with the vehicular networks to form the vehicular cloud (VC) concept. The VC takes advantage of the vehicles sensing, calculation and storage capacities to extend the clouds which offer various kinds of stable services [8]. As of 2014, researchers started working on the internet of vehicles [5] [9] which is a subtype of the internet of things and the evolution of VANETs.

Google's first self-driving and a real implementation of autonomous vehicles started as a project in 2009. It continued its trials and tests and first hit the public road in 2015. In 2016, the project was named Waymo and became independent under Alphabet as a self-driving technology company [10]. Meanwhile major car companies such as Mercedes, Audi, Tesla, Renault, etc. have been competing to launch their own self-driving vehicles [11].

## 1.4. Architecture

The autonomous vehicles also known as the self-driving vehicles are smart. They are divided into two types (see Figure 1.1): The first one is the self-dependent (self-contained), in which the vehicle relies only on its computational capacities and smarts (algorithms and programs) to process the sensed data, take decisions and execute the instructions. The second type is the interdependent, in which the vehicle is either connected to a control server to exchange data and instructions via Vehicle-to-Infrastructure (V2I). Or, it is connected to other vehicles and network nodes to exchange sensed data via Vehicle-to-Everything (V2X). The second type is often referred to as the vehicular networks. Although the types differ, but, the design and components of the smart vehicles are similar [12].

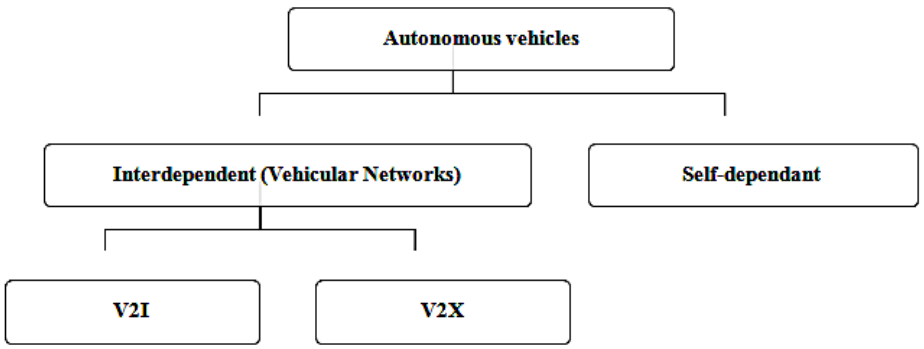



**Figure 1. 1 : Autonomous Vehicles**

The Vehicular networks, in general, follow the basic architecture of VANETs. It is composed of vehicles known as nodes or Onboard Units (OBU) and Road Side Units (RSU). The OBU can record, calculate, locate, and send messages over a network interface [5]. It is composed of a Resource Command Processor (RCP), a read/write memory used to store and retrieve information, a user interface, and a network device for short-range wireless communication based on IEEE 802.11p radio technology [13].

The RSUs broadcast information and advertisements or relay data sent by vehicles [5]. It is equipped with network devices for a dedicated short-range communication based on IEEE

802.11p radio technology, and for communication within the infrastructural network [13]. The basic components of the smart vehicle were initially resumed in the use of sensors, radar, GPS, network interfaces, onboard computer (processing and storage) and a human-friendly interface like illustrated in Figure 1.2.

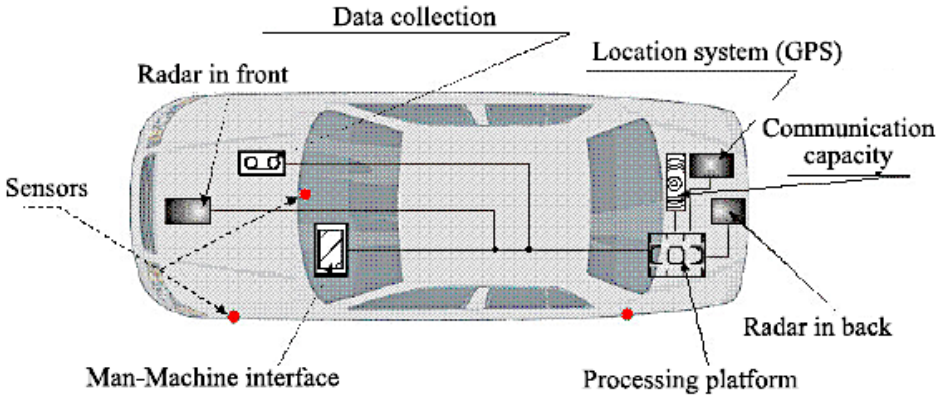



**Figure 1. 2** : Intelligent Vehicle **[7]**

However, the technology is continuously developing and many car makers competing on the implementation and testing of these intelligent vehicles. Therefore, the components are becoming more refined, sophisticated and advanced. Google smart car is an example of the current sophisticated smart cars [14].

## 1.5. Characteristics

Vehicular networks are particular in nature, due to the high dynamicity of vehicles, special characteristics differentiate this type of networks, among which are:

- Highly dynamic topology due to the high speed of vehicles
- Predictable movements because the vehicle runs on known roads and paths
- Frequent fragmented networks which might cause a delay or the non-delivery of messages
- The use of internal and external sensors of different types and for various purposes
- Unlimited battery power and storage capacity [15]
- Variable network density (in the city, in rural areas, in roads, during daytime, during night-time …etc.) [13]
- The obstacles such as tall buildings
- Security and privacy challenges [16]
- Available real-time geographic position of the vehicles [17].
- Geographical communications based on location information [18].

## 1.6. Technical Challenges and issues

The implementation of vehicular networks in real-world is challenged by some technical obstacles and issues that need to be resolved. In this section, we mention a few of them:

- Signal fading due to the huge distance between cars (sparse network) or because of the multiple obstacles (urban areas)
- Bandwidth limitation, which can cause congestion if excessive simultaneous applications are used being in urban areas with high vehicle density. In this case, even the fair use of the bandwidth can increase the latency.

- Connectivity problems due to the vehicles' high mobility and to the network small effective diameter frequent fragmentation of the network may occur.
- Keeping a balance between security and privacy in VANETs
- Due to the rapid change of topology, designing a reliable routing protocol for VANETs has been the focus of a lot of researchers. These protocols should deliver the packets in the shortest time possible even in a dense network (scalability) with a lot of obstacles. [13]
- VANETs inherit the problem of hidden and exposed terminals from MANETs.
- The high cost of the Infrastructures and roadside units, the connectivity and the IT-management issues are the reasons that are holding back the implementation of VANET in the real-world [6].

## 1.7. Wireless Technology

Various wireless technologies may be used to ensure the connectivity between the VANET components, among which are:

- **Cellular Systems:** The main idea is to use the existing cellular systems for VANETS to exchange data and messages. Among the reused systems are: The Global System for Mobile (GSM) also known as 2G, the General Packet Radio Service (GPRS) also known as 2.5 G, Enhanced Data rates for GSM Evolution (EDGE) also known as 2.75 G, 3G, the Universal Mobile Telecommunication System (UMTS), High-Speed Downlink Packet Access (HSDPA), the CMDA2000, LTE 4G and 5G.
- **WLAN/Wi-Fi:** It can be used to provide wireless access to enable V2V or V2I communications.
- **WiMAX:** Worldwide Interoperability for Microwave Access also known as IEEE 802.16e. If it is used, it achieves high data rate, covers a wide transmission range and has a high quality of service
- **DSRC/WAVE:** The 75MHz licensed spectrum at 5.9 GHz in the USA and at 5.8 GHz in Europe and Japan. It can be used solely for vehicle-to-vehicle and vehicle-to-infrastructures communications.
- **Combined Wireless Access Technology:** It combines a set of wireless technologies such as GSM, GPRS, 3G [13].

## 1.8. Standards

To specify the operation of vehicle networks from physical to application layer, a set of protocols were standardized. The standards are mainly developed in Europe, Japan and North America. There are two major standardization groups the IEEE WAVE stack and the ETSI ITS-G5 protocols in North America and Europe respectively [19].

The vehicles communicate with other vehicles and road side units through Dedicated Short-Range Communications (DSRC). The DSRC provides high data transfers and low communication latency in small communication zones. In 1999, the United States Federal Communications Commission (FCC) allocated 75 MHz of spectrum at 5.9 MHz to be used by DSRC. The DSRC is free but licensed spectrum organized into seven channels of 10 MHz each. One channel is for safety communications only, two other channels are reserved for special purposes and the remaining four are service channels [20]. The data rate can be 6, 9,

12, 18, 24 and 27 Mbps for 10Mhz channel. It can be increased to 54 Mbps for 20 MHz channels.

### 1.8.1. IEEE WAVE stack

The WAVE IEEE standards define the set of standards for each layer. It has a stack for safety and for non-safety applications, Figure 1.3 illustrates the IEEE WAVE standards [21], and Figure 1.4 shows a simplified view of it.

<table>
<tr><td></td><td>Safety applications</td><td>Non-safety applications</td></tr>
<tr><td></td><td>Safety application sublayer</td><td>Application</td></tr>
<tr><td rowspan="2">Security IEEE1609.2</td><td>Message sub-layer SEA J2735</td><td>Transport (TCP/UDP) IETF RFC 793/768</td></tr>
<tr><td>WSMP (IEEE 1609.3)</td><td>Network (IP V6) IETF RFC 2460</td></tr>
<tr><td></td><td colspan="2">LLC Sublayer IEEE 802.2</td></tr>
<tr><td></td><td colspan="2">MAC sublayer extension IEEE1609.4</td></tr>
<tr><td rowspan="2">802.11P</td><td>MAC sublayer</td><td>MAC layer</td></tr>
<tr><td>PHY sublayer</td><td>PHYSIC layer</td></tr>
</table>

**Figure 1. 3 :** IEEE WAVE standards **[21]**

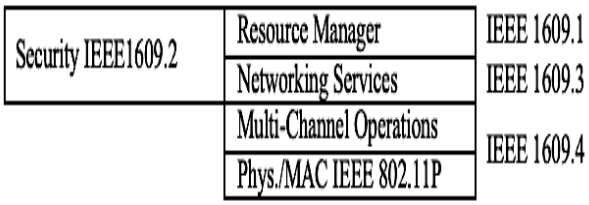



**Figure 1. 4:** A Simplified WAVE Standard View **[22]**

- **The IEEE 802.11P:** IEEE 802.11p mac protocol for VANET which extends the 802.11e.
- **The IEEE1609.1:** defines the messages formats and their responses.
- **The IEEE 1609.2:** defines the formatting, processing and exchange of secure messages.
- **The IEEE 1609.3:** defines the routing and transport layer services.
- **The IEEE 1609.4:** defines the multichannel operations [22].

### 1.8.2. ETSI standards

The ETSI standard illustrated in Figure 1.5 is the equivalent of the US IEEE WAVE standards for ITS and vehicular networking in Europe. The access technologies layer is the adapts of the IEEE 802.11p standard on the European standard. It defines the physical and MAC layers protocols. The network and transport layers define the geo-networking and IP-based protocols, besides the transport layer protocols. The facilities layer manages the messages and services and it supports information, communications and applications. The Application layer defines a basic set of applications related to road safety and traffic efficiency. The management layer is cross-layer that plays a central role in controlling all the layers. The security layer defines the protocols ensuring the privacy, the integrity, the non-repudiation and the authentication [21].

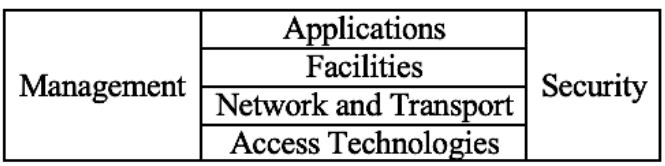



**Figure 1. 5:** ETSI TC ITS protocol stack **[21]**

### 1.8.3. *GPP standard*

The 3GPP V2X enhances the DSRC by leveraging traditional cellular networks, it offers double range for V2V communications than the DSRC. Also, it functions both in-coverage of cellular networks and out-of-coverage via V2V communications. It offers robust Vehicle-to-Network (V2N) and V2I communications [23]. Compared with IEEE 802.11p, cellular-based V2X can provide better QoS support, larger coverage, and higher data rate for moving vehicles. Additionally, V2X is synchronous, while IEEE 802.11p is asynchronous. Although V2X services can coexist with IEEE 802.11p based radio access in adjacent channels, V2X has the additional advantages of being evolvable and scalable [24]. Noting that in 3GPP V2X standard the periodical messages have variable payloads of 50-300 bytes and frequency up to 10 messages per second. While the event-triggered messages have payloads up to 1200 bytes [25].

## 1.9. Types

The vehicular networks represent various types of networks in which the vehicles on roads are the main type of nodes. Many people are familiar with the VANET term that they confuse all the vehicular network types as being it. However, it is true that the VANET is the first type introduced, but, as the time passed, the concept evolved with the introduction of new needs, purposes and applications. VANET can now be seen as the building block of more sophisticated, global and high-level vehicular technologies and networks which will be explained in the subsections below.

### 1.9.1. The Autonomous Vehicle *(self-dependent)*

The self-contained (self-dependent) autonomous vehicles rely solely on its processing abilities, artificial intelligence and sensing powers. The vehicles which are equipped with GPS, maps, cameras and radars; make decisions locally. No instructions nor commands are sent from afar server or control unit, also no network is used in the process [12].

### 1.9.2. VANET

The VANET refers to the vehicular networks composed of Vehicles as main nodes also known as onboard unit and road side units. The communication between the vehicles is wireless through Dedicated Short-Range Communication (DSRC) known as the vehicle-to-vehicle (V2V). The DSRC is also used between the vehicle and the infrastructure or the RSU. This communication is known as Vehicle-to-Roadside unit (V2R). The VANET was developed mainly for safety applications that would decrease road accidents and causalities. In addition to the infotainment applications it offers to provide the road users with information and services. Therefore, the vehicles generate different kinds of messages which are classified into safety messages such as the periodic state beacons and the event-based alert message. Additionally, to the non-safety messages which are the service messages focusing on entertainment, information and comfort applications [6] [13].

### 1.9.3. Vehicular *Clouds*

The vehicular cloud extends the conventional clouds to the vehicular network edge. Owing to the fact that, each vehicle is equipped with an onboard unit responsible for processing the

data besides the storage and sensing resources. These capacities may be exploited to form clouds known as vehicular clouds or VANET clouds.

In [26] authors suggested the exploitation of vehicle sensing and storage capacities to better manage the traffic. They proposed a vehicular cloud-based navigation system and an urban surveillance system that would save the on-road sensed data. It uses the vehicles' cameras to read vehicle palates numbers and film roads. These data and videos are saved locally in the vehicle with their summary saved on the internet to help forensic investigators and police to harvest them. The videos may contain proofs against criminals especially in (hit-and-run) accidents, assault or bombing. In their paper, the authors focused on the applications rather than on the architecture of the vehicular types.

Authors of [27] gave the various applications that may be offered by the vehicular clouds such as:

- The network-as-a-service (NAAS), in which the vehicles that have internet access may offer this facility to other vehicles that need it.
- The storage-as-a-service (STAAS), the vehicle can rent its storage capacity to other vehicles in need to for example save large files or do back-ups.
- The cooperation-as-a-service (CAAS), vehicles can cooperate to collect and disseminate the data basing on the interest. In other words, the data will be routed basing on its content to the interested parties in a fast way. Thus, the vehicular cloud will be divided into content-based clusters.
- Computing as service, the vehicles are equipped with sophisticated onboard units that are responsible for the calculations and the processing of sensed data. However, it was noticed that most of these vehicles are idle in the parking lots for various hours a day. Therefore, it is best to exploit the processing capacities of these idle units to offer computing as a service.
- Picture-as-a-service, the vehicles are equipped with high-resolution cameras. Being mobile on road, they can offer a better vision on the road than the static infrastructures. They can provide real-time images on road state and valid proofs for the police if a crime occurs.
- Information-as-a-service (INAAS), the vehicle may provide or consume various kind of information either safety related for the driver, or entertainment information for the passengers onboard.

The authors classified the vehicular cloud architecture into three types: the static, the dynamic and the infrastructure-based. In the static VC, vehicles extend the conventional clouds. They unify their capacities and resources to offer services to the users. An example of such a cloud can be in parking lots of the malls, offices or airports. The dynamic VC is formed by the on-road running vehicles. Adjacent vehicles can unify their resources to form these local clouds. The infrastructure-based VCs are found in urban areas where the infrastructures are distributed across roads, the infrastructure and the vehicle form the cloud. The infrastructure or RSU can play the role of the cloud coordinator as well as extends the VC to the conventional clouds.

Authors of [28] claimed that the vehicular clouds are more suitable for software as a service and infrastructure as a service but not very suitable for the platform as a service. Noting

that in the latter, the user is offered development platform so as s/he is able to develop applications remotely. Furthermore, they classified the VANET Cloud into three types which are the Vehicular clouds, the Vehicle Using the Cloud (VuC) and Hybrid Vehicular Cloud is (HVC). In the VC, the vehicles which can be either static or dynamic unify their resources to form a cloud where they can rent their services. In the VuC, the vehicles use the conventional cloud services on road and in the HVC, the vehicular clouds formed by the vehicles use conventional cloud services. The HVC is the combination of VC and VuC.

### 1.9.4. Internet of Vehicles

The internet of vehicles is an integral part of the internet of things (IoT) and one of its instantiations [5] [9]. It is the evolution and the extension of the VANETs. It integrates humans, vehicles, things and environment. The human includes the people within the vehicles (driver or passenger) and people surrounding it such as cyclists and pedestrians. The things refer to other devices and entities that are neither human nor vehicles such as traffic signs or access points. The environment includes humans, vehicles and things [9].

The IoV relies on the use of vehicular clouds as its core technology [5]. It uses various wireless technologies such as the DSRC, WIMAX, cellular networks (3G, 4G, 5G), satellite networks. Therefore, it offers various types of real-time and non-real-time services that are more stable and global [9].

The IoV has two main technology directions. The first is the vehicle's networking which consists of the VANET, vehicle telematics (exchange of data) and mobile internet. The second is the vehicle's intelligence which reflects the combination of the vehicle and the user, the artificial intelligence usage, deep learning and cognitive computing [9]. Noting that, the vehicle in the IoV is considered as a swarm of sensors that are used to collect data about the road, the vehicle’s condition and its surroundings. Besides its sophisticated processing units and large storage capacities [2].

Authors of [1] illustrated the seven-layers models of the IoV which are:

- ***The User Interface Layer:*** it is the layer that facilitates the interaction between the user and the vehicle, it enables him/her to query the onboard system, use the IoV services and receive notifications.
- ***The Data Acquisition Layer:*** It collects the data either by the use of the vehicles’ sensors or by receiving sensed information from other vehicles and infrastructure.
- ***The Filtering and Pre-processing Layer:*** This layer filters and pre-process the data basing on their utility, validity and used-service.
- ***The Communication Layer:*** The communication and the emission of messages can be done using various technologies such as DSRC, WIFI, WiMax, 3G, 4G, 5G.
- ***The Control and Management Layer:*** It uses different traffic management policies and packet inspections methods to manage the received information.
- ***The Processing Layer:*** It uses vehicular clouds and conventional clouds capacities to process and store the collected and received data.
- ***The Security Management Layer:*** This layer is transversal. It is responsible for ensuring security properties for all the layers.

Due to the autonomous vehicle's intelligence and deep learning mechanisms, a new concept appeared which is considered as the evolution of IoV which is the Cognitive-IoV (C-IoV) [29]. It combines the autonomous vehicles intelligence with the vehicular networks, cloud computing and cellular networking. It is more accurate in term of perceptive ability concerning the vehicle's surroundings and interactions as well as more reliable when making decisions also more efficient in using resources.

The architecture of C-IoV has 5 layers:

- ***Sensing Layer:*** collects the data.
- ***The Communication Layer:*** It includes the cloud interactions and conventional vehicular networks communications.
- ***Cognition layer:*** It processes the data using machine learning, deep learning, data mining, pattern recognition, etc.
- ***Control layer:*** It relies on the use of distributed decision making for fast response and expected QoS of vehicular networks.
- ***Application layer:*** It provides various stable services and applications.

### 1.9.5. Social Internet of Vehicles

With the emergence usage of social media networks and considering that the vehicle is the third place where people probably spend most of their time in after their home and office. The extension of social network concept to the vehicular network is becoming a necessity. Drivers and passengers may share real-time events about the roads (road works, accidents), restaurants and café offers, new shops and gyms, or even beautiful scenery [30]. This gave birth to vehicular social network and more precisely to the social Internet of Vehicles which is a use case of the Social IoT.

The social IoV is defined as the social interactions between vehicles and between the drivers. Some defined it as a network formed by the drivers in the same area with a similar interest. Others defined it as the interactions between autonomous vehicles to exchange data and services [3]. Authors of [31] defined the social IoV as a cyber-physical application over the physical vehicle networks of WAVE. In which the RSU, home and OBUs form a cyber-physical social network to exchange data. The interactions of data form a social graph where the entities represent the graph nodes and the exchanged data represents the graph links [31].

However, the authors of [3] affirmed that the social IoV will be defined in the future as the social interactions of drivers, passengers and vehicles. It allows the vehicles ranking basing on certain characteristics. The ranks can be used to help taking interaction decisions. It can be exploited in the trust and reputation building which are important security properties in vehicular networks.

### 1.9.6. Data named vehicular networks

Information Centric Network on Wheels or IC-NOW is a vehicular network that focuses on the information content rather than the conventional addressing methods. The information scope is defined by the relevance of its space, time and user's interest. It is also known as the vehicular named data networks or vehicular NDN in which the routing between vehicles is content-based rather than IP-based [4].

The packets exchanged between vehicles and roadside units can be information centric which mean they are shared between users with the same interest and spatiotemporal scope. Yet, this does not mean that these networks are totally independent from the conventional IP based networks. The IC NOW encapsulates the V2V, V2I exchanged packets in IP packets, if it needs to send these packets over the internet or when using cloud services [4].

Noting that, each NDN node maintains three data structures: Forwarding Information Base (FIB), Pending Interest Table (PIT) and Content Store (CS). The vehicle that is interested in a packet, sends an interest packet (IntPk). If the requested content is found in the CS, the DataPk is sent to the requester. Otherwise, the IntPk is inserted in the PIT to be forwarded to a potential CS from the FIB [32] [33].

### 1.9.7. Software Defined Vehicular Networks

In the Software Defined Vehicular Networks (SDVN), the communication of data is logically controlled by the centralized control plane. The difference between the SDVN and the vehicular NDN is that the NDN focuses on the content-based routing of data. While SDVNs separate the control and the data plane to make various services manageable without physical interference with switches and routers. Noting that the vehicles in SDVN have multiple interfaces [34].

The SDVN is composed of:

- SDN controller has a global overview of the networks. It orchestrates its elements to perform the NDN operations which are the cashing, the intelligent interest, data forwarding…etc.
- The cashing: which is a fundamental operation performed by forwarding nodes. The choice of these nodes and the format in which the content is cashed are important in ensuring fast query/response. The content may be non-compressed, compressed, chunked saved all in one node or in multiple ones.
- The content naming is another essential component which is responsible for naming the contents and their chunks. The naming facilitates the search for the data when an interest request is received by the vehicle. Noting that each content has space and time information it belongs to.
- The intelligent forwarding: The Forward Interface Base (FIB) is responsible for maintaining the content communication. Every time a content is satisfied through a face, this face gets ranked. If the face satisfies no interest, its rank drops and as a result it gets purged from FIB. If the FIB is empty the requests are forwarded to the controller to be satisfied otherwise.
- The push-based forwarding is used to deliver warning in fast way for potentially interested nodes.
- The intrinsic data security: every data message is digitally signed. The SDN controller disseminates the vehicles security policies regarding a content to other vehicles interested in it.
- Congestion control: due to the popularity of certain contents, the congestion may occur. Therefore, each node needs to send the traffic status at every face so as the controller can alleviate the congestion by evenly distributing the traffic over various cashing points.
- The topology indicator: each vehicle provides its position, speed and direction to the control manager to help select and disseminate the forwarding rules.

- The content prefix manager, every node sends to the controller its content store (cashed data) with its validity and expiry to help in forwarding the interest requests.
- The state information is calculated by each vehicle per each interface. It gives a report on the requests/ satisfied queries to help the controller come with a better cashing/forwarding policy [34].

## 1.10. Test-Beds and real Implementations

Middlesex University - UK created the Middlesex VANET Research Test-bed. The Test-bed is located at Hendon Campus in London and has four RSUs mounted on various buildings. The test-bed was created to test their VANET research network [35].

The Porto Living Lab – Portugal has two independent test-beds for VANET: urban and harbor, located at the city of Porto and at the harbor of Porto, respectively. In both the harbor and urban test-beds, each vehicle is equipped with an OBU, which includes a GPS receiver, and DSRC, Wi-Fi and cellular communication interfaces. Vehicles connect to the Internet through RSU or by cellular communications. The V2V and V2I communications are through DSRC. The majority of the deployed RSUs at the urban test-bed were installed at traffic light poles and traffic control camera poles and at buildings managed by the University of Porto [36].

The UCLA-USA has developed its vehicular test-bed C-VeT, to do an experimental evaluation of protocols and models for MAC and Network Layers. MIT-USA developed CarTel and Cabernet test-bed. Massachusetts Amherst- USA also developed two projects named Dome and DieselNet projects [37]. Microsoft has its own Test-bed for VANET called VanLan, established in 2008 [38]. There is also the ITS corridor from Amsterdam through Germany to Vienna project which is still in progress [39].

Among the completed projects in Europe are the Compass4D (2016) [40], DRIVE C2X (2014) [41], SimTD (2013) [42].

Also, there are over 200 ITS-related projects underway across Canada, including two Connected Vehicle “test-beds” at the Universities of British Columbia and Alberta [43].

## 1.11. Services and Applications

The vehicular networks were developed to ensure users safety, comfortable driving, maintain smooth traffic, reduce fuel consumption and air pollution, …etc. They offer various applications and services such as [7] [13] [15] [44]:

- **Safety application:** it has the highest priority because it helps prevent accidents and thus, it saves the human lives. Among its examples are:
  - *Alert in case of accident*: it helps prevent other road causalities. It ensures a faster response by rescue services (Ambulance, Police). It facilitates the road evacuation and assist in planning secondary roads and detours.
  - *Cooperative driving*: it helps a better management of traffic, and fuel consumption. It is sometimes referred to as vehicle platooning.
  - *Collision avoidance*: to avoid bumps and crashes, vehicles use their in-build sensors, radar and lidars to detect and quickly responds to the road obstacles. Furthermore, every vehicle broadcast real-time accurate information about its current position, speed and

headings, to avoid the collision especially when changing lanes, doing U-turns, or upon sudden brake, etc.

- *Security distance warning*: the vehicles keep a security distance which is usually either a specific fixed number of meters or that is dependent on the response time in case of sudden brake for example which is the time that the vehicle takes for it to execute the instruction of stopping. This distance depends also on the vehicle's speed. If the security distance is not kept the warning is sent.
- *Lane changing*: the vehicle reports that it is changing its lane for other vehicles to know to avoid colliding with them. Just like using turn sign when manually driving.
- *Navigation and Map Location*: most of the recent vehicles are equipped with a navigation system that matches your current location obtained from GPS with the in-built map to allow users to plan their trajectories.
- *Alert in case of a traffic jam or road work*: these event-based alerts are propagated in the networks to help users plan secondary routes.
- *Public safety* (SOS, approaching emergency vehicle, post-crash warning…)
- *Vehicle diagnostic and maintenance*: vehicles can be diagnosed on road. In case of issues, priory reports can be sent to the nearest car care Centre for faster and more efficient service provision.

▪ **Comfort application**: It groups the application that aims to entertain and comfort the users such as:

- Internet access, video streaming, chat between car users, network games and other advanced stable services.
- Weather warnings and forecasts.
- Advertisement messages (near/cheap/expensive or excellent) Hotel, restaurant, gym, petrol station or touristic information…. etc.

▪ **Driver Assistance:** It helps the driver, provides necessary warnings and support information.

- Parking management and spot reservation
- Automatic Parking
- Driverless or the self-driving Vehicle: in which, the vehicle can be completely autonomous when it drives relying only on its system or semi-autonomous where the driver is still needed to interfere. Figure 1.6 illustrates the different levels of automated driving [45] which are explained below [3] [24]:
  - *Level 0*: The driving system needs a human driver to drive and monitor the driving environments.
  - *Level 1*: The driving system assists either in steering ***or*** acceleration/deceleration on the current driving environment.
  - *Level 2*: The driving system supplies both steering ***and*** acceleration/deceleration assistance based on the current driving environment.
  - *Level 3*: The driving system intervenes in the dynamic driving tasks based on the driving environment, while drivers respond to the intervention requests.
  - *Level 4*: The driving system intervenes in the dynamic driving tasks based on the driving environment, with or without the driver's responses to the intervention requests.

- *Level 5*: The driving system executes all dynamic driving tasks just like the human driver.

| | | |
|---|---|---|
| Human Driver Monitors the driving environment | 0 | No Automation |
| | 1 | Driver Assistance |
| | 2 | Partial Automation |
| Automated driving System Monitors driving environment | 3 | Conditional Automation |
| | 4 | High Automation |
| | 5 | Full Automation |

**Figure 1. 6:** Automated driving levels

## 1.12. Public Opinions

In [46] report, a survey was conducted to study the public's opinion about autonomous and self-driving vehicles in the UK, USA and Australia. The majority of respondents were familiar with the technology or at least aware of its existence. While most of them had high expectations about this technology, they also expressed their concerns about it in terms of reliability, security and privacy. Additionally to their concerns about the technology being self-dependent with no human intervention and they questioned whether it can be as good as the human driver. Noting that females were more cautious and expressed more concerns about using this technology than males. To sum up, despite showing interest in the technology, the plurality of respondents were unwilling to pay extra money for obtaining it at the time.

A similar polling was conducted by the office of privacy commissioner of Canada in which over third of the Canadian expressed their privacy concerns if to use these connected cars. Similarly, over half of the respondents favored their privacy over the benefits of connected cars services. Moreover, they showed their concerns about their personal data and privacy and insisted that the vehicle is their private space, in a more recent survey conducted in the US, Germany, Spain and UK [43].

## 1.13. Conclusion

This chapter introduced the vehicular networks, the purpose they were made for, the technologies it uses and the applications it offers. It also clarified the various existing types and evolutions of the vehicular networks. It ended up with the public opinion polling which illustrates how hesitated the users are to use the technology and how concerned they are about the secrecy of their private lives and the reliability of this technology.

The privacy and the security in the vehicular networks are unquestionably important. They are also among the issues halting the penetration of the vehicular networks in the markets and the main concern of the end users. Therefore, we explain more about these issues in the next chapter and we survey the existing solutions to resolve it.

# CHAPTER 2

# PRIVACY AND SECURITY IN VEHICULAR NETWORKS

## 2.1. Introduction

We introduced in the previous chapter, the vehicular networks with their types and characteristics. In this chapter, we focus on the two key issues hindering the real adoption on vehicular networks on a large scale. These issues are the privacy and the security. Both are critical to ensure the safety of road users. Any tampering with the security system of the vehicle or the network may implicate destructive causalities. Among the existing security issues, we concentrate on the authentication because it impacts the identity privacy. The identity privacy and location privacy in vehicular networks are intertwined. Exposing one of them may lead to the exposure of the other. The vehicle continuously sends clear heartbeat state messages with their positions, velocity and temporal public key (pseudonym). It may also send event-based messages to report exceptional incidents and/or service messages which are infotainment related. Although the purpose of using pseudonyms with anonymous (identity-less) certificates is to protect the identity privacy. If the pseudonyms are correctly linked after their updates and the vehicle location is successfully tracked by the attacker, resolving the identity of its owner is just a matter of time, if the attacker matches his/her collected traces with the specificity of each visited location using social engineering techniques, s/he would identify the vehicle owner. Let's say that a vehicle during week-days frequents the location B departing from A. A is a house address and B is a workplace. Even if multiple persons live in A, probably only one of its habitants works at B. Therefore, that one is the owner of the vehicle. Consecutively, if the identity is used on the network, its usage is tracked, leading to the violation of location privacy. The Privacy in particular and security in general is risked in the vehicular networks because they rely on wireless communications making the attacker's intervention either passively (eavesdropping) or actively (alteration, injection or dropping) easier.

This chapter is organized as follows:

Part 2 explains the privacy issue in vehicular networks and highlights its importance in preserving the user's safety for both moral and physical threats. It also lists its types and answers the questions about who threats the privacy, when, how and what are the consequences of such a threat. At the end, it defines our attacker model and explains its executed attacks.

Part 3 reviews, classifies and analyses the existing state-of-art location privacy-preserving schemes and evaluates their advantages and disadvantages.

Part 4 highlights the prominent security attacks on vehicular network.

Part 5 explains the authentication issue in vehicular networks, defines what is being authenticated and lists the authentication types. It also highlights how the authentication risks the privacy.

Part 6 gives a brief review of identity privacy preservation authentication solutions.

Part 7 explains the evaluation methodology used for both security and privacy issues

Part 8 concludes the chapter.

## 2.2. Privacy Issue in Vehicular Networks

Privacy in general is crucial and it is important to ensure before the deployment of any technology or network. Humans by nature like to keep parts of their lives private. They like to keep some matters confidential. They tend to choose carefully what, when, and with whom to share their secret. They dislike being under someone's radar. They hate being spied on. They

loathe being pestered in any way, and they strongly object being stalked. These requirements emerged to cyber-world as well. With a similar mindset, the cyber-world users dislike being tracked by their cyber-activities where they sense the freedom to express their minds. The users are probably most honest in front of their screens where they send their queries, their used services and their comments. Although, they willingly share their daily updates, pictures and videos on their social network. They would object the data being retrieved from their devices implicitly without their knowledge by an unknown person (hacker).

In vehicular networks, the type of the shared data, their accuracy and frequency adds to the cruciality of protecting the privacy. Furthermore, they emphasize the jeopardy of exposing this data by an attacker aiming to track the vehicle's owner through his/her cyber-activity on road.

So far, we have been writing about privacy without explaining it properly. It was first defined by Warren & Brandeis back in 1890 as "the right to be let alone" [47]. Then, by Alan Westin in 1967 as "the right to control, edit, manage, and delete information about themselves and decide when, how, and to what extent information is communicated to others" [48] [49]. Adrienn Lukács surveyed in his paper [50] the privacy history and its diverse definitions through the eras following the evolution of the technology and the society. In the context of vehicular networks, authors of [51] defined it as the ability of the vehicle user to control which information is being sent by the vehicle even in the case of forwarding and the lifetime of this information.

### 2.2.1. Its types

In vehicular networks, the privacy is classified into three types [52]:

- ***The identity Privacy***: it is identifying the vehicle user by his/her activity. This is either done by his/her real identity, public key or network addresses.
- ***The location Privacy***: the vehicle shares its real location for the safety requirements of the network which leads to tracking both its past and current locations [53].
- ***The data Privacy***: the data privacy, is related to the exchanged messages contents, requested and used services, shared files, images and videos. It is more related to infotainment services.

Authors of [54] classified the privacy into three types as well: semantic, syntactic and robust. The *semantic* privacy means that the vehicles shall not be traced, and their trajectories not be reconstructed from their broadcasted beacons. *Syntactic* privacy means that vehicles need to update their pseudonyms periodically. *Robust* privacy is related to the resiliency against the internal attacker and the impact s/he may cause on the system.

Due to the fact that data privacy (confidentiality) may be preserved by the use of encryption, researchers pay more attention to the location and identity privacy in vehicular networks. Because they can be correlated leading to the vehicle being tracked through its activity on the road. The consequences are directly related to the safety of the user.

### 2.2.2. Threats on Privacy

The location and identity are fundamental to ensure the correct functionality of the network. The location data helps other vehicles to take decision assuring safe driving, such as

avoiding accidents caused by sudden slow down, lane change, U-turn, braking ...etc. It ensures the cooperation of vehicles to drive smoothly. The identity which is the certified public key of the vehicle is used to prevent false data injection by an external attacker. It ensures the authenticity of the messages, also, the accountability and non-repudiation of behavior. If the vehicle sends false data or misbehaves in the network, it is held responsible for that behavior by being revoked. The misbehavior may either be caused by: a hardware failure, compromising the vehicle by an attacker or an internal attacker. The revocation prevents other honest vehicles from trusting and interacting with the misbehaving nodes. Noting that the malicious user may be juridically prosecuted if needed, the accountability guarantees an undeniable evidence.

The importance of the identity and location making their use essential, eliminating them is impossible. Nevertheless, their usage risks the privacy causing the tracking of the vehicles which is the cyber equivalent of stalking. It is when the vehicle's safety messages are intercepted. Also, whenever the user uses his/her identity in the networks especially in authentication and beaconing. Finally, when the user utilizes location-based services.

### 2.2.3. Privacy Threat Model

We explained before when and how the privacy is threatened. Now, we discuss who may be interested in risking and violating user's confidentiality. The attacker may be an individual or an organization. S/he may target a specific user or do a general tracking looking for potential prey. S/he may be a location service provider, or even the authorities such as the police. Regardless of the identity of the attacker, s/he is anyone able to track the vehicle without the knowledge and approval of its user.

The vehicle may easily be tracked using road surveillance cameras and vehicles on-dashboard cameras. It is further facilitated by the use of automatic plate number reader which reads the vehicle's license plate automatically, making its search easy across the roads [51]. Although the use of this method is famous, it is not easily done by the attacker unless all roads are covered by cameras, s/he has full access to all those road cameras, and s/he can hack the vehicle's onboard cameras to use them. This method is generally used by the police and authorities where the vehicles may provide access to their cameras to cooperate with them or may rent their cameras usage as a service. Both, the high cost and the difficulty of this method prevent the attacker from using it.

The attacker may also physically follow his/her targeted vehicles. This is also known as stalking. We do not consider this type of threat although it is a high risk on the privacy. But this stalking has nothing to do with the user's cyber-activity on road. This issue is handled legally by the intervention of the police and it is out of the scope of our research.

The attacker may use a cheaper method to track the vehicle by its cyber-activity on-road; we explained previously that the vehicle networks require that each vehicle sends periodic messages containing accurate real-time location, speed, direction and identity data. These state messages are fundamental in ensuring the functionality of the network and the safety of the users. However, being sent wirelessly in clear is inviting enough for the attacker who would install his/her receivers across the road to intercept these messages and track the vehicle's movements on road. This motivates both the active and passive attackers to use this cheaper, more efficient and more accurate method to track the vehicles.

In the rest of the thesis, we continue to consider this type of method to intercept communication which is to rely solely on the wireless activity tracking and not any other mean such as tracking by cameras.

### 2.2.4. Our Attacker Model

The attacker model targeting identity privacy in the authentication phase uses the wireless communications to eavesdrop and actively executes the following attacks: replay attack, man-in-the-middle, impersonation which were explained above.

As for the attacker model targeting location privacy on roads, it is an external global passive attacker. S/he spread its receivers across the observation area to fully cover it as illustrated in Figure 2.1. It is passive because s/he does not inject, alter or drop the message. This gave him/her the secrecy and implicitly traits which harden its detection by the victim vehicle. In other words, the vehicle may be tracked for a long time before it detects the attacker's presence. It may also continue being tracked without discovering that it is being tracked. Unless the attacker uses the collected data in other attacks or for other purposes such as blackmailing. The attacker is external which means that s/he cannot compromise and use other vehicles to execute the eavesdropping, because:

- The cost of using vehicles is highly expensive. The attacker needs to possess (buy and use) a large number of vehicles. They need to cover the road either by being at static positions or running all the time on it. This assumption is not acceptable for various reasons, such as:
  - The high cost of fuel the running vehicles would consume daily.
  - The vehicles may not be allowed to park in the attackers desired spots.
  - Even if the attacker affords to deploy all this number of vehicles, this method of tracking draws the attention. It may not only be discovered easily but also be reported to the police by the tracked vehicles as being physically stalked.
- If the attacker cannot purchase the vehicles, another hypothesis for the internal attacker is either that s/he uses his/her vehicle to stalk the victim vehicle which is out of the scope of our research. Or, s/he may hack the vehicles system to control them. This assumption is not only extremely difficult but even if it was possible to hack a vehicle system, it is smarter for the attacker to directly hack the victim vehicle system, rather than, choosing the hard, costly, unsure way of hacking all or at least few of the target's neighbors. Furthermore, the vehicles' systems although comes of different constructors are expected to have at least the same level of security which must be high and unbreakable within the vehicle's lifetime using nowadays technology.

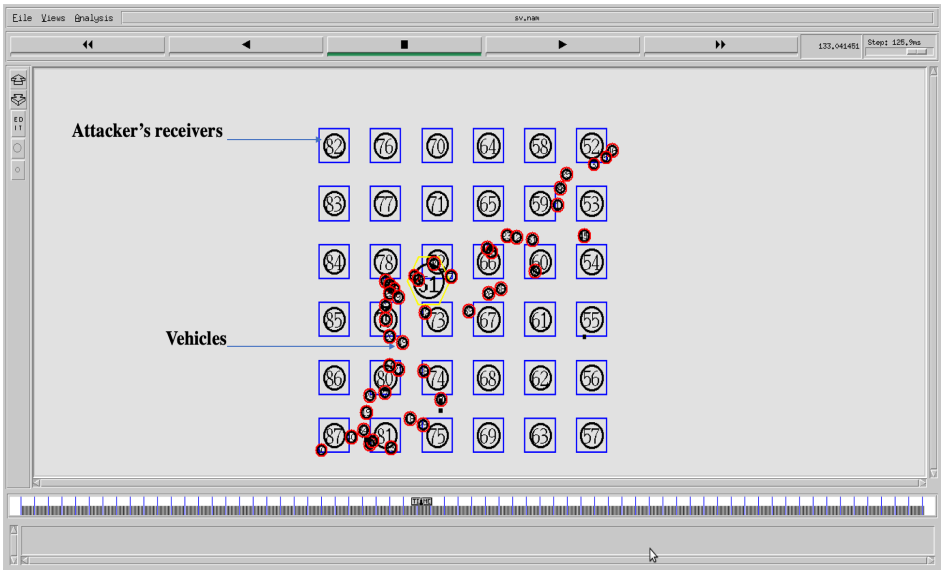



**Figure 2. 1:** Attacker's receivers' dispositions to cover the observed area.

Although, the internal attacker is favored in studying the robustness of security solutions requiring active attacks. They are rarely used in the case of passive tracking, because of their cost, difficulty and easy detection. If the attacker is ready to pour that much of cost on tracking, it would have been smarter, wiser and more economical to just install a small GPS tracker on the target vehicle. This method is out of our scope of research which aims to reduce and prevent the traceability of the vehicle by its cyber-activity. Therefore, in the rest of the thesis, we continue our discussion about the external global passive attacker which executes one or more of the following attacks:

- ***Semantic Linking attack*** [19]

In this attack, the external global passive attacker (GPA), uses the intercepted beacons to form a knowledge-base about the road, the parsed vehicles, their disposition and their speed. The GPA uses the acquired knowledge to predict the vehicles future positions. When the vehicle updates its identifier also known as a pseudonym, the GPA matches the predicted position with the real emitted positions to link the old pseudonym with the new one. This linking allows it to continue tracking the vehicle even when it is using a new freshly updated pseudonym. Figure 2.2 illustrates this attack, where A, B, C and D are neighbor vehicles having $V_A$, $V_B$, $V_C$ and $V_D$ as their pseudonyms respectively. Correspondingly, $P_A$, $P_B$, $P_C$ and $P_D$ are their current positions. Each vehicle sends beacons containing their position and pseudonyms. To facilitate the reading, we consider P as a vector containing the position coordinates, the speed and direction. After the vehicles update their pseudonyms, they continue to send beacons with their new pseudonyms. We denote below the emitted beacon before and after the change of pseudonyms [19].

- ***Before*** the **change**: Beacon ($V_A$, $P_A$), Beacon ($V_B$, $P_B$), Beacon ($V_C$, $P_C$), Beacon ($V_D$, $P_D$).
- ***After*** the **change**: Beacon ($V_{A'}$, $P_{A'}$), Beacon ($V_{B'}$, $P_{B'}$), Beacon ($V_{C'}$, $P_{C'}$), Beacon ($V_{D'}$, $P_{D'}$).

The GPA match the real locations $P_{A'}$, $P_{B'}$, $P_{C'}$ and $P_{D'}$, with the predicted location from $P_A$, $P_B$, $P_C$, and $P_D$ to conclude that: $V_A$ and $V_{A'}$ belong to the same vehicle "**A**". Similarly, $V_B$, $V_{B'}$ belong to "**B**", $V_C$ and $V_{C'}$ belong to "**C**", $V_D$ and $V_{D'}$ belong to vehicle "**D**".

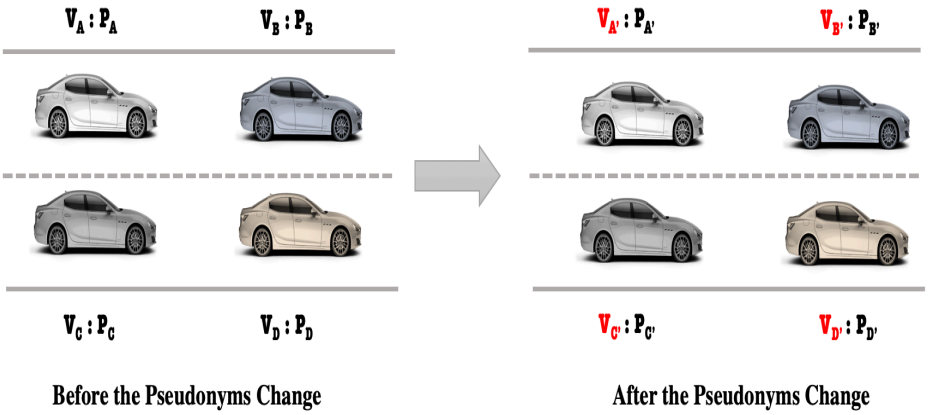



**Figure 2. 2:** Semantic Linking Attack **[19]**

- ***Syntactic Linking attack*** [19]

We continue to use the same notions. In this attack, the attacker uses the knowledge s/he accumulated about the road and the vehicles dispositions to learn which vehicles changed their pseudonyms and which did not. Figure 2.3 illustrates the syntactic attack, wherein, only vehicle **A** changes its pseudonym from $V_A$ to $V_{A'}$. While, vehicles B, C and D do not. Therefore, the attacker compares the beacons before and after the change to conclude that A is the only vehicle that did the change and continues tracking it. Noting that the possibility that $V_{A'}$ belongs to a new vehicle is neglected because it is impossible for a vehicle to appear at that position in tenth seconds between the beacons [19].

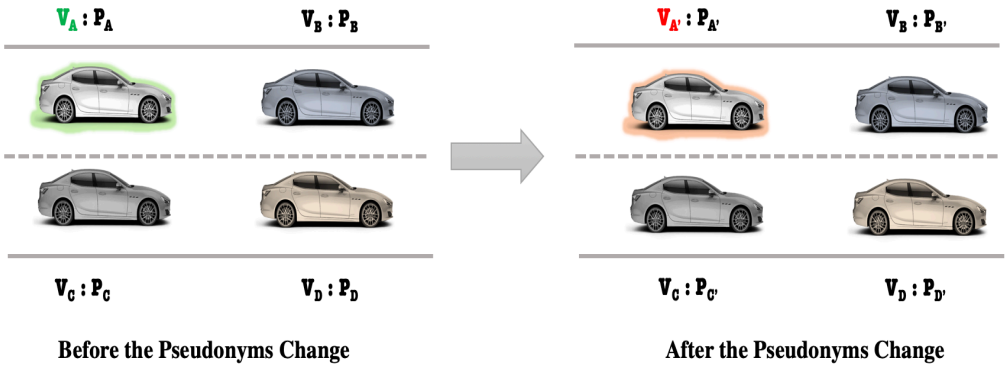



**Figure 2. 3:** Syntactic Linking Attack **[19]**.

- ***Observation mapping attack*** [55]

The previously explained attacks rely on beacons interception. Because these heartbeat messages are periodical, accurate, and contain sensitive clear data. In this attack and the next one, we consider linking the vehicle by both its safety messages and cloud location-based service messages. We used these attacks to evaluate privacy-preserving schemes in internet of vehicles and vehicular clouds, etc. where beside their pseudonyms, the vehicles have other unique identifiers that are used in the cloud, which are the Virtual Machine Identifiers (VMID). The VMID is the identifier of the customized space to serve the vehicle's queries in the cloud which is also changed to avoid linkability. In this attack, the GPA links the pseudonym in the beacon with the VMID in the service message by matching the location information in the

beacon with the location in the service message. Figure 2.4 illustrates this attack where $V_A$ is the pseudonym of vehicle "A", $VM_A$ is its VMID and $P_A$ is its position. The attacker observes the vehicle activity in three time slots where it continuously changes its pseudonym but keeps using the same VMID [55].

- At $\mathbf{t_1}$, the vehicle sends these messages, BCN ($V_A$, $P_A$) and LBS ($VM_A$, $P_A$) where BCN is the beacon and LBS is the location-based service message.
- At $\mathbf{t_2}$, the vehicle sends BCN ($V_{A'}$, $P_{A'}$) and LBS ($VM_A$, $P_{A'}$).
- At $\mathbf{t_3}$, BCN ($V_{A''}$, $P_{A''}$) and LBS ($VM_A$, $P_{A''}$).

The attacker then concludes that $V_A$, $V_{A'}$, $V_{A''}$, and $VM_A$ belong to the same vehicle "**A**". This means that regardless of how many times the vehicle changes its pseudonym, they are linked as long as it continues using LBS with the same VMID. The same is correct if the vehicle changes its VMIDs while it keeps using the same pseudonym, the VMIDs are linked causing the continuous tracking of the vehicle.

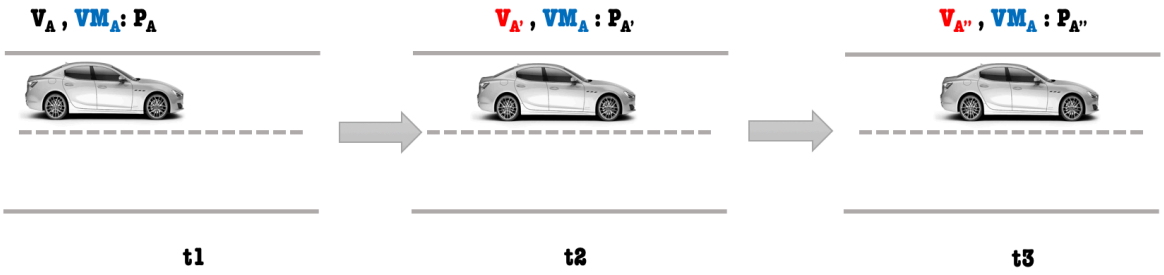



**Figure 2. 4:** Observation Mapping Linking Attack.

- ***Linkage mapping attack*** [55]

We follow the same notation as before. However, this attack links the VMID and pseudonym even when they are both changed as illustrated in Figure 2.5. The attacker who is always eavesdropping the exchanged the messages at each slot builds his/her knowledge accumulatively.

- At $\mathbf{t_1}$, the vehicle sends these messages, BCN ($V_A$, $P_A$) and LBS ($VM_A$, $P_A$). The attacker intercepting these messages matches the location from both messages and concludes that $V_A$ and $VM_A$ belong to the same vehicle.
- At $\mathbf{t_2}$, the vehicle sends BCN ($V_{A'}$, $P_{A'}$) and LBS ($VM_A$, $P_{A'}$). Similarly, s/he concludes that $V_{A'}$ and $VM_A$ belong to the same vehicle.
- At $\mathbf{t_3}$, upon the reception of BCN ($V_{A'}$, $P_{A''}$) and LBS ($VM_{A'}$, $P_{A''}$), the attacker concludes that $V_{A'}$ and $VM_{A'}$ belong to the same vehicle. The attacker global knowledge is that $V_A$, $V_{A'}$, $VM_A$, $VM_{A'}$ belong to the same vehicle.

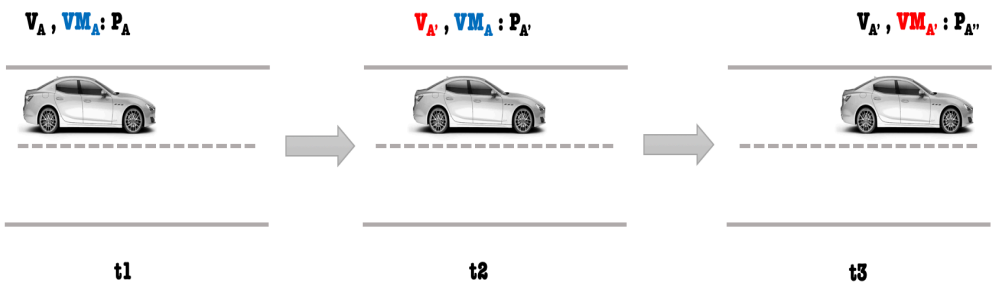



**Figure 2. 5:** Linkage Mapping Attack.

### 2.2.5. Privacy Violation Consequences

The tracking is as annoying as the stalking. It is even more dangerous because it is unnoticeable, and it is harder to detect. The attacker unless having a personal grudge to track a vehicle usually aims for the profits from the tracking. Collecting vehicles tracks may be used to achieve different purposes:

- If tracked by the police for example, it may be used to issue speed tickets or parking violation ticket. It may also be utilized to compel the users to provide testimonies and force them to be witnesses on violations that occurred in their vicinity.
- If used by a service provider, it may help in sending targeted advertisements.
- The consequences get more brutal as the attacker maliciousness gets. The tracks may be used by a malicious harmful attacker to:
  - Change routes,
  - Blackmail, threat and control the user.
  - Cause deliberate delay, traffic jams.
  - Induce road accidents and causalities
  - Plan traps, kidnaps and assassinations

  These are but few examples of the potential danger resulting from vehicle tracking.

### 2.2.6. Protecting the Privacy in Vehicular Networks

To protect the privacy of the identity, the IEEE 1609.2 [56] suggested the pseudonyms usage which are certified temporal keys. The certificates are anonymous, yet, they ensure the non-repudiation. They are also revocable guaranteeing they are not being used beyond their lifetime or when the vehicle is misbehaving. Furthermore, being issued and controlled by the authorities prevents the vehicle from having multiple valid pseudonyms at the same time, and thus to execute Sybil. This method ensures the conditional privacy, which means that the vehicle privacy is protected until it misbehaves.

Other methods suggested that the vehicle self-generates and self-signs its keys, to upgrade its privacy from being conditional to being fully protected. Indeed, this solution does protect the privacy even from the authorities, but it covers the misbehaving vehicle's traces. It also allows Sybil attack; it is non-revocable and can be repudiated. Another approach suggests forming a group where all the vehicle share the same public key (Group Leader Key) to check the message authenticity and each having its individual private key to sign the message. The hybrid approach proposes that each vehicle generates its own individual pair of temporal public and private keys which they request their certification from the Group Leader (GL). The GL then uses its key to sign their certificates [57].

Another approach replaces the pseudonym usage and the asymmetric cryptography with symmetric cryptography. The vehicles rely on the shared key used to sign and check the authenticity of messages instead of pseudonyms. This method is not commonly accepted or used in literature. Therefore, we continue our discussion about asymmetric based signature [19] [58].

Regardless, the identity usage in safety application is preserved by the use of pseudonyms. However, the identity privacy may be at risk. When authenticating to service providers and to

the authorities to request pseudonym refilling. In short, it may be at risk whenever used on road. Moreover, service providers may not be trustworthy. They may sell users data or use it to track them, especially when using the location-based services. Even when the end party is trusted such as what we assume about the authorities, the continuous usage of the identity even in encrypted communications may lead to the vehicle tracking. The repetitive use of the encrypted pattern representing the identity leads to tracking what is also known as matching by pattern. Cisco already started developing a solution to detect real-time threats in encrypted traffic without the need to decrypt the traffic [59]. The attacker may use a similar method to track the use of the identity. Therefore, we should replace the identity-based authentication methods by an anonymous authentication method, ensuring the same requirements.

Although the use of pseudonyms instead of real identities or permanent (long-term) public key preserves the identity privacy, but it does not remedy the location privacy from tracking. The pseudonyms, if updated randomly and hastily in unfavorable context may present the same level of privacy as when using a unique pseudonym. This is because when the attacker is able to link all the changed pseudonyms to the same vehicle, s/he is then able to track its movements through its parsed trajectory as illustrated in Figure 2.6 and Figure 2.7.

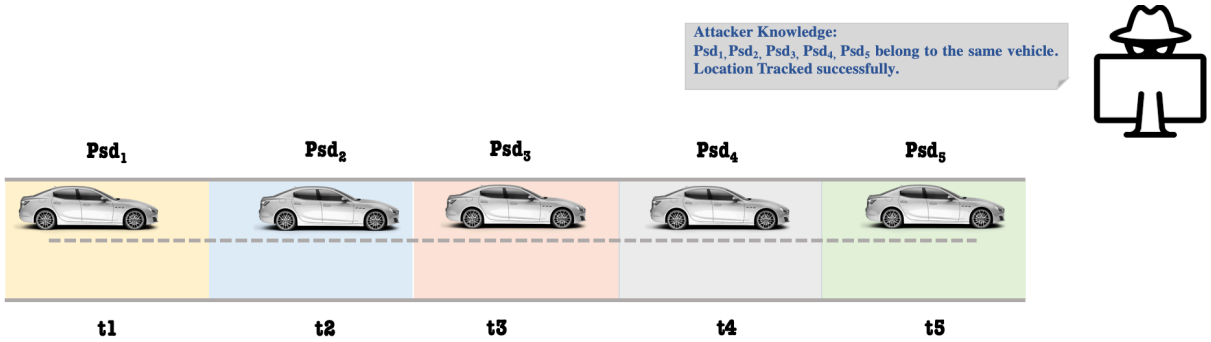



**Figure 2. 6:** The vehicle tracked successfully even with the pseudonym change

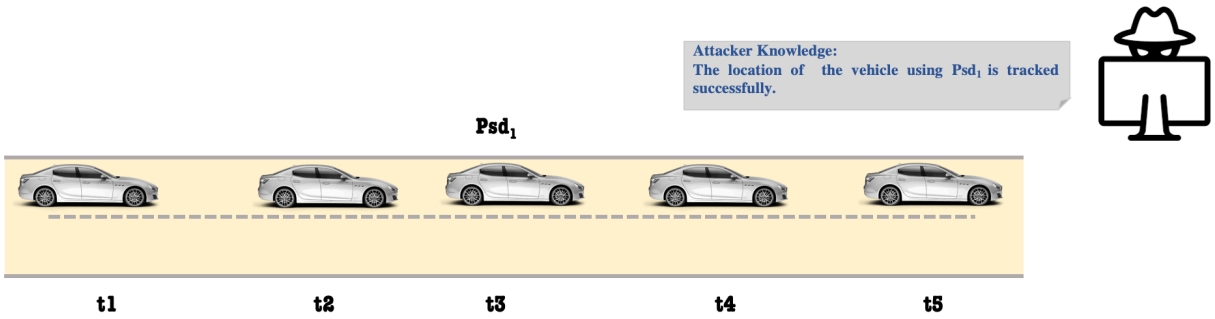



**Figure 2. 7:** Vehicle Tracked successfully when no pseudonym update is done.

To thwart the linkability and avoid tracking the pseudonym update should be executed in a strategic manner that confuses the attacker and erupts his/her tracks. These methods are known as the pseudonym change strategies. The literature is rich with various proposals, some researchers focus on preventing linkability of vehicles independently. Each vehicle executes its update strategy, regardless of its surrounding. They may follow the change with a silent period to break the attacker's predictions. Others suggest that the vehicles synchronize their change also known as changing within a cooperative crowd. This includes mix-zone based methods, cooperative change and hybrid methods that combine various principals to reduce linkability [57].

To protect the location privacy, the obfuscation of the location field is another approach. However, the work in this area requires precautions because it may affect the safety applications and location-based services which rely on the position's accuracy. Figure 2.8 gives a board classification of the privacy-preserving methods in safety-related applications. It is explained in more details in the next section.

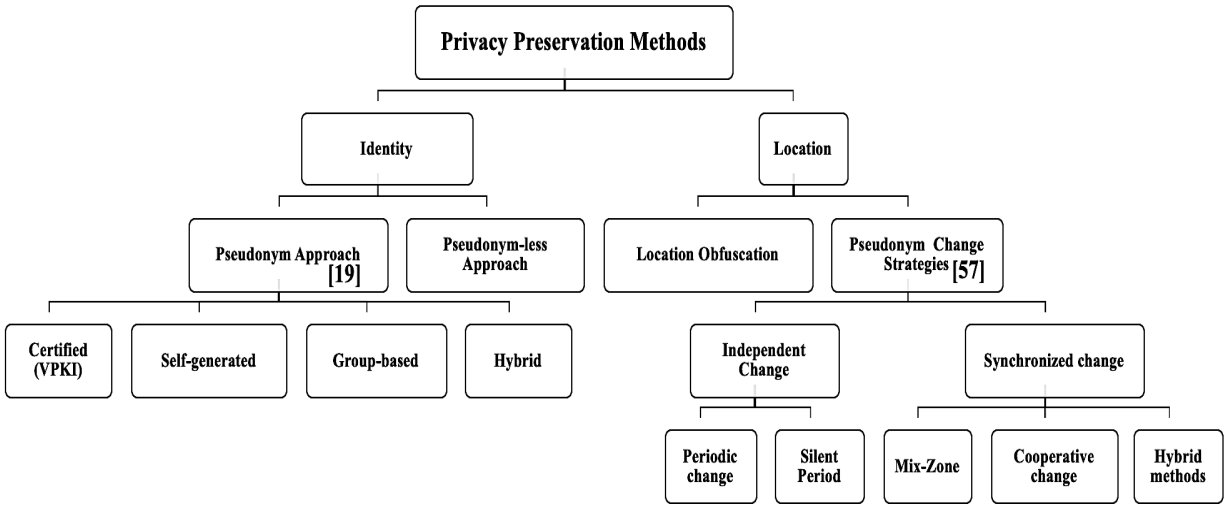



**Figure 2. 8:** Privacy Preservation Methods when using Safety Applications.

## 2.3. Existing Location Privacy-Preserving Solutions

This section reviews the existing pseudonym change strategies which are commonly used to preserve not only the identity privacy but also the location of the users from tracking, they were subject to the ETSI ITS pre-standard technical report [60]. In which the privacy solution parameters and the trade-off between the privacy and security as well as the important issues related to the pseudonym usage and change were studied. Also, the location privacy evaluation metrics were specified. Here in, we classify the prominent existing solutions into cooperative (infrastructure or infrastructure-less), non-cooperative, silence and hybrid approaches. We resumed in Table 2.2 the advantages and disadvantages of each solution in each category after explaining its principal in overall.

### 2.3.1. The non-cooperative change

These change strategies include solutions that are executed by the vehicles independently. The vehicle does the pseudonym update without any cooperation or synchronization with neighbors. Example of non-cooperative pseudonym change strategies are found in Table 2.1 rows 1-2.

### 2.3.2. The silence approaches

This is one of the earliest approaches proposed to break the attacker's continuous tracks. Instead of just changing the pseudonym periodically upon its expiry, the vehicle goes on silence then it continues its cyber-activity using the new freshly updated pseudonym. The silence as operation refers to the vehicle ceasing its message emitting and broadcasts. The silence serves

as a mystifier to puzzle the attacker. In Table 2.1, rows 3-5, we cite relevant state-of-art works that were proposed using the silent method.

### 2.3.3. The mix-zone approach infrastructure-based

This approach is inspired by the network-mix proposed first by Chaum D. L. in [61]. He proposed anonymizing the communication by relaying the messages through a sequence of trusted intermediaries defined as mixes to prevent the eavesdropper from identifying the sender [62]. In the vehicular context, various solutions relied on the use of mix-zones to prevent the linkability of pseudonyms upon their updates. A mix-zone is defined as a zone where the attacker cannot track the vehicles activity [63] [64]. In the initial proposal, it was supposed to be an uncovered region where the eavesdropper has his/her receivers on its extremities (its borders) but not within it. Thus, s/he is able to know the order and time of vehicles entering and exiting it. In later proposals, the mix-zone is created, maintained and advertised by the infrastructure (RSU). It is independent from the assumption on the attacker to be having uncovered areas. Instead, the mix-zones are becoming areas that even if the attacker reaches, s/he cannot eavesdrop the communications within it. Because the vehicles exchange encrypted messages or cease their broadcast (apply silence) within it. This approach is infrastructure dependent. The emplacement of these zones [65], the number of vehicles within them and the time spent inside them are critical criteria to study in order to achieve a good unlinkability level. Examples of the mix-zone change strategies are cited in Table 2.1 rows 6- 14.

### 2.3.4. The cooperation approach (Distributed mix-zone)

In this approach, vehicles synchronize with each other to do the change of their pseudonyms at the same time to thwart the linkability and confuse the attacker's tracks. It is also known as the distributed mix-zones. They do not rely on the infrastructure to synchronize their change by creating and advertising the existence of such a zone. Table 2.1, rows 15-18 resumes relevant state-of-art distributed mix-zone based solutions.

### 2.3.5. Hybrid Approach

The hybrid approach mixes one or set of methods from the previously mentioned approaches. The various possible resulting combinations make the contribution open in this category. It can even include new unclassified solutions basing on new criteria of change. Also, it may combine location obfuscation techniques with a pseudonym change strategy to get a more secure solution that is resilient to tracking. Table 2.1, rows 19-32 resumes existing solutions belonging to this category.

Noting that the presence of the "+" in Table 2.1 column indicates that the corresponding solution matches the relative criterion it appears under.

**Table 2. 1:** State-of-Art Pseudonym Change Strategies

| N# | Strategy | Year | Principle of functioning | | | | | | | | | Dependency | | | | Environment | | Privacy for | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Cooperative (infrastructure less) | Non-Cooperative | Infrastructure-based Mix-Zone | Silence Usage | Transmission Power variation | Message Encryption | Location Alteration/Noise | Beacon frequency change | Reputation-Aware | Virtual Crowd | Map/Road | Crowd | Speed | Infrastructure | VANET | IoV | Safety Apps | LBS Apps |
| **1** | Song J. H. et al. [66] | **2010** | | + | | | | | | | | | | + | | | + | | + | |
| **2** | Kang J. et al. [55] | **2016** | | + | | | | | | | | | | | | + | + | + | + | + |
| **3** | Huang, L. et al. [67] | **2005** | | + | | + | | | | | | | | | | | + | | + | |
| **4** | Sampigethaya K. et al. [68] [69] | **2005 2007** | | + | | + | | | | | | | | + | | | + | | + | + |
| **5** | Chaurasia, B. K. Et al. [70] | **2009** | | + | | + | + | | | | | | | + | | | + | | + | |
| **6** | Freudiger J. et al. [63] | **2007** | | | + | | | + | | | | | + | | | + | + | | + | |
| **7** | Buttyán L. et al. [71] | **2007** | | + | | | | | | | | | | | | | + | | + | |
| **8** | Palanisamy B. et al. [72] [73] | **2011 2012** | | | + | | | | | | | | + | | | + | + | | + | |
| **9** | Lu R.et al. [74] [75] | **2011 2012** | | | + | | | | | | | | + | | | + | + | | + | |
| **10** | Mathews S. et al. [76] | **2014** | | | + | | | | | | | | + | | | + | + | | + | |
| **11** | Liu, X. et al. [77] | **2012** | | | + | | | | | | | | + | + | | + | + | | + | |
| **12** | Ying B. et al. [78] | **2013** | | | + | | | + | | | | | + | + | | + | + | | + | |
| **13** | Boualouache A. et al. [79] | **2016** | | | + | + | | | | | | | + | | | + | + | | + | |

| | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **14** | Kang J. et al. [80] | **2018** | | | + | | | + | | | | | | + | | + | + | + | + | + |
| **15** | Liao J. et al. [81] | **2009** | + | | | | | | | | | | | + | | | + | | + | |
| **16** | Pan Y. et al. [82] [83] [84] | **2012 2013 2017** | + | | | | | | | | | | | + | | | + | | + | |
| **17** | Emara K. et al. [85] | **2015** | + | | | + | | | | | | | | + | | | + | | + | |
| **18** | Ying B. et al. [86] | **2015** | + | | | | | | | | | | | + | | | + | | + | |
| **19** | LI M. et al. [87] | **2006** | + | | | + | | | | | | | + | + | | | + | | + | |
| **20** | Burmester M. et al. [88] | **2008** | | + | | + | | | | | | | + | + | | | + | | + | |
| **21** | Buttyán L. et al. [54] | **2009** | | + | | + | | | | | | | | | + | | + | | + | |
| **22** | Hang D. et al. [89] | **2009** | | | + | + | | | | | | | | | | + | + | | + | |
| **23** | Boualouache A. et al. [90] | **2014** | | | | + | | + | | | | | + | | | + | + | | + | |
| **24** | Xingjun S. et al. [91] | **2014** | | | + | | | | | | | | | + | | + | + | | + | |
| **25** | Ying B., et al. [92] | **2015** | | | + | | | | | | + | | | + | | + | + | | + | |
| **26** | Eckhoff, D. et al. [93] | **2016** | | + | | | | | + | + | | | | | | | + | | + | |
| **27** | Boualouache A. et al. [94] | **2017** | + | | | + | | | | | | | | + | + | | + | | + | |
| **28** | Wang S. et al. [95] | **2018** | | | + | | | | | | | | | + | | + | + | | + | |
| **29** | Memon I. et al. [96] | **2018** | | | + | + | | | | | | | | + | | + | + | | + | |
| **30** | Khacheba I. et al. [97] [98] | **2017 2018** | + | | | + | | | | | | | | + | | | + | | + | |
| **31** | Belal A. [99] | **2018** | | | + | | | + | | | | + | | | | + | + | | + | |
| **32** | Guo N. et al. [100] | **2018** | + | | | | | + | | | | + | | | | | + | | + | |

**Table 2. 2:** The pseudonym Change Strategies

| *Category* | *Principal* | *Advantages* | *Disadvantages* |
|---|---|---|---|
| *Non-cooperative* | The non-cooperative change includes methods that are executed by the vehicles independently without synchronizing with their neighbor vehicles. | • The update process is fast.<br>• It is road, crowd and infrastructure independent. | • The frequent independent change does not necessarily reduce the linkability.<br>• Those schemes are not resilient to syntactic linking. |
| *Silence* | The silence-based approached rely on ceasing the broadcast of safety messages which are beaconed with high frequency until after the pseudonym update. | • The silence breaks the vehicle tracking and prevents the linkability between the old and newly updated pseudonyms.<br>• Silence-based schemes are more likely to be resilient to semantic linking (position-based linking) if applied correctly and adequately. | Silence impacts negatively the safety applications which are the fundamental incentive behind the creation of vehicular networks. Impacting safety application implicates risking the lives of users onboard of the vehicles. |
| *Infrastructure-based Mix-Zone* | The mix-zone is maintained and advertised by the RSU. It is usually placed at intersections and junction where the vehicles change their direction after the update. Within a mix-zone, the vehicles either stay silent or exchange encrypted communication. | The linkability is reduced when the change happens within a cooperative crowd. The attacker's confusion increases as the number of cooperative vehicles does, especially when they change their directions and speed after the change. | • These schemes are road, crowd and infrastructure dependent.<br>• To create and maintain the mix-zone extra calculation and overhead is added.<br>• The mix-zone using silence or encryption impacts safety applications efficiency. |
| *Distributed infrastructure-less mix-zone* | This type of mix-zones is self-formed by the vehicles dynamically on roads when they need to update their pseudonym. The vehicles synchronize with each other to change their pseudonyms simultaneously. | • The cooperative change strategy reduces the linkability.<br>• This type of mix-zone is infrastructure and road independent. | • The synchronization between vehicles and the use of silence or encryption may add extra overhead and impact safety application<br>• The solution is crowd dependent.<br>• Even if the vehicles simultaneously update their pseudonyms, road restrictions may lead to linkability. |
| *Hybrid* | This category includes various solutions that combine existing approaches together to overcome their lacks. Also, it combines new contexts that reduce the linkability. It is the category that may include different new solution. | The combination of various strategies is for the aim of reducing the linkability. | Unless the combination of schemes is done carefully. Their drawbacks may be inherited to the new used method. |

## 2.4. Security issues in Vehicular Networks

In this section, we list the famous security attacks on vehicular networks. Figure 2.9 illustrates the cybersecurity threats, which may be hardware or software related also known as physical and logical issues respectively. It classifies the logical security threats basing on what they target into the information, network and system. The right part of the figure lists, the prominent used solutions. The figure is followed by the explanation of the security attacks.

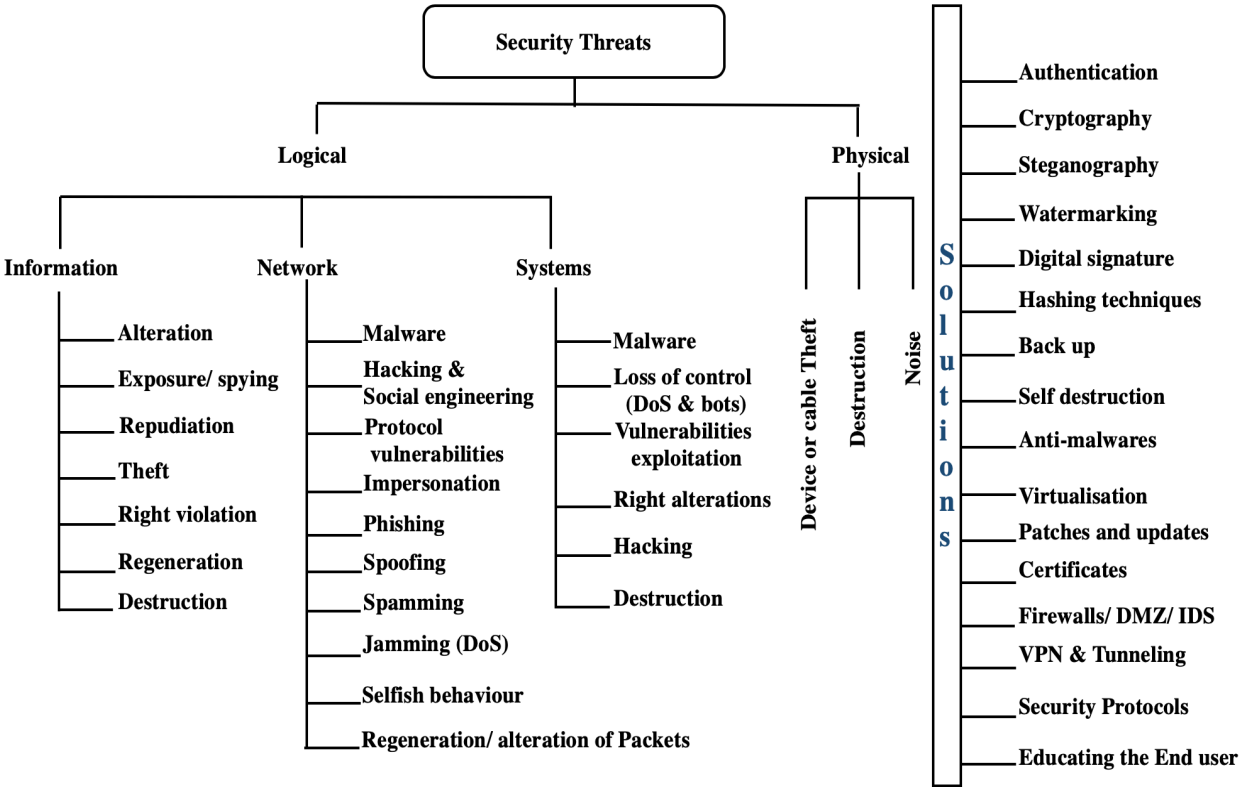



**Figure 2. 9:** Cyber-Security Threats and Solutions **[101]**

The vehicular network security attacks are [47] [101]:

- ***Session hijacking,*** the attacker forges unprotected sessions after its initiation (authentication, sequence number generation) by replacing the legitimate node and carrying-on the session [102].
- ***Denial of Service (DoS),*** one of the most dangerous attacks on the availability. It targets the network or a system to prevent it from providing services. The attacker may use one (DoS) or multiple machines (DDoS) to generate a targeted traffic toward the victim node or system to congest it and paralyze it [103].
- ***Sink-hole attack***, in this attack the malicious node attracts the network traffic to pass through it. However, it does not forward all the messages. Instead, it selects which packet to forward and which to drop. This is known also as the selective forwarding [104].
- ***Black-hole Attack,*** unlike the sink-hole attack, the malicious node executing this attack forward no packet. Instead, it drops them all [105].
- ***Malware***, are code portions written to cause harm to the systems and networks. It includes the viruses, adware, spyware and worms…etc.
- ***Replay Attack,*** where the attacker records exchanged message for later usage [102].
- ***GPS Spoofing:*** the attacker impersonates the GPS (Global Positioning System) trying to replace by generating a stronger signal with fake positions to the vehicle which accepts it assuming it came from the legitimate GPS [106].
- ***Masquerading or impersonation,*** is an attack where the attacker pretends to be (pose as) a legitimate node to execute other attacks such as data alteration or injection [105].
- ***Sybil attack,*** is an attack where a node obtains and uses multiple identities at the same time to get extra advantages or avoid tracing [106] [107].

- ***Tunneling or worm-hole,*** in this attack the malicious node intercepts the packet from a location and selectively tunnel them to another location. Then, retransmit them to the network from that location [108].
- ***Eavesdropping,*** it is a passive attack where the attacker intercepts, records and analyses the exchanged packets within its coverage [109].
- ***Man-in-the-middle,*** it can be considered as the active eavesdropping. The attacker here first eavesdrops the traffic to learn about the nature of exchanged messages. Then, breaks the chain by impersonating the endpoint (the user) and continuing the communication as it. The legitimate node is usually isolated to prevent it from resuming the communication or re-initiating it [110].
- ***Isolation attack,*** in this attack, the attacker prevents a node or a set of nodes from interacting with the rest of the network nodes [109].
- ***Social engineering, or human hacking***, the attacker uses his/her psychological tricks and social skills to conduct background research about his/her target. In the vehicular network context, it may be preceded by the eavesdropping and tracking attacks. For example, the attacker tracking vehicle "A" may link the frequented places to identify the target and collect more information about him/her. S/he may use this information to threaten and blackmail the victim [111].
- ***Linkability and tracking attacks*** are privacy targeting attacks. They mainly focus on linking the used pseudonyms and the locations of the vehicle to continue tracking it.
- ***Cheating attacks,*** it is a privacy targeting attack that aims to reduce the anonymity set size of the vehicle by using compromised vehicles (internal attackers). This attack aims to facilitate the linkability of the pseudonyms even when executing cooperative change strategy. Thus, it enables the vehicle tracking. The attacker deludes the vehicle changing its pseudonym with its cooperation in the change, when in fact it does not, making the vehicle linkable [100]. Authors of [112] defined the cheating attack to be executed by an attacker with selfish behavior aiming to take advantage of roads by injecting false data either messages with fake locations, events, identifiers and road conditions or by spreading false routes and mimicking congested routes.

## 2.5. Authentication Issue in Vehicular Networks

The authentication is a fundamental security property. It protects against intrusion and helps in ensuring accountability. It is the essential step to identify the internal users, organizing their right access rules and tracing their activity. Furthermore, it prevents non-registered users from accessing the system or the network.

### 2.5.1. Authentication in Vehicular Networks

In vehicular networks (VN), there are two types of authentications:

- **The authentication of users to access VN services,**

This authentication is between the vehicle's user and a server which can be a service provider, authority or RSU to obtain a service, pseudonyms and certificates. It is preceded by a registration phase where the user registers to this server by providing the essential needed information, agreeing on the rights provided also on the identification information and

parameters. Once authenticated, users benefit from the authorized services and continue their secure queries with the server. Naturally, all the exchanges messages and actions done by this user are mapped to his/her account, ensuring the accountability on one hand, and the possibility to revoke the users if a misbehavior or role abuse is detected on the other hand.

- **The authentication of messages,**

In this authentication, the messages are authenticated. This is a fundamental operation in VN to accept or reject a message especially those required by safety applications. This is a security measure to prevent an external attacker from injecting bogus messages.

Before we continue explaining this type of authentication, we remind the readers that every vehicle signs its safety messages also known as beacons with its pseudonym. The last is a certified pair of temporal public and private keys. They are certified by the authority and are temporal because they have a short validity time and space where they can be used. Also, to avoid Sybil attack, every vehicle has a unique valid pseudonym at a given time slot. The certificates of these pseudonyms are identity-less, in another word anonymous. This is essential in ensuring the privacy and avoiding tracking. Therefore, the authentication aims are to check that the message comes from an authentic node without identifying it. The identification is required only when a misbehavior occurs, and the misbehaving is held accountable and then revoked.

When a vehicle receives a message from another vehicle, it first checks the certificate validity. I.e. it is still fresh and not expired. Then, it checks that this certificate is signed by the authority's key and that it is not tampered with. Once the certificate checking is done, the receiving vehicle checks that the certified pseudonym is not in the freshly updated revocation list (CRL), i.e. not revoked/blacklisted. Upon the end of pseudonym verification, the receiving vehicle checks the integrity of the message by checking the digital signature. This operation not only proves that the message was not altered, but also that the pseudonym used for the verification belongs to the same owner who signed the message with the private pair of this pseudonym.

### 2.5.2. Authentication types

The authentication is commonly classified into three types, which are based on the way the user is identified into either by what s/he ***knows***, what s/he ***has*** or what s/he ***is***. We explain each type below [101]:

- *The **knowledge**-based authentication* also known as the authentication with something the user knows. This is one of the most commonly used methods. A famous example is the password-based authentication where the user only needs to provide his/her identifier or username and password assigned to him/her upon registration. The username and password are referred to also as credentials [113] [114] [115].
- *The **possession**-based authentication* or the authentication with something the user has. This is one of the preferred authentication methods at workplaces and hotels. The user possesses a dongle, smart card or badge that s/he uses to authenticate to a system [115].
- *The **physiology**-based authentication,* the user uses his/her unique features to identify him/herself to the system. It is also known as the biometric authentication, famous

examples are the authentication by iris, fingerprint and face. It also includes behavioral authentication methods such as handwriting, gait and signature [113].

In table 2.3, we compare these methods and highlight their advantages and disadvantages.

**Table 2. 3:** Advantages and Disadvantages of Authentication Types.

| *Authentication Type* | *Advantages* | *Disadvantages* |
|---|---|---|
| ***Knowledge-based*** | • Easy implementation<br>• Commonly accepted and used<br>• Can be saved in cookies | • May be forgotten easily<br>• Vulnerable to cracking and guessing attacks |
| ***Possession-based*** | • Practical and convenient for industrial usage.<br>• Does not require memorizing anything, mastering any technology or having IT background. | • Costlier than knowledge-based methods.<br>• Can easily be forgotten or lost. |
| ***Physiology-based*** | • More secure and harder to emulate or crack. | • Costlier than the other approaches.<br>• Prune to light and noise.<br>• Vulnerable to injuries, burns and cuts. |

### 2.5.3. Authentication Risks on Privacy

The above-explained types of authentication risk the privacy. The user who needs to access a system or a service must provide the required information to establish the authentication. S/he may have to provide his/her identity and biometric data in the registration phase. Most service providers emphasize their respect to privacy policies. However, we often hear the news that these data are exchanged for profit, were leaked by hackers or provided to juridical systems when asked for cooperation. Furthermore, vehicular networks are sensitive because they are related to the user's safety. The vehicle may use various services requiring authentication. Also, they may ask pseudonym refilling from the authorities frequently on roads. The repetitive authentication using the same credentials (data) may lead to the vehicles tracking on the road even if the communication is secured.

In here to highlight the privacy importance, we list some famous privacy leakage and breaches from prominent service providers [116]:

- Facebook and Cambridge Analytica scandal which caused the leakage of about 50 million accounts (2018).
- In 2016, Uber was hacked; 57 million users were impacted by this attack.
- Yahoo suffered from attacks in 2013-2014 which were reported in 2016 that 3 billion accounts were hacked.
- eBay was attacked in 2014 and 150 million accounts privacy were breached.

These examples prove that not all service providers are trusted. Even though they claim to be. Even if we want to trust them to be. Attacks targeting them may lead to the exposure of our private data we entrusted them with. The more you share, the more the risks are. For example, if a user uses his/her fingerprint to unlock his/her phone and uses it to access to his/her home and office, then, any breach or leakage in one of the systems storing his/her fingerprint lead to the vulnerability of other systems where the fingerprint is used.

However, to use a system you need to provide proofs that we are who we claim to be, and that we are authorized to use this system. At the same time, we need to preserve the privacy.

Therefore, there needs to be a balance between the privacy and authentication. We need to provide the minimum required information to ensure the authentication and at the same time preserve the privacy. This is what led to the appearance of a new set of authentication mechanisms. They are known as the anonymous authentication, privacy-preserving authentication or also as the challenge (zero-knowledge) authentication methods. In the next section, we give an overview of the usage of these authentication methods in vehicular networks.

## 2.6. Existing Identity Privacy Preservation Authentication Solutions

We explained in section 2.5.1. that in vehicular networks, the authentication is used either to identify the user or to check the authenticity of the message. The second is usually done by the verification of pseudonym used in the signature. It checks if it was certified by the authority, or it is a group key. Some even suggested the use of symmetric keys to sign the beacons [57] [58]. Regardless, of the method, as long as it relies on the use of temporal keys (pseudonym) and not the identity of the user, then, it preserves the privacy. The researchers emphasize this requirement when developing any solution. It is the main aim of the introduction of pseudonyms in VN. In our work, we concentrate on the user authentication as it requires identity exchange. Moreover, it is repetitive as the vehicle on road may periodically request pseudonym refilling from the authorities, or requests services from service providers. In this section, we review existing solutions belonging to a new type of authentication methods that balances the privacy and security properties by ensuring the successful identification of the users without exposing his/her identity privacy.

For pseudonym refilling and/or certifying in vehicular networks, many proposals exist among which is the work of [117] where the authors used one-time tickets issued by the Long-Term Certification Authority (LTCA) to request the certification of self-generated pseudonyms from the Pseudonym Certification Authority (PCA). Similarly, the authors of [118] also utilized the tickets to obtain pseudonym certificates from the PCA but the difference was that the same valid anonymous ticket may be used for multiple requests. In both works [117] and [118], the tickets are obtained upon the vehicle's successful identity-based authentication to LTCA. Schaub et al. suggested in [119] the token usage to request the pseudonym provider to certify the vehicle's generated temporal keys (pseudonyms). To obtain these tokens, the vehicle authenticates itself to the certifying authority using its identifier. The multiple token requests using the same identifier are linkable leading to the vehicle's tracking on road. Authors of [120] suggested the anonymous tickets' usage to request the certifying of the vehicles generated pseudonyms which are obtained after successful authentication using the long-term certificate. The solution preserves the privacy but the repetitive use of long-term certificate to obtain tickets leads to tracking. Also, because the tickets are anonymous, they may be vulnerable to impersonation attack where the tickets are used by this attacker to certify his/her keys. This further violates the accountability propriety.

Authors of [121] suggested an anonymous service request using the group concept and the pseudonym certificates. They suggested that when the vehicle is issued a pseudonym certificate. This certificate is to include all the services that the vehicle is registered to, in other words, the service provider register to the Regional Authority (RA), and the vehicle register through the RA to these service providers. When it does, the information about the registered

services is included in the pseudonym certificate using a blind signature. This way each service provider is able to verify if the vehicle is registered or no to use their service. To further improve the solution, they suggested that the vehicles request services from within a group to avoid linkability. The solution preserves the identity privacy but requires the vehicles to know all of their needed services before requesting pseudonyms. It is commonly known that the pseudonyms are short-lived which means that the process of inserting the registered services is repetitive adding more computational cost on the RA. Also, the certificate size will grow linearly as the number of service registrations increases. Authors of [122] proposed a random identity-based authentication. In their proposal, they used one-time randomly generated identity for each authentication. The user registers to the registration server using his/her real identifier. Then, an initial random identity is created and sent to both the vehicle user and the verification server. The vehicle may then use it to generate its own random identifiers. To authenticate itself to a service provider or other vehicles, the user sends his/her random identity in the authentication request to the verification server then to the other interacting party denoted as P. P sends a request to the verification server which has already received an authentication request from the vehicle. The server acknowledges the request and confirms to P that the user is the real owner of the used random identity. To ensure traceability, the cooperation of the Verification Server (VS) and Registration Server (RS) is needed. Noting that only RS knows the real identity of the vehicle user. Also, only it keeps the records of authentication history. The VS does the verification only and discards the old identity once the new is proved. Finally, both the RS and the vehicle have a time interval seed list which is used by the vehicle to generate new identity every time interval. Also, it allows the RS to keep track of the vehicles' identities without the need to be constantly informed upon every identity generation. Their proposal ensures authentication while preserving privacy, it is also secure against replay and man-in-the-middle attacks. However, it is server dependent, the authenticating parties need initially to check with the VS to be able to finish the authentication. This may be a drawback, attacks on the availability (single point of failure) of the server to hinder the authentication. Also, as the number of users and authentication requests increase the server's response may be slow.

## 2.7. Evaluation Methodology

In our thesis, we use various combinations of proofing and analysis methods for the evaluation of our security and privacy schemes as illustrated in Figure 2.10. Before we continue explaining their usage in the rest of the coming chapters, we will first in this chapter explain them separately basing on their usage for either security or privacy schemes.

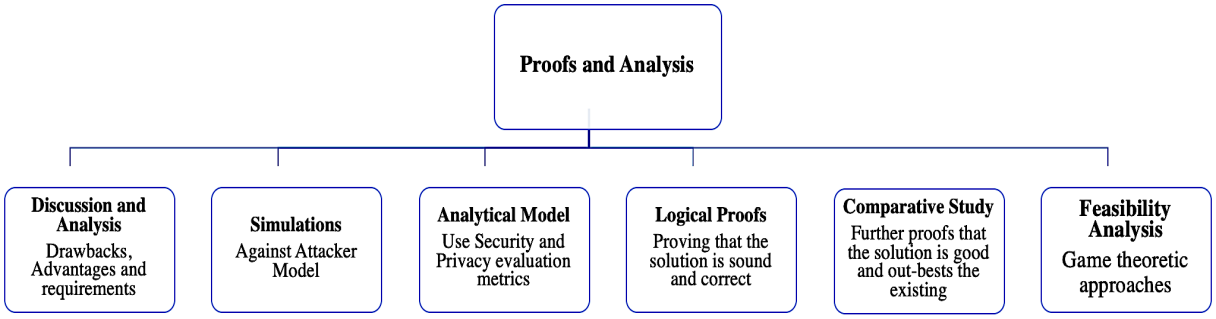



**Figure 2. 10:** Privacy and security proof and analysis methods

### 2.7.1. Security

In this section, we explain the various used methods of proving the robustness of a security solution.

#### 2.7.1.1. BAN Logic

It is a belief-based logic introduced by BURROWS, ABADI and NEEDHAM to formally write authentication protocols and analyze their security [123]. The logic is used to prove the correctness of a protocol on one hand and to prove that it achieves the underlined aims it was developed to fulfil on the other hand. The demonstration starts by first writing the protocol in terms of its exchanged messages between entities. These messages are then idealized. The demonstration starts from using the idealized messages, the set of protocols assumptions and logic postulates to arrive to the specified goals.

#### 2.7.1.2. SPAN and AVISPA

Automated Validation of Internet Security Protocols and Applications (AVISPA) and its Security Protocol Animator (SPAN). They are used to analyze the security protocols which are specified using High Level Protocol Specification Language (HLPSL) [124].

AVISPA checks the validity of security protocols while SPAN illustrates graphically the exchanged sequence of messages using Message Sequence Chart (MSC). It also includes an active attacker implementation to build attacks on the security protocols, detect their weakness and analyses their performance robustness and resiliency to commonly known attacks. The tool comes with a set of libraries of pre-specified known security protocols which helps both in understanding and learning the language logic and instructions. Furthermore, it may help academics to do comparative studies and ameliorate the existing solutions [125].

#### 2.7.1.3. Attack Tree

Attack trees [126] are a method to describe the security systems, evaluate them in terms of resiliency to attacks and therefore improve them. The attacks on a security solution are represented as a tree where the root node is the goal of the attack and the leaf nodes are the attacks executed. The OR nodes represent the various possible ways to execute an attack. While the AND nodes represent the different needed steps to execute an attack. If attack A can be executed either using method A1 and A2 then the combining node is OR. If both A1 and A2 are required to happen for attack A to be successful, then AND is used. Each leaf is then assigned a value or a set of values depending on a set of criteria. A simple example would be a Boolean value indicating the possibility to execute an attack such as 1 if it is possible and 0 if it is not. The nodes values are then calculated basing on the leaf values from down to top by applying the calculation rules for the “AND” & “OR”. This operation is recursive until the value of the top-level node known as the security objective is found. The value presents the likability of the attack goals to be achieved and therefore gives an overview of the security level of the solution. It illustrates the system weaknesses and vulnerabilities. Then, it helps the analyst in improving it. It may be appended by the countermeasure done against each attack. It also presents the system assumptions and allows the comparison of security systems after rigorously evaluating and analyzing them. Several tools exist that builds the attack trees of

systems and calculate the possibility of achieving the underlined attack goal of a system such as Isograph [127] and ADTool [128].

### 2.7.2. Privacy

In this section, we explain the various existing methods for privacy-preserving schemes proofing and analyzing empirical and analytical methods.

#### 2.7.2.1. Simulation

Simulation is one of the mostly used methods to test protocols and analyze them. Before real-world implementation. It is less costly in comparison with real test-beds. It allows the general evaluation of a given solution under different scenarios which helps in detecting its abnormalities and improving them. To simulate the vehicular networks two types of simulators are used. The first one is the mobility simulator which generates the maps and the traffic. The second one is the network simulator which simulates the vehicles' behavior.

Authors of [129] did an earlier investigation on the vehicular network simulators. In their paper, they considered Matlab, NS2, NS3 and OMNET simulators and they analyzed each tool's weaknesses and strengths, besides conducting a statistic on the use of each tool in literature. The authors found that NS2 is the mostly favored and used by researchers for vehicular simulation. Table 2.4 resumes the comparison we elaborated between these tools.

**Table 2. 4:** Simulation Tools Comparative Study

| **Criteria** | **Matlab** [130] | **NS2** [131] | **NS3** [132] | **OMNET** [133] |
|---|---|---|---|---|
| **Core component** | Matlab | C++ | C++ | C++, NED |
| **Scenarios** | Matlab | OTcl | C++ | Ini configuration |
| **Graphical interface** | Tool-interface | NAM | NetAnim | IDE |
| **Documentation** | Available for subscribers | Available | Available | Available |
| **Ease-of-Use** | Easy for Mathematical oriented users | Easy for network simulations | Easy for network simulations | Requires the manipulation of various types of files as modules |
| **Used Since** | 1994 | 1989 | 2009 | 1997 |
| **Community** | Large | Large | Large | Large |
| **License** | Proprietary software | Free software | Free Software | Free Software |
| **Platform** | Cross Platform (Windows, Linux and Mac Os) | Linux and Windows (via Cygwin) | Cross Platform (Windows, Linux and Mac Os) | Cross Platform (Windows, Linux and Mac Os) |

In our work, we used Mobisim [134] [135] for the generation of mobility models and NS2 for the vehicular network's simulations. We made this choice taking in consideration the above criteria, besides our familiarity with the tools, their ease of use, their extensive utilization in

related works literature, their stability, their large community, and the availability of tutorial and documentation.

#### 2.7.2.2. Analytical model

Authors of [136] defined five privacy analytical evaluation metrics:

- **The certainty**

The certainty metrics measure the attacker's ambiguity in finding a unique answer such as the location or the identity. It includes the level of privacy or the anonymity set size and the entropy. We give below the formulas for each metric:

The Anonymity Set Size (ASS) defined in Equation 2.1 is the number of neighbor vehicles with similar state as the subject vehicle $V_s$ that would make this vehicle undistinguishable by the attacker from the rest of the set members. Let $V_i$, $i \in [1..k]$, be the vehicle with similar state as $V_s$ and k the number of all the neighbor vehicles with similar state as $V_s$.

***Equation 2. 1:*** $$ASS = |V_i| = k$$

The entropy [59] defined in Equation 2.2 expresses the attacker uncertainty when linking the new pseudonym after the change to the subject vehicle, it is defined as follows:

***Equation 2. 2:*** $$Entropy = -\sum_{i=1}^{ASS} p_i \log(p_i)$$

Where $P_i$ is the probability the attacker assigns to each member of the ASS being the subject vehicle.

The normalized entropy [59] is calculated in Equation 2.3 as follows:

***Equation 2. 3:*** $$Entropy_n = \frac{Entropy}{Entropy_{max}}$$

Where $Entropy_{max}$ [59] is the maximal value the entropy achieves if the distribution of vehicles is uniform, it is calculated in Equation 2.4 as follows:

***Equation 2. 4:*** $$Entropy_{max} = log_2(ASS)$$

- **The correctness**

The correctness metric considers the attacker success rate which is the probability of the attacker successful tracks. In trajectory tracking, it is the probability of continuous successful tracks over successive observation slots and areas. It also includes the measurement of error rate in the prediction of positions, this is known as distance-based metric which calculates the distance between the real position $x$ and the predicted one $\hat{x}$ and multiply it by the probability of estimating $\hat{x}$ based on earlier observations o, it is defined in Equation 2.5 as follows:

***Equation 2. 5:*** $$\sum_{\hat{x}} P(\hat{x}|o) d(x, \hat{x})$$

- **The information gain and loss**

These metrics consider the amount of data that the attacker intercepts and collects. The more is the gain of the attacker, the less is the privacy of the user (loss). The less is the attackers gain, the higher is the level of the user's privacy.

- **Geo-indistinguishability**

This metric evaluates location privacy-preserving solutions that avoid sending an exact position of the user but an appended one, so as the attacker would think that all vehicles within that area are equally likely to be the subject vehicle [137].

- **Time**

The time metrics include the maximum tracking time which is the maximum period of continuous correct tracking by the attacker. Another metric is the confusion time which is the period of time the attacker is uncertain about the correctness of tracks or confused about the predictions it makes.

#### 2.7.2.3. Game theory

The game theory is a mathematical-based method to formulate, structure, and analyze strategical issues that depends on different factors and decisions impacting its evolution. It was initially introduced by John Von Neumann in 1928. It was first applied to economy applications when he released the book entitled "Theory of Games and Economic Behavior" in 1944 which he co-authored with Oskar Morgenstern. Ever since, the game theory had been used for various strategical and predictability applications. Each issue is presented as a game with a set of players and strategies (moves) made by each player. Also, a payoff function which assigns each player with a payoff depending on his played strategy and the strategies of the other players [138]. In our work, we used game theory to analyze the feasibility of our proposed location privacy schemes more precisely the identifier change strategy.

## 2.8. Conclusion

In this chapter, we highlighted the privacy issue in vehicular networks with its importance and types. We also answered key related questions such as what are the privacy violation risks, who threats the privacy, how and why. We also reviewed existing privacy-preserving solutions shedding more light on their advantages and drawbacks. We ended with a categorical comparison and analysis to help guide the reader interested to develop a privacy-preserving solution to avoid the lacks in the existing schemes. Additionally, the chapter concentrated on authentication issues and included a brief review on existing privacy-preserving authentication methods.

We also presented the different proofing and analysis methods used to study the performance, feasibility and strength of both the security and privacy issues in vehicular networks. We focus particularly on the methods used for the evaluation of privacy-preserving authentication protocols and the location privacy-preserving schemes which are our main two research problematics and the subjects of this thesis.

# PART II: CONTRIBUTIONS

# CHAPTER 3

# PRIVACY-PRESERVING AUTHENTICATION METHODS

## 3.1. Introduction

In Chapter 2, we highlighted the importance of authentication which is fundamental for distinguishing authorized users of a system or a network. Most of these authentication systems rely on credentials, identity, certified keys, tokens, or biometric prints to identify their users which may risk the privacy. The chapter defined the authentication types and related state-of-art schemes.

In matter of fact, the authentication contradicts with the privacy which has been topping the priority of the users and the legislation system. The annual scandals related to privacy violation in cyber-world alone are enough to turn the public opinion against the violators and pressure the legislative system to strengthen the privacy law. The impact of privacy violation in vehicular networks is more dangerous due to its direct relation to the safety of the drivers. The identity privacy exposure may lead to tracking. Noting that the identity in vehicular networks is the pseudonym which is the vehicle's pair of life timed geo-limited public and private keys. These pseudonyms are used to authenticate messages, more precisely they are used to sign the messages and verify them. They can also be used to encrypt messages.

In this chapter, we present two anonymous authentication methods that preserve the identity privacy for two types of vehicular applications. The first is a mutual authentication scheme between the vehicles for resource sharing where the vehicles unify their resources on road to provide and use each other's services. We denoted this as the cloud enabled vehicular named data networks (CVNDN). The second application is the pseudonym refilling requests which require the vehicle to authenticate itself to the authority to obtain new sets of pseudonyms.

The chapter is organized as follows:

Part 2 explains the cloud-enabled vehicle named data networks formation and the proposed reputation-based anonymous authentication method between the vehicles.

Part 3 describes the on-road on-demand pseudonym refilling and the proposed anonymous challenge-based authentication method.

Part 4 concludes the work.

## 3.2. Vehicle Resource Sharing in Cloud-enabled Vehicle Named Data Networks

We already explained the vehicular cloud concept and that it is being the extension of conventional clouds to road edges in Chapter 1. In this chapter, we propose a new paradigm that combines the vehicular clouds with the data named networks, what we denoted as Cloud-enabled Vehicle Named Data Networks or CVNDN.

### 3.2.1. System Description

In the proposed CVNDN, the vehicles unify their resources while on roads to handle difficult computations, to sense wider regions, to store data, or to obtain a stable service. This is known as "vehicle as cloud". Noting that the road vehicles in the same geographical space are potentially interested in the road data and services of that area. Thus, have a similar interest because the data has a local relevance for example within a radius $r$ and time span $t$, a user is

more likely interested in road information related to geographical zone s/he is in, the services provided, the road conditions...etc. Moreover, since the services are known by their names or identifiers, it would be easier to search it, and faster to provide it. Due to the fact that the providing vehicles are various, the probability of finding a service providing vehicle in the requester vicinity is higher. Therefore, in CVNDN, the service name and geographical location are used to route packets within the local VC instead of conventional IP addresses, because the data and service are likely to have a local relevance and validity time then are discarded after their expiry. If the on-demand services have global relevance, the user does not discard the data. Instead, s/he would save it by uploading it to his/her central cloud via internet using cellular networks (3G, 4G or 5G), when s/he crosses an infrastructure (RSU) connected to the internet or uses another vehicle's internet as service. Since the migration of the local cloud vehicle's virtual machine and its state to the central cloud is done by internet, the IP based routing and addressing are used instead of content-based addressing. We emphasize that this migration is done through secure communication to preserve the confidentiality of the data and protect the privacy. The authentication to the central cloud managed by the trusted authority or to its subsidiaries is done anonymously as explained in section 3.2.4.

## 3.2.2. Forming Cloud-enabled Vehicle Data Named Networks

In this section, we explain how the infrastructure-less VC is formed and how the data is routed (see Figures 3.1, 3.2). Followed by the description of the privacy preservation authentication method is in the next section.

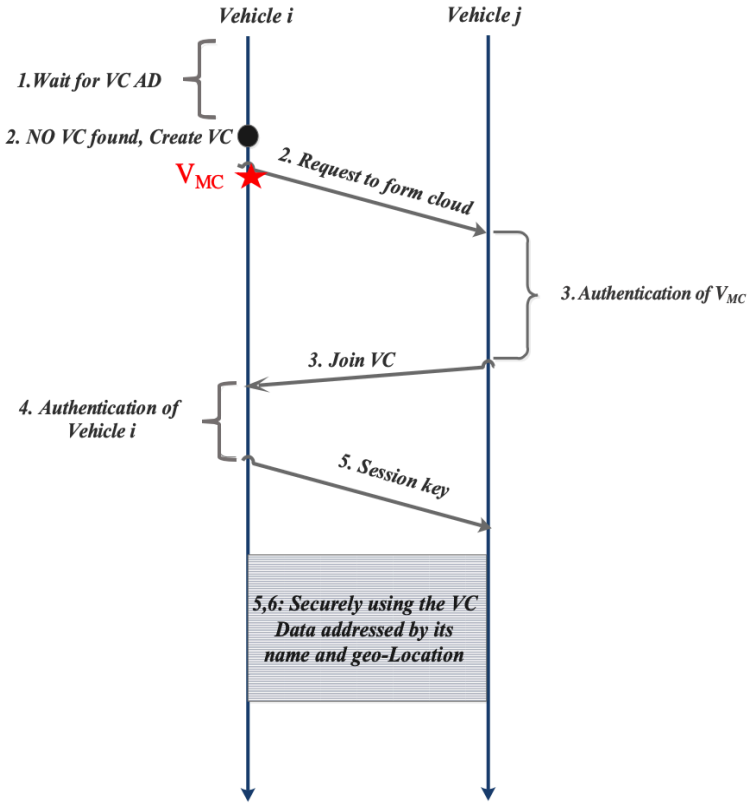



**Figure 3. 1:** Creating and/or Joining the vehicular cloud

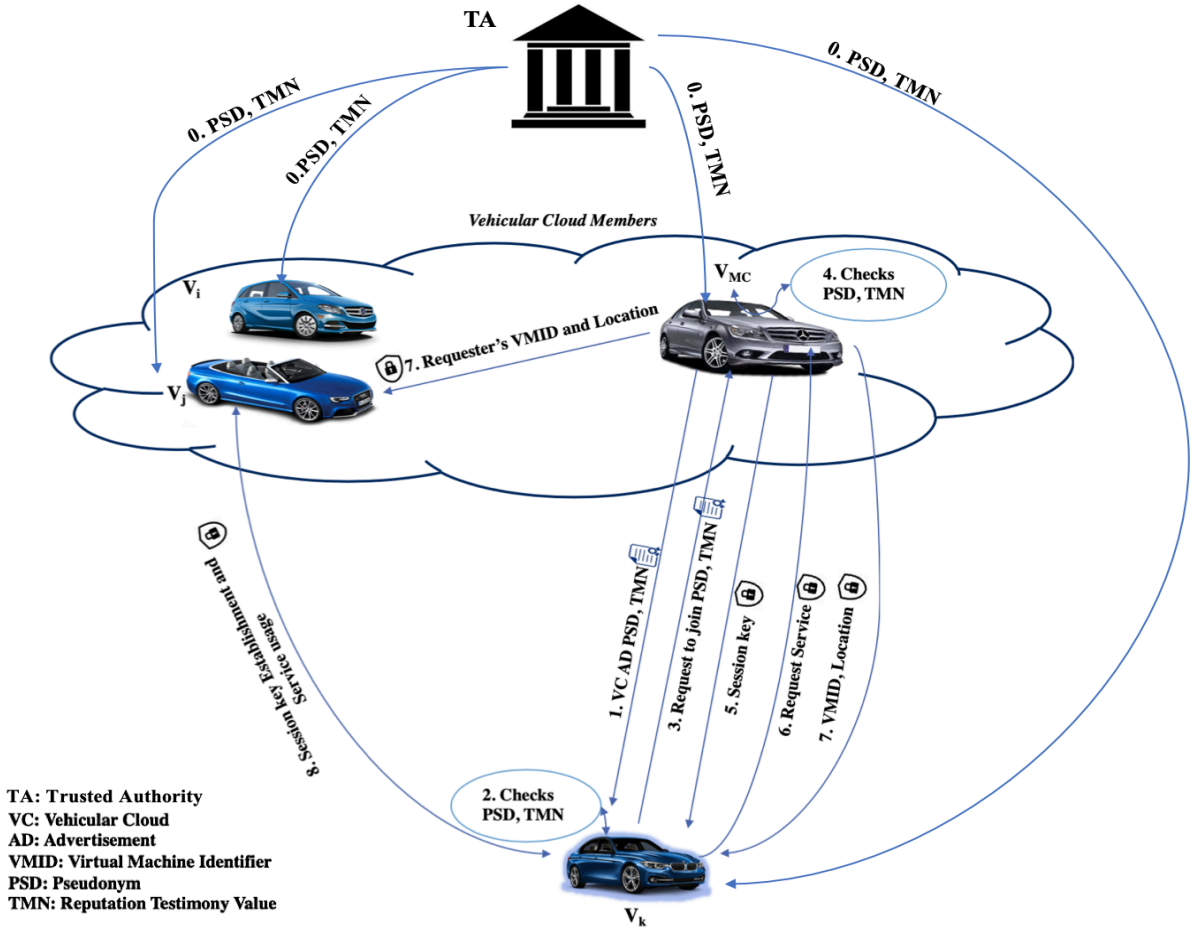



**Figure 3. 2:** Illustration of cloud-enabled vehicular data named networks joining and services usage process

The vehicle that wishes to participate in a vehicular cloud either by providing its services or resources waits to receive vehicular cloud advertisements for already existing clouds. Upon, the reception of an announcement, the vehicle first checks the announcer authenticity. Then, it sends a request to join to the vehicle managing the cloud $V_{MC}$. When the $V_{MC}$ receives such a request, it authenticates the requester. If this vehicle is willing to provide its resources and/or services, the $V_{MC}$ sorts, manages and registers this data to costume the vehicles resources and/or service to serve the future requesters. If the vehicle requesting to join the vehicular cloud is service requester, the $V_{MC}$ costumes a virtual machine (VM) to serve its queries. The VM may exist in the vehicle providing the service at a specific location or exists on various providing vehicles in adjacent locations. The communication between the provider and the requester is secure. The $V_{MC}$ plays the role of a proxy at the beginning to establish a secure session between the vehicles. Noting that the data/service within this cloud is routed basing on its name and time-location relevance.

If no in-vicinity cloud exists and the vehicle receives no announcement, it announces itself as a $V_{MC}$ and advertises its offered and needed resources and services to its neighbors. Vehicles interested in the received offers check the authenticity of the announcing vehicle. Then, they send their joining replies containing either their offers, as well as their needs of resources and/or services. Upon the successful authentication, the vehicles form the cloud and securely provide/use its services.

The $V_{MC}$ quits the cloud if the vehicle's service ends, it is going out of range of the rest of the members or when the cloud has no active members. Before it does, it forwards the cloud state and sessions to a new elected $V_{MC}$. If the cloud services are no longer used or no members exist, the cloud is deleted. Noting that users interested in saving their used services/data may migrate their local virtual machine to the central cloud.

### 3.2.3. Migrating the local cloud virtual machine to the central cloud

To migrate the local virtual machine to the central cloud, the vehicle user ought to authenticate itself the central cloud first. The user may use his/her credential to log in its cloud account, then the vehicle updates the central cloud with the local cloud data and services status. Noting that all these communications are secured with encryption to ensure confidentiality and data privacy. Once the update is done, the virtual machine VM is liberated. Noting that the local VM may either be used to update the central VM, merged with it or directly imported (as new VM or overwriting the existing) depending on the user's choices and needs.

### 3.2.4. Authentication to use/provide CVNDN services

We previously explained how the vehicle may create or join the vehicular clouds where we mentioned that both the requester and the provider need to check the authenticity of each other implicitly and indirectly. The authentication is done mutually between the vehicle managing the clouds ($V_{MC}$) and the joining members. Once the $V_{MC}$ authenticates and trusts the joining vehicles either as providers or requesters, the trust is established implicitly by transitivity between the vehicles. In matter of fact, the authentication is one of the essential and initial steps in creating, maintaining and using secure clouds. However, since it usually requires the credential usage, it threats the privacy of the vehicular cloud users in general and the CVNDN in particular. This is due to two reasons: the first is that the credentials may be linked with the pseudonyms and location. Thus, their repetitive usage may lead to the vehicle's tracking. The second is that the authentication is preceded by the registration phase, where the vehicle provides its user's identity or long-term certified public key to the $V_{MC}$. Therefore, the vehicle exposing itself to the risk of privacy in case this $V_{MC}$ decides to secretly and undetectably trade this data with other interested parties. To avoid risking the privacy while achieving the authentication, we propose the use of anonymous certificates signed by the trusted authority (TA). Also, a reputation testimony that is generated by the TA and continuously updated by the vehicle's testimonies about each other's behaviors while using the on-road vehicular cloud.

As we highlighted above, the authentication should be mutual between the vehicle managing the cloud and the vehicles providing/ requesting services. The $V_{MC}$ would not accept requests from a revoked (blacklisted) vehicle with a bad reputation or tagged as malicious. Similarly, the vehicles would not join a cloud created or maintained by a malicious blacklisted node with a bad reputation.

Note: The vehicle managing the cloud may be a service provider and a user or both.

#### 3.2.4.1. The Authentication Process

Before explaining the authentication process, we first clarify the notation used and their indications. $\mathbf{V_{MC}}$ is the vehicle managing the cloud. $\mathbf{V_j}$ is a vehicle providing or using the cloud

service. **M** represents the messages exchanged, while "→" is the sending operator on its left is the source and on its right is the destination. The authentication phase starts from checking the authenticity of the $\mathbf{V_{MC}}$ announcing the existence of the vehicular cloud and its provided/needed services and resources. The $\mathbf{V_{MC}}$ first sends M1 as denoted below, containing the list of services, an invitation to join, the certified pseudonym of the vehicle and its reputation. These last two fields are essential to anonymously authenticate the $\mathbf{V_{MC}}$ and ensure the accountability. The message also contains the location of the vehicle which is used along with the service name in data routing within the CVNDN.

- $\mathbf{V_{MC}} \rightarrow \mathbf{V_j}$;
  **M1**: {Broadcasts the list of provided services, an invitation to join, pseudonym, location, anonymous certificate (of the pseudonym) and the reputation testimony}

When $\mathbf{V_j}$ receives **M1,** it checks the pseudonym certificate validity. Then, it verifies that the pseudonym is not revoked, i.e. not found in freshly updated CRL (Certificate Revocation List). Finally, it examines if the reputation testimony value is higher than the threshold required. Upon the end of all the above-mentioned tests positively which means that $\mathbf{V_{MC}}$ is not revoked, its in-use pseudonym is still fresh, and its reputation is good. Then, the user of vehicle $\mathbf{V_j}$, if interested to use/provide this cloud's services requests to join it by sending the message M2 to $\mathbf{V_{MC}}$, M2 content is denoted below. It mainly contains the reputation value of the vehicle along with the certified pseudonym which are used to authenticate this vehicle.

- $\mathbf{V_j} \rightarrow \mathbf{V_{MC}}$**;**
  **M2:** {Request to join, pseudonym, location, anonymous certificate (of the pseudonym) and the reputation testimony (Signed by the TA and encrypted by the vehicle's Private Key corresponding to the pseudonym in-use)}

When $\mathbf{V_{MC}}$ receives **M2,** it checks the pseudonym certificate being valid. Then that the pseudonym is not in the CRL (not revoked). At the end, it confirms that the reputation value surpasses the minimum acceptable threshold. If all of these conditions are satisfied, then the vehicle's request to join the vehicular cloud is accepted. $\mathbf{V_{MC}}$ generates the message **M3** including a session key and sends it to $\mathbf{V_j}$. The session key is generated from: the location of $\mathbf{V_{MC}}$ and $\mathbf{V_j}$, pseudonyms and a random value to ensure its uniqueness. Moreover, **M3** is encrypted using the private key of $\mathbf{V_{MC}}$ and the public key of $\mathbf{V_j}$ (pseudonym). **M3** is denoted below:

- $\mathbf{V_{MC}} \rightarrow \mathbf{V_j}$;
  **M3**: {session key KS}

Upon receiving **M3**, $\mathbf{V_j}$ starts the secure communication with $\mathbf{V_{MC}}$. It specifies in message **M4** the requested service, the provided service or the resources that is willing to share. We emphasize that these communications are secured by symmetric encryption using the secretly shared session key KS. **M4** is denoted below:

- $\mathbf{V_j} \rightarrow \mathbf{V_{MC}}$;
  **M4**: {Service-name-requested and/or available-resources-shared, location} KS

After receiving **M4**, $\mathbf{V_{MC}}$ virtualizes the resources contained in **M4** if $\mathbf{V_j}$ is a service provider. If $\mathbf{V_j}$ is a service requester, it customizes a virtual machine to handle the requested service, the identifier of this virtual machine or VMID and its location is then forwarded securely to $\mathbf{V_j}$ in Message **M5** denoted below**:**

- $\mathbf{V_{MC}} \rightarrow \mathbf{V_j}$

  **M5**: {VMID, Location} KS.

It is noteworthy that the location field never points to an exact location where the vehicle is, but to a slightly larger location covered by the vehicle's receiver's range, to ensure that the vehicle gets the message but the location privacy is preserved in case the attacker tries to track the vehicle by its cloud activity and matching it with its safety beaconing. Also, when the vehicle requested service or resource is satisfied by multiple adjacent vehicles; the location field points to a larger area containing all of these vehicles. Similarly, the location in the $\mathbf{V_{MC}}$ messages is not the exact coordinates of the vehicles' position but of an area it is within and can cover. This way, the location privacy of all of the service provider, user and the vehicle managing the cloud is preserved.

The $\mathbf{V_{MC}}$ sends the requesting vehicle its VMID and the location of the service provider. The requester and the provider denoted as $\mathbf{V_j}$ and $\mathbf{V_k}$ respectively generate a session key to continue a secure communication while using the vehicular cloud services. This measure protects the user's confidentiality from an external eavesdropper, neighbor vehicles and even the vehicle managing the cloud. If the user is requesting a temporal storage service or internet access from the providing vehicle, s/he may even want to encrypt his/her data using his/her pseudonym (public key) to prevent the vehicle providing the serving from preying on it.

#### 3.2.4.2. The Reputation Testimony

In the previous section, we mentioned the vehicles' reputation as an essential metric in mutually authenticating the vehicles creating and joining the cloud. However, we did not mention how it is calculated or what does it mean. In this section, we shed more light on it and explain how it is being calculated.

Actually, the reputation and trust-based solutions in VANET have been used to complement the cryptography solutions questing the security and resiliency against the insider attacker model. Especially when the attacker is a dishonest vehicle injecting malicious or falsified data [139].

In the proposed CVNDN, the reputation is a value initially assigned by the trusted authority to the vehicles, it is signed by its private key to insure other vehicles its integrity and authenticity. This value is updated either by increasing it or decreasing it depending on the vehicle's behavior while using the vehicular cloud services. This behavior is reported by other adjacent vehicles playing the role of witnesses testifying about the behavior of each other and rating the quality of provided service. Each vehicle uploads its testimonies about other vehicles it interacted with to provide them with or use their services when it crosses an RSU or connects to the internet.

Upon the reception of testimonies, the TA calculates a new fresh reputation value and forwards it back to the corresponding vehicles. The vehicle uses the freshly received reputation which has a validity time span.

Noting that, the vehicle testifying about other vehicles must send their pseudonyms when it interacted with and their testimony value at the time. The reporting vehicle must sign the reputation testimony using its valid pseudonym. This is to ensure the integrity of the report and to hold the vehicle accountable for its testimonies and to prevent it from falsifying them.

By default, we initialize the state vehicles (police, ambulance, gendarmerie and military) reputation value to one. Other vehicles, to (0.5), we choose the average between 0 and 1 the born values of the reputation. Noting that the 0 indicates that the vehicle is not trusted and malicious and the 1 means that it is fully trusted because it is authoritarian. Assigning the average value to the vehicles means we are not biased or hold any prejudice about the vehicles being in either side (good or bad). This value is changed with the vehicles continuous feedbacks. It varies from 0 to 1. It is increased if good testimonies are sent and decreased otherwise. The vehicle is blacklisted (revoked) if its reputation reaches 0. The reputation value update is done by the Equations 3.1-3.3 :

***Equation 3. 1:*** $Reputation = \varphi(ORV) + (1-\varphi)(NRV). 0 \leq \varphi \leq 1$

Where ***ORV*** is the Old Reputation Value and ***NRV*** is the New Reputation Value and φ can be configured depending on the importance we give to the old value (history).

**NRV** is calculated based on the received testimonies (let **TMN** be the testimony). **NRV** is the mean of testimonies of vehicles i, ∀ i.

***Equation 3. 2:*** $\text{NRV}=\frac{\sum_{\forall i} TMN_i}{\sum i}$

Noting that, $\mathbf{TNM_i}$ is calculated by $\mathbf{vehicle_i}$ based on: service-continuity (**SC**), data-reliability (**DRL**), selfishness (**SF**) reflecting the vehicle's cyber-behavior, cooperation in the VC (**COO**) in term of service provision, the use of certified pseudonyms (**CPS**).

***Equation 3. 3:*** $TMN_i = ORV_i{*}(\alpha{*}SC + \beta{*}DRL + \gamma{*}SF + \delta{*}COO + \theta{*}CPS)$

***Where***: $\alpha+\beta+\gamma+\delta+\theta = 1;\ \{0 \leq \alpha \leq 1\ ;0 \leq \beta \leq 1\ ;0 \leq \gamma \leq 1\ ;0 \leq \delta \leq 1\ ;0 \leq \theta \leq 1\ \}$
***And*** $SC = \{0,1\};\ DRL = \{0,1\};\ SF = \{0,1\};\ COO = \{0,1\}\ ;\ CPS = \{0,1\}.$
**Noting that**, **1** means that the criterion is taken into consideration and **0** means that it was not

Further parameters may be added in the future. If the cloud services are fee-charged, or the resources are rented. Then, the metrics about the payment/rental are added as well.

## 3.2.5. Discussion and Analysis

After explaining the privacy-preserving authentication when joining the cloud. In this section, we analyze our proposal using BAN logic, then, we discuss how the security measures taken prevents security and privacy attacks.

The authentication is fundamental when forming the cloud to guarantee the correct functionality and to ensure liability and accountability. Also, to allow the TA to revoke misbehaving nodes. However, it may disclose certain required information about the user potentially threatening his/her privacy.

To preserve the privacy while joining the CVNDN (providing/using a service), we suggested the use of anonymous certificates instead of permanent certificates or credentials. The proposed method preserves the identity privacy. In this section, we prove that the proposed anonymous authentication achieves the aims served by conventional authentication methods. To do so, we use Burrows, Abadi and Needham logic [123], which is commonly used to analyze the correctness of authentication protocols [140] [141]. We first explain the notation

used and its meaning. Then, we give the idealized version of the authentication messages explained in section 3.2.4.1 using BAN idealization rules. Noting that only the three first messages are used since the fourth one is sent upon a successful authentication is done. We continue by underlying the mutual authentication objectives. In our case, the mutual authentication is between the vehicle requesting to join and the vehicle managing the cloud, where they are required to both trust each other. we finish with the demonstration explanation. It uses the assumption of the system and the BAN logic postulates to prove that the underlined objectives are reached and achieved from the sequence of exchanged messages.

***Notation***

- $P_{MC}$, $P_J$ and $P_{TA}$ are the public key of vehicles MC, J and trusted authority and $P_{MC}^{-1}$, $P_J^{-1}$, $P_{TA}^{-1}$ their corresponding private keys.
- $SIG_{P_{TA}^{-1}}(x)$ *signing message x using* $P_{TA}^{-1}$
- $KS$ *the Session Key*
- $RPT$ *Reputation Value*

***Messages (simplified and idealized following BAN Logic)***

- M1. $V_{MC} \rightarrow V_J$: $P_{MC}$ , $SIG_{P_{TA}^{-1}}(P_{MC})$, $\{RPT_{MC}, SIG_{P_{TA}^{-1}}(RPT_{MC})\}\ P_{MC}^{-1}$.
- M2. $V_J \rightarrow V_{MC}$: $P_J$ , $SIG_{P_{TA}^{-1}}(P_J)$, $\{RPT_J, SIG_{P_{TA}^{-1}}(RPT_J)\}\ P_J^{-1}$.
- M3. $V_{MC} \rightarrow V_J$: $\{\{KS\}_{P_{MC}^{-1}}\}\ P_J$.

***Assumptions***

- J believes TA ... (1)
- MC believes TA ... (2)
- MC believes (TA controls $MC \overset{P_J^{-1}}{\leftrightarrow} J$) ... (3)
- MC believes (TA controls $MC \overset{P_J}{\leftrightarrow} J$) ... (4)
- J believes (TA controls $MC \overset{P_{MC}^{-1}}{\longleftrightarrow} J$) ... (5)
- J believes (TA controls $MC \overset{P_{MC}}{\longleftrightarrow} J$) ... (6)
- MC believes ($\overset{P_{TA}}{\longrightarrow}$ TA) ... (7)
- J believes ($\overset{P_{TA}}{\longrightarrow} TA$) ... (8)

***Objectives***

- MC believes ($\overset{P_j}{\rightarrow} J$)
- J believes ($\overset{P_{MC}}{\longrightarrow} MC$)
- MC believes J believes $MC \overset{KS}{\leftrightarrow} J$
- J believes MC believes $MC \overset{KS}{\leftrightarrow} J$

***Demonstration***

Upon receiving M1, Vehicle J deducts the following:

1. J sees $P_{MC}$ , $SIG_{P_{TA}^{-1}}(P_{MC})$, $\{RPT_{MC}, SIG_{P_{TA}^{-1}}(RPT_{MC})\}\ P_{MC}^{-1}$ *....(Principal 4 of BAN Logic Postulates)*
2. J sees $P_{MC}$ *....(Principal 4 of BAN Logic Postulates)*
3. J believes (TA said $\overset{P_{MC}}{\longrightarrow} MC$) *....( from the assumptions 1, 5,6 and 8, Principal 1 and 3 of BAN Logic Postulates)*

4. J sees $RPT_{MC}$ *...(Principal 4 of BAN Logic Postulates, assumption 8 and first deduction)*
5. J believes (TA said $\overset{P_{MC}}{\longrightarrow} RPT_{MC}$) *....(using assumption 8 and 3 of BAN Logic Postulates)*
6. J believes ($\overset{P_{MC}}{\longrightarrow} MC$) *…(using the assumptions, above deductions and Principal 3: 'jurisdiction' of BAN Logic )*

*Upon receiving M2, Vehicle MC deducts the following: (demonstrated using the same method as above)*

1. MC sees $P_J$ , $SIG_{P_{TA}^{-1}}(P_J)$, $\{RPT_J, SIG_{P_{TA}^{-1}}(RPT_J)\}$ $P_J^{-1}$.
2. MC sees $P_J$
3. MC believes (TA said $\overset{P_J}{\rightarrow} J$) *....( from the assumptions 2, 3,4 and 7)*
4. MC sees $RPT_J$
5. MC believes (TA said $\overset{P_J}{\rightarrow} RPT_J$)
6. MC believes ($\overset{P_J}{\rightarrow} J$)

*Upon receiving M3, Vehicle J deducts the following:*

1. J sees $\{KS\}$ $P_{MC}^{-1}$ *....( from the assumption 6)*
2. J sees {KS} *... (from the assumption 8)*
3. J believes (MC said $MC \overset{KS}{\leftrightarrow} J$) *…(using the assumptions, above deductions and Principal 3: 'jurisdiction' of BAN Logic )*
4. J believes $MC \overset{KS}{\leftrightarrow} J$ *(using the assumptions, above deductions and Principal 3: 'jurisdiction' of BAN Logic)*
5. J believes MC believes $MC \overset{KS}{\leftrightarrow} J$ *(using the assumptions, above deductions and Principal 3: 'jurisdiction' of BAN Logic )*
6. MC believes J believes $MC \overset{KS}{\leftrightarrow} J$ *(using the assumptions, above deductions and Principal 3: 'jurisdiction' of BAN Logic )*

## 3.3. On-Road On-Demand Pseudonym Refilling

### 3.3.1. Network Model and System Functionality

This section describes the precise network model from security perspectives which is illustrated in Figure 3.3 where:

- ***TA*** registers every VANET vehicle upon its purchase. It issues two types of certificates which are: the permanent certificate containing the identity of the user and his/her long-term public key and the anonymous ticket containing only a reference number and digital signature. It is the sole authority saving the vehicle's and owner's private and sensitive data which are used exclusively when needed if the vehicle misbehaves and the cooperation with the juridical system is mandatory.
- ***RA*** are subsidiaries of the TA dispersed over diverse regions. They are responsible of issuing the temporal certified pseudonyms and/or their certificates (for self-generated pseudonyms). The RA keeps track of the used pseudonyms within its region without identifying their owners. Therefore, when a misbehavior occurs, the collaboration of TA and RAs is needed in order to revoke the malicious misbehaving vehicle.

We assume that these authorities (TA and RA) are trusted and resilient to attacks and intrusions. Also, that all the communications between them are secured by encryption and cannot be deciphered by a hacker.

- ***RSU*** which are static infrastructure with a wide coverage range for both emission and reception of messages. The reason for which we used them for packets retransmission.
- **OBUs** referring to the vehicles. They are mobile nodes with tamper resilient devices saving security parameters, keys and algorithms.

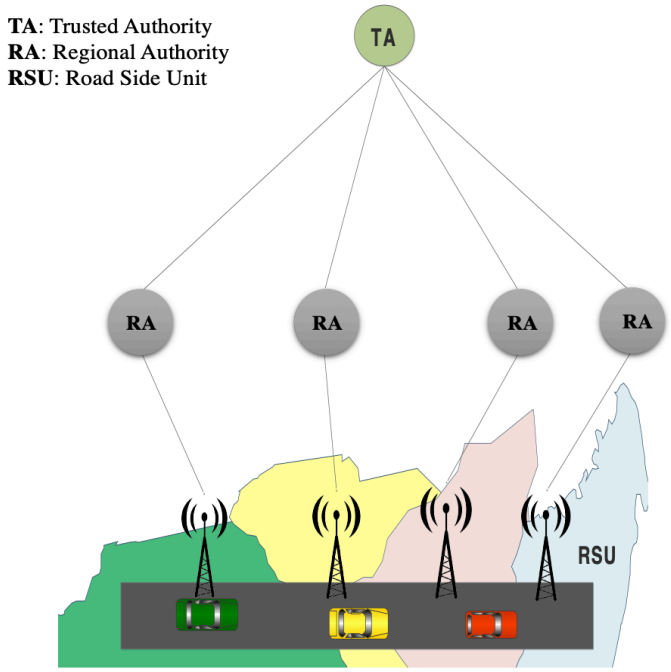



**Figure 3. 3:** Network Model **[142] [143]**

Having defined the network model, we continue now to describe the functionality of the system. When a vehicle registers to the TA, it obtains its unique set of parameters, settings and security algorithms which are stored in its Tamper Proof Device (TPD). It also receives a set of anonymous tickets and a certified long-term pair of public and private keys. We remind the reader that in our model, only the TA saves the vehicle and its owner's information. Moreover, the registration phase happens at the TA's facilities and it requires the vehicle ownership proofs provision. Also, since it involves no wireless communication, it is assumed to be safe and secure. Other assumptions about the network are that:

- The TA is trusted and secured against intrusions and attacks.
- The user's data is encrypted and saved in tamper resilient devices of the TA.
- The tickets are anonymous which means they are identity-less. A ticket contains only a reference number and the TA digital signature.

After the registration is done, the TA securely forwards the vehicle's issued tickets references and unique secret parameters to the RA where the owner of the vehicle lives. When the vehicle enters this region, it authenticates itself to the RA by providing one of its tickets to request a pool of pseudonyms and/or certificates for its self-generated pseudonyms. Noting that the ticket usage is followed by a challenge phase to prove that the vehicle is the real owner of the anonymous ticket. The details about the authentication phases are explained in the next

section. We emphasize that the communication between the RA and the vehicle is secured with encryption.

Regardless of whom generates the pseudonyms (RA or Vehicle). It is the RA who issue their corresponding certificates which include: a reference number, temporal public key (pseudonyms), geographical space, validity start and expiry time, and the RA's digital signature. Figure 3.4 illustrates the message sequence chart of the authentication and pseudonyms/certificate requests.

Note: The vehicle may travel and cross various regions where it needs to request pseudonym refilling from their corresponding RAs. In that case, the RA may forward the received ticket to the TA to obtain its related secret parameters which it uses to challenge the vehicle and authenticate it.

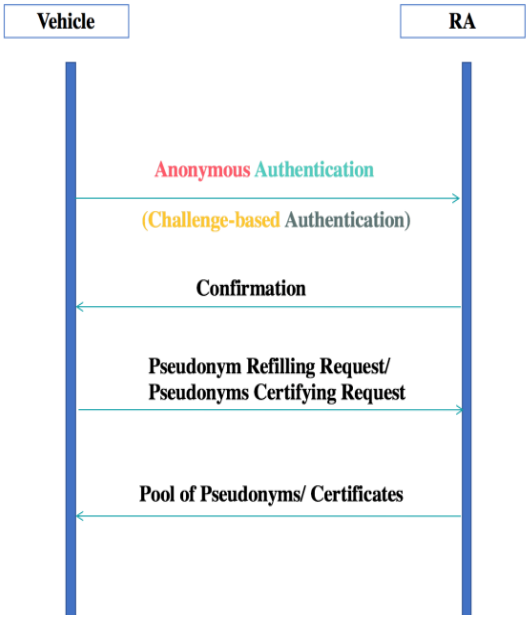



**Figure 3. 4**: Message Sequence Chart of the Pseudonym/Certificate Refilling Request

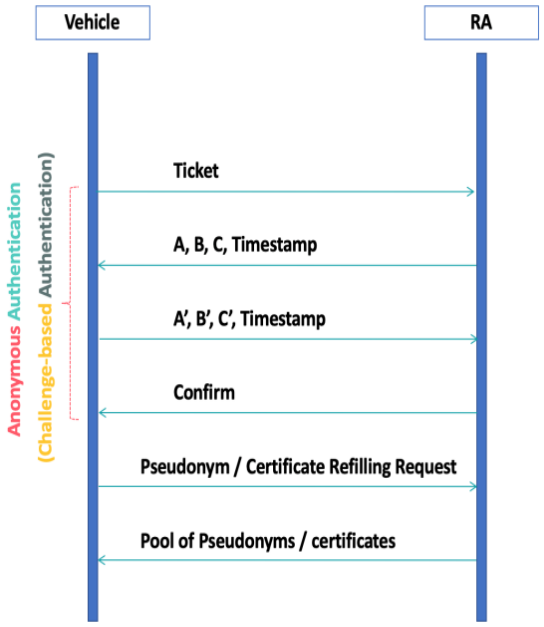



**Figure 3. 5:** Message Sequence Chart of the Anonymous Authentication Scheme

## 3.3.2. Proposed scheme

In the previous section, the network model components and the overall system functionality description were briefed. Also, we indicated that an anonymous authentication method is used to preserve the identity privacy. In this section, we explain this method in detail along with its phases.

The vehicle in a region intending to request pseudonym/certificate refilling have to first sends its ticket to the RA. The RA then quizzes the vehicle to check that it is the real owner of the received ticket. The vehicle responses to the challenge by anonymously authenticating itself without exposing its identity. Once this phase is successfully finished, the RA provides the vehicle with the pseudonyms and/or certificates. The certificates are delivered to the vehicle that self-generates its private keys. While the certified pseudonyms along with their corresponding private keys are supplied securely to the vehicles unable or unwilling to generate their own keys.

In Figure 3.5, we illustrated how the RA challenges the vehicles to prove its ownership to the ticket used in the pseudonym refilling request. We remind the readers that each registered vehicle has unique algorithms and parameters saved in their tamper resilient devices flashed by the TA. Also, that the RA has a copy of the parameters which are used in anonymous authentication challenge phase. Equation 3.4 represents the challenge algorithm used by the vehicles. This phase also named zero-based knowledge authentication because it preserves both the vehicle's and the owner's real identity.

***Equation 3. 4:*** $R^P \bmod Q$

P and Q are secret parameters unique to each vehicle, and R is a large prime random number.

To challenge the vehicle, RA first checks that the ticket is not revoked and still valid then it sends the vehicle an encrypted message containing three freshly generated large random prime numbers (nonces). Upon receiving this message, the vehicle needs to calculate and send its results within the underlined time span of response or else the authentication fails. The results are calculated by applying the algorithm in (Equation 3.4 ) on the received numbers generated by the RA. Equation 3.4 has unique secret parameters for each vehicle and all communications are encrypted to prevent the attacker from guessing or calculating the results. When RA receives the results within the authentication time span, it examines the results' correctness for the vehicle to be authenticated as the real owner of this anonymous certificate. The RA then checks that the vehicle has already consumed all its pseudonyms requested using an earlier ticket without being revoked for misbehaving before it satisfies its request. This is to ensure that the vehicle does not abuse its anonymity right persevered by the use of tickets to selfishly acquire multiple valid pseudonyms for the same time slots. This is done to prevent the pseudonym overlapping and the Sybil attack from occurring. Once this is done, the vehicle may request its pseudonyms to be certified or request certified pseudonyms (pseudonym + certificate) from the RA.

Noting that, the possibility that the attacker responses correctly to the three results within the given short time span without knowing neither the random numbers nor the secret values of P and Q is de minims. Also, the parameters extraction from results within the short span of authentication with today's technology is difficult (if not impossible) because it necessitates resolving discrete logarithm problem.

The pseudonym acquisition scheme is illustrated in Algorithm 3.1. We explain first the notation we used to facilitate the understanding of the algorithm.

- "**V →RA: m**" means that V sends RA the message m.
- "**V:**" precedes the vehicle executed code.
- **Encrypt (m, P)** encrypts **m** using the public key ***P***. The result is the encrypted message.
- **Decrypt (m, p)** decrypts **m** using the private key ***p***.
- **Generate ()** is the function that generates large prime numbers.
- **EQ(X)** is the implementation of Equation 3.4 on the random prime number X.
- **Current_Time ()** returns the system's current time.
- **AUTH_SPAN** is the authentication response maximal threshold.
- The symbols:
  - ":=" means assignment,

- "=" means equality, and,
- "[ ]" delimits the message fields.

- $\mathbf{P_{RA}}$, $\mathbf{P_V}$ are the public keys of the RA and the vehicle respectively.
- $\mathbf{P_{RA}^{-1}}$, $\mathbf{P_V^{-1}}$ are the private keys of the RA and the vehicle respectively.
- **PSD*i*** is a certified pseudonym.
- **PSD_Validity** is the validity time of the pseudonym.
- **Generate_PSD_Cert (PSD_Validity)** generates a non-overlapping pseudonym and/or certificate by assigning it a validity time that is higher than that of the last one generated.
- **Online (ticket)** checks if the vehicle using the current ticket is currently connected using another ticket, i.e. multiple simultaneous sessions.
- **Get-PSD-Validity ()** gets the last certified pseudonym validity time.
- A, B, C are random large prime numbers.
- A', B', C' are calculated by the vehicle using Equation 3.4 on A, B, C. They are of integer type.
- A", B", C" are calculated by the RA using Equation 3.4 on A, B, C. They are of integer type.

The algorithm is role based. Thus, the vehicle and RA codes are separately written. In the algorithm, there are three types of events which are:

- The local processing,
- The message emission and
- The message reception preceded by the keyword "***Reception of***"

**Algorithm 3. 1:** Pseudonym Acquisition Scheme

**V:**

***If*** (Check ($Certificate_{RA}$))
* Checking the Certificate of the RA before requesting Pseudonym refill*\
$Timestamp_V$:= Current_Time()
**V→RA:** Encrypt ([Ticket, $P_V$, $Certificate_V$] $P_{RA}$)
* Sending secure Pseudonym refill request using the anonymous certificate*\
***Endif.***
***Reception of*** **RA→V:** Encrypt ([A, B, C, $Timestamp_{RA}$], $P_V$)
Decrypt ([A, B, C, $Timestamp_{RA}$], $P_V^{-1}$)
***If*** ($Timestamp_{RA}$> $Timestamp_V$) ***AND*** (Current_Time()< ($Timestamp_V$ + AUTH_SPAN))
* Checking the freshness of the challenge*\
A':=EQ(A)
B':=EQ(B)
C':=EQ(C)
$Timestamp_V$:= Current_Time()
* Calculating the outcome of the challenge and sending its response to the RA*\
**V→ RA:** Encrypt ([A', B', C', $Timestamp_V$], $P_{RA}$)
***Else***
Authentication ***fails***
***Endif.***

**RA:**

**Reception of V→RA:** Encrypt ([Ticket, $P_V$, Certificate$_V$] $P_{RA}$)
Decrypt ([Ticket, $P_V$, Certificate$_V$], $P_{RA}^{-1}$)
***If*** (Check (Certificate$_V$) ***AND*** **Not** Online (Ticket))
* Ensuring that only one pseudonym request session is active *\
A:=Generate()
B:=Generate()
C:=Generate()
Timestamp$_{RA}$:= Current_Time()
* Generating the one-time three random number *\
A":= EQ(A)
B":= EQ(B)
C":= EQ(C)
* Calculating the challenge response on the one-time three random number *\
**RA→V:** Encrypt ([A, B, C, Timestamp$_{RA}$], $P_V$)
***Else***
Authentication ***fails***
***Endif.***
**Reception of V→ RA:** Encrypt ([A', B', C', Timestamp$_V$], $P_{RA}$)
Decrypt ([A', B', C', Timestamp$_V$], $P_{RA}^{-1}$)
***If*** (Timestamp$_v$> Timestamp$_{RA}$) ***AND*** (Current_Time()< (Timestamp$_{RA}$ + AUTH_SPAN))
* Checking if the vehicle responded to the challenge within the authentication time span*\
***If*** ((A'=A") ***AND*** (B'= B") ***AND*** (C'= C"))
* Checking the challenge response of the vehicle *\
Authentication ***Successful***
Timestamp$_{RA}$:= Current_Time()
***For*** (i=1,i<=n, i:=i+1)
PSD_Validity:=Get-PSD-Validity()
PSD$_i$:=Generate_PSD_Cert(PSD_Validity)
***Endfor***
**RA→ V:** Encrypt ([PSD$_1$, PSD$_2$,…PSD$_n$, Timestamp$_{RA}$], $P_V$)
**Else**
Authentication ***fails***.
***Endif.***
***Else***
Authentication ***fails***.
***Endif***

## 3.3.3.Analysis and Discussion

In this section, the performance of the proposed scheme is analyzed. Starting by the illustration that it fulfils security and privacy objectives expected from an authentication protocol. Followed by, a discussion about its resiliency to prominent security attacks. Then, proving that it is logically correct using BAN logic. Finishing with its verification using SPAN and AVISPA.

### 3.3.3.1. Security Analysis

In this subsection, the proposed solution is analyzed in terms of its satisfaction to security and privacy properties and its resiliency to well-known attacks

- ***The privacy (anonymity and unlinkability)***

For the privacy, we care to study the robustness of solution against Global Passive Attacker (GPA) aiming to identify the vehicle's owner and track his/her locations and parsed trajectories. We already explained the characteristics of this attacker in Chapter 2. In what follows, we justify and clarify how our protocol protects against GPA and the taken measures to prevent identification and linkability.

First, our scheme does not disclose the personal information of the user especially his/her real identity while driving on road. Not when authenticating to the RA nor when authenticating to vehicles because pseudonym certificates are identity-less. The user provides his/her

information solely to the trusted authority when doing the initial registration. This operation happens when s/he first purchases his/her vehicle. In other words, when s/he is physically present at the TA's service facility. Since this registration does not rely on wireless communication, it does not risk the user's privacy and is considered as secure.

Second, the anonymous certificate (ticket) is utilized to request the pseudonyms and/or certificates. Therefore, the user's identity is preserved.

Third, the linkability by ticket is prevented as the vehicle has multiple tickets to use. For each pseudonym/certificate refilling request, a new ticket is utilized in a round robin way to prevent the same ticket from being used for two consecutive demands. Therefore, two sequential requests will not be linked to the same user. These precautions are made to hinder the linkability by patterns in encrypted communication.

Finally, the privacy is conditionally preserved using our authentication method. This is an essential requirement to ensure the non-repudiation and the correct functionality of the network. It is important to keep the privacy a priority for honest user. However, it is also fundamental to be able to trace the misbehaving nodes and hold them responsible in order to preserve the correctness of the network. We explain more about it when we discuss the non-repudiation and accountability traits.

- ***Message Integrity***

The integrity of messages is important. Although, it is known that the altered messages are detected at the lower layers where they are dropped, and a retransmission is needed in that case. However, the integrity of clear messages containing the tickets, pseudonyms and certificates is further preserved by being digitally signed. While the encrypted messages containing the random number, or their corresponding results are ensured implicitly since only the intended parties could encrypt and decrypt the messages and alter their content (asymmetric cryptography).

- ***Short term linkability and long term linkability***

The short linkability is needed for the network's functionality. Thus, it must be guaranteed. Contrarily, the long-term linkability is undesirable, as it risks both the location and identity privacy. The multiple anonymous tickets usage for pseudonym requests prevents this type of linkability to happen when using our scheme. Since two successive requests with two different anonymous tickets are not linked by the GPA.

- ***Non-repudiation and accountability***

In our scheme, the RA does not know nor store the vehicle's (or its owner's) identity. However, the RA maps the pseudonym/certificate requests with the used ticket in the authentication phase. This enables it to ensure the non-repudiation of the vehicle on its cyber-activity while using these pseudonyms. Suppose that a vehicle misbehaves on road disrupting the correct functionality of the network. As soon as the misbehavior is reported to the RA by the vehicles, the RA confirms the reports. Then, it retrieves the ticket's reference used to obtain the pseudonym of the reported vehicle. The vehicle's valid non-used pseudonyms are revoked, and the ticket is blacklisted to prohibit its future usage. If needed, the identity may be resolved in cooperation with the TA. The ticket is sent by the RA to the TA which checks its issued

tickets to identify the subject ticket's owner. The TA also blacklist all the issued tickets of the misbehaving user and informs the RAs. The RAs update the vehicles with the revoked pseudonyms. Noting that, the identity may not necessarily be resolved upon each revocation, it depends on the severity of the misbehavior and the RA's policy of punishment.

- ***Forward security***

Forward security means that if the keys or sensitive encrypted data is exposed, how much of past and future communication is risked. In our scheme the forward security is ensured because even if the attacker can somehow know the encryption key of the vehicle, s/he may read A', B', C' sent in the challenge phase, s/he cannot extract the parameters P and Q or the nonces A, B, C from the sole knowledge of A', B', C'. Moreover, the pseudonym is a short-lived public key (temporal). If the corresponding private key is exposed, then only the messages encrypted with its public pair are read by the attacker and no other older messages or parameters. Therefore, the forward security property is satisfied. Noting that the knowledge of the private key is not possible as they are stored in the vehicle's tamper-proof device which is highly protected.

- ***Replay attack***

Our proposed authentication method is resilient to replay attack thanks to the challenge phase. This measure follows the use of anonymous tickets which without its addition, the attacker would be able to intercept any ticket and use it later to request his/her pseudonyms without them being linked to his/her real identity. In this case, the attacker would follow the replay attack with more severe active attacks such as the Sybil attack. Supposing an Attacker $A_{tk}$ is to re-use intercepted messages from earlier session sent by a vehicle containing the ticket $Ticket_V$ of vehicle $V$ and the results it calculated denoted as *A', B', C'*. Then, $A_{tk}$ sends $Ticket_V$ to RA which would start the challenge phase by generating three random numbers a, b, c and timestamps the message, the RA waits for a specific time before dropping the authentication session if it receives no valid response within it. $A_{tk}$ uses the intercepted message containing *A', B', C' and a timestamp* as its response to the challenge. RA rejects the received response and closes the authentication session as the timestamp from the received message is older than the current also the received values *A', B', C'* are different from the expected results. Thus, the replay attacker fails to authenticate him/herself successfully. The results obtained by AVISPA in figures 3.7 and 3.9 indicate that the protocol resilient to this attack.

- ***Session hijacking attack***

To protect against session hijacking, the communications were secured by encryption. Let's suppose that the attacker could interfere after the emission of the ticket, s/he have to resolve the challenge successfully to continue the communication. This is not possible because s/he is unable to read the encrypted message containing the nonces. Therefore, it cannot provide the expected results (see Table 3.1). If the attacker is to interfere after the authentication phase to either certify the pseudonyms or request for their refilling. S/he needs to send messages encrypted with the authority's public key. In response, the authority sends the requested certificates/pseudonyms encrypted with the vehicle's public key that has initiated this session. Hence, the attacker cannot read its content because s/he is not the owner of the (vehicle's) private key that may be used to decrypt the message.

Noting that in what has preceded, we started by supposing that the attacker "***could successfully interfere".*** This means that s/he correctly guesses the sequence numbers of the exchanged messages and is faster in generating his/her messages before the legitimate vehicle does. This is a difficult task to fulfil in the short time of authentication and refilling.

- ***Man-in-the-middle attack***

Our solution also protects against man-in-the-middle attacks (MITM) because of the use of certified keys. let's suppose that vehicle $V$ is authenticating itself to the RA and Attacker $A_{tk}$ is an internal attacker with legitimate certificate executing MITM attack. $A_{tk}$ cannot proceed as s/he is not the authority and the authentication fails after the examination of the key certificate. Therefore, our solution is resilient to MITM Attack. The results obtained by AVISPA in figures 3.7 and 3.9 indicate that the protocol is safe against such an attack.

- ***Impersonation attacks***

Similarly, the certificate usage prevents the attacker from impersonating both the vehicle and the RA. If we hypothetically suppose that s/he succeeds at surpassing the certificate verification, s/he will fail to provide the correct responses in the challenge phase on the sent nonces and thus fails to carry on with the authentication while impersonating nodes. This attack is a sub-phase of the MITM attack. Since the solution was proved with AVISPA to be resilient to the MITM attack, then, it is also resilient to the impersonation attack.

- ***Guessing and brute-force attacks***

In the challenge phase of our proposed solution, the RA freshly generated three random numbers for one-time usage (nonces), encrypts them with its public key and sends them to the vehicle. The attacker desiring to break the authentication scheme without the knowledge of the vehicle's secret parameters has to correctly guess A, B, C, P, and Q to calculate A', B', C' or brute-force all the possibilities to find A', B', C'. S/he must provide a correct response for all the three results within the authentication time span. With the random numbers being large, the attacker's chances to successfully guess/ brute-force the results accurately and quickly using nowadays technology is infinitesimal given that the modulus operator is not reversible also it means resolving discrete logarithm problem [18] which means finding the P in Equation 3.4 using S and R ($P=Log_R(S)$) where S is the result and R is the random number. $S=R^P \bmod Q$.

In Table 3.1, we illustrate using an example, the time required by the attacker to brute force A', B', C' values without knowing the parameters. We estimated the needed time to try all possibilities without knowing any parameters to find the values using HSIMP online tool [144]. We also utilized Mandy Lion Labs tool [145] to estimate the combinations (possibilities) needed to get to A', B', C'. Noting that, the used random prime numbers were obtained from University Tennessee at Martin random prime number list available at [146]. Also, that the decillion=$10^{33}$ and the duodecillion=$10^{39}$ [147].

**Table 3. 1:** Illustration of Brute-force estimated time of execution and number of Combinations

| Random Prime Numbers | Challenge response (Equation 3.4) | Equation 3.4 Parameters | | Execution Time | Brute Force Attack | |
|---|---|---|---|---|---|---|
| A, B, C | A', B', C' | P | Q | | Time estimation [144] | Number of tries [145] |
| 10 digits | 60 digits | 9 digits | 60 digits | 5 milliseconds | 2376 Duodecillion Year | 72 Decillion combinations |
| 20 digits | | | | | 2376 Duodecillion Year | |
| 30 digits | | | | | 950 Duodecillion Year | |
| 40 digits | | | | | 950 Duodecillion Year | |
| 50 digits | | | | | 950 Duodecillion Year | |
| 100 digits | | | | | 2376 Duodecillion Year | |

- ***Sybil attack***

Our solution prevents pseudonym overlapping by prohibiting the use of anonymous ticket to request multiple pseudonyms with the same validity time. Thus, the possibility of using multiple identities to execute Sybil attack. Owing to the fact that, the RA rejects the vehicle's requests using multiple tickets for pseudonyms with the same validity period to ensure that no two pseudonyms are used simultaneously.

Let's suppose that the vehicle $V_a$ utilizes both $Ticket_1$ and $Ticket_2$ to request its pseudonyms. Let $p_1$, $p_2$, $p_3$ be the pseudonyms obtained using $Ticket_1$ and $p_4$, $p_5$, $p_6$ the pseudonyms obtained using $Ticket_2$. $Vl_1$, $Vl_2$, $Vl_3$, $Vl_4$, $Vl_5$, $Vl_6$ are their validity times respectively. Presuming that $V_a$ can execute the Sybil attack. Then, it must be in possession of multiple pseudonyms that are valid during the same lifetime. If we assume that it can use two pseudonyms at the same time, then, this would mean that $Vl_1=Vl_4$, $Vl_2=Vl_5$ and $Vl_3= Vl_6$ for the $V_a$ to use $p_1$ and $p_4$ at the same time, $p_2$ and $p_5$ simultaneously, $p_3$ and $p_6$ at the same time each during its validity period. This cannot happen as our algorithm prohibits two simultaneous connections using two different tickets and it increases the validity between each generated pseudonym. This means that $Vl_1<Vl_2<Vl_3$ and $Vl_4<Vl_5<Vl_6$. Therefore, even if the requests are made using these tickets in a consecutive way, the Sybil attack cannot happen because $Vl_1<Vl_2<Vl_3<Vl_4<Vl_5<Vl_6$.

### 3.3.3.2. Burrows, Abadi and Needham (BAN) Logic

After studying the measures taken to satisfy security properties protect against well-known attacks, we continue in this section to prove that our anonymous scheme fulfils the authentication objectives using Burrows, Abadi and Needham logic [123]. To do so, we first write formally the scheme, then we use the postulates to demonstrate that the goals are achieved.

Before starting the correctness demonstration, we first explain the utilized notations. Then BAN logic postulates, followed by the formal idealization of the scheme's messages, assumptions of the solution and the underlined objectives.

- ***Notation:***

- Let **A, B, Q, P, RA, TA, $V_J$** be the entities where A, B, P and Q are abstract users; RA and TA are the regional and central trusted authorities respectively; $V_J$ is the vehicle.
- **$P_{TA}$**, **$P_{RA}$** and **$P_J$**, are the public keys of the trusted authority, the regional authority and the vehicle J. $\boldsymbol{P_{TA}^{-1}}$, $\boldsymbol{P_{RA}^{-1}}$ , $\boldsymbol{P_J^{-1}}$are the private keys of the TA, RA and vehicle J respectively,
- $\boldsymbol{SIG_{P_{TA}^{-1}}(x)}$ is the digital signing function that encrypts the hash of message x with the private key$P_{TA}^{-1}$,
- ***C*** corresponds to the three large prime random numbers known also as nonces,
- ***Par*** is unique to each vehicle and it stands for secret parameters.
- $< C > Par$ is the outcome of the challenge algorithm that takes as an input the random numbers (C) and the parameters *Par*,

- ***Messages (simplified and formally idealized using Logic of BAN):***

- M1. $V_J$ →RA: $P_J$, $SIG_{P_{RA}^{-1}}(P_J)$, $\{NUM, SIG_{P_{TA}^{-1}}(NUM)\}P_{RA}$.
- M2. RA→$V_J$: $P_{RA}$, $SIG_{P_{TA}^{-1}}(P_{RA})$, $(C)P_J$.
- M3. $V_J$ →RA: $(RA \overset{< C > Par}{\rightleftharpoons} V_J)P_{RA}$.
- M4. RA→$V_J$: (Pseudonyms, Certificates)$P_{RA}^{-1}$ …. *(M4 is not necessary for the demonstration)*

- ***Assumptions:***

- $V_J$ believes TA ... (1)
- RA believes TA ... (2)
- RA believes ($\overset{P_{TA}}{\longrightarrow}$ TA) ... (3)
- $V_J$ believes ($\overset{P_{TA}}{\longrightarrow} TA$) ... (4)
- $TA \overset{Par}{\rightleftharpoons} RA$ ... (5)
- $TA \overset{Par}{\rightleftharpoons} V_J$ ... (6)
- RA believes (TA controls RA $\overset{P_J^{-1}}{\longleftrightarrow} V_J$) ... (7)
- RA believes (TA controls RA $\overset{P_J}{\leftrightarrow} V_J$) ... (8)
- $V_J$believes (TA controls RA $\overset{P_{RA}^{-1}}{\longleftrightarrow} V_J$) ...(9)
- $V_J$believes (TA controls RA $\overset{P_{RA}}{\longleftrightarrow} V_J$) ...(10)

- ***Objectives:***

- $V_J$ believes RA
- RA believes $V_J$

- ***Demonstration:***

*RA deduces the following when it receives M1:*

1. RA sees $P_J$ , $SIG_{P_{RA}^{-1}}(P_J)$, $\{NUM, SIG_{P_{TA}^{-1}}(NUM)\}P_{RA}$..(BAN Logic Postulates, Principal 4)
2. RA sees $P_J$….(Principal 4 of BAN Logic Postulates)
3. RA sees NUM …. (Principal 4 of BAN Logic Postulates)
4. RA believes (TA said NUM)…. (BAN Logic Postulates 1 and 4, assumptions 2,3)

When Vehicle $V_J$ receives M2, it concludes the following:

1. $V_J$ sees $P_{RA}$ , $SIG_{P_{TA}^{-1}}(P_{RA})$, $(C)P_J$. …. (BAN Logic Postulates, Principal 4)
2. $V_J$ sees $C$…. (BAN Logic Postulates, Principal 4)
3. $V_J$ sees $P_{RA}$ …. (BAN Logic Postulates- Principal 4, assumption 1)

*After the reception of M3, RA deducts what follows:*

1. RA sees $RA \overset{<C>Par}{\rightleftharpoons} V_J$….( BAN Logic Postulates, Principal 4)
2. RA believes $V_J$ said $<C>Par$…. (BAN Logic Postulates-Principal 4, assumptions 5, 6)

*From the above deductions (M1.4, M2.2, M3.2), the assumptions, and BAN Logic Principal 3: 'jurisdiction'*

1. $V_J$ believes RA
2. RA believes $V_J$

#### 3.3.3.3. SPAN and AVISPA tool

The BAN logic demonstrated logic correctness of the scheme. Yet, this proof is not automated, and an additional automated robustness analysis is needed. Therefore, we specified the proposed anonymous authentication using HLPSL and verified it with the tools SPAN (Security Protocol ANimator) and AVISPA (Automated Validation of Internet Security Protocols and Applications). In our specification, we alleviated the algorithm defined by (Equation 3.4) to a simpler algorithm which is the XOR operation. Departing from the fact that if the scheme is deemed robust with XOR algorithm, then, it is so with the more complex algorithm given in (Equation 3.4). Both the vehicle and the regional authority specifications of the authentication protocol are presented in Figure 3.8.

The security objectives are:

- secrecy_of p0
- authentication_on vehicle_authority_ndef

In the specification, 'secret' instruction is used to ensure the secrecy of P0 from entities other than the regional authority and the vehicle. P0 refers to the ticket's reference number. The events 'request' and 'witness' are used to verify that the authenticating node is correct in trusting that its intended peer is participating in this session, is at a certain state, and agrees on a given fresh value [148]. In our specification, they were used to ensure the generated random numbers and the calculated outcomes' authenticity. Noting that the numbers (**d, e, f**) are the XORs of (**a, b, c**), where XOR is the alleviated challenge defined in Equation 3.4.

Figure 3.6 shows the specified authentication protocol Message Sequence Chart (MSC). Figure 3.7 illustrates exchanged messages in the presence of the intruder who intercept the messages but cannot read them and who tries to execute the replay attack but fails. This indicates that by using our scheme, the vehicle authenticates to the regional authority securely and anonymously even with the presence of an intruder's.

Figure 3.9 illustrates the OFMC verification output, which illustrates that the protocol is safe. OFMC verifier is an On the Fly Model Checker that analyses security protocols, it is used by the SPAN and AVISPA tool.

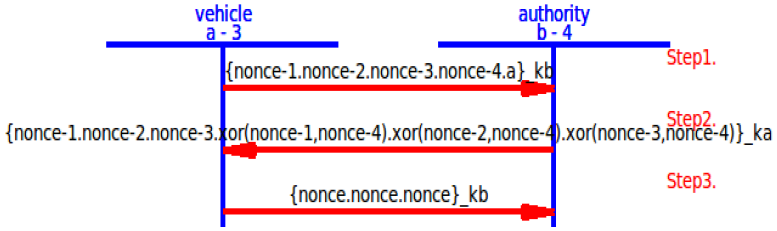



**Figure 3. 6:** Message sequence chart of the Specified authentication method

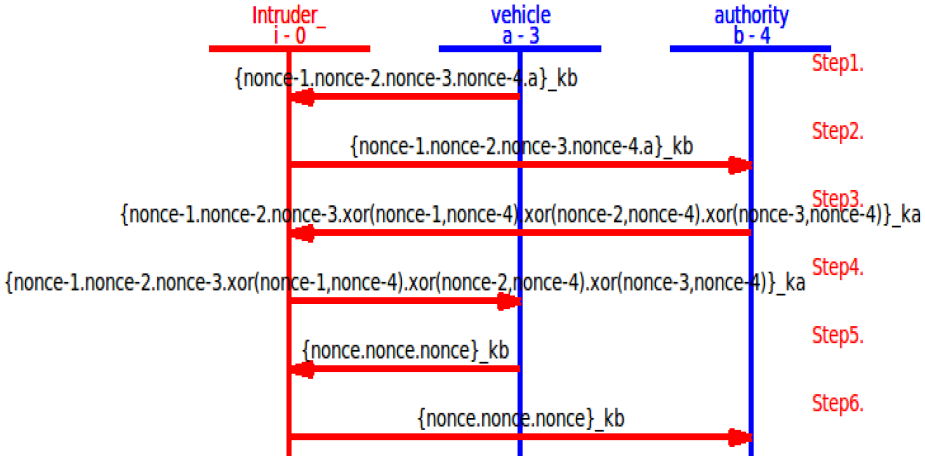



**Figure 3. 7:** Message sequence chart of the authentication method in the presence of Intruder.

**Vehicle code**

```
role vehicle (A, B: agent, Ka, Kb: public key, SND, RCV:
channel (dy))
played by A def=
  local State: nat,
   Na, Nb, Nc, Nd, Ne, Nf, P0: text,
  init State: = 0
  transition
    0.      State = 0 /\ RCV (start) =|>
            State': = 2 /\ Na': = new () /\ Nb': = new ()
                        /\ Nc': = new () /\ P0': = new ()
                        /\ SND ({Na'. Nb'. Nc'. P0'. A}_Kb)
                        /\ secret (P0', p0, {A,B})
/\witness (A, B, authority_vehicle_nabc, Na'. Nb'. Nc')
    2.  State = 2 /\ RCV ({Na.Nb.Nc. Nd'. Ne'. Nf'}_Ka) =|>
        State': = 4 /\ SND ({Nd'. Ne'.Nf'}_Kb)
/\ request (A, B, vehicle_authority_ndef, Nd'.Ne'.Nf')
end role
```

**Regional Authority Code**

```
role authority (A, B: agent, Ka, Kb: public_key, SND, RCV:
channel (dy))
played_by B def=
 local State: nat,
 Na, Nb, Nc, Nd, Ne, Nf, P0: text,
  init State: = 1
  transition
      1.  State = 1 /\ RCV({Na'.Nb'.Nc'.P0'.A}_Kb) =|>
          State': = 3 /\ Nd': = xor(Na',P0')
                      /\ Ne': = xor(Nb',P0')
                      /\ Nf': = xor(Nc',P0')
              /\ SND({Na'.Nb'.Nc'.Nd'.Ne'.Nf'}_Ka)
/\ witness (B, A, vehicle_authority_ndef, Nd'.Ne'.Nf')
      3.  State = 3 /\ RCV({Nd.Ne.Nf}_Kb) =|>
          State': = 5
/\ request (B, A, authority_vehicle_nabc, Na.Nb.Nc)
end role
```

**Figure 3. 8:** Vehicle's and RA's HLPSL Specification code

```
% OFMC
% Version of 2006/02/13
SUMMARY
 SAFE
DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
 /home/span/span/testsuite/results/sample.if
GOAL
 as_specified
```

**Figure 3. 9:** Result of the specified protocol using SPAN and AVISPA

## 3.4. Conclusion

In this chapter, we explained the anonymous reputation-based privacy-preserving authentication method used to preserve the privacy when forming/using the Cloud-enabled Vehicular Named Data Networks (CVNDN). The proposed method although anonymous, it ensures the correct functionality of the network and the accountability. We analyzed its correctness using BAN logic and proved that it achieves the authentication purposes.

Moreover, we also presented a secure privacy-preserving scheme for pseudonym refilling on-demand and on-road. The solution is distinguishable for ensuring anonymity and being identity-less. It ensures the accountability (non-repudiation), revocation of the misbehaving node and prevents Sybil attack. To demonstrate that the proposed scheme achieves the authentication objectives BAN logic was used, and to prove that it is safe and resilient to replay, man-in-the-middle and impersonation attacks the tools SPAN and AVISPA were utilized. The proposal is also designed to be resilient to the following attacks: Sybil, session hijacking, guessing and brute-force attacks.

# CHAPTER 4

# PRESERVING THE LOCATION PRIVACY OF VEHICULAR NETWORKS USERS

## 4.1. Introduction

We explained in the first chapter the types of vehicular networks and in the second chapter the privacy issue in these networks. Then, in the previous chapter, we proposed two anonymous authentication methods that preserved the identity privacy. The identity preservation helps in preventing tracking. However, the location privacy may be threatened by the vehicle's cyber-activity. More precisely, when it is periodically broadcasting state messages containing its locations. In this chapter, we propose two schemes that protect the location privacy on the road for vehicular ad hoc network users. The proposed solutions rely on obfuscation of location prior to the change. The first proposal uses a camouflage technique before changing the pseudonym. The second proposal takes advantage of the crowd if within dense roads and executes obfuscation technique elsewhere.

We also propose three solutions that preserve the location privacy when using cloud-enabled IoV location-based services and safety applications: the first is crowd-based to thwart identifier linkability and protect against tracking. We analyzed its performance against a modelled global passive attacker executing semantic, syntactic, observation mapping and linkage mapping attacks. We also compared it to a state-of-art solution through simulation by using NS2. The second proposal strengthens the previous one with the use of concerted silence. In the third proposal, we enhanced the second solution by adding obfuscation method on the location fields.

We remind the readers that we already surveyed the prominent related state-of-art works in Chapter 2. Our solutions developed to protect VANET users are different from the existing because they are designed to be road, crowd and infrastructure independent as none of the above conditions may be continuously available during the update phase. While the solutions developed to protect the IoV users are crowd and obfuscation based. All of the proposed schemes, when analyzed, demonstrated optimistic protection levels against the modelled attacker.

The chapter is organized as follows:

Part 2 describes the attacker model.

Part 3 explains the solutions proposed to preserve the location privacy for VANET users along with their analysis.

Part 4 illustrates the solutions proposed to preserve the location privacy for IoV users along with their analysis.

Part 5 concludes the chapter.

## 4.2. Adversary model

We already explained in Chapter 2 how the attacker may intercept the vehicle's wirelessly broadcasted beacons and use them to track its past and current locations. We defined various types of linking attacks that are executed by the attacker to achieve his/her aim. In this chapter, our attacker is Global Passive Attacker (GPA) that implicitly installs his/her receivers to fully cover the road (observation area). The GPA executes four linking attacks which are the semantic, the syntactic, the observation and the linkage mapping attacks. We remind the readers that these attacks were already explained in Chapter 2. The attacker model was simulated using NS2 simulator with a grid of 100 receivers, the range of each 500m fully

covering the road. This model was used to evaluate the performance of our proposals explained in this chapter. Noting that to evaluate the performance of the solutions proposed to preserve the location privacy in VANET, our attacker executes semantic and syntactic attacks only. While the evaluation of the solutions proposed for CE-IoV is against the attacker executing all of the four mentioned attacks.

Noting that the GPA being passive is difficult to detect. This gives him/her various advantages such as the long tracking periods, wider knowledge about the road restrictions, cyber-profiling, the possibility to trade the user's tracks and secrets undetectably. The GPA would know the victim user vehicle's entire parsed trajectory without the victim user even taking notice. Thus, the GPA has the upper hand over the targeted victim which is unaware of him/herself being tracked. Just as Sun Tzu said in his book art of war: "*If you know the enemy and know yourself, you need not fear the result of a hundred battles*" [149] [150]. Table 4.1 resumes the parameters settings of the GPA.

**Table 4. 1:** Simulation parameters of the attacker

| | |
|---|---|
| Tools | NS 2, |
| Simulation time | 900 seconds |
| Map | 1000x1000, Manhattan Grid |
| Number of attacker's receivers | 100 |
| Attacker coverage range | 500m |

## 4.3. Preserving Location Privacy for VANET Users

### 4.3.1. Proposed Camouflage-based location privacy-preserving scheme

To preserve the location privacy, we use a camouflage mechanism prior to the update of pseudonym to thwart the linkability even within roads with low density. Before the vehicle pseudonym's minimum lifetime $T_e$ is reached, the vehicle starts executing the camouflage technique, let this time be denoted as $T_s$ where ($T_s < T_e$). For time $\Delta t = T_e - T_s$ the vehicle is executing the camouflage technique and at $T_e$ it does the change. The change strategy is illustrated in Algorithm 4.1 and the camouflage technique in Algorithm 4.2.

**Algorithm 4. 1**: Pseudonym Change Scheme

```
Input: Ts, Te: time; k-fake: integer.
While (true)
    Current_Time:= getCurrentTime()
    If (Current_Time=Ts)
            While (Current_Time ≤ Te)
            Camouflage_Technique(k-fake)
            Current_Time:= getCurrentTime()
            EndWhile
    Pseudonym:= new Pseudonym ()
    Position:= CurrentPosition()
    Speed:= CurrentSpeed()
    Send Beacon (Pseudonym, Position, Speed)
    EndIf
EndWhile
```

The camouflage technique generates a virtual crowd before doing the change by creating fake messages to confuse the attacker. That is why our solution is crowd independent and protects the privacy even within low-density roads. The fake messages contain fake pseudonyms, locations and speeds. The locations follow the road restrictions and are not random to prevent the attacker that is aware of the road map from detecting them as fake. The fake messages are sent along with the real ones. This gives the attacker the illusion that there are *k* vehicles on road that are broadcasting *k* beacons with *k* pseudonyms during Δt and slightly after the change. We remind the readers that the tracking is done by message interception. No cameras nor signal tracking tools are used. The fake pseudonyms are either self-generated not certified, signed by the vehicle's expired pseudonyms, not signed at all or a set of expired pseudonyms.

**Algorithm 4. 2**: Camouflage_Technique (integer k)

```
\*Creating virtual crowd*\
Psd:= CurrentPseudonym()
Pos:= CurrentPosition()
Speed:= CurrentSpeed()
Send Beacon (Psd, Pos, Speed)
For (i=1; i≤k; i+1 )
    Psdi:= FakePseudonym()
    Posi:= FakePosition()
    Speedi:= FakeSpeed()
    Send Beacon (Psdi, Posi, Speedi)
End-for
```

#### 4.3.1.1. Analytical Model

We already defined the analytical metrics in Chapter 2. In this chapter we use the anonymity set size ASS, and the entropy as our evaluation metrics. The ASS is calculated as follows:

Let V be a vehicle doing the change, ***k*** number of fake messages sent before the change with ***k*** fake pseudonyms. Therefore, it can be considered as ***k*** virtual fake vehicles. ***m*** is the number of cooperative neighbor vehicles changing their pseudonyms simultaneously with V. ***l*** is the number of non-cooperative neighbor vehicles which they do not do the change, or they do it asynchronously with V.

The following cases are distinguished in Equations 4.1-4.4:

1- V is alone when it changes its pseudonym:

***Equation 4. 1:*** $ASS = k$

2- V is within ***m*** vehicles when it changes its pseudonym:

***Equation 4. 2:*** $ASS = k\,(m + 1)$

3- V is within ***l*** vehicles when it changes its pseudonym:

***Equation 4. 3:*** $ASS = k + l$

4- V is within ***l + m*** vehicles when it changes its pseudonym:

***Equation 4. 4:*** $ASS = k\,(m + 1) + l$

The entropy H is calculated as follows in Equation 4.5:

***Equation 4. 5:*** $H = -\sum_{i=1}^{ASS} p_i log_2(p_i)$

Where $p_i$ is calculated in Equation 4.6 :

***Equation 4. 6:*** $$p_i = \frac{1}{k(m+1)+l}$$

The tracking time **T** is divided on ***n*** time interval $t_i$ which is the lifetime of the pseudonym. Tracking the vehicle for **T** means tracking its trajectory parsed during **T**. Therefore, the probability of tracking the vehicle in ***n*** consecutive observation interval $t_i$ is the probability to track its parsed trajectory noted as $P_{trajectory}$ (defined in Equation 4.7), where the probability of tracking it in $t_i$ is $p_i$

***Equation 4. 7:*** $$P_{trajectory} = p_1 * p_2 * \dots * p_i * \dots * p_n$$

We now compare analytically the probability of tracking the vehicle's parsed trajectory, if it is alone on road during all the observation period T. Knowing that the vehicle without using our camouflage technique can certainly be tracked whether it changes its pseudonym or not. i.e. $p_i$=1, i∈ [1, n] and $P_{trajectory}$=1.

In our case, if V is alone on the road, $p_i$ would be calculated as illustrated in Equation 4.8:

***Equation 4. 8:*** $$p_i = 1/k,\ k>1$$

and $p_i$ is identical in all intervals.

Therefore, $P_{trajectory} = (P_i)^n < 1$,

This further proves that our solution reduces the tracking as the observation period increases and the vehicle continues its pseudonym change using our camouflage technique.

### 4.3.1.2. Simulation

#### 4.3.1.2.1. Settings

We continue in this section explaining the simulation settings and scenarios and the process used to sort the results. The simulation was done using NS2 simulator. Both of the attacker's and the vehicle's code were written in C++ language. The scenarios were written in TCL files where we specified the simulation settings given in Table 4.2. The mobility models of the vehicle were generated using Mobisim tool on a Manhattan grid map where the vehicles' number variated from low to high density.

**Table 4. 2:** Simulation parameters

| | |
|---|---|
| Tools | NS 2, Mobisim |
| Mac layer | 802.11p |
| Simulation time | 900 seconds |
| Map | 1000x1000, Manhattan Grid |
| Pseudonym minimum lifetime | 30 seconds |
| Vehicle Range | 300 m |
| Number of vehicles | 10-200 |

Before explaining the results treatment process, we first explain how we fixed the number of vehicles in the created virtual crowd denoted as *k-fake* or shortly *k,* and the duration for which the camouflage technique is used $\Delta t$ *or dt.* To decide their values, we investigated their impact on the level of privacy provided by trying various values. We also considered their impact on the resulted overhead by evaluating the number of sent and received messages. We conducted the investigation on a scenario with 25 vehicles with the same map specified in

Table 4.2. Figure 4.1 resumes the investigation results. We found that the tracking ratio was the lowest with almost full resiliency to syntactic attack when Δt=2 and k-fake=3. Also, the overhead and message dropping interpreted by the number of sent and received messages were acceptable. Therefore, we choose to use these values for *k, Δt* in the rest of the simulation.

Noting that because we are concentrating on the safety applications requiring the periodic broadcast of state messages known as beacons, it is hard to calculate the dropping ratio as the destination is not unique. Also, because these messages are sent even if the vehicle is alone on road. Instead, we compared the exchanged messages to investigate the impact of increasing the number of generated fake beacons during Δt interval which we found that it overally increased.

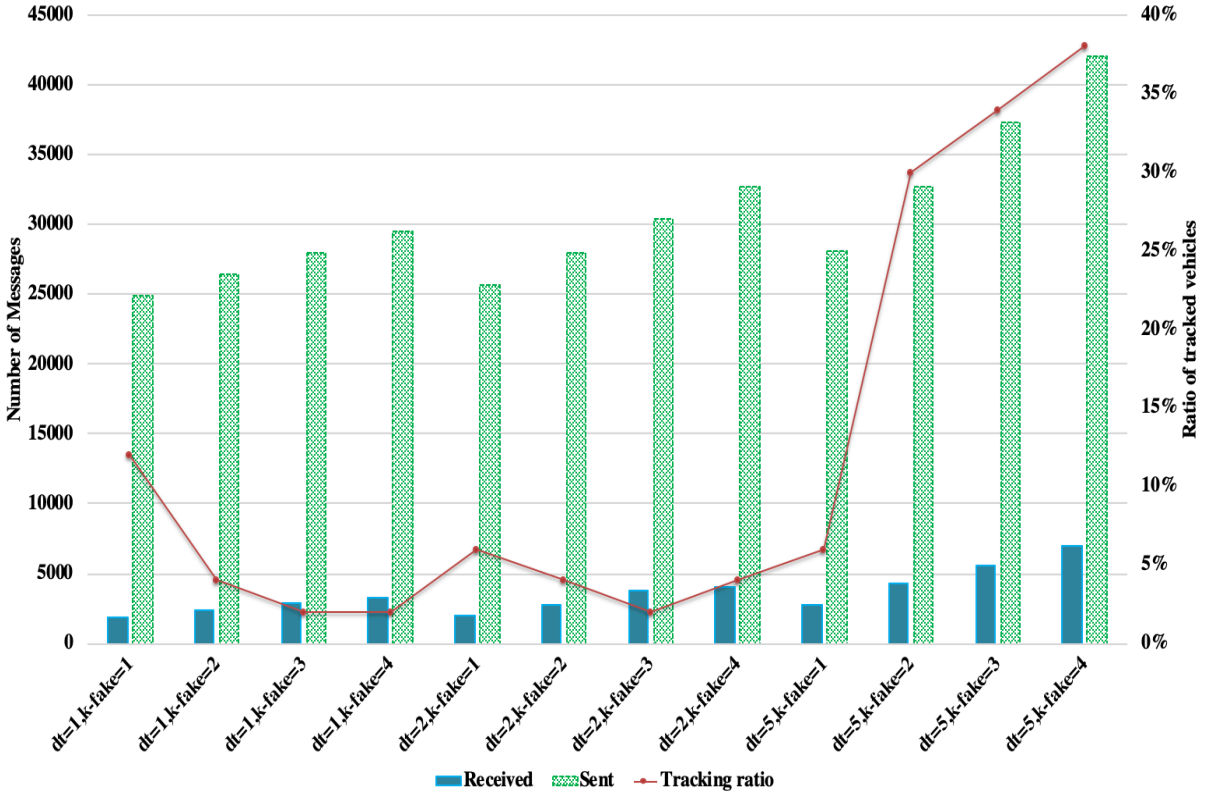



**Figure 4. 1:** Investigating the impact of varying Δt and k-fake on the privacy, number of sent and received messages.

#### 4.3.1.2.2. Results and analysis

Now that the *Δt* and *k* values are fixed to give the lowest tracking ratio with the minimum impact on the overhead and dropping ratio. We continue to explain how the simulation results were processed and the tracking ratio is calculated. Then, we illustrate the results in the coming figures, we comment and analyze them.

Our simulation generates trace files for the vehicle's activity and the attacker's tracks. The vehicle's trace file is sorted and organized to enable the extraction of the number of the pseudonym change as well as the verification of the attacker's tracks accuracy. While the attacker's trace file is processed to separate the tracks by attack and calculate the tracking ratio and the pseudonym linking ratio.

Let $R_{track}$ be the tracking ratio of the attacker, $R_{Sem}$ is the tracking ratio of the Semantic attack and the $R_{Syn}$ is for the Syntactic attack. $T_{psd}$ is the total number of pseudonym changes.

$T_v$ is the total number of vehicles. $L_{psd}$ is the total ratio of linked pseudonyms; $L_{psd1}$ is the ratio of linked pseudonyms by semantic attack and $L_{psd2}$ by the syntactic attack. $l_{psd1}$ is the number of linked pseudonyms by the semantic attack and $l_{psd2}$ by the syntactic attack. $V_{sem}$ is the number of tracked vehicles by the semantic attack and $V_{syn}$ by the syntactic attack.

The ratios are calculated as explained in the equations (4.9-4.14):

***Equation 4. 9:*** $$R_{sem} = \frac{V_{sem}}{T_v}$$

***Equation 4. 10:*** $$R_{syn} = \frac{V_{syn}}{T_v}$$

***Equation 4. 11:*** $$R_{track} = (R_{sem} + R_{syn})/2$$

***Equation 4. 12:*** $$L_{psd1} = \frac{l_{psd1}}{T_{psd}}$$

***Equation 4. 13:*** $$L_{psd2} = \frac{l_{psd2}}{T_{psd}}$$

***Equation 4. 14:*** $$L_{psd} = (l_{psd1} + l_{psd2})/2$$

Figure 4.2 shows the attacker's tracking ratio ($R_{track}$). This ratio was between 17% for high-density scenario and 40% for low-density scenario. Thus, the privacy is preserved with at least 60% which is the ratio obtained in the worst-case scenario when the update happens in low-density roads. This is considered as a high ratio for such a scenario.

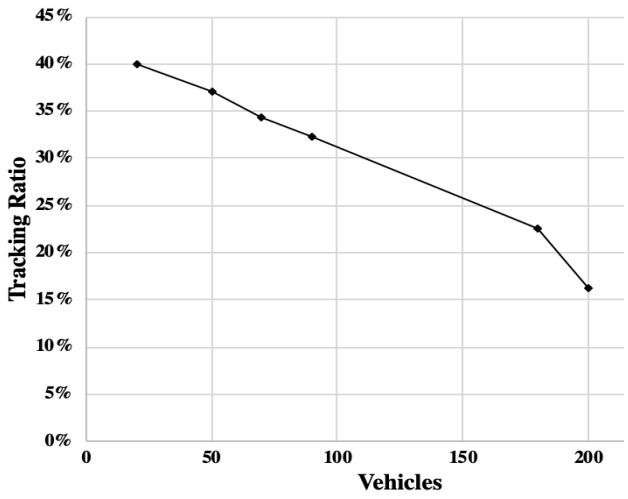



**Figure 4. 2:** Ratio of tracked vehicles

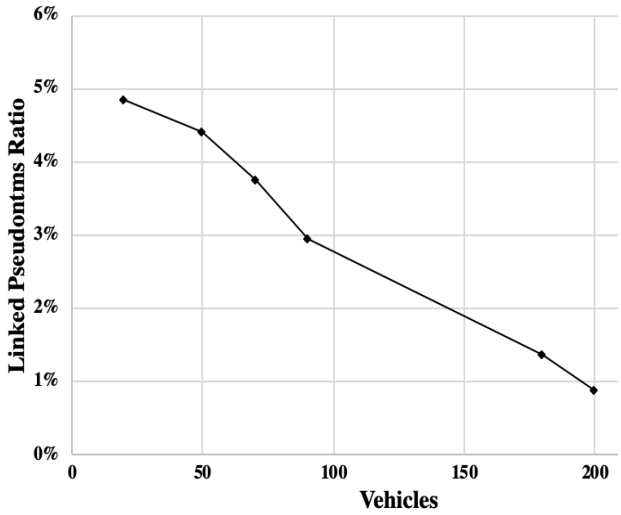



**Figure 4. 3:** Ratio of linked Pseudonyms.

Figure 4.3 resumes the linked pseudonyms ratio $L_{psd}$ which varied from 0.9-4.8% and overally did not exceed 5%. This further proves the robustness of the solution in achieving the pseudonyms unlinkability upon their update. Thus, preventing the trajectory tracking and preserving the location privacy.

When we compared our solution to the periodical pseudonym change scheme where the vehicles update their pseudonyms upon their expiry independently without taking any extra measure. We found that our solution has a lower ratio than that of the periodic change especially in low-density roads where the tracking ratio difference is huge. It was 70% when using periodic change and 15% when using our solution against an attacker executing the syntactic attack. Therefore, our solution reduces considerably the tracking ratio. Especially, in

the case of low-density roads outperforming the standard periodic change solution in persevering the location privacy. Figure 4.4 illustrates the obtained tracking ratio for both solutions.

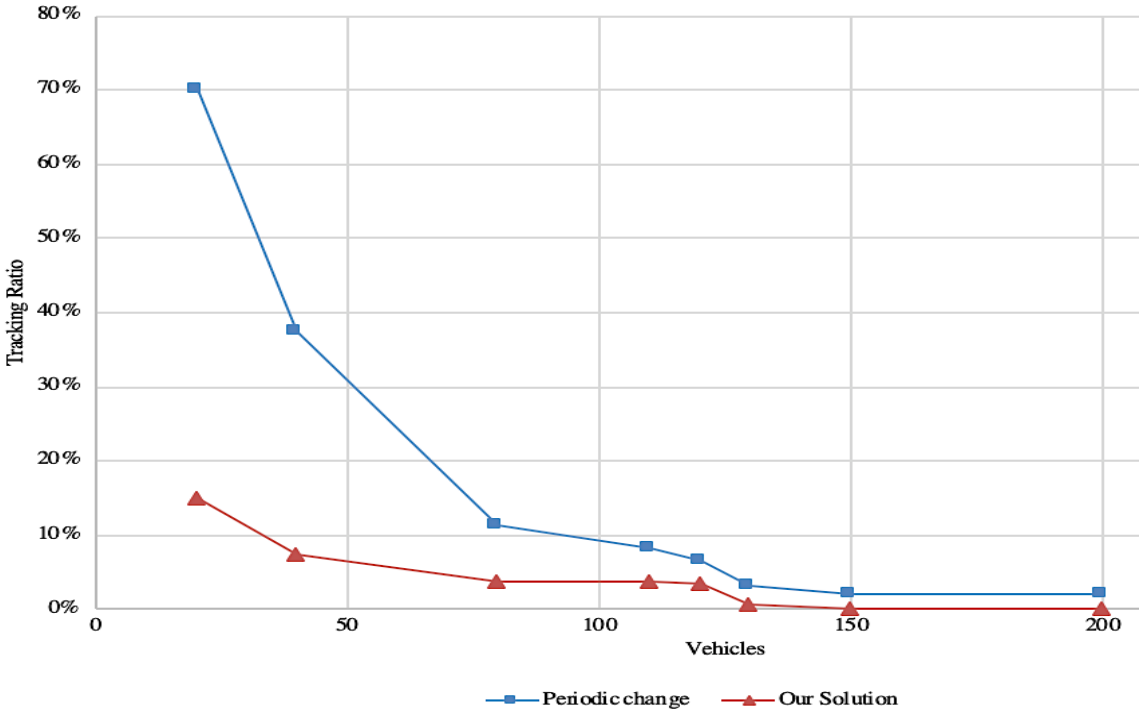



**Figure 4. 4:** Ratio of tracked vehicle

## 4.3.2. Proposed Hybrid Pseudonym Change Strategy

In this section, we explain the second proposal. We start first by describing the used assumptions then illustrating the proposed scheme followed by the simulation results.

### 4.3.2.1. Hypothesis and Assumptions

We follow the IEEE 1609.2 standard indicating that the public key certificate has a validity time and space. This means that the pseudonyms are time and space slotted. For example: let vehicle V1 have three pseudonyms (A, B, C), and V2 have three pseudonyms (D, E, F).

- 'A' is valid within region R1 and has the lifetime of 60 seconds starting from t1= 11h30min.
- 'B' is valid within region R1 and has a lifetime of 60 seconds starting from t2= 11h31min.
- 'C' is valid within region R1 and has a lifetime of 60 seconds starting from t2= 11h32min.
- 'D' is valid within region R1 and has a lifetime of 60 seconds starting from t1= 11h30min.
- 'E' is valid within region R1 and has a lifetime of 60 seconds starting from t2= 11h31min.
- 'F' is valid within region R1 and has a lifetime of 60 seconds starting from t3= 11h32min.

Therefore, both vehicles V1 and V2 change their pseudonyms at the same time and within the same region. If these vehicles happen to be in the same vicinity (neighbors). Then, this change is implicitly cooperative without the explicit synchronization between the vehicles. The privacy level achieved is the same as that of the schemes supposing the change to happen within a cooperative crowd.

### 4.3.2.2. Changing the Pseudonyms

Figure 4.5 illustrates the change scenarios, which is triggered either by:

- Reaching the limits of authorized geographical space (see Figure 4.5 I.A, II.A).
- Expiry of validity time (see Figure 4.5 I.B, II.B)

Part 'I' of Figure 4.5, is the illustration of the example explained above. The vehicle is within a crowd when it updates its pseudonym either because it reaches the geographical limits (A) or the expiry of its lifetime (B). Therefore, it explains the case of implicit cooperative change.

In part 'II', the vehicle senses its neighborhood prior to the update. If it finds that it is within less dense roads with a number of neighbors less than the expected threshold *k*. It starts executing an obfuscation method by altering the beacon's location and speed fields before the pseudonym update to confuse the attacker. For Δt period of time, the vehicle sends beacons with the speed field set to 0, and the position set to the one before the change. After the update, the vehicle sends beacons with its real position and speed and freshly changed pseudonym. By doing so, the attacker is deluded that the vehicle has stopped on road while it is running. Therefore, cannot link the new pseudonym used from a new far location from that announced by the vehicle using the old pseudonym. The vehicle with the new pseudonym is detected as a new one instead of linking the freshly used pseudonym with the old one (see Figure 4.5 II. A, B).

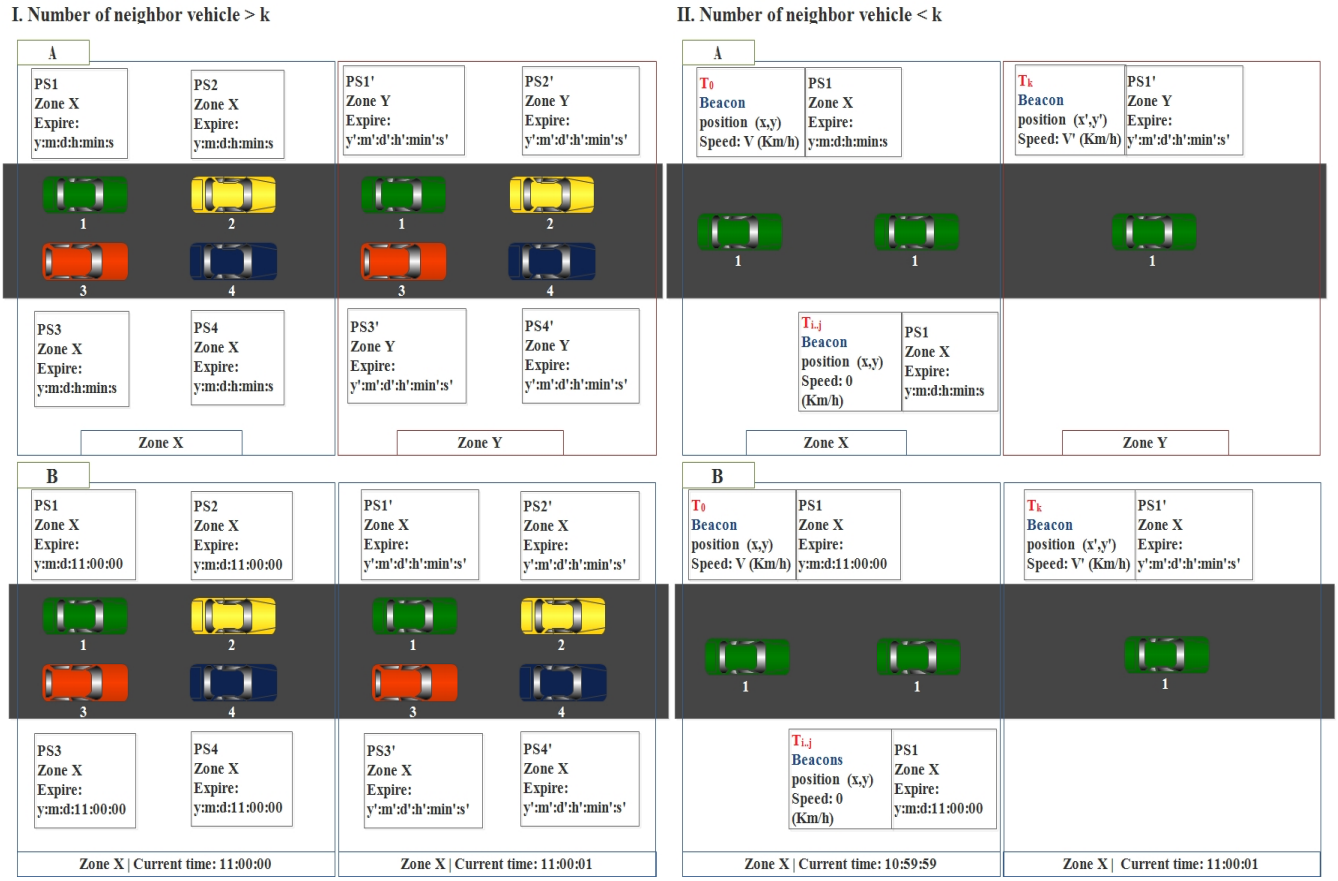



**Figure 4. 5:** The Proposed Pseudonym Changing Scheme

Like we explained before, Δt is the time needed to confuse the attacker through the use of the obfuscation to break his/her accurate predictability. Noting that the attacker relies on the vehicle's current and past locations, velocity and headings to predict its next location. Thus, when s/he receives erroneous or inaccurate spatiotemporal data, his/her predictions become wrong and fuzzy.

Although we aim to protect the privacy, we give the highest priority to safety applications. Thus, if an urgent event occurs requiring the vehicle to send its real location in a report, it ought to do so.

Figure 4.6 gives a flow chart description of the proposed pseudonym changing process when the trigger is the expiry of the pseudonym.

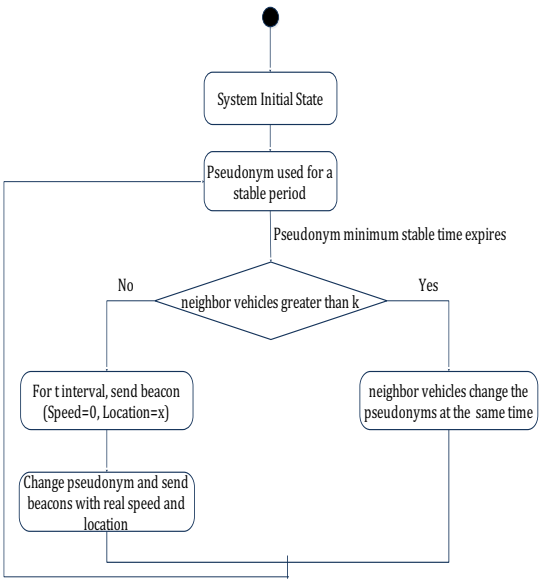



**Figure 4. 6:** Pseudonym Changing Process

Algorithm 4.3 resumes the pseudonym change algorithm triggered either by the expiry of the pseudonym lifetime or the attainment of geo-space limit.

**Algorithm 4. 3**: Pseudonym Change Algorithm

```
Begin
  While (true)
      Current_neighbors = Count-neighbors()
      If (Pseudonym Lifetime expire) OR
        (Pseudonym exceeds Geo-space limits) then
          If(Current_neighbors>= threshold-neighbors) then
            Pseudonym= new pseudonym ()
          Else
            Current_position= position()
            Speed=0
            Current_pseudonym= Pseudonym
            While (Time < Tchange)
             \* Alluding the attacker that the vehicle is stopping while its running*\
              Beacon (Current_pseudonym, Current_position, Speed)
              Send (Beacon)
            EndWhile
            Pseudonym= new pseudonym ()
          Endif
      Endif
    Beacon (Pseudonym, position (), speed())
    Send (Beacon)
    EndWhile
End
```

#### 4.3.2.3. The Simulation

After explaining the proposed scheme, we continue to resume the simulation results of our solution against a GPA. The implementation was done using NS2 simulator. The process of sorting the results is similar to the one used in the previous solution and so does the simulation settings which were resumed previously in Table 4.2. We used three simulation scenarios with low, medium and high traffic density (50, 100 and 150 vehicles respectively). Noting that we use the description low, medium and high taking the distributions of the vehicles and the map surface into consideration, therefore, these expressions do not have a fixed quantitative equivalent and may be used in the continuity of the thesis in other scenarios with different vehicle densities. The GPA modelled executes two linking attacks which are the semantic and the syntactic.

Figure 4.7 resumes the obtained tracking ratio for each scenario. Overally, the tracking ratio decreased as the traffic density increased which means that there are more chances that the vehicle changes its identifier within a cooperative crowd. Moreover, the solution's robustness and high performance in preserving the location privacy was translated by the low tracking ratios which did not exceed 17%.

Figure 4.8 illustrates the linked identifiers ratio by both attacks per each scenario. Although the total number of pseudonym changes is large, the ratio of linked pseudonyms is low. It did not exceed 1%. This further proves that the solution is robust.

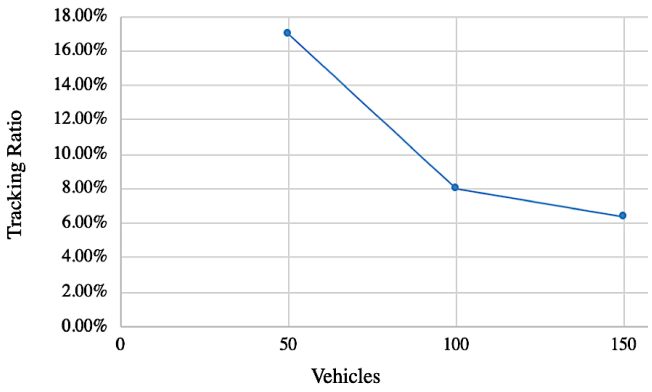



**Figure 4. 7:** Ratio of tracked vehicles

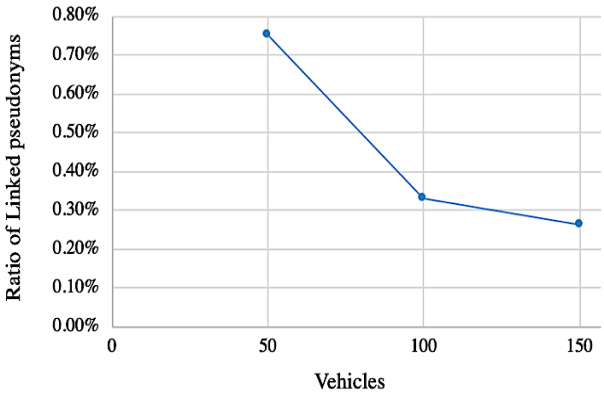



**Figure 4. 8:** Ratio of linked pseudonyms

To further analyze the performance of our solution. We compared it with the periodical pseudonym change strategy. Figure 4.9 illustrates the obtained tracking ratio for both solutions per scenario. Our solution has a lower ratio than the periodical change solution. Thus, a higher resiliency to the implemented attacker model executing semantic and syntactic.

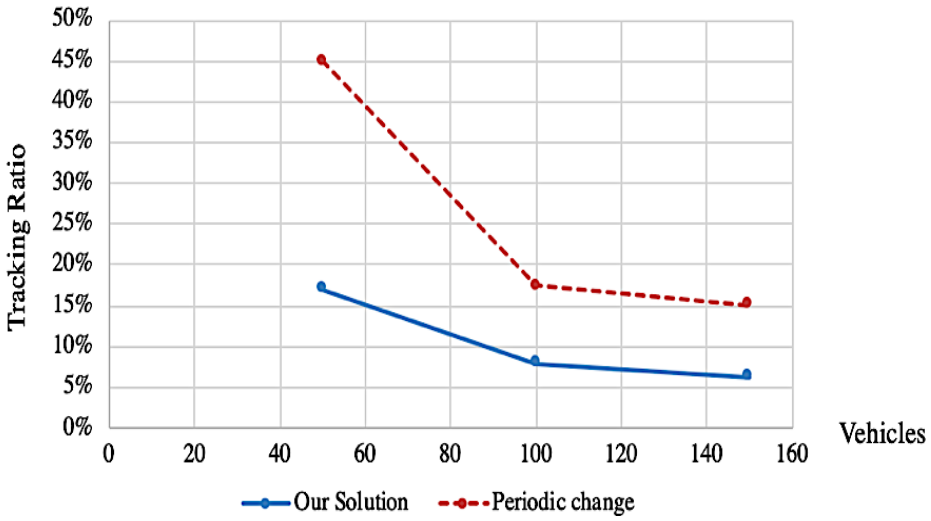



**Figure 4. 9:** Ratio of tracked vehicle for both solutions

## 4.4. Preserving Location Privacy for CE-IoV Users

### 4.4.1. CLPPS: Cooperative-based Location Privacy-Preserving Scheme for Internet of Vehicles

In this section, we explain the first proposed scheme to protect the location privacy for cloud-enabled internet of vehicles which is illustrated in Figure 4.10. The scheme protects the privacy on two levels: the safety beaconing level and the CE-IoV LBS level. The details of each level are given in the following subsections separately.

- **Anonymity and location privacy in safety beaconing level**

To ensure the anonymity, the pseudonyms are used and their change with robust strategies is needed to protect the location privacy from linkability and tracking. Our change strategy relies on the cooperation of neighbors. The vehicle needs to synchronize its pseudonym change with its neighbors to thwart linkability. However, since we mentioned that the privacy solution should not influence negatively the network functionality, the synchronization between vehicles need to be optimal without adding extra messages or increasing the overhead on the network. Especially that the more vehicles are there in the vicinity, the higher are the chances for collision, message drop or broadcast storms to occur. Therefore, to implement our scheme with the least overhead possible, we utilized two bits from the beacon header extra non-used bits, one is RDC (Ready to Do the Change) set to 1 when the vehicle wants to announce its will and readiness to update its pseudonym and to 0 otherwise. The other bit is DC (Do the Change) which is set to 1 when the vehicle has satisfied its pseudonym update context and to 0 otherwise. Noting that the expiry of the minimum stable lifetime of the vehicle's pseudonym is the trigger to set RDC to 1. The pseudonym change context is receiving $k$ beacons from $k$ distinct neighbor vehicles willing to do the change which means their RDC is set to one. When the vehicle sets its DC to 1, it does the change on the next time slot. Hence, its next beacon would be signed with the freshly updated pseudonym. Similarly, vehicles that receive DC flagged beacons also change their pseudonyms in the next time slot and resume their beaconing with their newly updated pseudonyms. Achieving a simultaneous change and reducing the attacker's tracking accuracy from 1 to $1/k$ for his/her target being anyone from the $k$ potential

candidates. Naturally, the confusion increases as the number of neighbor vehicles simultaneously doing the change does.

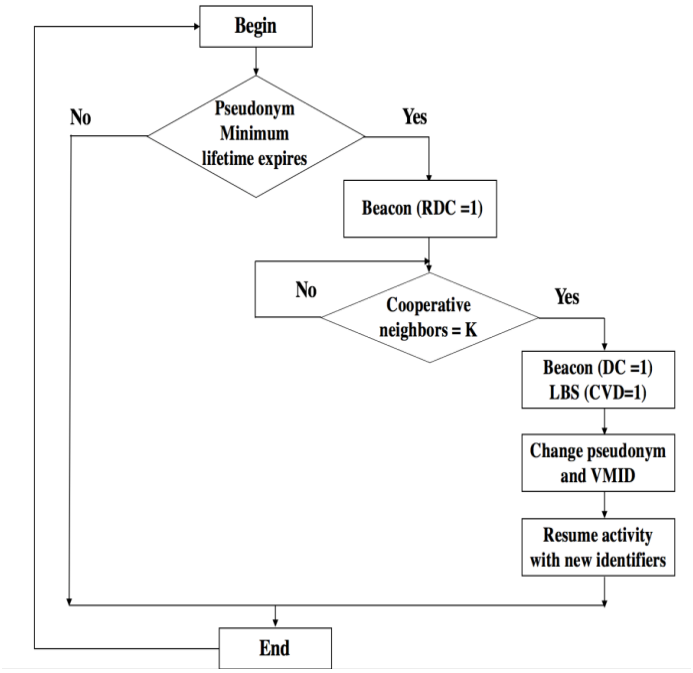



**Figure 4. 10:** Diagram of the Proposed Identifier Changing Scheme **[151]**

- **Anonymity and location privacy in CE-IoV LBS level**

When the vehicle updates its pseudonym used in the safety beacons, it also simultaneously changes its VMID used in CE-IoV LBS. Similarly, we use a bit as in the service messages header CVD (Change VMID) to inform the CM of the VMID change which in its turn record this change. We remind the readers that the aim of using the organized list of VMID is to help both the CM and the vehicle know the next VMID to be used without the need to send extra messages as both have the same copy of the ordered list. Since the vehicle updates its VMIDs sequentially from the list, the CM can map and record that easily.

Therefore, the VMIDs are updated simultaneously with the pseudonyms in a cooperative way like explained before. Upon the successful change, the vehicle and its cooperating neighbors update their identifiers and continue their activities with their new VMIDs and pseudonyms without the need to re-do the authentication to the service provider. Furthermore, since the CM records the change, it informs the service provider of the new VMID to tunnel all the pending queries with the old VMID to its destination after the update. Thus, ensuring a continuous service.

#### 4.4.1.1. Simulation

In this section, we explain how we simulated our proposal and tested it against the modelled GPA explained in section 4.2 executing four types of linking attacks. We start first by resuming the settings then analyze the obtained results.

#### 4.4.1.1.1. Settings

**Table 4. 3:** Simulation parameters for the vehicles

| | |
|---|---|
| Tools | NS 2, Mobisim |
| Mac layer | 802.11p |
| Simulation time | 900 seconds |
| Map | 1000x1000, Manhattan Grid |
| Pseudonym minimum lifetime | 30 seconds |
| Vehicle Range | 300 m |
| K cooperative neighbors | 2 |
| Scenario 1 vehicle number | 10 |
| Scenario 2 vehicle number | 50 |
| Scenario 3 vehicle number | 100 |
| Scenario 4 vehicle number | 150 |
| Scenario 5 vehicle number | 200 |

We simulated our proposal using NS2 simulator on Manhattan map grid with its mobility model for moving vehicles generated by Mobisim tool noted shortly as scenarios. We created five scenarios on the same map with the same simulation span (900 seconds) where the number of vehicles per scenario increased from 10 vehicles for low density, to (50, 100) vehicles for medium density then to (150, 200) vehicles for high density. Each vehicle periodically broadcasts state messages to its neighbors and sends LBS messages to a service provider and connectivity messages to the CM. The vehicles' simulation settings are explained in Table 4.3.

#### 4.4.1.1.2. Results

After explaining the simulation settings, we continue to clarify how the results are sorted and processed to be meaningful and illustrative in analyzing the solution's performance against the modelled attacker. After sorting them and extracting the needed ratios, we illustrate them in the coming figures. Then, we comment and analyze them.

Our simulation generates two trace files, one for the vehicle's cyber-activity including its beacons and LBS messages. The other is for the attacker's tracks when eavesdropping and intercepting vehicles messages. The vehicle's trace file is processed to separate its activities where each activity trace is saved in a separate file. Thus, we obtained a beaconing trace file and LBS messages file. These files are used to confirm that the pseudonym and VMID are changed simultaneously, to obtain the number of updates and also to check the attacker's tracks correctness and accuracy.

The attacker trace file was also processed to separate the tracks by attack resulting in four trace files each for an attack type which are the semantic, the syntactic, the linkage mapping and the observation mapping. For each attack, the number of correctly tracked nodes and correctly linked identifier change was extracted which were used to calculate the ratios defined in Equations 4.15-4.17 and presented in the Figures 4.11-4.16:

***Equation 4. 15:*** $$\textbf{ratio of tracked vehicles per attack} = \frac{\textit{number of correctly tracked vehicles per attack}}{\textit{total number of vehicles per scenario}}$$

***Equation 4. 16:*** $$\textbf{ratio of tracked vehicles} = \textbf{AVERAGE}\,(\textbf{ratios of tracked vehicle per attack})$$

***Equation 4. 17:*** $$ratio\ of\ linked\ identifier\ per\ attack = \frac{number\ of\ correctly\ linked\ identifiers}{total\ number\ of\ changed\ identifiers\ per\ scenario}$$

Figure 4.11 illustrates the calculated tracking ratio of the modelled GPA when the vehicles execute our proposed scheme. In general, the ratio was low not exceeding 30% which means that the location privacy was preserved with 70%.

Also, except for the second scenario which was less than 27%, all of the other scenarios tracking ratio were less than 15 %. We remind the reader that the vehicles' distribution on roads is random. Although we controlled the map, simulation duration and vehicles number per each scenario, we decided not to impose any constraint obliging the vehicles to be close or in the same vicinity with approximate mobility. This was done to ensure the fairness of simulation conduct and to avoid obtaining over-estimated results coming from favorable settings. Therefore, in scenario 2 where the ratio was higher than the rest, it is most likely due to the vehicle not being in a favorable context all the time. Another observation on the ratios is that they decreased as the number of vehicles increased. Noting that the lower is the tracking ratio, the higher is level of privacy, the best is the solution.

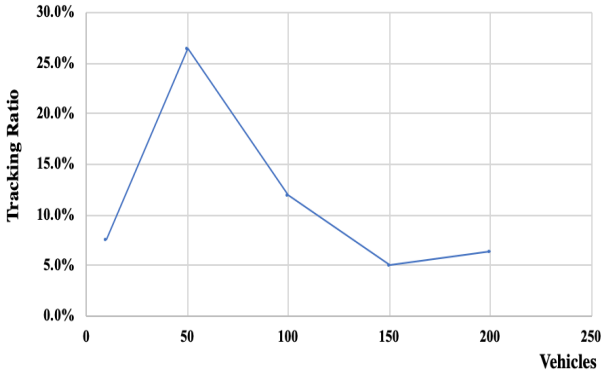



**Figure 4. 11:** Ratio of Tracked Vehicles

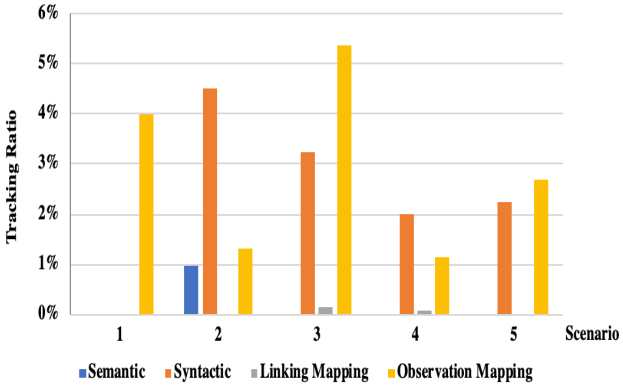



**Figure 4. 12:** Ratio of tracked vehicles per each attack

In Figure 4.12 the tracking ratios per each attack for each scenario are illustrated where the number from 1 to 5 reflects the simulated scenarios as given in Table 4.7. We notice that the tracking ratios for semantic and linking mapping attacks were approximately null for all scenarios. The syntactic attack tracking ratio was less 5%. While the observation attack tracking ratio was less than 6%. Both ratios were less than 10%. This indicates that we can ensure with more than 94% that the solution is almost resilient to these attacks, and therefore it preserves the privacy.

#### 4.4.1.1.3. Comparative study and performance analysis

To further illustrate the performance of the proposed solution against the modelled attacker, we decided to compare it with a state-of-art solution of Kang J. et al [55]. Table 4.4 resumes the key differences between our solutions and highlight the advantages and disadvantages of each solution.

To do the comparative performance study, the solution of Kang J. et al [55] was simulated under the same settings, scenarios resumed in Table 4.3 and against the same modelled attacker. Similarly, the resulted trace files were processed like ours to extract the tracking ratios as we explained previously. The results are illustrated in the Figures (4.13-4.16).

Figure 4.13 presents the ratio of tracked vehicles by the GPA for both solutions. It can be seen that our tracking ratio is lower than that of Kang J. et al. This means that our proposal outperforms of Kang J. et al. as a lower ratio means a stronger privacy protection.

Figures 4.14, 4.15 and 4.16 illustrate the obtained tracking ratio by the syntactic, semantic and observation mapping attacks respectively for both solutions. The results obtained by our solution are better for all of the above attacks. Noting that both solutions gave low tracking ratio against the semantic and linkage mapping attacks under the simulated scenarios.

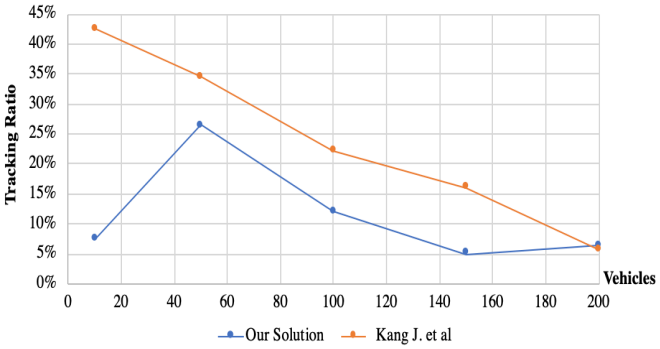



**Figure 4. 13:** Ratio of tracked vehicles for both solutions

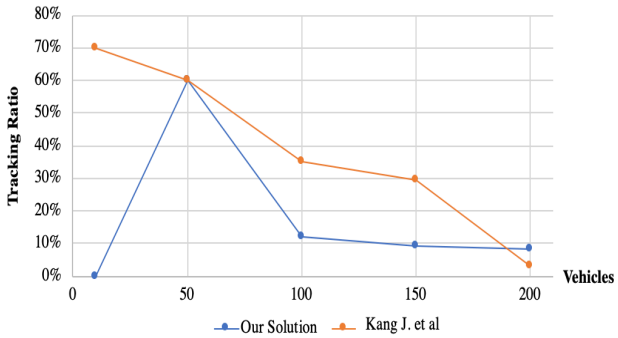



**Figure 4. 14:** Syntactic Attacker's ratio of tracked vehicles for both solutions

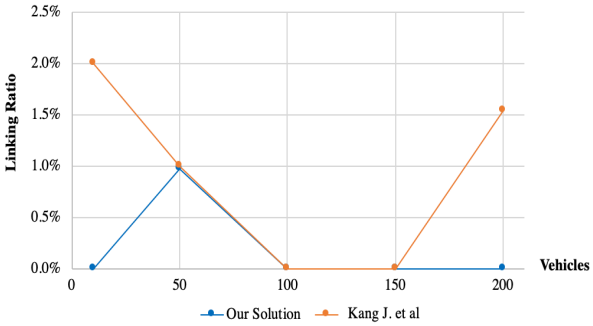



**Figure 4. 15:** Semantic Attacker - Ratio of linked identifiers

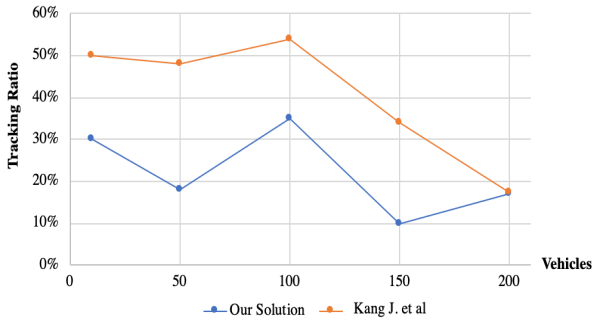



**Figure 4. 16:** Observation Mapping Attack - Ratio of tracked vehicle

Another comparison metric that may be considered as well is the number of identifiers change for each solution. Believing that the frequent identifier change alone does not necessarily improve the privacy protection. Contrariwise, it may cause service disruption and identifier over-consumption. Therefore, we designed our solution to enable the identifier change to happen only within a favorable context that would reduce the linkability which is to change within a cooperative crowd. Our argument is further proved by the obtained results where our solution gave a higher protection and a lower tracking ratio compared to Kang J. et al solution suggesting the frequent identifier update independently upon expiry. Although the number of identifiers' changes in their solution is about 3 times on average greater ours.

Additionally, our solution in comparison with Kang J. et al reduces the overhead of synchronization. In their solution, various messages are exchanged with the cloud manager (CM) to do the VMID change including the request of the change, getting the approval, continuous time synchronization, choosing a VMID, and informing the CM about it to record it. In the other hand, our solution relies on the use of flagged messages with two bits at maximum being used for synchronization purpose. We also optimized the VMID request, approval and record messages by the use of organized VMID lists. Thus, the vehicle only needs

to inform the CM about the change in a flagged message and the CM would be aware of the next VMID to be used.

**Table 4. 4:** Comparative Study between our Proposed Solution and Kang et al **[55]** Proposal.

| Privacy approaches | Non-Cooperative | Cooperative |
|---|---|---|
| | **Kang et al** | **Our Strategy** |
| **Principle** | -The pseudonyms and VMIDs are changed simultaneously.<br>- The vehicle synchronizes with the CM to do this change. The synchronization process implies the request to change, getting the approval, checking the time continuously, choosing VMID, and informing the cloud manager to record it. | The identifiers (pseudonym, VMID) are changed simultaneously using flag-based cooperative change strategy to ensure the unlinkability and anonymity. The cloud manager does not need to be included and synchronized with to do the change. Instead, it is just informed to record it. |
| **Advantage** | - The simultaneous change of identifiers protects against observation and mapping linkage attacks.<br>- prevents repetitive authentications. | - Preserves the identity and the location privacy.<br>- Prevents services interruption and repetitive authentication<br>- The use of Flags and organized list of identities (CE-IoV) optimizes the network over-head.<br>- Protects against observation mapping, linkage mapping, syntactic and semantic attacks, |
| **Drawback** | -The strategy used to change the pseudonym is not mentioned. However, judging by the given details and seeing that there was no cooperation between adjacent vehicles before or after the change. Thus, it does not protect against syntactic linking attack.<br>-The synchronization process causes over-head to the network. | - |

### 4.4.2. CSLPPS: Concerted Silence-based Location Scheme for Internet of Vehicles

In the previous section, we presented a cooperative based solution to preserve the location privacy in the cloud-enabled internet of vehicles. The solution gives optimistic results when tested through simulations against global passive attacker which is known to be a strong attacker model where the overall tracking ratio was between 5% and 27% approximately.

In this section, we aim to further reduce this tracking ratio by proposing a solution named Concerted Silence-based Location Privacy-Preserving Scheme for Internet of Vehicles (CSLPPS). CSLPPS is an amelioration of CLPPS proposed earlier. It relies on both the cooperation of the vehicles and their synchronized silence as the identifier change strategy used to simultaneously update the Pseudonym and VMID.

#### 4.4.2.1.The proposed solution

Similarly with the previous proposal, we use the same principal of flagged messages where the flags (bits) RDC, DC, CVD means respectively ready to change, do change and change VMID. The first two are customized un-used bits from the beacon's header and the last is from the service/connectivity message header. The CM is informed of the VMID change to record it through the reception of a flagged message with CVD set to 1.

We assume that upon the initial registration of the vehicle to the regional authority, the change strategy along with its parameters which are the threshold of cooperating vehicle $K$, and the silent period $T$ were flashed in it and that the cloud managers are aware of them.

When the vehicle pseudonym is about to expire, it senses its neighbor vehicles and informs them about the change by setting RDC to 1. Vehicles that have a similar state, i.e. desiring to change their pseudonyms, send beacons with RDC=1 as well. When a vehicle receives K beacons from K different neighbors willing to change their pseudonyms as well, it sets its DC in beacons to 1 and CVD in service/connectivity message to 1. The first is to inform the neighbor vehicles to enter silence then do the change. The second is to inform the CM to record the change and inform the service provider with the new VMID to be used. The vehicle ceases broadcasting although it may still receive messages. The CM cashes the pending queries and responses until the change is done (end of silence) and relays them to the vehicles using its new VMID. When the silent period ends, all vehicles that updated their identifiers may resume their activities using the newly changed identifiers. They can continue beaconing with their fresh pseudonyms and continue exchanging LBS messages via the new VMIDs without the need for re-authentication.

4.4.2.2.Simulation results

To evaluate CSLPPS and study its performance, we simulated it against a global passive attacker using the same tools, parameters, maps and scenarios as previously explained in the cooperative approach. The results were also compared to Kang J. et al solution.

We first give the simulation results. Then, we provide the comparative study details. Figure 4.17 presents the ratio of correctly tracked vehicles when changing their identifiers CSLPPS obtained by the GPA executing four linkability attacks. The attacks are the semantic, the syntactic, the observation mapping and the linkage mapping attacks. The ratio is calculated using the same methods explained in section 4.4.1.1.2. The overall ratio did not exceed 16% and it decreased to reach approximately 6% as the number of vehicles per scenario increased. In average, the tracking ratio was 10.1% which is lower than the results obtained by the previous proposal which was 11.5% in average and even lower than that of Kang J. et al which was 24.2% in average.

Figure 4.18 illustrates the ratio of tracked vehicles per each attack. The solution is almost robust to semantic and linking mapping attacks. The results for the other two attacks can be noticed to decrease as the number of vehicles increases. The tracking ratio for the syntactic attack was between 0-16% and for the observation attack was between 20-45%.

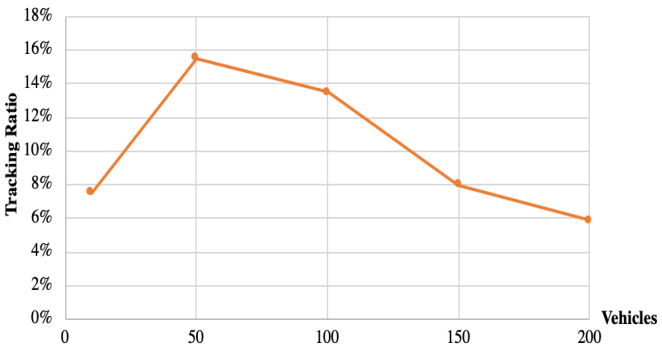



**Figure 4. 17:** Ratio of Tracked Vehicles

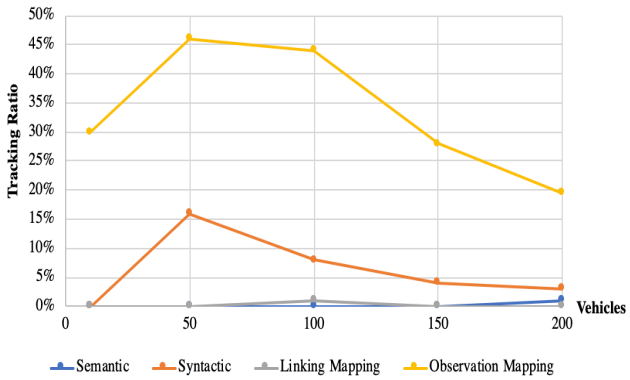



**Figure 4. 18:** Ratio of tracked vehicles per each attack

4.4.2.3.Comparative study and performance analysis

We compared our proposal to Kang J. et al. solution. The results obtained and illustrated in Figure 4.19 demonstrates that our solution is better translated by the lower tracking ratios for all scenarios. Figures 4.20-4.22 show the detailed tracking ratios by attack type for both solutions which are the syntactic, the semantic and the observation mapping attacks respectively.

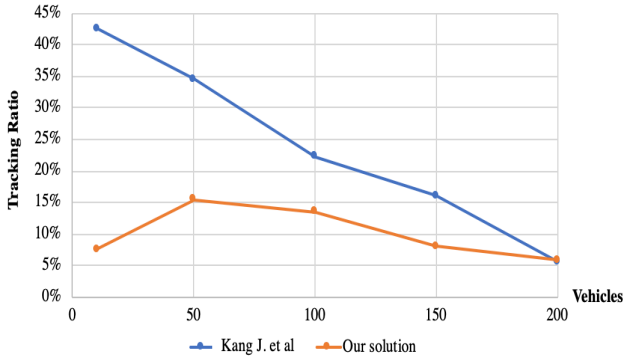



**Figure 4. 19:** Ratio of tracked vehicles

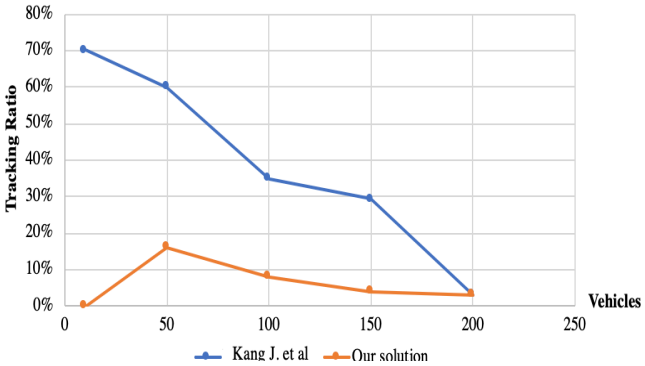



**Figure 4. 20:** Syntactic Attacker's ratio of tracked vehicles

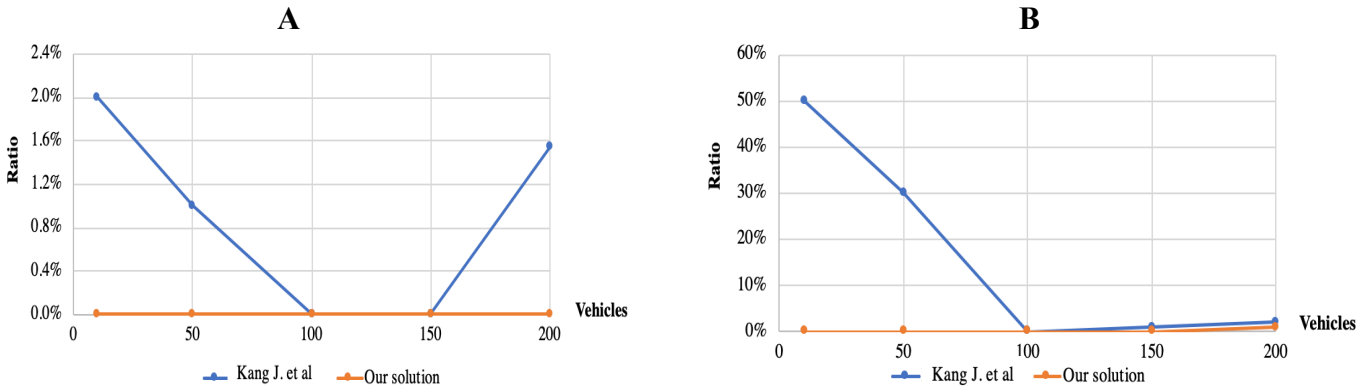



**Figure 4. 21:** Semantic Attacker (A. ratio of linked identifiers, B. ratio of tracked vehicles)

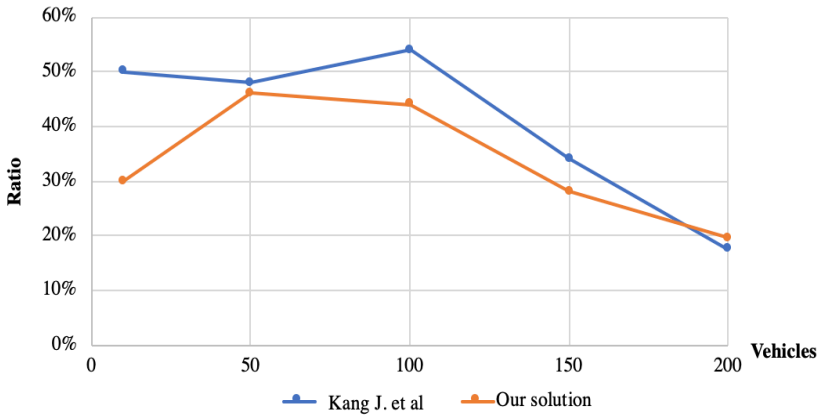



**Figure 4. 22:** Observation Mapping Attack - ratio of tracked vehicle

### 4.4.3. Obfuscation-based Location Privacy-Preserving Scheme in Cloud-enabled Internet of Vehicles

The above-explained proposals protect the location privacy by reducing the linkability of identifiers. Both relied on strengthening the update strategy. The first relies on the cooperation of the neighbors and the second additionally uses concerted silence. With the aim to further decrease the tracking ratio, we polish the proposal by adding obfuscation method to protect the location of the vehicles. So, in this final solution, we combine the cooperation, silence and obfuscation to develop a robust identifier strategy that showed the best results so far when tested through simulation against a GPA with an average tracking ratio of 7.15 %. The proposed solution and its analysis are explained in the coming sections.

#### 4.4.3.1. The proposition

The solution uses the same logic as the previous two proposals which is resumed in the use of flagged message to coordinate the change between the vehicles and inform the CM.

When the vehicle wants to update its identifiers, it sets the RDC flag (bit) in the beacon to 1 informing the neighbor vehicles of the change. Vehicles receiving this beacon and desiring to update their identifiers as well set their RDC flag to 1 and their locations to that of the sending vehicle. Upon the reception of $k$ beacons from $k$ distinct neighbors, the vehicle sets its DC to 1 and CVD to 1 in both its beacon and service/connectivity message and enters silence. Vehicles receiving the DC flagged beacons set their DC to 1 as well and enter silence. The CM records the change and informs the service provider about the next VMID to be used. It cashes the coming responses to the vehicle until after the change. Noting that vehicles not participating in the change may continue sending messages to the vehicles updating their pseudonyms. The vehicles cease broadcast when in silence but may continue receiving messages. Since the messages are broadcasted, even if the location is not accurate as long as it is within the vehicle's range it can reach it. Figure 4.23 illustrates the proposed identifier change strategy organized in 5 successive steps: Step 1 is of the vehicle announcing its identifier change. Step 2 is of the vehicles announcing their cooperation by unifying their positions to that of the sender and informing each other about their willingness to do the update. Step 3 is of the vehicle's confirming the change, informing the CM and entering silence. Step 4 illustrates that all vehicles cease their broadcast and are silent for the designated period. Step 5 the vehicles resume their activities with their newly updated identifiers.

As we saw in the previous sections, the frequent identifier change within unfavorable context does not enhance the privacy level. On the contrary, it over-consumes the identifiers uselessly. Therefore, in our solution, the identifiers are not changed unless the vehicle is within a cooperative crowd.

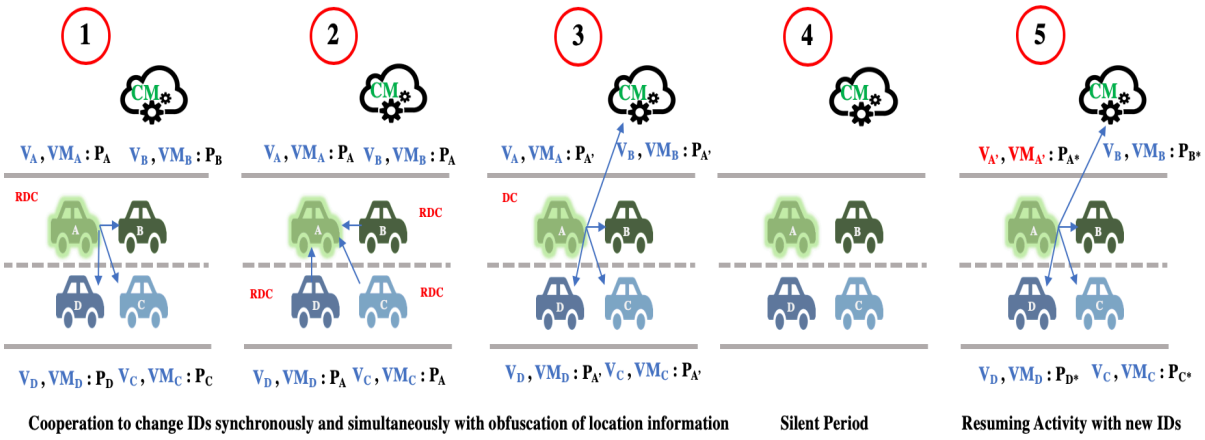



**Figure 4. 23:** Pseudonym and VMID change strategy

4.4.3.2.Study of feasibility using Game Theoretic Approach

To study the feasibility of the proposed solution we used the game theory. The change strategy is considered as the game G. Like in [84] we used a dynamic game (G) with complete and perfect information. G is defined as the triplet (P, S, U), where P, S is a set of players and strategies respectively and U are payoff functions. G has two stages:

- ***Stage one***: It is more or less related to the announcing vehicle actions and decisions. This initial stage is the announcement of the change and requesting cooperation of neighbors. To do so, the vehicle sets its RDC to one and waits to have ***k*** neighbors with RDC equals 1. Next, basing on the other vehicles (players) cooperation, it decides to do the change when it has at least ***k*** cooperative neighbors by setting its DC flag 1 and broadcasting the decision. The DC flag is set to 0 otherwise.
- ***Stage two***: is related to the neighbor vehicles cooperation where they decide upon the reception of RDC flagged message representing the cooperative change announcement. The decision is either to do the change or not of their pseudonyms and VMID.

Let P=$\{P_i\}_{i=1}^{n}$ consist of the set of players. Let P1 be the announcer in stage 1 and $P_2$, …, $P_n$ be the neighbors. $P_1$ has two moves: ready to do the change defined as R and not ready defined as NR. Thus, the set of strategies $S_1$ for $P_1$ is equal to {R, NR}. For the rest of the players $P_i$ ($i \in [2, n]$), $S_i$= {C, NC} where C means cooperative and NC means not cooperative to do the change.

The location privacy loss denoted by $d_i$ is calculated as follows:

1. $d_i$=0, if the vehicle is silent,
2. $d_i=\lambda(T_c-T_i)$, else, the vehicle is not silent.

where λ is the tracking power of the attacker,

$T_c$ is the current time and

$T_i$ is the time since the last pseudonym VMID successful change.

The cost of change ɣ is the sum of the cost of acquiring new pseudonym $\gamma_{psd}$ and VMID $\gamma_{vmid}$, the cost of this change affecting the routing of data $\gamma_{rt}$, and the cost of this change affecting it safety applications $\gamma_{sa}$.

$$\gamma = \gamma_{psd} + \gamma_{vmid} + \gamma_{rt} + \gamma_{sa}$$

The payoff function U= $\{U_i\}_{i=1}^{n}$ is defined for player $P_i$ as $U_i$, and is calculated using $d_i$ and ɣ as follows:

1- $U_i = -d_i$, if $P_i$ does not change its pseudonym and VMID.

2- $U_i$= -$d_i$- ɣ, if $P_i$ does the change within a non-cooperative crowd.

3- $U_i = \frac{-d_i}{k}$ - ɣ, if $P_i$ does the change within a cooperative crowd (k neighbors).

4- $U_i$= -ɣ, if $P_i$ does the change within a cooperative crowd (k neighbors) execute the obfuscation method and enters a silent period.

In our solution, we propose that the vehicle either do the change within a cooperative crowd after applying the silent period, or it does not. Thus, $U_i$= -ɣ or - $d_i$ respectively. For the rest of the demonstration, we set the threshold of cooperative neighbors *k* to 3.

We first consider four players $P_1$ the initiator and $P_2$, $P_3$, $P_4$ the neighbor vehicles. If $P_1$ chooses NR, the game is over for all the vehicles and none of them does the change. Thus, $U_1$=-$d_1$, $U_2$=-$d_2$, $U_3$=-$d_3$ and $U_4$=-$d_4$.

If P1 chooses R and P2, P3, P4 choose C then the change happens for all the four vehicles followed by a silent period, the payoff function would be then $U_1$= -ɣ, $U_2$= -ɣ, $U_3$= -ɣ and $U_4$= -ɣ. If P1 chooses R and one or more neighbor(s) P2, P3, P4 choose NC, the change does not happen and the payoff function would be: $U_1$=-$d_1$, $U_2$=-$d_2$, $U_3$=-$d_3$ and $U_4$=-$d_4$. The same conclusion can be drawn if the game had n players (n>k). This proves the feasibility of the solution.

4.4.3.3.The simulation

We simulated both the vehicles and the attacker model using NS2 on Mobisim generated mobility files. Table 4.5 resumes the simulation parameters. The attacker model is a passive global attacker that executes four linkability attacks which are the semantic, syntactic, observation mapping and linkage mapping attacks. The attacker spread his/her receivers as a grid to fully cover the map.

**Table 4. 5:** Simulation parameters

| | |
|---|---|
| Tools | NS 2, Mobisim |
| Mac layer | 802.11p |
| Simulation time | 300 seconds |
| Map | 700x700,<br>5 lanes Freeway |
| Pseudonym minimum lifetime | 30 seconds |
| Vehicle Range | 300 m |
| K | 3 |
| Silent period | 2 seconds |
| Number of attackers | 36 |
| Attacker coverage range | 500m |
| Scenario 1: number of vehicles | 50 |
| Scenario 2: number of vehicles | 100 |
| Scenario 3: number of vehicles | 200 |
| Scenario 4: number of vehicles | 250 |

Figure 4.24 presents the tracking ratio per attack for each scenario. It can be noticed that the solution is almost resilient to semantic, syntactic and linking mapping attacks. The tracking ratio using observation attack varied from 23% to 32%. The vehicle may be tracked during the lifetime of its identifier. However, as long as the identifier update is not linked, the long-term linkability is avoided and trajectory tracking is prevented and so does the identification through the profiling. This is ensured with our solution as in more than 90% of the cases, the vehicle is

perceived by the attacker as a new one after it updates its identifiers without its old and new identifiers being linked.

Figure 4.25 illustrates the overall tracking ratio obtained by the GPA the four linking attacks (semantic, syntactic, linkage and observation). The ratio was between 6% and 9%. It was decreasing as the number of vehicles per scenario increased. This is because the more vehicles are, the higher the chances of having close vehicles are, the more the chances of cooperation are and the larger the anonymity set size (cooperative crowd) is. Noting that larger anonymity set sizes increase the confusion of the attacker and decreases the accuracy of his/her tracks.

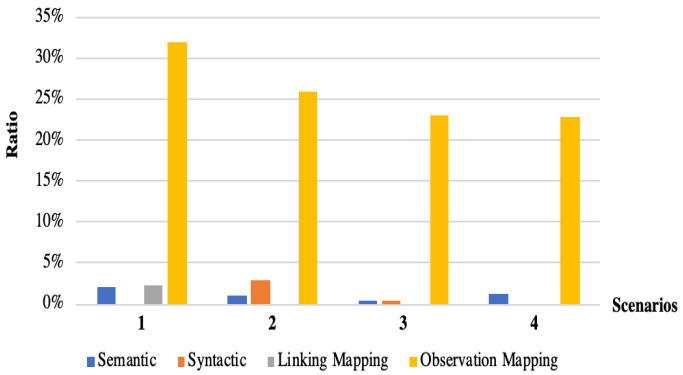



**Figure 4. 24:** Attacker's tracking ratio per each attack

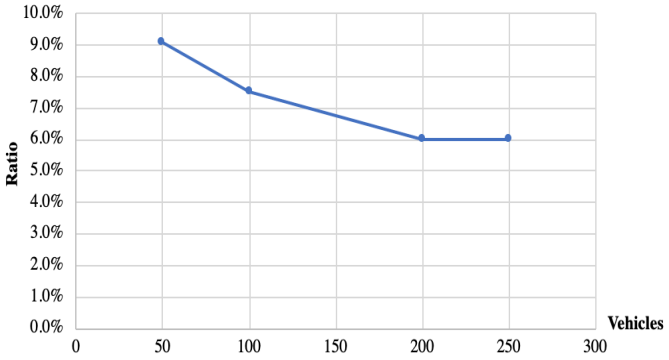



**Figure 4. 25:** Average ratio of tracked vehicles

We illustrated in Figures 4.24 and 4.25 the tracking ratio which did not exceed 10% in overall with almost full resiliency to semantic, syntactic and linking mapping attacks. For the observation linking attack, we used another metric known as the entropy or the quality of privacy defined in Chapter 2. The authors of [55] stated that the higher the H is, the higher the location privacy level is. When we applied this metric on our results, we obtained high entropy values. It means that the location privacy was preserved, and it was hard for the attacker to link the pseudonym changes.

### 4.4.3.4.Analytical model

Like we explained in Chapter 2, the location privacy is measured by various metrics. In this section, we use three metrics to analytically analyze the robustness of our proposed solution which are the average anonymity set size, the entropy and the normalized entropy.

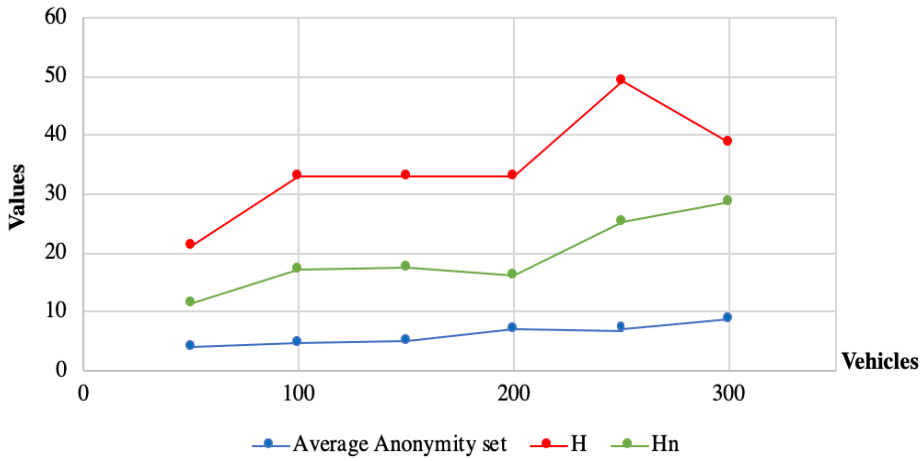



**Figure 4. 26:** Average Anonymity Set, Entropy and Normalized Entropy

Figure 4.26 illustrates the obtained results when applying these metrics on the simulation results. We notice that all of the average anonymity set size, entropy and normalized entropy increase as the number of the vehicles per scenario does. The anonymity set size augmentation with the increase of vehicles is related to the rise of possibilities of having crowded and dense roads during the identifier update phase. Moreover, the high values obtained for the entropy indicate the robustness of the solution in preserving the location privacy.

4.4.3.5.Comparative study

Just like the two previous proposals, we conducted a comparative study between our solution and Kang J. *et al.* Both solutions were simulated under the same settings defined in table 4.5, against the same attacker model, using the same scenarios.

Figure 4.27 illustrates the overall tracking ratio for both solutions. Our solution gave lower ratios reducing by half approximately the tracking ratio of Kang J. *et al.*

Figures 4.28-4.30 present tracking ratios for both solutions by attack which are the semantic, the syntactic and the observation mapping respectively. We can see that our solution is almost resilient to both the semantic and syntactic attacks outperforming the solution of Kang J. el al. which gave tracking ratio between 10-25% for the semantic attack and 2-16% for the syntactic attack. Both solutions were almost resilient to linkage mapping attack. Our solution out-bested that of Kang J. et al. with lower tracking ratio by the observation mapping attack.

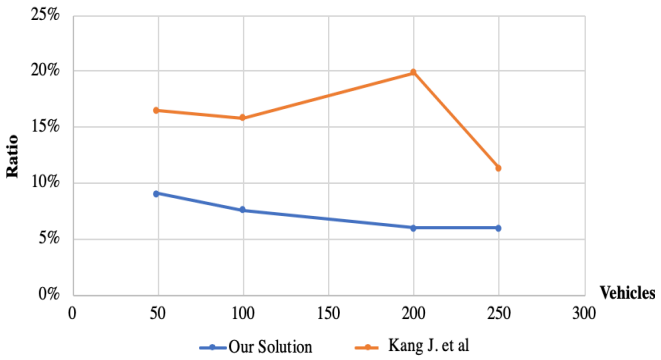



**Figure 4. 27:** Average ratio of tracked vehicles

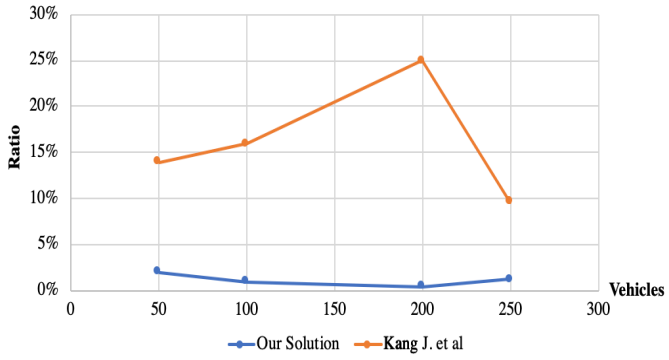



**Figure 4. 28:** Ratio of tracked vehicles-Semantic Attack

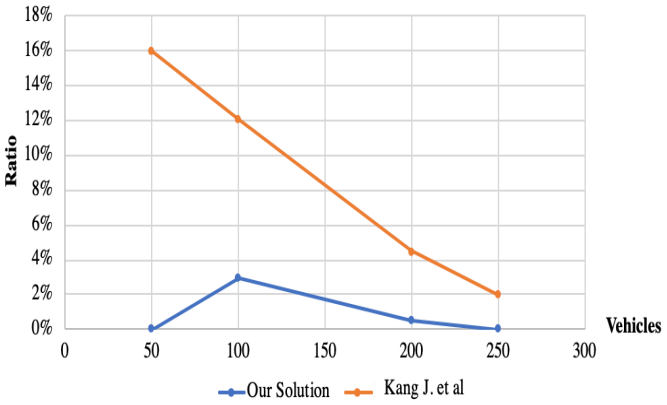



**Figure 4. 29:** Ratio of tracked vehicles -Syntactic Attack

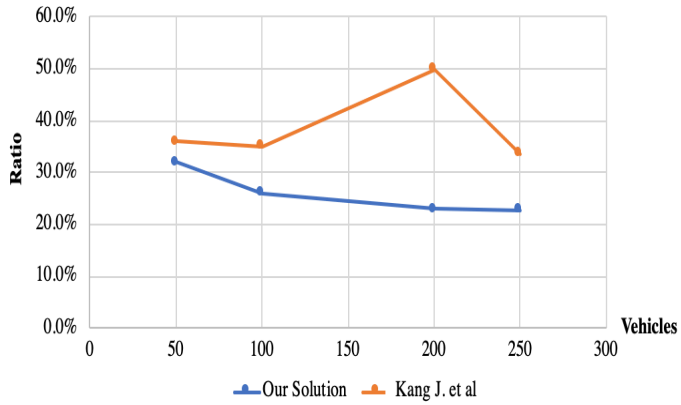



**Figure 4. 30:** Ratio of tracked vehicles-Observation Mapping

## 4.5. Conclusion

This chapter illustrated two new obfuscation pseudonym-based change strategies that reduce the linkability and tracking to preserve the location privacy of the VANET users from tracking.

The first solution uses a camouflage technique by creating a virtual crowd to confuse the attacker and reduce the linkability. The solution proved both analytically and through simulations to have a good protection level and it reduced the tracking ratio from 100% (without the use of a change strategy) within low-density roads to 40% only. It gave an average tracking ratio of 27% which is good as it means that the privacy is protected with over 73%.

To further reduce this tracking ratio, we proposed another obfuscation solution to delude the attacker and reduce his/her accuracy. This solution is neighbor-aware, and pseudonyms slotted. This means that if the vehicle is within a crowd, they all change at the same time as the pseudonyms have the same end validity time. If the vehicle is within less dense roads, it deludes the attacker prior to the change with beacons indicating that it is stopping. Then when it does the update, it continues broadcasting its accurate position and speed. Since the attacker relies on the accurate beacon content to track the vehicle and predict its locations, erroneous and inaccurate beacons lead to fuzzy prediction and tracking failure. Indeed, the solution gave an average level of protection of 89.6% with an average tracking ratio of 10.4% varying from 6.3% to 17% at worst. We remind the readers that neighbor vehicles may rely on their camera, lidars and radars to make up for the one-hop neighbor vehicle inaccurate beacons. Also, that the vehicle may halt the obfuscation technique to report emergency events if they occur, as we maintain the highest priority to safety applications.

The chapter also included three location privacy-preserving solutions that prevent linkability and tracking for IoV users. The solutions achieved a high level of privacy protection and each amelioration increased the protection level starting from 70% to 90%. These ratios are considered in the worst case against the strongest attacker covering the road completely. The proposals rely on the use of temporal identifiers in both the LBS queries and beaconing known as the VMID and pseudonyms respectively. Both of which are changed simultaneously. In the first proposal, the change happens within a cooperative crowd. The privacy was preserved with more than 70%. In the second proposal, we strengthened the first scheme by using silence (concerted silence) to preserve the privacy with over 84%. In the third proposal, we further enhanced the solution by adding obfuscation measure to thwart the linkability to achieve a protection level that exceeded 90%.

# CHAPTER 5

# BLOCKCHAIN-BASED PRIVACY AWARE PSEUDONYM MANAGEMENT FRAMEWORK FOR VEHICULAR NETWORK

## 5.1. Introduction

In the previous chapters, we concentrated on the privacy issue in vehicular networks where the security system is centered around the public key infrastructure. The central Vehicular Public Key Infrastructure (VPKI) has a Certifying Authority (CA) to certify the long-term and short-term public keys (pseudonyms). The VPKI system is strong and powerful both in terms of security and privacy level it provides. Its strength is originated from it being centralized and private. Only the CA may register the vehicles and their owners and only it may issue the certificates. When the vehicle uses a certified pseudonym, its activities are traced by the issuing CA. In case of a misbehavior, it may be revoked and held accountable (conditional privacy). In other words, the CA has a complete control over the user's registration, key generation/certifying, update and revocation process. Noting that, the centralization and confidentiality of the VPKI may be considered as its weaknesses which are common with all centralized systems. These vulnerabilities expose it to targeted attacks leading to it being a single point of failure.

Before explaining our potential replacement to the VPKI that resolves the single point of failure issue. We first brief the role of pseudonyms in vehicular networks and how the VPKI handle them. This helps to extract the main traits that a potential replacement solution must have and the tasks it must handle. Like we explained in Chapter 2, the pseudonyms are either utilized to encrypt data/service messages or to sign beacons which are sent on periodical basis to exchange state data. The signature in the beacon serves to authenticate the message and to check its integrity before accepting it [152]. The message authentication prevents the injection of random bogus data from an outsider attacker and, it ensures that the internal attacker is held accountable, cannot deny his/her behavior and is revoked from the network to limit his/her influence. The revocation mechanism is executed by the CA after it receives reports from vehicles about a detected misbehavior. The revoked pseudonyms are then added to Certificate Revocation List (CRL) that is timestamped and signed by the CA and distributed to the vehicles to alert them and prohibit them from interacting or trusting the revoked node. One more unique trait to the VPKI is that the certificates of the pseudonyms are anonymous to preserve the identity of the vehicle users.

In a nutshell, a potential replacement framework of the centralized VPKI ought to ensure these requirements:

- ***The security***: the keys/certificates delivery are through secure communication channels. The integrity, authenticity and non-repudiation are to be ensured. The keys and security algorithms are to be encrypted, to be confidential and to be stored securely against intrusions.
- ***The privacy***: the certificates are anonymous and identity-less to protect the privacy. They are signed by the certifying authority key and are traced back to this issuing authority. The main two traits to respect are the anonymity and the unlinkability. The pseudonyms of the same user should not be linked to each other nor to his/her identity.
- ***The revocation***: which has to be fast and efficient is essential to maintain the correct functionality of the network. In VPKI, the revocation is ensured by the CA that would revoke all the pseudonyms of a misbehaving user and may even disclose his/her identity to the juridical system if it is needed.

In this chapter, we design a secure decentralized pseudonym management framework as a potential replacement of the VPKI. The solution resolves the single point of failure issue, satisfies the above requirements and provide the same role and even a higher security level. The framework utilizes the public and distributed blockchain technology. It is a blockchain of blockchains formed by the pseudonym blockchain maintained by the vehicles and a revocation blockchain managed by roadside units. The framework takes advantage of the vehicular network components which are the vehicles and RSU dispersed on roads to create secure distributed public replacements of VPKI that preserves the privacy and ensures the revocation. Thus, it reduces the cost of deploying and maintaining a certifying authority and its subsidiaries.

This chapter is organized as follows:

In part 2, the fundamental perquisites such as the public key infrastructure (PKI), vehicular PKI, blockchain technology and the blockchain of blockchains are explained.

Part 3 resumes the related works.

Part 4 clarifies the key needed security concepts related to our proposed solution.

Part 5 explains the proposed framework.

Part 6 analyses the security and privacy properties of the framework.

Part 7 summaries a comparative study between the vehicular PKI and our proposed framework.

Part 8 concludes the work.

## 5.2. Background

This section explains the key background related concepts that facilitate the understanding of the proposed solution which are:

### 5.2.1 Public Key Infrastructure (PKI)

The public key infrastructure is also referred to as the two-key cryptography systems where the key used in the encryption is different from the one used in the decryption. Although these pair of keys are mathematically related, it is difficult to derive the private key from the public key. The conventional PKI by digitally certifying the public keys resolves the impersonation issue which occurs when a user pretends to be the owner of a public key that is not his/hers. A digital certificate not only maps the public key to its owner but also timestamp it and specify its lifetime. It may be updated by prolonging its lifetime and revoked if misused. In what follows, we explain the key certifying process, the certificate verification and revocation processes. Also, the private key recovery process.

- ***The certifying process***

The pair of public and private keys are generated by the user and the public key is sent to the CA to be certified. The CA generates a certificate containing the user's name, the public key and a validity period. The certificate is signed using the CA's private key.

The certificate X.509 contains the following fields: version, serial number, signature algorithm identifier, issuer distinguished name, validity interval, subject distinguished name, subject public key information, issuer unique identifier, subject unique identifier, extensions, signature.

- ***The certificate verification process***

The verification of a certified public key starts by checking the CA's public key. Then, using this key to extract the hash value from the digital signature. This value is compared with the calculated one to ensure the received certificate integrity. Finally, the validity of the public key is verified which means that it is not expired yet and not revoked. The public key is accepted once all of the above conditions are satisfied, i.e.: It is valid, non-revoked and integral.

- ***The certificate revocation***

The certificate is revoked if the private key is disclosed, if its holder is expelled or if s/he misuses it for its non-intended aims. The CA saves the revoked certificates in a list called the Certificate Revocation List (CRL). The CRL records the serial number of the certificate, the revocation date and reason. The list is timestamped and signed by the CA.

- ***The recovery of the private key***

The private key is fundamental for both the decryption and the signing process. Therefore, it is necessary to have a back-up copy that can be used if the original key is lost or ruined. The user may choose to either make local back-ups to preserve his/her privacy. Or, to save a copy at the CA which may risk the privacy. If the user chooses to store a copy at a third-party company, not only his/her privacy may be risked but also the confidentiality of his/her data may be violated if the private key is used to expose the encrypted content of messages because the key owner becomes the data owner. The private key may also be split into parts where each is saved separately on different servers, entities or cards to prevent the risk of exposing the data confidentiality. When needed, the key is reconstructed by assembling its composing parts together [153] [154].

### 5.2.2 Vehicular PKI

The VPKI has a Root Certifying Authority (RCA), a Pseudonym Certificate Authority (PCA), a Long-Term Certificate Authority (LTCA) and a Pseudonym Resolution Authority (PRA). Each vehicle obtains upon registration a long-term certified pair of public and private keys and a set of pseudonyms also known as short-term pairs of public and private keys. The RCA signs the other authorities (PCA, LTCA and PRA) certificates. The Long-term certificates are used to request pseudonyms from PCA are issued by the LTCA. The identity resolving of the pseudonym revocation is handled by the PRA. The VPKI guarantees the security properties ensured by the conventional PKI which are the authenticity, non-repudiation and integrity. Besides ensuring the identity privacy as the pseudonym certificate does not include the owner's identity. It includes only the serial number, the short-termed public key, the validity period and the PCA signature. In the VPKI, the revocation of a node is caused by its cyber misbehavior on road. The PRA receives the misbehavior reports and includes the misbehaving node's pseudonyms in the revocation list CRL which is forwarded to the vehicles to alert them about this malicious node. The collaboration of RCA, PCA and LTCA is needed to resolve the identity of the misbehaving user [155].

### 5.2.3 Blockchain technology

The interest about the blockchain (BC) technology has increased ever after the introduction of Bitcoins in Nakamoto Satoshi paper a decade ago. Recently, the attention of various researchers and professionals is directed towards developing blockchain based distributed applications. They are trying to shift application orientation from being centralized suffering from a single point of failure problem to being distributed and decentralized build over the blockchains. The blockchain or the public ledgers are distributed immutable databases of transactions about physical or digital assets where each transaction is validated by the network peer's consensus [156].

The blockchain architecture is organized on six layers [157] to facilitates its understanding: the application, data ledger, consensus, P2P exchange, network and hardware layer. In the following we briefly explain each layer:

- The application layer: crypto-currencies such as Bitcoin [158], Ethereum [159] and Monero [160] are famous but not the exclusive type of blockchain applications. In fact, this layer defines the blockchain role. In this chapter, our defined application is a pseudonym management framework that may replace the VPKI.
- The *data ledger layer:* this layer identifies the transactions, blocks and the blockchain structure which depends on the nature of the recorded assets.
- The *consensus layer*: the transaction/block validation procedures and consensus protocol are specified in this layer depending on the blockchain type being permissioned or permission-less.
- The *P2P exchange layer*: the blockchain is formed by connected peers forming the peer-2-peer network competing on the transaction's validation and the block's creation. Also, they interchange the validated blocks to keep up to date blockchain.
- The *network layer*: the p2p networks used by the blockchain is overlaid over the internet where the users download and register to the blockchain.
- The *hardware layer*: this layer is related to the servers and machines utilized by the blockchain peers for the blocks and the transactions' validation.

- ***The transactions content***

A transaction (Tx) archives physical or a digital asset ownership change. Its content depends on the blockchain implementations and purpose. In general, it has: the sender's address, sender's public key, a digital signature, transaction inputs and outputs. The input of the transaction lists the assets to be transferred and its source. The output of the transaction defines the amount of transferred asset, the identifier of the new owner(s) and the spending conditions of this asset or value. The identifier of the sender/receiver is either a public key or its cryptographic hash known as the one-time address.

The transaction validation depends on the implemented protocols requirements, such as ensuring that the owner possesses enough assets, that s/he satisfies its spending conditions and that no double spending occurring simultaneously, etc. The transaction authenticity proves that the sender of an asset has owned it. It is ensured by signing the transaction's input by the sender's private key. To check the authenticity, the blockchain peers use the sender's public

key found in the asset source transaction's output to check the hash [161]. Figure 5.1 illustrates the transactions' structure.

- ***The block structure***

When the user creates a transaction, it is in a pending state until it is validated by the blockchain peers. The validation of a transaction is affirmed by creating and successfully publishing a block containing it. The block has two parts, the header known as the metadata and the data which are the valid transactions [161] as illustrated in Figure 5.2.

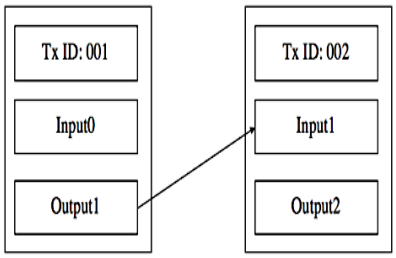



**Figure 5. 1:** Transactions illustration

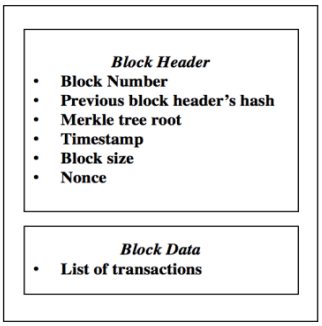



**Figure 5. 2:** Bloc structure

- ***Chaining the blocks***

We previously mentioned that the transaction validation is confirmed by being published in a block. The blocks are not orphan and not independent. For the block to be accepted, it must be chained correctly to the blockchain. To do so, the nodes compete to resolve a challenge. The first peer to resolve it, adds the block. The chaining is by the hashes usage like illustrated in Figure 5.3 where each block contains a hash of the previous one. This prevents the alteration and injection of blocks [161].

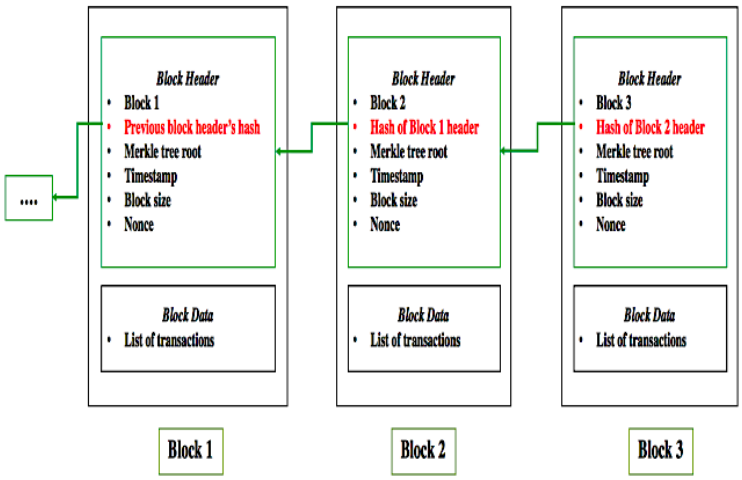



**Figure 5. 3:** Chains of blocks (blockchain)

- ***Consensus models***

The consensus process differs basing on the blockchain type and implementation. In the permissioned blockchains, only permitted nodes create and publish valid blocks. Contrarily to

the permission-less blockchains where all peers are able to create blocks following a consensus model. In the following, few existing consensus models are briefed [161]:

- **Proof of Work (PoW)**

The addition of a block is done by the node that first resolves the puzzle such as the one that finds a hash of block header that is less than the threshold value. I.e.: looking for a nonce to add to the block header that by hashing it, we get the desired threshold.

- **Proof of Stake (PoS)**

Unlike PoW, PoS does not need intensive calculations. Instead, it relies on the invested stakes in the blockchain. Assuming that users who have more stakes are less likely to abuse the blockchain. Therefore, the user that has the highest stakes is likely to be the one to add the next block. Instead of being rewarded for the block creation like in PoW, the user receives transaction insertion fees.

- **Round robin**

This method is used in permissioned blockchains where each node waits for its turn to come for it to add a block to the blockchain. Thus, all permitted nodes eventually participate in the block's creation.

- **Proof of authority**

The proof of authority or identity is another model that is used in permissioned blockchains where only the blockchain authorized nodes are permitted to create blocks.

- **Proof of elapsed time**

In this model, nodes are assigned with random wait timers within which they stay idle. The node whose timer expires first creates and publishes the block. This process is repeated for every block to be published.

- ***Blockchain Types***

We mentioned earlier that there are two types of blockchains which are the permissioned and permission-less blockchains. In here, we explain each of these types.

In the public also known as the permission-less blockchain, all nodes have writing access and they compete by resolving the PoW to create and publish blocks.

On the other hand, the permissioned also known as private blockchain only a set of specific nodes have the writing access to create blocks and the other majority of peers have read access only. Corporations and organizations prefer this type of blockchain technology and customize it to serve their needs. Noting that sometimes the blockchain is public and permissioned (consortium) and other times it is completely private [162] [163].

### 5.2.4 Blockchain of Blockchains

This concept was first introduced in OneLedger project [164], it is a blockchain of various blockchains either of permissioned, permission-less or consortium types. The composing blockchain may not be implemented using the same technology but they are interoperable and compatible to serve the same aim.

## 5.3. Related works

This section resumes the state-of-art solutions for the blockchain-based PKIs:

### 5.3.1 Blockchain-based PKI

The PKI is the secure data exchange backbone over the internet. However, it is vulnerable to the single point of failure issue where the single point is the CA. It may be the favorite target of attackers and hackers aiming to violate the end user's security. Authors of [165] implemented a blockchain-based PKI management framework that is immutable, public and traceable. The Ethereum-based framework offers an efficient certificate revocation without the use of Certificate Revocations Lists (CRLs). It is also resilient to the man-in-the-middle attack or session hijacking because the blockchain is public, timely updated and distributed. Moreover, it eliminates the single point of failure issue of PKI. The certificates are confirmed through the chain of trust validation from leaf to root CA. The revocation is done by shifting the certificate reference from the CA's smart contract white list to its blacklist.

### 5.3.2 Privacy-aware blockchain-based PKI

The previous framework does not preserve the privacy as it focuses on the traceability feature. However, the author of [166] introduced a privacy-aware blockchain-based PKI. In which, only if a misbehavior occurs requiring the node revocation and the consensus of the user under the request of authorities is obtained that the user identity may be backtracked and exposed. Otherwise, it is protected. In other words, the privacy level is either controlled by the users or the application type using this technology. The generated keys are valid if they can be linked back to the previously used key. This keys linkability is done implicitly and the author claimed that the keys linkability test returns a logical value and not the public key itself. Thus, unless a misbehavior occurs or the secret keys are lost, this linkability cannot threaten the privacy. However, as the blockchain is public, a malicious node aiming to link the keys to resolve the user's identity can do this test differently. Therefore, this framework does not ensure the forward privacy.

### 5.3.3 Blockchain-based vehicular PKI

The authors of [167] proposed a blockchain-based PKI for vehicular networks to make the pseudonyms authentication and revocation efficient and fast. They choose the private blockchain type which they proposed to be maintained and accessed by the CA, the revocation authority and the RSU. While they prevented the vehicles or the OBU from having access to the blockchain. Noting that the RSUs have reading rights only. In their framework, the vehicle is registered to the CA which issues its pseudonyms that are stored as blockchain transactions. Since the vehicles have no access to the blockchain, the pseudonym verification and authentication are done via the RSU. The vehicle sends the index of the pseudonym transaction in the blockchain to the RSU that checks its existence in the blockchain and challenges the vehicle to prove its ownership of this pseudonym for the authentication to be successful.

The vehicle is also reported to the RSU if it misbehaves. The RSU then forwards the report to the RA which issues the vehicle a revocation transaction. This solution preserves the privacy and guarantees the pseudonym authentication, non-repudiation and integrity. However, the described framework is more like a central database with multiple up-to-date back-ups than like a blockchain. Yet, it does reduce the certifying authority dependability and eliminate the certificate revocation list usage.

## 5.4. Key concepts

In this section, we explain the key concepts behind the privacy preservation in our proposed blockchain which ensure both the anonymity and the unlinkability. These concepts are the ring signature which we used to hide the identity of the signer, and the one-time address which we used to ensure the unlinkability between the pseudonyms and their generator.

### 5.4.1 Ring signature

The ring signature is used in Monero [160] to protect the sender's privacy. Also, to prevent the linkability and the traceability. The users although are certain about the transactions unforgeability, they are unable to identify their signers. The ring signature signing, and verification are given below in algorithms 5.1 and 5.2 respectively:

***Notation*** [160]

**G**: The generator of points in the elliptic curve (EC). **l**: The order of the EC
$\mathbf{K_i}$: The public key of *i*. $\mathbf{k_i}$: The private key of *i*.
The $\mathcal{R}$ in $\alpha_i \in_{\mathcal{R}} \mathbb{Z}_l$ means that $\alpha_i$is randomly selected from {0, 1, 2, … , *l*-1}.
$\mathbb{Z}_l$: is all integers (mod l).
**m:** is the message and in our case the pseudonym in the transaction's input.
***R*:** a set of public keys.
$\mathcal{H}_n$: a hash function mapping to integers from 1 to *l*.

***Assumptions*** [160]

$R = \{K_i, j_i\}\ for\ i \in \{1,2,\dots,n\}\ and\ j_i \in \{1,2,\dots,m_i\}$
$\{K_i, j_i\}$ is like a bookshelf of public keys with n shelves and on each shelf are $m_i$ public keys.
$\pi_i$ is the index of the public key on the shelf π.

**Algorithm 5. 1:** Ring Signature **[160]**

1. For each shelf $i \in \{1,\dots,n\} \pi_i \neq m_i$
   a. Generate a random value $\alpha_i \in_{\mathcal{R}} \mathbb{Z}_l$
   b. Seed the shelf's loop: set $c_{i,\pi_i+1} = \mathcal{H}_n(\mathfrak{m}, [\alpha_i G])$
   c. Build the first half of the loop from seed: if $\pi_i + 1 \neq m_i$ and for $j_i = \pi_i + 1, \dots, m_i - 1$ generate random numbers $r_{i,j_i} \in_{\mathcal{R}} \mathbb{Z}_l$and compute $c_{i,j_i+1} = \mathcal{H}_n(\mathfrak{m}, [r_{i,j_i} G + c_{i,j_i} K_{i,j_i}])$
2. For $i \in \{1,\dots,n\}$ generate random numbers $r_{i,m_i} \in_{\mathcal{R}} \mathbb{Z}_l$. Take all $r_{i,m_i}, c_{i,m_i}$ , and $K_{i,m_i}$ and combine them in the connector

$$c_1 = \mathcal{H}_n(\mathfrak{m}, [r_{1,m_1} G + c_{1,m_1} K_{1,m_1}], \dots, [r_{n,m_n} G + c_{n,m_n} K_{n,m_n}])$$

If $\pi_i = m_i$, instead of $r_{i,m_i}$, generate $\alpha_i$ and put in $\alpha_i G$ in $c_1$

3. For each shelf For $i \in \{1,\dots,n\}$:
   a. Build a second half loop from connector:
   if $\pi_i \neq 1$, for $j_i = 1, \dots, \pi_i - 1$ generate random numbers $r_{i,j_i} \in_{\mathcal{R}} \mathbb{Z}_l$ and compute $c_{i,j_i+1} = \mathcal{H}_n(\mathfrak{m}, [r_{i,j_i} G + c_{i,j_i} K_{i,j_i}])$, noting that $c_{i,1}$ is interpreted as $c_1$.
   b. Tie loop end together: set $r_{i,\pi_i}$ such that $\alpha_i = r_{i,\pi_i} + c_{i,\pi_i} k_{i,\pi_i}$
   The signature:

$$\sigma = (c1, r_{1,1}, \dots, r_{1,m_1}, r_{2,1}, \dots, r_{2,m_2}, \dots, r_{n,m_n})$$

This signature is sent along with *R* the set of public keys used in the signing process and the signed message $\mathfrak{m}$.

**Algorithm 5. 2:** Ring Signature Verification **[160]**

Given $\mathfrak{m}$, $R$and $\sigma$, the verification if performed as follows:

1. For $i \in \{1, \dots, n\}$ and $j_i = 1, \dots, m_i$ build each loop:

$$L'_{i,j_i} = r_{i,j_i}G + c'_{i,j_i}K_{i,j_i}$$
$$c'_{i,j_i+1} = \mathcal{H}_n(\mathfrak{m}, L'_{i,j_i})$$

Noting that $c'_1$is interpreted as $c_1$, and that it is unnecessary to compute $c'_{i,m_i+1}$.

2. Compute the connector:

$$c'_1 = \mathcal{H}_n\left(\mathfrak{m}, L'_{1,m_1}, \dots., L'_{n,m_n}\right).$$

If $c'_1 = c_1$ then the signature is valid.

### 5.4.2 One-time address

To preserve the transaction receiver's output privacy, a one-time address is generated by the sender from the receiver's public key. It is put as his/her identifier/address in the transaction's output to avoid tracing the asset transaction history in the blockchain. Thus, only the intended receiver may read this output. In our framework, the vehicle self-generates its own pseudonyms. Therefore, the transaction's output contains the vehicle's one-time address. We used the one-time address concept as it avoids traceability of transactions, linkability of pseudonyms and preserves the privacy which is critical in the vehicular networks. It is calculated from the vehicle's public key, the hash of the transaction and the vehicle secret key. Let $H$ be the hash function that has as parameters: $K_v$ the vehicle's public key, $S_v$ the vehicle's secret key and $h_{tx}$ the transaction hash.

***The one-time address = H ($K_v$, $S_v$, $h_{tx}$)***

## 5.5. Proposed solution

In this section, we explain our proposed distributed privacy-aware blockchain-based VPKI.

### 5.5.1 General description

The proposed framework is a blockchain of two blockchains. The generated pseudonyms are saved in a permission-less public blockchain, and the revoked pseudonyms are recorded in a permissioned public blockchain. The first blockchain is accessed by the registered vehicles. While the second is maintained by the RSUs which have writing access rights and accessed by the vehicles with reading rights only. Figure 5.4 illustrated, in general, the proposed framework by demonstrating its main three functionalities. The first (A) is the vehicle registration phase. The second (B) is the pseudonym generation and addition to the $BC_{cert}$ blockchain. The third (C) is the pseudonyms revocation and addition to the $BC_{rev}$ blockchain.

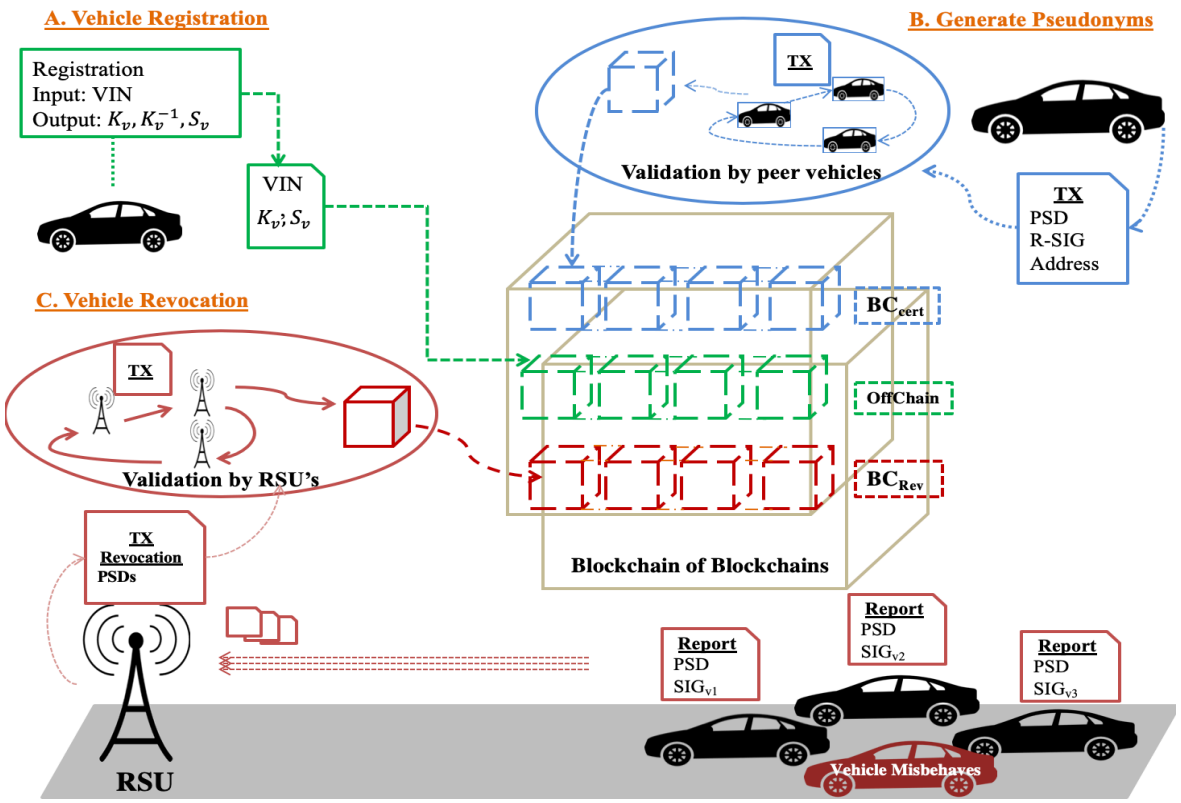



**Figure 5. 4:** Blockchain-based Pseudonym management for vehicular networks

A vehicle is initially registered by its owner to the blockchain system upon its purchase. Once registered, each vehicle is preloaded with our pseudonym management framework. This allows it to generate its own pseudonyms. The vehicle creates a transaction for each generated pseudonym and publishes it to be added to the blockchain. The transactions are assembled in blocks. They are added to the blockchain in a distributed manner by the vehicles basing on a defined consensus model without the need for the central certifying authority or a point of trust to interfere. Our framework is privacy-aware. Thus, the public blockchain does not disclose the user's or the vehicles identities. Yet, the vehicles are still able to check the pseudonym validity without linking it to its owner or to the previously generated pseudonyms. In other word, it ensures both the anonymity and the unlinkability. Noting that, the blockchain publishes only the public key and not the private key. Being unlinkable, anonymous and untraceable are the vehicular networks essential requirements. However, maintaining the security and functionality of the network, as well as the non-repudiation and the misbehaving nodes revocation are other crucial requirements to satisfy. In our framework, to fulfil these properties, the unlinkable ring signature is used to sign the transactions and the one-time address is used to hide the vehicle's identifier both of which were explained in section 5.4, while the revocation process is handled by the RSUs.

### 5.5.2 Registration to the blockchain

The vehicle registration in the blockchain is done upon its purchase using the unique Vehicle Identification Number (VIN). Once registered, the vehicle obtains a secret key $S_v$, and a pair of public and private keys $(K_v, k_v)$. The private key is fundamental, and it should be backed up. It is used for the ring-signatures and its owner may track all its related transactions and the

generated pseudonyms. The secret key is not published in the blockchain. It is stored along with the public key in an offline chain that can only be accessed by the RSUs. It is solely used in the creation of the one-time address and not used neither in the signature nor in encryption.

### 5.5.3 Certifying process

There is no certifying process in the traditional meaning. However, the fact that a pseudonym is inserted correctly in the blockchain and cannot be found in the revoked blockchain proves it to be valid. Thus, achieving the same aims ensured by the certificate without explicitly using it. When the vehicle generates its own pseudonyms, it inserts each one in a transaction containing a validity time. To keep the system distributed and eliminate the need for a central certifying authority, each vehicle signs its own transaction without exposing its privacy using ring signature (explained in section 5.4.1) that conceals the signer within a set of potential signers and attach all of the signers' public keys with the transaction. The transaction's receiver checks the signature validity without identifying its signer. The used public keys are arbitrarily chosen from the blockchain's available public keys. Moreover, the transaction's output must include the pseudonym owner. Yet, it should be done while preserving his/her identity privacy and avoiding the traceability of his/her generated pseudonyms for which we used the one-time addresses (explained in section 5.4.2).

### 5.5.4 Revocation process

The framework is distributed and does not require a central point of verification or revocation. The vehicles detect and report misbehaving nodes to the RSUs. The RSUs maintaining the revocation blockchain verify the received reports and revoke the pseudonym of the misbehaving vehicle. They also use the one-time address and ring-signature list of signers to identify the public key of the misbehaving node. They recompute the one-time address using the secret keys saved in the offline chain for the all the signers' public keys until they find the public key from which the one-time address was extracted. Then, this key is revoked and so are the other valid unused pseudonyms generated by it. The RSUs insert the revoked pseudonyms and the vehicle's public key in a revocation transaction. They sign this transaction and add it to the public blockchain.

### 5.5.5 Transaction structure and validation

We previously mentioned two transactions types which are the valid pseudonym transaction and the pseudonym revocation transaction. Each is saved in its corresponding blockchain. In what follows, we explain the structure and validation process for each type separately:

- ***The pseudonym transaction***

A pseudonym transaction is created for each pseudonym generated by the vehicle. It is self-signed using ring signature algorithm and self-addressed with one-time usage address. Figure 5.5 illustrates a pseudonym transaction's structure. Algorithm 5.3 explains the certifying process.

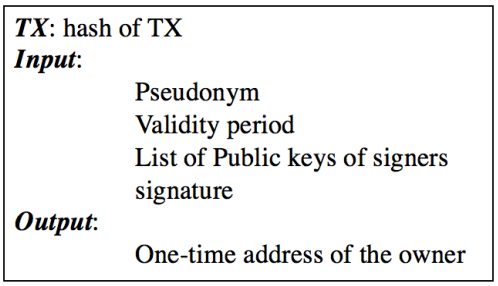



**Figure 5. 5:** Certifying transaction structure.

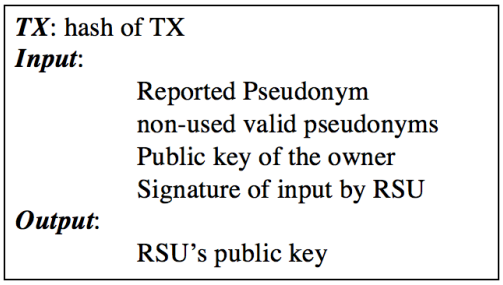



**Figure 5. 6:** Revocation certificate structure.

The verification process of the pseudonym transaction may be executed by any vehicle in the blockchain. It consists of the signature verification, the verification that the public keys used in the ring signature are not revoked and that the pseudonym validity time is not expired. Algorithm 5.4 gives the verification process.

**Algorithm 5. 3:** Pseudonym Certifying Process

***Notation:***
**V**: Vehicle
**TX:** transaction
**RING-SIG:** ring signature
**R:** the set of public keys used in the Ring Signature
**One-time-Address:** creates a unique address from the vehicle's public key for single usage only.
**Algorithm**
**V: Begin**
1- Generate pseudonym
2- Create TX {RING-SIG (Pseudonym, Validity-period, R, One-Time-Address (Public-key))}
3- Publish TX
**End**

**Algorithm 5. 4:** Pseudonym Verification Process

***Notation:***
**V**: Vehicle
**RING-SIG**: ring signature
**R**: the set of public keys used in the Ring Signature
**$P_K$:** Public key
**Algorithm**
V: **Begin**
1- Check for $P_K \in R$, Non-Revoked ($P_K$)= true.
2- Check RING-SIG
3- Check Not-expired (validity)= true.
4- Add to block.
**End**

- ***The revocation process***

The RSUs revoke nodes upon the verification of their malicious behavior received in the vehicles reports. The revocation certificate structure is illustrated in Figure 5.6. It is signed by the RSU's private key and it includes: the revoked pseudonym, the valid non-used pseudonyms and the public key of the misbehaving vehicle. Algorithm 5.5 explains the revocation process

executed by the RSU. Noting that the blocks verification process may be done by any RSU, it consists of the RSU's key validity and signature verification.

**Algorithm 5. 5:** Pseudonym Revocation Process

***Notation***
**$V_r$**: reported Vehicle
**Blacklist**: a list of blacklisted pseudonyms
**R**: the set of public keys used in the Ring Signature
**$P_K$**: Public key
**One-time-Address**: the function that creates a unique address from the vehicle's public key for single usage only.
**P@d**: one-time address
**Get-$V_r$-$P_K$**: gets the public key of the reported vehicle from the offline chain.
**Get-List-$P_K$-R**: gets the list of transactions in which the public key is used in the ring signature.
**Algorithm**
RSU: **Begin**
1- Receive reports from ***i*** vehicles about $V_r$ misbehavior.
2- Confirm misbehavior of $V_r$.
3- Blacklist ($Pseudonym_r$)
4- $P_K$=Get-$V_r$-$P_K$ (R, P@d, offline-chain).
5- R'= Get-List-$P_K$-R (Blockchain, $P_K$)
6- For P@d ∈ R'
   a. If (One-time-Address ($P_K$= P@d))
      Blacklist (pseudonym in R')
7- Blacklist ($P_K$)
8- Create transaction (Blacklist)
**End**

### 5.5.6 Blocks structure and validation

The block structure follows the blockchain type and the composing transaction type which were explained above. Naturally, the block validation process is different as well. Therefore, we describe them separately:

- ***The certifying block***

The vehicles generate their own pseudonyms and publish them in the blockchain for validation. The vehicles assemble the pending transactions in blocks. They simultaneously execute the proof of elapsed time consensus model (see section 5.2.3) where the vehicle with the shortest timer gets to publish the block and chains it to the blockchain by adding the hash of the previous block to it.

- ***The revocation block***

The RSUs create and publish the revocation blocks after verifying and assembling the pending transactions. The RSUs take turns using the round robin consensus model (see section 5.2.3) to create and publish blocks.

### 5.5.7 Authentication using Blockchain

In VPKI based vehicular networks, the state message authentication between vehicle relies on the use of certificate to ensure the integrity, authenticity and non-repudiation. As the beacons are signed by the private key corresponding to the certified pseudonym. The authentication is done on two phases: the first is to check the certificate validity by verifying

that it was issued by the CA and not altered. Also, that the pseudonym is valid and not revoked. The second phase is to check the beacon signature to prove that it is signed by the pseudonym owner and that the message has not been altered.

Similarly, our framework ensures the messages authentication without the need to use certificates issued by the certifying authority. When the vehicle receives a signed beacon containing the pseudonym and its reference in the blockchain, it checks that this pseudonym does exist in the pseudonym blockchain and does not exist in the revocation blockchain. Then, it verifies the pseudonym validity time and the beacon's signature to ensure the message authenticity and integrity. Figure 5.7 illustrates the authentication process into two sections (A and B). Section A presents the beacon broadcast and section B explains how the RSU and the vehicle use our framework to authenticate received beacons.

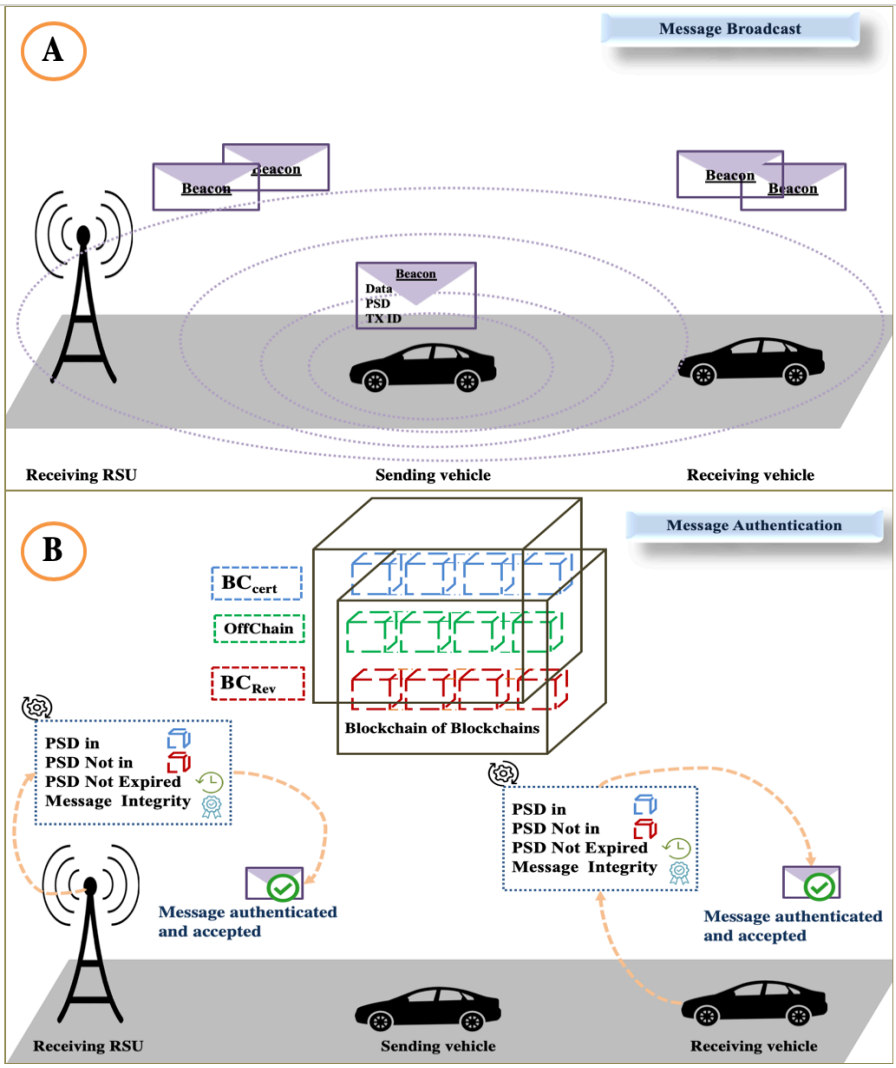



**Figure 5. 7:** Message authentication

## 5.6. Analysis

We designed the framework to ensure the security and privacy essential requirements guaranteed by current central VPKI while over-coming it lacks as well. In what follows, we explain the ensured security properties:

- ***The security***

The blockchain technology ensures the security by relying on cryptography and hashing usage. Our solution inherits the security strength of the blockchains. To compare the VPKI with our solution in term of security robustness, we used the attack tree defined by Schceier B. [126] using Ad tool [128] for both solutions (see Figure 5.8). We enumerate the potential security breaches then calculate the probability of them to occur and break the security, leak and alter the data for each solution.

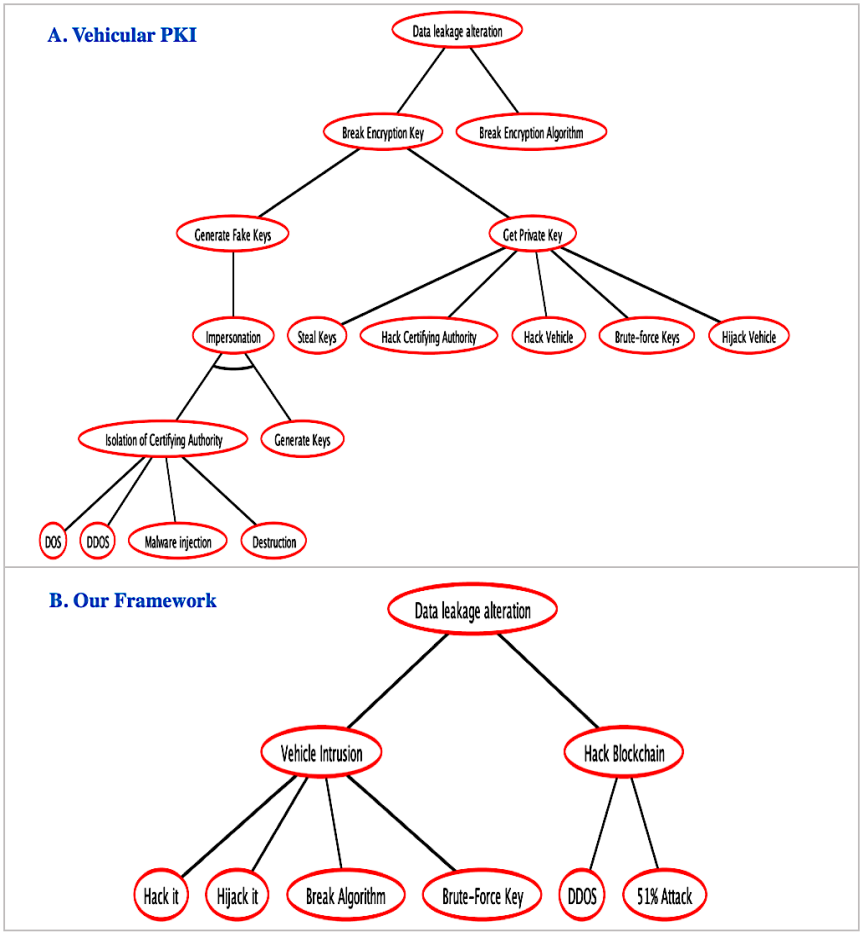



**Figure 5. 8:** Attack Tree for vehicular PKI and Our proposed framework

The occurrence probability is calculated for each leaf node using the formula defined in [168], and the grade standard resumed in Table 5.1. The calculated probabilities, as well as the grades per each attack for both of our proposed framework and the VPKI, are resumed in Table 5.2.

We calculated the probability of occurrence $P_o$ using Equation 5.1 where: $x$ is the execution difficulty, $y$ is the detection difficulty, $z$ is the cost. $U$ is the utility function and $w \in [0,1]$ is the weight attached to each parameter, which is considered here to be equal to 1/3 for each parameter. The utility function (Equation 5.2) is calculated like in [168].

***Equation 5. 1:*** $$P_o = w\,(U(x) + U(y) + U(z))$$

***Equation 5. 2:*** $$U(f) = C_f/f, \text{ where } C_f=0.2$$

The probability *P* of achieving the aim at the tree root, which is to break the security, leak and alter the data is calculated from the attack tree. Noting that this tree is Boolean algebra based where the OR is considered as sum operation, AND is translated as multiplication operator. For better illustration, we explain with an example how to calculate the probability of occurrence *P* of the impersonation attack (Equation 5.3) and the isolation of certifying authority (Equation 5.4) from the attack tree in Figure 5.8.

***Equation 5. 3*:** P(impersonation) = P (isolation of certifying authority) * P (generate Keys)

***Equation 5. 4:*** P (isolation of certifying authority) = P (DOS) + P (DDOS) + P (Malware injection) + P (destruction)

**Table 5. 1:** Standard Grade chart

| *Attack cost evaluation* | | *Technical difficulty of executing* | | *Detection Difficulty* | |
|---|---|---|---|---|---|
| *Grade* | *Cost* | *Grade* | *Difficulty* | *Grade* | *Difficulty* |
| 5 | Quite costly | 5 | Quite difficult | 5 | Quite difficult |
| 4 | Costly | 4 | Difficult | 4 | Difficult |
| 3 | Moderate cost | 3 | Mediate | 3 | Mediate |
| 2 | Cheap | 2 | Simple | 2 | Simple |
| 1 | Quite cheap | 1 | Quite simple | 1 | Quite simple |

**Table 5. 2:** Probability of occurrence

| *Our proposed framework* | | | | |
|---|---|---|---|---|
| *Attack* | *Difficulty of execution* | *Detection Difficulty* | *Attack cost evaluation* | *Probability of occurrence* |
| Hack it | 4 | 3 | 5 | 0.05 |
| Hijack it | 2 | 1 | 1 | 0.17 |
| Break Algorithm | 5 | 5 | 5 | 0.04 |
| Brute-force Key | 5 | 5 | 5 | 0.04 |
| DDOS | 4 | 2 | 5 | 0.06 |
| 51% Attack | 5 | 4 | 5 | 0.04 |
| **Probability of achieving main aim** | | | | **0.41** |
| *VPKI* | | | | |
| *Attack* | *Difficulty of execution* | *Detection Difficulty* | *Attack cost evaluation* | *Probability of occurrence* |
| DOS | 2 | 1 | 2 | 0.13 |
| DDOS | 3 | 2 | 5 | 0.07 |
| Generate keys | 3 | 3 | 3 | 0.07 |
| Steal Key | 3 | 2 | 1 | 0.12 |
| Hack certifying authority | 5 | 4 | 5 | 0.04 |
| Hack vehicle | 4 | 4 | 5 | 0.05 |
| Brute-force keys | 5 | 4 | 5 | 0.04 |
| Break encryption Algorithms | 5 | 4 | 5 | 0.04 |
| Hijack vehicle | 2 | 1 | 1 | 0.17 |
| Malware injection | 4 | 3 | 3 | 0.06 |
| Destruction | 4 | 4 | 4 | 0.05 |
| **Probability of achieving main aim** | | | | **0.59** |

The probability P of successfully breaking the security for both solutions indicates that the proposed framework is more secure than the centralized vehicular PKI as it has a lower probability (0.41) than that of the VPKI (0.59).

- ***The identity privacy***

Our framework does not record the pseudonym owner identity in the public blockchain. Although the generated pseudonyms are attached to their owner's account, this link is implicit and does not expose the privacy. Because the user's public key is concealed in a group of potential signers when used for signing or is seeded to the cryptographic hash function for the one-time address generation.

- ***The unlinkability***

The use of ring signature and one-time address prevents the linkability between the user's public key and his/her generated pseudonyms and also between the pseudonyms themselves. It allows the other vehicles to check that the vehicle owns the pseudonyms it uses, that they are valid and non-revoked or expired without explicitly linking them to the owner's identity. As a consequence, the blockchain peers cannot see the vehicle history of generated pseudonyms. This is fundamental to ensure, otherwise, an attacker that knows all of the vehicle's generated pseudonyms may track it when using them on road.

- ***No single point of failure***

The blockchain is distributed. All of the vehicles and RSUs participate in the creation, maintenance and update of the blockchain of blockchains framework. Thus, no certifying authority is needed, and the single point of failure problem is resolved. Furthermore, the participating peers can be considered as a multiple back up and restoration points.

- ***Non-repudiation***

Although, we designed the framework to preserve the vehicle's privacy in the fully distributed public blockchain. The non-repudiation is another guaranteed property that ensures that the misbehaving vehicles cannot deny their committed actions and can be held responsible.

The blockchain nature ensures that the inserted elements cannot be altered or removed. Therefore, once the pseudonym is inserted in the blockchain, the vehicle can no longer deny having generated it. If it misbehaves while using this pseudonym it gets revoked. The revocation includes the reported pseudonym, the other still valid unused pseudonyms and the vehicle's public key. The public key revocation prevents the vehicle from inserting any other pseudonyms in the blockchain. We ensured that by using an offline chain storing the public key, secret key and VIN maintained by the RSU. Noting that to resolve the vehicle's owner identity, the juridical system may obtain the VIN from the RSU and investigate to whom it belongs to identify the owner.

## 5.7. Comparative study

In the previous section, we highlighted our proposed framework characteristics and evaluated its security. In this section, in Table 5.3, we continue to compare between the central vehicular PKI and our solution in terms of security properties, functionalities, complexity and characteristics. Also, we evaluate each solution advantages and disadvantages.

**Table 5. 3:** Comparative Study between our Proposed framework and the vehicular PKI.

| Comparison Criteria | | Vehicular- PKI | Our proposed framework |
|---|---|---|---|
| **Main Functionalities** | ***Registration*** | ***To***: trusted certifying authority<br>***Input***: identity and VIN<br>***Output***: Permanent certified pair of public and private keys used to request pseudonyms or their certificates. | ***To***: blockchain system<br>***Input***: VIN<br>***Output***: Pair of public and private Keys, secret key. |
| | ***Pseudonym Generation and Certification*** | Self-generated and certified by the trusted authority; ***OR***<br>Generated and certified by the trusted authority. | Self-generated and self-signed using ring signature. |
| | ***Pseudonym Change*** | Upon expiry | Upon Expiry. |
| | ***Pseudonym Refilling*** | Periodical at the certifying authority facilities. ***OR,***<br>On-road, on-demand after authentication to the certifying authority. | Self-refilling. |
| | ***Vehicle Revocation*** | ***Vehicles***: Detect and report misbehaving nodes<br>***Trusted authority***: Investigate reports, revoke misbehaving node, distribute the updated CRL to vehicles. | ***Vehicles***: Detect and report misbehaving nodes.<br>***RSUs***: Investigate reports, add vehicles keys to the blockchain of revoked pseudonyms |
| | ***Message authentication*** | Check:<br>-The authority's Key certificate and validity.<br>-The pseudonym certificate (integrity and validity)<br>- The pseudonym being not revoked<br>- The message integrity. | Check:<br>-The pseudonym in Blockchain<br>-The pseudonym not being revoked and valid<br>-The message integrity. |
| | ***Message decryption*** | Check:<br>-The authority's key certificate and validity.<br>- The pseudonym certificate (integrity and validity)<br>-The pseudonym being not revoked<br>Decrypt the message. | Check:<br>-The pseudonym in Blockchain<br>-The pseudonym not being revoked and valid<br>Decrypt message. |
| **Security Properties** | ***Availability*** | Single point of failure | Ensured by redundancy |
| | ***Privacy*** | Conditional, preserved from peer vehicles but not from authorities | Conditional, preserved unless a misbehavior occurs. |
| | ***Non-repudiation*** | Ensured | Ensured |

| | | | |
|---|---|---|---|
| **Security Properties** | ***Integrity*** | Ensured by the use of digital signatures and certificates | Ensured by digital signature and the use of blockchain |
| | ***Alteration*** | Only authority (or a hacker who can compromise it) | Once validated no transaction can be altered, nor data can be injected into the blockchain. |
| | ***Resiliency to attacks*** (As explained in Table 5.2) | High | Extra-high |
| **Characteristics** | ***Redundancy*** | Back up | All nodes save a copy of the blockchain |
| | ***Authority*** | Mandatory | Not needed |
| | ***Consensus*** | Centralized | Distributed |
| **Complexity** | ***Implementation and design*** | Medium | High |
| | ***Security schemes used*** | High | Extra-high |
| | ***HMI Usage*** | High | Extra-high |
| | ***The difficulty of the system breaking*** (As explained in Table 5.2) | High | Extra-high |
| **Evaluation** | ***Advantages*** | Simplicity and security | Security, Availability, optimization and overhead reduction, public, decentralized, authority-free. |
| | ***Disadvantages*** | Long CRL and revocation process,<br>Single Point of failure,<br>Reliance on the certificate authority to continuously provide pseudonyms/certificates for vehicles.<br>Overhead caused by attaching the certificates to the messages, the exchange of CRL, the refilling requests. | Complexity of implementation. |

## 5.8. Conclusion

The chapter proposed a blockchain-based framework to resolve the pseudonym managements issue in vehicular networks which currently is central-based VPKI. The VPKI suffers from being a single point of failure targeted by attacks, which if compromised causes perilous security damages. The designed framework is public and distributed ensuring both the privacy and non-repudiation which we often shorten as the conditional privacy. I.e. the privacy is preserved for vehicles that demonstrate a correct behavior. The framework is composed of two connected blockchains: the untraceable, unlinkable permission-less public pseudonym

blockchain maintained by the vehicles, and the permissioned public revocation blockchain maintained by the RSUs containing an offline private chain and online public chain. The framework inherits the security strength of blockchains. It is distributed and public. So, it eliminates the need for revocation lists usage. Also, it prevents the reliance on the CA to authenticate the vehicle's messages and all the engendered messages required by the process. Thus, the network overhead is reduced, and the bandwidth usage is optimized. Moreover, it illustrated a better resiliency to attacks than the conventional vehicular PKI.

# CONCLUSION AND FUTURE WORKS

# Conclusion

In this thesis, we achieved our underlined objectives highlighted in the introduction as being our research problematic. The aim of our research is to provide privacy and security solutions that ensure the safe usage of vehicular networks. In the thesis, we guided the reader to learn about the vehicular networks and their various types, technologies and challenges. These networks were initially developed to ensure the safety of their users and to extend the internet services to the road. However, the cyber-activity of these users on road may endanger their privacy. This causes their tracking, the exposure of their secrets and may even impact their safety.

The privacy in vehicular network is at risk because of the requirements imposed by the system. The wireless exchange of heartbeat messages containing the vehicle's identity and spatiotemporal data facilitates the tracking for the attackers. The tracking is passive which gives the attacker the chance to track his/her victims for long periods before being detected. The attacker may use the collected data to profile his/her victims, blackmail them, or trade their data for profit. The consequences may be more perilous such as causing road causalities.

Therefore, we followed the footsteps of senior researchers and proposed in this thesis new privacy-preserving solutions. Before we had proposed these schemes, we first surveyed and analyzed the existing solutions in the literature. Then, we specified the attacker targeting the privacy, his/her executed attacks and used means. Finally, we decided on the proofing methodology to use in order to evaluate our proposals.

In our research, we concentrated on two security issues which are the authentication and the privacy. These two issues are contradictory by nature as most authentication methods rely on identifying data unique to each user among which is the identity. The privacy on the other hand especially in vehicular networks prohibits the exchange of identifying data. Because identity and location can be correlated, i.e. exposing the identity leads to tracking on road and vice-versa. Therefore, we needed to find solutions that ensure the authentication while preserving the privacy. In this regard, we proposed the reputation-based anonymous authentication methods for cloud-enabled vehicular named data network. Also, we proposed another anonymous authentication method for pseudonym refilling in VANET.

To preserve the location privacy, we developed two solutions to protect the VANET users. They were both-crowd, infrastructure and road-map independent. They were designed to reduce the vehicle tracking even when within low-density roads. They were analyzed against a global passive attacker and showed low tracking ratios in overall. We also proposed three location privacy-preserving solutions for cloud-enabled internet of vehicles users. The solutions were designed to reduce the tracking ratio which was decreased to approximately 10% in the last scheme.

The last contribution of this thesis contained the design of a framework that could potentially replace the centralized vehicular PKI. The framework is distributed and public. It reduces the overhead caused by the multiple queries to the authorities to request pseudonyms, to check certificate or to exchange the certificate revocation lists. It also resolves the single point of failure issue found in VPKI. It is privacy-aware. It ensures both unlinkability and anonymity.

It also insures the security properties of non-repudiation, integrity, availability authenticity and revocation. When analyzed, it illustrated a higher level of security than the conventional VPKI.

## Future Works

In our future works, we intend to design an anonymous payment system for vehicular networks. The vehicles may provide each other with services and resources for free. In that case, only the authentication is required to maintain the traceability and the correct functioning of the network. In this regard, we already proposed an anonymous authentication method in Chapter 3. However, if these services and resources are rented, then an anonymous payment method is needed. The payment should be done in a way that:

- The service or resource provider's privacy should be preserved.
- The service requester's privacy should be preserved.
- The money value needs to be correct.

More importantly, we should ensure that the service/resource provider gets paid the correct amount of money. At the same time, we should make sure s/he provided the service/resource as agreed upon. We shall think of refunding and fining policies if the contrary case occurs. Similarly, the service requester must pay for the service/resource s/he benefitted from and not evade the payment.

Our second objective is to redesign the blockchain-based pseudonym management framework to allow the vehicles to generate pseudonyms for each other as a service. This service may be free or for profit. Initially, we need to decide on the consensus model used by the vehicle for that case. Also, because the pseudonym is, in reality, a pair of public and private keys, we have to ensure the forward security. The vehicles may generate pseudonyms for each other. Yet, they shall not expose each other's secrets or read each other's encrypted messages.

Our third objective is to organize our simulation codes into a framework to allow the researchers establish comparative studies with our solutions. The framework would include our attacker model, scenarios, privacy-preserving solutions and state-of-art modelled solutions.

Our fourth objective is the release of the blockchain vehicular pseudonym management framework after the finalization of the implementation.

## Key Contributions

- **Paper**
  - **(2020)** BENAROUS Leila, Kadri Benamar. The quest of privacy in public key infrastructure. Int. J. of Blockchains and Cryptocurrencies.
  - **(2019)** BENAROUS Leila, Kadri Benamar, Bitam Salim and Mellouk Abdelhamid. Privacy-preserving Authentication Scheme for OnRoad OnDemand Refilling of Pseudonym in VANET, special issue: Smart Communications for Autonomous Systems in Network Technologies. John Wiley & Sons, Ltd. International Journal of Communication Systems. DOI:10.1002/dac.4087.
- **Conference Papers**
  - **(2020)** BENAROUS Leila, Kadri Benamar, Boudjit Saadi. Alloyed Pseudonym Change Strategy for Location Privacy in VANETs. 2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC).
  - **(2018)** Benarous Leila, Kadri Benamar. Privacy-preserving Scheme for pseudonym refilling in VANET. 2018 7th IEEE International Conference on Smart Communications in Network Technologies (Saconet), P: 114-119. 27-31 Oct, 2018. EL Oued- Algeria. (**Best Paper Award**)
  - **(2017)** Benarous Leila, Kadri Benamar. Ensuring Privacy and Authentication for V2V Resource Sharing. 2017 Seventh International Conference on Emerging Security Technologies (EST), 6-8 September 2017. Canterbury, UK. ISBN: 978-1-5386-4017-3.
- **Book chapters**
  - **(2017)** Benarous Leila, Kadri Benamar and Bouridane Ahmed. Chapter 15: A Survey on Cyber Security Evolution and Threats: Biometric Authentication Solutions. In: R. Jiang et al. (eds.), Biometric Security and Privacy, Signal Processing for Security Technologies, DOI: 10.1007/978-3-319-47301-7, 2017, URL: http://www.springer.com/us/book/9783319473000.
  - **(2019)** Benarous Leila, Kadri Benamar. Chapter 11: A Novel Privacy-Preserving Scheme for Users of Cloud-Enabled Internet of Vehicles. In: Mahmood, Zaigham (Ed.), Security, Privacy and Trust in the IoT Environment, DOI: 10.1007/978-3-030-18075-1_11, 2019, URL: https://www.springer.com/gp/book/9783030180744.
- **Papers Under Review**
  - Benarous Leila, Kadri Benamar and Boudjit Saadi. Camouflage-based location privacy-preserving scheme in Vehicular Ad hoc Networks. Inderscience, International Journal of Vehicle Information and Communication Systems (IJVICS).
  - Benarous Leila, Kadri Benamar. Hybrid Pseudonym Change Strategy for Location Privacy in VANET. International Journal of Information Privacy, Security and Integrity.
  - Benarous Leila, Kadri Benamar and Bouridane Ahmed. Blockchain-based Privacy Aware Pseudonym Management Framework for Vehicular Networks. Springer, Arabian Journal for Science and Engineering.
  - Benarous Leila, Kadri Benamar. Obfuscation-based Location Privacy-Preserving Scheme in Cloud-enabled Internet of Vehicles. Ad Hoc & Sensor Wireless Networks Journal.

## ▪ Submitted Patent

- Benarous Leila, Kadri Benamar. Vehicular Anti-theft, Anti-kidnapping System.

## ▪ Other Scientific Activities

- Benarous Leila, Kadri Benamar. Security and Privacy in Vehicular Networks, Doctorial day on Information and Communication Systems and Technologies, June 26th, 2019, STIC Labs, University Abou Bekr Belkaid, Tlemcen.
- Benarous Leila, Certified Reviewer at Wiley International Journal of Communication Systems.
- Organizing member of MISC 2018 5th edition symposium (5th International Symposium on Modelling and Implementation of Complex Systems) at the university of Laghouat in collaboration with the university of Constantine2, December 16-18th, 2018.
- Benarous Leila, Kadri Benamar. Security and Privacy in Vehicular Networks, Doctorial day on Information and Communication Systems and Technologies, June 25th, 2018, STIC Labs, University Abou Bekr Belkaid, Tlemcen.
- **Teaching**: Microsoft Office tools practical training, Computer Science Department, Faculty of science, University of Amar Telidji (2018).
- **Teaching**: Practical Training on Network Administration, Telecommunication Department, Faculty of technology, University of Amar Telidji (2018).
- 3 days CISCO training, Networking and Security Fundamentals, Tlemcen, February 2017.
- IELTS Certificate Level B2, British Council, Algiers, February 2016.

# Bibliography


[1] Contreras-Castillo, J., S. Zeadally, and J.A. Guerrero-Ibañez, *Internet of vehicles: architecture, protocols, and security.* IEEE Internet of Things Journal, 2017. **5**(5): p. 3701-3709.

[2] Bonomi, F. *The smart and Connected Vehicle and the Internet of Things*. in *Invited Talk, Workshop on Synchronization in Telecommunication Systems*. San Jose'. 2013.

[3] Maglaras, L.A., et al., *Social internet of vehicles for smart cities.* Journal of Sensor and Actuator Networks, 2016. **5**(1): p. 3.

[4] Bai, F. and B. Krishnamachari, *Exploiting the wisdom of the crowd: localized, distributed* information-*centric VANETs [Topics in Automotive Networking].* IEEE Communications Magazine, 2010. **48**(5): p. 138-146.

[5] Gerla, M., et al. *Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds*. in 2014 IEEE world forum on internet of things (WF-IoT). 2014. Seoul, South Korea. IEEE.

[6] Hartenstein, H. and K. Laberteaux, *VANET: vehicular applications and inter-networking technologies*. Vol. 1. 2009: John Wiley & Sons.

[7] Meraihi, R., et al., *Vehicle-to-Vehicle Communications: Applications and Perspectives.* Wireless Ad Hoc and Sensor Networks, 2008: p. 285-308.

[8] Gu, L., D. Zeng, and S. Guo. *Vehicular cloud computing: A survey*. in *2013 IEEE Globecom Workshops (GC Wkshps)*. 2013. Atlanta, GA, USA. IEEE.

[9] Yang, F., et al., *An overview of internet of vehicles.* China communications, 2014. **11**(10): p. 1-15.

[10] Team, Waymo. *Self-driving vehicles*. [2018] [19 12 2018]; Available from: https://waymo.com/journey/.

[11] Research, Predictive. *Top companies for self-driving vehicles*. 2013-2020 [2018] [19 12 2018]; Available from: https://www.predictiveanalyticstoday.com/top-companies-autonomous-cars-self-driving-car/

[12] Glancy, D.J., *Privacy in autonomous vehicles.* Santa Clara L. Rev., 2012. **52**: p. 1171.

[13] Al-Sultan, S., et al., *A comprehensive survey on vehicular ad hoc network.* Journal of network and computer applications, 2014. **37**: p. 380-392.

[14] Autocare, National Tyres. *10 Astonishing Technologies That Power Google's Self-Driving Cars*. [cited 2018 20 12 2018]; Available from: https://www.national.co.uk/tech-powers-google-car/.

[15] Kumar, V., S. Mishra, and N. Chand, *Applications of VANETs: present & future.* Communications and Network, 2013. **5**(01): p. 12.

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

[17] Sivasakthi, M. and S. Suresh, *Research on vehicular ad hoc networks (VANETs): an overview.* International Journal of Applied Science and Engineering Research, 2013. **2**(1): p. 23-27

[18] Da Cunha, F.D., et al., *Data communication in VANETs: a survey, challenges and applications.* [Research Report] RR-8498, INRIA Saclay. 2014.

[19] Boualouache, A., *Security and privacy in vehicular AD-HOC networks.* , PhD Thesis, *Computer Science*. 2016, USTHB, Algiers, Algeria: 2016.

[20] Zeadally, S., et al., *Vehicular ad hoc networks (VANETS): status, results, and challenges.* Telecommunication Systems, 2012. **50**(4): p. 217-241.

[21] Sjöberg, K. Standardization *of Wireless Vehicular Communications within IEEE and ETSI*. in *IEEE VTS Workshop on Wireless Vehicular Communications*. 2011.

[22] Rawashdeh, Z.Y. and S.M. Mahmud, *Communications in vehicular networks.* Mobile Ad-Hoc Networks: Applications, 2011: p. 20-40.

[23] Lucero, S., *Cellular–vehicle to everything (C-V2X) connectivity.* IHS Technology, Internet Everything, 2016.

[24] Wang, X., S. Mao, and M.X. Gong, *An overview of 3GPP cellular vehicle-to-everything standards.* GetMobile: Mobile Computing and Communications, 2017. **21**(3): p. 19-25.

[25] 3GPP, "ETSI TS 122 185 V14.3.0 LTE; Service requirements for V2X services (3GPP TS 22.185 version 14.3.0 Release 14)," 3GPP, (2017-03).

[26] Gerla, M. *Vehicular cloud computing*. in 2012 The 11th annual mediterranean ad hoc networking workshop (Med-Hoc-Net). 2012. Piscataway, NJ. IEEE.

[27] Whaiduzzaman, M., et al., *A survey on vehicular cloud computing.* Journal of Network and Computer applications, 2014. **40**: p. 325-344.

[28] Hussain, R., Z. Rezaeifar, and H. Oh, *A paradigm shift from vehicular ad hoc networks to VANET-based clouds.* Wireless Personal Communications, 2015. **83**(2): p. 1131-1158.

[29] Chen, M., et al., *Cognitive internet of vehicles.* Computer Communications, 2018. **120**: p. 58-70.

[30] Lequerica, I., M.G. Longaron, and P.M. Ruiz, *Drive and share: efficient provisioning of social networks in vehicular scenarios.* IEEE Communications Magazine, 2010. **48**(11): p. 90-97.

[31] Alam, K.M., M. Saini, and A. El Saddik, *Toward social internet of vehicles: Concept, architecture, and applications.* IEEE access, 2015. **3**: p. 343-357.

[32] Chen, M., et al., *Vendnet: Vehicular named data network.* Vehicular Communications, 2014. **1**(4): p. 208-213.

[33] Bouk, S.H., et al., *Named-data-networking-based ITS for smart cities.* IEEE Communications Magazine, 2017. **55**(1): p. 105-111

[34] Ahmed, S.H., et al., *Named data networking for software defined vehicular networks.* IEEE Communications Magazine, 2017. **55**(8): p. 60-66.

[35] Mapp, A.P.D.G. *The future of driving is here*. [19 03 2017]; Available from: https://mdxminds.com/2016/01/11/the-future-of-driving-is-here/.

[36] Silva, J.B.C. *Final Report Summary - FUTURE-CITIES* 2016 [ 20 03 2017]; Available from: http://cordis.europa.eu/result/rcn/188104_en.html

[37] Lutterotti, P., et al. *C-vet, the ucla vehicular testbed: An open platform for vehicular networking and urban sensing*. in *International Conference on Wireless Access for Vehicular Environments (WAVE 2008)*. Lucca, Italy.

[38] Agarwal, B.Z.J.P.S. *VanLan: Investigating Connectivity from Moving Vehicles*. [27 02 2008] [21 03 2017]; Available from: https://www.microsoft.com/en-us/research/project/vanlan-investigating-connectivity-from-moving-vehicles/.

[39] *Cooperative Traffic Systems –safe and intelligent*. [21 03 2017]; Available from: http://c-its-korridor.de/?menuId=1&sp=en

[40] *Compass 4d Project Europe*. [21 03 2017]; Available from: http://www.compass4d.eu/.

[41] *Drive C2X*. [21 03 2017]; Available from: http://www.drive-c2x.eu/project

[42] Simtd. [21 03 2017]; Available from: http://www.simtd.de/index.dhtml/enEN/news/Presse.html.

[43] Lawson, P., B. McPhail, and E. Lawton, *The Connected Car: Who is in the Driver's Seat? A Study on Privacy and Onboard Vehicle Telematics Technology.* 2015.

[44] Seuwou, P., D. Patel, and G. Ubakanma, *Vehicular ad hoc network applications and security: a study into the economic and the legal implications.* International Journal of Electronic Security and Digital Forensics, 2014. **6**(2): p. 115-129.

[45] Litman, T., *Autonomous vehicle implementation predictions*. 2017: Victoria Transport Policy Institute Victoria, Canada.

[46] Schoettle, B. and M. Sivak, *A survey of public opinion about autonomous and self-driving vehicles in the US, the UK, and Australia*. 2014, University of Michigan, Ann Arbor, Transportation Research Institute.

[47] Warren, S.D. and L.D. Brandeis, *The right to privacy.* Harvard law review, 1890: p. 193-220.

[48] Westin, A.F., *Privacy and freedom Atheneum.* New York, 1967. **7**: p. 431-453.

[49] AmreShakimov, E.C. *Privacy and Networks CPS 96*. [02 03 2019]; Available from: https://studylib.net/doc/15143690/privacy-and-networks-cps-96-eduardo-cuervo-amre-shakimov.

[50] Lukács, A., *What Is Privacy? The history and definition of privacy.* 2016.

[51] Petit, J., et al., *Pseudonym schemes in vehicular networks: A survey.* IEEE communications surveys & tutorials, 2014. **17**(1): p. 228-255

[52] Lim, H.-J. and T.-M. Chung, *Privacy treat factors for VANET in network layer*, in *Soft Computing in Information Communication Technology*. 2012, Springer. p. 93-98.

[53] Beresford, A.R. and F. Stajano, *Location privacy in pervasive computing.* IEEE Pervasive computing, 2003. **2**(1): p. 46-55.

[54] Buttyán, L., et al. *Slow: A practical pseudonym changing scheme for location privacy in vanets*. in *2009 IEEE Vehicular Networking Conference (VNC)*. 2009. Tokyo, Japan. IEEE.

[55] Kang, J., et al., *Location privacy attacks and defenses in cloud-enabled internet of vehicles.* IEEE Wireless Communications, 2016. **23**(5): p. 52-59.

[56] T. Kurihara, "1609.2-2013 - IEEE Standard for Wireless Access in Vehicular Environments ? Security Services for Applications and Management Messages," VT - IEEE Vehicular Technology Society, 2013.

[57] Emara, K.A.A.E.-S., *Safety-aware location privacy in vehicular ad-hoc networks*. PhD Thesis. 2016, Technische Universität München.

[58] Hussain, R., S. Kim, and H. Oh. *Towards privacy aware pseudonymless strategy for avoiding profile generation in vanet*. in *International Workshop on Information Security Applications*. 2009. Springer. Berlin, Heidelberg.

[59] Cisco *White Paper- Encrypted Traffic Analytics*. 2019

[60] ETSI, "Intelligent Transport Systems (ITS); Security; Pre-standardization study on pseudonym change management," ETSI TR 103 415 V1.1.1, 2018-04.

[61] Chaum, D.L., *Untraceable electronic mail, return addresses, and digital pseudonyms.* Communications of the ACM, 1981. **24**(2): p. 84-90.

[62] Danezis, G. *Mix-networks with restricted routes*. in *International Workshop on Privacy Enhancing Technologies*. 2003. Springer. Berlin, Heidelberg.

[63] Freudiger, J., et al. *Mix zones for location privacy in vehicular networks,‖ presented at the Int*. in *Workshop Wireless Netw. Intell. Transp. Syst., Vancouver, BC, Canada*. 2007.

[64] Freudiger, J., R. Shokri, and J.-P. Hubaux. *On the optimal placement of mix zones*. in *International Symposium on Privacy Enhancing Technologies Symposium*. 2009. Springer.

[65] Sun, Y., et al., *Mix-zones optimal deployment for protecting location privacy in VANET.* Peer-to-Peer Networking and Applications, 2015. **8**(6): p. 1108-1121.

[66] Song, J.-H., V.W. Wong, and V.C. Leung, *Wireless location privacy protection in vehicular ad-hoc networks.* Mobile Networks and Applications, 2010. **15**(1): p. 160-171.

[67] Huang, L., et al. *Enhancing wireless location privacy using silent period*. in *IEEE Wireless Communications and Networking Conference, 2005*. New Orleans, LA, USA. IEEE.

[68] Sampigethaya, K., et al., *CARAVAN: Providing location privacy for VANET*. 2005, Washington Univ Seattle Dept of Electrical Engineering.

[69] Sampigethaya, K., et al., *AMOEBA: Robust location privacy scheme for VANET.* IEEE Journal on Selected Areas in communications, 2007. **25**(8): p. 1569-1589.

[70] Chaurasia, B.K., et al. *Pseudonym based mechanism for sustaining privacy in vanets*. in *2009 First International Conference on Computational Intelligence, Communication Systems and Networks*. 2009. Indore, India. IEEE.

[71] Buttyán, L., T. Holczer, and I. Vajda. *On the effectiveness of changing pseudonyms to* provide *location privacy in VANETs*. in *European Workshop on Security in Ad-hoc and Sensor Networks*. 2007. Springer. Berlin, Heidelberg.

[72] Palanisamy, B. and L. Liu. *Mobimix: Protecting location privacy with mix-zones over road networks*. in *2011 IEEE 27th International Conference on Data Engineering*. 2011. Hannover, Germany. IEEE.

[73] Palanisamy, B., et al. *Location privacy with road network mix-zones*. in *2012 8th International Conference on Mobile Ad-hoc and Sensor Networks (MSN)*. 2012. Chengdu, China. IEEE.

[74] Lu, R., et al. *Anonymity analysis on social spot based pseudonym changing for location privacy in VANETs*. in 2011 IEEE International Conference on Communications (ICC). 2011. Kyoto, Japan. IEEE.

[75] Lu, R., et al., *Pseudonym changing at social spots: An effective strategy for location privacy in vanets.* IEEE transactions on vehicular technology, 2011. **61**(1): p. 86-96.

[76] Mathews, S. and B. Jinila. *An effective strategy for pseudonym generation & changing scheme with privacy preservation for vanet*. in *2014 International Conference on Electronics and Communication Systems (ICECS)*. 2014. Coimbatore, India. IEEE.

[77] Liu, X., et al. *Traffic-aware multiple mix zone placement for protecting location privacy*. in *2012 Proceedings IEEE INFOCOM*. 2012. Orlando, FL, USA. IEEE

[78] Ying, B., D. Makrakis, and H.T. Mouftah, *Dynamic mix-zone for location privacy in vehicular networks.* IEEE Communications Letters, 2013. **17**(8): p. 1524-1527.

[79] Boualouache, A., S.-M. Senouci, and S. Moussaoui, *Vlpz: The vehicular location privacy zone.* Procedia Computer Science, 2016. **83**: p. 369-376.

[80] Kang, J., et al., *Privacy-preserved pseudonym scheme for fog computing supported internet of vehicles.* IEEE Transactions on Intelligent Transportation Systems, 2017. **19**(8): p. 2627-2637.

[81] Liao, J. and J. Li. *Effectively changing pseudonyms for privacy protection in vanets*. in *2009 10th International Symposium on Pervasive Systems, Algorithms, and Networks*. 2009. Kaohsiung, Taiwan. IEEE.

[82] Pan, Y. and J. Li. *An analysis of anonymity for cooperative pseudonym change scheme in one-dimensional VANETs*. in *Proceedings of the 2012 IEEE 16th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*. 2012. Wuhan, China. IEEE.

[83] Pan, Y. and J. Li, *Cooperative pseudonym change scheme based on the number of neighbors in VANETs.* Journal of Network and Computer Applications, 2013. **36**(6): p. 1599-1609.

[84] Pan, Y., Y. Shi, and J. Li. *A novel and practical pseudonym change scheme in VANETs*. in *International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*. 2017. Springer. Cham.

[85] Emara, K., 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. 2015.

[86] Ying, B. and D. Makrakis. *Pseudonym changes scheme based on candidate-location-list in vehicular networks*. in 2015 IEEE International Conference on Communications (ICC). 2015. London, UK. IEEE.

[87] Li, M., et al. *Swing & swap: user-centric approaches towards maximizing location privacy*. in *Proceedings of the 5th ACM workshop on Privacy in electronic society*. Alexandria Virginia USA. 2006.

[88] Burmester, M., E. Magkos, and V. Chrissikopoulos. *Strengthening privacy protection in vanets*. in *2008 IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*. 2008. Avignon, France. IEEE.

[89] Dok, H., R. Echevarria, and H. Fu. *Privacy issues for vehicular ad-hoc network*. in *International Conference on Future Generation Communication and Networking*. 2009. Springer

[90] Boualouache, A. and S. Moussaoui. *S2si: A practical pseudonym changing strategy for location privacy in vanets*. in *2014 International Conference on Advanced Networking Distributed Systems and Applications*. 2014. Bejaia, Algeria. IEEE.

[91] Xingjun, S. and X. Huibin, *An effective scheme for location privacy in VANETs.* Journal of Networks, 2014. **9**(8): p. 2239

[92] Ying, B., D. Makrakis, and Z. Hou, *Motivation for protecting selfish vehicles' location privacy in vehicular networks.* IEEE Transactions on Vehicular Technology, 2015. **64**(12): p. 5631-5641.

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

[94] Boualouache, A. and S. Moussaoui, *TAPCS: Traffic-aware pseudonym changing strategy for VANETs.* Peer-to-Peer networking and Applications, 2017. **10**(4): p. 1008-1020.

[95] Wang, S., et al., *A trigger-based pseudonym exchange scheme for location privacy preserving in VANETs.* Peer-to-Peer Networking and Applications, 2018. **11**(3): p. 548-560.

[96] Memon, I., et al., *Pseudonym changing strategy with multiple mix zones for trajectory privacy protection in road networks.* International Journal of Communication Systems, 2018. **31**(1): p. e3437

[97] Khacheba, I., et al. *Location privacy scheme for VANETs*. in *2017 International Conference on Selected Topics in Mobile and Wireless Networking (MoWNeT)*. 2017. Avignon, France. IEEE.

[98] Khacheba, I., et al., *CLPS: context-based location privacy scheme for VANETs.* International Journal of Ad Hoc and Ubiquitous Computing, 2018. **29**(1-2): p. 141-159.

[99] Amro, B., *Protecting privacy in VANETs using mix zones with virtual pseudonym change*. *International Journal of Network Security & Its Applications (IJNSA).* 2018. *(*10)1.

[100] Guo, N., L. Ma, and T. Gao, *Independent mix zone for location privacy in vehicular networks.* IEEE Access, 2018. **6**: p. 16842-16850.

[101] Benarous, L., B. Kadri, and A. Bouridane, *A survey on cyber security evolution and threats: biometric authentication solutions*, in *Biometric Security and Privacy*. 2017, Springer. p. 371-411.

[102] Fadlullah, Z.M., T. Taleb, and M. Schöller, *Combating against security attacks against mobile ad hoc networks (MANETs).* Security of Self-Organizing Networks: MANET, WSN, WMN, VANET, 2010. **173**: p. 1-13

[103] Gu, Q. and P. Liu, *Denial of service attacks.* Handbook of Computer Networks: Distributed Networks, Network Planning, Control, Management, and New Trends and Applications, 2007. **3**: p. 454-468.

[104] Raazi, S.M.K.-u.-R., Z. Pervez, and S. Lee, *Key management schemes of wireless sensor networks: A survey*. Department of Computer Engineering, Kyung Hee University, Global Campus, Korea, 2011.

[105] Laurendeau, C. and M. Barbeau. *Threats to Security in DSRC/WAVE. in International Conference on Ad-Hoc Networks and Wireless.* 2006. Springer, Berlin, Heidelberg.

[106] Mejri, M.N., J. Ben-Othman, and M. Hamdi, *Survey on VANET security challenges and possible cryptographic solutions.* Vehicular Communications, 2014. **1**(2): p. 53-66.

[107] Sen, J., *A survey on wireless sensor network security.* arXiv preprint arXiv:1011.1529, 2010.

[108] Hu, Y.-C., A. Perrig, and D.B. Johnson, *Wormhole attacks in wireless networks.* IEEE journal on selected areas in communications, 2006. **24**(2): p. 370-380.

[109] Sen, S., et al., *Security threats in mobile ad hoc networks.* Security of Self-Organizing Networks: MANET, WSN, WMN, VANET, 2010: p. 127-147

[110] *Cyber Attacks Explained Man In The Middle Attack*. 2008 [27 02 2019]; Available from: https://www.valencynetworks.com/articles/cyber-attacks-explained-man-in-the-middle-attack.html.

[111] Mitnick, K.D. and W.L. Simon, *The art of deception: Controlling the human element of security*. 2003: John Wiley & Sons.

[112] Huang, D., S.A. Williams, and S. Shere. *Cheater detection in vehicular networks*. in *2012* IEEE *11th International Conference on Trust, Security and Privacy in Computing and Communications*. 2012. Liverpool, UK. IEEE.

[113] Pfleeger, C. and S. Pfleeger, *Security In Computing (4th Edition, 2006).* 2016.

[114] Egan, M. and T. Mather, *The executive guide to information security: Threats, challenges, and solutions*. 2004: Addison-Wesley Professional.

[115] Stolfo, S.J., et al., *Insider attack and cyber security: beyond the hacker*. Vol. 39. 2008: Springer Science & Business Media.

[116] Butler, S. *10 Worst Internet Privacy Scandals To Date*. [02 06 2018][14 03 2019]; Available from: https://www.technadu.com/worst-internet-privacy-scandals/30236/.

[117] Khodaei, M. *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*. Paderborn Germany. 2016.

[118] Alexiou, N., et al. *Vespa: Vehicular security and privacy-preserving architecture*. in *Proceedings of the 2nd ACM workshop on Hot topics on wireless network security and privacy*. Budapest Hungary. 2013

[119] Schaub, F., et al. *V-tokens for Conditional Pseudonymity in VANETs*. in *2010 IEEE Wireless Communication and Networking Conference*. 2010. Sydney, NSW, Australia. IEEE.

[120] Khodaei, M., H. Jin, and P. Papadimitratos. *Towards deploying a scalable & robust vehicular identity and credential management infrastructure*. in *2014 IEEE Vehicular Networking Conference (VNC)*. 2014. Paderborn, Germany. IEEE.

[121] Weerasinghe, H., H. Fu, and S. Leng. *Anonymous service access for vehicular ad hoc networks*. in *2010 Sixth International Conference on Information Assurance and Security*. 2010. Atlanta, GA, USA. IEEE.

[122] Jiang, W., et al. *No one can track you: Randomized authentication in vehicular ad-hoc networks*. in *2017 IEEE International Conference on Pervasive Computing and Communications (PerCom)*. 2017. Kona, HI, USA. IEEE.

[123] Burrows, M., M. Abadi, and R.M. Needham, *A logic of authentication.* Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences, 1989. **426**(1871): p. 233-271.

[124] Yann Glouche, T.G., Olivier Heen, Erwan Houssay and Ronan Saillard. *SPAN*. [2006-2017 ] [19 02 2019]; Available from: http://people.irisa.fr/Thomas.Genet/span/.

[125] *AVISPA [*19 02 2019]; Available from: http://www.avispa-project.org/.

[126] Bruce, S., *Attack trees.* Dr Dobb's Journal, 1999. **24**(12).

[127] *Attack Tree - Isograph*. [20 02 2019]; Available from: https://www.isograph.com/software/attacktree/.

[128] *Attack Tree - ADTool*. [20 02 2019]; Available from: http://satoss.uni.lu/members/piotr/adtool/.

[129] Kim, O.T.T., V. Nguyen, and C.S. Hong, *Which network simulation tool is better for simulating Vehicular Ad-hoc network?* Korean Information Science Society (한국정보과학회 학술발표논문집), 2014: p. 930-932.

[130] *Matlab*. [21 02 2019]; Available from: https://uk.mathworks.com/products/matlab.html

[131] *NS2*. [21 02 2019]; Available from: https://www.isi.edu/nsnam/ns/.

[132] *NS3 Tutorial*. [08 01 2019] [21 02 2019]; Available from: https://www.nsnam.org/docs/release/3.29/tutorial/ns-3-tutorial.pdf

[133] *Omnet*. [21 02 2019]; Available from: https://omnetpp.org/intro/

[134] Javadi, M.M. *Mobisim*. Automn 2006-2011 21 02 2019]; Available from: http://masoudmoshref.com/old/myworks/documentpages/mobility_simulator.htm

[135] Mousavi, S.M., et al. *Mobisim: A framework for simulation of mobility models in mobile ad-hoc networks*. in *Third IEEE international conference on wireless and mobile computing, networking and communications (WiMob 2007)*. 2007. New York, USA. IEEE

[136] Liu, B., et al., *Location privacy-preserving mechanisms*, in *Location Privacy in Mobile Applications*. 2018, Springer. p. 17-31.

[137] Andrés, M.E., et al. *Geo-indistinguishability: Differential privacy for location-based systems*. in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. 2013. Berlin, Germany.

[138] Hotz, H., Lecture Notes, *A short introduction to game theory.* Retrieved on, 2006. **21.** Ludwig-Maximilians-Universität München. 2017.

[139] Kerrache, C.A., et al., *Trust management for vehicular networks: An adversary-oriented overview.* IEEE Access, 2016. **4**: p. 9293-9307.

[140] Liu, Y., Y. Wang, and G. Chang, *Efficient privacy-preserving dual authentication and key agreement scheme for secure V2V communications in an IoV paradigm.* IEEE Transactions on Intelligent Transportation Systems, 2017. **18**(10): p. 2740-2749.

[141] Benarous, L. and B. Kadri. *Ensuring privacy and authentication for V2V resource sharing*. in *2017 Seventh International Conference on Emerging Security Technologies (EST)*. 2017. Canterbury, UK. IEEE

[142] Benarous, L. and B. Kadri. *Privacy preserving scheme for pseudonym refilling in VANET*. in 2018 International Conference on Smart Communications in Network Technologies (SaCoNeT). 2018. El Oued, Algeria. IEEE.

[143] Benarous, L., et al., *Privacy-preserving authentication scheme for on-road on-demand refilling of pseudonym in VANET.* International Journal of Communication Systems, 2019: p. e4087.

[144] *How secure is my password?* [10 04 2019]; Available from: https://howsecureismypassword.net/.

[145] *Brute Force Calculator*. [10 04 2019]; Available from: http://www.mandylionlabs.com/index15.htm.

[146] Caldwell, C.K. *Small Primes*. [10 04 2019]; Available from: https://primes.utm.edu/lists/small/small.html.

[147] *Scientific Notation: Table of Large Numbers*. [10 04 2019]; Available from: http://sunshine.chpc.utah.edu/Labs/ScientificNotation/ManSciNot1/table.html.

[148] *HLPSL Tutorial*. [19 04 2018]; Available from: http://www.avispa-project.org/package/tutorial.pdf.

[149] Tzu, S. *Art of War*. [26 03 2019]; Available from: https://suntzusaid.com/.

[150] Sun, W. and L. Giles, *Sunzi Bingfa Sun Tzŭ on the Art of War. The Oldest Military Treatise in the World. Translated from the Chinese with Introduction and Critical Notes by Lionel Giles. Chinese & Eng*. 1910: Luzac & Company.

[151] Benarous, L. and B. Kadri, *A Novel Privacy Preserving Scheme for Cloud-Enabled Internet of Vehicles Users*, in *Security, Privacy and Trust in the IoT Environment*. 2019, Springer. p. 227-254.

[152] Al-Momani, A., F. Kargl, and C. Waldschmidt, *Physical Layer-Based Message Authentication in VANETs*. In GI/ITG KuVS Fachgespräch Inter-Vehicle Communication 2016, 31 March - 1 April, Humboldt-Universität zu Berlin, Germany. 2016.

[153] Lozupone, V., *Analyze encryption and public key infrastructure (PKI).* International Journal of Information Management, 2018. **38**(1): p. 42-44.

[154] Gianluca. Dini, *Lecture Notes Public Key Infrastructures Security in Networked Computing Systems*, U.o.P. Dept. of Ingegneria dell'Informazione, Editor. 2018: Pisa.

[155] Khodaei, M., *Secure vehicular communication systems: Design and implementation of a vehicular PKI (VPKI)*. PhD Dissertation. 2012.

[156] Crosby, M., et al., *Blockchain technology: Beyond bitcoin.* Applied Innovation, 2016. **2**(6-10): p. 71.

[157] Dib, O., et al., *Consortium blockchains: Overview, applications and challenges.* International Journal On Advances in Telecommunications, 2018. **11**(1&2).

[158] Nakamoto, S., *Bitcoin: A peer-to-peer electronic cash system.* White paper. *(2008)*.

[159] Buterin, V., *A next-generation smart contract and decentralized application platform.* White paper, 2014. **3**(37)

[160] Alonso, K.M., *Zero to Monero, First Edition a technical guide to a private digital currency; for beginners, amateurs, and experts.*

[161] Yaga, D., et al., *NISTIR 8202 Blockchain Technology Overview.* National Institute of Standards and Technology. Recuperado de: https://nvlpubs. nist. gov/nistpubs/ir/2018/NIST. IR, 2018. **8202**.

[162] Zheng, Z., et al. *An* overview *of blockchain technology: Architecture, consensus, and future trends*. in *2017 IEEE international congress on big data (BigData congress)*. 2017. Honolulu, HI, USA. IEEE.

[163] Schmid, P. *The Blockchain: What Is It? And Why Is It Important to Risk Management and Insurance?* 2017 [24 02 2020]; Available from: https://sandiegorims.org/membership/2017-conference-handouts/.

[164] *Blockchain for Business*. 2019 14 11 2018]; Available from: https://oneledger.io/

[165] Yakubov, A., et al. *A blockchain-based pki management framework.* in *The First IEEE/IFIP International Workshop on Managing and Managed by Blockchain (Man2Block) colocated with IEEE/IFIP NOMS 2018, Tapei, Tawain 23-27 April 2018*. 2018.

[166] Axon, L., *Privacy-awareness in blockchain-based PKI.* Cdt technical paper series, 2015. **21**: p. 15.

[167] Malik, N., et al. *Blockchain based secured identity authentication and expeditious revocation framework for vehicular networks*. in *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*. 2018. New York, NY, USA IEEE.

[168] Ren, D., S. Du, and H. Zhu. *A novel attack tree based risk assessment approach for location privacy preservation in the VANETs*. in *2011 IEEE International Conference on Communications (ICC)*. 2011. Kyoto, Japan. IEEE.