

Abou Bekr Belkaid University
Tlemcen, Algeria



جامعة أبي بكر بلقايد

تلمسان الجزائر

PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA

الجمهورية الجزائرية الديمقراطية الشعبية

MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH

وزارة التعليم العالي والبحث العلمي

FACULTY OF SCIENCES

DEPARTMENT OF COMPUTER SCIENCES

A Thesis

Presented for obtaining the degree of:

DOCTORATE

In: Computer Science

Specialty: Networks and Distributed Systems

By:

Messaoud **BABAGHAYOU**

Theme

Safety-Oriented Identity and Location Preservation in Internet of Vehicles

Thesis defended on June 08, 2021 at Tlemcen in Front of the Jury Composed of:

Mr Azzedine CHIKH	Full Professor	University of Tlemcen	President
Mme Nabila LABRAOUI	Associate Professor	University of Tlemcen	Supervisor
Mr Ado Adamou ABBA ARI	Associate Professor	University of Maroua	Co-Supervisor
Mr Mohamed FEHAM	Full Professor	University of Tlemcen	Examiner
Mr Bouabdellah KECHAR	Full Professor	University of Oran 1	Examiner
Mr Omar Rafik MERAD BOUDIA	Associate Professor	University of Oran 1	Examiner

Academic Year 2020/2021

“Everything has a reality, and the servant will not reach the reality of faith until he knows that what afflicted him could never miss him, and that what missed him could never have afflicted him.”

– Prophet Muhammad (PBUH)

Dedication

I proudly dedicate this thesis to:

- The sake of Allah, my creator and the creator of everything by whom I was blessed with the ability to learn & progress, the creativity and the reasoning & wisdom.
- My great teacher and messenger, Mohammed -May Allah bless him-, who taught us the purpose and guidelines to a better life.
- My family: Mother, Father and Sister. You were all the support that I relied and keep relying on to tackle the diverse life obstacles.
- Those who pushed me to keep working and doing the research activities even when things get stuck.
- All my Professors and every person who gave me tips, ways and knowledge till the moment this words are written.

– *Babaghayou Messaoud*

Acknowledgements

Firstly, all praise and thanks go to Allah who gave me the power and courage to conquer life challenges in general and to pursue my higher studies in particular; I am thankful.

I would like to give my sincere thanks to M^{me} Nabila LABRAOUI for accepting supervising me and for her continuous encouragements when I thought that I am facing a hard thesis times and when I got despairs. Also, my thanks go to Mr Ado Adamou ABBA ARI for accepting to be my co-supervisor and for his advises and tips regarding the academic research.

I am pleased and want to express my thanks to the jury members who accepted the invitation and whom their honorary presence will, with no doubt, give this modest thesis a valuable value. Thank you (1) Mr Azzedine CHIKH, whom we were lucky to have him back again as a real addition to the CS department, (2) Mr Mohamed FEHAM, one of the main pillars of our STIC Lab and the CS department, (3) Mr Bouabdellah KECHAR whose researches and contributions on the field of wireless networks and communications are indispensable and (4) Mr Omar Rafik MERAD BOUDIA who assisted with us in many events and activities organized in our STIC Lab despite his academic preoccupations.

I want to give my deep gratitude to Mr Mohamed LEHSAINI, the STIC lab head and our PhD Project Manager for giving me the opportunity to be part of their active group members in STIC and for giving me the chance to do the research activity that I liked.

I would like, with no doubt, to give my sincere gratitude to my family members:

- Dad, thank you for being strict with your rules since I was kid. It is now when I truly could see the full sight behind them where, after following them, I was able to conquer the life's hard circumstances including the moments related to this thesis's preparations.
- Mom, thank you for making me realize that I am worth much things in this world. You kept encouraging me against the obstacles that stand in front of my progress whether in this thesis or in general life, I am always appreciating it.
- Sister, thank you for being, in every time with me. Your interest and provided support had a positive impact in my successes in this thesis in particular and in other aspects in general. I will be returning this to you as well.

Without each one of you, I'd be nowhere near the person who I am right now (and the person who I am aiming for).

Additionally, I am not forgetting the people who I am consider as a support and were so dependable during my whole research work and thesis preparation I mention them as an example, not limited to: (1) Mr Nasreddine LAGRAA who was one of the important and wise teachers that I ever met in my study carrier, he also had a real impact on my PhD realized works with his continuous support even after graduating from the Master degree, (2) Mr Mohamed Amine FERRAG, he was one of the most vital and active researchers who had a big impact in my last research papers, he also guided and gave me a lot of advises to foster my PhD career and (3) Mr Leandros MAGLARAS, his research works and engagements do fairly describe his value not to mention his countless helpings for me when I got the hard times with the frustrating reviews and decisions, he kept giving me the enough support to continue the journey.

Finally, deepest thanks go to anyone who has had a significant impact on my graduation career, my personality and the things I've learned till now. You all have provided me the enough support, encouragement and motivation to keep going on my thesis. I would not be the person who I am today without you all, thanks again.

– *Babaghayou Messaoud*

Abstract

This thesis deals with the problem of identity and location privacy in the context of Internet of Vehicles (IoV) while making road-safety into consideration. This problematic emerged with the advent of different safety-achieving techniques provided by IoV applications. There exist many techniques that cope with the identity and location privacy problem but while sacrificing safety. In our thesis, we focus on the solutions that are based on the pseudonymity concept and many techniques related to this category were proposed. With this said, we provide a comprehensive survey that deals with the aforementioned problem. then, we propose three techniques that ensure high level of location privacy while considering road-safety as an objective. The obtained results show that road-safety can still be achieved in conjunction with location privacy while using our techniques.

keywords: IoV, VANET, identity and location privacy, road-safety, location tracking, pseudonym changing, silent period, transmission range changing techniques.

Résumé

Cette thèse traite le problème de la préservation de la vie privée de l'identité et de l'emplacement dans le contexte de l'Internet des véhicules (IoV) tout en prenant en compte la sécurité routière. Cette problématique est apparue avec l'avènement de différentes techniques de sécurité fournies par les applications IoV. Il existe de nombreuses techniques qui permettent de résoudre le problème de la confidentialité de l'identité et de l'emplacement, mais tout en sacrifiant la sécurité. Dans notre thèse, nous nous concentrons sur les solutions basées sur le concept de pseudonymat et de nombreuses techniques liées à cette catégorie ont été proposées. Cela dit, nous fournissons un état de l'art complet qui traite du problème susmentionné. Ensuite, nous proposons trois techniques qui garantissent un haut niveau de confidentialité de l'emplacement tout en considérant la sécurité routière comme un objectif. Les résultats obtenus montrent que la sécurité routière peut encore être obtenue en conjonction avec la confidentialité de l'emplacement tout en utilisant nos techniques.

mots-clés: IoV, VANET, confidentialité de l'identité et de l'emplacement, sécurité routière, suivi de l'emplacement, changement de pseudonyme, période de silence, techniques de changement de portée de transmission.

مُلخّص

تتناول هذه الأطروحة مشكلة المحافظة على خصوصية الهوية و الموقع في سياق إنترنت المركبات (IoV) مع إعطاء سلامة الطريق اعتبارًا مهمًا. ظهرت هذه المشكلة مع ظهور مختلف التقنيات المستعملة لتحقيق سلامة الطريق و التي توفرها تطبيقات IoV. توجد العديد من التقنيات التي تتعامل مع مشكلة خصوصية الهوية و الموقع ولكن مع التضحية بالسلامة. في أطروحتنا، نركز على الحلول التي تستند إلى مفهوم الاسم المستعار وتم اقتراح العديد من التقنيات المتعلقة بهذه الفئة. بناءً على هذا، نقدم مسحة شاملاً، في شكل دراسة حالة، يتعامل مع المشكلة المذكورة أعلاه. بعد ذلك، نقترح ثلاث طرق تضمن مستوى عالٍ من خصوصية الموقع مع مراعاة سلامة الطريق كهدف. أظهرت النتائج التي تم الحصول عليها أنه لا يزال من الممكن تحقيق سلامة الطريق جنبًا إلى جنب مع خصوصية الموقع أثناء استخدام تقنياتنا.

الكلمات المفتاحية: إنترنت المركبات (IoV) ، شبكة العربات المخصصة (VANET) ، خصوصية الهوية و الموقع، سلامة الطريق، تتبع الموقع، تغيير الاسم المستعار، الفترة الصامتة، تقنيات تعديل نطاق الإرسال.

List of Publications

Journal Publications

1) Messaoud BABAGHAYOU, Nabila LABRAOUI, Ado Adamou ABBA ARI, Mohamed Amine FERRAG, Leandros MAGLARAS and Helge JANICKE. "WHISPER: A Location Privacy-Preserving Scheme Using Transmission Range Changing for Internet of Vehicles". *Sensors*, 21.7, (2021), 2443. (A-Rank, IF=3.275)

<https://www.mdpi.com/1424-8220/21/7/2443>

2) Messaoud BABAGHAYOU, Nabila LABRAOUI, Ado Adamou ABBA ARI, Nasreddine LAGRAA and Mohamed Amine FERRAG. "Pseudonym change-based privacy-preserving schemes in vehicular ad-hoc networks: A survey". *Journal of Information Security and Applications*, 55, (2020), 102618. (A-Rank, IF=2.327)

<https://www.sciencedirect.com/science/article/abs/pii/S2214212620307833>

3) Messaoud BABAGHAYOU, Nabila LABRAOUI, Ado Adamou ABBA ARI and Abdelhak Mourad GUEROUI. "Transmission range changing effects on location privacy-preserving schemes in the internet of vehicles". *International Journal of Strategic Information Technology and Applications (IJSITA)*, 10.4, (2019), 33-54. (B-Rank)

<https://www.igi-global.com/article/transmission-range-changing-effects-on-location-privacy-preserving-schemes-in-the-internet-of-vehicles/252879>

4) Messaoud BABAGHAYOU, Nabila LABRAOUI and Ado Adamou ABBA ARI. "Location-privacy evaluation within the extreme points privacy (epp) scheme for vanet users". *International Journal of Strategic Information Technology and Applications (IJSITA)*, 10.2, (2019), 44-58. (B-Rank)

<https://www.igi-global.com/article/location-privacy-evaluation-within-the-extreme-points-privacy-epp-scheme-for-vanet-users/241867>

Conference Communications

1) Messaoud BABAGHAYOU, Nabila LABRAOUI, Ado Adamou ABBA ARI, Nasreddine LAGRAA, Mohamed Amine FERRAG and Leandros MAGLARAS. "SAMA: Security-Aware Monitoring Approach for Location Abusing and UAV GPS-Spoofing attacks on Internet of Vehicles". International Wireless Internet Conference (EAI WiCON), 2021. Canada. [Accepted]

2) Messaoud BABAGHAYOU, Nabila LABRAOUI, Mohamed Amine FERRAG and Leandros MAGLARAS. "Between Location protection and Overthrowing: A Contrariness Framework Study for Smart Vehicles". International Conference on Consumer Electronics (ICCE), 2021. Greece.

3) Messaoud BABAGHAYOU, Nabila LABRAOUI, Ado Adamou ABBA ARI, Mohamed Amine FERRAG and Leandros MAGLARAS. "Preserving the Location Privacy of Drivers Using Transmission Range Changing Techniques in Internet of Vehicles". The 4th International Symposium on Informatics and its Applications (ISIA), 2020. Algeria.

4) Messaoud BABAGHAYOU, Nabila LABRAOUI, Ado Adamou ABBA ARI, Mohamed Amine FERRAG and Leandros MAGLARAS. "The Impact of the Adversary's Eavesdropping Stations on the Location Privacy Level in Internet of Vehicles". 5th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM), 2020. Greece.

5) Messaoud BABAGHAYOU, Nabila LABRAOUI, Ado Adamou ABBA ARI, Nasreddine LAGRAA and Mohamed Amine FERRAG. "Security-Aware Monitoring Approach for Location Abusing and Suspicious Behavior in Internet of Vehicles". International Pluridisciplinary PhD Meeting (IPPM'20), 2020. Algeria. [Best Oral Presentation Award]

6) Messaoud BABAGHAYOU and Nabila LABRAOUI. "Transmission range adjustment influence on location privacy-preserving schemes in vanets". International Conference on Networking and Advanced Systems (ICNAS), IEEE, 2019. Algeria.

7) Messaoud BABAGHAYOU, Nabila LABRAOUI and Ado Adamou ABBA ARI. "EPP: Extreme Points Privacy for Trips and Home Identification in Vehicular Social Networks". JERI, 2019. Algeria.

Messaoud Bbaghayou: Contacts & Works

✉ BabaghayouMessaoud@hotmail.com


✉ messaoud.babaghayou@univ-tlemcen.dz

🎓 www.researchgate.net/profile/Messaoud-Babaghayou

🌐 sites.google.com/view/Messaoud-Babaghayou

🆔 orcid.org/0000-0001-9508-7134

Google Scholar
June 2021

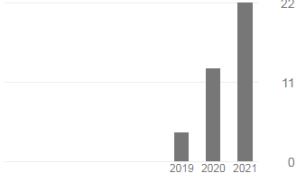


Messaoud Babaghayou
PhD student in vehicular ad-hoc networks security, Tlemcen University
 Verified email at univ-tlemcen.dz - [Homepage](#)
[identity and location privacy](#) [pseudonym change](#) [security in IoVs](#)

FOLLOW
GET MY OWN PROFILE

Cited by

	All	Since 2016
Citations	40	40
h-index	4	4
i10-index	1	1



TITLE	CITED BY	YEAR
Between Location protection and Overthrowing: A Contrariness Framework Study for Smart Vehicles <small>M Babaghayou, N Labraoui, MA Ferrag, L Maglaras 2021 IEEE International Conference on Consumer Electronics (ICCE), 1-5</small>	2	2021
SAMA: Security-Aware Monitoring Approach for Location Abusing and UAV GPS-Spoofing attacks on Internet of Vehicles <small>M Babaghayou, N Labraoui, AA Abba Ari, N Lagra, MA Ferrag, ... EAI</small>	2	2021
WHISPER: A Location Privacy-Preserving Scheme Using Transmission Range Changing for Internet of Vehicles <small>M Babaghayou, N Labraoui, AA Abba Ari, MA Ferrag, L Maglaras, ... Sensors 21 (7), 2443</small>	2	2021
The Impact of the Adversary's Eavesdropping Stations on the Location Privacy Level in Internet of Vehicles <small>M Babaghayou, N Labraoui, AAA Ari, MA Ferrag, L Maglaras 2020 5th South-East Europe Design Automation, Computer Engineering, Computer ...</small>	2	2020
Cyber security for fog-based smart grid SCADA systems: Solutions and challenges <small>MA Ferrag, M Babaghayou, MA Yazici Journal of Information Security and Applications 52, 102500</small>	14	2020
Security-Aware Monitoring Approach for Location Abusing and Suspicious Behavior in Internet of Vehicles <small>M BABAGHAYOU, N LABRAOUI, AA ABBAARI, MA FERRAG, ... International Pluridisciplinary PhD Meeting (IPPM'20)</small>	2	2020
Preserving the Location Privacy of Drivers Using Transmission Range Changing Techniques in Internet of Vehicles <small>M BABAGHAYOU, N LABRAOUI, AA ABBAARI, MA FERRAG, ... The 4th International Symposium on Informatics and its Applications (ISIA)</small>	2	2020
Pseudonym change-based privacy-preserving schemes in vehicular ad-hoc networks: A survey <small>M Babaghayou, N Labraoui, AA Abba Ari, N Lagraa, MA Ferrag Journal of Information Security and Applications 55, 102618</small>	3	2020
Transmission range changing effects on location privacy-preserving schemes in the internet of vehicles <small>M Babaghayou, N Labraoui, AAA Ari, AM Gueroui International Journal of Strategic Information Technology and Applications ...</small>	5	2019
Transmission Range Adjustment Influence on Location Privacy-Preserving Schemes in VANETS <small>M Babaghayou, N Labraoui 2019 International Conference on Networking and Advanced Systems (ICNAS), 1-6</small>	4	2019
EPP: Extreme Points Privacy for Trips and Home Identification in Vehicular Social Networks. <small>M Babaghayou, N Labraoui, AAA Ari JERI</small>	7	2019
Location-privacy evaluation within the extreme points privacy (epp) scheme for vanet users <small>M Babaghayou, N Labraoui, AAA Ari International Journal of Strategic Information Technology and Applications ...</small>	5	2019

Co-authors

- 

Nabila Labraoui
Université de Tlemcen, Algérie

>
- 

Ado Adamou Abba Ari, Ph.D.
University of Versailles Saint-Qu...

>
- 

Mohamed Amine Ferrag
Associate Professor (PhD, Habilli...

>
- 

Leandros Maglaras
Associate Professor / Reader in ...

>
- 

Mehmet Akif Yazici
Istanbul Technical University, Inf...

>
- 

Abdelhak Mourad GUEROUI
Maitre de Conférences, Universit...

>
- 

Nasreddine Lagraa
University of Laghouat

>
- 

Helge Janicke
Cyber Security Cooperative Res...

>

Table of Contents

Dedication	iii
Acknowledgements	iv
Abstract	vi
List of Publications	ix
Table of Contents	xii
List of Figures	xvi
List of Tables	xix
List of Algorithms	xx
List of Abbreviations	xxi
Preamble	1
1 General Introduction	1
2 Motivation	2
3 Problematic in a nutshell overall	3
4 Objectives & Contributions	4
5 Thesis Outline	5
PART ONE: LITERATURE REVIEW	10
Chapter I:	
Vehicular Networks and their Security: A Background	10
1 Preface	11
2 Initiation to Vehicular Networks	11
2.1 Wireless Technology: in a Glance	11
2.2 VANET Network	12

	2.2.1	Overview	12
	2.2.2	Architecture	12
	2.2.3	Features	13
2.3		IoV: A Novel Paradigm	14
	2.3.1	Overview	14
	2.3.2	Environment Awareness	15
	2.3.3	Implications on Road-Safety	16
2.4		The Technology in Practice	16
	2.4.1	Potential Applications	16
	2.4.2	Communication Model & Standards	17
3		Security Issues in IoV	17
	3.1	Security Requirements and Aspects	17
	3.2	Adversary’s Potentials and Strength	19
	3.2.1	Adversary Types	20
	3.2.2	Security Threats	21
	3.2.3	Research Efforts	22
4		Privacy Issues in IoV	23
	4.1	Privacy: A Crucial Parameter	23
	4.1.1	Privacy Requirements	24
	4.1.2	Privacy Metrics	26
	4.1.3	Privacy Implications on Safety	27
	4.2	Adversary Identity and Location Privacy	27
	4.3	Pseudonymity	28
	4.3.1	Pseudonym Schemes	28
	4.3.2	Pseudonym Lifecycle and Phases	30
	4.3.3	Pseudonym Requirements	31
	4.3.4	Radio-based Location Tracking Techniques	32
5		Summary	35

PART TWO: SCIENTIFIC CONTRIBUTIONS 57

Chapter II:			
Pseudonymity: A State of Art and Taxonomic Study			36
1	Preface		37
2	Extended Related Work		37
3	Pseudonym Change Taxonomy		48
	3.1 Comparison of existing strategies		49
	3.2 Our proposed taxonomy for pseudonym change strategies		49

3.3	The changing technique considerations	52
4	Summary	55
Chapter III:		
Location Privacy Evaluation for Trips and Home identification in VANET		57
1	Preface	58
2	Background	58
3	The Proposed EPP Strategy	60
3.1	Motivation	60
3.2	Deployment of Zones	60
3.3	Behavior of Vehicles in the System	62
3.4	Definitions and Properties	63
4	Simulation Setup and Results	64
4.1	The simulation runs	65
4.2	Scenario <i>I</i>	66
4.3	Scenario <i>II</i>	68
4.4	Scenario <i>III</i>	68
4.5	Privacy of Vehicles After Leaving the District	70
5	Location Privacy Protection and Overthrowing	72
5.1	Protecting Location Privacy, an Ego-Perspective	72
5.2	Overthrowing Location Privacy, an Adversary-Perspective	75
5.3	Summarizing the Impacts, a Descriptive Table	77
6	Summary	77
Chapter IV:		
Transmission Range Changing Effects on IoV Users' Location Privacy		79
1	Preface	80
2	Background	80
2.1	Network Model	81
2.1.1	Vehicles	81
2.1.2	Infrastructures	82
2.1.3	Authorities	82
2.1.4	Extension hosts/things	82
2.2	Adversary Model	82
2.3	Potential Privacy Attacks	82
3	Transmission-range Control Adaptation	83
3.1	Demonstration and Motivation of the Study	84
3.2	Choice of Transmission Powers	84

3.3	Pseudo-Algorithm of TRA	85
3.4	Complexity of TRA	85
3.5	Strong Points of TRA	87
3.6	Probable Drawbacks of TRA	87
4	Performance Evaluation	87
4.1	Simulation Setup	87
4.2	The impact of TRA on Location Privacy	89
4.2.1	The resulting traceability	90
4.2.2	The resulting confusions per pseudonym change	90
4.2.3	The resulting confusions per trace	91
4.2.4	The achieved maximum anonymity set size and maximum entropy per trace	91
4.3	The impact of TRA on Verified Beacons	92
5	Discussion, Comparison and Open Work Directions	93
6	Summary	95
Chapter V:		
WHISPER: a Safety-Aware and Location Privacy Scheme for IoV		97
1	Preface	98
2	Background	98
3	System Model	100
3.1	Network Model	100
3.2	Threat Model	102
3.3	Assumptions	103
3.4	Certificates Management	104
4	The Proposed WHISPER Strategy	105
4.1	System Initialization	105
4.2	Receiving Beacon Messages Protocol	108
4.3	Transmission Range Adjustment Protocol	109
4.4	Pseudonym Change Trigger Protocol	111
4.5	The Adversary's Achieved Traceability	113
4.6	The Adversary's Achieved Normalized Traceability	114
4.7	Pseudonym Consumption	115
5	Discussion and Future Work	116
6	Summary	118
Conclusion		119
Appendices		122
References		133

List of Figures

1	The diagram of this thesis' phases and chronology	8
2	VANET and its relation with other networks	12
3	VANET architecture and its main components	13
4	V2X technology illustration	15
5	BSM beacon format	15
6	Some of the essential security requirements	18
7	Pseudonym life cycle and its different phases	30
8	Linking the new changed pseudonym (used at t2) with the old one (used at t1)	33
9	Linking all pseudonyms that are changed simultaneously using prediction techniques	34
10	Exploiting beacons' information to do the semantic linking attack	34
11	The novel taxonomy of pseudonym change strategies	51
12	An Illustration figure for the proposed EPP Zones division	61
13	The abstract network and threat models in EPP	63
14	The three scenarios: <i>I</i> , <i>II</i> and <i>III</i>	66
15	Additional illustrations about the map	66
16	The simulation runs (scenarios*4)	66
17	The four simulations of scenario <i>I</i>	67
18	The four simulations of scenario <i>II</i>	69

20	The anonymity set size(ASS) off all VSN users in All scenarios	70
19	The four simulations of scenario <i>III</i>	71
21	The relationships between the different entities including the adversary	72
22	The location privacy protection from the ego-perspective	74
23	The location privacy Overthrowing from the Adversary-Perspective . .	76
24	Network model illustration	81
25	Adversary model illustration	83
26	A TRA functioning scenario	85
27	The taken portion of Tlemcen town, Algeria map	88
28	The illustrative diagram of the different used simulation tools	89
29	SLOW, CAPS, SLOW_TRA and CAPS_TRA traceability measuring .	90
30	SLOW, CAPS, SLOW_TRA and CAPS_TRA confusions per pseudonym change measuring	91
31	SLOW, CAPS, SLOW_TRA and CAPS_TRA confusions per trace measuring	92
32	SLOW vs. CAPS using the maximum anonymity set size per trace metric	93
33	SLOW vs. CAPS using the maximum entropy per trace metric	94
34	SLOW and SLOW_TRA network performance evaluation by sent and received BSM packets	94
35	CAPS and CAPS_TRA network performance evaluation by sent and received BSM packets	95
36	V2X technology illustration	99
37	BSM beacon format	99
38	The different entities of the vehicular network	101
39	Threat model and its resources, capabilities and coverage	102
40	The used coverage mode (moderate mode) details	103
41	The state diagram of WHISPER	107

42	WHISPER behavior in the presence and influence of general neighbors on the transmission range adjustment	109
43	WHISPER behavior in the presence and influence of road neighbors on the transmission range adjustment	109
44	WHISPER, pseudonym change process triggered by a close neighbor's status	112
45	The achieved traceability by SLOW, RSP, CPN and WHISPER within different densities	114
46	The achieved normalized traceability by SLOW, RSP, CPN and WHISPER within different densities	115
47	The pseudonyms consumption of CPN, WHISPER, RSP and SLOW within various densities	116

List of Tables

1	A set of standards that support the ITS applications	17
2	Comparison of existing strategies according to a set of metrics	50
3	The three scenarios used in the evaluation of EPP	64
4	The parameters of the district VSN users's departure, gateway and heading	65
5	The parameters of each scenario of VSN users's class	65
6	The map simulation details	65
7	The authority and the attacker and their influences on the application layers	77
8	The transmission range, the needed power and the triggering speed values of TRA	85
9	The simulation parameters	88
10	WHISPER keywords, concepts and detailed definitions	106
11	Simulation parameters and values	113
12	A brief comparison of SLOW, RSP, CPN and WHISPER strategies according to a set of metrics	117

List of Algorithms

1	Beacon Transmission Range Adjustment	86
2	Receiving Beacon	108
3	Sending Beacon	111
4	Checking Pseudonym Change Trigger	112

List of Abbreviations

AI Artificial Intelligence.

ASS Anonymity Set Size.

AU Application Unit.

BSM Basic Safety Message.

CA Certificate Authority.

CAM Cooperative Awareness Message.

Car2UAV Vehicle to Unmanned Aerial Vehicle.

CLL Candidate Location List.

CPN Cooperative Pseudonym Change.

CPS Coupling Privacy with Safety.

DENM Decentralized Environmental Notification Message.

DLP density-based location privacy.

DMLP Dynamic Mix-zone for Location Privacy.

DoS Denial of Service.

DSRC Dedicated Short-Range Communication.

DTN delay tolerant network.

ECDSA Elliptic Curve Digital Signature Algorithm.

EPP Extreme Points Privacy.

EPZ Endpoint Protection Zone.

ETSI European Telecommunications Standards Institute.

FANET Flying Ad-Hoc Network.

GPA Global Passive Adversary.

GPS Global Positioning System.

GW Gateway.

HD Heading.

HMAC Hashed Message Authentication Code.

IBC Identity-Based Cryptography.

IoT Internet of Things.

IoV Internet of Vehicle.

ITS Intelligent Transportation System.

LBS Location Based Service.

MMLPP Multiple Mix-zones with Location Privacy Protection.

MPSVLP Motivation for Protecting Selfish Vehicles' Location Privacy.

nO-TS-PP non-Overlapping Time-Slotted Pseudonym Pools.

OBU On-Board-Unit.

OMNeT++ Objective Modular Network.

OSM OpenStreetMap.

PCC Pseudonym Change based on Candidate-location-list.

PCS Pseudonym Change at Social pot.

PKI Public Key Infrastructure.

POI Point Of Interest.

PP Pseudonym Provider.

QoS Quality of Service.

REP random encryption periods.

RPC Random Changing Pseudonyms.

RSU Roadside Unit.

S2SI Silent & Swap at Signalized Intersection.

SLOW Silent at LOW speed.

SM Silent Mix-zone.

SPCP Synchronized Pseudonym Changing Protocol.

SUMO Simulation of Urban MObility.

TAPCS Traffic-Aware Pseudonym Changing Strategy.

TPD Tamper-Proof Device.

TRA Transmission Range Adjustment.

UAV Unmanned Air Vehicle.

UPCS Urban Pseudonym Changing Strategy.

V2C Vehicle to Cloud.

V2H Vehicle to Home.

V2I Vehicle to Infrastructure.

V2P Vehicle to Pedestrian.

V2V Vehicle to Vehicle.

V2X Vehicle to Everything.

VANET Vehicular Ad-hoc Network.

VID Vehicle Identifier.

VLPZ Vehicular Location Privacy Zone.

VSN Vehicular Social Network.

WANET Wireless Ad hoc Network.

WAVE Wireless Access in Vehicular Environment.

Preamble

1 General Introduction

As the world is proceeding faster towards the adoption of new technologies and innovations, we get the birth of different protocols, communication means, transport ways and even new learning methods. These are just few examples of what humanity, in this current era, is exploiting and focusing at. To this end, all of the governments, manufacturers and research communities are -intensively- doing the efforts of accelerating the development progress and the proposition of new solutions to nowadays challenges. Despite the promising solutions, many gaps are still open because not all of the provided solutions are holistic. This is in a part, in the other part some of these solutions do introduce other side-issues and side-challenges which lead to emerging vulnerabilities and, depending on the context, can put the whole technology domain into use-preservation, i.e., threatening the use of the technology itself. Among nowadays technologies, the domain of transportation systems is, undoubtedly, putting itself on top of the delicately-considered challenges. Noting that, most of the life-issues that are targeted for an enhancement do focus on safety (the absence of unreasonable risk of harm) as a primary goal.

2 Motivation

With the exponential growth of urbanism in one hand and the population explosion in the other hand, different scientific and governmental bodies are seeking for providing dependable means of transportation that are safe, smooth and entertaining (that considers the road-dangers, congestion and entertaining driving experience respectively). In light of this, many automobile projects were put into development where they focus on smart vehicles that are able to sense their environment (safety), minimize trips time and energy consumption (congestion-avoiding) and fulfill the comfort of the driver and his passengers (entertainment). To this extent, two categories are on the rollout phase: autonomous and semi-autonomous driving. The autonomous (like WAYMO ¹) category is based on giving the vehicle the full control on how to handle the given tasks such as driving from two points, taking a decision on a specific scenario, etc. This category is still under reservations due to events like: "Self-driving Uber kills Arizona woman in first fatal crash involving pedestrian" ². The semi-autonomous category, at the contrary, is getting much attention in where the main aim is to support the driver with wider vision, notification and mechanisms to enhance his driving experience. Some companies are already applying this category (Mercedes, Audi, Tesla, Hyundai, etc.). Safety of drivers are achieved with different means like using computer vision and letting vehicles be able to communicate between themselves. This later requires the vehicle to be equipped with embedded sensors and devices to both sense the external environment and exchange such information (like their exact locations) with the neighbor vehicles and that what boosted the safety efficiency of such a technology. The use of this technology opens new and different challenges related to the identity and

¹<https://waymo.com/>

²<https://www.theguardian.com/technology/2018/mar/19/uber-self-driving-car-kills-woman-arizona-tempe>

location privacy and are giving in more details in the next section.

3 Problematic in a nutshell overall

The integration of semi-autonomous vehicles with its wide range of applications had drastically mitigated the number of road-crashes and fatalities; thanks to the safety applications provided by this technology. Yet, the use of safety applications involves sending some sensitive data: the fine-grained location of the sending car is a good example. Additionally, the special characteristics of the sent data let the use of data-protective techniques be non-applicable, as an example: the use of encryption during sending this data to ensure that the neighbor vehicles are the only receivers is not recommended in the standardization efforts of the research community which lets this data be receivable by anyone who has the necessary receiving devices that work in the same WIFI frequency band as the other vehicles.

With this said, the willingness of adopting the technology by automobile consumers is at stake. Now to have a pretty good idea on what exploits can an unauthorized person do are represented in: knowing the succession of locations of the sending car, keeping the history of the one's trips, knowing whether he is at home or not, knowing his political and religious directions, being able to track him in real time which can result in a crime. These are just for example but not limited, thus, many other critical exploits can be executed. Obviously, privacy advocates are opposing the integration of such a double edged sword technology as long as privacy is not ensured with dependable means.

4 Objectives & Contributions

While all of the industry, governments and research bodies are seeking for robust mechanisms to deal with the identity and location privacy resulted from the integration of such intelligent vehicles, a holistic privacy-solution is still not provided. To reiterate, despite the large body of the proposed schemes that aim at solving the identity and location privacy, no holistic solutions are provided. This kept the work be ongoing to reach a certain level of privacy (maximizing the privacy) while still providing safety.

As a result, the main contributions of this thesis are stated as follows (and explained in the next "Thesis outline" section):

- 1- *Location-privacy evaluation within the extreme points privacy (epp) scheme for vanet users*: gives the first contribution in kind of a privacy scheme that takes a district in Tlemcen, Algeria as an environment for evaluating this privacy scheme. The chapter does also provide a conceptual framework study to demonstrate and describe the location privacy in two perspectives: the defender and the attacker.
- 2- *Transmission range changing effects on location privacy-preserving schemes in the internet of vehicles*: suggests and evaluates the transmission range changing technique on two of the already proposed privacy schemes by the literature. The motivation behind this study is that the transmission range changing technique was not exploited before in the context of identity and location privacy of vehicle users.
- 3- *Whisper: A location privacy-preserving scheme using transmission range changing for internet of vehicles*: proposes a novel identity and location privacy scheme that is built upon the technique of transmission range

changing that is tackled in its preceding chapter but this time: the novel scheme's protocols synchronize at the aim of exploiting the transmission range changing technique while doing the pseudonym changes to remarkably-rise the privacy level of vehicle users.

With this said, and as stated earlier in the examples of privacy-exploitation, we are aiming for evaluating, studying the characteristics and providing novel solutions to the identity and location privacy in the domain of automobile but, concurrently, taking road-safety as a main objective (without its sacrificing).

5 Thesis Outline

This thesis deals with the identity and location privacy problem and is composed of two main parts: (a) LITERATURE REVIEW in where we give an introduction to the stated problem accompanied with an exhausted related work study and this is done in two chapters. While in the second part (b) SCIENTIFIC CONTRIBUTIONS, we start by proposing solutions and giving contributions on the same research field and this is done in three chapters. Thus, a composition of five chapters per thesis.

The thesis begins with the LITERATURE REVIEW and is outlined as follows:

- Chapter 1 starts by giving basic notions on vehicular networks, their security, the privacy issues in general and the pseudonymity in particular; that is a preface to the whole thesis.
- Chapter 2 dives into the identity and location privacy problematic where a detailed state of the art is given with a large body of related work followed by a novel taxonomy for the pseudonym change schemes and a comparative table for some recent pseudonym change schemes. At the end, the chapter

gives important concepts and conclusions at the aim to provide directions for the future privacy-preserving schemes.

Right after that preliminary entry, the thesis continues with a SCIENTIFIC CONTRIBUTIONS part which is outlined as follows:

- Chapter 3: Location Privacy Evaluation for Trips and Home identification in VANET (contribution 1).
- Chapter 4 Transmission Range Changing Effects on IoV Users' Location Privacy (contribution 2).
- Chapter 5 WHISPER: a Safety-Aware and Location Privacy Scheme for IoV (contribution 3).

Each chapter, is based on at least one scientific publication and the last three chapters (i.e., of the SCIENTIFIC CONTRIBUTIONS part) are devoted to bring forth identity and location privacy schemes and solutions. In light of this, we mention at each chapter's end the scientific publication(s) and/or the communication paper(s) from where the chapter is built upon.

In the final stage, we give a general conclusion to the thesis as whole, a discussion to the identity and privacy problematic and future work that this thesis had given as insights.

In the followings, we give, in more or less, the different work phases of this thesis in addition to its chronology: we target the privacy problematic (Identity and Location privacy "evaluation" and "schemes") and dived -slightly- in treating a specific security issue that is related to location data falsification (Location abusing "detection"). An illustration in form of a diagram is shown in Figure 1 and a brief description is given below:

Noting that (a) "**Ext**" refers to "an extended version", (b) "**Chx**" to "Chapter

x", (c) "/" not included in the thesis due to the work's irrelevance to this thesis' exact topic or for lower importance and (d) "*" for an ongoing work(s).

Identity and Location privacy schemes

- EPP: Extreme Points Privacy for Trips and Home Identification in Vehicular Social Networks.
- Location-privacy evaluation within the extreme points privacy (epp) scheme for vanet users. [Ext, Ch3]
- Transmission range adjustment influence on location privacy-preserving schemes in vanets.
- Transmission range changing effects on location privacy-preserving schemes in the internet of vehicles. [Ext, Ch4]
- Preserving the Location Privacy of Drivers Using Transmission Range Changing Techniques in Internet of Vehicles.
- WHISPER: A Location Privacy-Preserving Scheme Using Transmission Range Changing for Internet of Vehicles. [Ext, Ch5]

Identity and Location privacy evaluation

- Pseudonym change-based privacy-preserving schemes in vehicular ad-hoc networks: A survey. [Ch1, Ch2]
- The Impact of the Adversary's Eavesdropping Stations on the Location Privacy Level in Internet of Vehicles. [/]
- Between Location protection and Overthrowing: A Contrariness Framework Study for Smart Vehicles. [Ch3]

Location abusing detection

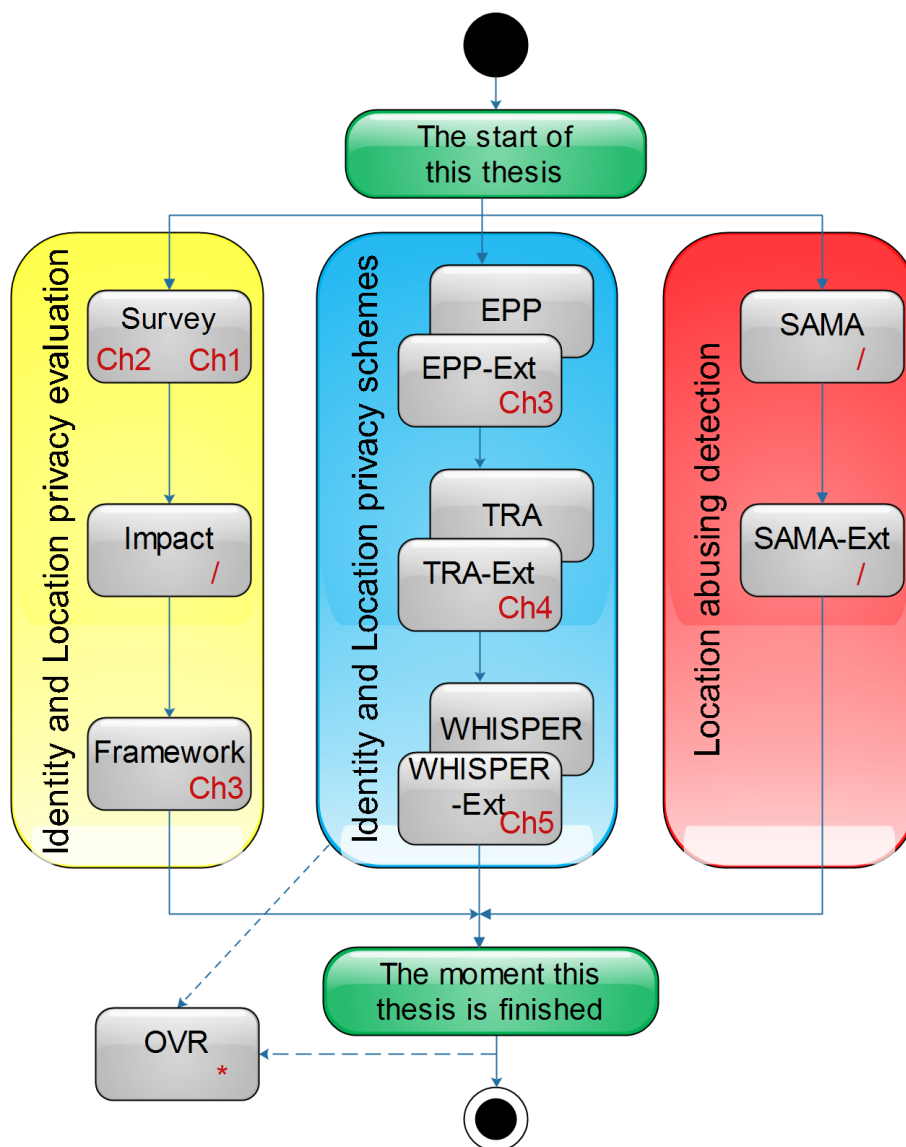


Figure 1: The diagram of this thesis' phases and chronology

- Security-Aware Monitoring Approach for Location Abusing and Suspicious Behavior in Internet of Vehicles. [/]
- SAMA: Security-Aware Monitoring Approach for Location Abusing and UAV GPS-Spoofing attacks on Internet of Vehicles. [Ext, /]

Post-thesis work(s)

- A Safety-Friendly and Road-Congestion Monitoring Location Privacy-Preserving Scheme For IoV. [*]

PART ONE: LITERATURE REVIEW

*Chapter I: Vehicular Networks and their
Security: A Background*

*Chapter II: Pseudonymity: A State of
Art and Taxonomic Study*

*Chapter I:
Vehicular Networks and their Security:
A Background*

“The way to get started is to quit talking and begin doing.”

– Walt Disney

1 Preface

This preliminary chapter aims at giving a start-up setup to both: the LITERATURE REVIEW part and the thesis as whole. Starting with basic notions, we provide an introduction to the vehicular networks technology where we spot light on two categories: Vehicular Ad-hoc Network ([VANET](#)) and Internet of Vehicle ([IoV](#)) with their applications and communication models. Additionally, we highlight the implications of the technology on road-safety. Next, The chapter details the security issues that are emerging as challenges against a successful IoV deployment. Later on, the chapter dives deeply on the privacy issues in IoV and sheds light on the pseudonymity solution. We give a summary on the current chapter at the last stage, that is the summary section.

2 Initiation to Vehicular Networks

Over the past few decades, the world had witnessed a huge evolution in different sides (e.g., the wireless communication technologies area and automobile industry), this had let all of the government, industry and the research community to start thinking on how to get benefit from this evolution to overcome the current world challenges [1]. The augmentation of the vehicles number and the implications (road safety, traffic efficiency, congestion problems, etc.) are good examples for such challenges [2]. In addition to these problems, there are also comfort-related problems that aim at providing entertainment for both the driver and his passengers like connection to the internet, sharing files, real-time conversation between drivers, etc.

2.1 Wireless Technology: in a Glance

Wireless communications are in no more or less a new technology. Its first appearance was in 1897 with the wireless telegraphy demonstrations done by Marconi which was followed by a radio reception across the Atlantic Ocean in 1901 and that was a big step towards nowadays advancement [3].

In these passed hundred years, a bunch of Wireless systems had emerged and vanished at the same time. The television transmission, previously, was broadcasted wirelessly using radio transmitters but was replaced with cable transmission afterwards. In the same way, the point-to-point microwave circuits that was forming telephone network backbone are currently replaced by optical fiber.

In both previous examples, the appearance of new wired technologies (like optical fiber) had contributed in the transition into wired options. Yet, today has an opposite effect: wireless technologies like cellular technologies are overwriting the wired telephony networks especially in the case where these wired networks are not well-developed. Also, it is crystal clear that the world is rushing towards wireless technologies like 5G and 6G. [4]

2.2 VANET Network

2.2.1 Overview

The yearly damages caused by vehicular accidents (which is 1.3 million deaths with \$518 billion costs in the globe [5]) let the emerging of VANET to exploit the advances in the field of wireless communications. Its main creation purpose is to reduce the overall costs in terms of lives and in economy [6]. Moreover, the unique nature of ad-hoc networks which allows the fast spread of information let VANET, that is extended from MANET [7], be considered as an appropriate wireless network that is used to solve the previous problems [8]. Figure 2 gives the position of VANET according to some other networks like MANET which is, by itself, a subclass of Wireless Ad hoc Network (WANET) [9]. With this in mind, VANET inherits most of the characteristics of WANET where the shared wireless medium present a lot of issues and vulnerabilities as will be shown next.

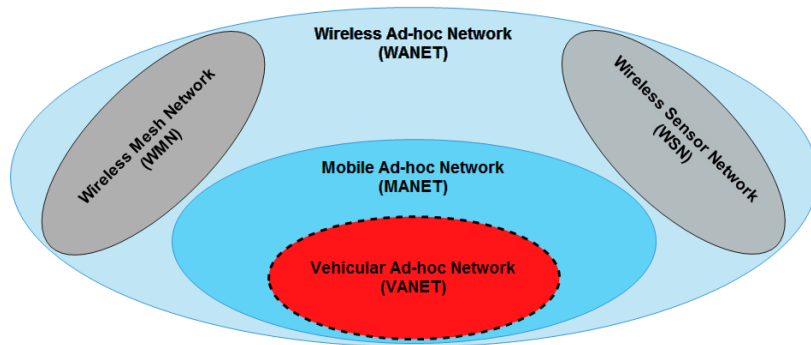


Figure 2: VANET and its relation with other networks

2.2.2 Architecture

Communications inside VANET need a predefined architecture. The vehicle, which is the essential element in this network, must be equipped with an On-Board-Unit (OBU) that allows it to transmit over the wireless medium, namely the Wireless Access in Vehicular Environment (WAVE) [10]. OBUs are used to exchange data

between VANET components. Another equipment which may be used in coordination with the OBU is the Application Unit (AU), the role of this device is to connect and communicate with other services in the network [11]. In the components other than vehicles we may find:

- B) Cell phones (sometimes referred to pedestrians)
- C) Unmanned Air Vehicle (UAV) [12, 13], a drone/Flying Ad-Hoc Network (FANET) system that may assist the VANET system
- D) Roadside Units (RSUs), which are devices fixed right in the roadside
- F) Cell towers (3/4/5/6G [4, 14] technologies provided to VANETs)
- G) Different kinds of servers (location, authentication, application servers) [15]

Figure 3 shows the previous VANET components and the various modes of exchanges between them.

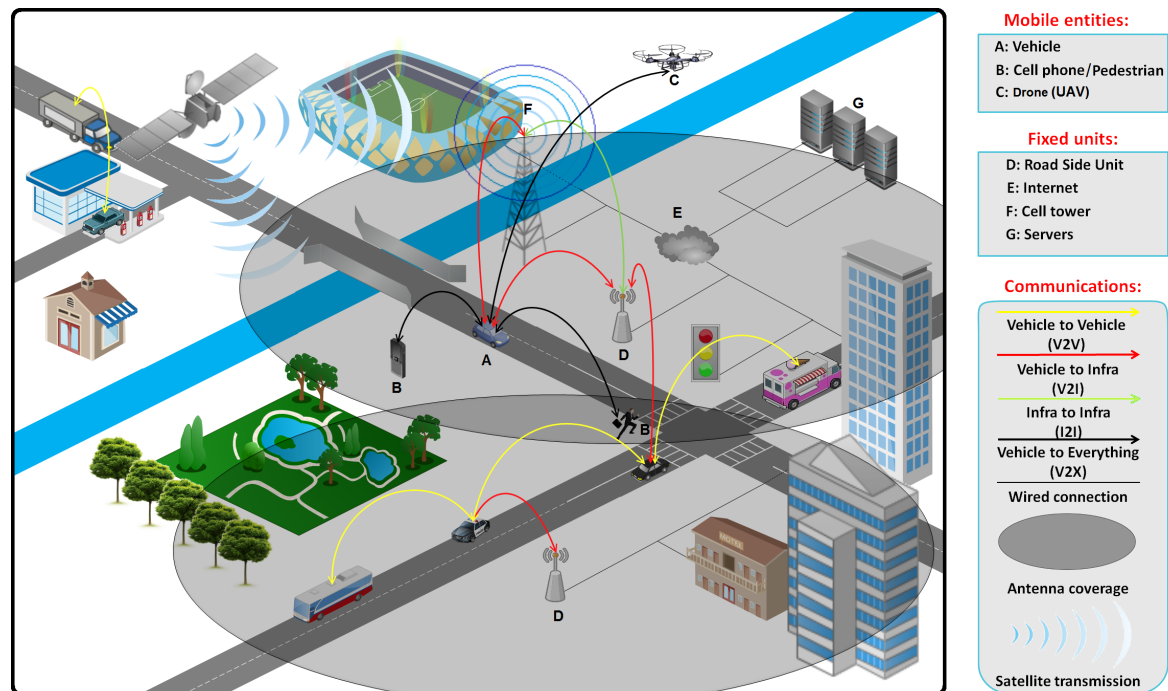


Figure 3: VANET architecture and its main components

2.2.3 Features

VANET is a subclass of MANET, this results in an inheritance of most of MANET characteristics. However, due to the characteristics of VANETs [16, 17], there exists the following special features:

1. No energy constraints: the big amount of battery energy with the on-the-driving recharge ability remove the energy constraint that is not existing in most of the other wireless networks.
2. Fast topology change: since the speeds of vehicles are remarkably high, the frequency of topology changes resulting in influencing some fundamental functionalities such as routing algorithms and congestion applications.
3. High Computational ability: strong and modern CPUs are used which result in efficient and non time-consuming calculations [18].
4. A non-static network density: because the topology is changing so fast as stated before, this results in the variation of network density spatial and/or temporal.
5. A known mobility pattern: since the movement is restricted by roads and highways, it is likely to be easily predictable.
6. Safer and comfortable driving: because of the communication ability between vehicles, ensuring an environment awareness between them for the safety sake becomes possible [19].
7. A non-secure communication medium: because of the wireless medium's nature, the security of the wirelessly exchanged information is going to be challenging.

2.3 IoV: A Novel Paradigm

2.3.1 Overview

IoV is emerging as a promising paradigm in Intelligent Transportation Systems (ITS) to enhance and exploit the existing VANETs by entailing the Internet of Things (IoT) [20, 21]. IoV is a vehicular network model which consists of vehicles, users and other smart devices connected to the network and aims to provide various safety, road-management as well as comfort applications and services [22]. By doing this, they are able to exchange information and to fulfill both network efficiency and road safety requirements. The exploiting of infrastructures can also be used to enhance the communications between the vehicles especially in sparse scenarios. There exist two types of communications over the Dedicated Short-Range Communication (DSRC) protocol are enabled: Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) [23]. Figure 4 shows the Vehicle to Everything (V2X) external communications and internal equipments. A vehicle using V2X is able to enhance the road-safety

by broadcasting, through its OBU, a status-form beacon message named the Basic Safety Message (BSM) with a 300m range with a frequency of 1 to 10 BSMs per second according to the standardization [24]. The data included in BSMs are illustrated in Figure 5. This lets vehicles be aware of the potential dangers coming from the nearby vehicles in addition of giving the option to manage road-congestion through the implemented RSUs. Noting that the BSM concept is considered in the U.S. standard while for the European standard, we find both (a) the Decentralized Environmental Notification Message (DENM) for event triggered messages and (b) Cooperative Awareness Message (CAM) for periodically exchanged messages [25].

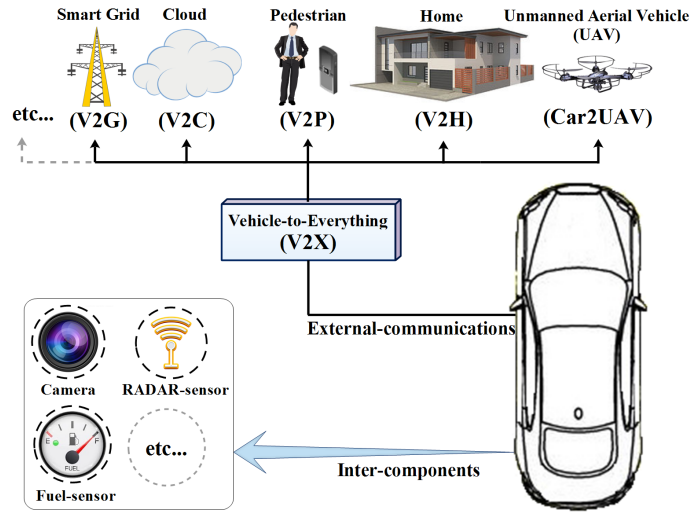


Figure 4: V2X technology illustration

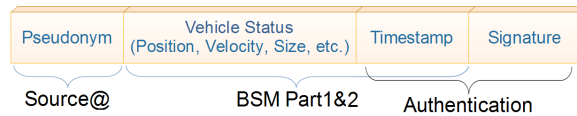


Figure 5: BSM beacon format

2.3.2 Environment Awareness

IoV comes to assist the design of Vehicular Ad-hoc Networks (VANETs) that focus on reducing the number of fatalities by enabling V2V and V2I communications over the DSRC protocol [26] in addition to the various Vehicle-to-Everything (V2X) communications [27]. Thus, fast reactions may be taken by drivers during the dangerous situations. To achieve this goal, each vehicle has to periodically broadcast its status in terms of location, speed, velocity, time, etc. placed in a beacon message. This kind of beacon is called BSM [28]. Despite the interesting V2X applications like

vehicle platooning, incorporated sensors and automated driving, vehicles suffer from some serious security and privacy vulnerabilities and issues.

2.3.3 Implications on Road-Safety

Despite being the privacy mechanisms, especially those basing on the pseudonym change, beneficial to the user's privacy to some extent, they also open safety issues since being in silent periods, which will be discussed later in more details, lets the vehicle be invisible not just from the tracker but also from nearby legitimate vehicles and this leads to both fooling the tracker and those nearby vehicles. Also, exchanging the used pseudonyms between vehicles has the same effect which will endanger the users' safety as stated by the European Telecommunications Standards Institute (ETSI) in "ETSI TR 103 415" standard [29] that also discusses the current existing project working on the aspect of pseudonym change (for a more details, we redirect the reader to the "ETSI TR 103 415" standard); that is the "trade-off" between privacy and safety.

2.4 The Technology in Practice

2.4.1 Potential Applications

The different types of sensors and the Global Positioning System (GPS) device give the vehicle the ability to know its environment through collecting and processing the gathered information. Then, spreading it to other vehicles that are in the vicinity [30]. Thus, other potential IoV applications are suggested by the researchers under a bunch of IoV projects and they are up to be implemented. We can distinguish two main application categories:

- *Safety related applications*: their main objective is to make decisions, warn the driver about the situation [31], improve road safety and to avoid as much accidents and fatalities as possible. There are lots of safety related applications including: emergency electronic brake light, traffic signal violation warning, pre-crash sensing, lane-change warning and others. [30]
- *Entertainment/infotainment (or non-safety) related applications*: In some works, they are splitted into (1) *Entertainment* and (2) *Traffic Efficiency Applications*. This category of applications aims at achieving a good level of traffic management and infotainment for both the driver and his passengers [32]. A set of non-safety applications can be: co-operative navigation, global internet service, speed management, etc. [33]

2.4.2 Communication Model & Standards

As mentioned in the VANETs architecture section, the protocol suite used by vehicles to communicate is WAVE. The protocol layers of WAVE are well-stated in the conducted work done in [33] by Karagiannis et al. IoV exploits VANETs, these later consist of different communication types, V2V and V2I are the most used. Therefore, the DSRC emerged and went through several standardization phases to well-fit the vehicular wireless nature; coming with promising features (3 to 27 Mbps as a transfer rates, a low latency to operate in a range up to 1 Km, etc.). The DSRC was accompanied by the 1609 (described in Table 1) standards family to solve some issues like establishing communications in various channels. There is a variety of vehicular communications other than V2V and V2I, the general term to describe such communications is Vehicle to everything (V2X), where it creates a vast research area (V2P for Vehicle to Pedestrian, V2N for Vehicle to Network, etc.)

Table 1: A set of standards that support the ITS applications

Standard	Description
<i>IEEE 1609.1</i>	Provide OBUs with the ability to use external resources to enhance their calculation potentials
<i>IEEE 1609.2</i>	Secure message formats in WAVE
<i>IEEE 1609.3</i>	The WAVE network layer (routing and addressing tasks)
<i>IEEE 1609.4</i>	Appends the multi-channel operation to the IEEE 802.11p
<i>IEEE 802.2</i>	The Logical Link Control (LLC) in the link layer
<i>IEEE 802.11p</i>	Physical and MAC layers management and an improvement of the IEEE 802.11 standard to permit the WAVE protocol

3 Security Issues in IoV

The main objective of IoV is to ensure both safety and entertainment with various safety related and non-safety related applications respectively. However, if the communications used in the IoV is not secured, the results will be disastrous in terms of fatalities and economically. This is due to the different types of attacks that may be launched against these networks, and that is why the study of security attacks, requirements and countermeasures ought not to be neglected [6, 34].

3.1 Security Requirements and Aspects

In VANETs, a set of security requirements must be guaranteed [9, 35, 36]. The most important requirements are presented in Figure 6 and defined as follows:

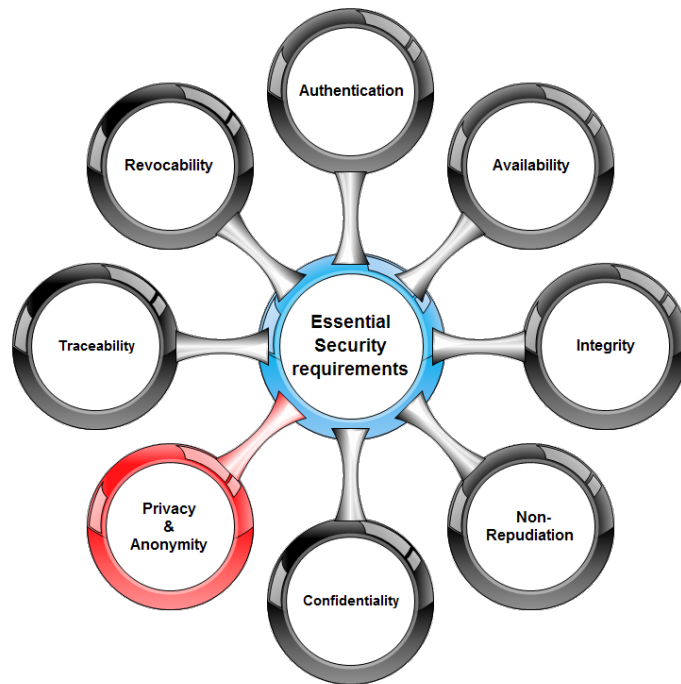


Figure 6: Some of the essential security requirements

Authentication: when a node (vehicle) receives a message, it must be able to know if the generated message is from a legitimate sender or not. This is mostly done using the verification of the sender’s signature which may add a certain amount of latency. Therefore, this process has to be done in as short period as possible using fast authentication schemes [37].

Availability: Despite the high mobility and the existence of some security attacks (e.g., Denial of Service attacks that is going to be shown next), the network must always be available for receiving/sending messages especially for the safety-related messages.

Integrity: it means that the delivered message must not be altered by a malicious node. Integrity is relevant to the authentication, where the verification of the received message tells if it is correct or corrupted (altered or not respectively).

Non-Repudiation: where the real sender of a message must not be able to deny the fact that he was the origin of that sent message. The proof would be assured via cryptographic techniques (based on the private key used for signature).

Confidentiality: during the communication, only the concerned members involved in this communication have to be able to decrypt the messages; a good example is

the group members' broadcasts, no other than this group can read the messages. Yet, in safety-related messages, the encryption is not recommended due to the additional latency. So, confidentiality is not considered as an important characteristic for safety-related applications.

Privacy and Anonymity: the driver's personal information ought to be kept private and protected against unauthorized access. Due to the nature of the wireless medium[38], it becomes hard to achieve a total privacy because the security related messages are sent in clear due to the latency problem when is encrypted, that is why there is a big trade-off between privacy and security. Privacy has strong relations with anonymity, where the anonymity refers to the ability to prevent the unauthorized entities from physically identifying the originator of the messages, and by consequence, matching the identifier used in the message with the person's real identity. This causes some serious problems when the attacker tracks his target basing on his car's broadcasts (the periodic locations are sent in clear due to the safety-applications requirements). This lets privacy be considered as one of the essential security requirements.

Traceability: it must be possible to know the origin of the safety message and to trace it at any given time. However, this ability must be preserved to authorized entities like the Law Enforcement Authority (glslea). The safety messages are supposed to be kept in the Event Data Recorder (glsedr) [35].

Revocability: it means the exclusion of a misbehaving node from the network. Actually, this depends on the responsible decision of the authority. According to the research work performed in [39] Wasef et al., there are two revocation mechanisms: centralized and decentralized revocation which means either by a specific authority or by the node's neighbors respectively.

3.2 Adversary's Potentials and Strength

Before we proceed to the real problem, it is important to know the features and characteristics of the environment that the driver is dealing with. The adversary type in addition to what kind of attacks he can execute are very important factors to make better decisions and countermeasures.

3.2.1 Adversary Types

There are a lot of adversary/attacker types as stated in [9, 40, 41, 42]. They can be classified, according to the research papers and our observation, based on the following perspectives:

- 1- **"Actively" (Active or Passive):** An active attacker can alter, remove or generate new messages in order to affect the performance of the network. On the contrary, a passive attacker does not do more than eavesdropping the exchanged communications. Thus, he cannot directly harm the network.
- 2- **"Behaviourally" (Malicious or Rational):** The primary objective of a malicious attacker is to execute a destructive attack that damages the network with various methods. The rational attacker aims to achieve a personal benefit from his attack. This means his actions are more predictable than those of a malicious attacker.
- 3- **"Locationally" (Insider or Outsider):** The insider attacker is an authenticated member in the IoV network . He is by then able to perform a lot of serious attacks on the network [43]. Whereas the outsider attacker does not have the ability to directly participate in the network. Hence, the insider attacker is more dangerous than the outsider one.
- 4- **"Proprietarily" (Global or Local):** A global adversary controls a large area in terms of radio stations deployed across the network. Thus, he can easily detect the mobile entities inside the covered area (also called region of interest). The local adversary controls less network entities than the global one; hence, he is limited in terms of the covered area. The utilization of the collected data may vary, we see some dangerous attacks resulting from the unauthorized data collection in the next chapters.
- 5- **"Movably" (Static or Dynamic):** The adversary's eavesdropping stations are either put fixed in some specific spots or moving across the observed map. The strength of each of these kinds depends on the used mechanisms and algorithms. The moving ones need a delicate processing (e.g., moving to follow a specific node) which is hard to be ensured. But, it is useful in the case where the adversary has few stations. On the other hand, the fixed stations do not need a lot of management except the synchronization and the sharing resources management.

This one provides the adversary with a good monitoring ability if he has enough stations to cover an area. If not so, then he cannot monitor whatever he wants.

- 6- “Occasionally” (Permanent or Temporal):** The adversary could be seen as a permanent or a temporal observer of the covered area. A permanent observer is more dangerous due to the fact that he gathers data and eavesdrops the different communications that occurs all the time. Contrary, a temporal observer would just eavesdrop at some period of times depending on his interests, intentions and benefits.

3.2.2 Security Threats

The nature of the shared wireless network grants the attacker the ability to execute and launch diverse attacks. Each attack has its specific characteristics and benefits. Many researches done in this scope had highlighted the potential attacks that may exist in this area [7, 9, 36, 39, 44, 45]. Because our work is dealing more with location privacy, we recall the attacks that mainly affect the privacy of individuals as follows:

1. *Denial of Service*: in the Denial of Service (**DoS**), the attacker focuses on paralyzing the targeted service [46]. In this scope, it may be the service responsible of delivering the set of pseudonyms used by vehicles to ensure their privacy.
2. *Eavesdropping attack*: in where the attacker eavesdrops (i.e., listens to) the transmitted packets over the shared wireless medium. This attack can be seen as a preamble to other critical attacks that are based on the collected data.
3. *Identity disclosure*: in identity (or ID) disclosure attacks, the malicious node reveals the location of its neighbor node. In most cases, it does this after being infected by a virus [9] sent by the attacker at the aim of getting the current location of a specific node. By this, he targets the node’s neighbor (or neighbors) where it periodically discloses its neighbor’s location. It is clear that this attack strongly breaches the privacy of drivers.
4. *Location tracking*: because of the periodic broadcasts imposed by safety applications, the attacker can read the location of his target vehicle [47] after eavesdropping its safety broadcasts (beacons). He can later benefit from a lot of private data like the real identity of the driver, the frequent visited places and other sensitive information. We will talk about location tracking and other

privacy related issues (the pseudonym linking attacks) in the next section.

5. *Malware attack*: as viruses and malwares infect computers, vehicles are also susceptible to be infected by malwares. Thus, an anti-malware framework should be further developed in order to be deployed on the different entities (i.e., OBUs, RSUs, etc.). The malware can expose the individual's most critical and secret data such as his location, heading and so on.
6. *Man in the middle attack*: in such attacks, the attacker interferes in the communication between two other nodes; he firstly eavesdrops the communication, then, he acts as the other part involved in the communication so that he can intercept and reply to each side with his own created packets (the original two parts do not know that they are dealing with an attacker) [48]. The attacker can also extract private data that is related to the individuals' privacy.
7. *Masquerade attack*: in order to exploit the network, the attacker impersonates a legitimate node (faking his authentication by taking a legitimate identity of another authenticated node) then he executes a lot of attacks, like extracting privacy related data, that could not be done without being authenticated.

3.2.3 Research Efforts

To provide the right solution against a specific attack, it is recommended and important to know the characteristics of that attack in its exact context.

In [45], Laurendeau and Barbeau. classified the different attacks according to the appropriate security requirement. They categorized them into attacks related to availability (DoS, malware, etc.), authenticity (masquerading, GPS spoofing, etc.) and confidentiality (eavesdropping, location tracking).

Mokhtar and Azab classified in [36] the attacks according to the targeted network layer (Application, transport, network, link and physical layer). They mentioned the most serious attacks with the corresponding solutions basing on the operating layer.

Another interesting research is that of [9], where La and Cavalli made a detailed survey on the attacks, their characteristics and their convenient countermeasures. We mention some of them: as in the bogus information attack, they recalled that the Elliptic Curve Digital Signature Algorithm ([ECDSA](#)), which is a message authentication scheme, is the suitable solution for this kind of attacks. Or, in the DoS

attack, the solution is to base on a particular processing unit which is a support for the OBU. This piece indicates to the OBU that it is under a DoS attack resulting in a necessity to switch the current communication channel for example. Also, for black hole attack, they pointed out that allowing more than one route for the packet delivery is an acceptable solution.

Finally, despite the diverse and large number of attacks that are threatening the security, there are a lot of efforts that were undertaken to intercept these attacks. The most satisfying and used solution is that of the Public Key Infrastructure (PKI) schemes [7, 49] where it uses cryptographic techniques based on public and private keys in order to secure the end-to-end communications [50]. However, PKI itself cannot solve all security related issues. For example, it cannot protect from the location tracking (discussed in more details in the next section) because the location of vehicles must remain revealed for safety-related requirements. It is also important to mention that cryptographic techniques add a remarkable latency which is not so suitable for safety applications .

4 Privacy Issues in IoV

Because the employing of IoV comes to provide safety, entertainment and traffic management efficiency, vehicles need to broadcast their status in terms of identifier, position, velocity and other useful information. However, from the position information gotten after an eavesdropping, an adversary can easily track the vehicle and identify its driver [51]. This can only be a preamble to sensitive information that breaches the driver's personal life and his privacy, as an example: from the collected traces, the attacker will be able to know all the driver's trips, health condition, political and religious direction, people who is dealing with, etc. and this is a crucial factor that, if it is not considered seriously, going to affect the adoption of IoV especially by privacy advocates.

4.1 Privacy: A Crucial Parameter

There is no doubt that the privacy of the driver must be rigorously maintained. The common solution to provide an acceptable level of privacy is the use of "pseudonyms". Pseudonyms are a replacement of the real identifier that is used in the beacon messages. They solve the problem of driver identification when dealing with a basic adversary but when it comes to an advanced adversary, this latter can identify the driver even

while using pseudonyms by analyzing the trajectory of its vehicle and the history of its trips and hence, he links his pseudonym with his real identifier [52]. In order to break the continuous linkage of the vehicle's locations, the use of pseudonyms change techniques must be performed and this is considered as an acceptable solution for the aforementioned privacy issue [53, 54]. To get a good idea about the problem of privacy, we state the most important characteristics that should be considered. With this said, the location privacy and pseudonym change techniques are described in the following subsections.

4.1.1 Privacy Requirements

When we come to the question of how to quantify the achieved location privacy in the VANET scope, a set of various proposed metrics arises. Among the most relevant metrics we find the following ones as in the research of Wagner and Eckhoff. [55]:

1. *Set of Anonymity Size (SAS)* : It refers to the indistinguishability of a target vehicle in comparing to other vehicles in the same context. This metric is characterized by its simplicity in terms of calculation and imposition of the privacy problem. Also, it highly depends on the total number of the existing vehicles. It is important to mention that this metric does not describe the anonymity level in all scenarios because the adversary may find out that the tracked vehicle is not fully undistinguishable by observing the heading direction, velocity, power of the used signal and other features to determine and identify it successfully.
2. *Entropy (Ent)*: This metric emerged just after finding that the SAS is not a well-describing metric. Thus, researchers trended towards the entropy metric which refers to the uncertainty in a random variable [55]. By combining this concept with the SAS, we find that the entropy is just the measure of a vehicle's anonymity inside the set; i.e., not all vehicles are alike in terms of being the target inside that set [56]. The Entropy's formula is given in Equation 12.

$$H_p = - \sum_{i=1}^{|AS|} p_i \log_2 p_i \quad (1)$$

Where $|AS|$ refers to the SAS and p_i refers to the probability of vehicle i being the target. The more the vehicles are equally in the probability of being the target, the more the entropy metric gives its highest value H_{max} which is described in Equation 13.

$$\forall i : p_i = \frac{1}{|AS|}, H_{pmax} = - \sum_{i=1}^{|AS|} p_i \log_2 p_i = \log_2 |AS| \quad (2)$$

3. *The degree of anonymity (d)*: It treats the scenario where the adversary, at the beginning, has no knowledge about the vehicle's anonymity set. Here, the expected value of the measure would not be equal to that of the other scenario where he already has a certain amount of knowledge. Hence, the degree of anonymity (d) was proposed in [57] which aims to normalize the evaluated anonymity. (d) is described in Equation 14.

$$d = 1 - \frac{H_{max} - H}{H_{max}} = \frac{H}{H_{max}} \quad (3)$$

4. *Adversary's Success Rate (ASR)*: As the adversary's exact purpose may change depending on his interests, knowing exactly what he is looking for would be more significant. Thus, the adversary's success rate concerns the privacy property targeted by the adversary against a specific vehicle. Despite the meaningful results that are revealed after applying this measurement, it also introduces some challenges. As an example, a significant question emerges: "does the adversary really target the supposed privacy property?". In sum, this metric only works in the case of applying it according to what exactly the adversary is searching for.
5. *Maximum Tracking Time (MTT)*: In most cases, the main goal of an adversary is to achieve the longest vehicles tracking time as possible. Thus, this measurement concerns the ability of that adversary to accumulatively tracking the vehicles. Additionally, it supposes that performing a pseudonym change at a certain time will make the adversary become confused. Unfortunately, this metric does not consider the case where the adversary uses additional techniques like probabilistic conclusions and benefits from an historic paths log of his target that is recorded/obtained earlier.
6. *Statistics on Pseudonym Change (SPC)*: From its name, statistics on pseudonym change metric aims to measure anything that has a relation with pseudonym changes like the total number of successful pseudonym changes; i.e., the unlinkability [58]. This metric had only investigated the unlinkability property in most researches that used it [55].

It is extremely important to point out that not every metric is applicable to all pseudonym change strategies. The nature and the characteristics of the pseudonym change strategy are the only key that determines the correctness and applicability of such metrics. Therefore, it does not make sense to compare between a set of strategies that are not studied using the same metrics, and telling which strategy is the best in this scenario would not be significant.

4.1.2 Privacy Metrics

Before employing pseudonyms, we need to ensure a set of properties to fulfill the different IoV requirements and to avoid unwanted abnormalities that may occur and lead to putting the network functionality down [41]:

1. **Distinct identity:** Each vehicle must have a unique pseudonym at a given time. To ensure this property, the use of a strong and coherent cryptographic mechanism to generate (i.e., not to overlap with other vehicles' pseudonyms) and maintain pseudonyms is needed.
2. **Ensuring availability of pseudonyms:** At a specific time, if a vehicle needs a new pseudonym that pseudonym must be available. A common way to achieve this would be by storing a large set of pseudonyms in the OBU.
3. **Ensuring limited duration of pseudonyms:** The use of a pseudonym must not be infinite because, if it is so, the location tracking attack will be easily performed by an adversary. To force the discontinuity of using a pseudonym, adding a duration time to the signed certificate that accompanies the used pseudonym would solve the problem.
4. **Identity full change:** If a vehicle decides to change its pseudonym, it must change all its other identifiers used recently in its communication layers stack; because changing one identifier and letting the others would be useless and renders the breaking of its anonymity an easy job. In this way, the adversary links the new pseudonym with the old one according to his analysis and matching of the other communication layers' identifiers.
5. **Pseudonym change block ability:** The frequent changes and the overuse of pseudonyms cause several problems like the *Sybil attack* and the *high overhead* respectively. Thus, stopping pseudonym change must be assessed by the corresponding authorities or by a strong reputation system that can detect and

remove any malicious vehicle from the system if it breaches this feature.

4.1.3 Privacy Implications on Safety

Despite being the privacy mechanisms, especially those basing on the pseudonym change, beneficial to the user's privacy to some extent, they also open safety issues since being in silent periods, which will be discussed in details later, lets the vehicle be invisible not only to the tracker but also to the nearby legitimate vehicles which leads to both fooling the tracker and those nearby vehicles. Also, exchanging the used pseudonyms between vehicles has the same effect which endangers the users' safety as stated and detailed in "ETSI TR 103 415" standard [29] that also discusses the current existing project working on the aspect of pseudonym change (we redirect the reader to the "ETSI TR 103 415" standard for a more details); that is the "trade-off" between privacy and safety.

4.2 Adversary Identity and Location Privacy

The identity privacy is the act of preventing unauthorized entities from knowing the real identity of the driver. We mean by unauthorized entities the different entities other than the trusted authorities [59]. keeping the identity hidden must be conditional due to the fact that revealing the real identity is mandatory in case of a revocation or resolution process launched by a law authority after observing a suspicious behavior of one of the vehicles. The other concept is Location privacy which is defined as the ability to prevent other entities from knowing the current and/or past location of an individual [60]. Besides, location services play a vital role nowadays in different areas (e.g., informing the user about the nearest hotel, a less-congested road suggestion, etc.) they also cause privacy issues by revealing the user's location in an appropriate circumstance.

Individuals do not want their location to be exposed especially in sensitive areas [61], thus, giving them the option to be invisible is likely to let them feel safer [62]. The fact of the possibility to know the exact location of an individual at a specific time will bother him. Moreover, knowing all his exact location during a wide duration that occurred in the past few days may expand his worries and annoyance enormously. Thus, location privacy must be maintained carefully by only letting the allowed parties to have the ability to get the location of the individual and preventing (or limiting) as maximum as possible the unwanted parties from getting such sensible

location information. There are other privacy models like interest privacy, backward privacy, content oriented privacy and other models [63]. We only described the two models; namely identity and location privacy. Due to their indispensable importance in VANETs, the majority of drivers want to get a good level of such privacy models. Among the most interesting solutions to ameliorate both identity and location privacy we find pseudonym schemes deployment. It is worth mentioning the efforts of the pseudonym management standardization like that of the "ETSI TR 103 415" standard [29].

4.3 Pseudonymity

Instead of using one static identifier all the time; which fosters the tracking and the identification of that vehicle, the use of different identifiers, the so called pseudonyms, must be employed. Basically, a set of pseudonyms is stored in the OBU. This set plays the role of useable identifiers that enhances enormously the driver's privacy. There are a lot of proposed schemes to achieve high privacy levels basing on the use of pseudonyms.

4.3.1 Pseudonym Schemes

To achieve a robust communication system with a high level of privacy, the need to implement effective pseudonym schemes arises. The desired schemes should base on cryptographic techniques that fulfill the privacy requirements. Due to the importance of such schemes, many works and suggestions were done in this scope. Petit et al. [41] had mentioned four pseudonym schemes, namely asymmetric cryptography, symmetric cryptography, group signature and Identity-based cryptography schemes. These schemes are described as follows:

4.3.1.1 Asymmetric cryptography schemes

Asymmetric cryptography or often called public key cryptography is based on pair of keys mechanism. One key is public; used to encrypt data or to verify the digital signature set in the packet. The second key is private; used to decrypt the encrypted data or to make digital signatures. Moreover, among the main characteristics of asymmetric cryptography we find the mathematics bind between these two keys [7]. Even though asymmetric cryptography provides high efficiency, it also introduces an additional overhead and requires big computational processes which do not fit the real-time applications and constraints of IoV.

4.3.1.2 Symmetric cryptography schemes

Symmetric cryptography schemes are characterized by their high efficiency in the authentication phase and do not consume a lot of computational time as asymmetric cryptography does. The symmetric cryptography uses a Hashed Message Authentication Code ([HMAC](#)) to authenticate messages. This is done by hashing the message and a secret key. For that, the other nodes, who aim to verify the validity of the received message, must also have the private key in order to use it for verification and to send their own messages as well. There is an interesting benefit from this technique which is the extension of its anonymity set because every node that knows the private key can generate valid authenticated messages letting it be indistinguishable. However, this breaches the accountability requirement because this scheme implies the impossibility of achieving the non-repudiation of the sender [41].

4.3.1.3 Group signature schemes

Because using a set of pseudonyms has a bad impact in terms of generating, delivering, storing and verifying these pseudonym certificates, the group signature schemes mainly base on the self-creation of signatures used to sign the message by a group member. This message can be verified by a common group public key. It enormously reduces the overhead since the need of other authorities and entities like the Certificate Authority ([CA](#)) or the Pseudonym Provider ([PP](#)) becomes mostly unnecessary. However, the group manager should determine the real identity of the sender inside that group because he is responsible for providing the group member secret key used in the communication [64].

4.3.1.4 Identity-based cryptography schemes

Identity-Based Cryptography ([IBC](#)) resembles the asymmetric cryptography in where they both use a key to encrypt the sent data [65] except that the key in IBC is the identifier itself of the node. In what concerns the private key, it can be generated (by authorized entities) from the same identifier of that node. By this notion, the verification of any message only requires the knowledge of the sender's public identifier [41]. In this scheme, the need for a centralized trusted authority to manage private keys is necessary to prevent the unappropriated nodes from deriving and generating private keys from a specific identifier, thing which breaches the authenticity requirement. By this way, the node's authenticity is well-guaranteed due to the fact that the centralized

trusted authority gives the node its private key that will work with its public identifier.

For a detailed description of the aforementioned schemes, we redirect the reader to the survey of Petit et al. [41] since authors had focused on the those pseudonymous schemes in their research work.

4.3.2 Pseudonym Lifecycle and Phases

Despite the large proposed schemes that could be used to achieve pseudonymity, there are always phases that accompany the use of pseudonyms. To provide vehicles with pseudonyms, and to ensure an acceptable functionality of the system, the lifecycle (called abstract pseudonym lifecycle in [41]) shown in Figure 7 must be respected. The different phases are explained as follows:

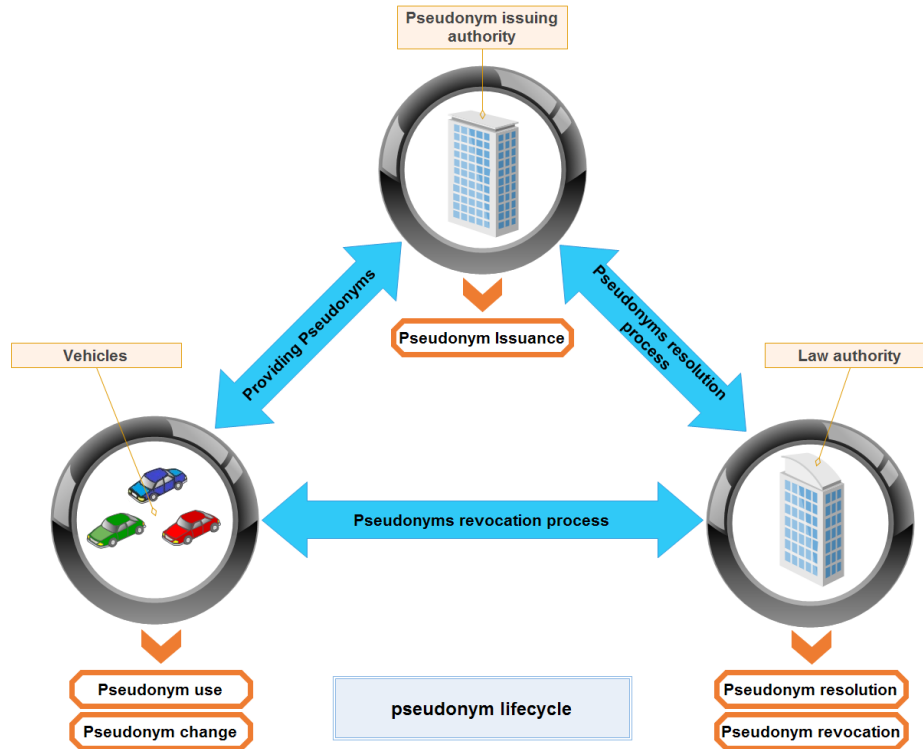


Figure 7: Pseudonym life cycle and its different phases

1. *Pseudonym issuance*: In order to let the vehicle be able to communicate inside the system, it needs to be authenticated. This is done by authenticating its OBU using the Vehicle Identifier (VID); a long-term signed certificate and pre-installed in the vehicles OBU [41]. Using its VID, a vehicle gets the ability to obtain pseudonyms, if necessary, from the pseudonym issuance authority after contacting it. Thus, the authentication step is a must before obtaining valid pseudonyms.

2. *Pseudonym use:* After acquiring a set of pseudonyms, a vehicle can use one of those pseudonyms in its ordinary broadcasts and communications. Pseudonyms are used to (a) sign the outgoing packets; i.e., for authenticating its messages. And to (b) verify the incoming packets to ensure that the received packet is valid. This signature and verification are ensured by the cryptographic mechanisms that respect the general security requirements.
3. *Pseudonym change:* Because the use of one pseudonym all the time leads to critical security issues such as location tracking that was described before, the need for changing pseudonyms is an absolute necessity. However, this change must respect a set of rules and must be maintained carefully because a pseudonym change performed in an inappropriate location/moment will just consume the pseudonyms set and add additional overhead while requesting new pseudonyms which decreases the performances of the system. We will see pseudonym change in more details in the next sections.
4. *Pseudonym resolution:* when the law authority wants to know the identity of a sent message's holder, it requests a pseudonym resolution process from the pseudonym issuing authority. The reasons may vary, so it depends on the case, but it will not change the result of this request which is the acquisition of the VID. Therefore, it reduces the individual's privacy considerably.
5. *Pseudonym revocation:* Sometimes, a vehicle may not use its authentication properly; we talk about the case of a malicious node. If the monitoring authority, like the law authority, detects an illegal behavior from one or more vehicles inside the system, it may proceed to the pseudonym resolution process [66] in order to know the exact identity of the sender. Afterwards, it revokes its pseudonym. The scenario where the vehicle uses its other stored pseudonyms to continue participating in the system must also be maintained. Thus, a mechanism to find out all of the vehicle's pseudonyms and revoking them must be ensured.

4.3.3 Pseudonym Requirements

Before employing pseudonyms in IoV, we need to ensure a set of properties to fulfill the different requirements and to avoid unwanted abnormalities that may occur and lead to drop the system functionality down [41]:

1. **Distinct identity:** Each vehicle must have a unique pseudonym at a given time.

To ensure this property, the use of a strong and coherent cryptographic mechanism to generate (i.e., not to overlap with other vehicles' pseudonyms) and maintain pseudonyms is needed.

2. **Ensuring availability of pseudonyms:** At a specific time, if a vehicle needs a new pseudonym that pseudonym must be available. A common way to achieve this would be by storing a large set of pseudonyms in the OBU.
3. **Ensuring limited duration of pseudonyms:** The use of a pseudonym must not be infinite because, if it is so, the location tracking attack will be easily performed by an adversary. To force the discontinuity of using a pseudonym, adding a duration time to the signed certificate that accompanies the used pseudonym would solve the problem.
4. **Identity full change:** If a vehicle decides to change its pseudonym, it must change all its other identifiers used recently in its communication layers stack; because changing one identifier and letting the others would be useless and renders the breaking of its anonymity an easy job. In this way, the adversary links the new pseudonym with the old one according to his analysis and matching of the other communication layers' identifiers.
5. **Pseudonym change block ability:** The frequent changes and the overuse of pseudonyms cause several problems like the *Sybil attack* and the *high overhead* respectively. Thus, stopping pseudonym change must be assessed by the corresponding authorities or by a strong reputation system that can detect and remove any malicious vehicle from the system if it breaches this feature.

4.3.4 Radio-based Location Tracking Techniques

Due to the severity of knowing the one's location, and what it implies from threatening his life in some cases, preventing the adversary from getting the exact location and the trajectory of that individual becomes imperative. The Adversary's methodology and tracking techniques may diverse. However, the one that we focus on in our work is that of the *Radio-based Location Tracking Techniques*.

Such techniques do benefit from the feature of beaconing used by vehicles [58]. Because the vehicle broadcasts safety messages with a high frequency, an eavesdropper can easily exploit the broadcasted safety messages and knows a lot of information that facilitates the process of gathering and storing the vehicles' success locations and

the corresponding pseudonyms used during its trip. We give two examples of such techniques as follows:

A.1) *Syntactic linking attack*: By continuously hearing the wireless shared medium, the adversary tends towards monitoring all the vehicles by eavesdropping their safety messages. More precisely, by focusing on (1) the pseudonym and (2) the time it was used in. If a pseudonym change happens, the adversary looks after the recently disappeared pseudonym and matches it with the newly one resulting in identifying the same vehicle that had changed its pseudonym. This attack becomes stronger when the vehicles do not perform the pseudonym change synchronously. In the other case, a synchronized pseudonym change will render this attack useless. Figure 8 shows how the adversary can link pseudonyms changed (from 178 to 203) by just one vehicle where Psd means pseudonym, $[A,T]$ means [Pseudonym value, corresponding time] and Δt means the time difference between the two time instants.

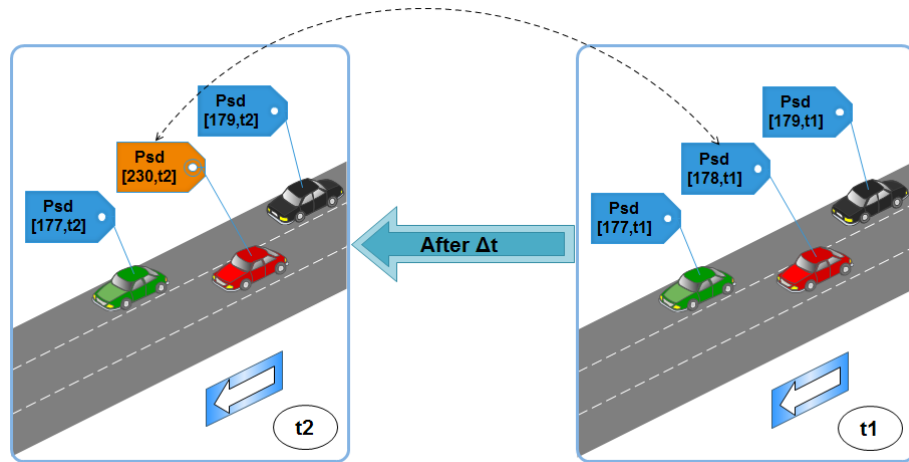


Figure 8: Linking the new changed pseudonym (used at t_2) with the old one (used at t_1)

A.2) *Semantic linking attack*: It also exploits the information inside the safety messages. Even if the pseudonym change is done synchronously, the adversary can still identify and matches each new pseudonym with its corresponding old one. This is due to the fact that a safety message contains the vehicle's location and velocity which gives the adversary the ability to predict the vehicle's next position. Moreover, the higher the frequency of beacon messages is, the better is the achieved precision by the adversary. An illustration of this attack in Figure 9 shows that even changing pseudonyms simultaneously at an instant t_2 the

adversary can still be able to resolve the matching (using prediction techniques). Thus, this kind of adversaries is more dangerous than that of the linking attack.

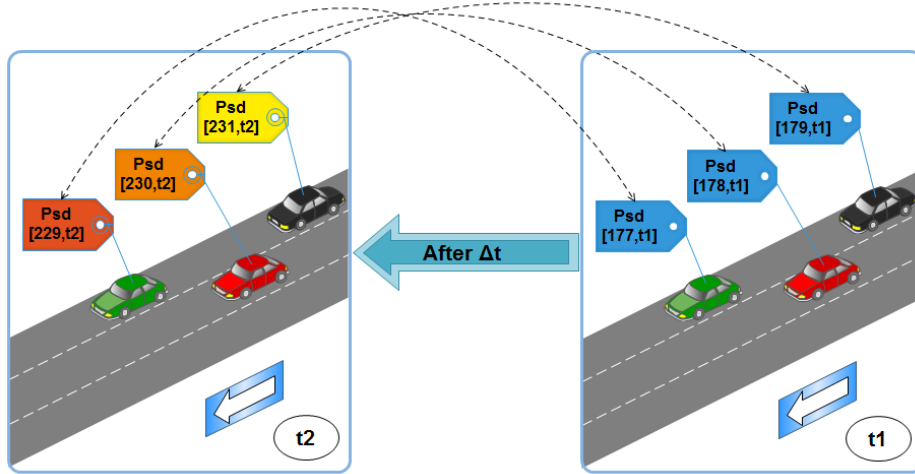


Figure 9: Linking all pseudonyms that are changed simultaneously using prediction techniques

The exploited fields in the beacon messages to predict the next position are generally: the x & y geographic coordinates, the timestamp and the velocity of the vehicle. Figure 10 shows that the adversary predicted the next position of the three vehicles V1, V2 and V3. According to that, he could match each vehicle's old and new pseudonyms.

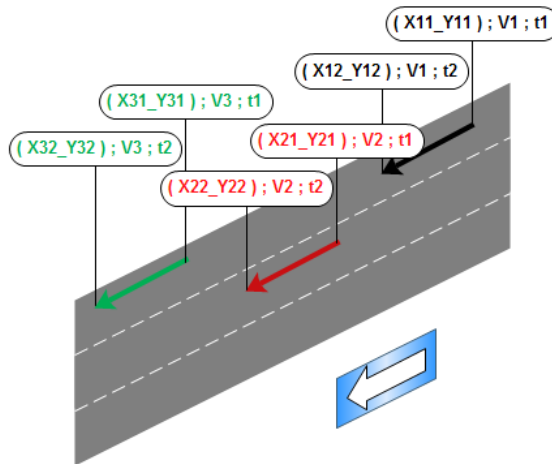


Figure 10: Exploiting beacons' information to do the semantic linking attack

5 Summary

In this chapter, we presented the fundamentals about vehicular networks technology: VANET and IoV with a focus on the modus-operandi of these technologies. Another aspect was put into light: the security issues that are threatening the successfulness of the technology where privacy-related attacks and the pseudonymity concept were given. In the next chapter, we see the privacy in IoV with an extensive and detailed state of the art.

Journal and Conference Papers Related to the Chapter

Jr) Pseudonym change-based privacy-preserving schemes in vehicular ad-hoc networks: A survey

Messaoud BABAGHAYOU, Nabila LABRAOUI, Ado Adamou ABBA ARI, Nasreddine LAGRAA and Mohamed Amine FERRAG. "Pseudonym change-based privacy-preserving schemes in vehicular ad-hoc networks: A survey". Journal of Information Security and Applications, 55, (2020), 102618. (A-Rank, IF=2.327)

Chapter II:
Pseudonymity: A State of Art and
Taxonomic Study

*“Errors, like straws, upon the surface flow; He who
would search for pearls, must dive below.”*

– John Dryden

1 Preface

In this chapter, we -continuously- dive through the privacy in IoV problematic. Initially, we give an extended and large literature review of the most recent related work in a chronological way. This study focuses on privacy-preserving and pseudonymous schemes which emerged during the last two decades. Following that, the chapter provides a comprehensive comparative table of some of the aforementioned pseudonymous schemes alongside a novel taxonomy to classify them according to a new perspective. This chapter also draws important concepts at the aim of making a solid base for the future pseudonym change schemes that are going to be proposed. Finally, we give a summary on this current state-of-art-oriented chapter.

2 Extended Related Work

The problems of re-identification and location tracking come generally from the supplementary information provided either by the car's transmitted messages under the corresponding protocol (e.g., the BSMs under WAVE) or by querying the Location Based Service (LBS) [67]. Stopping the generation of such sensitive information (the fine-grained locations of the vehicle) is not a suitable solution due to the fact that such information would enormously serve the individual and the whole system [60], and that what made a lot of researches and projects arise. Using and keeping one identifier by a vehicle for its diverse communications inside the system is not acceptable for sure according to the standardization and as discussed previously. Using pseudonyms instead and making them temporary changed is fair enough to achieve a better privacy level. However, a simple change of these pseudonyms is not sufficient because of some techniques used by the adversary to link pseudonyms and even reveal the real identity of the driver. We present in the following, an exhaustive and chronological state of the art of a large body of privacy-preserving and pseudonymous schemes emerged during the last two decades:

In [68], Sampigethaya et al. propose CARAVAN, a scheme that employs the group forming technique and the use of silent periods between pseudonym changes. Indeed, because forming groups not only reduces the amount of redundant transmissions but, also gives the vehicles other than the leader the ability to stay silent, which for sure, enormously enhances the privacy of vehicles. However, this technique may only be employed in a probe vehicle scenario where the vehicles may stay silent for quite

long periods without beaconing safety-messages. Additionally, the general case and standardization enforce the safety-message broadcasts in a high frequency so as to meet the requirements of safety-applications. Also, the leader's privacy is not fulfilled since it communicates all the time instead of its members.

Huang et al. [69] explore the silent period concept that can be used either temporally (at a variable time) or spatially (at a fixed location). After taking the MTT metric in their study, they showed that using silent periods brings a good enhancement to the privacy of wireless nodes.

Because the user-centric approach, which mainly bases on the vehicle's independent desire, lacks synchronization, Li et al. [70] present the Swing protocol that aims at increasing the number of vehicles changing their pseudonyms at an appropriate opportunity. They also present an amelioration of the Swing protocol; the use of the Swap protocol that enables the exchange of pseudonyms instead of a simple change. However, as they mentioned it, the exchange process is not suitable due to the accountability requirements (revocation, resolution of pseudonyms) and the management of identities. Hence, swap will highly depend on the infrastructure at any pseudonym exchange action (if we suppose that the exchange feature would be allowed).

Sampigethaya et al. [71] define the AMOEBA scheme that uses the group navigation as an advantage by letting vehicles belong to a group and only the group leader is able to communicate, on behalf of other members, with the LBS. Therefore, vehicles not only benefit from an extended silent period but also dispense with the redundant data that may be broadcasted by vehicles in the same vicinity. Authors also introduced the potential breaches of privacy that may occur while using the AMOEBA scheme which highly relies on the group concept; that has a set of vulnerabilities caused by the disclosure of one group member, like giving the group key used in communication to the adversary. This last one is the worst scenario that introduces a lot of privacy and security issues.

CMIX [72] is an another pseudonym change strategy that was proposed by Freudiger et al. that uses the idea of mix-zones, in addition to the encryption feature where vehicles inside the mix-zone encrypt their safety messages in order to prevent the adversary from accessing and reading the location information set in the packet. It is mainly formed by three phases: establishing the symmetric key by an RSU, ensuring

the forward of this key to coming vehicles before they reach the mix-zone and finally the key update management where the RSU generates a new key (mostly when the traffic density reduces) and ensures the deliverance of that key to the CA (in case of a potential resolution or revocation process). Despite the effectiveness of this strategy against the unauthorized collection of location traces done by the adversary, the strategy introduces a set of challenges like the overhead minimization and synchronizing the key management between RSUs to let only one symmetric key in the system.

Gerlach and Guttler employ the Mix-context strategy [73] that uses an algorithm which aims at letting vehicles change their pseudonym synchronously when they meet some specific triggers. By adding a flag (or bit, “called ready to change flag”) in the normal beacon messages, the vehicle can show its desire and need for a pseudonym change operation and all other vehicles having the same desire will collaborate to make a synchronous pseudonym change.

In an earlier time (2003), Beresford et al. adopt the mix-zone concept [60] in pervasive computing, which is defined as a spatial region where the node would not provide any location information to other entities (even to location applications). The key in this technique is to perform the pseudonym change inside that zone so that the adversary would be confused because of the existing vehicles at the same time inside the zone. Once the vehicle leaves the zone, the adversary would not be able to distinguish it from the other vehicles that entered the zone. However, a high scale zone is not recommended because the adversary would estimate the time needed for a vehicle to leave that zone. Also, a low density zone helps the adversary to identify vehicles even after performing the pseudonym change. Basing on the same concept, Buttyán et al. [74] evaluate the effectiveness of the mix-zone against an adversary that has already some knowledge about the used technique to face location tracking. They found after various simulations that the achieved level of privacy highly depends on the strength of the adversary where the stronger the adversary is, the less privacy level is achieved. The optimal deployment of the mix-zones is an open issue and has a high impact on the provided location privacy and it was investigated by other researchers like Freudiger et al. in [75].

Chaurasia and Verma investigate in [76] the real anonymity of a vehicle inside a set of vehicles (z zone in their work) and found that before joining the anonymity zone, the old communications used by a vehicle have a negative impact on the indistinguishability

of that vehicle from its neighborhood vehicles due to the non-uniform probability distribution. Thus, not all vehicles inside the zone are really contributing to the effective privacy level. According to that, they proposed a heuristic pseudonym change that aims at finding the right time and place when there are a certain number of neighbors in order to maximize the anonymity with only few (optimal) pseudonym changes.

Buttyán et al. provide a pseudonym change strategy called **SLOW** [77] (Silent at LOW speed). In SLOW, vehicles stop broadcasting safety messages when their speed drops below a certain threshold. It is true that this strategy not only prevents the adversary from tracking his target while it is silent, but also gets rid of the verified beacons amount by each vehicle (especially in high traffic jam where the condition of the low speed is fulfilled). However, forcing vehicles to stop beaconing safety messages is not always acceptable even if the accident probability is low in low speeds (a sudden brake in a low speed is a good example of the utility of safety messages). A better solution may be reducing beaconing frequency instead of stopping it definitely.

In order to maximize the number of vehicles that simultaneously change their pseudonyms, Liao and Li suggest a pseudonym change strategy which uses an algorithm that is called synchronous pseudonym change [78]. This algorithm uses triggers (like the vehicle's status) to guarantee a high synchronization between vehicles that have a similar status. After simulating and comparing their strategy (using traffic density and penetration rate as parameters) with other basic pseudonym change strategies (like random and fixed pseudonym change), they found that the level of privacy achieved by their synchronous pseudonym change algorithm is better than the other ones. However, the same trigger may differ depending on the chosen accuracy. In one hand, the more specific the precision of the trigger is, the more the pseudonym change (if performed) is successful and the less chance to meet it at the same time. In the other hand, the higher the trigger is global, the less pseudonym change is useless and the more chance to meet that trigger.

In another context, Lu et al. employ SPRING [79], a protocol dedicated for delay tolerant networks (**DTNs**) where they have shown that SPRING is both good for packet delivery in such sparse networks after holding the packet until a coming opportunity, and, for packet tracing prevention because the packet is stored for a while before it is sent. Using RSUs in this protocol is also possible and serves as a mix-zone. They

tested the effectiveness of the protocol against black-hole (grey-hole implicitly) attacks using a customized Java simulator, and it was shown up that it can resist against such attacks.

Song et al. present a density-based location privacy scheme ([DLP](#)) [32]. In DLP each vehicle knows about its vicinity (neighboring vehicle count or density as they called it). The density of vehicles is the main parameter that is used as a threshold for pseudonym changes. With the use of density zones of one intersection of four road sections per zone, they simulated their scheme and showed that the probability of a success tracking by an adversary relies on both the vehicles' variation of speeds and the arrival rates to the density zones. The more these two parameters are high the less chance there is for an adversary to perform a successful tracking attack.

In [80], Wasef and Shen apply the random encryption periods ([REP](#)) scheme. The main idea of REP is to ensure an effective and hidden (from the adversary) pseudonym change by letting all legitimate vehicles have a set of symmetric keys that helps them to provide one shared secret key. When a vehicle wants to change its pseudonym, it uses the shared secret key to create an encryption zone with the help of its neighbors. Thus, REP could be seen as a dynamic CMIX-zone since it is created on demand instead of at fix places like intersections. The strategy seems to be interesting and promising compared to CMIX since it dispenses with RSUs, however, when there is a high density, the encryption process may slow down the overall performances and introduces an additional overhead.

In the same scope, a new metric called time-to-confusion (explained in the metrics section) and an algorithm called the uncertainty-aware path cloaking algorithm are given by Hoh et al. in [81] for two main privacy issues; target tracking and home identification. To test their algorithm, a real world GPS data set was used. Because GPS location traces (especially in low density areas) lead the adversary to identify, with a high certainty, his target, the proposed algorithm removes these location traces. Moreover, the algorithm deals with the case of vehicles that are driving in an opposite direction from the other ones. Hence, their location traces are removed as well.

The location privacy could be breached by ways other than safety messages. The investigation done in [82] by Ishtiaq et al. reveals the effect of the wireless tire pressure monitoring system on the driver's location privacy. Each vehicle in their model is wirelessly equipped with four tire pressure sensors (due to the nature of tires, there

is no wire connections). These sensors have IDs to communicate with and to send the tires' status. However, because the design of this interesting technique does not take privacy risks into consideration (no cryptography means used), an adversary can easily track the vehicle target by eavesdropping its tire pressure sensors' messages in a distance of about 40 meters. Indeed, the work tells that privacy of vehicles must be treated delicately in order not to let any potential privacy risks that may be used by adversaries to perform a successful tracking.

In [10], Eckhoff et al. propose Slotswap, a location privacy enhancement approach. Slotswap uses a set of pseudonyms (time-slotted pseudonym pool). In each time slot, the vehicle changes its pseudonym, more precisely it will use the current time slot pseudonym. The benefits of this technique would be the independence of many authorities like the CA and it prevents them from resolving the vehicle's real identity. Yet, the privacy, as it is described, must be conditional. The identity resolution must be always available for the appropriate (law) authorities. The authors mentioned the possibility of performing pseudonym exchange between vehicles that desire (have the trigger) to change their pseudonyms. This last proposition will increase the effectiveness of the synchronous pseudonym changes. However, pseudonym exchange is not suitable in IoV systems due to the accountability requirement.

Pan et al. [51] study analytically the effectiveness of Random Pseudonyms Changing (RPC) scheme. They simulate and compare this scheme using two distributions: the uniform discrete distribution (taking into consideration the minimum and maximum use time) and the age-based distribution (refers to the pseudonym use time). They found that the RPC under the uniform discrete distribution gives better results than the age-based distribution in terms of location privacy.

Synchronized Pseudonym Changing Protocol (SPCP) [83] is another privacy-preserving scheme that is proposed by Weerasinghe et al., in where SPCP mainly bases on the use of groups. Indeed, groups provide high synchronization which implies high location privacy. The protocol uses six phases that, some of them do, perform an initial phase (registering and providing vehicles with some parameters), forming and joining the group to the final phase of changing pseudonyms. They run a set of simulations and they showed after comparing their protocol with other strategies like the silent period, AMOEBA and REP that the proposed SPCP is the best among the other ones while it gives a higher privacy level.

Another idea in privacy-preserving is that of Lu et al. which is Pseudonym Change at Social spot (PCS) [84] strategy. The strategy aims at maximizing the number of simultaneous pseudonym changes and for that, the authors defined the right moment as the gathering of many vehicles at the same time and place (e.g., road intersections with a recent turning to red traffic light or parking lots near shopping malls). To show the effectiveness of their strategy, they developed two analytic models of anonymity set. They described a mandatory model (called KPSD) used by PCS to securely generate and provide vehicles with a set of on-demand short-life keys. Indeed, changing pseudonyms in such a condition ensures a high synchronization. However, there are other road conditions that let the vehicle stay for a long time without finding the mentioned opportunities.

By exploited the social feature, Babaghayou et al. [85] highlighted the problem of identifying the quitting event of a person living in a specific district. They considered the scenario of an adversary who is monitoring the entrance of the district by a radio station. By this, they proposed to cease beaconing, in a scheme called EPP, while on the district (they justified it by the low crashes probabilities in the district). Their simulation showed that the more the vehicles respect the EPP scheme the longer the adversary can identify the quitting event of his target.

Pan and Li provide a Cooperative Pseudonym Change scheme [86] that is based on the vehicle's neighbors number (CPN). The scheme mainly benefits from the different triggers and helps the vehicle to choose the right moment for changing the pseudonym. Indeed, using triggers like the number of neighbors ensures a synchronized pseudonym change which leads to an effective location privacy enhancement compared to the individual behavior (the non-CPN). The proposed CPN is interesting because it achieves better location privacy results. However, it highly depends on the number of neighbors which is, unfortunately, not suitable in many other road scenarios. We mean here the dispersed distribution of vehicles (like in DTNs) in where the performances of CPN will surely decrease.

In the Endpoint Protection Zone (EPZ) [87] scheme, which have addressed the problem of colluding LBS and RSU operators, lets vehicles use the same login credentials while in the same zone (devided by the protocol) in order to extend their anonymity while requesting the LBS frequently. However, in order not to expose their locations included in the BSMs, vehicles are required to stay silent while in such zones;

which, as Corser et al. claim, reduces some system functionalities.

Freudiger et al. study the effect of selfish nodes on the achieved location privacy (i.e., evaluating the achieved location privacy in a selfish environment). Because changing pseudonyms may be costly in terms of network performances and overhead, nodes prefer not to participate in the pseudonym change process. The authors use a game-theoretic model (called pseudonym change game) that has helped them in modeling and evaluating the location privacy. Using the gathered results, a pseudonym change protocol (namely PseudoGame [88]) was proposed. The proposed PseudoGame protocol mainly aims at balancing the privacy and the involved cost of pseudonym changes. If the selfish nodes find out that the pseudonym change cost is high and costly but their privacy level is low, they will try to cooperate in order to maximize their location privacy to a certain level.

Dynamic Mix-zone for Location Privacy strategy (**DMLP**) [89] is introduced by Ying et al. for the location privacy problematic. DMLP forms mix-zones dynamically according to some properties like the vehicle's predicted location and privacy requirements and/or road traffic statistics and history. DMLP is also characterized by the encryption of its messages when the vehicle is inside the Dynamic mix-zone which makes it impossible for an adversary to find out what messages are exchanged without the use of encryption keys. Authors tested the DMLP strategy in various scenarios and they found that it provides a high location privacy level. However, if the dynamic mix-zone is dense to some extent, the encryption of messages will cause a huge overhead and it will affect negatively the overall performances.

Boualouache and Moussaoui give the Silent & Swap at Signalized Intersection (**S2SI**) [90] scheme. The S2SI scheme uses two protocols: one is responsible for creating safe silent mix-zones and the other one for exchanging pseudonyms. Just like the swap protocol used in [70], performing an exchange is not welcomed due to the implicated accountability issues which is the main obstacle that prevents the use of such a technique by standardization.

Basing on the same DMLP strategy discussed earlier, Ying et al. employ the Motivation for Protecting Selfish Vehicles' Location Privacy (**MPSVLP**) [91] which is a strategy that deals with the selfish environment. Indeed, due to the overhead and bandwidth consuming, vehicles prefer not to participate in the pseudonym change. The role of MPSVLP is to motivate vehicles to cooperate by adding a reputation system.

Each time a vehicle needs to update its pseudonym it creates a dynamic mix-zone and can by then earn reputation credits after performing a pseudonym change.

Inspired by the dynamic mix-zone concept, Ying and Makrakis propose the Pseudonym Change based on Candidate-location-list (PCC) [92] scheme. PCC forms mix-zones dynamically by taking the Candidate Location List (CLL) into consideration. CLL, which contains the vehicle's status information such as the ID, position, timestamp, etc., is maintained by each vehicle and it is broadcasted periodically so that the values inside the CLL will determine when and where should the vehicle perform a pseudonym change; without requesting the creation of a mix-zone, the CLL is enough to help it doing the task. The effectiveness of PCC was shown in the different simulations and it was compared to other strategies like the CPN and DMLP.

Basing on the PCS scheme [84] that exploits the social spots feature of individuals and basing on their own remark that is "the wasted opportunities between frequently meeting vehicles in other than social spots; the individual spots", Yu et al. present MixGroup [93], a scheme that benefits from both the social spots and the individual spots to enlarge the vehicles' pseudonym mixture. By letting vehicles join the available groups after entering their area, vehicles use the same group identifier gotten from the group leader to stay anonymous with the option of exchanging their own pseudonyms between themselves and validating the operation once they meet an RSU at the end of the zone. In spite of its promising simulation results, the scheme introduce high communication overhead and group leader privacy loss.

In [57], Boualouache et al. suggest the Vehicular Location Privacy Zone (VLPZ) principle for location privacy. VLPZ is similar to infrastructures like the RSU (e.g., gas stations or toll booths). They assume that the map is divided into grid cells, and that each grid cell contains at least one VLPZ responsible for the pseudonym management and change. VLPZ is formed by an entry point (they called it the router) and an exit point (the aggregator) and a limited lanes number starting from two lanes. Authors evaluated their strategy both analytically and numerically. They found that the number of vehicles and the capacity of VLPZs have an important role in enhancement of the location privacy level.

Boualouache and Moussaoui propose a pseudonym changing strategy for urban environments, the Urban Pseudonym Changing Strategy (UPCS) [94]. By exploiting the already existing signalized intersections, UPCS benefits from such places to

construct one Silent Mix-zone ([SM](#)) or more. UPCS is able to either use pseudonym change or pseudonym exchange (that has accountability problems) techniques. Authors also proposed another strategy: the Traffic-Aware Pseudonym Changing Strategy ([TAPCS](#)) [95] that uses silent periods. In TAPCS, the pseudonym change is performed according to the road conditions, more precisely, the strategy implements the following parts: detecting the traffic congestion, electing an initiator (like the leader of the group that will extend the silent period), creating silent mix-zones, extending the silent mix-zone (it is performed while the road congestion is still on) and finally the detection of the traffic congestion's end. TAPCS was simulated and authors showed the effectiveness of their strategy after studying the analytic evaluation of its location privacy level. The strategy was then compared to prior strategies like CARAVAN, PCS and DMLP.

The location privacy does not always rely on the vehicles' safety messages and broadcasts but also on the use of the different available services (mainly LBSs like map services). Arain et al. suggest the use of a new strategy called the Multiple Mix-zones with Location Privacy Protection ([MMLPP](#)) [96]. Unlike traditional mix-zone strategies that do not take the map services' impact into consideration, MMLPP prevents the leakage of the vehicle's sensitive location information that may be exposed after requesting a route query; that contains the start and the end of the trip. It does so by replacing the end point of the trip by another point that is called Point Of Interest ([POI](#)), more precisely: by another nearest POI to that vehicle. Graph theory was used in MMLPP to build their multiple mix-zone model and the strategy was analyzed using real route queries provided by map services.

In [8], Eckhoff and Sommer propose and study the effect of a privacy-preserving scheme, similar to that of [10], which is safety-preserving solution with the use of non-Overlapping Time-Slotted Pseudonym Pools (referred as [nO-TS-PP](#) in here). Authors perfectly described the problem of safety-privacy trade-off with a special way; that is, the claim that defeating safety by rising privacy level is not an acceptable solution, hence, the pseudonym change strategies that may confuse the adversary may also confuse safety-critical applications. Against a local passive adversary, authors investigate their nO-TS-PP performances in various scenarios. The strategy bases on a circular synchronized time-slotted system that uses pseudonyms in predefined time-ranges (time-slots) defined by the length of the pseudonym pool in addition to the validity duration of each pseudonym. Since all vehicles do change their pseudonyms

synchronously; because of the GPS, the confusion of the local adversary achieves its high levels (expressed by the tracking fail rate metric in their paper).

Zidani et al. present ENeP-AB [97], an adaptive beaconing approach for privacy-preservation. EneP-AB allows vehicles to change their pseudonyms when there is a high probability to confuse the adversary. For this, vehicles set a flag-bit named Readyflag in their paper to declare the willingness to pseudonym change in the next slot time. By this, vehicles will be able to synchronize their pseudonym changes. Another feature is used by EneP-AB is the Adaptive Beaconing Rate Approach, that is E-ABRP, which lets vehicles change the time, that was constant, between two successive beacons; resulting in a defending against the temporal correlation attack. However, the strategy lacks effectiveness in sparse densities especially with the high and precise location beaconing.

In the context of Vehicular Social Networks (VSNs), Babaghayou et al. [85], and motivated by the fact that the VSN user's start point (e.g., home) reveals his identity, suggested to cease beaconing while leaving the user's district and only resumes broadcasting when exiting his district (called gateway in their work). The study is also accompanied by simulations in where just a percentage of VSN users apply the scheme. The results show that the more VSN user apply the scheme, the more the adversary is confused about the one's leaving probability.

One of the factors that allows an adversary to easily track his targets is the eavesdropping coverage. Babaghayou and Labraoui, by then, deployed a Transmission Range Adjustment (TRA) [24] mechanism into two of the well-known privacy schemes; CAPS [98] and SLOW. TRA aims at reducing the transmission range on-the-fly when vehicles are driving with low speeds (they mentioned 4 speed levels). With this technique, the adversary loses much eavesdropping capabilities as the probability of eavesdropping packets will be diminished compared to when vehicles are broadcasting with the standardized 300m safety-messages range. The authors used metrics such as the traceability and found that the traceability was dropped indeed after integrating TRA on both CAPS and SLOW giving the option to apply such mechanisms in the upcoming privacy-preserving schemes.

Most privacy-preserving schemes rely on the pseudonymous identities and certificates but the majority of such works do neglect the pseudonym issuance and refilling phases. By this motivation, Benarous et al. [99] have developed an on-demand

pseudonyms and/or certificates refiling scheme. Their scheme bases on (1) anonymous tickets and (2) challenge-based authentication. The scheme's performances against the most prominent security requirements are investigated using a set of methods and tools such as the BAN logic, SPAN and AVISPA tools that have proved the feasibility and robustness of the scheme.

Coupling Privacy with Safety (CPS) [100] is another scheme that is given by Wahid et al. to mitigate the location privacy exposing. CPS uses the principle of "talk only when necessary" meaning that vehicles, and unlike other silent period schemes as authors claim, will keep the radio on in order to fast-react when emergent events occur. The scheme mainly bases on RSU, once vehicles enter to its range, a call to a function that uses the vehicle's speed and the RSU's range to calculate "trip-time" which is an extendable estimated time for the vehicle to last in the RSU's range. Vehicles do not send BSMs while inside the range and while the timer does not expire. In spite of the less resulting overhead, the scheme is still using the principle of silent period which is not highly recommended according to the standardization.

WHISPER [101], an identity and location privacy-preserving scheme that uses the transmission range adjustment techniques is proposed by Babaghayou et al. in the context of IoV. WHISPER aims mainly at maintaining road-safety by making sure that the neighbor vehicles are always informed (via safety-beacon messages) which ensures road-safety and at the same time, reducing the transmission range whenever the safety is present in order to escape the continuous tracking by the adversary. Their scheme was evaluated using privacy and QoS metrics and was compared to some other schemes (SLOW, RSP and CPN) where the scheme showed promising results.

3 Pseudonym Change Taxonomy

In this section, and unlike in the other surveys, we give a novel taxonomy that is based on the opportunity perspective instead of other considerations like mix-zone vs mix-context or distributed vs centralized, etc. The reason we make such a classification is due to the fact that the adversary observes and focuses on the time and/or place (i.e. opportunity) when/where the pseudonym change takes place. This, in our opinion, is more meaningful compared to other classifications. Thus, knowing how, when and where pseudonyms may change is the key towards a better pseudonym change strategy conception that deals with the adversary's thinking. We firstly start with

a comparative table in order to characterize each strategy. Then, we proceed to our proposed pseudonym change taxonomy. Finally, we mention some very important concepts that absolutely affect the effectiveness of pseudonym change schemes.

3.1 Comparison of existing strategies

Each proposed pseudonym change strategy has its own features. To better understand them, a set of metrics has to be used. According to the research done in [58] and the studies of some other strategies and our own observations, we present a comparative table (Table 2) of the different strategies that emerged from 2005 until 2019 with different metrics like (a) the synchronization method (namely: Protocol, Infrastructure or GPS), whether it (2) uses the silent period or not, (3) uses the encryption or not, (4) the brought amount of overhead, (5) the conducted study's evaluation method (by simulation "S" means, analytically "A" or both "B"), (6) if the accountability mapping is still applicable by the appropriate law authority or not and (7) if it is LBS resistant or not (whether it deals with and takes the problem of compromised LBSs into account or not).

3.2 Our proposed taxonomy for pseudonym change strategies

The proposed taxonomy (as presented in Figure 11) uses the opportunity that may be exploited by the strategy when it decides to perform a pseudonym change. Hence, we distinguish two main distinct categories: the Trigger-based and the Trigger-Free. In the Trigger-based category, the pseudonym change action is performed when a specific event occurs. The event can be:

- (1) Entering a fixed zone which is predefined.
- (2) When reaching an exact time (or time elapsed since the last pseudonym change).
- (3) When one of the following conditions is satisfied:
 - (*) When the number of neighbors reaches or exceeds a certain threshold number.
 - (*) When a vehicle finds other vehicles in the vicinity that have its same status (e.g. same velocity, lane and/or group) / wanting to perform the pseudonym change, here, the vehicle will cooperatively participate with them in this action / when there is a specific distance between the two vehicles, one of the reasons it is important because the adversary will be more confused when the two vehicles change their pseudonyms at the same time while

Table 2: Comparison of existing strategies according to a set of metrics

Strategy	Year	Synchronization by	Staying Silent	Using Encryption	Overhead Cost	The Evaluation Method	Authority Mapping	LBS Resistant
CARAVAN [68]	2005	Protocol	✓	✗	Low	B	✓	✓
Swing & Swap [70]	2006	Protocol	✓	✓	High	B	✗	✗
CMIX [72]	2007	Infrastructure	✗	✓	High	S	✓	✗
Mix-Context [73]	2007	Protocol	✗	✗	Low	S	✓	✗
SLOW [77]	2009	Protocol	✓	✗	Low	S	✓	✗
DLP [32]	2010	Protocol	✗	✗	Low	A	✓	✗
REP [80]	2010	Protocol	✗	✓	High	S	✓	✗
SlotSwap [10]	2011	GPS	✗	✗	High	S	✗	✗
SPCP [83]	2011	Protocol	✗	✗	High	S	✓	✗
SocialSpots [84]	2012	Infrastructure	✗	✗	Low	B	✓	✗
CPN [86]	2013	Protocol	✗	✗	Low	B	✓	✗
DMLP [89]	2013	Protocol	✗	✓	High	S	✓	✗
EPZ [87]	2013	Protocol	✓	✗	Low	S	✗	✓
MixGroup [93]	2016	Protocol	✗	✗	High	S	✓	✗
MMLPP [96]	2018	Protocol	✗	✗	High	S	✓	✓
nO-TS-PP [8]	2018	GPS	✗	✗	Low	S	✓	✗
ENeP-AB [97]	2018	Protocol	✗	✗	Low	S	✓	✗
CPS [100]	2019	Infrastructure	✓	✗	Low	B	✓	✗
WHISPER [101]	2021	GPS	✗	✗	Low	S	✓	✗

they are close (i.e., cannot easily make the prediction according to the past coordinates) / when there are other vehicles conducting the same action

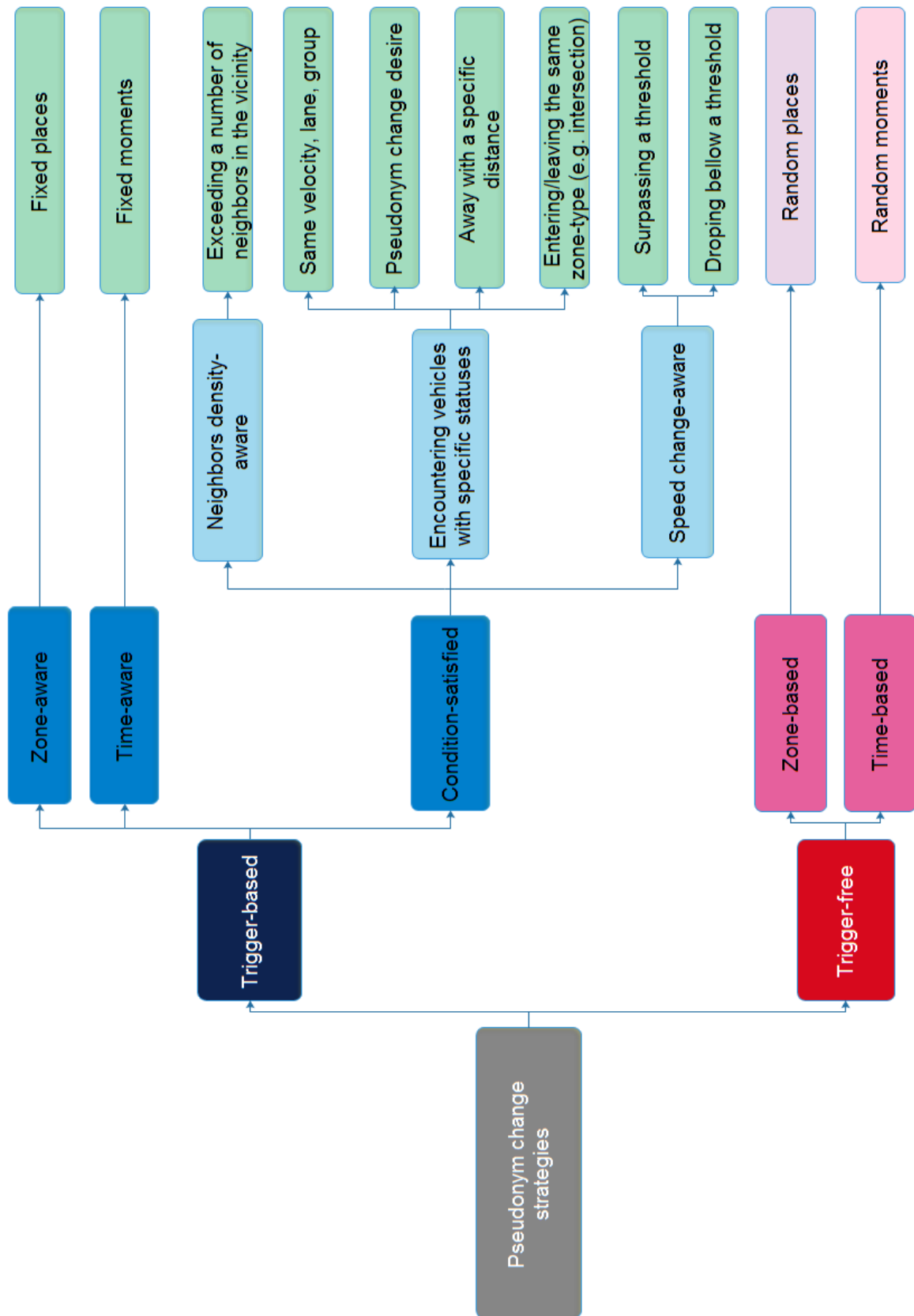


Figure 11: The novel taxonomy of pseudonym change strategies

(e.g., changing pseudonyms synchronously while entering an intersection with another vehicle that is entering or leaving the same intersection, turning to the same direction, quitting the same parking lot, etc.).

- (*) When the vehicle's speed reaches or exceeds a specific threshold (hard trajectory and future coordinates prediction) / when the speed drops below a specific threshold (generally, in low speed environments, the number of vehicles is sufficient, hence, more cooperating vehicles).

On the other hand, in the Trigger-Free category, the notion of trigger or opportunity does not exist. As an example, the pseudonym change action, in this class, is performed according to random moments (after random times) or places (entering random road segments or zones without specification). This class is characterized by the randomization and it is better than keeping the same pseudonym along the whole trip. However, it is not based on logic and best opportunities. Hence, the adversary can, in majority of cases, predict the pseudonym change action and succeeds in linking the old and new pseudonyms.

3.3 The changing technique considerations

For a tough and robust privacy mechanism, each pseudonym change strategy must -delicately- take the following elements into account:

- *Silent period*: because the pseudonym change may be observable by the adversary in some, if not most, situations (e.g., non-dense scenarios, low speeds with high beaconing frequency, etc.), a silent period of time that happens between safety broadcasts is needed. This aims at confusing the adversary while he is trying to link the old and the new pseudonym basing on the time/location of the old disappeared pseudonym. The negative effect caused by the silent period mainly appears in the safety-related applications due to the exigence of the high safety beaconing frequency; the less frequency there is, the less achieved safety will be.
- *Pseudonym exchange*: in the presence of neighbors, the pseudonym change strategy gives better results because the adversary will be more confused when the vehicles change their pseudonyms cooperatively. However, the adversary can still observe and know that the pseudonym change is done. To avoid this scenario, the exchange of pseudonyms, instead of using new ones, is preferred. By this, the adversary will not be sure whether the pseudonym change was performed in the

- first place or not. This technique works perfectly against the *syntactic linking attack* but it is useless against the *semantic linking attack* because he still can find it by calculating the velocity of vehicles (for example) and makes a prediction of the next coordinates, hence, linking the exchanged pseudonyms. The negative effect of this technique is represented in the accountability feature (accountability mapping) loss if no mechanism is deployed, which is an important requirement for a basic functioning since exchanging pseudonyms implies giving the secret key used in signing messages to the exchanging vehicle; giving the latter the option to read the sent messages that are encrypted (or even impersonating other vehicles).
- *Pseudonym encryption*: in fact, the main reason for why the pseudonym concept is created is to send the vehicle's status in clear (a sender with its visible status). This is needed because of the IoV unique requirements in where the negative effect comes from. Because, a heavy computational process of encryption/decryption implies a low functioning. Thus, if it comes into a high necessity to encrypt the vehicle's status, using light encryption algorithms would have a good impact on preventing the outsider adversaries from performing the data collection properly and ensures a basic functioning. The encryption by this, introduces a trade-off between safety and privacy.
 - *Transmission strength-aware*: in the case of advanced adversaries, the transmission strength of vehicles, while performing their normal communications, plays a significant role in determining the vehicle's whereabouts, i.e., its location; that is, the triangulation technique. Even if it is not evidently apparent, the transmission strength must be taken into account while designing a pseudonym change mechanism. Varying the strength (even if it is a hardware-related more than being software-related solution) must always be an available option.
 - *All layers Identifier change (cross-layer)*: when the strategy decides to perform the pseudonym change, the vehicle's other identifiers (e.g., the mac and the IP address identifiers) must also be changed; because changing one identifier and letting the other one is absolutely useless. The negative effect in this technique is the heavy overhead caused by the repeated changing of these identifiers. In other words, affecting the overall performances like routing by retransmitting the packets when the old identifier is no longer available. Schoch et al. [102] have studied the impacts of the frequent pseudonym changes on geographic routing

- protocols and have found that it affects negatively the performances of the system.
- *Manufacturer's unique fingerprint identification avoidance*: if there are no unified transmission devices, the distinguishability of each vehicle will be possible by the adversary. Thus, benefiting from this to enhance his tracking algorithms and mechanisms. As an example, if two vehicles A and B that are not created (or at least their communication devices) by the same manufacturer, the possibility of analyzing the fingerprint resulting by the transmission signals of vehicles will be feasible; leading to identifying these vehicles. Just like in the case of protocols (softwares) in any research field, the effort towards applying unified hardwares that will be used in IoV is still challenging.
 - *Tamper-Proof Device (TPD) robustness*: to ensure that any credentials (like pseudonyms) are securely stored in the OBU, i.e., it is not possible for an adversary to read, write or move these credentials, the use of TPDs is needed. However, using such techniques and embedding them in the OBU does cost compared to the creation of ordinary OBU devices. Fortunately, and in spite of the cost, most recent OBUs do integrate TPDs in their design.
 - *Sensors manipulation resistance*: the defense against data manipulation and forgery is ensured by the different security mechanisms such as the use of cryptography and authentication means. However, the adversary can still jeopardize the system by physically affecting the sensors which will cause the acceptance of false data (semantically) inside the system. Performing GPS spoofing attack or affecting the thermometer sensor by external heat or freeze factors is a good example of such a problem. It is true that most drivers are not interested by these vulnerabilities, but this does not change the fact that we still may find spoilers who have different reasons beyond performing this kind of physical attacks.
 - *Divided and distributed keys to different authorities*: the ability to execute delicate and crucial actions like pseudonym resolution, which leads to reveal the individual's identity, must not be entrusted to only one single organization. Hence, distributing/separating the resolution process and letting it be doable if and only if all organizations cooperate and agree on the necessity of this process must be ensured. It is a pretty good solution towards the single probable collusive (suspicious) organization.

- *Extra and exploitable information avoidance*: Some of the data, that is already standardized, included in frequently sent packets can, if well exploited, dramatically augment the unlikelihood of other vehicles to be the target, resulting in determining the target with higher probability. As an example of such data we find the vehicle's size included in BSM messages [8], the reputation value of a vehicle in case the system includes reputation and the communication channel number on which the communication and the packets are sent in.

4 Summary

In this state-of-art-oriented chapter, we saw an exhaustive study on the most recent related work followed by a comparative study of some of the reviewed pseudonymous schemes. This chapter did provide a taxonomy to classify the pseudonym change strategies but from another angle of view which is unlike the other literature review works. We gave important points and concepts that will, if exploited effectively, strengthen the future pseudonym change schemes that are going to be proposed. This chapter's final lines are not only the closing of both: itself and the LITERATURE REVIEW part but also the transition to the second part of this thesis, which is: the SCIENTIFIC CONTRIBUTIONS part in where we see three of our proposed schemes to deal with the identity and location privacy problem.

Journal and Conference Papers Related to the Chapter

Jr) Pseudonym change-based privacy-preserving schemes in vehicular ad-hoc networks: A survey

Messaoud BABAGHAYOU, Nabila LABRAOUI, Ado Adamou ABBA ARI, Nasreddine LAGRAA and Mohamed Amine FERRAG. "Pseudonym change-based privacy-preserving schemes in vehicular ad-hoc networks: A survey". Journal of Information Security and Applications, 55, (2020), 102618. (A-Rank, IF=2.327)

PART TWO: SCIENTIFIC CONTRIBUTIONS

*Chapter III: Location Privacy Evaluation
for Trips and Home identification in
VANET*

*Chapter IV: Transmission Range
Changing Effects on IoV Users' Location
Privacy*

*Chapter V: WHISPER: a Safety-Aware
and Location Privacy Scheme for IoV*

*Chapter III:
Location Privacy Evaluation for Trips
and Home identification in VANET*

“Inaction breeds doubt and fear. Action breeds confidence and courage. If you want to conquer fear, do not sit home and think about it. Go out and get busy.”

– Dale Carnegie

1 Preface

This chapter is the beginning of our contributions on the field of identity and location privacy-preservation. Those contributions are gathered in the current part that we call the SCIENTIFIC CONTRIBUTIONS part. In what follows, we propose Extreme Points Privacy (EPP) for Trips and Home Identification in VSNs, a privacy scheme that exploits the nature of the end points that are common between VSN users in order to create shared zones for anonymization purposes. EPP is evaluated using the Anonymity Set Size (ASS) metric while we study the scheme in a small district from Tlemcen town, Algeria. The reason behind this study, despite being the pseudonym change strategies offering a good level of privacy, is that even by changing pseudonyms, the vehicle could still be tracked if the adversary has a prior knowledge about the potential start and end points of a particular driver who has social interactions (e.g., with neighbors) which introduces the concept of VSNs.

The remainder of this chapter is organized as follows. In section 2, we introduce the proposed EPP strategy. In section 3, we give the experimental results in addition to the details about the evaluation. In section 4, we describe the privacy concept with a defender and an adversary points of view. Finally, we conclude the chapter by giving a summary in section 5.

2 Background

The emerging of wireless technologies had big impact on different fields which led to the birth of VSNs, one of the wireless technology applications in the field of vehicles; or the so called VANETs. The evolution and enhancement of VANET capabilities has significant influence on the successfulness of the ITS [84, 103, 104]. In VANETs there exist two kinds of communications and they are self-describing: V2V and V2I. In order to be able to communicate, vehicles are equipped with OBUs; specific devices that allow vehicles to: communicate, process data, receive GPS signal and use variant sensors. For a better system, vehicles may often communicate with central infrastructures. Such infrastructures may be RSUs [105]. VANET applications may be diverse; however, the number one reason for what it was proposed is to reduce the number of crashes and fatalities [68]. The vehicle will succeed to do so by enabling periodic broadcasts (also called beacons or heartbeat messages) so that the vehicle includes its status in kind of location, speed, velocity and other information that can lead the neighborhood for

better environment knowledge and that is the BSMS. According to the standard “SAE J2735”, the frequency of BSMS is set to be each 100ms with a 300 meter transmission range of its radius [87].

The frequent and precise location provided by BSMS helps enormously the safety-related applications but, at the same time, reduces dramatically the privacy of VSN users since the BSMS’ location is not encrypted for fast reaction and less delay (it is the requirements of safety-applications). Thus, any adversary willing to monitor and track the VSN users can do that in real time with just the possession of eavesdropping station(s) which does not cost him a lot and is not easily detectable. Among the solutions to defend against such privacy threats we find the use of pseudo-identifiers (pseudonyms) instead of the unchangeable real identifiers. This last solution increases the anonymity of drivers but the adversary can match the real identity with the pseudonym by observing the trips of the vehicle. Making the pseudonyms changeable over time can be seen as an acceptable solution since the adversary can no longer see just one pseudonym. However, even so, if the vehicle changes its identifier in inappropriate situation (e.g., alone inside a set of vehicles), the adversary here can easily link the old (vanished) pseudonym with the new (emerging) one. For this last problem, the cooperation between vehicles by making a synchronous pseudonym change was the best countermeasure since the adversary will be confused on the new pseudonym of a vehicle inside the set of potential targets.

Unfortunately, because of the exact and frequent periodic location, the adversary can predict the moves of the monitored vehicles [106] inside the region of interest which helps him to link each new pseudonym with the old one for all those vehicles even though the changes were done simultaneously. For this advanced challenge, the concept of silent period was proposed in [69] for wireless networks and it is explained as a transition period of time between the newly changed pseudonym and the old one. By this definition, the vehicles will keep silent and during this silence time, they do change their pseudonyms and not sending BSMS until the time is ended. When the time is ended, the vehicle is allowed to use the new changed pseudonym. This technique was integrated in the field of VANETs in works done in [68, 77]. Silent periods highly enhance the privacy of VSN users but with the cost of safety, that is the sacrificing of privacy or the trade-off between safety and privacy. For this reason, such trade-off was widely debated.

3 The Proposed EPP Strategy

In this section we outline the principals of the proposed scheme EPP which is a zone division-based that exploits the nature of the VSNs and we give the possible behavior of any VSN user and its implication of the privacy of these users.

3.1 Motivation

Since the pseudonym change strategy, which defends against the location tracking and re-identification, is not working in all scenarios, new techniques must be deployed to fill this gap. An example of such scenarios is when vehicles starts/ends from/at a predefined spot. Here, if the adversary has some knowledge (represented by social engineering) can match the used pseudonym with the real identity of its driver whatever the strength of the deployed pseudonym change strategy is. In order not to let the used strategies and the privacy of VSN users go in vain, we suggest the use of the EPP scheme which is built basing on the characteristics of the end points (either start or end) that, in general, do belong to specific zones which have specific nature like: (1) the speeds of vehicles are low since they are in the starting or stopping status. Also, due to the capabilities of the new generation of vehicles, (2) they provide high environment sensing and movement/objects detection by using, for example, the distance sensors, radars, ultrasonic sensors, high definition cameras, etc. [107] letting the BSMs be an option instead of a must. By this definition and assumptions, we present the different zones and techniques used in combination with the pseudonym change strategies used for the location tracking and re-identification. The next subsection shows the zones division and elements.

3.2 Deployment of Zones

As shown in Figure 12, the map, according to EPP, is divided into: District zones, Gateway zones and the Outside Environment and are explained in details in what follows:

- A. District Zones:** they contain the start and end points of specific VSN users who do use these points (spots) more frequently. Such spots may be the home of a VSN user, a parking spot of his work place or just a frequently visited place. The nature of such zones, as described before, allows dispensing with BSMs. It is obviously because of the capabilities of new vehicles and their efficiency in dealing with the environment and neighborhood vehicles who are not presenting

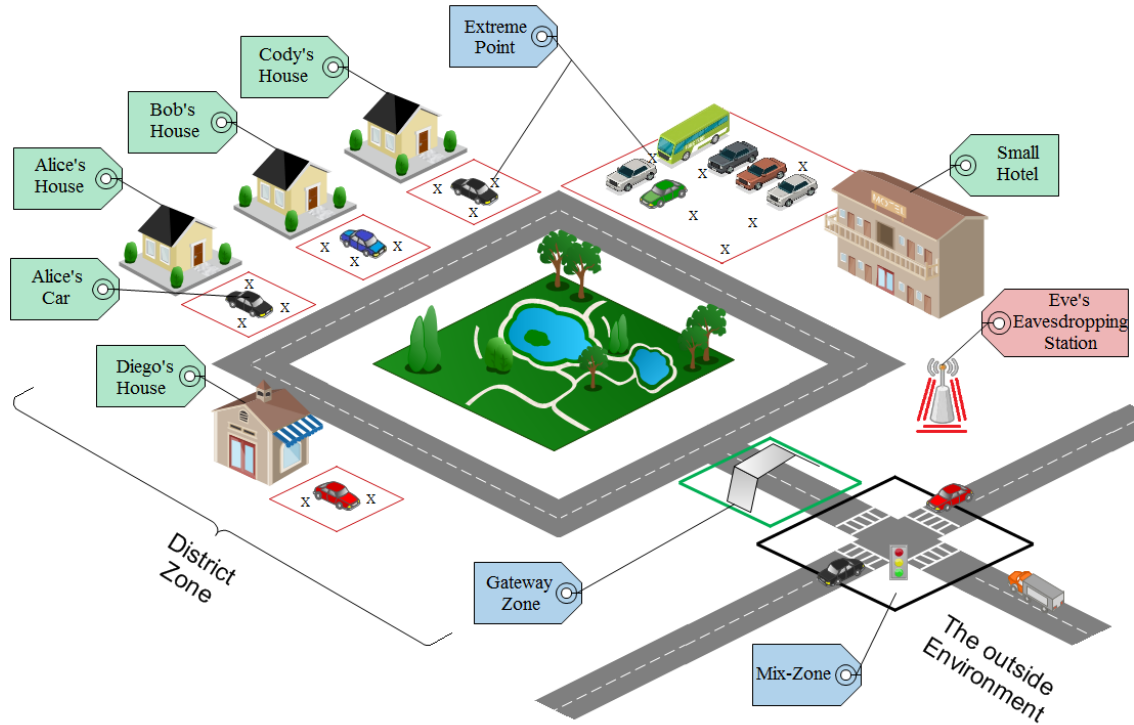


Figure 12: An Illustration figure for the proposed EPP Zones division

a big threat with their current speed and situation. The vehicles then will be authorized to stay silent while they are inside the district zone(s) without safety dangers and threats.

- B. Gateway Zones:** according to our model, each district is attached with the outside environment. The main reason for what gateways (GWs) are parts of the EPP is to let the outside environment vehicles know about the newly coming vehicles from the district because outside the district there exist potential dangers on the vehicles. To deal with these threats, BSMs are become a must (instead of being an option in district zones) and that is the reason for the gateways existence; an introducer/rely zone. In addition, a district may have more than one gateway and for each gateway they may exist one or more headings (HDs). A heading is a direction that a vehicle can take once it leaves the gateway. It generally determines the trip of the driver.
- C. The outside Environment:** it is the remaining part of the network in where vehicles are between the start and end points. In such zones, a privacy mechanism like pseudonym change strategy in mix-zones is used. The vehicle protects its location privacy by changing (or updating) its current pseudonym into a new

one in specific places. The intersections are claimed to be so efficient since they gather a lot of vehicles at the same time [91] which will (1) stop beaconing, e.g., use silent periods when they enter the mix-zone with a slow speed, (2) change their pseudonyms then (3) emerge from the outside of this mix-zone with a new pseudonym letting the tracker be confused in which direction the vehicle target had gone.

3.3 Behavior of Vehicles in the System

As explained in the previous subsection, a VSN user starts from the district, more precisely from his appropriate spot inside that district. In our model we assume that the adversary is advanced, e.g., is considered as Global Passive Adversary (GPA) [105] with a backward knowledge about all VSN users inside the district acquired from means like social engineering. The adversary then knows about each vehicle's potential spots, exiting/entering gateway and the heading of the trip. With ordinary strategies, the adversary will know for sure about the events of: (1) quitting the home and the frequent places and (2) entering them. In EPP, VSN users are supposed to be in control of enabling and disabling the radio-silence feature which enhances and removes the inner's privacy respectively. We define then the next three possible scenarios (or vehicle classes) that may occur:

- A set of VSN users who are aware of the privacy concept. Thus, they enable the radio-silence feature to better-protect their privacy. This set is defined as "X".
- A set of VSN users who are not aware of their privacy. Thus, they disable the radio-silence feature. The reason may also be that they need to use some services which require the vehicle to be connected. This set is defined as "Y".
- A set of VSN users who may not be able or cancel their appointments, works, visits, etc. for whatever reason. This kind of vehicles surprises the adversary since they act unexpectedly to his thoughts. This set is defined as "Z".

The adversary is also supposed to be aware of the approximate movement time of his target(s) and it is also due to the social engineering techniques. Figure 13 shows both of the network model and the threat model in relation to the proposed scheme.

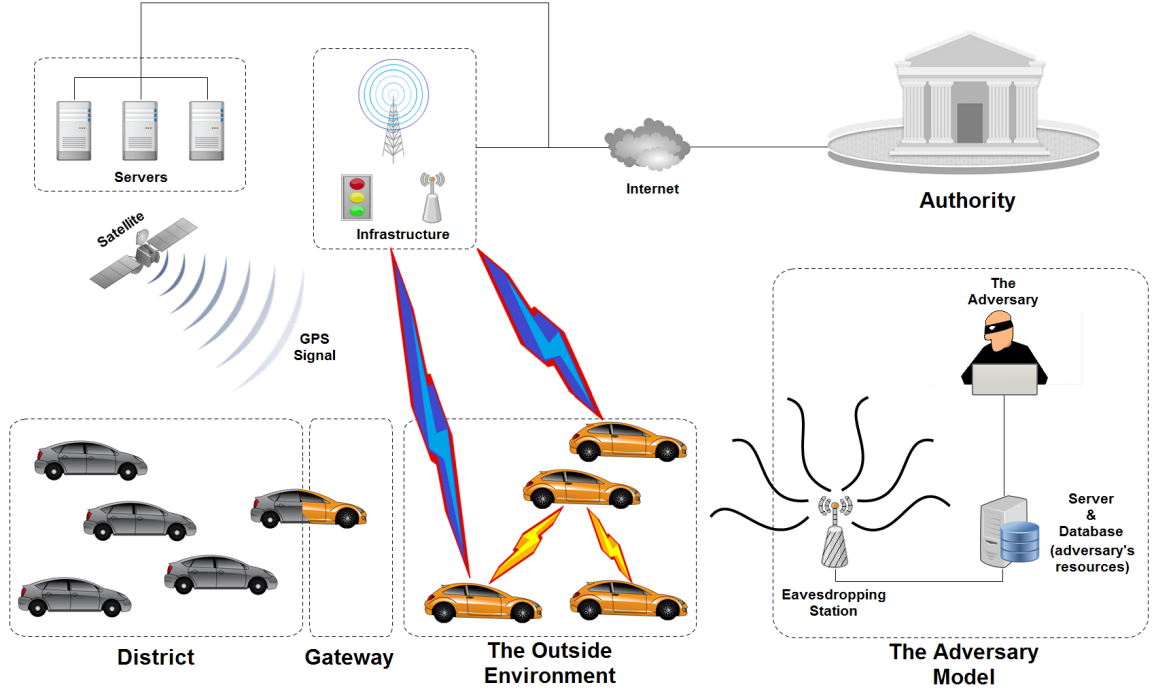


Figure 13: The abstract network and threat models in EPP

3.4 Definitions and Properties

In this part we explain the entities of the network with their definitions for better comprehension:

Let the set of VSN users who belong to the district be:

$$S_{sim(i)} = \{v_j \in S : Similarity(v_i, v_j) = 1\} \quad (4)$$

The set of VSN users who are still inside the district:

$$S_{in(i)} = \{v_j \in S_{sim(i)} : State[v_j] = "Inside"\} \quad (5)$$

The set of VSN users who quitted the district:

$$S_{out(i)} = S_{sim(i)} - S_{in(i)} \quad (6)$$

The set of VSN users who quitted the district for sure in the thoughts of the adversary with a 100% of certainty:

$$S_{clearly_out(i)} = \{v_j \in S_{out(i)} : Class[v_j] = "Y"\} \quad (7)$$

by these definitions, we can formulate the adversary,s probability metric to quantify the privacy of VSN users. In other words: the exact probability of quitting the district

by his target which is formulated as follows:

Firstly the probability of being inside the district:

$$P_{inside}(v_i) = \begin{cases} 0 & IF(Class[v_i] = "Y")AND(State[V_i] = "Outside") \\ \frac{|S_{sim(i)}| - |S_{out(i)}|}{|S_{sim(i)}| - |S_{clearly_out(i)}|} & Else \end{cases} \quad (8)$$

Finally the probability of being outside, e.g. had probability of quitting as follows:

$$P_{outside}(v_i) = 1 - P_{inside}(v_i) \quad (9)$$

4 Simulation Setup and Results

In this section, we evaluate the effectiveness of the proposed EPP scheme. For this aim, we consider a set of 10 VSN users of a specific district (taken from Tlemcen town, Algeria) that contains two gateways and two heading per each gateway. Our main task is to evaluate the adversary's certainty about the exiting/quitting of a target(s) (V_i) which is among the 10 vehicles. Each VSN user can belong to either classes (X , Y or Z). The number of gateways and headings are also manipulated in order to see its effect on the achieved privacy (and the attacker's successfulness as well). Additionally, the anonymity of all VSNs users who quitted the district was evaluated using the (ASS) after passing by the first mix-zone. In fact, there is other used metrics in the literature to evaluate the location privacy, we advise the reader to take a look on these works [108, 109, 110]. Actually, the privacy of VSN users in the outside environment is not a main evaluation goal for this study. The simulations were done by taking three scenarios (namely: I , II and III). In I , a real district that contains two gateways and two heading per each gateway was taken. We modified by then this real map fragment and transformed it into II then III (see Table 3).

Table 3: The three scenarios used in the evaluation of EPP

Scenario	Gateways Number per scenario	Headings Per Scenario
I	2	2 * 2
II	1	1 * 2
III	1	1 * 1

We used SUMO to make realistic VSN users traces. For this purpose, we generated a vehicular road traffic starting from 7 : 40 until 8 : 15. The reason we took this interval of time is because users often leave their homes in such a period to either: work, study, etc. we then (via a c++ program) randomly generated our ten district

vehicles' departure times, the exiting gateways and the headings (their departure is between 7 : 45 and 8 : 15) as shown in Table 4.

Table 4: The parameters of the district VSN users's departure, gateway and heading

Vi	Departure Time			The trip's characteristics (GW , HD)		
	I	II	III	I	II	III
1	08:07:43	08:11:29	07:54:14	1 , 2	1 , 2	1 , 1
2	08:06:28	07:57:52	07:55:06	2 , 2	1 , 1	1 , 1
3	08:14:38	08:08:17	08:10:11	1 , 1	1 , 2	1 , 1
4	08:07:50	07:57:30	07:49:24	1 , 1	1 , 1	1 , 1
5	08:14:53	08:00:32	07:57:04	2 , 1	1 , 1	1 , 1
6	08:03:28	08:08:01	08:11:13	2 , 2	1 , 1	1 , 1
7	07:49:05	07:53:21	07:59:55	2 , 2	1 , 2	1 , 1
8	07:50:09	07:53:14	07:56:28	1 , 2	1 , 1	1 , 1
9	07:59:31	07:53:00	07:55:05	2 , 1	1 , 2	1 , 1
10	08:04:12	08:03:10	08:01:02	2 , 1	1 , 2	1 , 1

We also made four parameters per each scenario by varying the number of vehicles in each class (see Table 5).

Table 5: The parameters of each scenario of VSN users's class

Class	Parameterizing per Scenario			
	1	2	3	4
X	60%	70%	80%	90%
Y	30%	20%	10%	-
Z	10%			

Table 6 shows the parameters of the chosen original map. Figure 14 and Figure 15 are also included to show more details about the three scenarios and the chosen map respectively.

Table 6: The map simulation details

	Network Characteristics
Map's Location	District in Tlemcen town, Algeria
Total Lane Length (km)	13,19
Map's Surface (km*km)	(1,02 * 0,89)
Mix-Zone Radius (m)	25
Vehicles per District	10

4.1 The simulation runs

As explained before, we choose three scenarios and per each scenario we make four runs, we then evaluate the probability of identification (knowing whether the target had quitted or not) acquired by the adversary. The evaluated targets are taken randomly from each class (i.e. from X , Y and Z which is only one since it is 10% from 10).

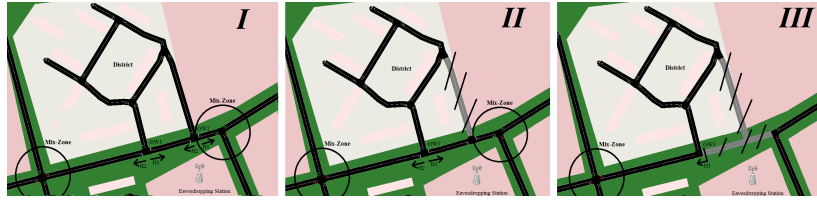


Figure 14: The three scenarios: *I*, *II* and *III*

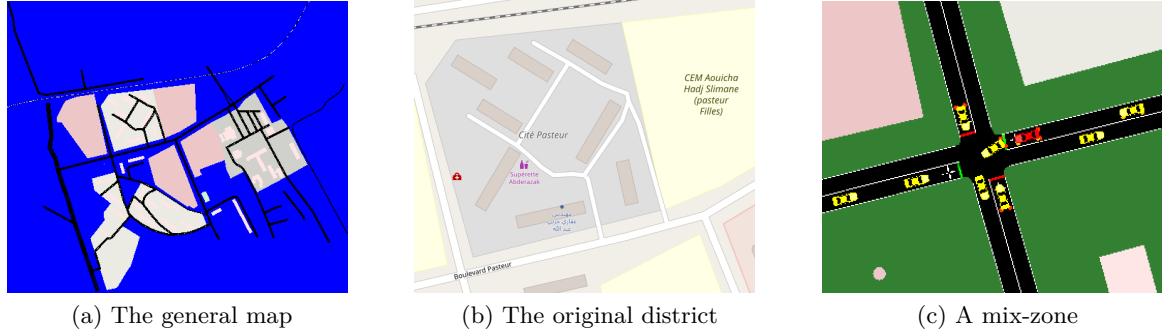


Figure 15: Additional illustrations about the map

Additionally, Figure 16 shows the simulated samples and runs with the appropriate value of the gateways and hidings in a part, and the "X", "Y" and "Z" classes in the other part.

4.2 Scenario I

We start by the scenario of two gateways with two hidings per each. The taken Vehicle from each class is mentioned in the graphs. The obtained results are as follows:

The results in Figure 17 shows that the VSN user who does not activate/enable the privacy mechanism (class "Y") fail both: (a) easily and (b) faster than other classes. The next one is the VSN user of the class "X", because he does not expose himself by staying silent until he quits the district. However, class "Y" VSN users affect him

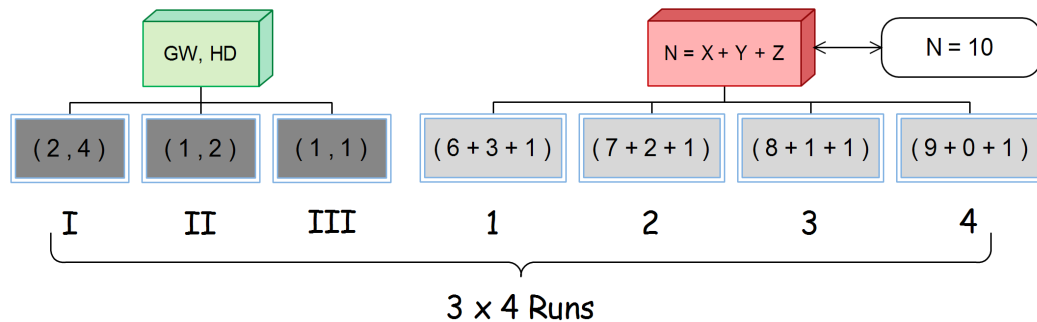
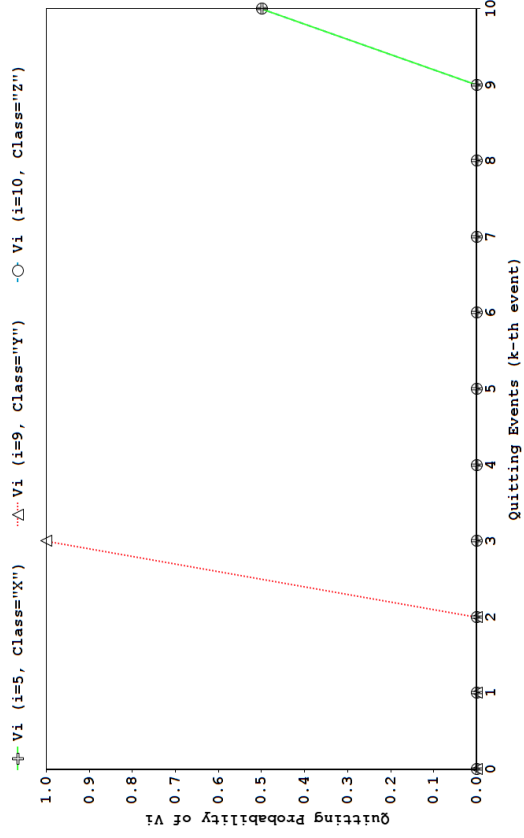
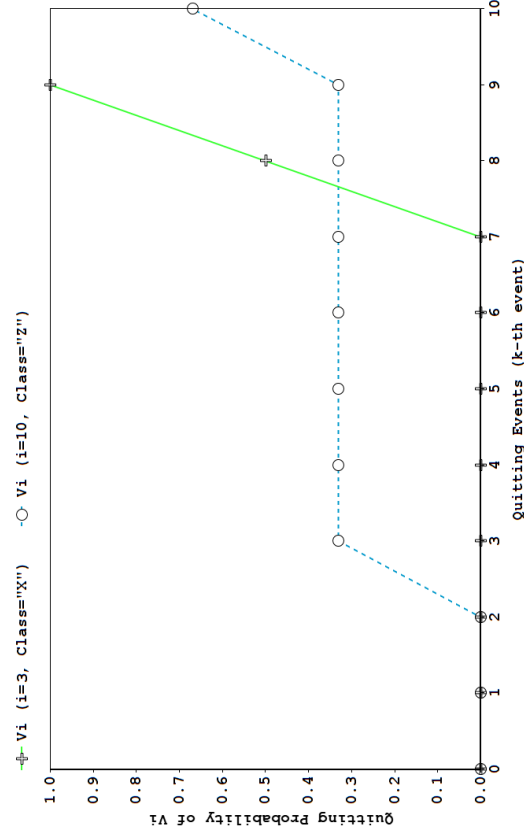


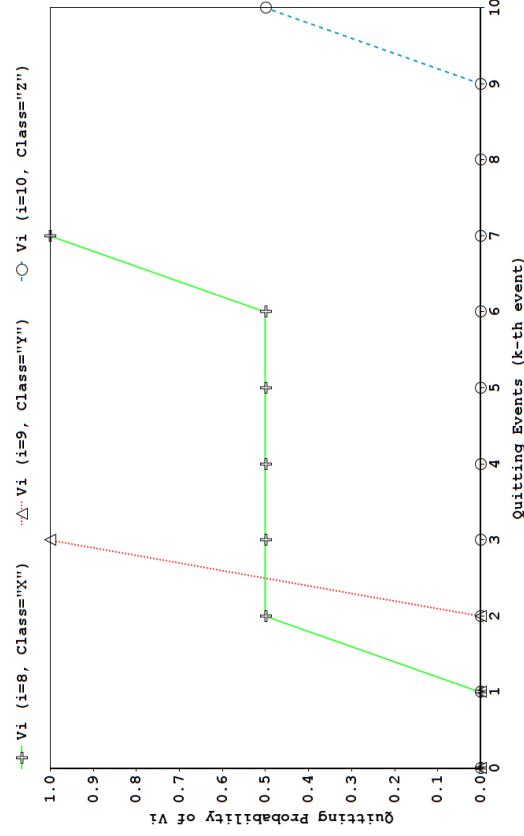
Figure 16: The simulation runs (scenarios*4)



(a) I.1



(b) I.2



(c) I.3

Figure 17: The four simulations of scenario I

as well since, by letting the adversary know about their quitting events, they affect the anonymity of other classes. The last category ("Z") comes with the best privacy level since it does not quit the the district letting its privacy preserved in addition to preserving other VSN users who share the same similarity. A similarity in our scheme reflect the gateway and heading, if a set of vehicles share the same gateway and heading then they are similar. It is important to mention that class "Z" had never been exposed with "100%" of quitting certainty in addition to the long privacy duration maintaining (the opposite of "Y" users).

Two other observations from the four results in Figure 17 show that (1) by reducing the number of "Y" users and rising the "X" users the overall users will last longer before the adversary starts identifying their quitting events (probability of quitting). (2) the change of quitting probability for all VSN users rises rapidly and this is due to that users do not share the same gateway and heading which means that if a user quits, he may be the only user in that district who has such gateway heading combination, thus, he will be rapidly identified and rapidly affect the privacy of his neighborhood.

4.3 Scenario II

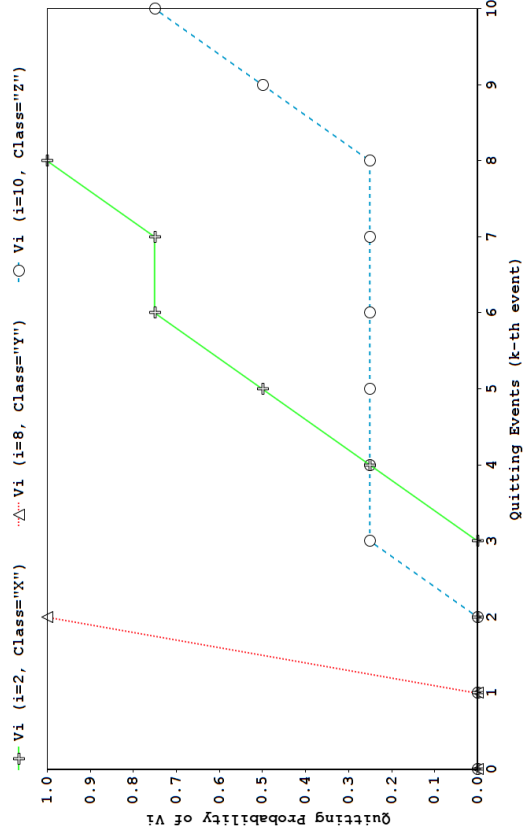
In this scenario, the scenario is formed by only one gateway but with two hidings. The taken Vehicle from each class is mentioned in the graphs (as in scenario I). The obtained results are the followings:

The results' interpretation is almost the same as in scenario I where "Y" users are the first to be exposed followed by the class "X" then lastly class "Z" maintains its privacy perfectly as in Figure 18. The additional observations are: (1) VSN users in II stay longer before being exposed and this is because more vehicles have the same similar since in such a scenario there is only one gateway and (2) despite the higher identification probability in compared to I, VSN users's probability does not change with big amounts thus the probability of knowing the quitting event needs that a lot of users quit in order to affect the privacy of the target.

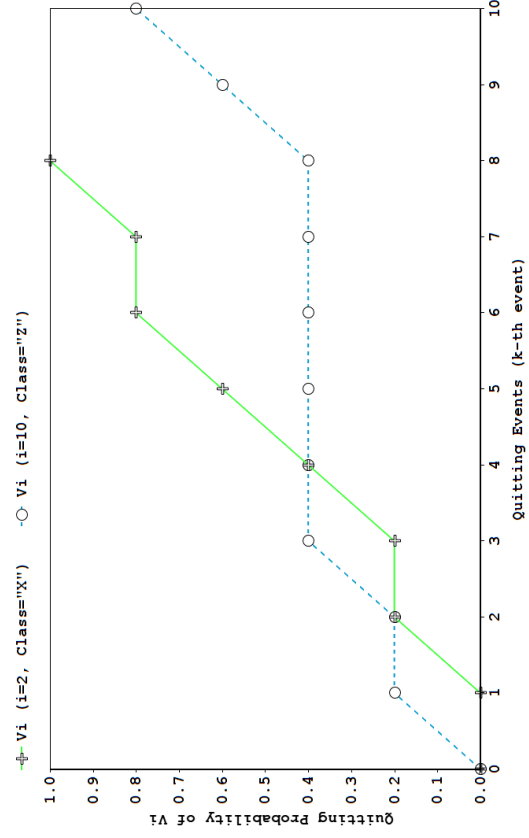
4.4 Scenario III

In this last scenario, the scenario is formed by one gateway and only one hiding. The taken Vehicle from each class is mentioned in the graphs. The obtained results are represented as follows:

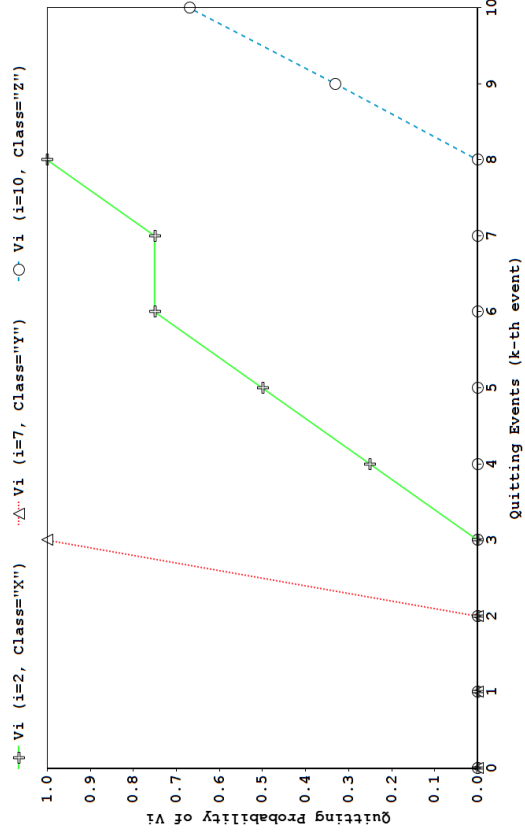
The VSN user in this scenario share the same characteristics as the previous two



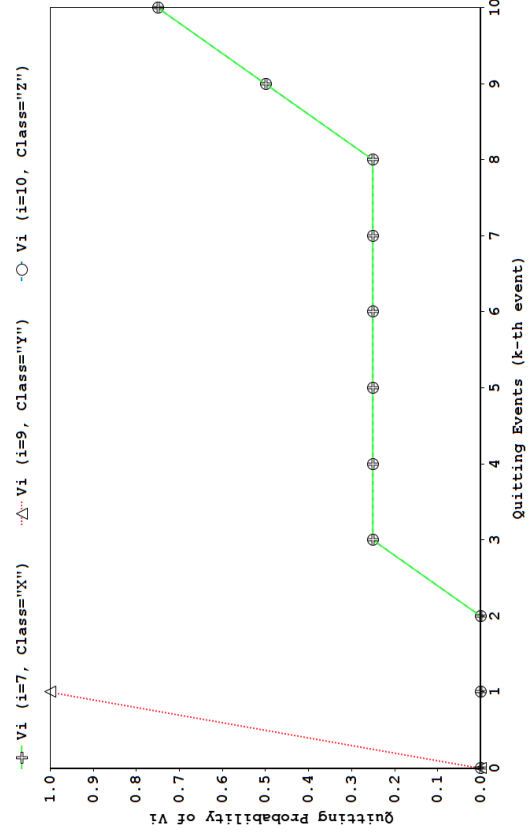
(a) II.1



(b) II.2



(c) II.3



(d) II.4

Figure 18: The four simulations of scenario II

scenarios e.g. class "Z" are the best in privacy preserving followed by class "X" then class "X" comes in the last place by observing Figure 19. The special characteristic in such scenario is that all VSN users are similar to be the target because of the unique gateway and heading and that is translated into the following observations: (1) VSN users stay longer than both the two scenarios (*I* and *II*) before being exposed (2) the users' (except "Y" users) probability of quitting is not rising with big amounts per quitting event thus the adversary needs more users to quit in order to be able to determine the quitting event of a monitored target.

4.5 Privacy of Vehicles After Leaving the District

We also provide a simple privacy measuring of VSN users who quitted the district. As said in the related works section, users' privacy is enhanced perfectly if they use the mix-zone strategy. By this definition, we evaluated each user's anonymity set size and the results are shown in Figure 20. The obtained results show almost good level even though the users had met only one mix-zone while in fact they would meet next other mix-zones hence: better privacy.

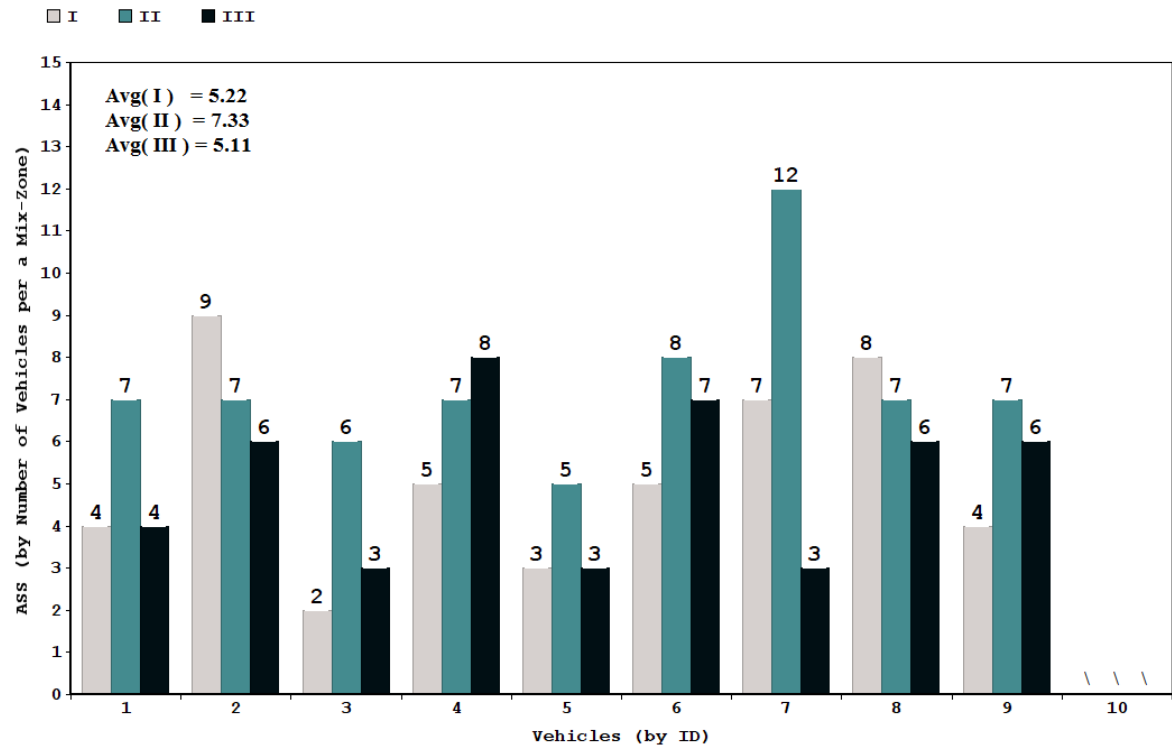
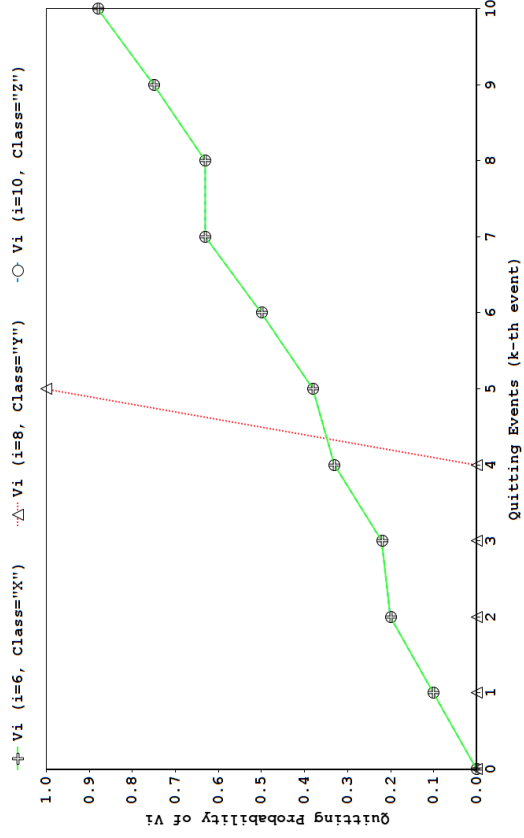
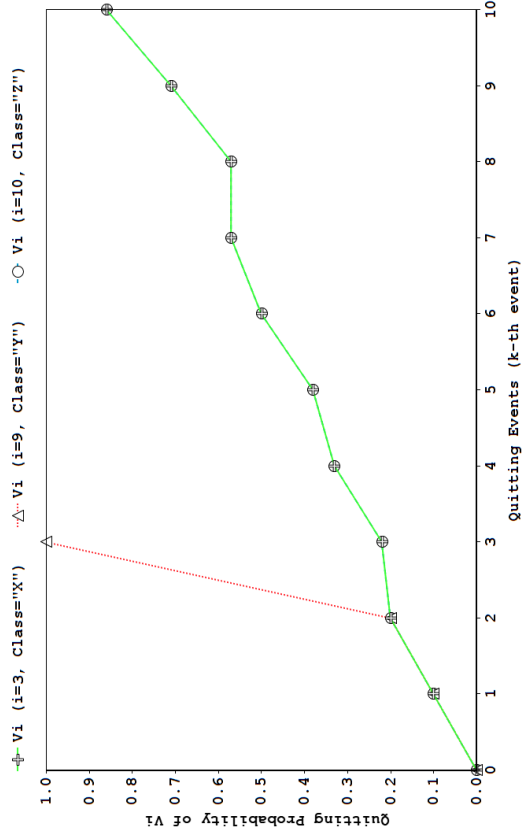


Figure 20: The anonymity set size(ASS) off all VSN users in All scenarios

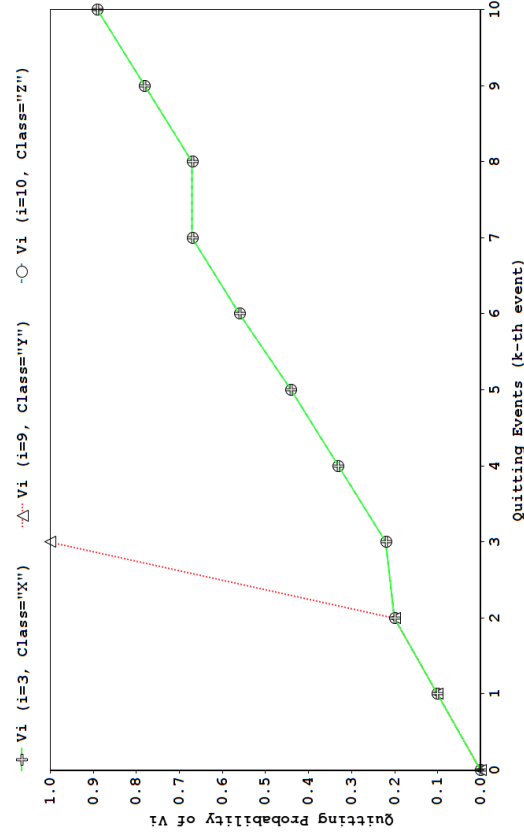


(a) III.1

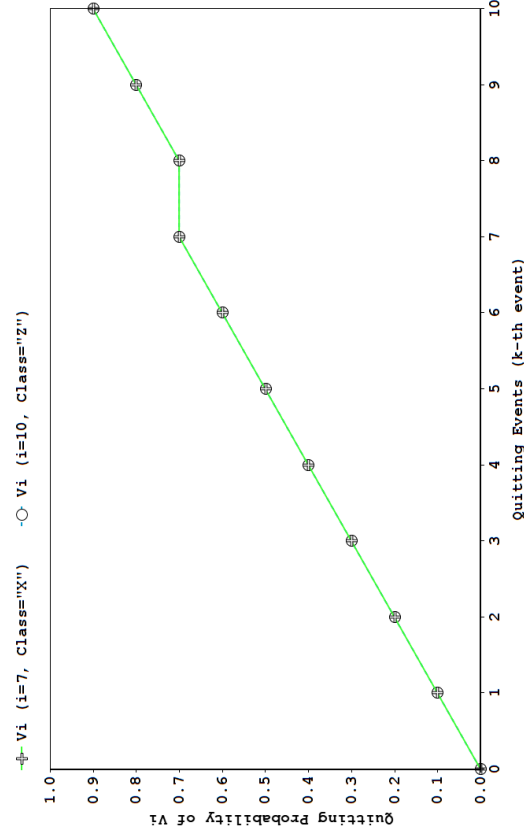
71



(b) III.2



(c) III.3



(d) III.4

Figure 19: The four simulations of scenario III

5 Location Privacy Protection and Overthrowing

In this section, we trend towards giving a holistic view on the location privacy problem but (basing on the entities that are illustrated in Figure 21) from two perspectives, namely: the ego-perspective and the adversary-perspective [111]. More details are given in the followings:

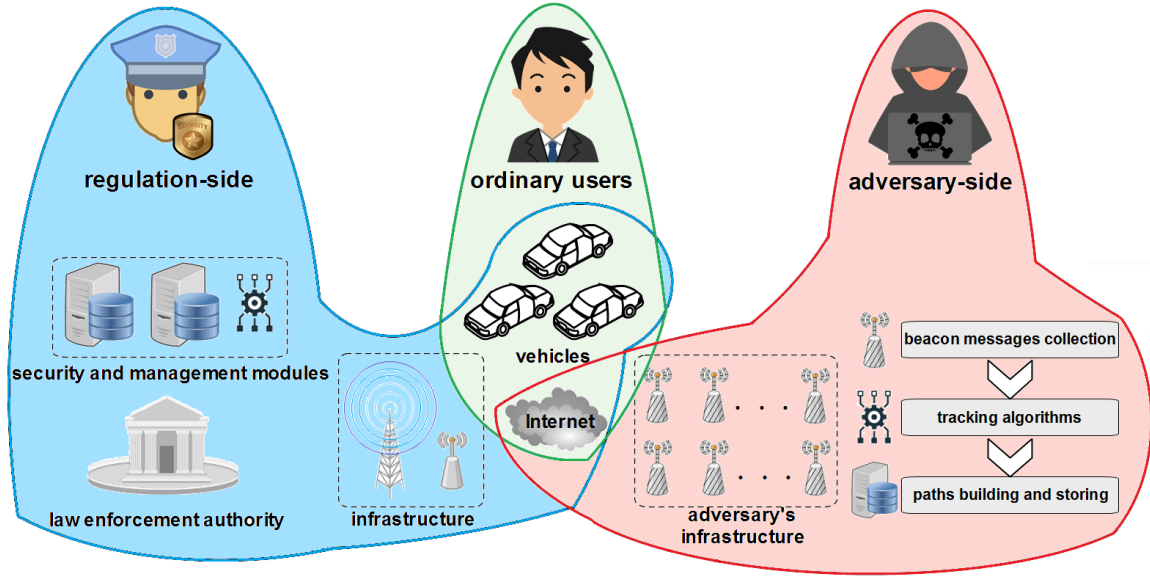


Figure 21: The relationships between the different entities including the adversary

5.1 Protecting Location Privacy, an Ego-Perspective

As the location privacy is a primary goal for the SCs users, and more precisely: the privacy advocates, the authority and regulation bodies devote their efforts to provide privacy-preserving solutions for a successful use of the SCs technology and its flourish.

To reiterate, understanding the goals and the trade-offs between the different privacy-preserving solutions is as crucial as proposing new mechanisms. In fact, it helps proposing robust and less trade-off implying mechanisms that do not affect drastically the overall SCs functioning.

In Figure 22, we show the benefits alongside exposing the negative impacts of some of the well-known mechanisms and modules used to cope with the location privacy issue. For instance, (1) the pseudonym change (may be accompanied with an exchange) do, remarkably, enhance the location privacy of the SCs users by thwarting the attacker when trying to trace and identify his targets based on their broadcasted BSMs. Yet, this triggers the network and routing applications to reestablish the routing tables as

the identifier is changed. Thus, confusing the attacker does also confuse the friendly applications. Some other techniques are used in conjunction with the pseudonym change, we talk about an efficient pseudonym change that takes into account the context of the SC in addition to the potential exploits that an attacker can benefit from, that is, (2) the advanced precaution module. Unfortunately, such a technique hampers a lot of safety applications, we mention for example the use of the encryption. It implies an additional decryption delay for those real-time safety applications. Another module, which is the most influencing as a privacy booster: (3) the silent period which is a period of time where the SC is not sending the BSMs. This conceals the whereabouts of the SC user but also affects drastically his safety; that is the privacy-safety trade-off.

Besides the modules, there are some other parameters that influence the application layers. In this perspective, namely the ego-perspective, all of (a) the use of pseudonyms, (b) the cooperativeness and (c) the density of SCs have a big impact on the location privacy as they reduce the precision of the attacker notably. But, and from the same perspective, the attacker level is seen to be an opposite factor that reduces the location privacy level of the SC users.

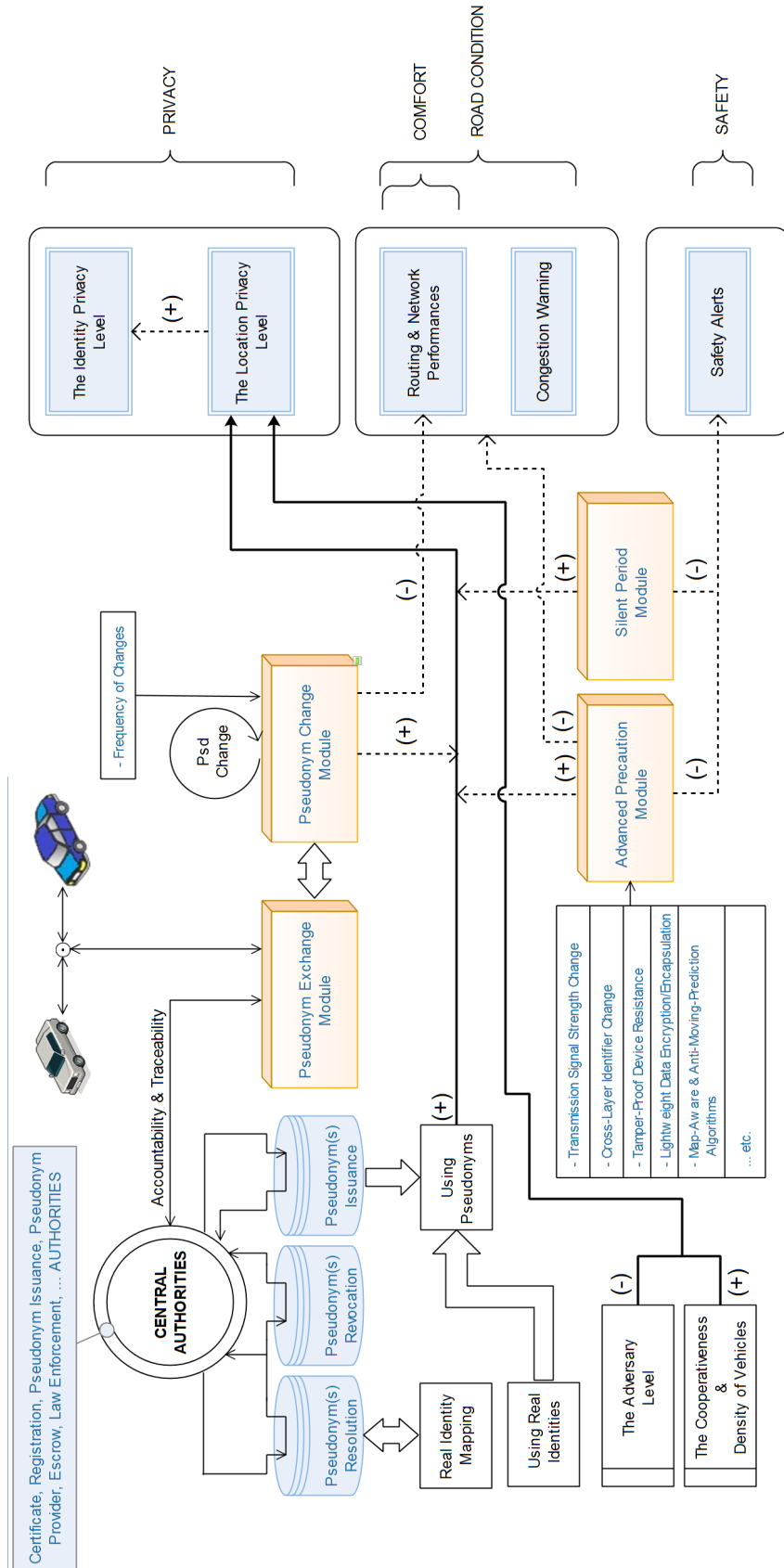


Figure 22: The location privacy protection from the ego-perspective

5.2 Overthrowing Location Privacy, an Adversary-Perspective

The attacker in the other hand has, as an objective, to overthrow the efforts of protecting the location privacy ongoing by the authority-side. With the same reasoning as the previous perspective, the attacker also possesses a set of modules and parameters (As shown in Figure 23) that are exploited with the intention of defeating the location privacy of the SC users. Among his main modules we find (1) the prediction algorithms. These later make intelligent mappings between the gathered locations and pseudonyms since they use mathematical models to calculate the next position and matching probabilities. (2) The license plate recognition systems had already shown their great potentials in determining the objects with the computer vision field, thus, a tracker may combine this module with his ordinary tracking process to achieve higher results. Additionally, leveraging (3) the historical data and analyzing it using the Artificial Intelligence (AI) [112] is considered to be a big influence towards very high precision and decisions that are taken by the attacker. Lastly, (4) the adversary type itself can influence the obtained results as, for example, a global eavesdropper can achieve better results than a local one.

A bunch of techniques can be used by the attacker as well and we cite some of the important ones as follows: (a) The eavesdropping stations' number, coverage and strength do all impact the successfulness of the attacker on tracking and identifying his target(s). Whilst (b) the faced privacy-preserving schemes do thwart him from achieving high objectives.

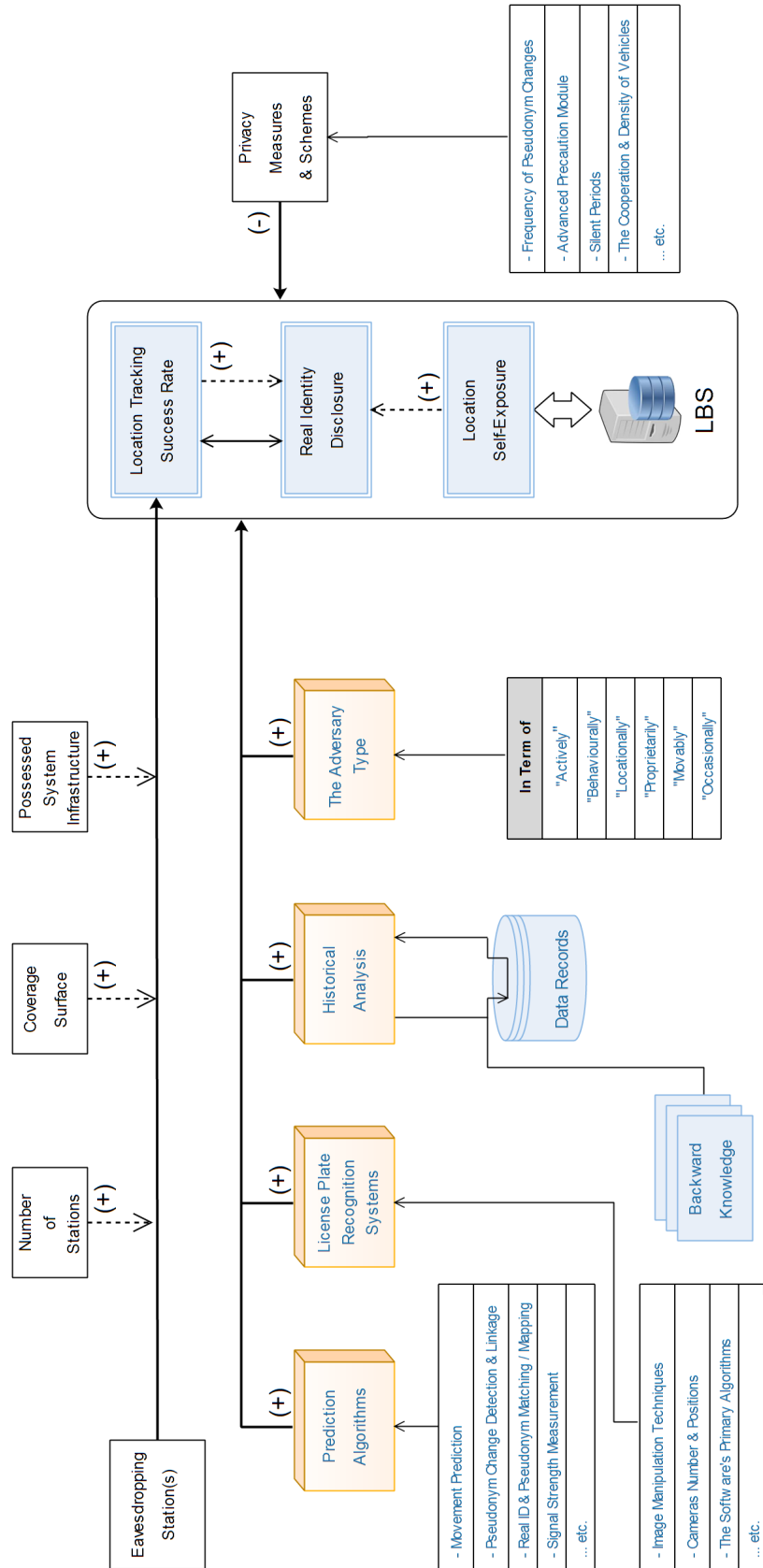


Figure 23: The location privacy Overthrowing from the Adversary-Perspective

5.3 Summarizing the Impacts, a Descriptive Table

We summarize in this part the aforementioned observations by giving a descriptive table (Table 7) that states the impact of both the authority’s and the attacker’s modules and parameters on the different application layers, namely: safety, comfort, road-congestion and privacy.

Table 7: The authority and the attacker and their influences on the application layers

		The Application Layers						
		Safety	Road Condition		Privacy			
			Congestion	Comfort				
Modules	Pseudonym exchange & pseudonym change		↓		↑	↓	Adversary type	
	Advanced precaution	↓	↓	↓	↑	↓	Historical analysis	
	Silent period	↓			↑	↓	LP recognition systems	
=====		=====		=====				
Parameters	Using pseudonyms				↑	↓	Eavesdropping stations' number, coverage & strength	
	Adversary level				↓			
	Cooperativeness & density of SCs				↑	↑	Faced privacy schemes	

6 Summary

In this chapter we investigated the issue of home and work (we named it end points) location privacy and identification problem. We did at first the introducing of our EPP scheme. We accompanied this with different simulations under various scenarios after we varied the number of gateways, headings and VSN users’ different classes (those who enable, disable or not leave the district) via extensive runs. The acquired results showed that the more the users follow the EPP scheme the more they are protected against quitting-event exposition. Additionally, we found out that the class "Y" VSN users affected negatively the privacy of other users. As a conclusion, we got that in order to ensure a high privacy levels, VSN users have to avoid being selfish and should be aware of the privacy terms at the aim of not only protect their own privacy but also others’. The nature of district and other parameters like the number of gatewats and heading have a significant impact on the achieved privacy level. Lastly but not least, EPP should be accompanied with a pseudonym change scheme like mix-zones in order to maintain the privacy of VSN users when they leave the district and that is to ensure their privacy in the outside environment.

Finally, we gave a conceptual framework study for the location privacy issues that

was in a two-fold view: the authority-side (ego-perspective) and the attacker-side (adversary-perspective). The two perspectives were compared vs the fundamental application layers that are safety, comfort, road-congestion and privacy. The conclusions were formulated in a table where the positive and negative effects of each module and parameters were presented.

In the next chapter, we see another interesting scheme that exploits the transmission range changing technique to enhance the location privacy of the drivers.

Journal and Conference Papers Related to the Chapter

Jr) Location-privacy evaluation within the extreme points privacy (epp) scheme for vanet users

Messaoud BABAGHAYOU, Nabila LABRAOUI and Ado Adamou ABBA ARI. "Location-privacy evaluation within the extreme points privacy (epp) scheme for vanet users". International Journal of Strategic Information Technology and Applications (IJSITA), 10.2, (2019), 44-58. (B-Rank)

Cn) EPP: Extreme Points Privacy for Trips and Home Identification in Vehicular Social Networks

Messaoud BABAGHAYOU, Nabila LABRAOUI and Ado Adamou ABBA ARI. "EPP: Extreme Points Privacy for Trips and Home Identification in Vehicular Social Networks". JERI, 2019. Algeria.

Cn) Between Location protection and Overthrowing: A Contrariness Framework Study for Smart Vehicles

Messaoud BABAGHAYOU, Nabila LABRAOUI, Mohamed Amine FERRAG and Leandros MAGLARAS. "Between Location protection and Overthrowing: A Contrariness Framework Study for Smart Vehicles". International Conference on Consumer Electronics (ICCE), 2021. Greece.

*Chapter IV:
Transmission Range Changing Effects on
IoV Users' Location Privacy*

*“It is during our darkest moments that we must focus
to see the light.”*

– Aristotle

1 Preface

In the same flow of proposing new techniques and schemes to cope with the privacy in IoV issue, this chapter apply the mechanism of transmission range changing/adjustment (we call it TRA) to enhance the identity and location privacy of IoV users. From the well-known privacy in IoV issues we state: identity exposing and location tracking. This is due to allowing vehicles to send their statuses to themselves via beacon messages (for the good). The changing of the transmission range while sending beacons to enhance the identity and location privacy was not exploited before in the literature and that what gets our motivation and attention to investigate this technique (TRA). In this chapter we see how does the level of location privacy be affected after we apply TRA on two location privacy schemes: SLOW and CAPS. We evaluate the two modified techniques against the achieved location privacy using a set of metrics and (2) the network performances. We also compare the used strategies in perspective of a set of security attacks.

The remainder of this chapter is organized as follows: In section 2, we give a background and demonstrate our system model and potential attacks. Then in section 3, we define the detailed functioning of our TRA mechanism, its characteristics and the complexity of the used algorithm followed by performance evaluation and that is in section 4. Later in section 5, we discuss the overall results of TRA, provide comparative table and give open work directions. Finally, we conclude our research in kind of a summary and that is in section 6.

2 Background

IoV, a special type of IoT [113], is considered as a hot research topic in the last few years. IoV comes to assist the design of Vehicular Ad-hoc Networks (VANETs) that focus on reducing the number of fatalities by enabling V2V, V2I communications over the DSRC protocol [26] in addition to the carious Vehicle-to-Everything (V2X) communications [27]. Thus, a fast reaction may be taken by drivers during dangerous situations. To achieve this goal, each vehicle has to periodically broadcast its status in terms of location, speed, velocity, time, etc. set in a beacon message. This kind of beacon is called BSM [28]. Despite the interesting V2X applications like vehicle platooning, incorporated sensors and automated driving, vehicles do suffer from some serious security and privacy vulnerabilities and issues.

For fast reaction and less delay, BSM content is not encrypted and sent at least once per second with a radius of about 300 meters [28]. Thus, any entity having a dedicated eavesdropping station would have an access to the driver's location and this will be exploited next to generate user profiles [114] which has a negative impact on the IoV users' location privacy. One of the solutions is to use pseudonyms instead of real identities while broadcasting these BSMs and furthermore, making them temporal and changeable over time [115]. Also, a cross-layer identifier (like mac and ip) change is needed [102]. However, if the pseudonym change was not done in an appropriate time and/or space, a correlation attack may be performed by the adversary to link the new and the old pseudonym. The aforementioned issue had motivated the research community to investigate the problem and develop a lot of robust schemes like [10, 24, 60, 68, 69, 72, 77, 84, 85, 98, 116, 117].

2.1 Network Model

In our network model, which is also represented in Figure 24, we consider the following entities:

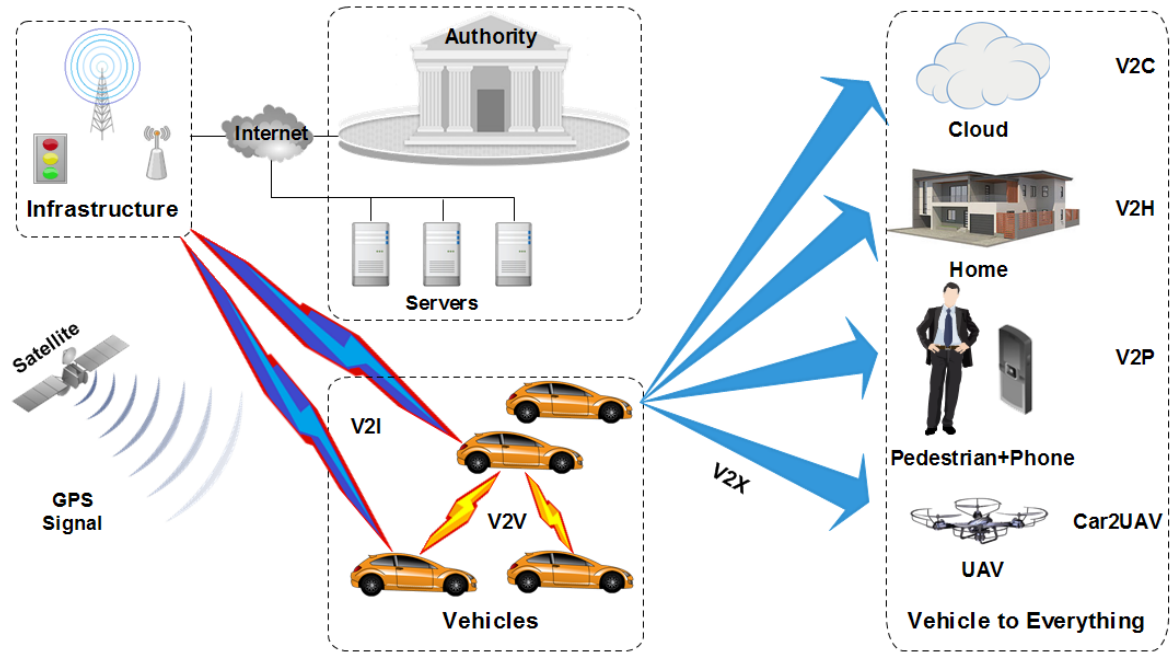


Figure 24: Network model illustration

2.1.1 Vehicles

They are the primary units that construct the IoV system. The set of vehicles is defined as $S = \{v_1, v_2, \dots, v_n\}$ where n is the total number of vehicles.

2.1.2 Infrastructures

They facilitate the connectivity between the different entities of the network for the different communication purposes. e.g., the Internet access.

2.1.3 Authorities

Depending on the type of the authority, each one has a specific role like: distributing the pseudonyms, issuing them, making a pseudonym resolution or revocation process, etc.

2.1.4 Extension hosts/things

The V2X technology makes it possible to benefit from a lot of connections and communication types including Vehicle to Cloud (V2C), Vehicle to Home (V2H), Vehicle to Pedestrian (V2P), Car to Unmanned Aerial Vehicle (Car2UAV), etc.

2.2 Adversary Model

The threat model taken in our study is the GPA model [41] which is considered as a strong adversary with, almost, a full coverage. For this, the adversary uses some eavesdropping stations that are fully distributed after studying their necessary numbers in accordance with the vehicles' ordinary transmission range. In location privacy perspective, this attacker seeks, with the use of these eavesdropping stations, to make spatial and temporal traces of his target(s) at the aim to breach their privacy by tracking them and making a profile generation. The model is described in Figure 25. The GPA, in fact, can execute a bunch of attacks as surveyed in [63] and is considered as the used threat model in most of VANET and IoV privacy schemes.

2.3 Potential Privacy Attacks

The IoV had opened, in addition to its beneficial applications and services, a bunch of security and privacy threats [7]. We mention in the following some of the attacks that target the IoV users:

- Eavesdropping: the eavesdropping attacks is defined as collecting the sent data from the different targets at the aim of getting useful information for divers and further treatment (a preamble to other attacks).
- Location tracking: is a step after executing a successful eavesdropping attack. The adversary exploits the collected packets in order to track the target by his position.

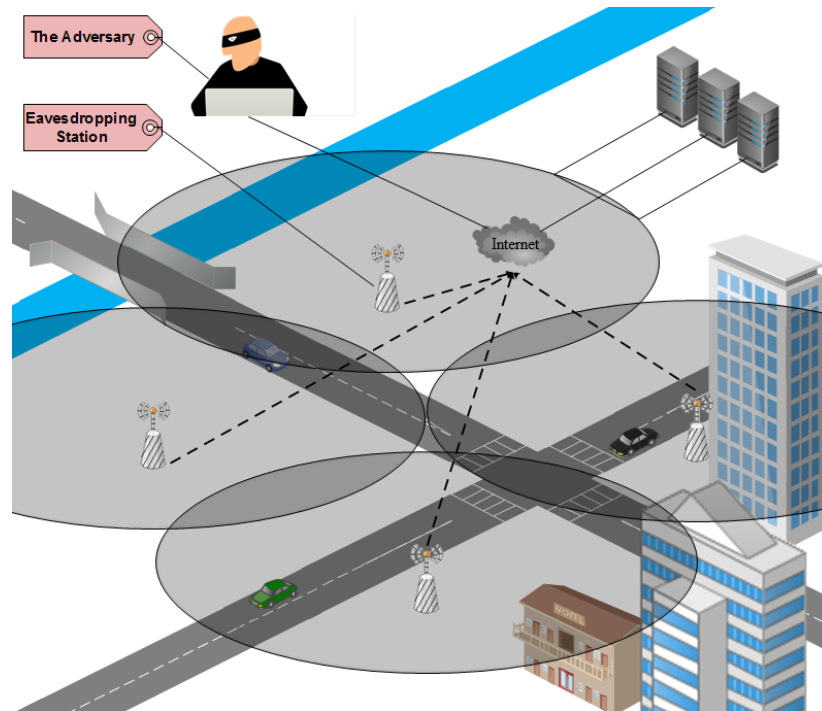


Figure 25: Adversary model illustration

The reasons of course are not predefined, ranging from stalking celebrities to criminal and assassination operations which makes it a sever attack.

- Bogus information: this attacks bases on altering and/or creating false data and spread it on the IoV system. Generally, it is for disturbing the overall functioning for their own benefit.
- Impersonation: getting an authentication to access, use and participate in the IoV system would be possible by impersonating other legitimate entities. The grants from such a successful attack not only gives the adversary the option to insert false data and benefit from the services, but also affects the reputation of the innocent impersonated vehicles since he participates on-behalf of them in addition for him being able to receive some sensitive data.
- Denial of Service: the DoS attack is considered as the most powerful attack that targets the availability requirement. The way this attack is realized may take different forms like jamming the channel and the resources consumption attacks. The aim here is to render the target unable to participate and intercept the communications, i.e., out of order.

3 Transmission-range Control Adaptation

3.1 Demonstration and Motivation of the Study

Motivated by the fact and the observation that the adversary distributes his eavesdropping resources basing on the transmission range of vehicles in order to get a full coverage, we tend to adjust the transmission range of vehicles in order to overcome this full coverage and to make this full coverage a quasi-full coverage. The simulation study will show whether this feature's exploitation will bring forth an addition in term of location privacy and network performances or not. The principle of the TRA feature is simple, vehicles on-the-fly adjust their transmission power for the purpose of occasionally hiding themselves from the full coverage of the pre-installed adversary eavesdropping stations. The more the speed is high, the more power vehicles will use in order to impose their presence in the neighborhood. Vice versa, when the speed is low, they reduce their transmission power while broadcasting BSMs. The motivation behind this adjustment is because the risk of fatalities will be considerably low when the speed is low. Hence, informing the very close neighbors is sufficient. The same reasoning happens with high speeds; they introduce high crashes probabilities. The TRA does not apply for emergence and high level dangerous situations, e.g., accident events dissemination.

We used TRA on two already-existing schemes: (1) SLOW [77] that is proposed by Buttyán et al. and that lets vehicles independently decide the right moment, according to their own speeds when it drops under a certain threshold, to change their pseudonyms. Indeed, in low speeds the risk of accidents will be low. Thus, the vehicle is allowed to use silent periods. The only issue is represented in the standardization contradiction which oblige a beaconing frequency of at least once per second. We also used (2) CAPS: Context-Aware Privacy Scheme [98] that is proposed by Emmara et al. and that lets vehicles choose the appropriate context to enter the silent period and change their pseudonyms.

In our study, the values of the range-speed settings are taken heuristically. The TRA is illustrated in Figure 26.

3.2 Choice of Transmission Powers

To well-choose the appropriate transmission power for the corresponding distance, simulating various transmission powers and varying the distances between vehicles was necessary. We had chosen speed ranges in where the vehicles will adjust their

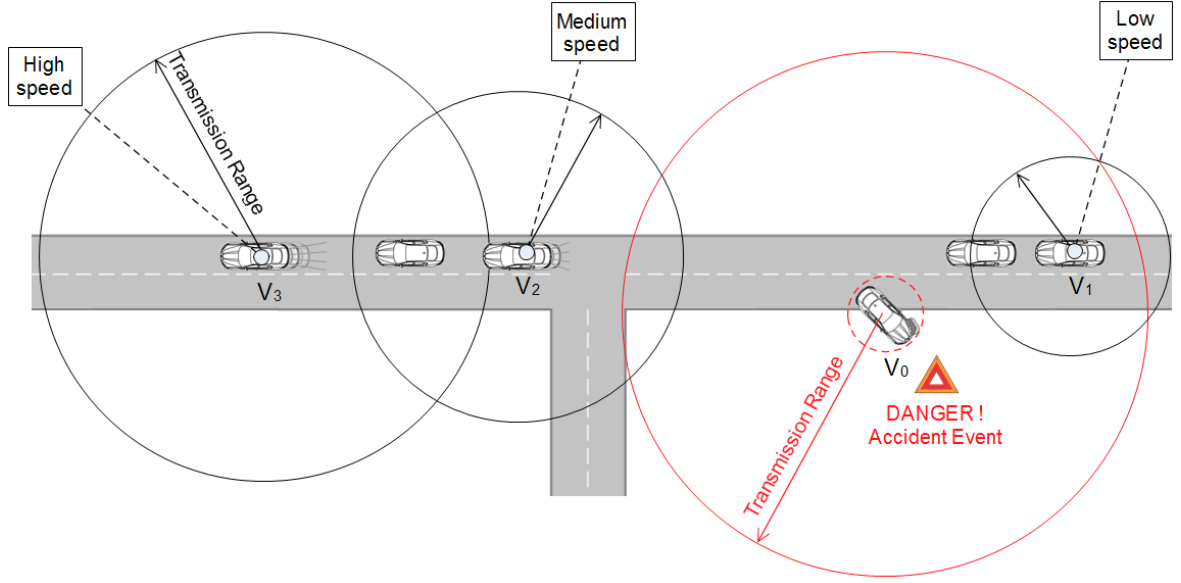


Figure 26: A TRA functioning scenario

transmission powers accordingly. The results are summarized in Table 8.

Table 8: The transmission range, the needed power and the triggering speed values of TRA

Transmission Range (m)	50	100	200	300
Needed Power (mw)	0.2	0.8	3.1	7
Triggering Speed (km/h)	[0..30[[30..50[[50..70[[70..+

However, in reality the transmission range is also affected by factors other than the transmission power like obstacle shadowing, interference, alpha factor, etc. For more details, we refer the reader to take a look at this paper [118].

3.3 Pseudo-Algorithm of TRA

The principle functioning is also explained, in kind of pseudo-algorithm, in Algorithm 1:

3.4 Complexity of TRA

The TRA technique's calculations are just represented in Algorithm 1, thus, the resulting complexity is that of the algorithm. We state four potential states:

- when speed is below 30km/h as the first possibility.
- when speed is above 30km/h and below 50km/h as the second possibility.

Algorithm 1 Beacon Transmission Range Adjustment

```

1: procedure CONTEXTUAL_BEACONING(BEACON* BSM)
2:   Prepare_Beacon(BSM);
3:   if ((Trn_Rng_Is_Active) and (No_Danger)) then
4:     if (Speed < 8.33) then ▷ m/s (30km/h)
5:       nic.mac80211p.txPower ← 0.2;
6:     else if (Speed < 13.89) then ▷ m/s (50km/h)
7:       nic.mac80211p.txPower ← 0.8;
8:     else if (Speed < 19.44) then ▷ m/s (70km/h)
9:       nic.mac80211p.txPower ← 3.1;
10:    else ▷ i.e., more than (70km/h)
11:      nic.mac80211p.txPower ← 7;
12:    end if
13:  else ▷ i.e., using 7mw for the default 300m radius
14:    nic.mac80211p.txPower ← Default_Value;
15:  end if
16:  Send_Beacon(BSM);
17: end procedure

```

- when speed is above $50km/h$ and below $70km/h$ as the third possibility.
- when speed is above $70km/h$ as the fourth possibility.

We also recal that the two methods, namely: $Prepare_Beacon(BSM)$ and $Send_Beacon(BSM)$ are not apart of the additional TRA technique as all schemes need to employ these two methods, thus, there complexity is aside of TRA.

The four potential states (Ptn_stt), in the worst of cases are evaluated as 4 instructions in each iteration. The number of iterations per second are related to the frequency of beaconing, i.e., packets number (Pck_nbr). According to the standardization, the frequency of beaconing ranges from 1 to 10 beacons per second, hence, the overall complexity is as follows:

$$\mathcal{O}(Pck_nbr * (Ptn_stt)) = \mathcal{O}(10 * 4) \quad (10)$$

Which means that the complexity is just:

$$\boxed{\mathcal{O}(1)} \quad (11)$$

3.5 Strong Points of TRA

TRA can be expected to valuably enhance the location privacy of users when combined with other strategies. This is due to its flexibility in adjusting the transmission range according to the vehicle's context which nullifies the full coverage of the GPA adversary letting it be a quasi-full coverage. The model of GPA itself, in practice, is hard to be achieved, i.e., somehow needs some national capabilities or a tremendous collaboration of many individuals and companies. Another important benefit that may come forth with the TRA is the network performance enhancement since the transmission range is reduced this will decrease the number of BSM packets collusion resulting in bandwidth-preserving for safety-related messages. The TRA does not affect routing and other VANET functionalities since it only operates, conditionally, for BSMs.

3.6 Probable Drawbacks of TRA

We can expect that TRA has some weak points like when the adversary changes his pre-installed eavesdropping stations, i.e., its capabilities in order to make sure he always have a full coverage (or, at least in some regions of interest). However, we believe this is an extremely hard task if it is not impossible since just the GPA model is considered expensive. As an example, a region of $3 * 3 \text{ km}^2$ will need about $8 * 8$ eavesdropping stations that are well-distributed just to achieve the aforementioned GPA model (i.e., of 300m radius coverage). If the adversary wants to overcome the TRA feature, a lower bound of transmission range (i.e., of 50m radius coverage) must be taken into consideration by him resulting in about $43*43$ eavesdropping station which is extremely expensive and hard to be implemented (≈ 29 times more expensive than ordinary GPA costs in the same $3 * 3 \text{ km}^2$ map). TRA may also affect, if coordinated with, other strategies that benefit from the beacon messages sent by the neighboring vehicles to achieve a synchronization or beneficial pseudonym change. Thus, TRA introduces a trade-off between such strategies' effectiveness and the adversary's eavesdropping range limitation.

4 Performance Evaluation

4.1 Simulation Setup

To evaluate the TRA feature and study its effects on the location privacy and the network performances, we used OpenStreetMap ([OSM](#)) [119] database to extract a

portion of Tlemcen town, Algeria map. With the use of [SUMO](#) mobility simulator [120], we transformed the map taken from OSM into a road network readable file for SUMO (see Figure 27 for the opened file after using the NETEDIT tool for visualisation) in where we generated four sets of vehicles using the python script *Randomtrips.py*. We used the Arrival rate command by varying the binomial options like the “-p” that is followed by $((t1 - t0)/n)$ where $t1$ and $t0$ are the end and start times of vehicle arrivals respectively (for a simulation time of 300s) and n is the desired number of vehicles. The results are represented as Inter-arrival times as in Table 9.

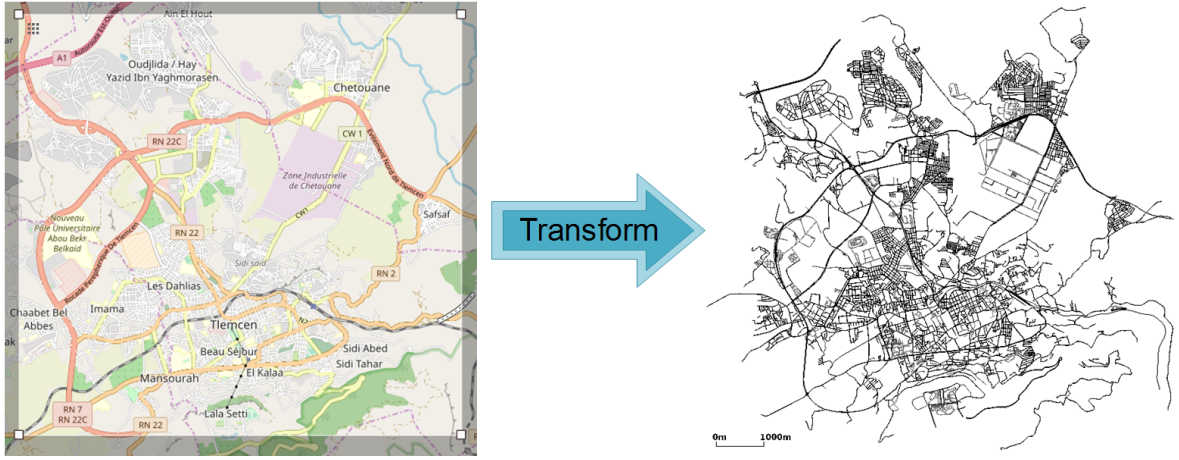


Figure 27: The taken portion of Tlemcen town, Algeria map

We integrate the TRA on some of the known privacy-preserving strategies in order to evaluate its impact on both (1) the location privacy and (2) the network performances.

For the network simulator, we use [OMNeT++](#) [121]; the component c++ based and discrete events simulator. OMNet++ allows the integration of diverse frameworks depending on the simulation nature like Veins [118]; the vehicular network simulator. Veins acts as a bridge between the mobility simulator SUMO and the network simulator OMNet++. We also employ the PREXT extension [122] that is developed by Emmara et al.; a Veins extension that integrates a set of privacy-preserving strategies and a set of the well-known metrics to evaluate the achieved privacy like the Anonymity

Table 9: The simulation parameters

Inter-arrival Times (s/veh)	6	3	2	1.5
Number of Generated Vehicles by SUMO (veh)	49	99	149	198
Tlemcen Map Size (km²)	≈ 100 (9.93x9.6)			

Set Size (ASS), Entropy, Traceability, confusions per pseudonym change, confusions per trace, etc. The way these metrics are developed are well-described in [115]. An illustrative diagram is elaborated in order to facilitate the comprehension of the interaction between the different simulation tools (shown in Figure 28). We integrate the TRA on some of the known privacy-preserving strategies in order to evaluate its impact on both (1) the location privacy and (2) the network performances.

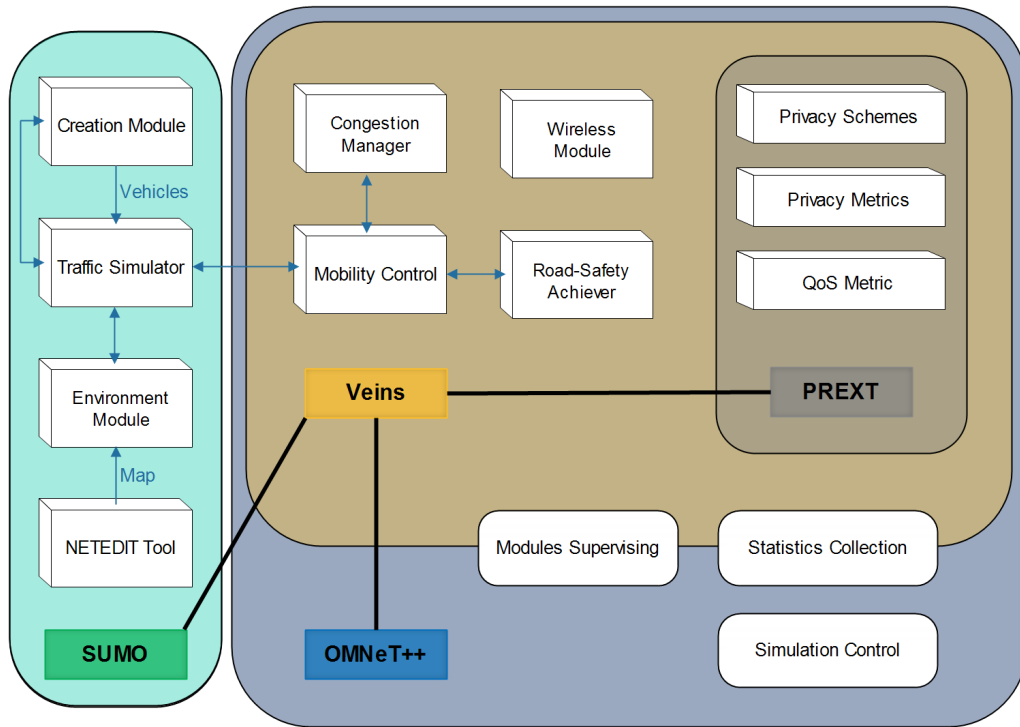


Figure 28: The illustrative diagram of the different used simulation tools

4.2 The impact of TRA on Location Privacy

As explained, TRA is integrated into SLOW and CAPS schemes in order to evaluate the resulting location privacy level. For this aim, the traceability, the confusions per pseudonym change and the confusions per trace metrics are used to see how the privacy level before and after using the TRA feature. As expected, since SLOW and CAPS themselves choose the perfect opportunity to change their pseudonyms; i.e., are user-centric approaches, the TRA integration had remarkably enhanced their performances. Figure 29, Figure 30 and Figure 31 show the achieved location privacy of SLOW and CAPS with and without the use of the TRA feature. The variation of vehicles number almost did not affect the achieved location traceability for both the pure and the enhanced strategies but the position of generation, trips and moving

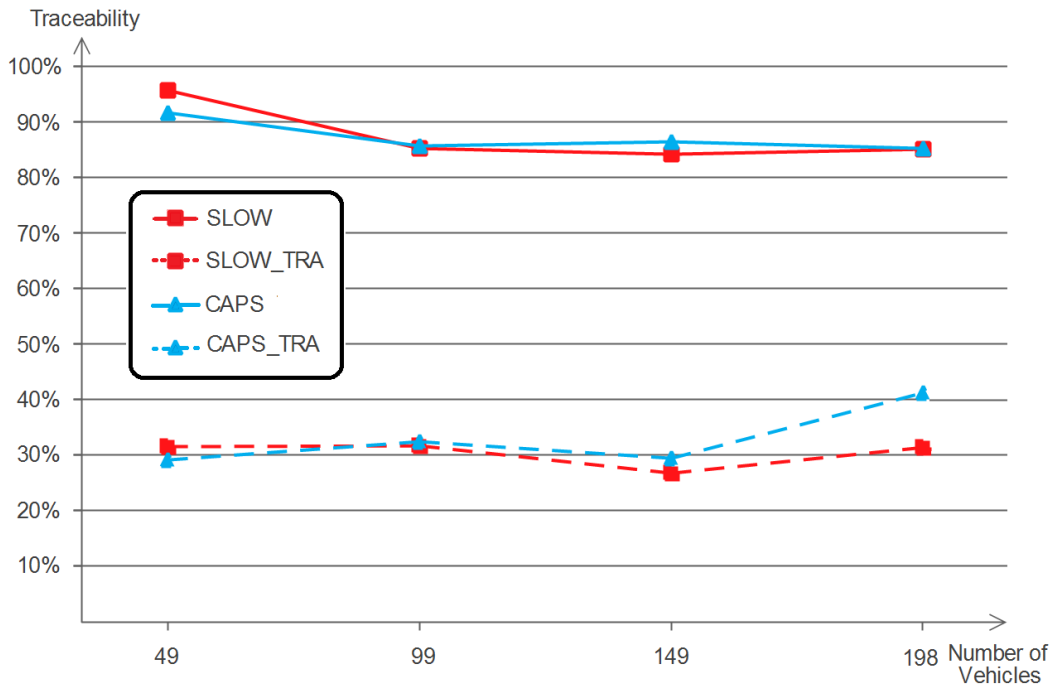


Figure 29: SLOW, CAPS, SLOW_TRA and CAPS_TRA traceability measuring

patters used by SUMO were responsible for some remarkable high and low values but still the overall interpretations is preserved.

4.2.1 The resulting traceability

Figure 29 shows an important enhancement represented as about a +54% (in both 99 and 198 vehicles) and about a +44% (in 198 vehicles) of minimum location privacy gain for SLOW and CAPS respectively. And most importantly, about a +64% (in 49 vehicles) and about a +62% (in 49 vehicles) of maximum location privacy gain for SLOW and CAPS respectively.

4.2.2 The resulting confusions per pseudonym change

Figure 30, by the same logic, proves that both SLOW and CAPS in their enhanced version (TRA) perform well than the normal ones with a variation between 3 to 14 confusions per pseudonym change with a remarkable high value in the 99 vehicles scenario that is, in our opinion, related to the generated trips resulted from the SUMO mobility simulator which uses random trips but the overall results still confirm the superiority of the enhanced schemes over the normal ones in addition of being SLOW better than CAPS in the same scope.

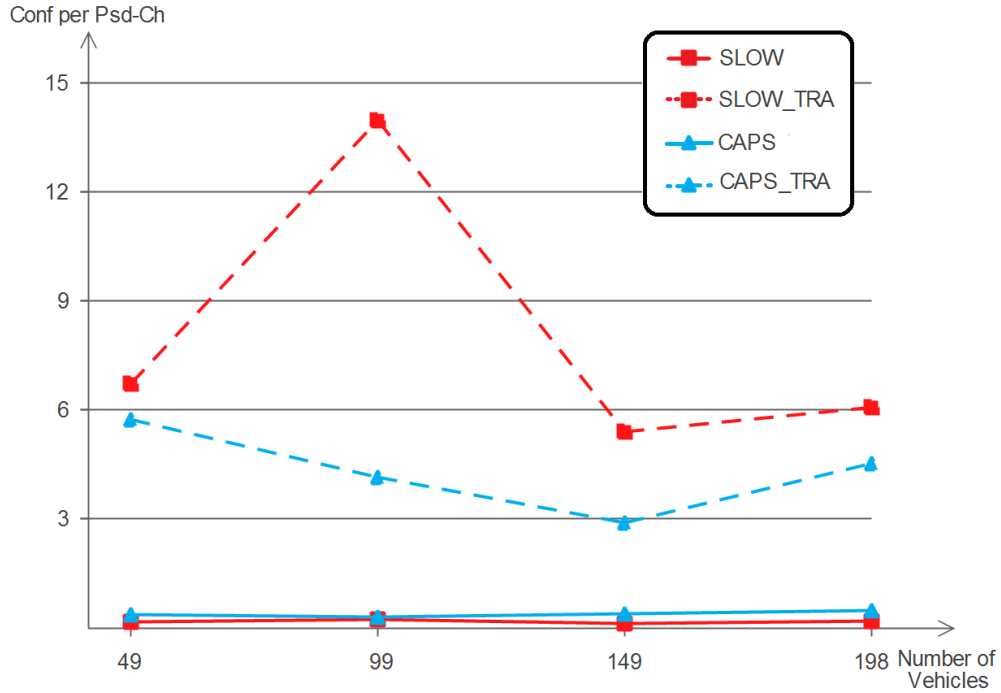


Figure 30: SLOW, CAPS, SLOW_TRA and CAPS_TRA confusions per pseudonym change measuring

4.2.3 The resulting confusions per trace

Figure 31, shows the achieved confusions per trace measure. Similarly to Figure 31's interpretation, the enhanced schemes still outperform the normal one (with SLOW being better than CAPS in the same scope) except for the 99 vehicles scenario which is also affected by the random generation of vehicles movement and trips. The value of confusions per trace varies from 0.1 to 1.1 under the four vehicles number scenarios.

4.2.4 The achieved maximum anonymity set size and maximum entropy per trace

We also aimed at comparing between the normal versions of SLOW and CAPS in other metrics like the maximum anonymity set size per trace (Figure 32) and the maximum entropy per trace (Figure 33). The results are as follows:

The results clearly show that SLOW performances exceed that of CAPS. SLOW varies from 0.4 up to 0.6 meanwhile CAPS varies from 0.2 to about 0.29 in its better performances (in the 149 vehicles number).

SLOW in here also outperforms CAPS. At the same time, both schemes did not perform well in low vehicles number scenario which is apparent in the 49 vehicles scenario. Then, their performances rise up 0.031 for SLOW and 0.013 for CAPS. The

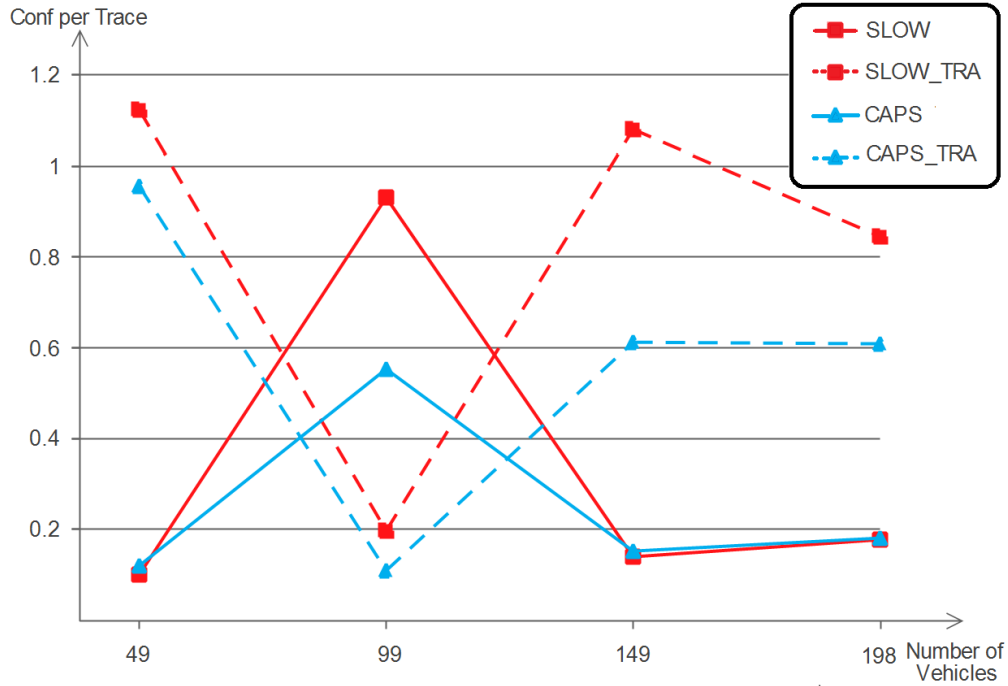


Figure 31: SLOW, CAPS, SLOW_TRA and CAPS_TRA confusions per trace measuring

convergence of the maximum entropy per trace is visible by augmenting the number of vehicles.

4.3 The impact of TRA on Verified Beacons

This evaluation aims at study the impact of the proposed TRA feature on the network performances, more precisely, the verification of received BSMs. It is already known that the augmenting of vehicles number had a negative impact on the VANET and IoV systems, like that of the broadcast storming problem. Hence, it makes it not scalable. Firstly, the effect of pure and enhanced SLOW scheme was investigated in Figure 34. it is very clear that the augmenting of vehicles number resulted in an almost exponential number of received beacons in comparing with the number of sent ones. Indeed, if a vehicle sends a beacon in a crowded area, a lot of vehicles will receive it. Effectively, after using the enhancement of TRA, the number of received beacons was dramatically reduced achieving a -55% (in 198 vehicles) of minimum and a -76% (in 49 vehicles) of maximum less broadcasts reception.

The same thing occurs with the CAPS scheme as shown in Figure 35, where an achievement of a -64% (in 198 vehicles) of minimum and a -81% (in 49 vehicles) of maximum less broadcasts reception. It is also important to mention that the reason behind the less sent and received broadcasts in SLOW is because the scheme, by nature,

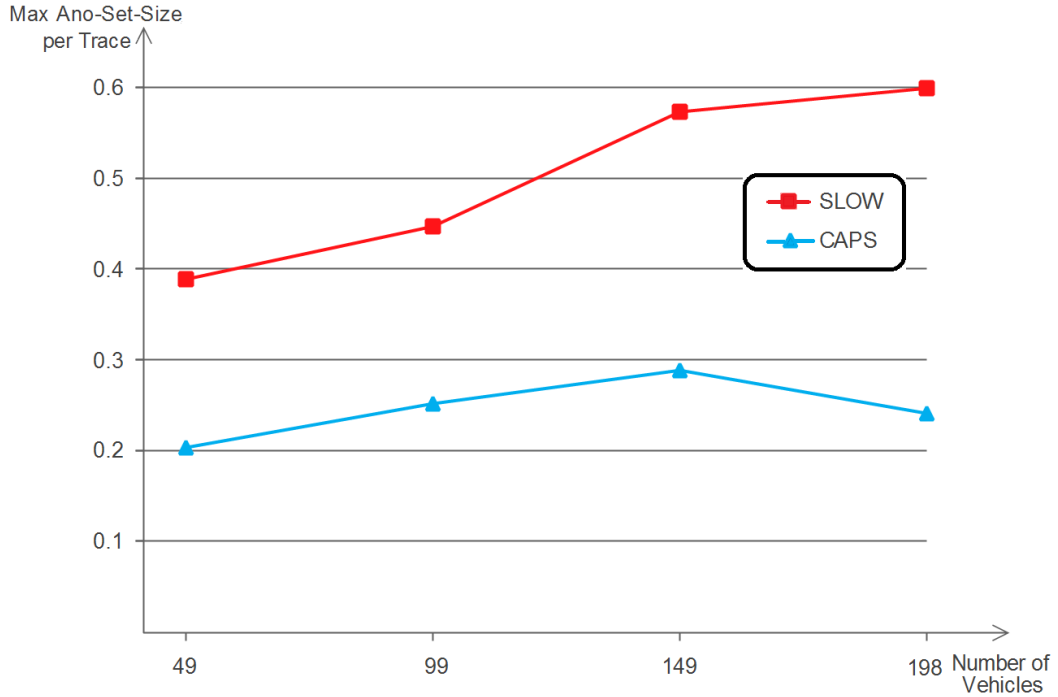


Figure 32: SLOW vs. CAPS using the maximum anonymity set size per trace metric

uses the silent period which is translated in no broadcasts while the vehicles are silent.

From the two network performance evaluations, it is clear that TRA, in conjunction with SLOW and CAPS, has enormously enhanced the network performances and the number of BSM signatures verification while protecting the safety of drivers (since they can rise the transmission range when driving with high speeds; where a necessity of wide line of sight and presence informing to the neighborhood is needed).

5 Discussion, Comparison and Open Work Directions

Generally speaking, from the previous two evaluations namely (1) the location privacy and (2) the network performances evaluations, it is clear that TRA brings an enhancement to the system in addition to thwarting the adversary by limiting his pre-installed stations' capabilities. However, TRA may not work perfectly with schemes that use the neighboring vehicles number estimation feature. This is natural, since these schemes rely on broadcasts coming from the neighborhood despite of the speed and the safety-situation; despite the transmission range. With this in mind, the adaptation of TRA, which is beneficial after the reported simulation results, can be integrated in strategies that use an independent (user-centric) context to enhance their performances.

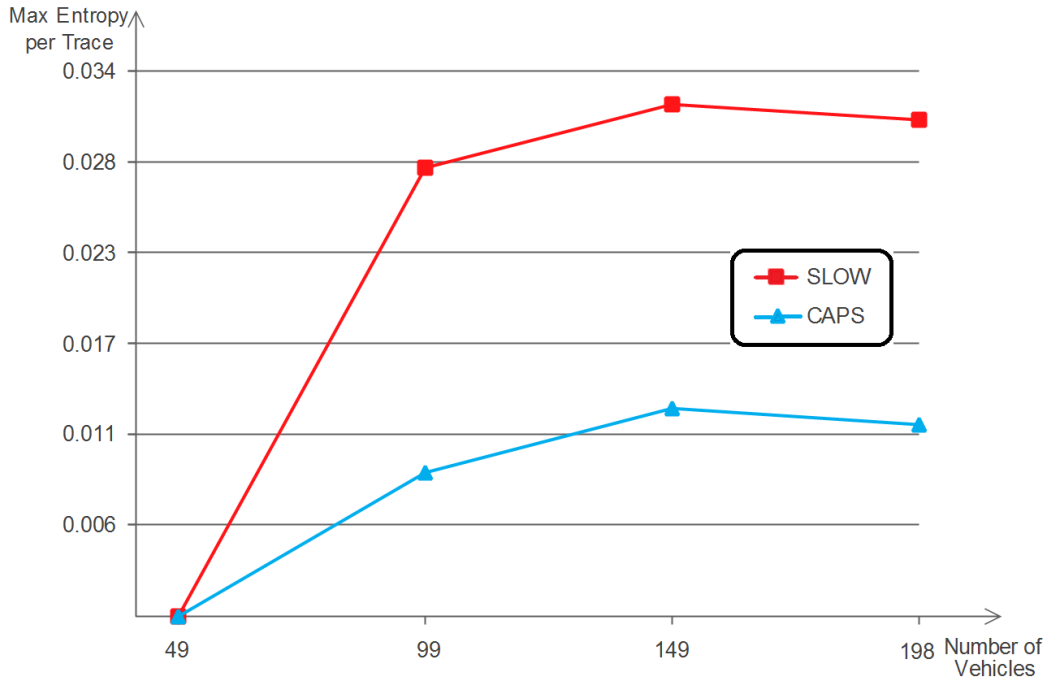


Figure 33: SLOW vs. CAPS using the maximum entropy per trace metric

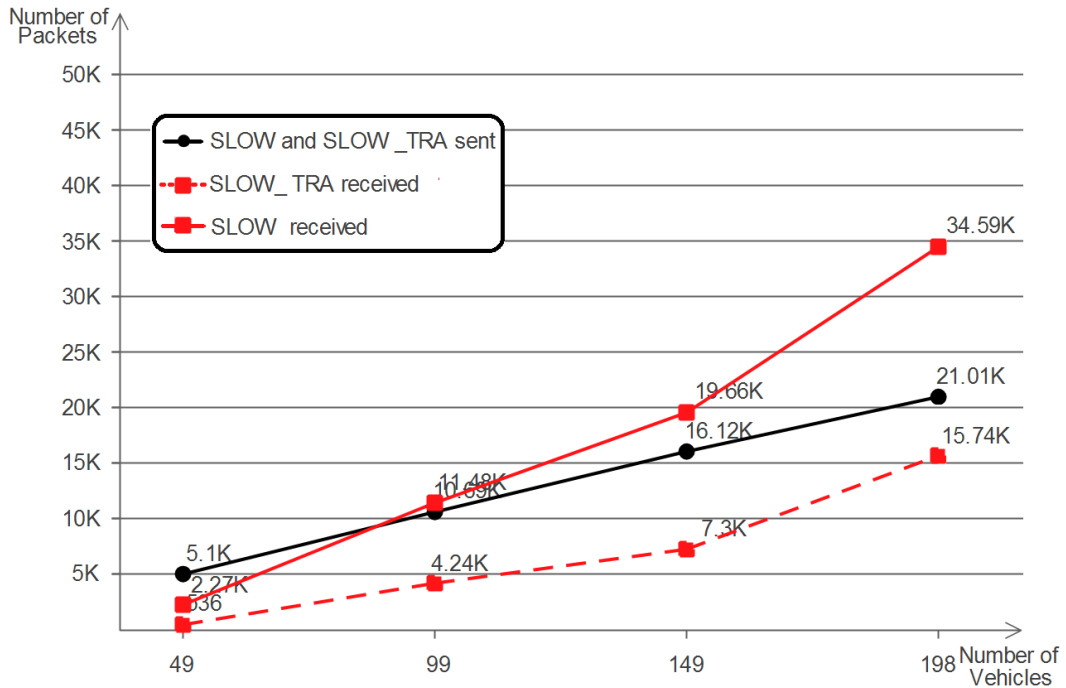


Figure 34: SLOW and SLOW_TRA network performance evaluation by sent and received BSM packets

Both bogus information and impersonation attacks are not possible for all schemes, thanks to the authentication by certificates mechanism used by most of privacy-preserving schemes; the adversary is only able to be authenticated if he has

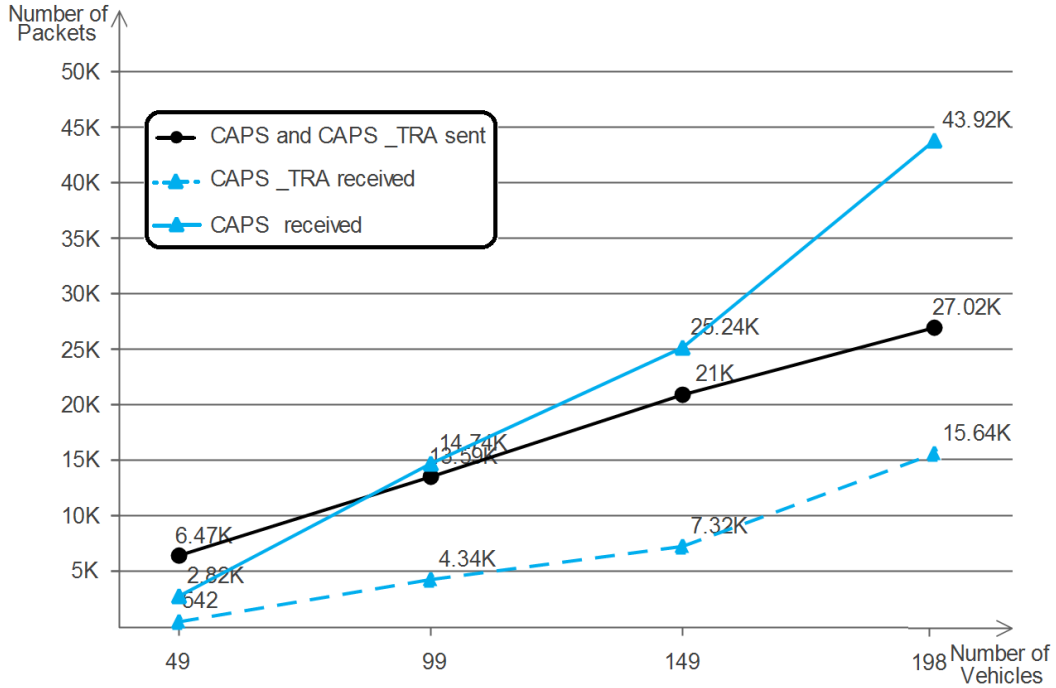


Figure 35: CAPS and CAPS_TRA network performance evaluation by sent and received BSM packets

a valid signed certificate from the appropriate authorities. By the other hand, the DoS attack is feasible as most of the techniques of this attack exploits the physical nature of the wireless shared medium and the known frequency band for the wireless communications, thus, the four schemes are vulnerable to such an attack. For the eavesdropping (the preliminary) and the location tracking (the next step) attacks, it is so obvious that the adversary is dramatically hampered since he is, in some occasions, unable even to get the broadcasted beacons after the vehicles using the TRA technique reduce their transmission range.

More importantly, we are now motivated to develop a pseudonym change scheme that includes and bases on the TRA feature in order to obtain a high level of privacy since TRA is both location privacy and QoS friendly. Another important evaluation may also be conducted; the study of the internal adversary(s) effects. i.e., when other vehicle members act as eavesdropping stations to extend and defeat the TRA mechanism.

6 Summary

In this chapter, we applied the Transmission Range changing/adjustment (TRA) which bases on the contextual transmission power control while sending beacon

messages for the location privacy problem. For the best of our knowledge, the technique was not exploited before in the field of location privacy in IoV by the other privacy schemes. As a result, we integrated TRA into two of the privacy schemes: SLOW and CAPS and that was in order to evaluate their performances. From the simulations, we showed that TRA not only could bring-forth an additional amount of privacy level; by decreasing the adversary (1) traceability successfulness, (2) confusions per pseudonym change and (3) confusions per trace, but also enhanced the network performances; after it reduced the number of received beacons. All of that is while preserving the safety of drivers according to the context.

The obtained results of TRA shown in this chapter did motivate us to further-exploit this promising feature (the change of the transmission range) in new privacy-preserving schemes but this time the scheme would be mainly based on the transmission range technique while developing its own protocols and pseudonym change techniques. In the next chapter we see a new pseudonym change scheme that purely bases on the transmission range technique in order to provide high privacy level, that is: WHISPER.

Journal and Conference Papers Related to the Chapter

Jr) Transmission range changing effects on location privacy-preserving schemes in the internet of vehicles

Messaoud BABAGHAYOU, Nabila LABRAOUI, Ado Adamou ABBA ARI and Abdelhak Mourad GUEROUI. "Transmission range changing effects on location privacy-preserving schemes in the internet of vehicles". International Journal of Strategic Information Technology and Applications (IJSITA), 10.4, (2019), 33-54. (B-Rank)

Cn) Transmission range adjustment influence on location privacy-preserving schemes in vanets

Messaoud BABAGHAYOU and Nabila LABRAOUI. "Transmission range adjustment influence on location privacy-preserving schemes in vanets". International Conference on Networking and Advanced Systems (ICNAS), IEEE, 2019. Algeria.

Chapter V:
WHISPER: a Safety-Aware and Location
Privacy Scheme for IoV

*“Life is the finest secret. So long as that remains, we
must all whisper.”*

– Emily Dickinson

1 Preface

As a sequel to the previous chapter that proposed TRA as a helping feature for privacy preserving schemes, in this chapter, we present WHISPER: the novel location privacy preserving scheme that is built purely basing on the transmission range adjustment while making the pseudonym changing in order to preserve privacy. One of the strongest points of WHISPER is providing high levels of privacy while still maintaining road-safety; without sacrificing safety. Thus, this chapter defines the techniques and protocols that are used by WHISPER and evaluates the scheme against some of the well-known privacy-preserving schemes that are: CPN [86], RSP [69] and SLOW [77]. The evaluation takes place in a manhattan-grid model and uses various vehicle densities with different location privacy and QoS metrics. Later on, a comparative table is drawn to summarize characteristics of these schemes including WHISPER.

With an exact outline, the remainder of this chapter is organized as follows: In section 2, we give a background on the study in subject. Then, we give our supposed system model that is assumed in the study in section 3. Next, we present WHISPER with its techniques and protocols alongside with the obtained results from the different simulations and that is in section 4. In section 5, we discuss the performances of WHISPER with regard to the other schemes. Finally, we conclude the study and give a concluding summary in section 6.

2 Background

IoV is an important sub-domain of IoT as well as a clear example of System of Systems domain [123]. Figure 36 shows the V2X external inter-vehicles communications [124] and internal equipments. A vehicle using V2X can enhance road-safety by broadcasting BSM [125, 126] beacon message with a 300m range and a frequency of 1 to 10 BSMs per second from its OBU [40, 63, 127]. BSMs include sensitive data as stated earlier in this thesis which allows receiving vehicles to be aware of the potential dangers posed by nearby vehicles in addition to managing the road-congestion, that is considered as one of the high-level challenges [128], through the network of RSUs.

Since BSMs contain fine-grained location data, even though they are useful for the road safety, they do open privacy-related issue: any entity with eavesdropping capability can monitor the whereabouts of IoV users. mart cars' safety and

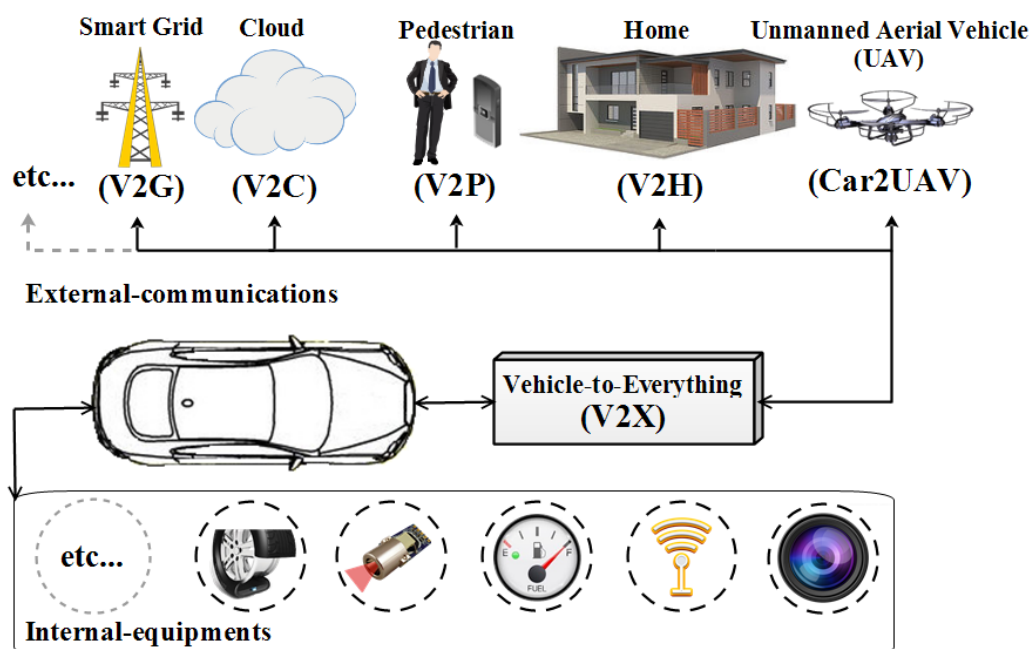


Figure 36: V2X technology illustration

infotainment applications may also reveal user private information. Using these data, a system that is ultimately designed to offer safety and comfort applications to drivers can be abused by third parties, such as employers, insurance companies or criminal organizations to track individuals[129]. The introduction of mechanisms that can preserve location privacy has become a new research trend that has attracted widespread attention among researchers. Most existing location privacy schemes, e.g., mix-zone, synchronized schemes, etc., are ineffective in achieving a high privacy level because of the very precise locations included in BSMs and because of their resource and overhead consuming characteristic. The better candidate mechanism used is that of the silent period schemes by ceasing BSMs broadcasting until emerging from another location with a new pseudo-identifier. However, the major drawback of such a technique is the sacrifice of safety for the sake of privacy [8].

As safety is way substantial requirement underpinning the introduction of V2X

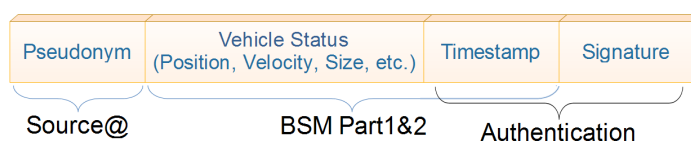


Figure 37: BSM beacon format

communication, silent period schemes have been received with reservations by the research community. Our motivation is to find a solution to allow the nearby vehicles to be aware (providing safety) and reduce an adversaries opportunity to employ eavesdropping attacks. The purpose of protecting user location privacy in the IoV context is related to the risk of user private information being disclosed. Location privacy is directly connected to other types of privacy. Location privacy leaks can reveal the home and work address of the driver, some visits to sensitive places, his travel habits, times of absence from home, etc. Correlation of this spatio-temporal information with other data allows an adversary to come to conclusions about health habits, social contacts, religion beliefs, etc. Protecting user location privacy has many benefits both to the users and the system. First of all privacy preservation improves the performance of IoV system and reduces users' concerns about security and privacy. Thus IoVs can attract more users to use their functions and applications, especially those that are related to safety, promoting further innovation and development in the automobile industry. In this chapter we propose a mechanism that is reducing the transmission range occasionally to just inform the nearby vehicles and prevent the adversary from tracking users through BSMs. The design of a pseudonym change scheme that exploits such a transmission range adjustment feature is inspired from our previous work [24] where we studied the effect of changing the transmission range using existing strategies. The novel method that is proposed in the current article, entitled "WHISPER", maintains road-safety since vehicles are only hidden from the tracker (occasionally) and not from their close vehicles (always) which makes the use of WHISPER an advantageous feature that comes in favor of safety and privacy.

3 System Model

In this section, we define and describe the Overall System Model comprised of network model, the threat/attacker model, a set of assumptions that are taken while making such a research study in addition to technical details and a mathematical model that reflects the fundamentals of using certificates under an IoV system.

3.1 Network Model

The network model used in this chapter is illustrated in Figure 38, and contains the following entities:

- Vehicles: They are the basic units of the VANET paradigm which provides a

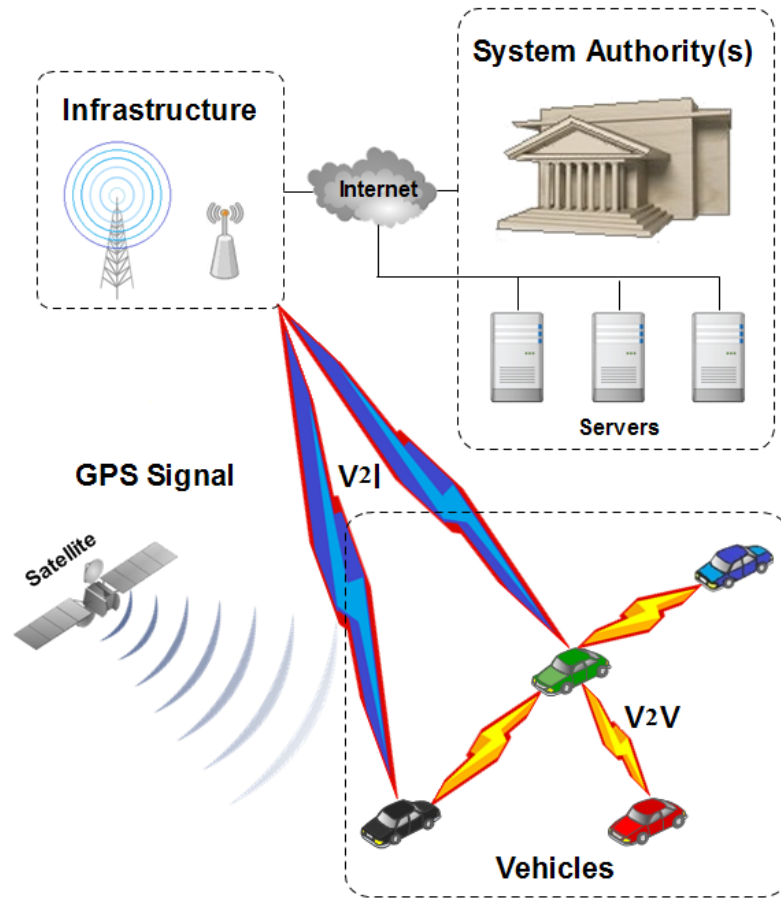


Figure 38: The different entities of the vehicular network

platform to the V2X applications. The communication is done via the 802.11p [27] standard and can perform V2V and V2I communications. The set of vehicles is defined as $V = \{v_1, v_2, \dots, v_n\}$.

- **System Authorities:** They are the the entities related to the law-side (e.g., governmental bodies) that have different resources, tasks and roles like: distributing, issuing, revoking pseudonyms, etc. [130]. It is also important that the system authorities almost always be able to fulfill the accountability requirement in order to track down and determine the misbehaving users [131].
- **Infrastructure:** Composed by different components and stations, its role is to relay and facilitate the connectivity between the vehicles and any potential attached network entity. The most interesting feature is the V2I communications. Additionally, V2X communications may exploit the Infrastructure.

3.2 Threat Model

The threat model is shown in Figure 39 and is composed from the following elements:

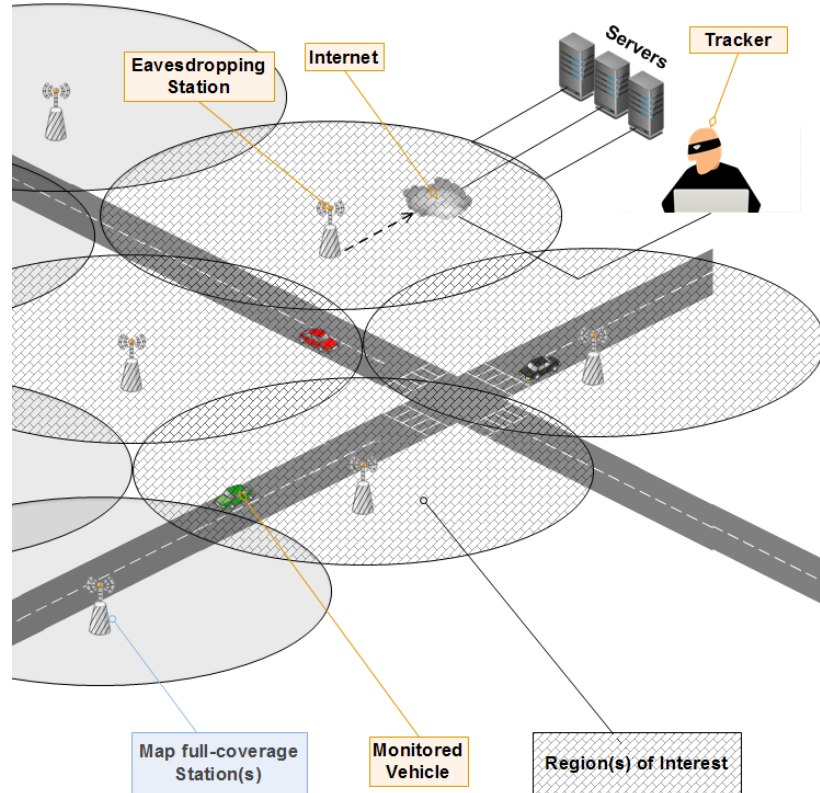


Figure 39: Threat model and its resources, capabilities and coverage

- **Tracker:** The malicious element in the system, even though it is not active, it still can execute many influencing attacks such as eavesdropping, tracking, profile-generation, etc. In most researches, the Global Passive Adversary (GPA) [63] is considered as the adversary type used while evaluating their own schemes. The GPA is a strong adversary that covers almost the whole map (or at least, the region of interest) and can obtain every sent message passively, i.e., no data forgery, modification or creation is executed by him.
- **Eavesdropping stations:** They are stations capable of collecting the transmitted BSMs where all of the coverage mode, the emplacement and the transmission range of vehicles do affect the amount of the collected packets.
- **Tracker resources:** They are the various materials and software used in

conjunction with the eavesdropping stations. They can be high performance servers, tracking algorithms and methods, etc.

3.3 Assumptions

We put a set of assumptions for what is included in this research:

- Vehicles are able to adjust their transmission range by changing the used transmission power.
- The adversary is setting eavesdropping stations in accordance to the standardization (300m of transmission range for vehicles).
- The distributed eavesdropping stations do overlap in 30m and have a moderate coverage mode to collect much BSMs by effectively exploiting his resources. This is illustrated in Figure 40.
- At a given time, the adversary can exclude the remaining of the map and only focuses on a region of interest. This is done at the aim of targeting only specific vehicles for better calculations and to well-exploit his resources (it is shown in Figure 40).
- Vehicles use the Public Key Infrastructure (PKI) certificates mechanism to communicate, thus, changing the used pseudonym implies using a new certificate. This later, is assumed to be issued from a trusted authority by doing the certificates refill request.

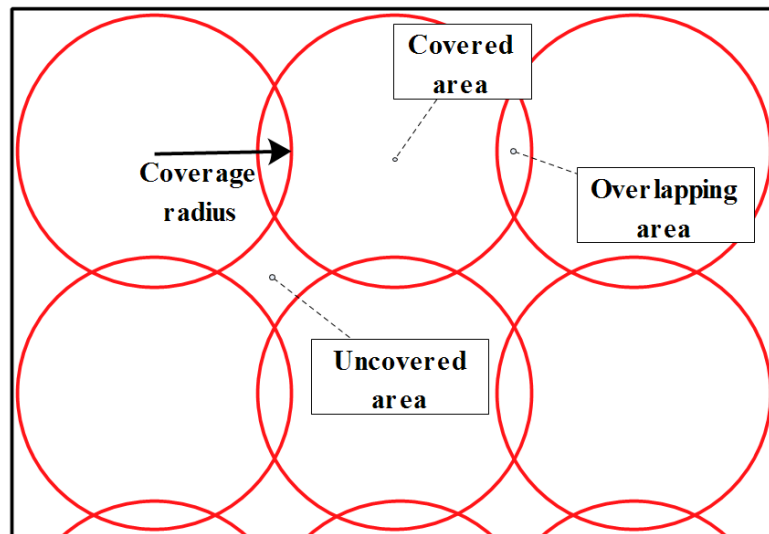


Figure 40: The used coverage mode (moderate mode) details

3.4 Certificates Management

Since the use of pseudonyms implies the use of certificates, a better management is envisioned in order not to affect the functioning of the whole system. With this said, having a large set of certificates with less consumption frequency would be preferred and hence minimizing their refill requests. In order to quantify the used certificates for each vehicle per unit of time, an estimation is highly needed. For that aim, we provide the following equations related to the used certificates:

- The estimated number of Certificates per day $NbrCerts_{day}$ without changing the certificate by a mean other that expiration is calculated as in Equation 12.

$$NbrCerts_{day} = NbrCerts_m * DrivTime_{day} \quad (12)$$

Where $NbrCerts_m$ is the number of used certificate per minute and $DrivTime_{day}$ is the estimated amount of time (in minutes) that the user is going to drive per day.

- The number of necessary certificates per year, assuming that a normal refill is made each year, is like in Equation 13.

$$NbrCerts_{year} = NbrCerts_{day} * 365 \quad (13)$$

- From here, the estimated remaining certificates after d days since the last yearly refill ($NbrRemainCerts(d)$) is calculated as written in Equation 14.

$$NbrRemainCerts(d) = NbrCerts_{year} - d * NbrCerts_{day} \quad (14)$$

- However, certificates may also get invalid due to a certificate change (triggered by a pseudonym change for example) and thus, the exact remaining certificates after d days since the last yearly refill ($RealNbrRemainCerts(d)$) can be calculated as in Equation 15.

$$RealNbrRemainCerts(d) = NbrCerts_{year} - d * NbrCerts_{day} - NbrCerts_{chngd} \quad (15)$$

Where $NbrCerts_{chngd}$ is the number of times the certificate got changed due to a reason other than a normal expiration.

4 The Proposed WHISPER Strategy

WHISPER uses the change of transmission power to preserve or at least augment the level of location privacy in addition to ensuring road-safety while driving. Vehicles monitor the neighborhood and their proper speeds on-the-fly in order to adjust their beacons transmission range. This is because the adversary, in our assumptions, distributes his eavesdropping stations intelligently and economically according to the standardization (that vehicles transmit with $300m$ of range). Thus, when driving in low speeds the vehicle (i.g., v_i) may reduce, according to the value of its speed (and the surrounding vehicles' speeds), its own range to ensure that:

- the safety of its neighbor vehicle(s) (e.g., v_j) is preserved unlike the case of the silent period schemes that do not make much safety-considerations when going to enter silent. This is fulfilled by continuously checking its own speed. Thus, when in high speeds, the risk of a sudden crash will be high that is why v_i ought to be earlier visible to the surrounding vehicles (v_j).
- its own safety. This is fulfilled by the neighbor vehicle(s) v_j that are using the same behavior as v_i while driving in different speeds. They aim, as a consequence, to inform v_i earlier when they are driving in high speeds. Once receiving a BSM with a powerful transmission range, v_i takes that as a parameter and adjusts, in its role, its own transmission range basing on that parameter and on its own speed. By doing so, v_i will be visible to the other neighbors v_j as well.
- the two aforementioned points lead to a collective awareness that will ensure the safety of both v_i and its neighbor v_j .
- to benefit and exploit the already deployed eavesdropping mode, as these eavesdropping stations will not be able to collect BSMs all the time even if the vehicles are inside the area of the eavesdropping station. This is because each eavesdropping station was placed at the aim of intercepting every sent BSM in the range of $300m$.

4.1 System Initialization

Each vehicle v_i is equipped with M certificates and each one of them is defined as ($Cert_{i,j}$) where j represents the i^{th} certificate of v_i . Thus, each vehicle v_i has a set of certificates C_i defined as follows: $C_i = \{Cert_{i,1}, Cert_{i,2}, \dots, Cert_{i,m}\}$. When referring to

a pseudonym change, this implies the use of another certificate.

Before we dive into the detailed modus-operandi of WHISPER, we define the set of concepts (find them in Table 10) that are key-parameters used to determine the exact behavior of WHISPER.

Table 10: WHISPER keywords, concepts and detailed definitions

The concept	Its definition
The different speed levels (km/h)	Low(≥ 0 & < 18), Medium(≥ 18 & < 36), beyond-Medium(≥ 36 & < 54), High(≥ 54)
My_Pos and $His_Pos(x, y, z)$	The position of v_i which does the calculation and v_j which sent the BSM
My_Speed and $His_Speed(km/h)$	The speed of v_i which does the calculation and v_j which sent the BSM
$Speed(km/h)$	The highest speed that was encountered while v_i was waiting
$Dist.(m)$	The distance between the sending vehicle v_j and the receiving vehicle v_i
$Calc_Dist(A, B)(m)$	Calculates the distance between point A and B .
$BSM.X()$ (depends)	$X()$ is the method applied on BSM to retrieve different fields like position, speed, etc.
$GeneralNR(m)$	A virtual range with the same value for each receiving vehicle v_i . This range determines whether a sending vehicle v_j is considered as a "General Neighbor" to v_i or not. If v_j is inside that range when sending its BSM, then it is considered to be v_i 's General Neighbor.
$RoadNR(m)$	A virtual range with the same value for each receiving vehicle v_i . This range determines whether a sending vehicle v_j is considered as a "Road Neighbor" to v_i or not. v_j is only considered as a Road Neighbor to v_i if it is inside the $RoadNR$ range and if it and v_i share the same road segment.
$CloseNR(m)$	A virtual range with the same value for each receiving vehicle v_i . This range determines whether a sending vehicle v_j is considered as a "Close Neighbor" to v_i or not. v_j is only considered as a Close Neighbor if it is inside the $CloseNR$ range. Noting that $CloseNR$ range ought to be very small in order to let both v_i and v_j be as much indistinguishable as possible to confuse the attacker when doing the pseudonym change action
$Close(boolean)$	A local variable that each vehicle v_i has. Being <i>True</i> means that v_i is currently at the proximity of another vehicle v_j . In the other case, when v_i is alone (with regard to the $CloseNR$ range), its value becomes <i>False</i> (to achieve road-safety, entertainment, congestion-aware actions, etc.)
$Process_Beacon(BSM)(procedure)$	This procedure uses the received BSM packet for the IoV objectives and requirements (to achieve road-safety, entertainment, congestion-aware actions, etc.)
$OBU_Is_On(boolean)$	A true or false value which means a sending vehicle v_i is on or off respectively
$Beacon_Interval_Time(s)$	An amount of time in where v_i is waiting before sending the next BSM
$Prepare_Beacon(BSM)(Beacon)$	Generates a BSM packet that will be ready for broadcasting
$nic.mac80211.txPower(milliwatt)$	The transmission power given to the network interface used to control the transmission range of v_i
$Counter(number)$	A counter variable used later on to decide the pseudonym change action
$Def_Val(number)$	The default value of <i>counter</i> . It is used to both reinitialize <i>counter</i> and to do a test to find out the eligibility of v_i for changing its pseudonym
$Send_Beacon(BSM)(Beacon)$	Gives the BSM packet to the lower layers which will broadcast it to the neighbors
$Checking_Pseudonym_Change_Trigger()$ (procedure)	Checking whether the trigger of v_i for changing its pseudonym is met or not
$Pseudonym_Change()$ (procedure)	Once the conditions are met and once it is executed correctly, v_i acquires a new pseudonym (and certificate respectively)

Generally speaking, in WHISPER, every vehicle v_i can be in one of the following main states:

- *Vehicle ON*: is the state when a vehicle is turned on (to be ready for driving).
- *Listening*: once On, v_i keeps monitoring the transmission medium to detect any

transmitted BSM. both its neighbor(s) status (found in their transmitted BSMs) and its own speed.

- *Receiving BSMs*: When receiving a BSM from v_j , v_i proceeds into diverse calculations at the aim of knowing the status of v_j .
- *Adjusting the transmission power*: in this status, v_i takes as parameters its own speed and the neighbors' speed and may, accordingly, adjust its transmission range in order to ensure road-safety and preserve location-privacy of the present vehicles.
- *Checking pseudonym change condition*: this status comes after the *Beacon_Interval_Time* expires. v_i will check its eligibility for a pseudonym (and certificate) change. When favorable, v_i moves into the next status.
- *Pseudonym change* in this status, a pseudonym change takes place and the BSM will be sent right after.
- *Sending a BSM* this status happen after the *Pseudonym change* action. Sometimes, the pseudonym change trigger will not be satisfied, thus, v_i just sends the BSM. In both scenarios, v_i returns to the next status(*Listening*) afterwards.
- *Vehicle OFF* the status where a vehicle is turned off and thus the ending status.

A state diagram is presented in Figure 41 which gives a better illustration and understanding on the aforementioned states and the existing transitions.

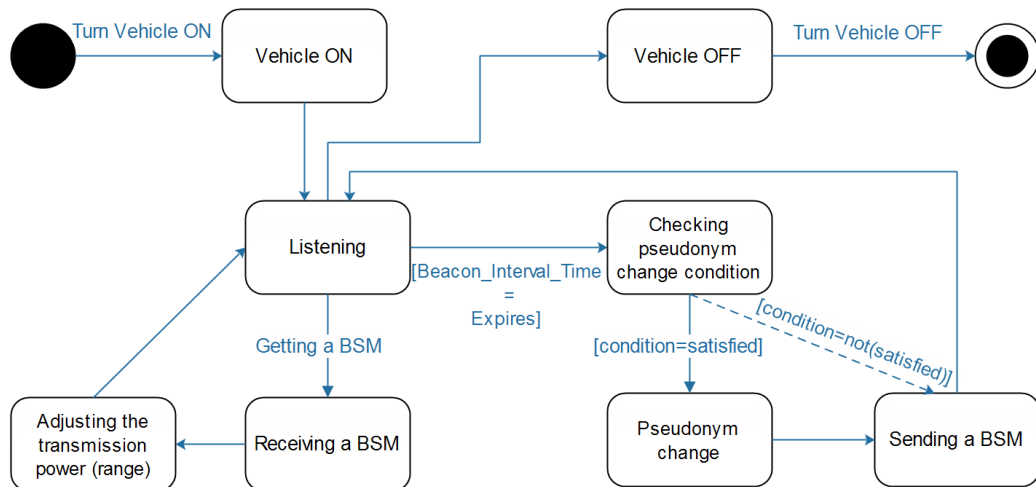


Figure 41: The state diagram of WHISPER

4.2 Receiving Beacon Messages Protocol

Vehicles are always ready to receive BSMs. When receiving a BSM, the receiving vehicle v_i considers the sender's position and calculates the distance between itself and the sender. By doing this simple calculation, v_i will be able to get a set of useful information that will determine its behavior. The pseudo-code of receiving a beacon message in WHISPER is illustrated in Algorithm. 2. The main conclusions that v_i is going to have after parsing the BSM sent by v_j , are the followings:

- Knowing the distance between itself and v_j .
- Whether to consider v_j 's BSM for transmission power adjustment or just ignore it.
- It considers v_j 's BSM for transmission power adjustment if $Dist$ is less than or equal to $GeneralNR$ (shown in the scenario that is illustrated in Figure 42).
- It considers v_j 's BSM for transmission power adjustment if $Dist$ is less than or equal to $RoadNR$ but also share the same road segment with each other (shown in the scenario that is illustrated in Figure 43).
- It considers itself eligible for the pseudonym change if $Dist$ is less than or equal to $CloseNR$. It does change $Close$ to $True$ as a consequence.

This protocol is called whenever v_i receives a BSM generated by v_j and with each

Algorithm 2 Receiving Beacon

```

1: procedure RECEIVING_BEACON(BEACON* BSM)
2:    $His\_Pos \leftarrow BSM.SenderPos()$ ;
3:    $Dist \leftarrow Calc\_Dist(My\_Pos, His\_pos)$ ;
4:   if  $((Dist \leq GeneralNR)$  OR  $((Dist \leq RoadNR)$  AND  $(MyRoadID =$ 
       $HisRoadID))$  then
5:      $His\_Speed \leftarrow BSM.SenderSpeed()$ ;
6:      $Speed \leftarrow Max(My\_Speed, His\_Speed)$ ;
7:     if  $(Dist \leq CloseNR)$  then
8:        $Close \leftarrow TRUE$ ;
9:     end if
10:  end if
11:   $Process\_Beacon(BSM)$ ;
12: end procedure

```

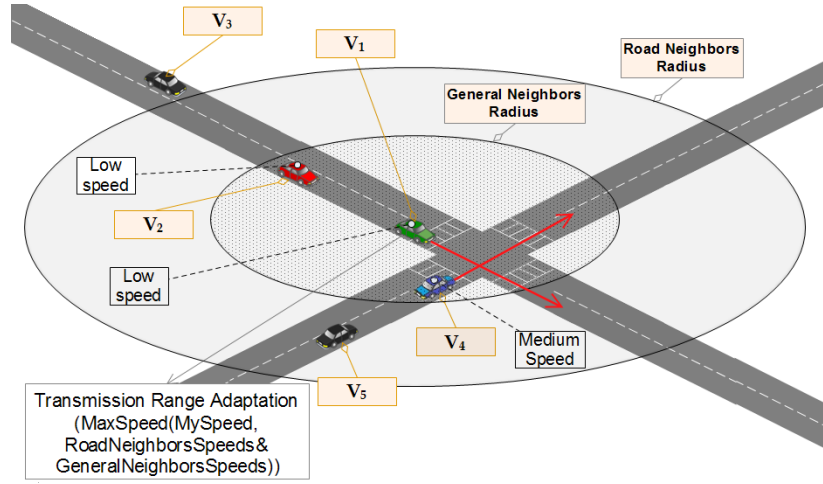


Figure 42: WHISPER behavior in the presence and influence of general neighbors on the transmission range adjustment

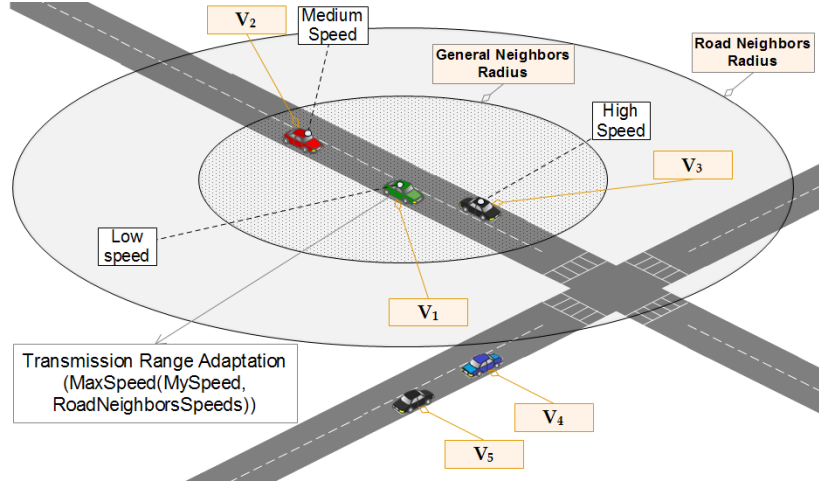


Figure 43: WHISPER behavior in the presence and influence of road neighbors on the transmission range adjustment

call, less than 10 instructions are executed; thus a linear complexity per each call $\mathcal{O}(10)$. With this said, by receiving (R) BSM, the complexity of the whole protocol will be as in Equation 16:

$$\mathcal{O}(R \times 10) = \mathcal{O}(n) \quad (16)$$

This indicates that the *ReceivingBeaconMessages* Protocol is neither time nor resources consumer.

4.3 Transmission Range Adjustment Protocol

Each vehicle v_i , and after the *Beacon_Interval_Time* expires, will send a BSM to inform the nearby vehicles about its location. Particularly, WHISPER adjusts the

transmission range prior to the final BSM broadcast. The adjustment is done each time a BSM is received by v_i as explained before. When going to broadcast, v_i uses the value of *Speed* to decide the appropriate transmission range (between all of the four levels: Low, Medium, beyond-Medium and High). Algorithm. 3 shows the pseudo-code of sending a BSM after making the transmission range adjustment step. Additionally, *Speed* is reinitialized to 0 after that and *Checking_Pseudonym_Change_Trigger()* is called during this protocol and that is to see the eligibility of changing v_i 's pseudonym (and certificate respectively). Moreover, *Counter* is decreased depending on the value of *Speed* and this is to trigger the pseudonym change (will be seen in the next point). However, if *Speed* is at max level, there will be no meaning for changing the pseudonym and that is because the attacker is able to collect every sent beacon (the maximum transmission range is used) and that is why *Counter* is reinitialized to its default value *Def_Val*.

This protocol is called whenever v_i *Beacon_Interval_Time* expires and thuse, one time per call. However, it calls, in its role, the *Checking_Pseudonym_Change_Trigger()* protocol. In total, there are (7) instructions without counting the called protocol ($\mathcal{O}(7)$). With this said, the complexity o the *TransmissionRangeAdjustment* Protocol is defined as in Equation 17:

Algorithm 3 Sending Beacon

```

1: procedure SENDING_BEACON
2:   while (OBU_Is_On) do
3:     Wait(Beacon_Interval_Time);
4:     Prepare_Beacon(BSM);
5:     Speed  $\leftarrow$  Max(My_Speed, Speed);
6:     if (Speed < 18) then
7:       nic.mac80211p.txPower  $\leftarrow$  0.2;
8:       Counter  $\leftarrow$  Counter - 5;
9:     else if (Speed < 36) then
10:      nic.mac80211p.txPower  $\leftarrow$  0.8;
11:      Counter  $\leftarrow$  Counter - 10;
12:     else if (Speed < 54) then
13:      nic.mac80211p.txPower  $\leftarrow$  3.1;
14:     else
15:      nic.mac80211p.txPower  $\leftarrow$  7;
16:      Counter  $\leftarrow$  Def_Val;
17:     end if
18:     Speed  $\leftarrow$  0;
19:     Checking_Pseudonym_Change_Trigger();
20:     Send_Beacon(BSM);
21:   end while
22: end procedure

```

$$\mathcal{O}(1 \times (7 + \mathcal{O}(\text{Checking_Pseudonym_Change_Trigger()}))) = \mathcal{O}(\text{Checking_Pseudonym_Change_Trigger()}) \quad (17)$$

This indicates that the *TransmissionRangeAdjustment* protocol does depend on the *PseudonymChangeTrigger* Protocol.

4.4 Pseudonym Change Trigger Protocol

In order to avoid wasting pseudonyms (certificates) in an inappropriate opportunity, finding an almost good opportunity requires that the pseudonym change trigger must be implemented delicately. Algorithm. 4 shows, in a pseudo-code, the way vehicles perform a check to see the eligibility for changing their pseudonyms. When the trigger *Counter* reaches or drops below (0) (which is an indicator that v_i was sending BSMs with a short range for some important period of time) v_i changes its pseudonym then initializes the trigger *Counter*. This whole process provides high confusion chances since

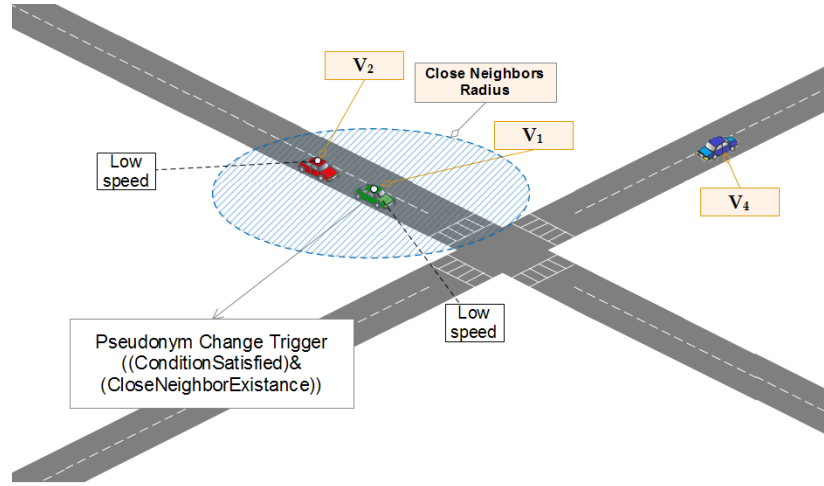


Figure 44: WHISPER, pseudonym change process triggered by a close neighbor's status

the pseudonym change is performed not in the favor of the tracker (see the scenario illustrated in Figure 44). The *PseudonymChangeTrigger* protocol is used each time the *TransmissionRangeAdjustment* is executed. Its complexity depends on a small and fixed number of instructions (5), thus, can be defined as in Equation 18:

$$\mathcal{O}(5) = \mathcal{O}(1) \quad (18)$$

The *PseudonymChangeTrigger* protocol has $\mathcal{O}(1)$ as a complexity.

Algorithm 4 Checking Pseudonym Change Trigger

```

1: procedure CHECKING_PSEUDONYM_CHANGE_TRIGGER
2:   if ((Counter <= (Def_Val/2)) AND (Close)) then
3:     Counter ← Def_Val;
4:     Pseudonym_Change();
5:   else if (Counter <= 0) then
6:     Counter ← Def_Val;
7:     Pseudonym_Change();
8:   end if
9:   Close ← FALSE;
10: end procedure
    
```

The mobility and environment information used for the simulation are presented in Table 11. The manhattan grid model consists of 9 intersected roads with attached segments where each segment has a length of 200m.

Table 11: Simulation parameters and values

	Parameters	Value
Mobility	Vehicles Number	Simultaneously=50,100,150,200 Total=100,200,300,400
	Insertion method	Quasi-Instant (first second insertion)
	Mobility Model	RandomTrips with minimum distance=1500(m)
Environment	Used Map	Manhattan grid model 9 roads, 200(m) per segment
	Map size	2000*2000($m * m$) 4(km^2)
	Simulation Time	300(s)
Evaluation	Privacy metrics	Traceability N_Traceability
	Pseudonym usage/ consumption	Number of changed-pseudonyms
	SLOW	Speed threshold=8(m/s) Silence threshold=5(s)
Strategy	RSP	Pseudonym duration=60(s) Silence period= from 3 to 9(s) randomly
	CPN	Neighbors radius=100(m) Neighbors threshold=2
	WHISPER	Road neighbors radius=100(m) General neighbors radius=30(m) Close neighbors radius=30(m) Counter default value=50

4.5 The Adversary's Achieved Traceability

Traceability, that is the location privacy metric used in this study, is defined as the correctness of an adversary to build the target vehicle's traces using its eavesdropped beacons [115]. The results, provided in Figure 45 show that WHISPER is outperforming SLOW, RSP and CPN in the traceability metric with a clear difference (that is ranging in the interval of 10% to 20%). An important remark is that at dense situations (e.g., with the density of 200 vehicle), the traceability gets augmented a bit. The reason behind the decrease in the privacy level is due to the higher density of

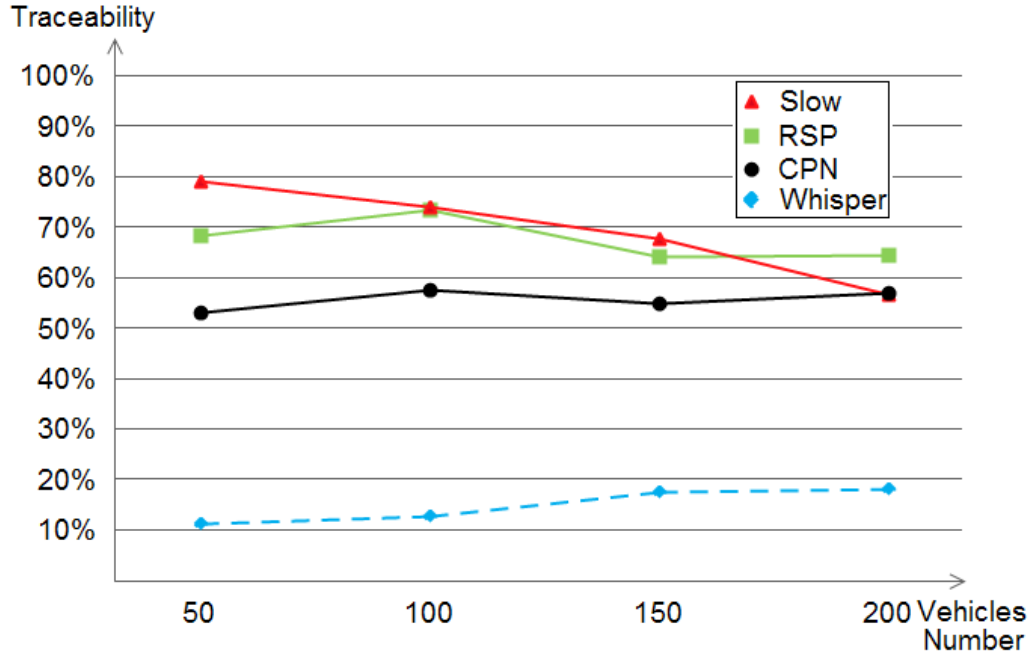


Figure 45: The achieved traceability by SLOW, RSP, CPN and WHISPER within different densities

vehicles, that can help the attacked collect BSMs from the legitimate cars.

In general, as presented in Figure 45, WHISPER performs better in terms the level of privacy that it offered since it achieves a traceability ranging in the interval of 10% to 20%. We interpret this as being WHISPER reducing the vehicle’s transmission range according to its and/or the neighbor vehicles’ speeds (according to the safety situation) followed by CPN, RSP then SLOW, in addition we observe that the traceability decreases when augmenting the number of vehicles in SLOW. The reason is that, in high densities, vehicles would drive with lower speeds, thus, SLOW performs better.

4.6 The Adversary’s Achieved Normalized Traceability

As some vehicles may not perform the pseudonym change, building their traces becomes easy, thus, excluding them gives more fairness to the real level of privacy [115]; that is the normalized traceability. With this definition, our conducted simulation under the normalized traceability is aiming to give a more credible and a better privacy-reflecting metric to quantify the achieved privacy level of WHISPER, SLOW, RSP and CPN (shown in Figure 46).

As stated above, by taking the case of just the vehicles which did change their pseudonyms, we get the achieved normalized traceability as shown in Figure 46. The

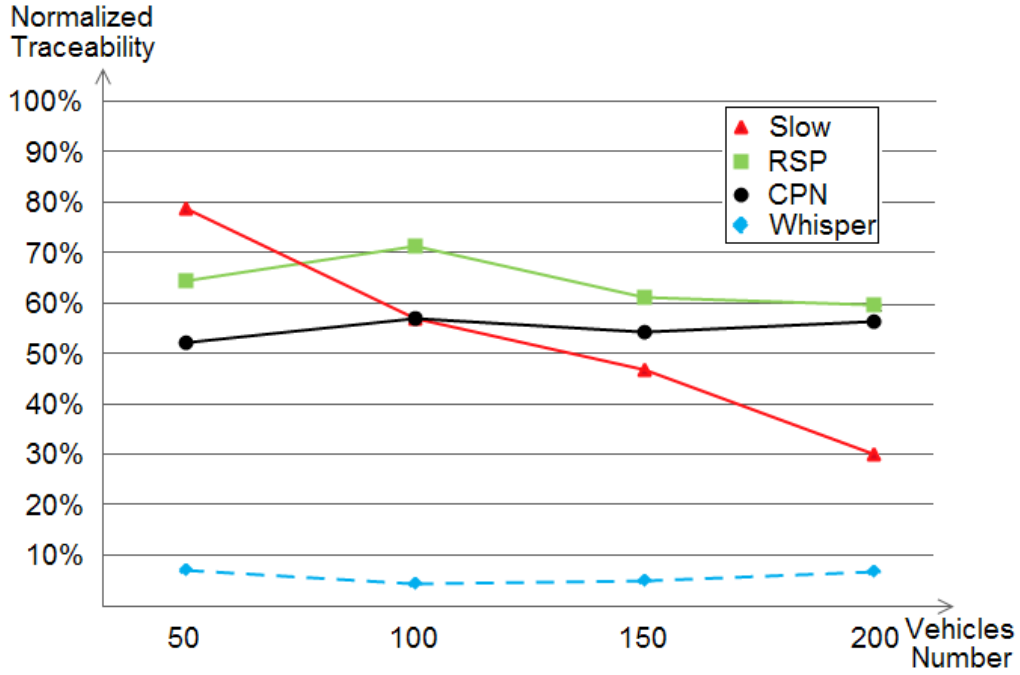


Figure 46: The achieved normalized traceability by SLOW, RSP, CPN and WHISPER within different densities

results always give WHISPER the leading position since it outperforms the other schemes but this time by achieving even higher privacy level represented in a lower than 10% of normalized traceability. The same order of performance remains; CPN, RSP then SLOW. However, SLOW has achieved a better normalized traceability of about 30% due to removing vehicles which did not change their pseudonyms at all from the calculation.

4.7 Pseudonym Consumption

Also considered as the QoS metric (as evaluated in Figure 47). The pseudonym consumption has multiple effects and impacts like the use of different pseudonyms (thus, certificates), extra-communications with the corresponding authorities to refill pseudonyms, affecting the routing algorithms [102], etc. For this reason, the pseudonym consumption metric is crucial. With a clear view, Figure 47 shows that SLOW is the less pseudonyms consuming scheme followed by RSP and WHISPER respectively, while CPN had a considerable high pseudonyms consumption level. We argue this by the scheme's nature, when the trigger of k neighbors is satisfied, a pseudonym change is performed and as k was taken as 2 by the default parameters, a lot of pseudonym changes occurred.

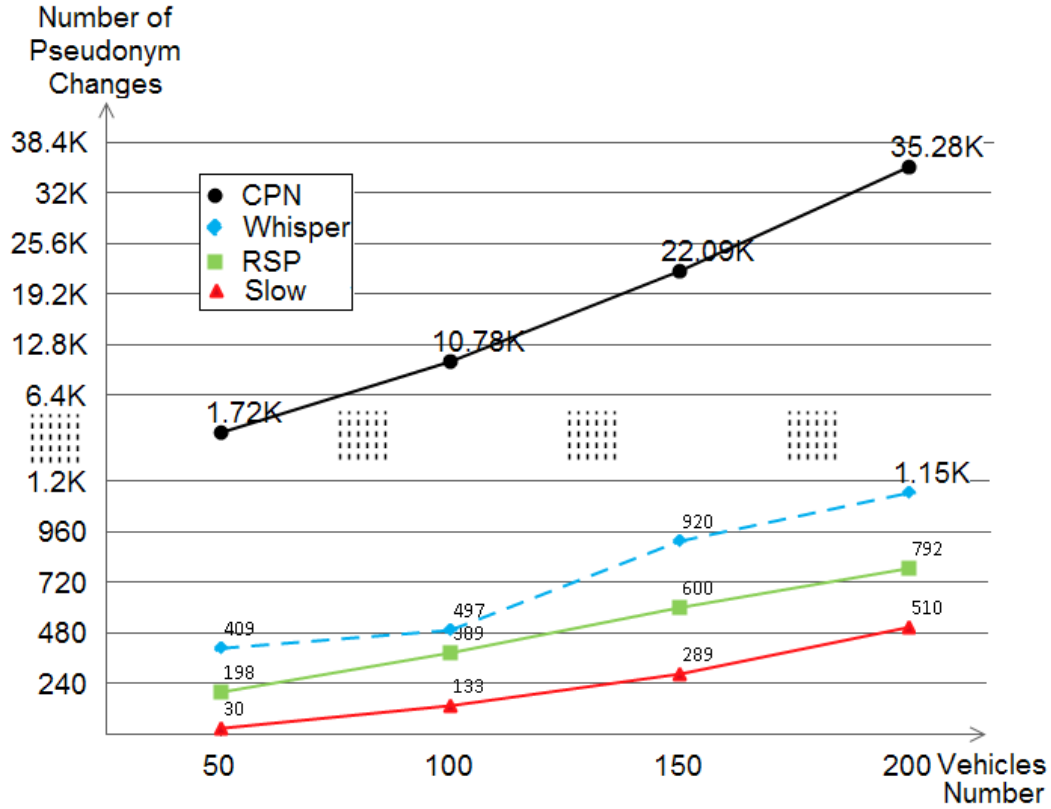


Figure 47: The pseudonyms consumption of CPN, WHISPER, RSP and SLOW within various densities

5 Discussion and Future Work

For an overall investigation, the performances of CPN, RSP, SLOW and WHISPER were evaluated in terms of (1) location privacy that gives WHISPER the leading in both (a) the traceability and (b) the normalized traceability and (2) QoS that comes in the favor of SLOW. CPN, under the default parameters (i.e., $k = 2$), has resulted in a very high pseudonyms consumption, thus, considered as a non-wise choice for a deployed pseudonym scheme. The results, clearly show that WHISPER has a very good level of privacy since it achieves a traceability ranging in the interval of 10% to 20%. In terms of normalized traceability WHISPER outperformed the other schemes achieving even higher privacy level.

Despite being WHISPER more pseudonym consuming (with a remarkably low amount in general) than SLOW and RSP, having it a very high location privacy level represented in the traceability and the normalized traceability gives it the leading position. Thus, we can say that WHISPER, as also compared and summarized in Table 12, has outperformed the other schemes especially in both of the safety and the

Table 12: A brief comparison of SLOW, RSP, CPN and WHISPER strategies according to a set of metrics

	Staying Silent	Monitoring Neighbors	Pseudonyms Consumption	Safety Ensuring	More Efficiency when
SLOW [77]	✓	✗	Low	✗	Driving in low speeds, hence, keeping silence
RSP [69]	✓	✗	Low	✗	Entering silence and changing pseudonyms synchronously
CPN [86]	✗	✓	Very high	✓	The set of vehicles happens to be large
WHISPER [101]	✗	✓	Medium	✓	Low transmission power condition is satisfied

location privacy that are known to be on the top of the security requirements.

Except from the evaluation comparison, WHISPER is an important solution that offers privacy preservation while maintaining at the same time road-safety. This is achieved, since vehicles are only hidden from the tracker (occasionally) and not from their close vehicles (always) which makes the use of WHISPER an advantageous method that comes in favor of safety and privacy.

As the technique of changing the transmission range was not exploited in the privacy field, we intend on making an evaluation for achieved location privacy level versus an internal attacker; the scenario when neighbor vehicles act as malicious eavesdropping stations to bypass the reduction of the transmission range and to increase the coverage of the tracker. Also, some of the values like those existing in Algorithm. 3 are set heuristically, this means that evaluating the performance by optimally adjusting the values dynamically will certainly enhance the privacy level of WHISPER. Also, technologies like blockchain [132, 133], cryptography [134], IDSs[135] and Edge Computing[136, 137] which are broadly recognized as key components for the IoV can be integrated and used in parallel with our solution. Finally, using metrics like the number of sent BSMs or the number of verified messages/signatures and evaluating the performances of WHISPER under various scenarios like the free-way model are some of our future plans.

6 Summary

In this chapter, WHISPER, we presented WHISPER: a novel location privacy-preserving schemes that exploits the reducing of the transmission range while sending safety beacon messaged. Further more, we gave WHISPER protocols techniques and algorithms where we compared it vs. other schemes, namely CPN, RSP and SLOW using various metrics like (a) the location privacy level (traceability and normalized traceability) and (b) the QoS (pseudonyms consumption) metrics. It was clearly shown that WHISPER did outperform the other three schemes in the location privacy evaluation, which is considered to be an important security requirement, but consumed -lightly- more pseudonyms compared to SLOW and RSP as shown in the QoS evaluation. The chapter also confirmed the robustness of WHISPER during the evaluation and that was apparent in (1) the road-safety that was missed by all other silent period schemes and (2) the location-privacy of the all evaluated schemes. The reason behind being WHISPER a road-safety ensurer is that the vehicles are only hidden from the tracker (occasionally) but not from their close neighbor vehicles (always). This made the use of WHISPER be an advantageous feature that came in the favor of both safety and privacy.

Journal and Conference Papers Related to the Chapter

Jr) WHISPER: A Location Privacy-Preserving Scheme Using Transmission Range Changing for Internet of Vehicles

Messaoud BABAGHAYOU, Nabila LABRAOUI, Ado Adamou ABBA ARI, Mohamed Amine FERRAG, Leandros MAGLARAS and Helge JANICKE. "WHISPER: A Location Privacy-Preserving Scheme Using Transmission Range Changing for Internet of Vehicles". Sensors, 21.7, (2021), 2443. (A-Rank, IF=3.275)

Cn) Preserving the Location Privacy of Drivers Using Transmission Range Changing Techniques in Internet of Vehicles

Messaoud BABAGHAYOU, Nabila LABRAOUI, Ado Adamou ABBA ARI, Mohamed Amine FERRAG and Leandros MAGLARAS. "Preserving the Location Privacy of Drivers Using Transmission Range Changing Techniques in Internet of Vehicles". The 4th International Symposium on Informatics and its Applications (ISIA), 2020. Algeria.

Conclusion

An exceed on the moving towards integrating technology means in different life-sides is taking place in the last few decades. Without any doubt, the use of technology had enhanced enormously the lifestyle of individuals by facilitating much difficulties and solving a bunch of intractable problems. Using the wireless medium and allowing vehicles to exploit it to solve the already present challenges brought forth robust transportation systems after giving the vehicle the option to sense its environment and sharing this vision with its neighbor vehicles mainly at the aim of achieving dependable road-safety.

Yet, some of the used technologies had introduced other drawbacks, we talk about the trade-offs. Our subject of interest (i.e., road-safety via data exchanges) is in no way safe from the equation. The use of safety applications that bases on exchanging data between the neighbor vehicles had introduced the safety-privacy trade-off, that is: by informing the nearby vehicles, a better vision and perception for the environment is fulfilled but in the other hand the identity and location privacy of vehicle users will get dropped considerably since their data is being read by unauthorized parties (represented in the attacker/tracker).

With this in mind, in this thesis we were interested on achieving high levels of identity and location privacy while maintaining the road-safety with a high degree. We followed a specific chronology while making our research and contributions that is as follows:

At first, we introduced the notion of intelligent vehicles that use advanced technologies like IoV with its characteristics, security challenges, privacy issues and implications on road-safety.

Later on, we focused on the literature review where we gave an extended state of the art of the identity and location privacy with more interest on the pseudonym change-based schemes that emerged in the last two decades. It was also resulted in a novel taxonomy on pseudonym change schemes alongside a comparative table of some of the schemes. This had concluded the first part that we called LITERATURE REVIEW.

With the first stage set (the LITERATURE REVIEW part), we started giving solutions and evaluating the issue from our side and we did that by introducing the EPP scheme where we evaluated it in a district in Tlemcen, Algeria. EPP studied the effects of using the silent period before leaving a district and how much this behavior can enhance the overall privacy of the users living in that district. The conclusion drawn by EPP was that the more residents that respect EPP the higher their privacy will be. Also, the vision of the identity and location privacy was studied but from two perspectives: from the defender (the authority) and the attacker (the adversary) and that gave better-understanding on the problematic as whole.

After that, We proposed the use the transmission range changing technique to provide higher identity and location privacy in a technique that we called TRA. TRA was used in conjunction with two privacy schemes that were already existing in the literature. The obtained results showed clearly that after integrating TRA on those privacy schemes, we got considerable high levels of privacy and that conclusion had pushed us to proceed into proposing our own scheme that exploits this special technique (TRA).

As a sequel from the previous work (TRA), we presented a novel identity and location privacy preserving scheme (we called it WHISPER) that adjusts the transmission range of vehicles, on-the-fly- to break the continuous location tracking applied by the adversary. WHISPER had its own protocols and techniques that were developed in order to maintain road-safety in conjunction with high levels of privacy. Indeed, the simulation runs and results had confirmed that by using the transmission range technique in a novel scheme, higher levels of privacy were achieved while always keeping road-safety ensured.

As a consequence, this thesis touched the problematic of preserving the identity and location privacy of individuals while ensuring a high amount of road-safety and it was crowned with:

(1) A survey paper for the used pseudonym change techniques in the recent years, (2) A novel scheme that is EPP which was interested on the achieved privacy inside a district (Tlemcen, Algeria in the study), (3) A novel technique that is TRA which was applied in two privacy-preserving schemes and (4) A novel scheme that is WHISPER which was inspired from TRA but with its own protocols with more focus on road-safety.

In the future, we intend on exploiting aspects other than those mentioned in the current thesis. As an example, we are interested in exploiting the social network concept in order to bring forth the identity and location privacy on the individuals. In fact, we already started on this step and we got, after developing our protocols and after we set the simulation environment, promising results. The work is in its finalization before submitting it for potential acceptance. Additionally, we are excited on using other technologies (like blockchains, UAV, 5G/6G, etc.) in conjunction with the automobile domain to enhance more the individuals' enjoyed level of privacy.

Appendices

1) WHISPER: A Location Privacy-Preserving Scheme Using Transmission Range Changing for Internet of Vehicles



Article

WHISPER: A Location Privacy-Preserving Scheme Using Transmission Range Changing for Internet of Vehicles

Messaoud Babaghayou ^{1,*}, Nabila Labraoui ¹, Ado Adamou Abba Ari ^{2,3}, Mohamed Amine Ferrag ⁴, Leandros Maglaras ^{5,*} and Helge Janicke ⁶

¹ STIC Lab, University of Abou Bekr Belkaid, Chetouane Tlemcen 13000, Algeria; nabila.labraoui@mail.univ-tlemcen.dz

² DAVID Lab, Université Paris-Saclay, University of Versailles Saint-Quentin-en-Yvelines, 45 Avenue des États-Unis, 78035 Versailles CEDEX, France; adoadamou.abbaari@gmail.com

³ LaRI Lab, University of Maroua, Maroua P.O. Box 814, Cameroon

⁴ Department of Computer Science, Guelma University, Guelma 24000, Algeria;

ferrag.mohamedamine@univ-guelma.dz

⁵ School of Computer Science and Informatics, De Montfort University, Leicester LE1 9BH, UK

⁶ Cyber Security Cooperative Research Centre (CSCRC), Perth, WA 6027, Australia;

helge.janicke@cybersecuritycrc.org.au

* Correspondence: messaoud.babaghayou@univ-tlemcen.dz (M.B.); leandros.maglaras@dmu.ac.uk (L.M.)

Abstract: Internet of Vehicles (IoV) has the potential to enhance road-safety with environment sensing features provided by embedded devices and sensors. This benign feature also raises privacy issues as vehicles announce their fine-grained whereabouts mainly for safety requirements, adversaries can leverage this to track and identify users. Various privacy-preserving schemes have been designed and evaluated, for example, mix-zone, encryption, group forming, and silent-period-based techniques. However, they all suffer inherent limitations. In this paper, we review these limitations and propose WHISPER, a safety-aware location privacy-preserving scheme that adjusts the transmission range of vehicles in order to prevent continuous location monitoring. We detail the set of protocols used by WHISPER, then we compare it against other privacy-preserving schemes. The results show that WHISPER outperformed the other schemes by providing better location privacy levels while still fulfilling road-safety requirements.

Keywords: location privacy; pseudonym change strategy; transmission range adjustment; iov privacy; iov safety; vanet



Citation: Babaghayou, M.; Labraoui, N.; Abba Ari, A.A.; Ferrag, M.A.; Maglaras, L.; Janicke, H. WHISPER: A Location Privacy-Preserving Scheme Using Transmission Range Changing for Internet of Vehicle. *Sensors* **2021**, *21*, 2443.

<https://doi.org/10.3390/s21072443>

Academic Editor: Antonio Guerrieri

Received: 9 March 2021

Accepted: 27 March 2021

Published: 1 April 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

A Vehicular Ad-hoc Network (VANET) with its variety of protocols (e.g., IEEE 802.11P, IEEE 1609) [1] and communication types like Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) [2] has served as a basis for the promising Internet of Vehicles (IoV) paradigm [3–5]. IoV benefits from VANET to extend the usability range by allowing non-conventional communications and applications, e.g., Vehicle to Everything (V2X) communications, to emerge. IoV is an important sub-domain of IoT as well as a clear example of System of Systems domain [6]. Figure 1 shows V2X external communications and internal equipments. A vehicle using V2X can enhance road-safety by broadcasting a Basic Safety Message (BSM) [7,8] beacon message with a 300-m range and a frequency of 1 to 10 BSMs per second from its OBU [9–11]. The data included in BSMs are illustrated in Figure 2. This allows receiving vehicles to be aware of the potential dangers posed by nearby vehicles in addition to managing road-congestion, which is considered a high-level challenge [5] through the network of Road-Side-Units (RSUs).

2) Pseudonym change-based privacy-preserving schemes in vehicular ad-hoc networks: A survey

Journal of Information Security and Applications 55 (2020) 102618



Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa

Pseudonym change-based privacy-preserving schemes in vehicular ad-hoc networks: A survey

Messaoud Babaghayou ^{a,*}, Nabila Labraoui ^a, Ado Adamou Abba Ari ^{b,c}, Nasreddine Lagraa ^d, Mohamed Amine Ferrag ^e

^a STIC Lab, Abou Belkaid University, P.O.Box 230, chrouane, Tlemcen 13000, Algeria

^b LI-PARAD Lab, Saint-Quentin-en-Yvelines University, 45 Avenue États-Unis 78035 Versailles cedex, France

^c LaRI Lab, Mersoua University, P.O. Box 814 Mersoua, Cameroon

^d LMI Lab, Amar Telidji University, P.O. Box 637, Route de Ghardaia (M'kass), Laghouat 03000, Algeria

^e Department of Computer Science, Guelma University, R.P. 401, 24000, Algeria

ARTICLE INFO

Keywords

VANET privacy
Location tracking
Anonymity
Identification problem
Pseudonym change techniques

ABSTRACT

Vehicular Ad-hoc Networks (VANETs), which are a subclass of Mobile Ad-hoc Networks (MANETs), received a widespread attention during the last decades. With these promising set of safety applications, which are the main reason why they were developed, VANETs are considered as a tremendous support for the Intelligent Transportation Systems (ITS). However, several key issues remain to be solved before VANET becomes fully applicable; one of them being privacy preservation. To fulfill safety-requirements in VANETs, the vehicle needs to broadcast its status wirelessly. Consequently, any adversary can hear the broadcast messages at the aim of analyzing them, identifying, tracking and generating profile of his target. In other words, privacy of individuals may be seriously breached in VANETs if no safety measures were been taken. Using pseudonyms instead of the real identities of individuals, and changing them periodically during the communication is a promising solution for such crucial problems. There is a significant body of research work addressing this issue and a lot of researchers proposed various privacy protections basing on pseudonym change strategies. In this survey paper, we present an introduction to the privacy problem and give a recent and detailed state of the art of the different suggested pseudonym change strategies and approaches. We also propose a novel taxonomy to classify these strategies to diverse concepts. Finally, we discuss, give future directions and open issues and mention some of the observations that lead to better identify this problem for better future strategies.

1. Introduction

1.1. Background

Over the past few decades, the world witnessed a huge evolution in different fields (e.g., the wireless communication technologies and automobile industry), which let all of the: government, industry and the research community think about benefiting from this evolution to overcome the current challenges that the world is facing. The augmentation of the vehicles number and its implications (road safety, traffic efficiency, congestion problems, etc.) are a good example for such challenges. In addition to these problems (namely safety-related problems), there are also comfort-related problems, aimed at providing

entertainment for both the driver and his passengers (connection to the internet, sharing files, instant conversation between drivers and passengers, etc.).

Vehicular Ad-hoc Networks (VANETs), that are essential for cooperative driving among vehicles on a given road, provide the communication among vehicles on the road and the Road Side Units (RSU) in an ad-hoc manner by using wireless technologies such as IEEE 802.11p. Taking their unique features (that include self-organization and self-management) in mind, these networks become key components for Intelligent Transportation Systems (ITS) [1,2]. Thus, the deployment of VANETs took part in this area. The main objective of VANETs is to give vehicles the ability to communicate either by Vehicle to Vehicle (V2V), Vehicle to Infrastructure (V2I) or even by Vehicle to everything (V2X) in

* Corresponding author.

E-mail addresses: messaoud.babaghayou@univ-tlemcen.dz (M. Babaghayou), nabila.labraoui@mail.univ-tlemcen.dz (N. Labraoui), adodamou.abbaari@gmail.com (A.A. Abba Ari), n.lagraa@lagh-univ.dz (N. Lagraa), ferrag.mohamedamine@univ-guelma.dz (M.A. Ferrag).

<https://doi.org/10.1016/j.jisa.2020.102618>


2214-2126/© 2020 Elsevier Ltd. All rights reserved.

3) Transmission range changing effects on location privacy-preserving schemes in the internet of vehicles


International Journal of Strategic Information Technology and Applications
Volume 10 • Issue 4 • October-December 2019

Transmission Range Changing Effects on Location Privacy-Preserving Schemes in the Internet of Vehicles


Messaoud Babaghayou, University of Tlemcen, Algeria

 <https://orcid.org/0000-0001-9508-7134>

Nabila Labraoui, University of Tlemcen, Algeria

 <https://orcid.org/0000-0002-5135-8972>

Ado Adamou Abba Ari, University of Maroua, Cameroon

 <https://orcid.org/0000-0001-5660-0660>

Abdelhak Mourad Gueroui, Ferhat Abbas University, Computer Science Department, Laboratory LRSD, Sétif, Algeria

ABSTRACT

The internet of vehicles (IoV) is getting a considerable amount of attention from different research parties. IoV aims at enhancing the driving experience with its wide range of applications varying from safety, road management to entertainment; however, some of such applications bring severe security and privacy issues; identity exposing, and location tracking are good examples. By enabling vehicles to send their statuses to themselves via beacon messages, this creates an environmental awareness for safety purposes but also exposes them to the aforementioned attacks. A lot of work has been done to mitigate the effect of such attacks but still does not provide a holistic solution. In this article, which is an extension to a prior work, the authors investigate the effects of changing the transmission range while sending beacons on the achieved level of location privacy based on two location privacy schemes: SLOW and CAPS. The authors use additional privacy metrics in addition to comparing the strategies in some well-known security attacks. The outcomes confirm the feasibility of using such a mechanism.

KEYWORDS

IoV, Location Privacy Preservation, Pseudonym Change Strategies, Transmission Power Adjustment

DOI: 10.4018/IJSITA.2019100103

Copyright © 2019, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

4) Location-privacy evaluation within the extreme points privacy (epp) scheme for vanet users


International Journal of Strategic Information Technology and Applications
Volume 10 • Issue 2 • April-June 2019

Location-Privacy Evaluation Within the Extreme Points Privacy (EPP) Scheme for VANET Users

Messaoud Babaghayou, University of Tlemcen, Tlemcen, Algeria

Nabila Labraoui, University of Tlemcen, Tlemcen, Algeria

Ado Adamou Abba Ari, University of Maroua, Maroua, Cameroon, & LI-PaRAD Lab, Université Paris Saclay, University of Versailles Saint-Quentin-en-Yvelines, Versailles, France

 <https://orcid.org/0000-0001-5660-0660>

ABSTRACT

The main purpose of designing vehicular ad-hoc networks (VANETs) is to achieve safety by periodically broadcasting the vehicle's coordinates with a high precision. This advantage brings a threat represented in the possible tracking and identification of the vehicles. A possible solution is to use and change pseudonyms. However, even by changing pseudonyms, the vehicle could still be tracked if the adversary has a prior knowledge about the potential start and end points of a particular driver who has social interactions (e.g., with neighbors) which introduces the concept of vehicular social networks (VSNs). This article extends the authors previous work, namely: "EPP Extreme Points Privacy for Trips and Home Identification in Vehicular Social Networks," which exploits the nature of the end points that are common between VSN users in order to create shared zones to anonymize them. The extension is represented by (a) the evaluation of the enjoyed location privacy of VSN users after quitting the district in addition to (b) detailing the used environment during the evaluation.

KEYWORDS

Anonymity, Home Identification, Location Privacy, VSN

INTRODUCTION

Background

The emerging of wireless technologies had big impact on different fields which led to the birth of vehicular social networks (VSNs), one of the wireless technology applications in the field of vehicles; or the so-called vehicular ad-hoc networks (VANETs). The evolution and enhancement of VANET capabilities has significant influence on the successfulness of the Intelligent Transportation Systems (ITSs) (Lu et al., 2012; Mfenjou et al., 2018; Ngossaha et al., 2018). In VANETs there exist two kinds of communications and they are self-describing: Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I). In order to be able to communicate, vehicles are equipped with onboard units (OBUs); specific devices that allow vehicles to: communicate, process data, receive GPS signal and use variant sensors. For a better system, vehicles may often communicate with central infrastructures. Such infrastructures may be roadside units (RSUs) (Al-Kahtani, 2012). VANET applications may be diverse; however, the number one reason for what it was proposed is to reduce the number of crashes

DOI: 10.4018/IJSITA.2019040103

Copyright © 2019, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

1) Between Location protection and Overthrowing: A Contrariness Framework Study for Smart Vehicles

Between Location protection and Overthrowing: A Contrariness Framework Study for Smart Vehicles

Messaoud Babaghayou and Nabila Labraoui
STIC Laboratory
 Tlemcen University, Algeria
 messaoud.babaghayou@univ-tlemcen.dz,
 nabila.labraoui@mail.univ-tlemcen.dz

Mohamed Amine Ferrag
Computer Science Department
 Guelma University, Algeria
 ferrag.mohamedamine@univ-guelma.dz

Leandros Maglaras
School of CS and Informatics
 De Montfort University, UK
 leandros.maglaras@dmu.ac.uk

Abstract—Internet of Vehicles (IoV) capabilities can be used to decrease the number of accidents by sharing information among entities like the location of the Smart Cars (SCs). This information is not encrypted due to several real-time communications requirements. Many methods were proposed by the literature to withhold the attacker from exploiting such a privacy gap and from affecting negatively other application layers like safety, comfort, and road-congestion. In this paper, we provide a holistic overview of the effects of existing techniques on both privacy and other application layers both from the attacker and the defender point of view.

Index Terms—Smart cars, IoV security and privacy, location tracking, eavesdropping attack, location and identity disclosure, anonymity protection

I. INTRODUCTION

Internet of Vehicles (IoV) is emerging as a promising paradigm in intelligent transportation systems (ITS) to enhance the existing capabilities of vehicular ad hoc networks (VANETs) by entailing the Internet of Things (IoT) [1], [2]. IoV is a vehicular network model consisting of vehicles, users and other smart devices connected to the network and aims to provide various safety, road-management as well as comfort services and applications [3]. By doing so, we got birth of the Smart Cars (SCs) that are able to exchange information and to fulfill both network efficiency and road safety requirements. The exploiting of infrastructures is also used to enhance the communications between the SCs especially in sparse scenarios. As shown in Fig.1, Two types of communications over the Dedicated Short-Range Communication (DSRC) protocol are enabled: Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) [4]. However, the security task is considered as a challenging issue for the successfulness of the SCs after this task became an eye-catching field for attackers [5], [6].

Generally speaking, IoV is responsible of mitigating the number of crashes by enabling the SCs to generate and broadcast a specific kind of messages; the Basic Safety Message (BSM) that contains the location of the ego-vehicle. An example of what kind of information would be included in such messages, in addition to the location, are illustrated in Fig.1. The location is sent to the neighborhood to provide a better vision and environmental awareness. The frequency of BSMs is recommended to be from 1 to 10 times per second

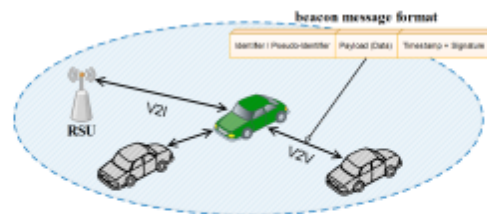


Fig. 1: The different communications and beacon message format in IoV

with a radius of about 300m according to the standardization [7] which gives a very precise awareness. In spite of this great and benign feature, it can be, at the same time, be a serious vulnerability that can be exploited by attackers to pinpoint their target(s) in real time only with the use of non-expensive and affordable eavesdropping devices that run in the same frequency-band as the SCs'. Fortunately, the research community is already making mechanisms to cope with this privacy issue [8]. The core principle of most of these mechanisms is the use of the so-called pseudonyms. A pseudonym is an identifier used instead of the real and permanent ID and is changed from time to time to break the continuous tracking. Nevertheless, the aforementioned solutions imply some trade-offs the most worthy considering are the privacy-safety, the privacy-road-congestion and the privacy-entertainment trade-offs. This had motivated us to investigate such trade-offs and to study the implication of the privacy mechanisms on the different application layers.

The main contributions of this paper are listed as follows:

- We provide a conceptual framework to characterize the location privacy issue from the authority and the SC user's perspective who aims at protecting his location privacy.
- We provide a conceptual framework to characterize the location privacy issue from the attacker's perspective who aims at overthrowing the location privacy.
- We summarize the existing trade-offs and remarks that exist in the two conceptual frameworks and formulating

2) Preserving the Location Privacy of Drivers Using Transmission Range Changing Techniques in Internet of Vehicles

Preserving the Location Privacy of Drivers Using Transmission Range Changing Techniques in Internet of Vehicles

1st Messaoud Babaghayou
STIC Laboratory

Tlemcen University, Algeria
messaoud.babaghayou@univ-tlemcen.dz

2nd Nabila Labraoui
STIC Laboratory

Tlemcen University, Algeria
nabila.labraoui@mail.univ-tlemcen.dz

3rd Ado Adamou Abba Ari
Li-Parad Laboratory

Versailles University, France
adoadamou.abbaari@gmail.com

4th Mohamed Amine Ferrag
Computer Science Department

Guelma University, Algeria
ferrag.mohamedamine@univ-guelma.dz

5th Leandros Maglaras

School of CS and Informatics
De Montfort University, UK
leandros.maglaras@dmu.ac.uk

Abstract—Internet of Vehicles (IoV) had remarkably enhanced the road-safety. Thanks to the environment sensing feature provided by the embedded devices and sensors. Nevertheless, this benignant feature had also introduced privacy issues; as vehicles spread their fine-grained locations at the aim of fulfilling safety requirements, adversaries can use this latter to track and identify the IoV users. Different privacy schemes and techniques are designed and evaluated like the mix-zone, encryption, groups forming, and silent-period based techniques. However, the majority do suffer from serious limitations inherited from the technique itself. In this paper, we propose a safety-friendly location privacy-preserving scheme, WHISPER, that adjusts the transmission range of vehicles on-the-fly in order to, occasionally, escape the continuous location tracking. We detail the protocols used by WHISPER, then we compare it against other privacy-preserving schemes using different metrics. The results show that WHISPER outperformed the other schemes after giving better location privacy levels while still keeping the road-safety fulfilled.

Index Terms—IoV privacy and safety, location privacy, pseudonym change strategy, transmission range adjustment.

I. INTRODUCTION

Vehicular Ad-hoc Network (VANET) with its variety of protocols (e.g., IEEE 802.11P, IEEE 1609, etc.) and communication types like Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) [1] has served as a basis for the promising Internet of Vehicles (IoV) paradigm [2]. IoV benefits from VANET to extend the useability range by allowing non conventional communications and applications, i.e., Vehicle to Everything (V2X) communications, to emerge. The strong and robust modern components and sensors give vehicles better environment sensing which results in better system functioning. Fig. 1 shows the V2X external communications and internal equipments. A vehicle using V2X can enhance the road-safety by broadcasting, through its On-Board-Unit (OBU), a status-form beacon message called the Basic Safety Message (BSM) with a 300m range and a frequency of 1 to 10

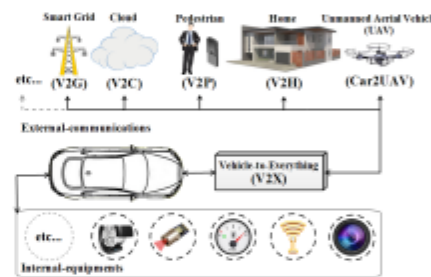


Fig. 1: V2X technology illustration

BSMs per second according to the standardization [3]. BSMs contain fields like identifier/pseudonym, position, velocity and size of the vehicle in addition to the timestamp and signature for security purposes. This lets vehicles be aware of the potential dangers coming from the nearby vehicles in addition to giving the option to manage the road-congestion through the implemented Road-Side-Units (RSUs).

Since BSMs contain fine-grained location data, even though they are useful for the road safety, they do open privacy-related issues because any entity that has some eavesdropping stations can monitor the whereabouts of its IoV user target(s) (when the eavesdropping stations are running in the frequency band of IoV).

Most location privacy schemes (e.g., mix-zone, synchronized schemes, etc.) are useless to achieve a high privacy level because of the very precise locations included in the BSMs and because of their resource and overhead consuming characteristic (group-based, encryption-based, etc.). The best mechanism used is that of the silent period schemes by ceasing

3) The Impact of the Adversary’s Eavesdropping Stations on the Location Privacy Level in Internet of Vehicles

The Impact of the Adversary’s Eavesdropping Stations on the Location Privacy Level in Internet of Vehicles

1st Messaoud Babaghayou
STIC Laboratory
 Tlemcen University, Algeria
 messaoud.babaghayou@univ-tlemcen.dz

2nd Nabila Labraoui
STIC Laboratory
 Tlemcen University, Algeria
 nabila.labraoui@mail.univ-tlemcen.dz

3rd Ado Adamou Abba Ari
LaRI Laboratory
 Maroua University, Cameroon
 adoadamou.abbaari@gmail.com
LI-PaRAD Laboratory
 Versailles University, France
 ado-adamou.abba-ari@uvsq.fr

4th Mohamed Amine Ferrag
Department of Computer Science
 Guelma University, Algeria
 ferrag.mohamedamine@univ-guelma.dz

5th Leandros Maglaras
Department of Computer Technology
 De Montfort University, United Kingdom
 leandros.maglaras@dmu.ac.uk

Abstract—The Internet of Vehicles (IoV) has got the interest of different research bodies as a promising technology. IoV is mainly developed to reduce the number of crashes by enabling vehicles to sense the environment and spread their locations to the neighborhood via safety-beacons to enhance the system functioning. Nevertheless, a bunch of security and privacy threats are looming; by exploiting the spatio-data included in these beacons. A lot of privacy schemes were developed to cope with the problem like CAPS, CPN, RSP and SLOW. The schemes provide a certain level of location privacy yet the strength of the adversary, e.g., the number of eavesdropping stations, has not been fully considered. In this paper we aim at investigating the effect of the adversary’s eavesdropping stations number and position on the overall system functioning via privacy and QoS metrics. We also show the performances of these schemes in a manhattan-grid model which gives a comparison between the used schemes. The results show that both the number and the emplacement of the eavesdropping stations have a real negative impact on the achieved location privacy of the IoV users.

Keywords—Location privacy, pseudonym change strategies, eavesdropping attack, IoV, VANETs

I. INTRODUCTION

A. Background

By leveraging the diverse sensors and communication technologies, IoV is considered to be the most fitting research axis that ensures safety, road management and entertainment for the car users by exploiting the Vehicle-to-Everything (V2X) technology [1] that is in the rollout phase. IoV uses the high sensing abilities provided by the inter-components that are embedded in the cars in order to get a better environmental awareness that is next spread to the neighborhood. Additionally, the V2X technology makes it easy for vehicles to communicate with heterogeneous networks and devices. Fig. 1 describes the emerging IoV paradigm.

978-1-7281-6445-8/20/531.00 ©2020 IEEE

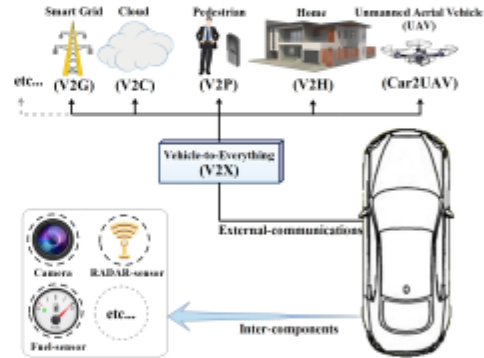


Fig. 1: The V2X communications of sensor equipped cars

B. Problematic and Research Motivation

Although V2X allows vehicles to prevent accidents, traffic jams and other road-related issues, much security and privacy efforts are needed [2]. Since vehicles share their locations in periodic beacons for the sake of safety, collecting such data becomes an easy task for the non-authorized entities. This data collection does only necessitate the possession of one or more eavesdropping stations. Since vehicles are meant to broadcast beacons with a range of 300m [3], creating a full eavesdropping area would be possible by malicious persons and/or colluding organizations; that is the Global Passive Adversary (GPA) [4]. The effect of the adversary’s eavesdropping stations amount and emplacement have a serious impact on the achieved location privacy level of the car users since it

4) Security-Aware Monitoring Approach for Location Abusing and Suspicious Behavior in Internet of Vehicles

ECHAHID HAMMA LAKHDAR UNIVERSITY - EL-OUED

Under the Supervision of the DGRSDT and in collaboration with the CRTI

International Pluridisciplinary PhD Meeting (IPPM'20)

23-26, 2020 1st Edition, February

Theme: Modern Technology and Fineness Life

Security-Aware Monitoring Approach for Location Abusing and Suspicious Behavior in Internet of Vehicles

Messaoud Babaghayou^{a*}, Nabila Labraoui^b, Ado Adamou Abba Ari^{c*}, Nasreddine Lagraa^d, Mohamed Amine Ferrag^e

^aSTIC Lab, Abou Bekr Belkaid University, P.O. Box 230, chetouane, Tlemcen 13000, Algeria

^bLI-ParAD Lab, Saint-Quentin-en-Yvelines University, 45 Avenue Etats-Unis 78035 Versailles cedex, France

^cLaRI Lab, Maroua University, P.O. Box 814 Maroua, Cameroon

^dLIM Lab, Amar Telidji University, P.O. Box G37, Route de Ghardaia (M'kam), Laghouat 03000, Algeria

^eDepartment of Computer Science, Guelma University, B.P. 401, 24000, Algeria

Email addresses: babaghayoumessaoud@hotmail.com (Messaoud Babaghayou), nabila.labraoui@mai.univ-lemcen.dz (Nabila Labraoui), adoadamou.abbaari@gmail.com (Ado Adamou Abba Ari), n.lagraa@lqyb-univ.dz (Nasreddine Lagraa), ferrag.mohamedamine@univ-guelma.dz (Mohamed Amine Ferrag)

Abstract

The fast and huge revolution on the wireless communication technologies and embedded systems had opened the gate towards promising implementations and applications: Vehicular-Ad-hoc Networks (VANETs) and the safety enhancing applications provided by the Internet of Vehicles (IoV) paradigm are one of them. By periodically broadcasting safety-beacons, vehicles can ensure a better safety driving experience as these beacons contain fine-grained location spread next to the neighborhood. Nevertheless, some attacks that modify, remove and encrypt location-related data included in beacons are threatening the road-safety considerably. In this paper, we provide a Security-Aware Monitoring Approach (SAMA) that protects against such a location abusing by allowing the Law-Side Authorities (LSAs) to monitor the potential malicious vehicles. SAMA is implemented using the well-known triangulation concept via Received Signal Strength Indicator (RSSI) in conjunction with `c++` map and multimap data-structures. The performances of SAMA are evaluated in terms of location-estimation precision and beacons collection per type (mono, duo and triangulation).

Keywords: location monitoring, position detection, triangulation, location privacy, malicious attacks, IoV, VANETs

1. Introduction

Vehicular Ad-hoc Network (VANET), the wireless network of cars had boosted the driving experience of road users enormously via communication types like Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) [1], in addition to providing a bases for the Vehicle to Everything (V2X) that serves as a core for the Internet of Vehicles (IoV) paradigm [2]. Parallely, location detection techniques such as GPS, RSU-aided and Location Based Service (LBS) [3] are getting much attention due to their high utility [4]. To avoid accidents and traffic jams, vehicles must broadcast safety-beacon messages that contain the vehicle's status [5] including its location which, as a consequence, forms an environment instantiation. This beaconing is done in a range of 300m and up to 10 beacons per second [6].

1.1. Problematic and Research Motivation

This beaconing had opened location-privacy issues which were an incentive for the research community to find mitigation to these limitations; using pseudonyms and changing them over time was accepted as a fair solution [7] and much schemes had emerged [6]. In spite of being these schemes benign to the IoV users' location-privacy, they also open an attack vector to malicious vehicles as they can escape monitoring when modifying and/or encrypting such spatio-related beacons from the Law Enforcement Authority (LEA) without a defending mechanism, in addition for giving the option to launch Sybil attacks [8]. Localization techniques are becoming a must in such a case.

1.2. Contributions and Paper Organization

The contributions of the paper are stated as follows:

- Introducing our system model that leverages the power and financial abilities of the Law-Side Authority to monitor and protect against the resulting vector attacks.
- Recalling and formulating the used triangulation technique to detect a node (vehicle) by its Received Signal Strength Indicator (RSSI) and the nearby monitoring stations.
- Providing our proposed Security-Aware Monitoring Approach (SAMA) that estimates the location of potential malicious vehicles and explaining the used `c++` map and multimap data-structures in addition to giving the pseudo-code of SAMA protocols and its results.

The remaining paper parts are presented as follows: Section 2, sheds light on legitimate privacy-schemes that encrypt beacon fields and discuss the localization-related state of the art. Next, the system model and coverage modes are described in section 3. Then, the proposed SAMA approach is explained in details in section 4. After

5) Transmission range adjustment influence on location privacy-preserving schemes in vanets

Transmission Range Adjustment Influence on Location Privacy-Preserving Schemes in VANETs

1st Messaoud Babaghayou

STIC Laboratory

Tlemcen University, Algeria

messaoud.babaghayou@univ-tlemcen.dz

2nd Nabila Labraoui

STIC Laboratory

Tlemcen University, Algeria

nabila.labraoui@mail.univ-tlemcen.dz

Abstract—Vehicular Ad-hoc Networks (VANETs) are in the rollout phase. VANETs are mainly instantiated to mitigate the number of crashes and fatalities by enabling an intensive beaconing that contains the fine-grained location of each vehicle at the aim of creating environmental awareness for safety purposes. However, this frequent location information may be obtained by adversaries after overhearing the beacons; giving an unauthenticated entity(s) the ability to monitor the vehicles' whereabouts in a region of interest. A lot of schemes to protect location privacy were proposed. In this paper, we provide an enhancement of a set of schemes by allowing vehicles to adjust their beacon transmission range to conditionally avoid tracking. For the best of our knowledge, and excluding the scopes other than location privacy in VANETs, this is the first evaluation of transmission adjustment influence on the achieved location privacy. We made an evaluation of this feature's performances after integrating it into some of the well-known strategies, namely: SLOW and CAPS, against (1) the achieved location privacy using the traceability metric and (2) the network performances. The results show the beneficial usability of such a feature.

Index Terms—Location privacy, pseudonym change strategies, transmission power adjustment, VANETs

I. INTRODUCTION

A. Background

Vehicular Ad-hoc Networks (VANETs) are becoming an active field of research during the last decades. VANETs are envisioned to mainly reduce the number of fatalities by enabling Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications over the Dedicated Short-Range Communication (DSRC) protocol [1]. Thus, a fast reaction may be taken by drivers during dangerous situations. To achieve this goal, each vehicle has to periodically broadcast its status in terms of location, speed, velocity, time, etc. set in a beacon message. This kind of beacon is called Basic Safety Message (BSM) [2].

B. Location Privacy Problem

For fast reaction and less delay, BSM content is not encrypted and sent at least once per second with a radius of about 300 meters [2]. Thus, any entity having a dedicated eavesdropping station would have an access to the driver's location and this will be exploited next to generate user

profiles [3] which has a negative impact on VANET users' location privacy. One of the solutions is to use pseudonyms instead of real identities while broadcasting these BSMs and furthermore, making them temporal and changeable over time [4]. Also, a cross-layer identifier (like mac and ip) change is needed [5]. However, if the pseudonym change was not done in an appropriate time and/or space, a correlation attack may be performed by the adversary to link the new and the old pseudonym. The aforementioned issue had motivated the research community to develop a lot of robust schemes like [6]–[16] (are shown in more details in section II) to well-protect the user's location and identity privacy.

C. Contributions and Organization of the Paper

This paper's contributions are represented as follows:

- Introducing the concept of transmission range adaptation (TRA) for location privacy enhancement.
- Integrating TRA into two of the well-known privacy schemes (SLOW and CAPS) then comparing their performances with and without the TRA integration.
- Investigating the impact of TRA in aspects other than privacy like the network performances (QoS) and showing its beneficial implementation.

The remainder of this paper is organized as follows: In section II, we briefly shed light on the most discussed strategies for the location privacy problem. Next in section III, we demonstrate our system model. Then in section IV, we define the detailed functioning of our TRA mechanism followed by a performance evaluation study in section V. Later in section VI, we discuss the overall of TRA and give potential opened work directions. Finally, we conclude our research in section VII.

II. RELATED WORK

The location privacy was highly debated in the last years. Beresford and Stajano introduced the concept of mix-group [6] inspired by the mix-network concept. A mix-group is a region where vehicles are mixed. i.e., their communication is not traceable. However, the inclusion of the fine-grained location in BSM messages does facilitate tracking of users. Basing on the same concept, Freudiger et al. proposed CMIX protocol [10]. CMIX uses mix-zones with cryptography. Thus, drivers' location is preserved by encrypting their BSMs while

6) EPP: Extreme Points Privacy for Trips and Home Identification in Vehicular Social Networks

EPP: Extreme Points Privacy for Trips and Home Identification in Vehicular Social Networks

Messaoud Babaghayou¹[0000-0001-9508-7134], Nabila Labraoui¹[0000-0002-5135-8972], and Ado Adamou Abba Ari^{2,3}[0000-0001-5660-0660]

¹ STIC Lab, Abou Bakr Belkaid University of Tlemcen, P.O. Box 230, chetouane Tlemcen 13000, Algeria

babaghayoumessaoud@hotmail.com, nabila.labraoui@mail.univ-tlemcen.dz

² LaRI Lab, University of Maroua, P.O. Box 814 Maroua, Cameroon
adoadamou.abbaar1@gmail.com

³ LI-PaRAD Lab, Université Paris Saclay, University of Versailles Saint-Quentin-en-Yvelines, 45 Avenue des États-Unis 78035 Versailles cedex, France

Abstract. The main purpose of designing Vehicular Ad-hoc Networks (VANETs) is to achieve safety by periodically broadcasting the vehicle's coordinates with a high precision. This advantage brings a threat represented in the possible tracking and identification of the vehicles. A possible solution is to use pseudonyms instead of real identities. However, even by changing pseudonyms, the vehicle can still be tracked if the adversary has knowledge about the potential start and end points of a particular driver who has social interactions (e.g., with neighbors) which introduces the concept of Vehicular Social Networks (VSNs). In this work we propose a location privacy scheme, namely: Extreme Points Privacy (EPP) for trips and home identification in VSNs by exploiting the nature of the end points that are common between many VSN users bringing the option to create shared zones to anonymize these users. An analytical study accompanied by a simulation using the realistic vehicular traffic mobility generator SUMO are presented to show the effectiveness of the proposed scheme.

Keywords: Location Privacy · Anonymity · Home Identification.

1 Introduction

The human behaviour and social interactions were almost apparent in drivers moving patterns which lead to the emergence of VSNs. The evolution and enhancement of VANET capabilities have significant influence on the successfulness of the Intelligent Transportation Systems (ITSs) [1, 2]. In VANETs, there exist two kinds of communications: Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I). In order to be able to communicate, vehicles are equipped with On Board Units (OBUs); specific devices that allow vehicles to: communicate,

References

- [1] Ajay Dureja and Suman Sangwan. A review: Efficient transportation—future aspects of iov. *Evolving Technologies for Computing, Communication and Smart World*, pages 97–108, 2021.
- [2] M Saifeddine Hadj Sassi and Lamia Chaari Fourati. Investigation on deep learning methods for privacy and security challenges of cognitive iov. In *2020 International Wireless Communications and Mobile Computing (IWCMC)*, pages 714–720. IEEE, 2020.
- [3] David Tse and Pramod Viswanath. *Fundamentals of wireless communication*. Cambridge university press, 2005.
- [4] Ado Adamou Abba Ari, Abdelhak Gueroui, Chafiq Titouna, Ousmane Thiare, and Zibouda Aliouat. Resource allocation scheme for 5g c-ran: a swarm intelligence based approach. *Computer Networks*, 165:106957, 2019.
- [5] Road Crash Statistics. <https://www.asirt.org/safe-travel/road-safety-facts/>. Accessed: 2021-04-12.
- [6] Albert Wasef. Managing and complementing public key infrastructure for securing vehicular ad hoc networks. 2011.
- [7] Fengzhong Qu, Zhihui Wu, Fei-Yue Wang, and Woong Cho. A security and privacy review of vanets. *IEEE Transactions on Intelligent Transportation Systems*, 16(6):2985–2996, 2015.
- [8] David Eckhoff and Christoph Sommer. Readjusting the privacy goals in vehicular ad-hoc networks: A safety-preserving solution using non-overlapping time-slotted pseudonym pools. *Computer Communications*, 122:118–128, 2018.
- [9] Hoa La Vinh and Ana Rosa Cavalli. Security attacks and solutions in vehicular ad hoc networks: a survey. *International journal on AdHoc networking systems (IJANS)*, 4(2):1–20, 2014.
- [10] David Eckhoff, Reinhard German, Christoph Sommer, Falko Dressler, and Tobias Gansen. Slotswap: Strong and affordable location privacy in intelligent transportation systems. *IEEE Communications Magazine*, 49(11):126–133, 2011.
- [11] Ram Shringar Raw, Manish Kumar, and Nanhay Singh. Security challenges, issues and their solutions for vanet. *International journal of network security & its applications*, 5(5):95, 2013.

-
- [12] Chaker Abdelaziz Kerrache, Abderrahmane Lakas, Nasreddine Lagraa, and Ezedin Barka. UAV-assisted technique for the detection of malicious and selfish nodes in VANETs. *Vehicular Communications*, 11:1–11, 2018.
- [13] Ado Adamou Abba Ari, Irépran Damakoa, Abdelhak Gueroui, Chafiq Titouna, Nabila Labraoui, Guidedi Kaladzavi, and Blaise Omer Yenké. Bacterial foraging optimization scheme for mobile sensing in wireless sensor networks. *International Journal of Wireless Information Networks*, 24(3):254–267, 2017.
- [14] Yichuan Wang, Yuying Tian, Xinhong Hei, Lei Zhu, and Wenjiang Ji. A novel iov block-streaming service awareness and trusted verification in 6g. *IEEE Transactions on Vehicular Technology*, 2021.
- [15] Shao-hui Sun, Jin-ling Hu, Ying Peng, Xue-ming Pan, Li Zhao, and Jia-yi Fang. Support for vehicle-to-everything services based on lte. *IEEE Wireless Communications*, 23(3):4–8, 2016.
- [16] Saif Al-Sultan, Moath M Al-Doori, Ali H Al-Bayatti, and Hussien Zedan. A comprehensive survey on vehicular ad hoc network. *Journal of network and computer applications*, 37: 380–392, 2014.
- [17] Shiau Hong Lim, Yeow Khiang Chia, and Laura Wynter. Accurate and cost-effective traffic information acquisition using adaptive sampling: Centralized and v2v schemes. *Transportation research procedia*, 23:61–80, 2017.
- [18] Qian Mei, Hu Xiong, Jinhao Chen, Minghao Yang, Saru Kumari, and Muhammad Khurram Khan. Efficient certificateless aggregate signature with conditional privacy preservation in iov. *IEEE Systems Journal*, 2020.
- [19] Nasreddine Lagraa. *Commandes non-linéaires et intelligentes des systèmes complexes: Application à la suspension des véhicules*. PhD thesis, Ecole Nationale Polytechnique, 2008.
- [20] Surbhi Sharma and Baijnath Kaushik. A survey on internet of vehicles: Applications, security issues & solutions. *Vehicular Communications*, 20:100182, 2019.
- [21] Ado Adamou Abba Ari, Olga Kengni Ngangmo, Chafiq Titouna, Ousmane Thiare, Alidou Mohamadou, Abdelhak Mourad Gueroui, et al. Enabling privacy and security in cloud of things: Architecture, applications, security & privacy challenges. *Applied Computing and Informatics*, 2019.
- [22] Nishant Sharma, Naveen Chauhan, and Narottam Chand. Security challenges in internet of vehicles (ioV) environment. In *2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC)*, pages 203–207. IEEE, 2018.
- [23] Messaoud Babaghayou, Nabila Labraoui, and Ado Adamou Abba Ari. Location-privacy evaluation within the extreme points privacy (epp) scheme for vanet users. *International Journal of Strategic Information Technology and Applications (IJSITA)*, 10(2):44–58, 2019.

-
- [24] Messaoud Babaghayou and Nabila Labraoui. Transmission range adjustment influence on location privacy-preserving schemes in vanets. In *2019 International Conference on Networking and Advanced Systems (ICNAS)*, pages 1–6. IEEE, 2019.
- [25] Chaker Abdelaziz KERRACHE. *Malicious messages detection and exclusion mechanisms in Vehicular Networks (VANETs)*. PhD thesis, 2017.
- [26] John B Kenney. Dedicated short-range communications (dsrc) standards in the united states. *Proceedings of the IEEE*, 99(7):1162–1182, 2011.
- [27] Jian Wang, Yameng Shao, Yuming Ge, and Rundong Yu. A survey of vehicle to everything (v2x) testing. *Sensors*, 19(2):334, 2019.
- [28] George P Corser, Alejandro Arenas, and Huirong Fu. Effect on vehicle safety of nonexistent or silenced basic safety messages. In *2016 International Conference on Computing, Networking and Communications (ICNC)*, pages 1–5. IEEE, 2016.
- [29] Ministry for Primary Industries. ETSI TR 103 415. Intelligent Transport Systems (ITS); security; pre-standardization study on pseudonym change management,, 2018. ETSI standards.
- [30] Hannes Hartenstein and LP Laberteaux. A tutorial survey on vehicular ad hoc networks. *IEEE Communications magazine*, 46(6):164–171, 2008.
- [31] Stéphanie Lefevre, Jonathan Petit, Ruzena Bajcsy, Christian Laugier, and Frank Kargl. Impact of v2x privacy strategies on intersection collision avoidance systems. In *Vehicular Networking Conference (VNC), 2013 IEEE*, pages 71–78. IEEE, 2013.
- [32] Joo-Han Song, Vincent W Wong, and Victor C Leung. Wireless location privacy protection in vehicular ad-hoc networks. *Mobile Networks and Applications*, 15(1):160–171, 2010.
- [33] Georgios Karagiannis, Onur Altintas, Eylem Ekici, Geert Heijenk, Boangoat Jarupan, Kenneth Lin, and Timothy Weil. Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions. *IEEE communications surveys & tutorials*, 13(4):584–616, 2011.
- [34] Chaker Abdelaziz Kerrache, Nasreddine Lagraa, Carlos T Calafate, and Abderrahmane Lakas. TFDD: A trust-based framework for reliable data delivery and DoS defense in VANETs. *Vehicular Communications*, 9:254–267, 2017.
- [35] Bum Han Kim, Kyu Young Choi, Jun Ho Lee, and Dong Hoon Lee. Anonymous and traceable communication using tamper-proof device for vehicular ad hoc networks. In *Convergence Information Technology, 2007. International Conference on*, pages 681–686. IEEE, 2007.
- [36] Bassem Mokhtar and Mohamed Azab. Survey on security issues in vehicular ad hoc networks. *Alexandria Engineering Journal*, 54(4):1115–1126, 2015.
- [37] Leila Benarous. *Security and Privacy in Vehicular Networks*. PhD thesis, 2020.

-
- [38] Y Bevish Jinila, G Merlin Sheeba, and S Prayla Shyry. Ppsa: Privacy preserved and secured architecture for internet of vehicles. *Wireless Personal Communications*, pages 1–18, 2021.
- [39] Albert Wasef, Rongxing Lu, Xiaodong Lin, and Xuemin Shen. Complementing public key infrastructure to secure vehicular ad hoc networks [security and privacy in emerging wireless networks]. *IEEE Wireless Communications*, 17(5):22–28, 2010.
- [40] Messaoud Babaghayou, Nabila Labraoui, Ado Adamou Abba Ari, Nasreddine Lagraa, and Mohamed Amine Ferrag. Pseudonym change-based privacy-preserving schemes in vehicular ad-hoc networks: A survey. *Journal of Information Security and Applications (JISA)*, 2020.
- [41] Jonathan Petit, Florian Schaub, Michael Feiri, and Frank Kargl. Pseudonym schemes in vehicular networks: A survey. *IEEE communications surveys & tutorials*, 17(1):228–255, 2015.
- [42] Claudia Diaz. Anonymity metrics revisited. In *Dagstuhl Seminar Proceedings*. Schloss Dagstuhl-Leibniz-Zentrum für Informatik, 2006.
- [43] Nabila Labraoui. *LA SÉCURITÉ DANS LES RÉSEAUX SANS FIL AD HOC*. PhD thesis, 2012.
- [44] Manjyot Saini and Harjit Singh. Vanet its characteristics attacks and routing techniques: A survey. *International Journal of Science and Research*, 5(5):1595–1599, 2016.
- [45] Christine Laurendeau and Michel Barbeau. Threats to security in dsrc/wave. In *International Conference on Ad-Hoc Networks and Wireless*, pages 266–279. Springer, 2006.
- [46] BCM Cappers. Interactive visualization of event logs for cybersecurity. 2018.
- [47] Lelio Campanile, Mauro Iacono, Fiammetta Marulli, and Michele Mastroianni. Designing a gdpr compliant blockchain-based iov distributed information tracking system. *Information Processing & Management*, 58(3):102511, 2021.
- [48] Yasmine Harbi. *Security in internet of things*. PhD thesis, 2021.
- [49] Djilali Moussaoui, Benamar Kadri, Mohammed Feham, and Boucif Ammar Bensaber. A distributed blockchain based pki (bcпки) architecture to enhance privacy in vanet. In *2020 2nd International Workshop on Human-Centric Smart Environments for Health and Well-being (IHSH)*, pages 75–79. IEEE, 2021.
- [50] Omar Rafik Merad Boudia, Sidi Mohammed Senouci, and Mohammed Feham. A novel secure aggregation scheme for wireless sensor networks using stateful public key cryptography. *Ad Hoc Networks*, 32:98–113, 2015.
- [51] Yuanyuan Pan, Jianqing Li, Li Feng, and Ben Xu. An analytical model for random changing pseudonyms scheme in VANETs. In *2011 International Conference on Network Computing and Information Security*, pages 141–145. IEEE, 2011.
- [52] Messaoud Babaghayou, Nabila Labraoui, Ado Adamou, Mohamed Amine Ferrag, and

- Leandros Maglaras. The impact of the adversary's eavesdropping stations on the location privacy level in internet of vehicles. *IEEE*, 2020.
- [53] Stephan Eichler. Strategies for pseudonym changes in vehicular ad hoc networks depending on node mobility. In *Intelligent Vehicles Symposium, 2007 IEEE*, pages 541–546. IEEE, 2007.
- [54] David Förster, Frank Kargl, and Hans Löhr. Puca: A pseudonym scheme with strong privacy guarantees for vehicular ad-hoc networks. *Ad Hoc Networks*, 37:122–132, 2016.
- [55] Isabel Wagner and David Eckhoff. Privacy assessment in vehicular networks using simulation. In *Proceedings of the 2014 Winter Simulation Conference*, pages 3155–3166. IEEE Press, 2014.
- [56] Brijesh Kumar Chaurasia, Shekhar Verma, GS Tomar, and Ajith Abraham. Optimizing pseudonym updation in vehicular ad-hoc networks. In *Transactions on Computational Science IV*, pages 136–148. Springer, 2009.
- [57] Abdelwahab Boualouache, Sidi-Mohammed Senouci, and Samira Moussaoui. Vlpz: The vehicular location privacy zone. *Procedia Computer Science*, 83:369–376, 2016.
- [58] Abdelwahab Boualouache, Sidi-Mohammed Senouci, and Samira Moussaoui. A survey on pseudonym changing strategies for vehicular ad-hoc networks. *IEEE Communications Surveys & Tutorials*, 20(1):770–790, 2018.
- [59] Branka Mikavica and Aleksandra Kostić-Ljubisavljević. Blockchain-based solutions for security, privacy, and trust management in vehicular networks: a survey. *The Journal of Supercomputing*, pages 1–56, 2021.
- [60] Alastair R Beresford and Frank Stajano. Location privacy in pervasive computing. *IEEE Pervasive computing*, (1):46–55, 2003.
- [61] Marco Gruteser and Xuan Liu. Protecting privacy, in continuous location-tracking applications. *IEEE Security & Privacy*, 2(2):28–34, 2004.
- [62] Einar Snekkenes. Concepts for personal location privacy policies. In *Proceedings of the 3rd ACM conference on Electronic Commerce*, pages 48–57, 2001.
- [63] Mohamed Amine Ferrag, Leandros Maglaras, and Ahmed Ahmim. Privacy-preserving schemes for ad hoc social networks: A survey. *IEEE Communications Surveys & Tutorials*, 19(4): 3015–3045, 2017.
- [64] Florian Schaub, Zhendong Ma, and Frank Kargl. Privacy requirements in vehicular communication systems. In *Computational Science and Engineering, 2009. CSE'09. International Conference on*, volume 3, pages 139–145. IEEE, 2009.
- [65] Qian Mei, Hu Xiong, Yanan Zhao, and Kuo-Hui Yeh. Toward blockchain-enabled iov with edge computing: Efficient and privacy-preserving vehicular communication and dynamic updating. In *2021 IEEE Conference on Dependable and Secure Computing (DSC)*, pages 1–8. IEEE.

-
- [66] Hamssa Hasrouny, Abed Ellatif Samhat, Carole Bassil, and Anis Laouti. Misbehavior detection and efficient revocation within vanet. *Journal of Information Security and Applications*, 46:193–209, 2019.
- [67] Anuj S Saxena, Debajyoti Bera, and Vikram Goyal. Modeling location obfuscation for continuous query. *Journal of information security and applications*, 44:130–143, 2019.
- [68] Krishna Sampigethaya, Leping Huang, Mingyan Li, Radha Poovendran, Kanta Matsuura, and Kaoru Sezaki. CARAVAN: Providing location privacy for vanet. Technical report, Washington Univ Seattle Dept of Electrical Engineering, 2005.
- [69] Leping Huang, Kanta Matsuura, Hiroshi Yamane, and Kaoru Sezaki. Enhancing wireless location privacy using silent period. In *Wireless Communications and Networking Conference, 2005 IEEE*, volume 2, pages 1187–1192. IEEE, 2005.
- [70] Mingyan Li, Krishna Sampigethaya, Leping Huang, and Radha Poovendran. Swing & Swap: user-centric approaches towards maximizing location privacy. In *Proceedings of the 5th ACM workshop on Privacy in electronic society*, pages 19–28. ACM, 2006.
- [71] Krishna Sampigethaya, Mingyan Li, Leping Huang, and Radha Poovendran. AMOEBA: Robust location privacy scheme for vanet. *IEEE Journal on Selected Areas in communications*, 25(8), 2007.
- [72] Julien Freudiger, Maxim Raya, Márk Félegyházi, Panos Papadimitratos, and Jean-Pierre Hubaux. Mix-zones for location privacy in vehicular networks. In *ACM Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS)*, number LCA-CONF-2007-016, 2007.
- [73] Matthias Gerlach and Felix Guttler. Privacy in VANETs using changing pseudonyms-ideal and real. In *Vehicular Technology Conference, 2007. VTC2007-Spring. IEEE 65th*, pages 2521–2525. IEEE, 2007.
- [74] Levente Buttyán, Tamás Holczer, and István Vajda. On the effectiveness of changing pseudonyms to provide location privacy in vanets. In *European Workshop on Security in Ad-hoc and Sensor Networks*, pages 129–141. Springer, 2007.
- [75] Julien Freudiger, Reza Shokri, and Jean-Pierre Hubaux. On the optimal placement of mix zones. In *International Symposium on Privacy Enhancing Technologies Symposium*, pages 216–234. Springer, 2009.
- [76] Brijesh Kumar Chaurasia and Shekhar Verma. Optimizing pseudonym updation for anonymity in vanets. In *Asia-Pacific Services Computing Conference, 2008. APSCC'08. IEEE*, pages 1633–1637. IEEE, 2008.
- [77] Levente Buttyán, Tamás Holczer, André Weimerskirch, and William Whyte. Slow: A practical pseudonym changing scheme for location privacy in vanets. In *Vehicular Networking Conference (VNC), 2009 IEEE*, pages 1–8. IEEE, 2009.

-
- [78] Jianxiong Liao and Jianqing Li. Effectively changing pseudonyms for privacy protection in vanets. In *Pervasive Systems, Algorithms, and Networks (ISPAN), 2009 10th International Symposium on*, pages 648–652. IEEE, 2009.
- [79] Rongxing Lu, Xiaodong Lin, and Xuemin Shen. SPRING: A social-based privacy-preserving packet forwarding protocol for vehicular delay tolerant networks. In *2010 Proceedings IEEE INFOCOM*, pages 1–9, March 2010.
- [80] Albert Wasef and Xuemin Sherman Shen. REP: Location privacy for VANETs using random encryption periods. *Mobile Networks and Applications*, 15(1):172–185, 2010.
- [81] Baik Hoh, Marco Gruteser, Hui Xiong, and Ansaif Alrabady. Achieving guaranteed anonymity in gps traces via uncertainty-aware path cloaking. *IEEE Transactions on Mobile Computing*, (8):1089–1107, 2010.
- [82] Rob Millerb Ishtiaq Roufa, Hossen Mustafaa, Sangho Ohb Travis Taylora, Wenyuan Xua, Marco Gruteserb, Wade Trappeb, and Ivan Seskarb. Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study. In *19th USENIX Security Symposium, Washington DC*, pages 11–13, 2010.
- [83] Hesiri Weerasinghe, Huirong Fu, Supeng Leng, and Ye Zhu. Enhancing unlinkability in vehicular ad hoc networks. In *Intelligence and Security Informatics (ISI), 2011 IEEE International Conference on*, pages 161–166. IEEE, 2011.
- [84] Rongxing Lu, Xiaodong Lin, Tom H Luan, Xiaohui Liang, and Xuemin Shen. Pseudonym changing at social spots: An effective strategy for location privacy in vanets. *IEEE transactions on vehicular technology*, 61(1):86, 2012.
- [85] Messaoud Babaghayou, Nabila Labraoui, and Ado Adamou Abba Ari. Epp: Extreme points privacy for trips and home identification in vehicular social networks. In *JERI*, 2019.
- [86] Yuanyuan Pan and Jianqing Li. Cooperative pseudonym change scheme based on the number of neighbors in vanets. *Journal of Network and Computer Applications*, 36(6):1599–1609, 2013.
- [87] George Corser, Huirong Fu, Tao Shu, Patrick D’Errico, and Warren Ma. Endpoint protection zone (epz): Protecting lbs user location privacy against deanonymization and collusion in vehicular networks. In *2013 International Conference on Connected Vehicles and Expo (ICCVE)*, pages 369–374. IEEE, 2013.
- [88] Julien Freudiger, Mohammad Hossein Manshaei, Jean-Pierre Hubaux, and David C Parkes. Non-cooperative location privacy. *IEEE Transactions on Dependable and Secure Computing*, 10(2):84–98, 2013.
- [89] Bidi Ying, Dimitrios Makrakis, and Hussein T Mouftah. Dynamic mix-zone for location privacy in vehicular networks. *IEEE Communications Letters*, 17(8):1524–1527, 2013.
- [90] Abdelwahab Boualouache and Samira Moussaoui. S2si: A practical pseudonym changing

- strategy for location privacy in vanets. In *2014 International Conference on Advanced Networking Distributed Systems and Applications (INDS)*, pages 70–75. IEEE, 2014.
- [91] Bidi Ying, Dimitrios Makrakis, and Zhengzhou Hou. Motivation for protecting selfish vehicles’ location privacy in vehicular networks. *IEEE Transactions on Vehicular Technology*, 64(12): 5631–5641, 2015.
- [92] Bidi Ying and Dimitrios Makrakis. Pseudonym changes scheme based on candidate-location-list in vehicular networks. In *Communications (ICC), 2015 IEEE International Conference on*, pages 7292–7297. IEEE, 2015.
- [93] Rong Yu, Jiawen Kang, Xumin Huang, Shengli Xie, Yan Zhang, and Stein Gjessing. Mixgroup: Accumulative pseudonym exchanging for location privacy enhancement in vehicular social networks. *IEEE Transactions on Dependable and Secure Computing*, 13(1):93–105, 2016.
- [94] Abdelwahab Boualouache and Samira Moussaoui. Urban pseudonym changing strategy for location privacy in vanets. *International Journal of Ad Hoc and Ubiquitous Computing*, 24(1-2):49–64, 2017.
- [95] Abdelwahab Boualouache and Samira Moussaoui. TAPCS: Traffic-aware pseudonym changing strategy for vanets. *Peer-to-Peer Networking and Applications*, 10(4):1008–1020, 2017.
- [96] Qasim Ali Arain, Imran Memon, Zhongliang Deng, Muhammad Hammad Memon, Farman Ali Mangi, and Asma Zubedi. Location monitoring approach: multiple mix-zones with location privacy protection based on traffic flow over road networks. *Multimedia Tools and Applications*, 77(5):5563–5607, 2018.
- [97] Ferroudja Zidani, Fouzi Semchedine, and Marwane Ayaida. Estimation of neighbors position privacy scheme with an adaptive beaconing approach for location privacy in vanets. *Computers & Electrical Engineering*, 71:359–371, 2018.
- [98] Karim Emar, Wolfgang Woerndl, and Johann 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*, page 21. ACM, 2015.
- [99] Leila Benarous, Benamar Kadri, Salim Bitam, and Abdelhamid Mellouk. Privacy-preserving authentication scheme for on-road on-demand refilling of pseudonym in vanet. *International Journal of Communication Systems*, page e4087, 2019.
- [100] Abdul Wahid, Humera Yasmeen, Munam Ali Shah, Masoom Alam, and Sayed Chhattan Shah. Holistic approach for coupling privacy with safety in vanets. *Computer Networks*, 148:214–230, 2019.
- [101] Messaoud Babaghayou, Nabila Labraoui, Ado Adamou Abba Ari, Mohamed Amine Ferrag, Leandros Maglaras, and Helge Janicke. Whisper: A location privacy-preserving scheme using transmission range changing for internet of vehicles. *Sensors*, 21(7), 2021. ISSN 1424-8220. doi: 10.3390/s21072443. URL <https://www.mdpi.com/1424-8220/21/7/2443>.

-
- [102] Elmar Schoch, Frank Kargl, Tim Leinmüller, Stefan Schlott, and Panos Papadimitratos. Impact of pseudonym changes on geographic routing in vanets. In *European Workshop on Security in Ad-hoc and Sensor Networks*, pages 43–57. Springer, 2006.
- [103] Martin Luther Mfenjou, Ado Adamou Abba Ari, Wahabou Abdou, François Spies, and Kolyang. Methodology and trends for an intelligent transport system in developing countries. *Sustainable Computing: Informatics and Systems*, 19:96–111, 2018.
- [104] Justin Moskolai Ngossaha, Raymond Houé Ngouna, Bernard Archimède, and Marcel Fouda Ndjodo. A simulation model for risk assessment in a smart mobility ecosystem based on the inoperability input-output theory. In *Proceedings of the 50th Computer Simulation Conference*, page 31. Society for Computer Simulation International, 2018.
- [105] Mohammed Saeed Al-Kahtani. Survey on security attacks in vehicular ad hoc networks (vanets). In *2012 6th International Conference on Signal Processing and Communication Systems*, pages 1–9. IEEE, 2012.
- [106] Hong Zhong, Jingyue Ni, Jie Cui, Jing Zhang, and Lu Liu. Personalized location privacy protection based on vehicle movement regularity in vehicular networks. *IEEE Systems Journal*, 2021.
- [107] Ahmad Ali, Yu Ming, Sagnik Chakraborty, and Saima Iram. A comprehensive survey on real-time applications of wsn. *Future internet*, 9(4):77, 2017.
- [108] George P Corser, Huirong Fu, and Abdelnasser Banihani. Evaluating location privacy in vehicular communications and applications. *IEEE transactions on intelligent transportation systems*, 17(9):2658–2667, 2016.
- [109] Jonathan Petit, Florian Schaub, Michael Feiri, and Frank Kargl. Pseudonym schemes in vehicular networks: A survey. *IEEE communications surveys & tutorials*, 17(1):228–255, 2014.
- [110] Abdelwahab Boualouache, Sidi-Mohammed Senouci, and Samira Moussaoui. A survey on pseudonym changing strategies for vehicular ad-hoc networks. *IEEE Communications Surveys & Tutorials*, 20(1):770–790, 2017.
- [111] Messaoud Babaghayou, Nabila Labraoui, Mohamed Amine Ferrag, and Leandros Maglaras. Between location protection and overthrowing: A contrariness framework study for smart vehicles. IEEE, 2020.
- [112] Aashma Uprety, Danda B Rawat, and Jiang Li. Privacy preserving misbehavior detection in iov using federated machine learning. In *2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC)*, pages 1–6. IEEE, 2021.
- [113] Mamata Rath. Big data and iot-allied challenges associated with healthcare applications in smart and automated systems. *International Journal of Strategic Information Technology and Applications (IJSITA)*, 9(2):18–34, 2018.

-
- [114] Björn Wiedersheim, Zhendong Ma, Frank Kargl, and Panos Papadimitratos. Privacy in inter-vehicular networks: Why simple pseudonym change is not enough. In *2010 Seventh International Conference on Wireless On-demand Network Systems and Services (WONS)*, pages 176–183. IEEE, 2010.
- [115] Karim Emara, Wolfgang Woerndl, and Johann Schlichter. Context-based pseudonym changing scheme for vehicular adhoc networks. *arXiv preprint arXiv:1607.07656*, 2016.
- [116] Andreas Tomandl, Florian Scheuer, and Hannes Federrath. Simulation-based evaluation of techniques for privacy protection in vanets. In *2012 IEEE 8th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pages 165–172. IEEE, 2012.
- [117] Ikram Ullah, Abdul Wahid, Munam Ali Shah, and Abdul Waheed. Vbpc: Velocity based pseudonym changing strategy to protect location privacy of vehicles in vanet. In *2017 International Conference on Communication Technologies (ComTech)*, pages 132–137. IEEE, 2017.
- [118] Christoph Sommer, Reinhard German, and Falko Dressler. Bidirectionally coupled network and road traffic simulation for improved ivc analysis. *IEEE Transactions on mobile computing*, 10(1):3–15, 2011.
- [119] OpenStreetMap contributors. Planet dump retrieved from <https://planet.osm.org> . <https://www.openstreetmap.org>. Accessed: 2021-04-12.
- [120] Daniel Krajzewicz, Jakob Erdmann, Michael Behrisch, and Laura Bieker. Recent development and applications of SUMO - Simulation of Urban MObility. *International Journal On Advances in Systems and Measurements*, 5(3&4):128–138, December 2012. URL <http://elib.dlr.de/80483/>.
- [121] András Varga and Rudolf Hornig. An overview of the omnet++ simulation environment. In *Proceedings of the 1st international conference on Simulation tools and techniques for communications, networks and systems & workshops*, page 60. ICST, 2008.
- [122] Karim Emara. Poster: Prext: privacy extension for veins vanet simulator. In *2016 IEEE Vehicular Networking Conference (VNC)*, pages 1–2. IEEE, 2016.
- [123] Giancarlo Fortino, Claudio Savaglio, Giandomenico Spezzano, and MengChu Zhou. Internet of things as system of systems: A review of methodologies, frameworks, platforms, and tools. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2020.
- [124] Nacera Bahnes, Bouabdellah Kechar, and Hafid Haffaf. Cooperation between intelligent autonomous vehicles to enhance container terminal operations. *Journal of Innovation in Digital Ecosystems*, 3(1):22–29, 2016.
- [125] Minglong Zhang, GG Md Nawaz Ali, Peter Han Joo Chong, Boon-Chong Seet, and Arun

- Kumar. A novel hybrid mac protocol for basic safety message broadcasting in vehicular networks. *IEEE Transactions on Intelligent Transportation Systems*, 21(10):4269–4282, 2019.
- [126] Rongxing Lu, Xiaodong Lin, Haojin Zhu, P-H Ho, and Xuemin Shen. Ecpp: Efficient conditional privacy preservation protocol for secure vehicular communications. In *IEEE INFOCOM 2008-The 27th Conference on Computer Communications*, pages 1229–1237. IEEE, 2008.
- [127] Messaoud Babaghayou, Nabila Labraoui, Ado Adamou Abba Ari, and Abdelhak Mourad Gueroui. Transmission range changing effects on location privacy-preserving schemes in the internet of vehicles. *International Journal of Strategic Information Technology and Applications (IJSITA)*, 10(4):33–54, 2019.
- [128] Kai Lin, Chensi Li, Yihui Li, Claudio Savaglio, and Giancarlo Fortino. Distributed learning for vehicle routing decision in software defined internet of vehicles. *IEEE Transactions on Intelligent Transportation Systems*, 2020.
- [129] Leandros A Maglaras, Ali H Al-Bayatti, Ying He, Isabel Wagner, and Helge Janicke. Social internet of vehicles for smart cities. *Journal of Sensor and Actuator Networks*, 5(1):3, 2016.
- [130] Michael E Nowatkowski, Jennie E Wolfgang, Chris McManus, and Henry L Owen. The effects of limited lifetime pseudonyms on certificate revocation list size in vanets. In *Proceedings of the IEEE SoutheastCon 2010 (SoutheastCon)*, pages 380–383. IEEE, 2010.
- [131] Siham Bouchelaghem and Mawloud Omar. Secure and efficient pseudonymization for privacy-preserving vehicular communications in smart cities. *Computers & Electrical Engineering*, 82:106557, 2020.
- [132] S. E. Merzougui, M. A. Ferrag, O. Friha, and L. Maglaras. Easbf: An efficient authentication scheme over blockchain for fog computing-enabled internet of vehicles. *Journal of Information Security and Applications*, 2021.
- [133] Ferheen Ayaz, Zhengguo Sheng, Daxin Tian, and Victor CM Leung. Blockchain-enabled security and privacy for internet-of-vehicles. In *Internet of Vehicles and its Applications in Autonomous Driving*, pages 123–148. Springer, 2021.
- [134] Christos Tselikis, Christos Douligeris, Leandros Maglaras, and Sarandis Mitropoulos. On the conference key distribution system with user anonymity. *Journal of Information Security and Applications*, 54:102556, 2020.
- [135] Dimitrios Kosmanos, Antonios Argyriou, and Leandros Maglaras. Estimating the relative speed of rf jammers in vanets. *Security and Communication Networks*, 2019, 2019.
- [136] Xiaolong Xu, Yuan Xue, Lianyong Qi, Yuan Yuan, Xuyun Zhang, Tariq Umer, and Shaohua Wan. An edge computing-enabled computation offloading method with privacy preservation for internet of connected vehicles. *Future Generation Computer Systems*, 96:89–100, 2019.

- [137] Meiyu Pang, Li Wang, and Ningsheng Fang. A collaborative scheduling strategy for iov computing resources considering location privacy protection in mobile edge computing environment. *Journal of Cloud Computing*, 9(1):1–17, 2020.

Abstract

This thesis deals with the problem of identity and location privacy in the context of Internet of Vehicles (IoV) while making road-safety into consideration. This problematic emerged with the advent of different safety-achieving techniques provided by IoV applications. There exist many techniques that cope with the identity and location privacy problem but while sacrificing safety. In our thesis, we focus on the solutions that are based on the pseudonymity concept and many techniques related to this category were proposed. With this said, we provide a comprehensive survey that deals with the aforementioned problem. then, we propose three techniques that ensure high level of location privacy while considering road-safety as an objective. The obtained results show that road-safety can still be achieved in conjunction with location privacy while using our techniques.

keywords: IoV, VANET, identity and location privacy, road-safety, location tracking, pseudonym changing, silent period, transmission range changing techniques.

Résumé

Cette thèse traite le problème de la préservation de la vie privée de l'identité et de l'emplacement dans le contexte de l'Internet des véhicules (IoV) tout en prenant en compte la sécurité routière. Cette problématique est apparue avec l'avènement de différentes techniques de sécurité fournies par les applications IoV. Il existe de nombreuses techniques qui permettent de résoudre le problème de la confidentialité de l'identité et de l'emplacement, mais tout en sacrifiant la sécurité. Dans notre thèse, nous nous concentrons sur les solutions basées sur le concept de pseudonymat et de nombreuses techniques liées à cette catégorie ont été proposées. Cela dit, nous fournissons un état de l'art complet qui traite du problème susmentionné. Ensuite, nous proposons trois techniques qui garantissent un haut niveau de confidentialité de l'emplacement tout en considérant la sécurité routière comme un objectif. Les résultats obtenus montrent que la sécurité routière peut encore être obtenue en conjonction avec la confidentialité de l'emplacement tout en utilisant nos techniques.

mots-clés: IoV, VANET, confidentialité de l'identité et de l'emplacement, sécurité routière, suivi de l'emplacement, changement de pseudonyme, période de silence, techniques de changement de portée de transmission.

مُلخَص

تتناول هذه الأطروحة مشكلة المحافظة على خصوصية الهوية و الموقع في سياق إنترنت المركبات (IoV) مع إعطاء سلامة الطريق اعتباراً مهماً. ظهرت هذه المشكلة مع ظهور مختلف التقنيات المستعملة لتحقيق سلامة الطريق و التي توفرها تطبيقات IoV. توجد العديد من التقنيات التي تتعامل مع مشكلة خصوصية الهوية و الموقع ولكن مع التضحية بالسلامة. في أطروحتنا، نركز على الحلول التي تستند إلى مفهوم الاسم المستعار وتم اقتراح العديد من التقنيات المتعلقة بهذه الفئة. بناءً على هذا، نقدم مسجاً شاملاً، في شكل دراسة حالة، يتعامل مع المشكلة المذكورة أعلاه. بعد ذلك، نقترح ثلاث طرق تضمن مستوى عالٍ من خصوصية الموقع مع مراعاة سلامة الطريق كهدف. أظهرت النتائج التي تم الحصول عليها أنه لا يزال من الممكن تحقيق سلامة الطريق جنباً إلى جنب مع خصوصية الموقع أثناء استخدام تقنياتنا.

الكلمات المفتاحية: إنترنت المركبات (IoV)، شبكة العربات المخصصة (VANET)، خصوصية الهوية و الموقع، سلامة الطريق، تتبع الموقع، تغيير الاسم المستعار، الفترة الصامتة، تقنيات تعديل نطاق الإرسال.