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 و البحث 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:

- aaa.

- bbb.

- ccc.

– *Full Name*

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.

– *Full Name*

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. بناءًا على هذا، نقدم مسحًا 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 المفتاحيّة: إنترنت المركبات (IoV) ، شبكة العربات المخصّصة (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) aaa

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) bbb

Full-Name: Contacts & Works

Full-Name@hotmail.com

Full-Name@univ.dz

www.researchgate.net/profile/Full-Name

sites.google.com/view/Full-Name

orcid.org/0000-0000-0000-0000

Google Scholar — June 2021

Messaoud Babaghayou

FOLLOW

GET MY OWN PROFILE

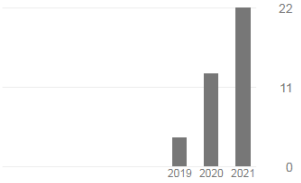
PhD student in vehicular ad-hoc networks security, Tlemcen University
Verified email at univ-tlemcen.dz - Homepage

identity and location privacy pseudonym change security in IoVs

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

Cited by

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



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, Habili...
- Leandros Maglaras — Associate Professor / Reader in ...
- Mehmet Akif Yazıcı — Istanbul Technical University, Inf...
- Abdelhak Mourad GUEROUI — Maître de Conférences, Universit...
- Nasreddine Lagraa — University of Laghouat
- Helge Janicke — Cyber Security Cooperative Res...

Table of Contents

List of Figures

List of Tables

List of Algorithms

Preamble

1 General Introduction

As the world is proceeding...

2 Motivation

With the exponential growth (like WAYMO [1])...

3 Problematic in a nutshell overall

The integration of semi-autonomous vehicles...

[1] https://waymo.com/

4 Objectives & Contributions

While all of the industry...

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

- 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)

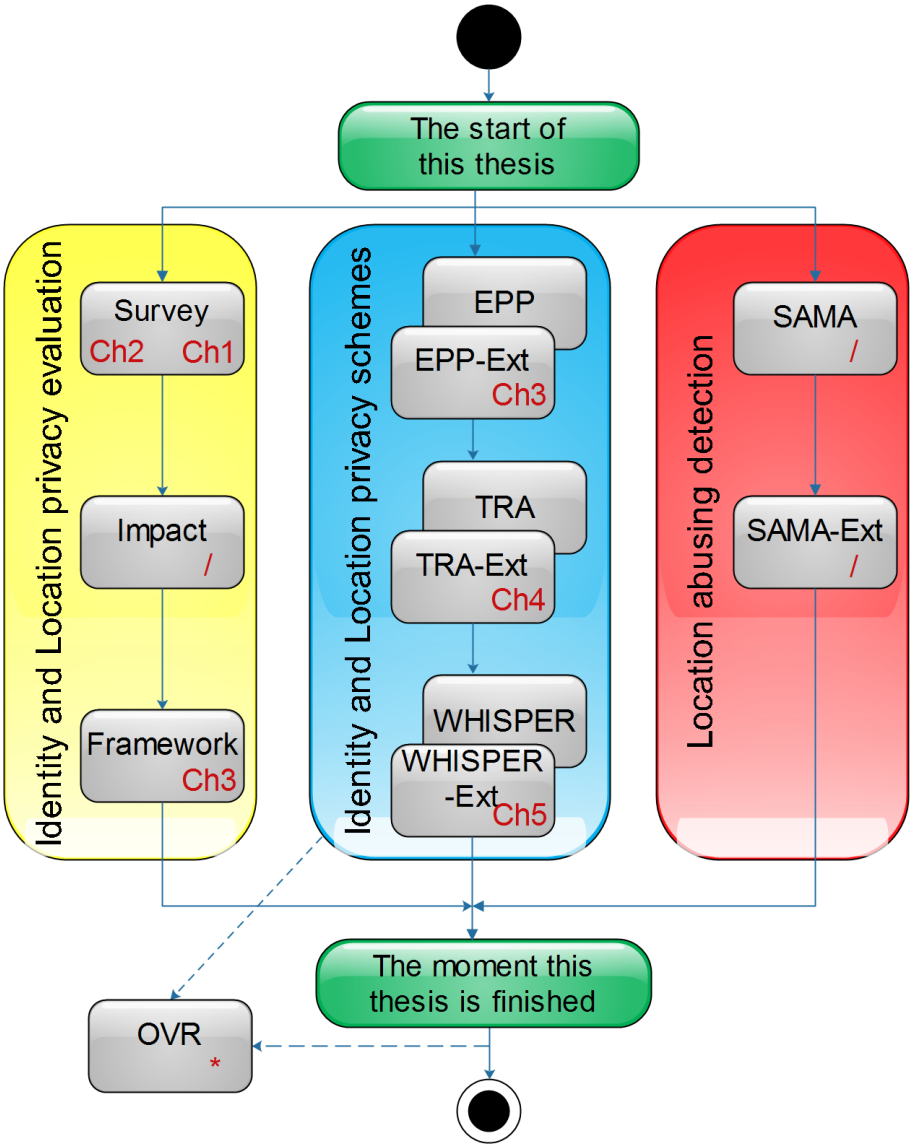


Figure 1: The diagram of this thesis' phases and chronology

- 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]...

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 [2]...

The yearly damages caused by vehicular accidents (which is 1.3 million deaths with $518 billion costs in the globe [3]) 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 [4]. Moreover, the unique nature of ad-hoc networks which allows the fast spread of information let VANET, that is extended from MANET [5], be considered as an appropriate wireless network that is used to solve the previous problems [6]. Figure 2...

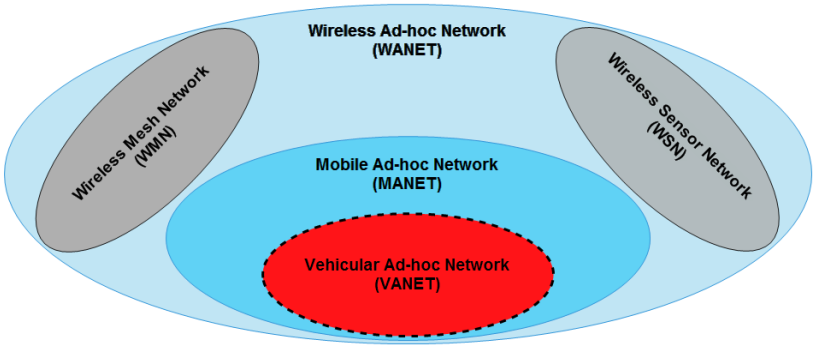


Figure 2: VANET and its relation with other networks

In the components other than vehicles we may find:

B) Cell phones (sometimes referred to pedestrians)

C) Unmanned Air Vehicle (UAV) [7, 8], a drone/Flying Ad-Hoc Network (FANET) system that may assiste the VANET system

D) Roadside Units (RSUs), which are devices fixed right in the roadside

F) Cell towers (3/4/5/6G [9, 10] technologies provided to VANETs)

G) Different kinds of servers (location, authentication, application servers) [11]

3 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.

1.1 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 [12] and the studies of some other strategies and our own observations, we present a comparative table (Table 1) 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).

Table 1: 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 [13]	2005	Protocol	✓	✗	Low	B	✓	✓
Swing & Swap [14]	2006	Protocol	✓	✓	High	B	✗	✗
CMIX [15]	2007	Infrastructure	✗	✓	High	S	✓	✗
Mix-Context [16]	2007	Protocol	✗	✗	Low	S	✓	✗
SLOW [17]	2009	Protocol	✓	✗	Low	S	✓	✗
DLP [18]	2010	Protocol	✗	✗	Low	A	✓	✗
REP [19]	2010	Protocol	✗	✓	High	S	✓	✗
SlotSwap [20]	2011	GPS	✗	✗	High	S	✗	✗
SPCP [21]	2011	Protocol	✗	✗	High	S	✓	✗
SocialSpots [22]	2012	Infrastructure	✗	✗	Low	B	✓	✗
CPN [23]	2013	Protocol	✗	✗	Low	B	✓	✗
DMLP [24]	2013	Protocol	✗	✓	High	S	✓	✗
EPZ [25]	2013	Protocol	✓	✗	Low	S	✗	✓
MixGroup [26]	2016	Protocol	✗	✗	High	S	✓	✗
MMLPP [27]	2018	Protocol	✗	✗	High	S	✓	✓
nO-TS-PP [6]	2018	GPS	✗	✗	Low	S	✓	✗
ENeP-AB [28]	2018	Protocol	✗	✗	Low	S	✓	✗
CPS [29]	2019	Infrastructure	✓	✗	Low	B	✓	✗
WHISPER [30]	2021	GPS	✗	✗	Low	S	✓	✗

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.

1.1 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:

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

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

$$S_{in(i)} = \{v_j \in S_{sim(i)} : State[v_j] = "Inside"\} \tag{2}$$

The set of VSN users who quitted the district:

$$S_{out(i)} = S_{sim(i)} - S_{in(i)} \tag{3}$$

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

$$S_{Clearly\_out(i)} = \{v_j \in S_{out(i)} : Class[v_j] = "Y"\} \tag{4}$$

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:

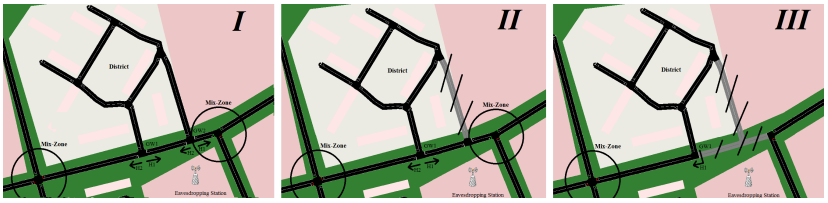
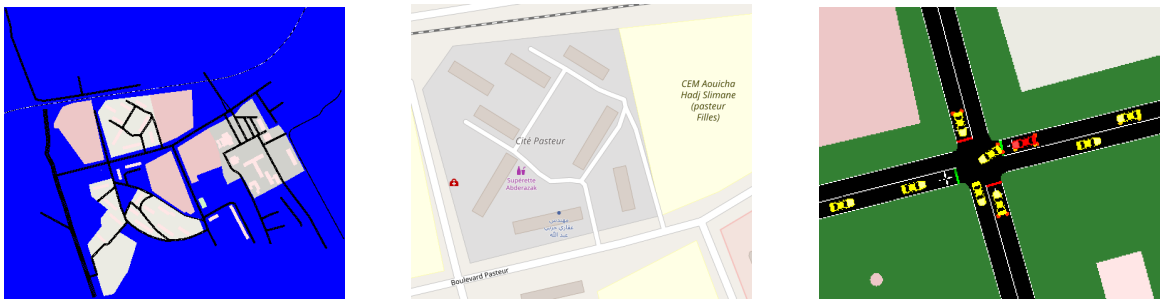


Figure 3: The three scenarios: I, II and III



(a) The general map (b) The original district (c) A mix-zone

Figure 4: Additional illustrations about the map

Firstly the probability of being inside the district:

$$P_{inside}(v_i) = \begin{cases} 0 & IF(Class[v_i] = "Y")AND(State[V_i] = "Outside") \\ \frac{|S_{sim(i)}|-|S_{out(i)}|}{|S_{sim(i)}|-|S_{Clearly\_out(i)}|} & Else \end{cases} \tag{5}$$

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

$$P_{outside}(v_i) = 1 - P_{inside}(v_i) \tag{6}$$

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.

1.1 Pseudo-Algorithm of TRA

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

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
```

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

Table 2: 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 [17]	✓	✗	Low	✗	Driving in low speeds, hence, keeping silence
RSP [31]	✓	✗	Low	✗	Entering silence and changing pseudonyms synchronously
CPN [23]	✗	✓	Very high	✓	The set of vehicles happens to be large
WHISPER [30]	✗	✓	Medium	✓	Low transmission power condition is satisfied

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 [23], RSP [31] and SLOW [17]. 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.

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...

Appendices

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

sensors

MDPI

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 benignant 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

check for updates

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.

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).

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**

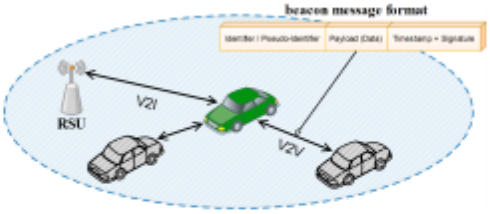


Fig. 1: The different communications and beacon message format in IoV

I. Introduction

Internet of Vehicles (IoV) is emerging as a promising paradigm in intelligent transportation systems (ITS) to enhance the existing capabilities of vehiclar 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 recommanded to be from 1 to 10 times per second 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

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] David Tse and Pramod Viswanath. *Fundamentals of wireless communication*. Cambridge university press, 2005.

[3] Road Crash Statistics. https://www.asirt.org/safe-travel/road-safety-facts/. Accessed: 2021-04-12.

[4] Albert Wasef. Managing and complementing public key infrastructure for securing vehicular ad hoc networks. 2011.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] Albert Wasef and Xuemin Sherman Shen. REP: Location privacy for VANETs using random encryption periods. *Mobile Networks and Applications*, 15(1):172–185, 2010.

[20] 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.

[21] 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.

[22] 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.

[23] 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.

[24] 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.

[25] 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.

[26] 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.

[27] 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.

[28] 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.

[29] 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.

[30] 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.

[31] 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.

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. بناءًا على هذا، نقدم مسحًا 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 المفتاحيّة: إنترنت المركبات (IoV) ، شبكة العربات المخصّصة (VANET) ، خصوصية الهوية و الموقع، سلامة الطريق، تتبع الموقع، تغيير الاسم المستعار، الفترة الصامتة، تقنيات تعديل نطاق الإرسال.