People's Democratic Republic of Algeria
Ministery of Higher Education and Scientific Research
Mohamed El Bachir El Ibrahimi University of Borj Bou Arréridj
Faculty of Mathematics and Informatics
Informatics Department

DISSERTATION

Presented in fulfilment of the requirements of obtaining the degree

Master in a computer system

Specialty: Networks and multimedia

THESIS

Security and Privacy in VANETs
Implementation of TRA protocol on OMNET++

Presented by:
AYAD Khaoula
GASMI Balkis

Publicly defended on: 29/06 /2022
In front of the jury composed of:
President: BEMESSAHEL Ilyes
Examiner: KHELIFI Hakima
Supervisor: MOUSSAOUI Boubakeur

2021-2022

ACKNOWLEDGMENTS

First and foremost, thank ALLAH, who gave us the strength and the Patience to accomplish this modest work.

We want to thank our supervisor Mr. **MOUSSAOUI Boubakeur** for his continuous and unlimited support, feedback, and adjustment of the research. Secondly, we would like to thank all teachers for their help and support during our studies.

A massive thanks to our parents who followed us during our studies.

Dedication

Special thanks to my parents:

The reason for what I have become today is my father (Kamel) and my Mother (Amel Naili)

I am grateful to both of you. You have been my inspiration and my soul mates.

To my brother and sister:

Thanks for your great support and continuous care.

To Karim and Khaoula:

Whose affection, love, and encouragement make me able to get such success and honor you for being in my life.

GASMI BALKIS

Dedication

I dedicate my master's thesis to:

My Dear mother (بولخصايم رفيقة), my father (عمار),

My brothers (Bilal, Nassim, Ahmed, and Mohammed)

And my sister (amal and her daughter yakin), my dear

My husband (Oussama), and my friend and partner in this

Work (Balkis) for the unlimited encouragement and

Support during my master's study.

AYAD KHAOULA

Abstract

Vehicular Ad-hoc Networks (VANETs) promise to ensure road safety and passenger comfort. However, this technology suffers from serious problems of security, mainly location privacy or vehicle tracking issues.

Pseudonym-changing strategies are the most recent proposed. A global adversary can predict and link various pseudonyms used by a vehicle, so it can easily track the driver or the vehicle. In this work, we present a state of the art of research solution in this field then we implement and simulate the protocol Transmission Range Adjustment (TRA) on OMNET ++.

Keywords

TRA, Vehicle Network, pseudonym change, Location privacy, the threat of tracking.

الملخص

تعد شبكات المركبات المخصصة (VANETs) بضمان السلامة على الطرق وراحة الركاب. ومع ذلك، فإن هذه التكنولوجيا تعاني من مشكلات أمنية خطيرة، لا سيما خصوصية الموقع أو مشكلات تتبع المركبات.

استراتيجيات تغيير الاسم المستعار هي الأحدث المقترحة. يمكن للعدو العالمي أن يتنبأ بالعديد من الأسماء المستعارة التي تستخدمها السيارة ويربطها، بحيث يمكنه بسهولة تتبع السائق أو السيارة. في هذا العمل، نقدم حالة من فن البحث عن حل في هذا المجال ثم نقوم بتنفيذ ومحاكاة بروتوكول ضبط نطاق الإرسال (TRA) على OMNET ++.

الكلمات المفتاحية:

ضبط نطاق الإرسال، شبكة المركبات، تغيير الاسم المستعار، خصوصية الموقع، تهديد التتبع.

Résumé

Les réseaux véhiculaires ad hoc (VANET) promettent d'assurer la sécurité routière et le confort des passagers. Cependant, cette technologie souffre de graves problèmes de sécurité, principalement des problèmes de confidentialité de la localisation ou de suivi des véhicules.

Les stratégies de changement de pseudonyme sont les plus récentes proposées. Un adversaire mondial peut prédire et relier divers pseudonymes utilisés par un véhicule, de sorte qu'il peut facilement suivre le conducteur ou le véhicule. Dans ce travail, nous présentons un état de l'art de la recherche de solution dans ce domaine puis nous implémentons et simulons le protocole Transmission Range Adjustment (TRA) sur OMNET++.

Mots clés :

TRA, Vehicle Network, changement de pseudonyme, confidentialité de l'emplacement, menace de suivi.

Table des matières

List of Tables

List of figures

List of acronyms

VANET: Vehicular Ad hoc Network

MANET Mobile Ad hoc Network

TA: Trusted authority

OBU: On-Board Unit

RSU: Road Side Unit

GPS: Global Positioning System

V2V: Vehicle to Vehicle

V2I: Vehicle to Infrastructure

DSRC: Dedicated Short Range Communication

IEEE: Institute of Electrical and Electronics Engineers

BSM: Basic Safety Message (aka beacon message)

SRT: Short time pseudonyms

DoS: Denial of Service

SUMO: Simulation of Urban Mobility (traffic simulator)

OMNET++: Objective Modular Network Testbed in C++

VEINS: Vehicular network simulation

SLOW: context-based privacy scheme

TRA: Transmission Range Adjustment

PeriodicalPC: Periodical Pseudonym Change

RSP: random silent period

CSP: Coordinated-Silent-Period

CPN: Cooperative Pseudonym change scheme based on the number of Neighbors

CAPS: Context-aware Privacy Scheme

ENEP-AB: Estimation of Neighbors Position privacy scheme with an Adaptive Beaconing

General introduction

About 1.25 million people die annually from traffic accidents, mainly in low- and middle-income countries. 90% of deaths are caused by traffic accidents worldwide, with an additional 1,816 deaths recorded on May 22, 2022, which is more than 9% compared to the same period in 2021.

Vehicular Ad-hoc Network (VANET) is a promised solution that aims to enhance traffic safety, reduce traffic accidents and contribute to maintaining road safety. Communicating nodes are either intelligent vehicles equipped with onboard units (processor, memory, GPS, transmitter/receiver, etc.) or fixed units placed on the side of the roads called Road Side Units (RSU). A vehicle communicates with another vehicle or an RSU. It uses the Vehicle to Vehicle (V2V) or Vehicle to Infrastructure (V2I) communication mode, respectively. During these communications, vehicles broadcast a highly sensitive range of information, such as location, speed, and direction. The latter is a loophole that allows the driver's privacy to be violated.

In this work, we have implemented and simulated Transmission Range Adjustment (TRA) protocol on the OMNET ++ simulator. Some comparisons of our results are made with other existing protocols of the PREXT module.

This thesis is organized into four chapters. In the first chapter, we define VANET, and in the second chapter, we present challenges of privacy and security issues in VANET networks. The third chapter discusses the most important schemes proposed to preserve privacy and the most important articles and previous works that we relied on in our study. In the last chapter, we explained everything we did from the first to the research results.

Chapter 01:

Vehicular Ad-Hoc Networks

I - Introduction

The VANET has been created mainly to reduce accidents and deaths in general, and this has already been achieved by allowing communication Between Vehicles (V2V) and Vehicle to Infrastructure (V2I) via Dedicated Short Range Communication protocol (DSRC) and sending beacons that contain vehicle status (location, speed, time, etc.) periodically through the router called Basic Safety Message (BSM).in this chapter we will talk about everything related to VANET.

II - Vehicular networks

VANETs (Vehicle Ad Hoc Networks) is a new emerging technology for Mobile Ad Hoc Networks (MANETs), where Smartphones, computers, radars, geolocation systems (GPS), and various types of sensors network engineers. VANET networks enable communication between vehicles (V2V) and Infrastructure (V2I). Different nodes can or information to improve road traffic safety [1].

III - VANETs component

A VANETs network consists mainly of three entities [2]:

1 - On-board unit (OBU)

It is a vehicle's radio device that broadcasts and receives beacons to other OBUs or RSUs on the VANET System. Their roles are to locate, receive, calculate, store and send data on the network. These are transceivers that ensure the connection of the vehicle to the network.

Road-side unit (RSU)

RSU is located along the road as a router between vehicles and is considered part of the network infrastructure. Their primary responsibility is to support the TA in traffic and vehicle management. They represent access points to the network and various traffic information.

Trusted authority (TA)

It is a source of the authenticity of the information. It ensures the management and registration of all entities on the network (RSU and OBU). MT should know all the true identities of vehicles and disclose them to law enforcement if necessary. Also, in some work, MT is responsible for issuing and awarding certificates and pseudonyms for communications [3].

IV - Communication Modes

There are two types of communication in the VANET:

1-1- Vehicle to vehicle (V2V)

V2V is direct communication between vehicles. Each vehicle represents a node and establishes the communication using its OBU. This communication did not require any infrastructure and was used to broadcast information in the network or transport it from one node to another.

1-2- Vehicle to infrastructure (V2I)

Communication is performed between nodes (Vehicles using the OBU) and fixed entities (RSU and CA). These allow vehicles to access various applications (such as Security, comfort, and management) and information such as traffic status and weather. This mode of communication provides relatively strong connectivity compared to communication in the V2V (vehicle-to-vehicle) mode, ensuring better utilization of network resources. The figure below shows V2V and V2I communication modes.

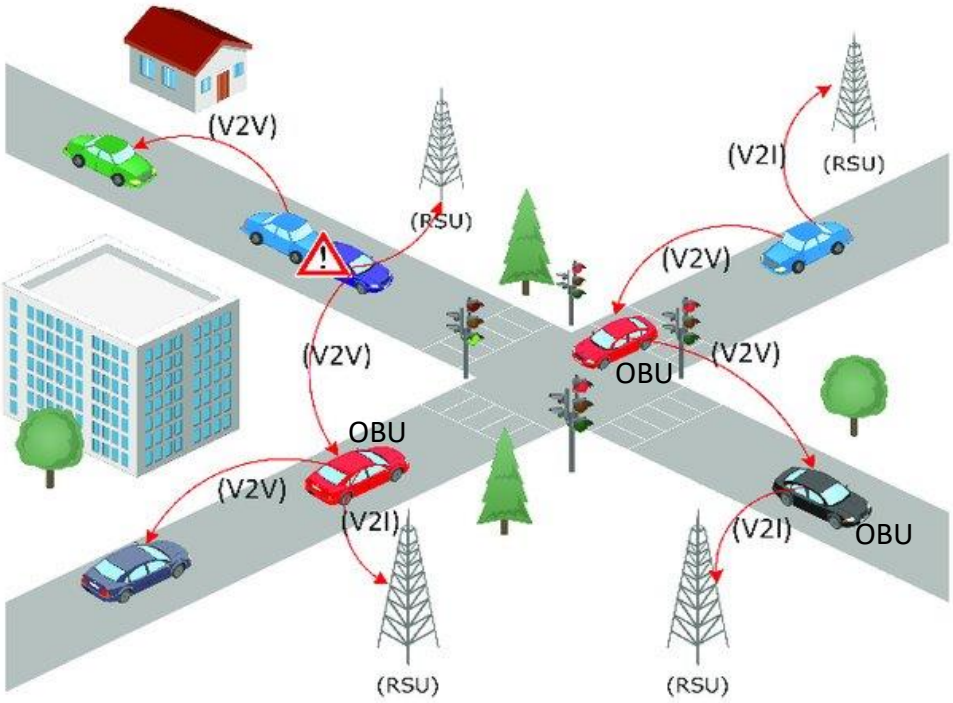

Figure 1.*VANET communication architecture.* [4]

V - Characteristics of VANETs

1 - Self-Organization

It allows a network to self-organize as a subclass of mobile Ad-Hoc does not need support from any centralized authority for self-organization.

Mobility

VANETs are mainly composed of fixed RSUs and moving vehicles. The vehicle's speed varies from very low to very high, leading to new communication challenges. Indeed, in areas of high traffic jams, vehicles are stopped or moving slowly, and therefore they have enough time to exchange messages. However, they face significant challenges due to vehicles' high density, such as data collision, channel fading, message dropping, and other interference problems. In areas of low traffic (e.g., highways), the vehicle speed is very high, leading to other communication challenges such as small communication windows (few seconds), link failures, and high end-to-end (ETE) delay.

2 - Movement Pattern

Node movement in VANETs differs from Mobile Ad-Hoc Networks (MANETs). In fact, in MANETs, mobile nodes are free to move anywhere. However, in VANET, vehicles follow the topology of road networks of the geographic areas where they drive. There are three situations: urban area, rural area, and highway. The urban area has a more complex road network, denser in terms of vehicles number than the rural area.

Furthermore, it contains more obstacles, traffic signals, and RSUs than rural areas and highways. In the latter, vehicles move in one direction over many lanes. The spatial attributes of the road network impact communication efficiency and effectiveness.

3 - Traffic density

It ranges from high to low density, depending on the geographic area (i.e., high traffic density in urban areas and low traffic density in rural areas and highways) and the time factor (i.e., low traffic density during off-peak hours and high traffic during rush hours). Traffic density raises crucial challenges related to the design of efficient VANET communication protocols. For instance, data dissemination protocols must deal with the network disconnection issue in rural areas with very low traffic density. However, advanced data dissemination

mechanisms should avoid the healthy-known broadcast storm issue in the case of very high traffic density, especially in an urban area during rush hours.

4 - Heterogeneity

VANET nodes have different characteristics and capabilities. For instance, vehicles are moving nodes with different communication ranges, sensing capabilities, and categories (i.e., private, authority, and maintenance vehicles). Whereas RSUs are stationary nodes placed in some suitable locations and equipped with exclusive Ad-Hoc features.

5 - Topology

As we know in MANET, the topology is dynamic, so even though the localization of the vehicles follows the layout of the streets, the roads, and the highways, it is somehow fixed. However, relatively high mobility leads to fast changes in network topology.

6 - Energy

The main issue is the battery, which powers the devices, consuming less energy while transmitting, listening, or processing the information. However, it is not an issue in VANET because the vehicle's battery is enough to transmit messages to other vehicles.

VI - VANET Applications

1 - Safety Applications

Safety applications aim to warn drivers at the right time about dangerous road situations to enhance driving safety. Some examples of safety use cases and their related requirements are introduced. In the following, we briefly describe the primary use cases.

1-1- Cooperative Forward Collision Warning

This use case aims to avoid rear-end collisions with other vehicles by assisting drivers. Rear-end collisions are generally caused by driver disturbance or sudden braking. To avoid a crash, vehicles share relevant information such as position, speed, and direction. When a critical situation (e.g., insufficient safety distance) is detected, the vehicle warns its driver.

1-2- Pre-Crash Sensing/Warning

Unlike the Cooperative Forward Collision Warning, this use case assumes that a crash is unavoidable and will take place.

1-3- Hazardous Location V2V Notification

This use case aims to share information about dangerous roadway locations, such as potholes, bottlenecks, and between vehicles in a particular area. To this end, the vehicle detecting a dangerous location uses the information to optimize its safety systems and then broadcasts it to neighboring vehicles in the surrounding area. Through V2V communications, the information is progressively shared with other concerned vehicles. Information about dangerous locations on the roadway can also be transmitted from external service providers to us, sending it to some vehicles in their communication ranges. After that, vehicles receiving the information can disseminate it to others via V2V communications.

2 - Traffic efficiency applications

Traffic efficiency applications aim to enhance the efficiency of transportation systems by providing traffic-related information to drivers or road operators. In order to achieve this goal, traffic information should be exchanged through the VANET. Therefore, road users and road operators will benefit from shorter travel times and reduced construction and maintenance costs. We briefly describe some traffic efficiency use cases introduced in the CAR-2-CAR Communication Consortium. Enhanced Route Guidance and Navigation: it enables the infrastructure owner to collect traffic data of a large region to predict traffic congestion on roadways. Predicted information will then be transmitted to vehicles via RSUs. Hence, the driver will be notified about the current and the expected traffic throughout the region, expected delays in reaching his destination, and better routes to avoid congested roads. This will undoubtedly lead to improving the overall efficiency of the transportation system.

2-1- Green Light Optimal Speed Advisory

It provides information related to the location of a signalized intersection and the signal timing (i.e., time to switch the light signal) to vehicles approaching the intersection, contributing to smoother driving and avoiding stopping. Receiving such information right, the vehicle can calculate the optimal speed to reach the intersection when the traffic signal is green. Therefore the driver will not have to decrease the vehicle's speed or stop. This will probably bring about a significant increase in the traffic flow and fuel economy.

2-2- Infotainment and others

Non-safety or traffic efficiency use cases are classified in this category. Some of these use cases provide entertainment or information regularly to drivers. Other ones are transparent to the driver and play an essential role in improving the vehicle's functions.

Eventually, it allows drivers and passengers to access the Internet via the VANET. In this case, RSUs act as internet gateways.

2-3- Point of Interest Notification

It allows traders and advertisement companies to advertise their business promotions to nearby vehicles. To this end, an RSU broadcasts the advertisement information (e.g., location, hours of operation, and pricing) to the contacted vehicles. Each vehicle will filter the received advertisements concerning the driver profile and context then appropriate advertisements are presented to the driver.

VII - Conclusion

In this chapter, we first define the vehicular AD-HOC network and describe its architecture, component, characteristics, application, and communication mode.

We also have security and privacy, which are very important in VANET, but we will discuss them in the next chapter.

Chapter 02:

Security and privacy in Vehicle Ad-Hoc networks

I - Introduction

VANET can reduce traffic accidents by broadcasting the vehicle. It indeed solved the problem of safety, but it created another problem of privacy. If there was an attacker who had an eavesdropping station, he could reach the beacons and their content. Then he violated the privacy of the vehicle or presents, which made security challenges and a problem that must be solved in VANETs.

II - Definition of security

Security is the ability of a system to protect its objects against unauthorized use and modification. It aims to ensure confidentiality, integrity, and availability of services essentially [5].

III - Security Requirements

In order to achieve security and confidentiality, the basic principles must not be absent, which are crucial [6].

1 - Authentication

Authenticity makes it possible to link a message or data to its sender. It allows the various network entities to have confidence in the messages and the data broadcast. Authenticity is the only requirement that allows cooperation within the network without risk, identifying all participants and checking the authenticity of the messages exchanged [7].

2 - Integrity

Integrity protects messages and prevents attackers from altering or modifying them. The integrity service ensures that sent messages are received quickly, without duplication, insertion, modification, rearrangement, or repetition.

3 - Confidentiality

Ensures that only trusted authorities have access to real vehicle identities to preserve vehicle secrecy and provide anonymity to senders of messages exchanged in the network. The use of cryptography can ensure confidentiality.

4 - Availability

This security requirement is intended to ensure that all resources and services provided on the network are available to authorized network entities. (Vehicles should be usable even if the network is down its handle with urgent data).

5 - Non-repudiation

This security requirement makes it possible to identify, with certainty, each entity that broadcasts a message on the network and to trace the source of erroneous messages even after the attack has occurred. This prevents attackers from spreading false information in the network [8].

IV - Types of attacks

There are many types of attacks in a network, and each attack has a specific method and method of attack and affects differently from other attacks, among them the following:

1 - Direct attacks

The attacker addresses the victim directly.

2 - Indirect attacks

The attacker sends the attack packets to an intermediate system, passing the attack to the victim.

3 - External attacks

These are intentional breaches of the security of a system or an asset. They originate on external hosts and are committed by unauthorized external users of an organization.

4 - Insider attacks:

These are unauthorized actions originating from internal hosts and initiated by internal users of an organization who abuse their privilege. Internal attacks constitute a large part of the attacks committed. Internal users are familiar with the systems and have direct access.

5 - Passive attacks

These are harmless actions. No manifestation is observable in terms of change in the system's state or modification of the data. An attack is said to be passive when an unauthorized

individual obtains access to a resource without modifying its content. Passive attacks can be eavesdropping, or traffic analysis, sometimes called traffic flow analysis. These two passive attacks have the following characteristics [9].

5-1- Listening (eavesdropping)

The attacker listens to the transmissions to retrieve the content of the messages. For example, a person listens to the transmissions on a LAN network between two stations or listens to the transmissions between a wireless telephone and a base station. Figure 2 elucidates an eavesdropping attack.

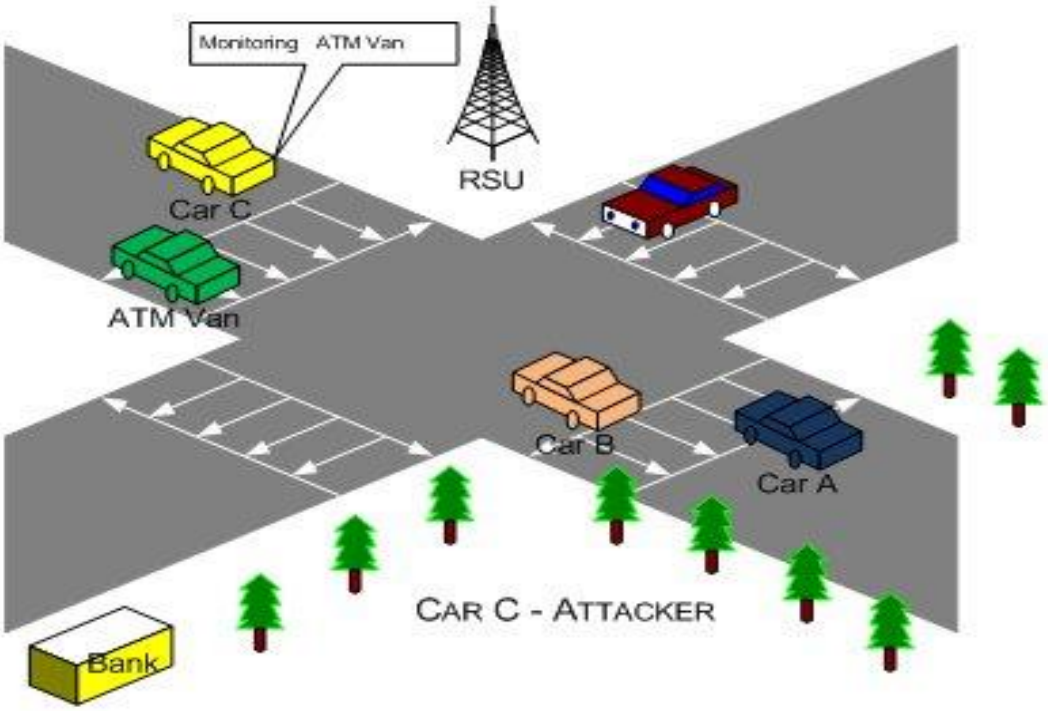

Figure 2 . *Eavesdropping Attack in VANET* [10]

5-2- Traffic analysis

The attacker obtains information by monitoring transmissions to detect common forms or patterns in communication. Much information is contained in the syntax of message streams transiting between communicating parties.

6 - Active attacks

These result in an illegal modification of the system's state, the disruption of its regular operation, or the alteration of data [9].

An active attack is when an unauthorized party changes messages, data streams, or files. Detecting this type of attack is possible. Active attacks can take the form of one of the following four types alone or in combination.

6-1- Masquerade

The attacker impersonates an authorized user and thus obtains certain access privileges.

6-2- Replay

The attacker monitors the transmissions (passive attack) and retransmits messages to a legitimate user.

6-3- Message modification

The attacker alters a legitimate message by deleting, modifying, or reordering content.

6-4- Denial of service

The attacker prevents or prohibits the regular use or the management of the means of communication. This last type of attack is a formidable threat to software security solutions since security is easily compromised in the event of malicious modification of the programs responsible for applying the protocols and control rules.

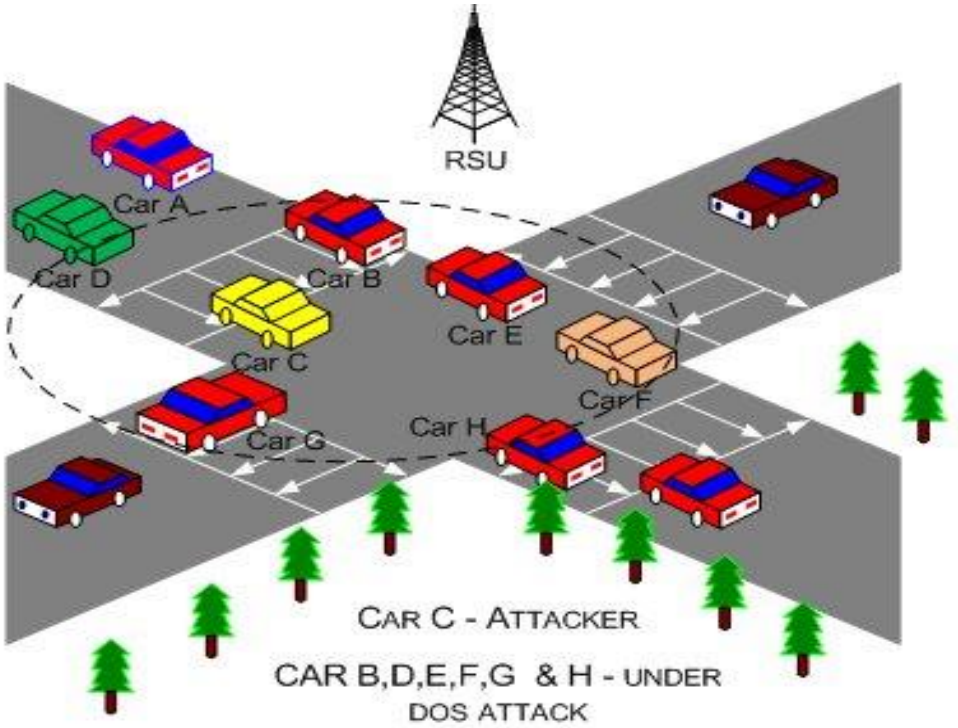

Figure 3 .*DoS Attack in VANET* [10]

V - Privacy definition

Privacy is an area of data protection that concerns the proper handling of sensitive data, including personal data and other confidential data, such as specific financial data and intellectual property data, to meet regulatory requirements and protect the confidentiality and immutability of the data.

1 - Privacy Requirements

During the communication in VANET, the attacker can steal the information and attack the system.

1-1- Identity privacy

The driver's personal information should be protected and highly secure during the message broadcast.

1-2- Unlinkability

Two messages in the same source or vehicle mean an adversary cannot sufficiently distinguish whether the Items of Interest used in vehicular networks are related or not. It is worth noting that the Unlinkability of the sender to a particular message can be termed anonymity, as this may breach the sender’s anonymity [11].

1-3- Confidentiality

This security service prevents the disclosure of message contents to unauthorized entities to maintain the user’s privacy.

1-4- Anonymity

The sender of a message must be indistinguishable or anonymous among a group of senders. In order to preserve the privacy of senders, VANET needs to provide anonymity to senders/accountability states that authorities must be able to determine the origin of any message sent anonymously to achieve security and privacy requirements.

1-5- Scalability

Scalability is a highly vital factor. A vehicle should promptly authenticate incoming messages, even in a high-density area. Moreover, a scheme that is not scalable is vulnerable to denial-of-service (DoS) attacks. Otherwise, some messages will be dropped before being verified if the security scheme is not efficient in high-density areas.

VI - Security mechanisms

After studying security and privacy requirements, we see a few Methods used to ensure secrecy and privacy in the network. Among them:

1 - Cryptography

Cryptography is the technology used to protect transmitted data containing various communications messages. Cryptography uses mainly keys and secret codes to encrypt (encode) the content of a message using an encryption algorithm to make it unreadable and therefore unusable by malicious entities. To make an encrypted message readable, the recipient entities have a key (code) and decryption algorithms appropriate to decrypt the message and make its content readable and usable. It exists two types of cryptography:

1-1- Symmetric Cryptography

A Message Authentication Code (MAC) is used for message authentication in symmetric schemes. The sender hashes the message and a secret key. Any receiver must know the secret key to verify the MAC by performing the same operation on the message. Thus, any node with knowledge of the secret key can generate valid MACs, but the sender accountability is not provided. The main benefits of this approach are the fast encryption and decryption times and less security overhead. In addition, the key distribution mechanism could be more straightforward and cost less than the deployment and maintenance of a PKI scheme. However, a reliable symmetric scheme requires that exposure of single or some secret keys should not compromise the authentication of all vehicles [12].

2 - The hash Function

The hash determines fixed and reduced size information called "the fingerprint or the digest" from a string of data provided as input of different length sizes. One-way hash functions are the most common. The particularity of this function is that it is straightforward to calculate and extract a hash from any given string but very difficult, if not impossible, to find the initial string from the hash. It is a function that is irreversible.

3 - Digital signature

A *digital signature* verifies that a particular digital document, message, or transaction is authentic. It provides a receiver the guarantee that the message was generated by the sender and

was not modified by a third party. The digital signatures rely on asymmetric key cryptography to ensure messages' authenticity, integrity, and non-repudiation.

4 - Digital Certificates

There are certificates among the results of cryptographic algorithms, which allow increasing the degree of security in VANET networks. Each vehicle has a single long-term certificate containing the identity and vehicle characteristics. It is mainly responsible for renewing short-term certificates. Thus, the vehicle has several short-term certificates, which contain a virtual identifier and communication pseudonyms. The certificates must allow the preservation of the privacy and anonymity of the vehicle.

VII - Conclusion

In this chapter, we discussed security and privacy, and we mentioned their requirement, the different types of attacks, and the mechanism that allows us to avoid them.

Chapter 03:

Pseudonym changing strategies & Related works

I - Introduction

Pseudonyms are vehicle identification units (nicknames). They are used to improve the location privacy in VANET, the Pseudonyms stored in the OBU. If the vehicle asks for a pseudonym, it will send a request to the nearby RSU for short time Pseudonyms (STP). It is necessary to change Pseudonyms frequently to prevent the attacker from linking the location up data of a moving vehicle.

The Pseudonyms must be unique and do not contain any personal information related to the vehicle's characteristics.

In this chapter, we will talk about the most prominent of what we read about privacy strategies and protocols and the security challenges faced by VANET developed by some researchers.

So we will give an overview of some research and explain the most important protocols in this field. Each of them depends on a different context.

II - Pseudonyms Linking Attack

There are two types of attacks of linking of pseudonyms developed by L.Buttyan and some authors in 2009 [13] [14], which are represented in:

1 - Syntactic linking

The figure below represents the syntactic linking of pseudonyms. If during Δt only one vehicle (B) changes its pseudonym (from B1 to B2) among three vehicles running on the road, the adversary can then easily link the pseudonyms B1 and B2.

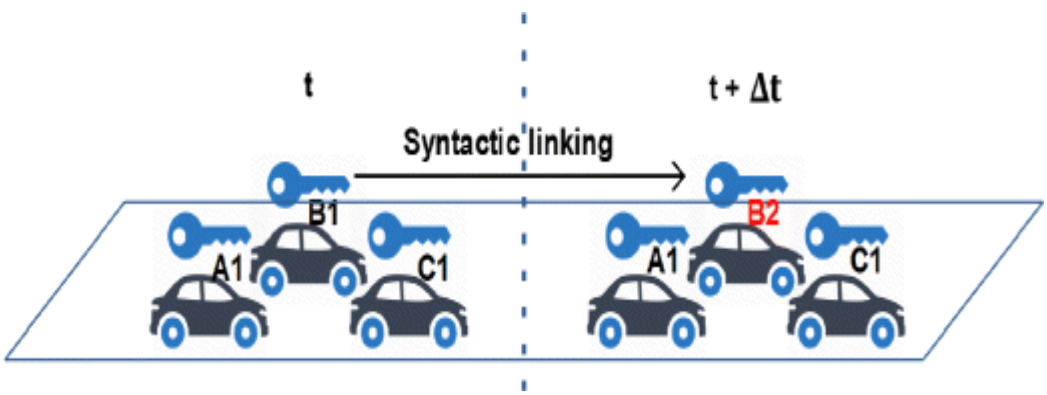

Figure 4 . *The syntactic linking of pseudonyms* [14]

2 - Semantic linking

Figure 5 represents the semantic linking of pseudonyms. This type of attack is more potent than the syntactic linking of pseudonyms because the adversary relies on the information included in safety messages to link the pseudonyms. For example, the adversary can predict the next position of the vehicle using a tracking method. Then, based on this prediction, the adversary can link the pseudonyms B1 and B2 even if the three vehicles, illustrated in Figure 5, change their pseudonyms simultaneously [15].

The protection against this type of attack can only be done by preventing the adversary from getting access to safety messages for some periods.

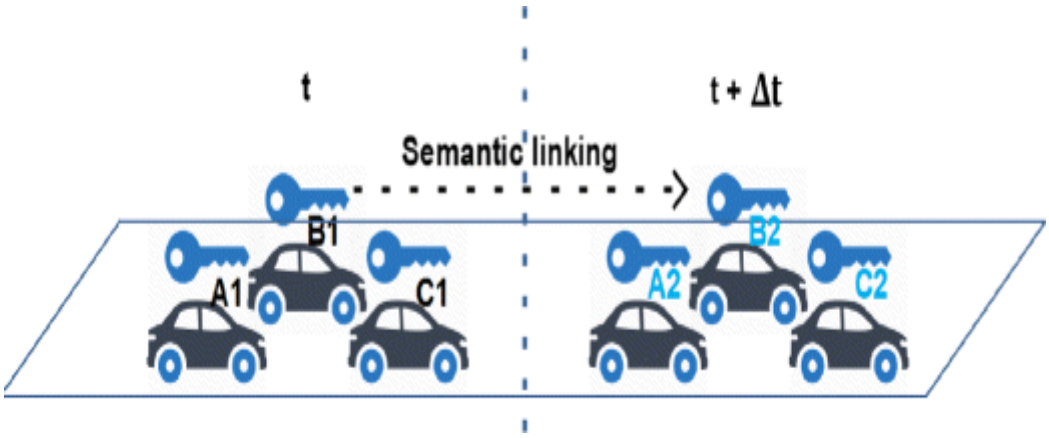

Figure 5. *The semantic linking of pseudonyms* [14]

III - Pseudonym changing strategies

Researchers have carried out many studies and strategies related to changing pseudonyms to protect against attacks which are divided as follows:

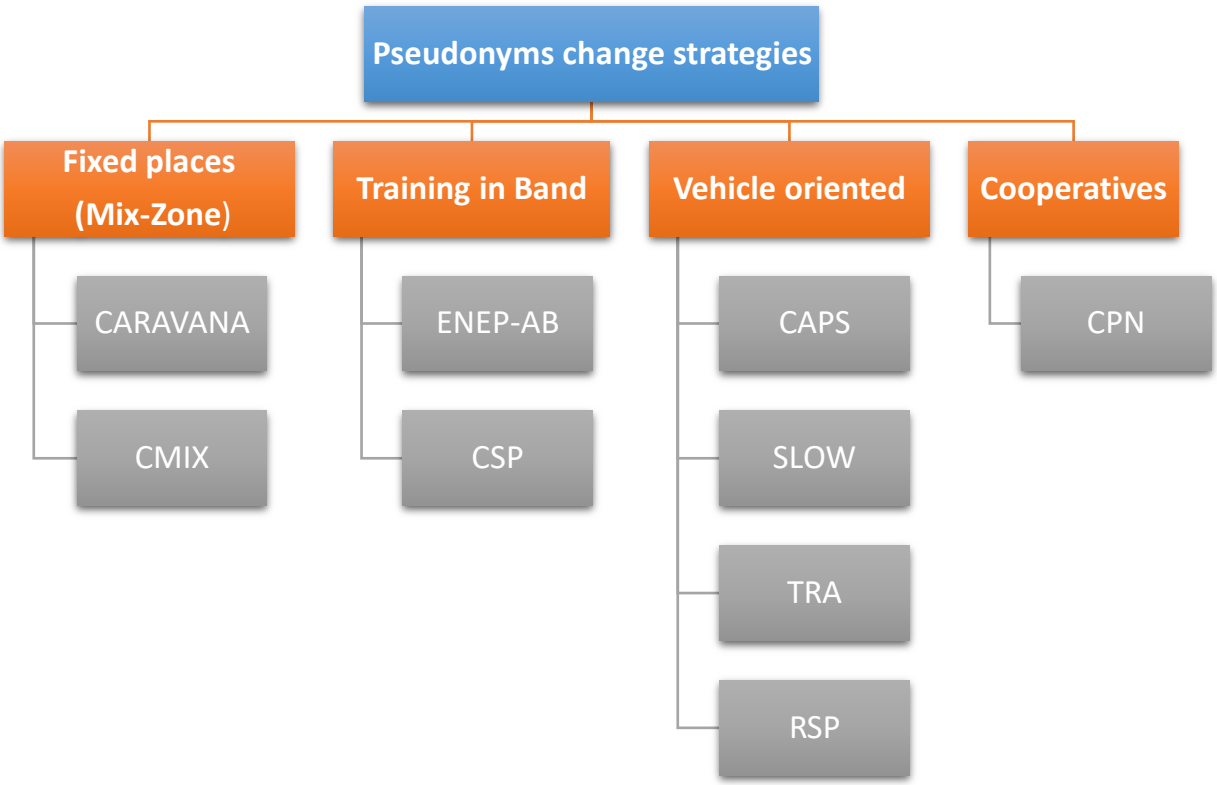

Figure 6 .*Pseudonyms change strategies*

1 - Fixed places (Mix-Zone)

In this paper, Freudiger ET al.2007 proposed the CMIX protocol [18].CMIX uses mix-zones with cryptography. Thus, drivers' location is preserved by encrypting their BSMs while in such zones. The protocol relies on infrastructures to provide the shared keys, making it challenging.

In this paper, samppigethaya ET al. proposed the CARAVAN scheme [19] where all vehicles belong to groups to protect their anonymity and use silent periods between pseudonym changes while in the group since the group leader can communicate on behalf of the other members. The silent period concept was first proposed in [20] by Huang et al. 2005 in wireless LAN systems. The principle as mentioned is to let the node stay silent, i.e., does not communicate for a short period to make it hard for the adversary to link its new and old pseudonyms, exceptionally efficient against the correlation attack [21]

2 - Training in Band

Zidani et al.2018 proposed using the Adaptive Beaconing rate approaches instead of the mix-zones concept and an Estimation of Neighbors Position privacy scheme with an Adaptive Beaconing approach [16], where the pseudonym changing is based on the number and the estimated positions of neighbors collected in the previous time slot. Also, to adjust the interval of sending beacons, expanding ENeP-AB with an Adaptive Beaconing approach, denoted Extended Adaptive Beaconing Rate Protocol (E-ABRP).

3 - Vehicle Oriented

In this paper, Buttyn et al. 2009 propose the SLOW protocol [13]. SLOW lets vehicles independently decide the right moment to change their pseudonyms according to their speeds when it drops under a certain threshold. Indeed, at low speeds, the risk of accidents will be low. Thus, the vehicle is allowed to use silent periods. The standardization contradiction represents the only issue, which obliges a beaconing frequency of at least once per second.

Tomandl ET al.2012 propose to study the effects of mix-zones and silent periods [22]. The work is furthermore implemented by Emara 2016. Their privacy extension PREXT [23] was named Coordinated Silent Period (CSP). Emara et al. also proposed a privacy scheme called Context-Aware Privacy Scheme (CAPS) [24] that first vehicles choose the appropriate context to enter the silent period and change their pseudonyms.

In this paper, the authors propose a protocol (RSP) based on a period of silence to achieve location privacy [20]. When a node enters a period of silence, it stops broadcasting messages and makes a change of pseudonym at the end of this period. This makes it more difficult to associate two pseudonyms received separately with the same station.

Babaghayou and Nabila Labraoui.2019 proposed to provide an enhancement of a set of schemes by allowing vehicles to adjust their beacon transmission range to avoid tracking [16] conditionally. To the best of my 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. They evaluated this feature’s performance after integrating it into some well-known strategies: SLOW and CAPS.

4 - Cooperatives

In this paper, “Pseudonym Synchronously Change” (PSC), Shi et al .2014 have assumed that each RSU periodically broadcasts the number of vehicles nearby transmitters. In this case, all vehicles can know the number of their neighbors. A vehicle with more or equal k neighbors sends a message to its neighbors to ask them to change their pseudonym synchronously [25].

Vehicles change their pseudonyms in a predefined location (e.g., in road intersections). The Cryptographic MIX is the first implementation in a fixed mix-zone, known as the CMIX protocol proposed by Freudiger et al. [16] [15].CMIX uses mix-zones with cryptography. The vehicles change their pseudonyms inside a CMIX zone and use a shared key distributed by an RSU to encrypt their safety messages.

The second implementation proposed by Lu et al. suggested changing pseudonyms on social spots where vehicles congregate heavily and frequently, such as intersections and parking lots. This confuses the attacker, making it difficult for him to locate the vehicles and their pseudonyms.

IV - Conclusion

In this chapter, we discussed first the types of linking attacks and the most common pseudonym-changing strategies. We present proposals and works carried out within the framework of preserving privacy in VANET vehicle networks. Each of them offers a massive plus in the area of privacy. Also, we have an interest in this last paper. We will implement the proposed protocol, and we will see the result in the next chapter.

Chapter 04: Contribution

I- Introduction

This chapter will discuss our simulation, how it is built, and the results obtained. Then we will describe the simulation tools that we have worked on used in our contribution. We will discuss our framework and all steps we have passed it. Lastly, we present a performance evaluation and comparative study [26].

II- TRA protocol

First, before we talk about TRA [15], we must explain what SLOW is. The protocol allows the vehicle to choose the appropriate moment according to their speed when it drops to a specific limit to change their pseudonyms. Because when low speed the risk of traffic accidents decreases and thus the vehicle enters a period of silence and its changes e their pseudonyms.

Now we start talking about the TRA protocol because it adopts the same context and method as the slow protocol, except that it does not enter into silence periods but rather adjusts the transmission range, whereas, at low speeds, it reduces and shrinks the transmission range to a certain extent and changes their pseudonyms, the same way as the slow. After all, it works at low speeds because the accident rate is low, and adjusting the transmission range does not affect safety at low speeds.

III - Simulation environment

In order to obtain accurate results, performance should not be measured in a suitable, realistic hardware environment. Because it is costly, we use simulation with a tool known for it’s close to absolute power. We chose OMNET++ 5.0 network simulator, widely used to simulate Security protocols and applications in wireless networks.

We also need a geographic map containing the roads and vehicles that rotate within the network. We chose the SUMO 0.25.0 Road Traffic Simulator. As part of our study, we also integrated an open-source framework called Veins 4.4, which combines SUMO and OMNET++ to get significant simulation results close to reality. We also need PREXT, which contains existing security schemas, and allows the implementation of new schemas.

Also, do not forget to mention that we used a computer with the following specifications to perform this simulation:

- ✓ Processor Intel(R) Core(TM) i5-4310M CPU @ 2.70 GHz 2.70 GHz
- ✓ Memoire RAM installed 8.00 GO
- ✓ Type of system: system exploitation 64 bits processor 64
- ✓ GREEN IT

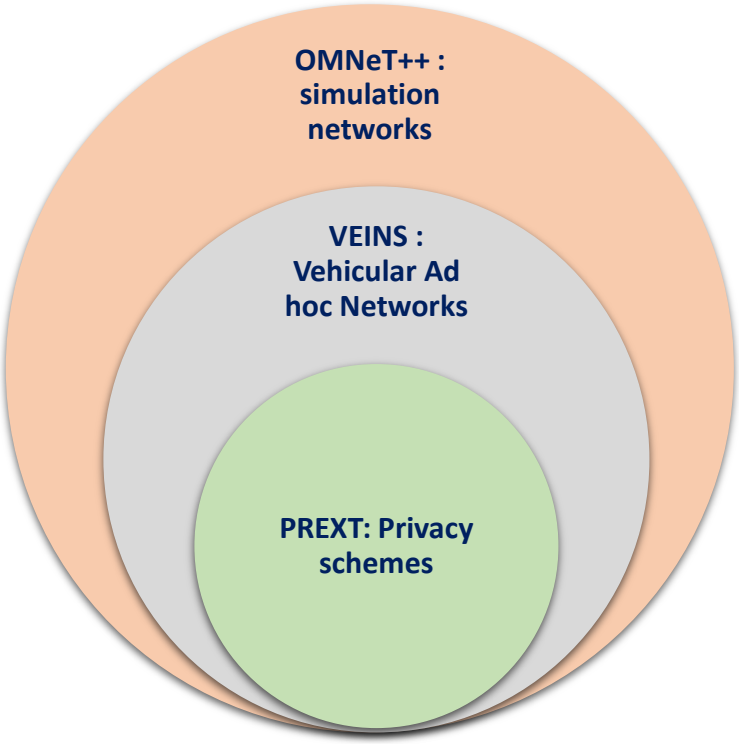

Figure 7. *Simulation environment*

1 - SUMO

It is an open-source, highly portable, microscopic, and continuous traffic simulation package designed to handle large networks. It allows for intermodal simulation, including pedestrians, and comes with a large set of tools for scenario creation [26].

2 - OMNeT++

It is an extensible, modular, component-based C++ simulation library and framework, primarily for building network simulators. “Network” is a broader term that includes wired and wireless communication networks, on-chip networks, queuing networks, and so on. Domain-specific functionality such as support for sensor networks, ad-hoc wireless networks, Internet protocols, performance modeling, photonic networks, etc., is provided by model frameworks developed as independent projects. OMNeT++ offers an Eclipse-based IDE, a graphical runtime environment, and various other tools. There are extensions for real-time simulation, network emulation, database integration, SystemC integration, and several other functions [27].

3 - VEINS

It is an open-source framework for running vehicular network simulations [28]. It is based on two well-established simulators: OMNeT++, an event-based network simulator, and SUMO, a road traffic simulator. It extends these to offer a comprehensive suite of models for IVC simulation.

4 - PREXT

It is a unified and extensible framework that simulates alias change schemes (such as privacy schemes) in VANET. Although PREXT was primarily developed for VANET scenarios, it can be used/adapted for simulations that allow mobile nodes to broadcast their Spatio-temporal information periodically. The central assumption in PREXT is that nodes broadcast beacon messages every short time. It contains its location, speed, timestamp, and a variable alias (i.e., temporary node identity). The general concept of privacy schemes in such scenarios is to periodically change aliases, followed by pausing/encrypting beacon messages for a period to prevent the chaining of cascading messages from each vehicle [29].

4-1- The confidentiality schemes of PREXT

Seven confidentiality schemes are implemented in PREXT. We will present and explains each strategy [23]:

4-1-1 Slow Protocol

In SLOW [13], a vehicle continuously checks its current speed and broadcasts beacons only when its speed is higher than a preset threshold SP. If a vehicle does not send beacons for ST seconds, it changes its pseudonym.

4-1-2 PeriodicalPC (Periodical Pseudonym Change)

In this strategy [30], the change of pseudonym is done in a way automatic after each period. This period can be fixed or random. A fixed period can increase the number of simultaneous changes in pseudonyms between neighboring vehicles, but the adversary may be able to know or predict when nicknames will be changed. A time of change randomness overcomes this prediction problem, but it can reduce the number of simultaneous changes of pseudonyms.

4-1-3 RSP

This privacy scheme allows a node to change its pseudonym after a fixed period (lifetime of a pseudonym). When the duration is over (duration of life expired), the vehicle enters a period of silence (does not send beacon messages or others), [19]. This period is chosen randomly from a well-defined interval [Mins, Maxs]. After this period of silence, the vehicle changes its nickname.

4-1-4 Caps Protocol

The basic concept of the Context-aware Privacy Scheme (CAPS) [23] is to determine the appropriate context in which a vehicle should change its pseudonym. This approach aims to increase the effectiveness of such changes against tracking and avoid wasting pseudonyms in easily traceable situations. Also, it determines the sufficient silence period that leads to possible tracker confusion. It employs an internal local vehicle tracker using beacons received by its onboard communication unit.

4-1-5 CSP (Coordinated-Silent-Period)

The CSP [22] coordinates all the vehicles in the network to enter a period of silence synchronously, then all vehicles come out of silence and change pseudonyms simultaneously. This strategy is much more theoretical since the overall coordination of silence among vehicles is complicated and requires.

4-1-6 CPN (Cooperative Pseudonym change scheme based on the number of Neighbors)

In CPN [31], each vehicle must check the number of its neighbors within a radius R. If the number of neighbors reaches a threshold K, the vehicle modifies the state of an internal “Ready Flag” parameter. It sends it in a “beacon” type message. It makes a change of pseudonym in the next beacon broadcast. When a vehicle receives a beacon with a “Ready Flag” change, it immediately changes its pseudo-identity despite not reaching the K neighbors.

4-1-7 Mix zone

It is a specific and previously known area ready for the change of nicknames. It is usually placed at road intersections, making it challenging to predict vehicle movements. Hiding messages in a Mix-zone is achieved by keeping silent (vehicles do not send messages) [32] or encrypting messages using a shared key obtained from RSU.

IV - Evaluation and performance

In this part, we evaluate and compare the TRA protocol after its implementation by demonstrating its efficiency and performance compared to other PREXT schemes.

1 - Simulation parameters

In the simulation, we used a road map of our state Borj Bou Arréridj whose size is 3, 6 x 4, 7 km², as shown in figure 7. This map is obtained from "Open Street Map" and converted to SUMO with the use of "net convert" and "poly convert" tools included in SUMO 0.25.0. The maximum speed of the vehicles is 50 km/h with an acceleration range between -4.5 m/s2 and 2.6 m/s2. Each vehicle broadcasts "beacon" control messages every second. The median trace lifetime is 300 s, while the median trace distance is approximately 4km. Each experiment is repeated five times. Table 1 summarizes these parameters.

Figure 8. *Geographical map of the city center of Bordj Bou Arréridj*

parameters	Value
Map area	3,6 x 4,7 km²
Maximum vehicle speed	50 km/h
Acceleration range	Between -4,5 m/s2 et 2,6 m/s2
Median trace lifetime	300 s
Median trace distance	4 km
Transmit power	0.2 Mw
Beacon throughput	1 Hz
Tracking interval	1 s
Headphone range	300 m
Headphone overlap	30 m

Table 1 . *Simulation parameters*

2 - Simulation Results

This protocol will be evaluated and compared with the diagrams available under PREXT in terms of Traceability %90, Normalized traceability %90, average Confusions per trace, Average Confusions per pseudonym change, and Average Pseudonym change per trace.

2-1- Traceability %90

We note from our data and Table 2 and 3 that the average traceability rate in the authority's protocol is low, and we found it 28.9655 Compared to other protocols.

At SLOW, we find 32.0755, up by nearly 3%, and at CAPS 89.4977 and RSP, it's 78.5714. We note that with the last two protocols, the traceability rate had increased by more than 50% compared to TRA.

DENSITY	0	30	50	70	90
SLOW	33,3333	32,0755	32,0755	32,7044	32,7044
TRA	25,3425	26,5306	28,9655	25,3425	26,5306
CAPS	93,4911	90,9548	89,4977	90,84526	91,8919
RSP	81,6327	76,9231	78,5714	87,5	80,9524

Table 2 . *Traceability 90%*

According to the results, we notice that the CAPS and RSP schemes almost have 100% traceability, compared to SLOW, which has reduced its traceability by 68%, and we also not TRA came back to us with the best result as it reduced the tracking rate by 74%.

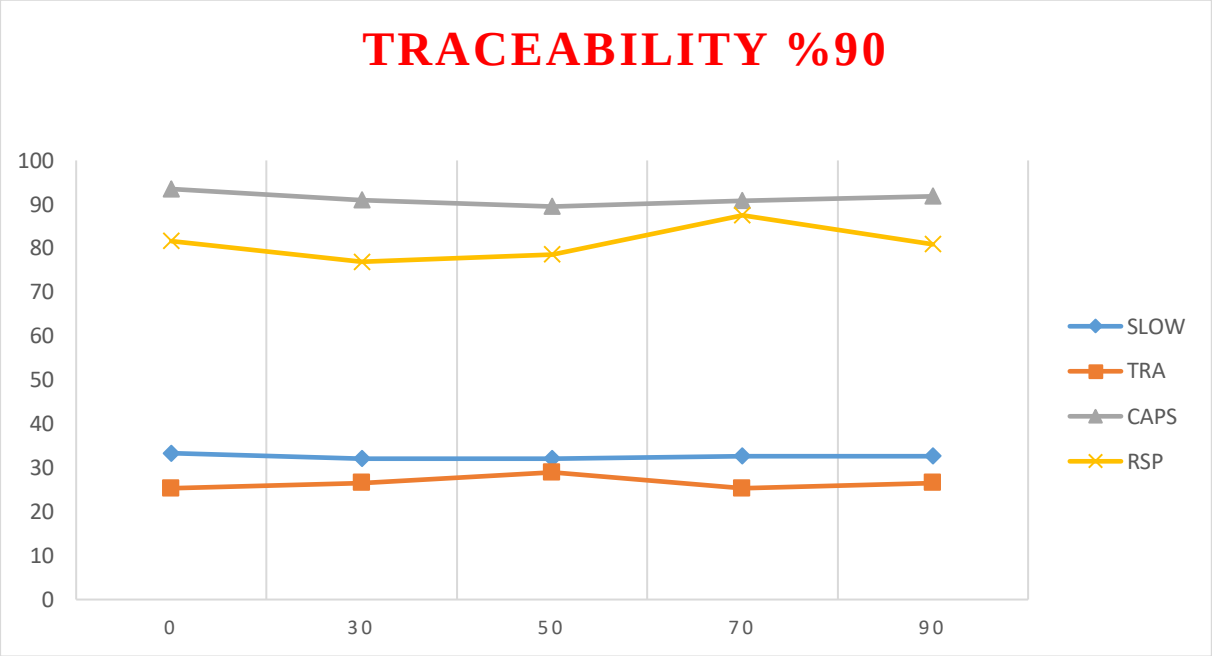

Figure 9.*Traceability*

We also do not forget that every time we do the simulations, we change the density to help us know the tracking ratio. It may also confuse the tracker so that we can get different results and rely on them to compare.

2-2- Normalized traceability 90%

We got the same results we obtained in the previous element, where we noticed that the traceability rate is low compared to other schemes. In contrast, the traceability rate in TRA protocol is meagre compared to other protocols, as it successfully confuses the tracer so that he cannot track it on the 90% path, which is an indication of the strength and success of this protocol in maintaining driver privacy.

DENSITY	0	30	50	70	90
SLOW	18,4615	16,5354	17,1875	18,9394	16,4062
TRA	7,9646	6,30631	6,42202	6,19469	7,01754
CAPS	84,6154	81,7204	81,3559	81,15651	87,2611
RSP	25	25	11,1111	23,5	16,6667

Table 3.*Normalized traceability*

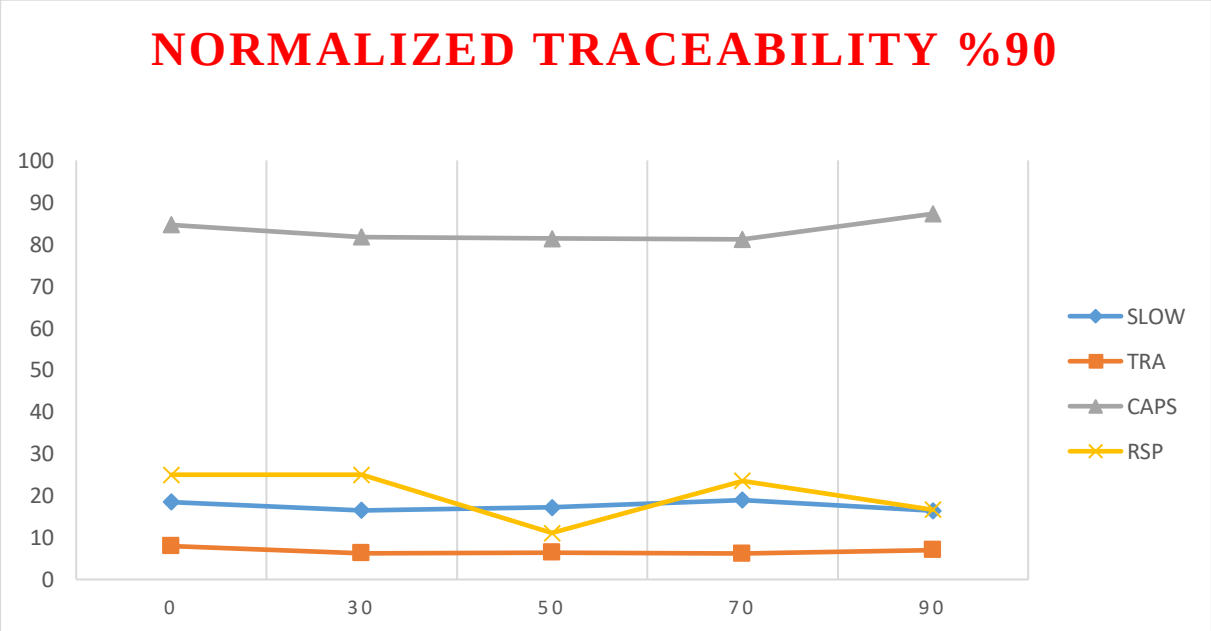

Figure 10.*Normalized traceability*

The average confusion for each effect, we note that its results are logical, as the moderate disorder is high for TRA, and we note that it increases with the high intensity due to the way

TRA works, as it works to modify the transmission range at the right moment and the right speed.

We know very well that I am a Vanet. Its vehicles communicate through beacons, carrying information related to speed and location to ensure the car's safety and the road. Communication is carried out through the stream of any transmission range. If these messages are not transmitted, a problem may occur related to the life and security of people, and one of the advantages of TRA is that it does not affect BMS exactly, but it works. It has to modify and expand the transmission range at precisely the right moments, as it reduces the transmission range when the speed of cars drops to less than 30 km. Here there is a change to the nickname so that we ensure that the attacker cannot eavesdrop and the followers because the transmission range does not exceed 0.2 Mw, and then expand it again And at a different rate every time and at every speed, which leads to confusing the attacker and making it very difficult to track the vehicles easily as in the case of:

2-3- Average Confusions per pseudonym change

Here the tracker loses the car he is following because he does not have the information of the vehicle he was following because every time after adjusting the transmission range, the car is stripped of its previous information and given new information. He will have difficulty linking the old data to the new vehicle, as he loses its trace because of pseudonym change.

DENSITY	0	30	50	70	90
SLOW	0,611765	0,623494	0,614458	0,594203	0,611276
TRA	0,792593	0,818519	0,806084	0,811321	0,819853
CAPS	0,26087	0,234043	0,207101	0,180713	0,151899
RSP	1,44444	2,11111	1,5	2,33333	2

Table 4. *Average Confusions per pseudonym change*

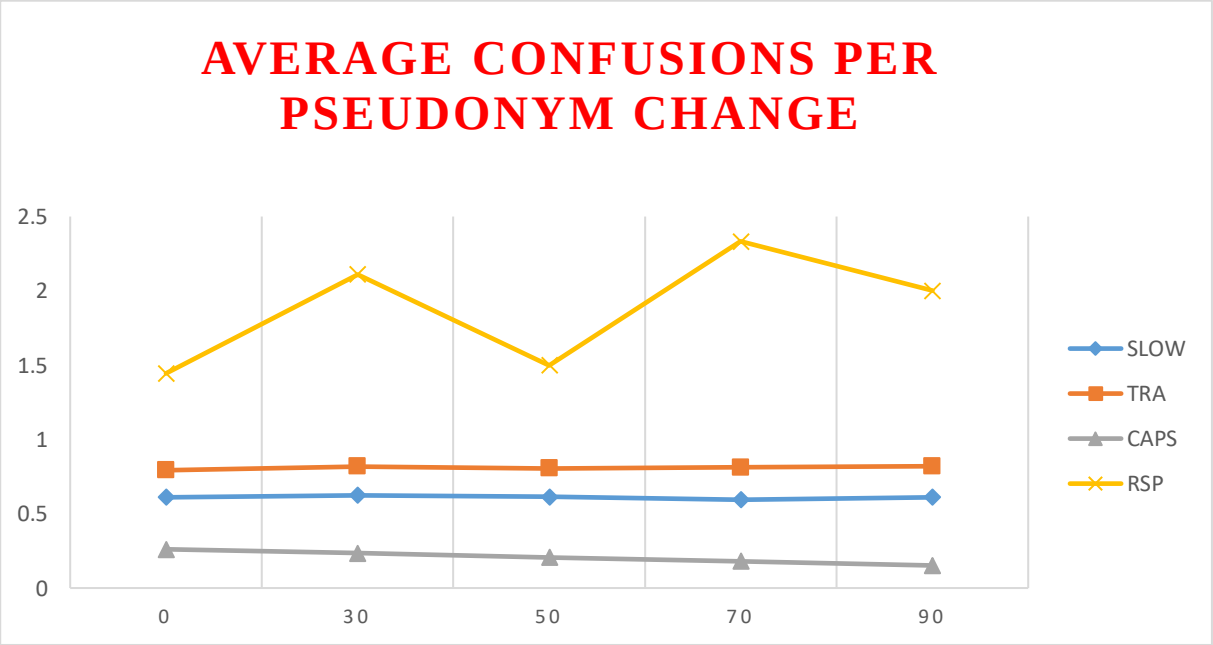

Figure 11.*Average Confusions per pseudonym change*

RSP make changes to pseudonyms periodically, so it can automatically have several changes smaller than TRA or slow protocols wish to make changes regarding velocity threshold, which means that the average confusion per pseudonyms will be generated in the RSP protocol, our results are best compared with the rest of the protocols.

2-4- Average Confusion Pseudonym change per trace

As we explained, modifying the transmission range every time makes the opponent confused. In this case, changing the nickname greatly confuses the tracker, as the car's exit with new information is the reason for the opponent's confusion. An increasing pseudonym shifts every time we increase in density as the higher density tweed in average confusion for each pseudonym change.

DENSITY	0	30	50	70	90
SLOW	2,13836	2,08805	2,08805	2,16981	2,1195
TRA	1,84932	1,83673	1,81379	1,811321	1,85034
CAPS	0,408284	0,472362	0,771689	0,560311	0,610039
RSP	0,183673	0,230769	0,238095	0,225	0,166667

Table 5.*Average Confusions per pseudonym change per trace*

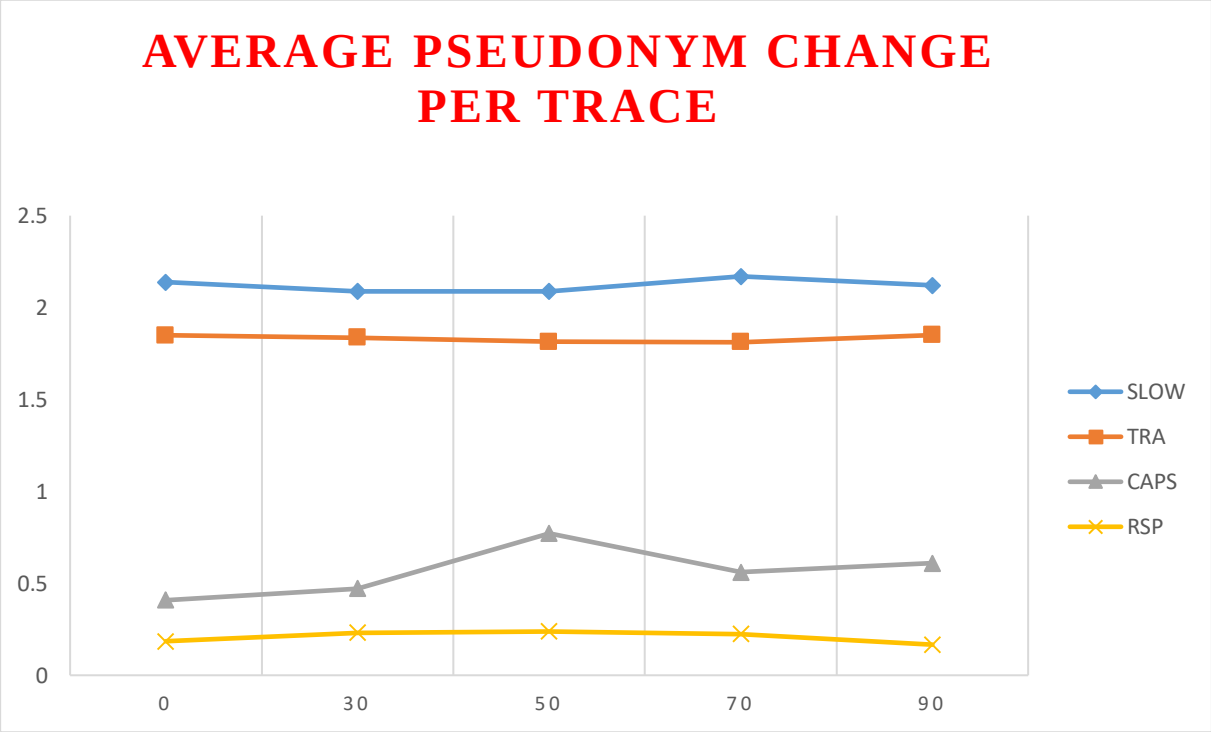

Figure 12.*Average Confusions per pseudonym change per trace*

2-5- Average Confusions per trace

Changing the transmission range every time confuses the attacker, causing him to lose track of the car he was following, as the car, after leaving the specified transmission range, comes out with a new identity and new information, which confuses the opponent and makes him lose track.

DENSITY	0	30	50	70	90
SLOW	1,30818	1,30189	1,28302	1,28931	1,2956
TRA	1,46575	1,5034	1,46207	1,4726	1,51701
CAPS	0,106509	0,110553	0,159817	0,140912	0,0926641
RSP	0,265306	0,487179	0,357143	0,525	0,33333

Table 6 .*Average Confusions per trace*

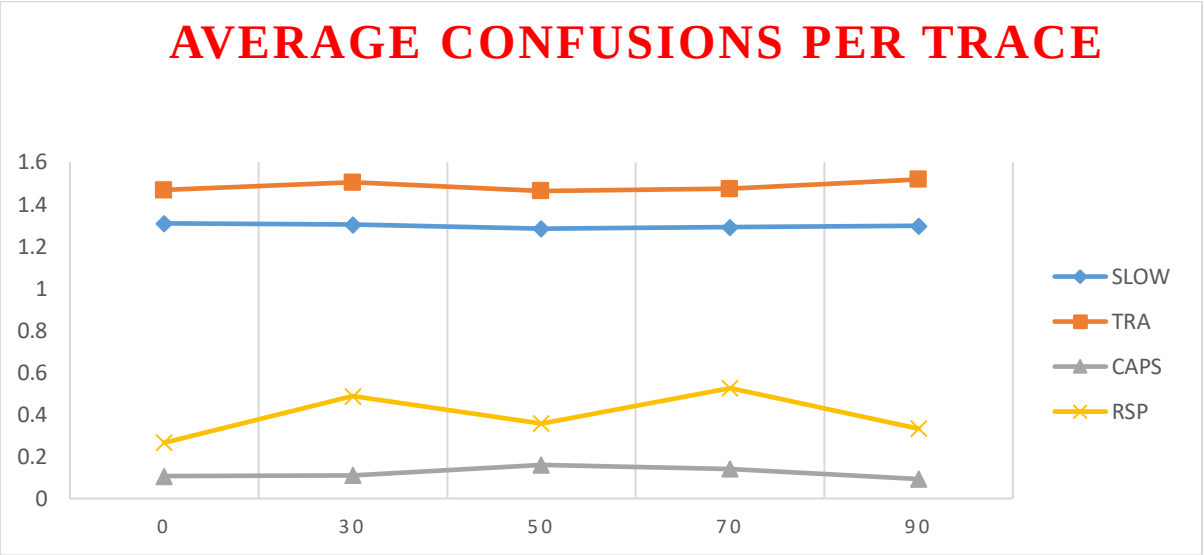

Figure 73.*Average Confusions per trace*

V - Conclusion

In this chapter, we presented the working environment of our approach and the simulation results where the TRA showed promising results in modifying the transmission range and appeared at traceability and confusion compared to other privacy schemes.

General conclusion

General conclusion

As we mentioned earlier, the importance of protection in the vehicle network, and with the expansion of the network, the importance of vehicle and driver privacy increases, and its security becomes the first obstacle. There is a lot of research and work in this field.

In this work, we first studied a lot of previous and current results and the essential protection protocols, especially those in PREXT, which attracted us more to work on the privacy feature as we applied new technology to the best of our knowledge that has not yet been worked on, as we studied the effect of modifying the transmission range in the vehicle network and integrating it In one of the most critical protection protocols, Slow, where we determined the transmission range every time and studied results, where good results appeared compared to the original protocol and other protocols such as RSP and CAPS, and among the most critical points that made it a successful technology is that it did not affect safety and protection applications, and this made it under the standards of safety protocols.

In our studies and simulations, we have relied on OMNET++ 5.0, widely used to simulate security protocols and applications in the wireless network. Our choice is due to the advantages it provides compared to other simulators. We also chose SUMO 0.25.0 for traffic, combined an open framework called VEINS 4.4, which combines OMNET++ and SUMO to get simulation results close to reality, and used the new open source project PREXT, which contains security diagrams existing and allows the creation of new schemas.

In the end, it will be interesting to develop this technique and work on it more to get better results because the results have proven effective and working on it more will give better results by a considerable percentage.

Bibliography

[1] K. Mochrraoui, “GESTION DE L’ANONYMAT DES COMMUNICATIONS DANS LES RÉSEAUX VÉHICULAIRES AD HOC SANS FIL (VANETs),” UNIVERSITÉ DU QUÉBEC, QUÉBEC, 2015.

[2] Y. Park, K. H. Rhee, and C. Sur, “A secure and location assurance protocol for location-aware services in VANETs,” 2011. doi: 10.1109/IMIS.2011.40.

[3] S. Busanelli, G. Ferrari, and L. Veltri, “Short-lived key management for secure communications in VANETs,” 2011. doi: 10.1109/ITST.2011.6060129.

[4] H. BENSEFIA, “Network Security Course, Chapter 1 Basic Concepts of IT Security Master 2 Networks & Multimedia.”

[5] “Jonathan”’ “Petit,” “Surcoût de l’authentification et du consensus dans la sécurité des réseaux sans fil véhiculaires,” Ph.D, UNIVERSITÉ DE TOULOUSE, 2011.

[6] “Noureddine” “CHAM,” “La sécurité des communications dans les réseaux VANET,” Master, Université Elhadj Lakhder-Batna, 2011.

[7] “ADETUNDJI”.’ ADIGUN’, “GESTION DE L’ANONYMAT ET DE LA TRAÇABILITÉ DANS LES RÉSEAUX VÉHICULAIRES SANS FIL,” Master, L’UNIVERSITÉ DU QUÉBEC À TROIS-RIVIÈRES, QUÉBEC , 2014.

[8] “Hakima” “Chaouchi” and “Laurent-Maknavicius” “Maryline,” *Wireless and Mobile Network Security*, vol. 744. Hermes science/Lavoisier, 2013.

[9] A. Upadhyaya, A. N. Upadhyaya, and J. Shah, “Attacks on VANET Security,” *International Journal of Computer Engineering & Technology (IJCET*, vol. 9, no. 1, pp. 8–19, [Online]. Available : http://www.iaeme.com/IJCET/index.asp8http://www.iaeme.com/ijcet/issues.asp?JType=IJCET&VType=9&IType=1JournalImpactFactor

[10] M. B. Mansour, C. Salama, H. K. Mohamed, and S. A. Hammad, “VANET Security and Privacy - An Overview,” *International Journal of Network Security & Its Applications*, vol. 10, no. 2, 2018, doi: 10.5121/ijnsa.2018.10202.

[11] “El-Sayed Emara” “Karim Ahmed Awad,” “Safety-aware Location Privacy inVehicular Ad-hoc Networks,” TECHNICAL UNIVERSITY OF MUNICH, MUNICH, 2015.

[12] L. Buttyán, T. Holczer, A. Weimerskirch, and W. Whyte, “SLOW: A practical pseudonym changing scheme for location privacy in VANETs,” 2009. doi: 10.1109/VNC.2009.5416380.

[13] A. Boualouache and S. Moussaoui, “Urban pseudonym changing strategy for location privacy in VANETs,” 2017.

[14] “Abdelwahab” “BOUALOUACHE,” “sécurité et vie privée dans les réseaux véhiculaires,” Ph.D, Université des sciences et de la technologie, Algiers, 2016.

[15] M. Babaghayou and N. Labraoui, “Transmission Range Adjustment Influence on Location Privacy-Preserving Schemes in VANETs,” 2019. doi: 10.1109/ICNAS.2019.8807823.

[16] F. Zidani, F. Semchedine, and M. Ayaida, “Estimation of Neighbors Position privacy scheme with an Adaptive Beaconing approach for location privacy in VANETs,” *Computers and Electrical Engineering*, vol. 71, 2018, doi: 10.1016/j.compeleceng.2018.07.040.

[17] J. Freudiger, M. Raya, M. Félegyházi, P. Papadimitratos, and J.-P. Hubaux, “Mix-zones for location privacy in vehicular networks,” 2007.

[18] K. Sampigethaya, L. Huang, M. Li, K. Poovendran, Radha Matsuura, and K. Sezaki, “CARAVAN: Providing location privacy for VANET,” *Embedded Security in Cars*, 2005.

[19] L. Huang, K. Matsuura, H. Yamanet, and K. Sezaki, “Enhancing wireless location privacy using silent period,” in *IEEE Wireless Communications and Networking Conference, WCNC*, 2005, vol. 2. doi: 10.1109/WCNC.2005.1424677.

[20] J. Petit, F. Schaub, M. Feiri, and F. Kargl, “Pseudonym Schemes in Vehicular Networks: A Survey,” *IEEE Communications Surveys and Tutorials*, vol. 17, no. 1. 2015. doi: 10.1109/COMST.2014.2345420.

[21] A. Tomandl, F. Scheuer, and H. Federrath, “Simulation-based evaluation of techniques for privacy protection in VANETs,” 2012. doi: 10.1109/WiMOB.2012.6379070.

[22] K. Emara, “Poster: PREXT: Privacy extension for Veins VANET simulator,” in *IEEE Vehicular Networking Conference, VNC*, 2016, vol. 0. doi: 10.1109/VNC.2016.7835979.

[23] K. Emara, W. Woerndl, and J. Schlichter, “CAPS: Context-aware privacy scheme for VANET safety applications,” 2015. doi: 10.1145/2766498.2766500.

[24] X. Shi and H. Xu, “An effective scheme for location privacy in VANETs,” *Journal of Networks*, vol. 9, no. 8, 2014, doi: 10.4304/jnw.9.8.2239-2244.

[25] “Simulation of Urban MObility download | SourceForge.net.” https://sourceforge.net/projects/sumo/ (accessed Jun. 14, 2022).

[26] “What is OMNeT++?” https://omnetpp.org/intro/ (accessed Jun. 14, 2022).

[27] “Veins.” https://veins.car2x.org/ (accessed Jun. 14, 2022).

[28] “GitHub - karim-emara/PREXT: PREXT is a unified and extensible framework that simulate pseudonym change schemes (i.e., privacy schemes) in VANET.” https://github.com/karim-emara/PREXT (accessed Jun. 14, 2022).

[29] D. Eckhoff, R. German, C. Sommer, F. Dressler, and T. Gansen, “SlotSwap: Strong and affordable location privacy in intelligent transportation systems,” *IEEE Communications Magazine*, vol. 49, no. 11, 2011, doi: 10.1109/MCOM.2011.6069719.

[30] Y. Pan and J. Li, “Cooperative pseudonym change scheme based on the number of neighbors in VANETs,” *Journal of Network and Computer Applications*, vol. 36, no. 6, 2013, doi: 10.1016/j.jnca.2013.02.003.

[31] L. Buttyán, T. Holczer, and I. Vajda, “On the effectiveness of changing pseudonyms to provide location privacy in VANETs,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2007, vol. 4572 LNCS. doi: 10.1007/978-3-540-73275-4_10.

[32] S. S. Shah, A. W. Malik, A. U. Rahman, S. Iqbal, and S. U. Khan, “Time Barrier-Based Emergency Message Dissemination in Vehicular Ad-hoc Networks,” *IEEE Access*, vol. 7, 2019, doi: 10.1109/ACCESS.2019.2895114.

[33] A. Boualouache and S. Moussaoui, “TAPCS: Traffic-aware pseudonym changing strategy for VANETs,” *Peer-to-Peer Networking and Applications*, vol. 10, no. 4, pp. 1008–1020, Jul. 2017, doi: 10.1007/s12083-016-0461-4.