الجمـــهوريـــة الجـــزائريـــة الديـمقـراطيـــــــة الشـــعبيـــــة
REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
وزارة التعـلـيـم الـعـالـــي و الـبـحـث الـعـلـمـي
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
جـامـعـة عمّـــار ثـلـيـــجـــي بالأغـــواط
UNIVERSITE AMAR TELIDJI LAGHOUAT
كـلـيـــــة الـعـلـــــوم
FACULTE DES SCIENCES
DEPARTEMENT DE MATHEMATIQUES ET INFORMATIQUE

Mémoire de MASTER

Domaine : Mathématiques et Informatique
Filière : Informatiques
Option : Réseaux, Systèmes et Applications Réparties

Par:
-Taibi Mohammed
-Begouga Mohammed Islam

THEME

Impact of silent period on pseudonym changing protocol

Soutenu publiquement devant le jury composé de :

Mr Bendouma Taher	*Professeur*	*Président*
Mr Amer Abdelkader Ilyas	*M.C.(A)*	*Examinateur*
Mr Noureddine Chaib	*M.C.(A)*	*Encadreur*

N …… Année Universitaire 2020/2021

Acknowledgments

Above all, we would like to thank Allah for our success in accomplishing this memorandum and acquiring knowledge through a new experience in this field.

We want to thank our supervisor, Mr. Noureddine Chaib, who helped us a lot in every step we took, the advice and guidance he gave us, we also thank the members of the jury very much for their sparing their precious time in order to evaluate our work, as well as for the advice given. Also, let's not forget to thank the professors who helped us throughout the course of our study. We also thank all of our colleagues and anyone who contributed even a little to help us in this experience.

In conclusion, we thank our families, especially our parents, for their continuous support and encouragement throughout our study path.

.

ملخص

تعد قضية الطرق والمرور وطرق تنظيمها من الموضوعات الأساسية في عصرنا. لذلك تلعب أنظمة وشبكات اتصالات المركبات دورًا مهمًا في تنظيم وسلامة حركة المرور وتقليل الحوادث الناجمة عن مشاكل الازدحام وغيرها ، ناهيك عن قدرة هذه الأنظمة على توفير اتصال آمن للمعلومات والبيانات بين المركبات. تعد خصوصية السائقين أمرًا ضروريًا لنجاح عمليات الاتصال. ومع ذلك ، فقد أصبحت هذه الأخيرة محورًا للمهاجمين الذين يمكنهم الحصول على المعلومات باتباع العديد من الأساليب والهجمات مثل تحديد الموقع. كحل لمشكلات الخصوصية يعد تغيير الأسماء المستعارة بعد الدخول في فترات صامتة ، حلا مقبولاً على نطاق واسع.

في هذه الرسالة ، ندرس تأثير الفترة الصامتة على أداء أنظمة الخصوصية.وذلك باستخدام إطار عمل مخصص للخصوصية ، يسمى "Prext" ، لدراسة بيئة المركبات. وجدنا قيمًا مختلفة لأفضل فترة صمت وفقًا لكل تطبيق.

Résumé

La question des routes, de la circulation et des moyens de les réguler est l'un des sujets essentiels de notre époque. Par conséquent, les systèmes et réseaux de communication des véhicules jouent un rôle important dans la régulation et la sécurité du trafic et la réduction des accidents causés par les problèmes de congestion et autres, sans parler de la capacité de ces systèmes à assurer une communication sûre des informations et des données entre les véhicules. La confidentialité des chauffeurs est essentielle à la réussite des opérations de communication. Reste que ce dernier est devenu la cible d'attaquants qui peuvent obtenir des informations en suivant plusieurs méthodes et attaques comme la localisation. En tant que solution aux problèmes de confidentialité, le changement de pseudonymes, après des périodes de silence, au lieu d'identifiants à long terme est une solution largement acceptée.

Dans cette thèse, nous étudions l'impact de la période de silence sur les performances des schémas de confidentialité existants. Nous avons considéré un cadre dédié à la vie privée, appelé "Prext" pour notre étude dans l'environnement véhiculaire. Nous avons trouvé différentes valeurs pour la meilleure période de silence selon chaque approche.

Abstract

The issue of roads, traffic, and ways of regulating them is one of the essential topics in our time. Therefore, vehicle communication systems and networks play a significant role in regulating and safety of traffic and reducing accidents caused by congestion problems and others, not to mention the ability of these systems to provide safe communication of information and data between vehicles. The privacy of the drivers is essential for the success of communication operations. Still, this latter has become the focus of attackers who can obtain information by following several methods and attacks such as locating. As a solution to privacy issues, changing pseudonyms, after silent periods, instead of long-term identifiers is a widely accepted solution.

In this thesis, we study the impact of the silent period on the performance of privacy existing schemes. We have considered a privacy dedicated framework, called "Prext" for our study in the vehicular environment. We found different values for the best silent period according to each approach.

Contents

List of tables

List of Figures

General introduction

Traffic and its activity have always been one of the most important daily matters for individuals worldwide, especially nowadays. Still, a large number of vehicles negatively affected traffic safety, such as the high rates of accidents in addition to other problems.

Road security is the critical point in this matter. The necessary information for the purpose of regulating traffic between vehicles can be provided through the exchange of messages, in addition to the detection of dangerous sites and the warning of vehicles by sending alert messages, these technologies fall under the name of VANETs (Vehicular Ad hoc Networks) were mentioned for the first time in 2001 under the conference "Car-to-Vehicle Mobile Communications and Networking applications", where networks can be formed and information transferred between cars. The vehicle to vehicle roadside communications architecture will coexist in VANETs to provide road safety, navigation, and other roadside services to reduce traffic congestion. So, the impact of the silent period on the performance of existing privacy systems is investigated in this thesis. For our investigation in the automotive context, we evaluated a privacy focused framework named "Prext." Depending on the approach, we discovered different values for the ideal silent period.

To discuss and study the aforementioned issue. We have organized our thesis as follows:

-In the first chapter, we provide an introduction to the vehicular environment.

-In chapter 2, we detail the privacy aspects and present different existing solutions.

-In chapter 3, we will conduct a simulation study that enhances the effect of silence time in changing pseudonym while deducing the best values for protecting user privacy.

- Finally we conclude our thesis and we provide future perspectives.

Chapter1 Introduction of vanets

1.1 Introduction:

With the rapid advancement in the automotive industry, vehicles are now coming with equipped sensors, onboard units, and other processing as well communication capabilities.VANETs has come into existence because of this advancement and has offered various research dimensions to the industry. VANET, considered as a distinct type of Mobile Ad Hoc Networks, holds the opportunity to make people's life and death decisions by predicting and helping the drivers and other people about the road safety and other critical conditions
One of the significant applications of VANET includes providing safety-related information to avoid collisions and offering warnings related to the state of roads and intersections. Also offering new comfort services to passengers, which makes driving more pleasant.
In this chapter, we present vehicle technology and its promising applications. Next, we describe the attacks on VANETs, and finally we review standardization work and the various projects and research groups in the VANET community.

1.2 Why vehicular networks ?

Vehicle networks were introduced to solve two main problems :

1.2.1 Road safety problem

Road traffic injuries constitute a significant health and development problem. Over 3700 people die on the world's roads every day. Every year the lives of approximately 1.25 million people are cut short as a result of a road traffic crash[1]

1.2.2 Economic problem

Economic cost of traffic congestion is one of the most debatable issues. Traffic congestion makes both public commuters and private motorists spend additional time on the roads, paying extra for fuel. Intelligent road traffic management will certainly reduce annual expenses.[2]

1.3 What is a VANET network

In the last decade, mobile communication techniques have transformed the automotive industry by providing anytime-anywhere communication between different devices. This ease of communication allows the exchange of valuable information between devices just on the go (see Figure 1.1)

Among these advancements, the concept of Vehicular Ad-hoc Networks (VANET)came into the limelight, which has opened new possibilities to use safety applications. VANET refers to a network created in an ad-hoc manner where different moving vehicles and other connecting devices contact a wireless medium and exchange useful information.

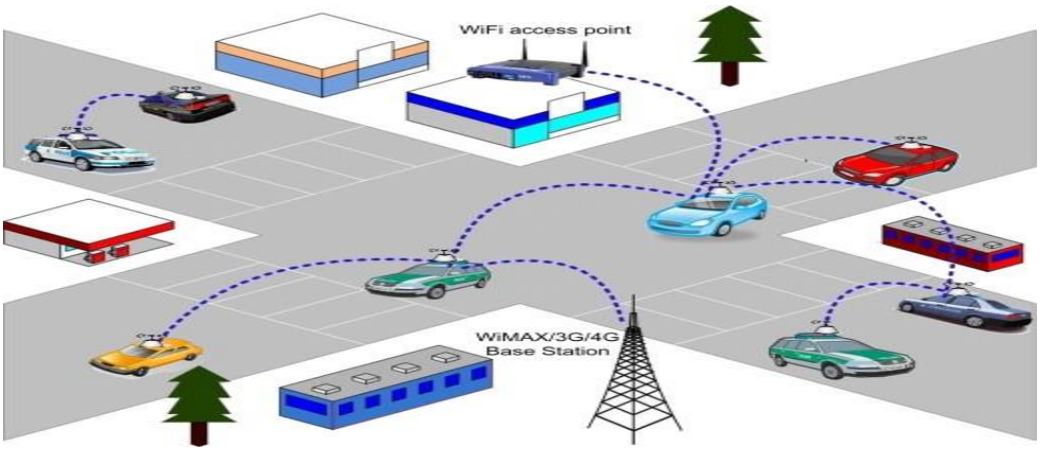

Figure 1.1 Example of a VANET*[3]*

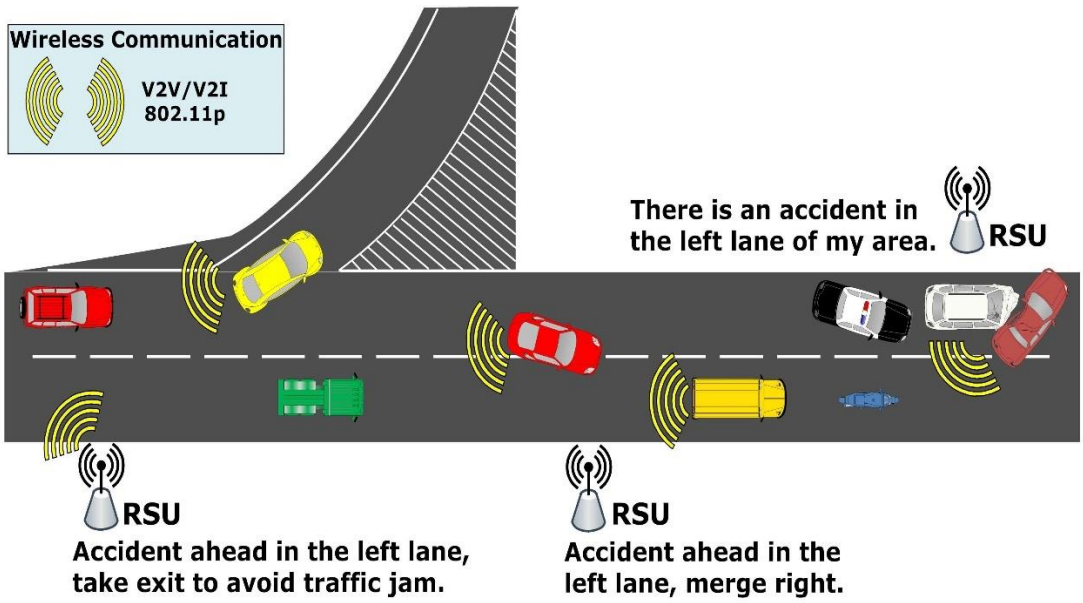

Figure 1.2 Alert message example

1.4 VANET network applications

Vehicular ad hoc networks (VANETs) have become a hot research area over the past few years. The main purpose of VANETs is to improve traffic safety, traffic efficiency, and driving comfort. Particularly, traffic safety attracts the great attention of government, academia, and industry because it is the most critical aspect of VANETs related to human lives. Therefore, many safety applications in VANETs have been proposed and investigated. However, how to guarantee the reliability of safety applications in VANETs is a big challenge, considering the nature of vehicle mobility and ad-hoc connection, we try to provide an overview of VANETs for safety applications, and for the purpose of illustration, VANET applications may be divided into :**[4]**

1.4.1 Road safety applications

To improve road safety, traffic efficiency, and driving comfort, governments have been investing research on Intelligent Transportation System and enhancing infrastructure construction. Recent technical breakthroughs in electronics, computing, sensing, and wireless communications have been promoting ITS development significantly. Vehicular ad hoc network which is a subclass of Mobile Ad Hoc Network (MANET), is one of the key enabling components in ITS. The primary objective of VANET is to establish wireless communications among a large number of vehicles in an ad hoc manner without central control. Vehicles can communicate with each other directly.

The United States Department of Transportation (DOT) estimated that VANET could avoid 81% of unimpaired light vehicle crashes in the United States[5]. In addition to improving transportation safety and traffic efficiency, VANET can also support infotainment applications to improve driving comforts.

1.4.2 Traffic management applications

Another application for VANETs is to tackle road congestions and provide the best route to a driver with updated road conditions. In this application, the vehicles could serve as data collectors and transmit the traffic condition information for the vehicular network. The information can be relayed by vehicles traveling in the other direction so that it may be propagated faster to the vehicles toward the congestion location. In this way, the vehicles approaching the congestion location will have enough time to choose alternate routes.

Crossing intersections in city streets can be tricky and dangerous at times. Traffic light scheduling can facilitate drivers to cross intersections and avoid congestions. The use of Visible Lighting Communications (VLC) can provide a

valid technology for communication purposes in VANETs, that can be used to automatically adjust the speed of the vehicle and inform the driver of the potential occurrence of a frontal collision condition or an intrisection(see Figure 1.3).[6]

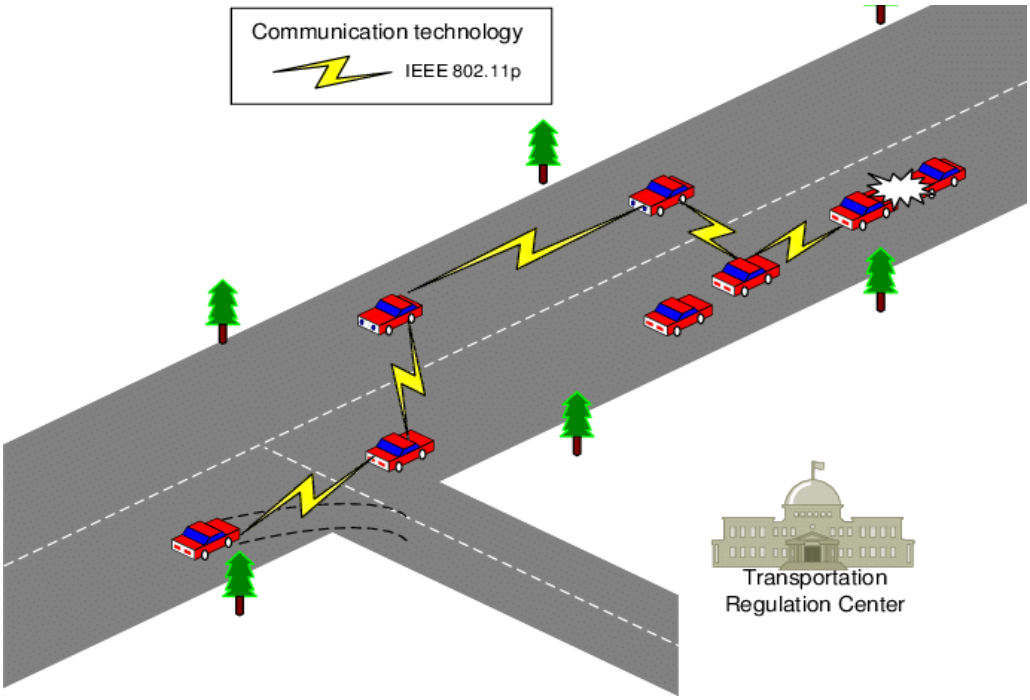

Figure 1.3 Safety application

1.4.3 Comfort and infotainment applications

VANET network applications aim to provide the road traveler with information support and entertainment to make the journey more pleasant. These applications include instant messaging, file sharing, video streaming, and online gaming, Internet access, using individual terminals next to their seats (see Figure 1.4), Finding the closest fuel station, restaurant...etc

Figure 1.4 An example of comfort applications in VANETs [7]

1.5 Communication modes in VANETs

The existence of this kind of network opens the way for a large range of applications for solving several traffic problems and for working in providing the drivers with new and useful services. There has been significant interest and progress in the field of vehicular ad hoc networks (VANETs) in recent years. Intelligent Transport System (ITS) is the major application of VANETs. Vehicle-to-vehicle communication is an important factor for safe driving applications such as blind crossing, prevention of collisions, and control of traffic flows. These applications require exchanges of vehicle information such as vehicle position, cruising speed, direction, and steering angle. In VANETs, the main network nodes are the smart vehicles and the roadside infrastructure units (RSUs) that are enabled to communicate with each other through the vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) communications.Vehicles can use one of these modes or combine them if they cannot communicate directly with the infrastructures. In this section, we give the principle and the utility of each mode：

1.5.1 Vehicle-to-Vehicle communication mode (V2V)

Greedy approach requires that the intermediate node position itself, position of its neighbor, and destination position. The goal of these protocols is to transmit data packets to the destination as soon as possible; that is why these are also known as min delay routing protocols. Various types of position-based greedy V2V protocols are GSR, GPSR, SAR, GPCR, CAR, ASTAR, STBR, CBF, DIR, and ROMSGP.

1.5.2 Vehicle to Infrastructure communication mode (V2I)

This mode of communication allows a vehicle to communicate and exchange information with the RSU (see Figure 1.5). Mainly for information and data gathering applications and other services such as Internet access, exchanging car-to-home data, traffic information, weather information, etc.

1.5.3 Hybrid communication mode (V2I)

In this scenario, a vehicle can communicate with the roadside infrastructure either in a single hop or multi hop mode,depending on the distance, it enables long-distance connection to the Internet or to vehicles that are far away.

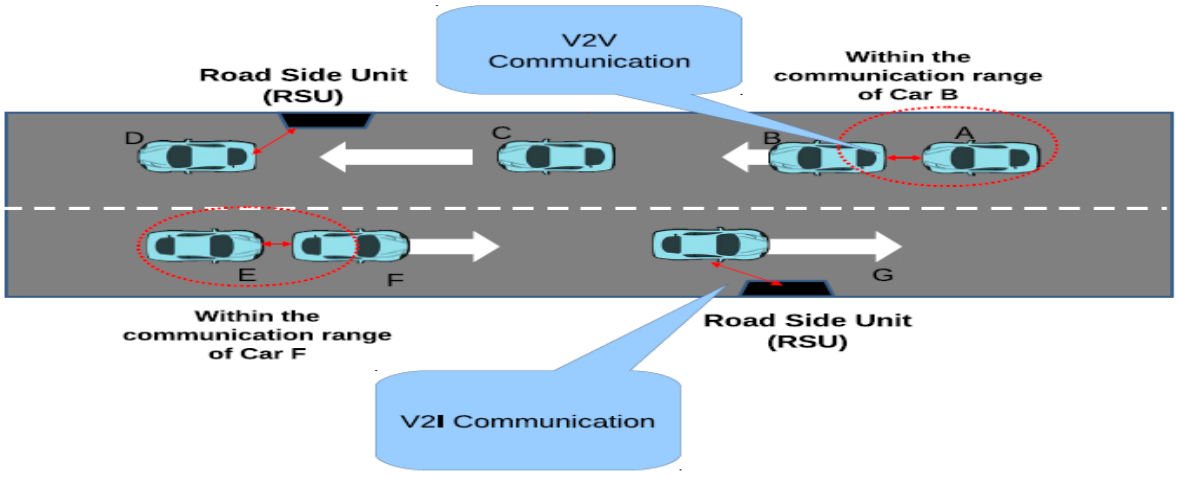

Figure 1.5 Communication modes in VANETs *[8]*

1.5.4 Vehicle-to-Road Side Unit (V2R) Communication

In this type of communication, as shown below, vehicles are able to communicate with fixed infrastructure alongside of the road in order to provide user communication and information services (see Figure 1.6).

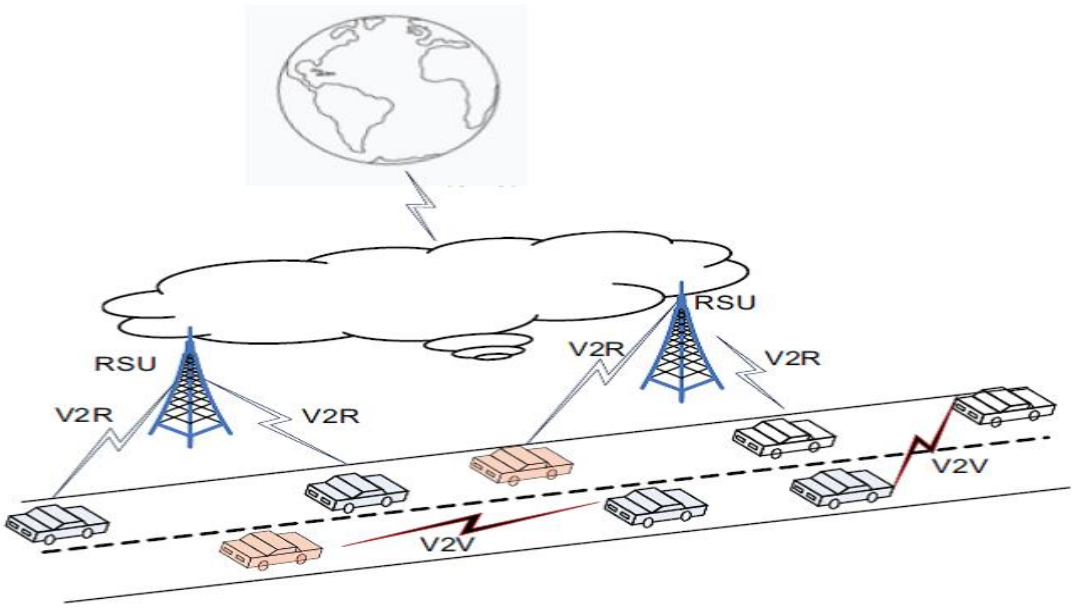

Figure 1.6 Vehicle to Road Side Unit Communication

1.5.5 Vehicle-to-Passenger communication mode (V2P)

This communication mode was introduced to allow the exchange of safety messages between vehicles and pedestrians using phones or any wireless, intelligent device. This kind of messages may contain information about pedestrians approaching the road and vehicles in return send warning messages to their smartphones (see Figure 1.7)

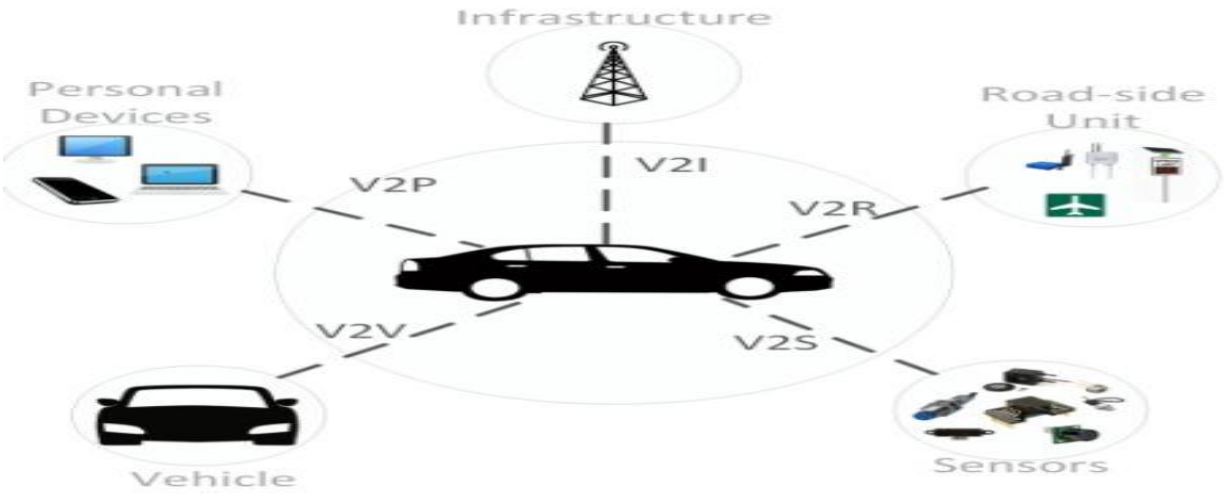

Figure 1.7 Vehicle modes communication

1.6 Beaconing

It is a periodic one-hop link-layer broadcast messages called (Beacons) diffused by each vehicle to other nodes in its radio zone to inform then about: identity, the geographic position, speed and direction (see Figure 1.8)

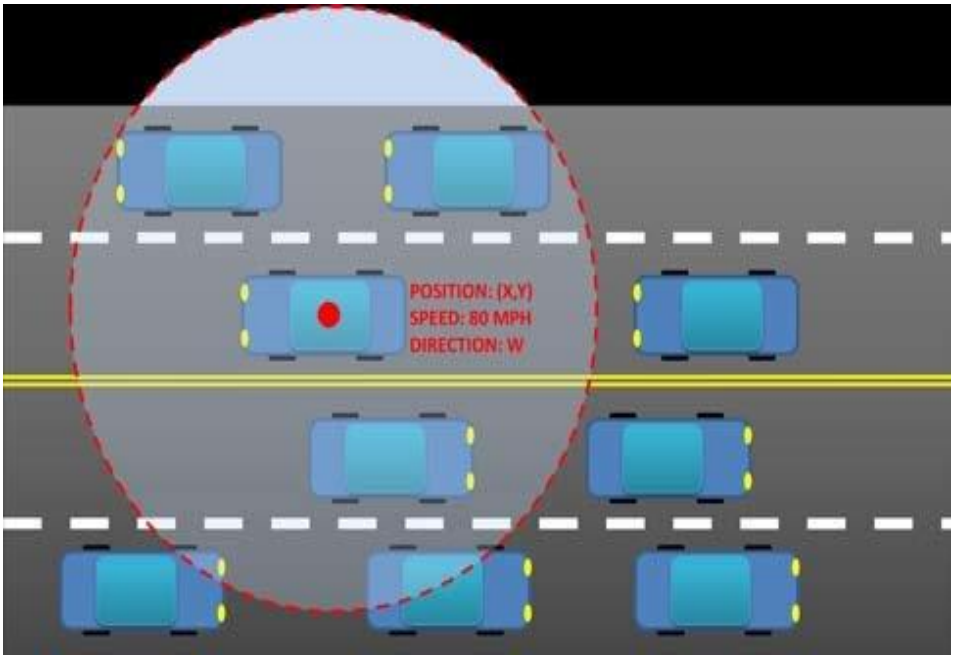

Figure 1.8 Beaconing in VANETs

1.7 VANETs charactrestiques

VANET is an application of MANET, but it has its own distinct characteristics, which can be summarized as:

- **High Mobility:** The nodes in VANETs usually are moving at high speed. This makes it harder to predict a node's position and making protection of node privacy.
- **Network topology**: Due to the high node mobility and random speed of vehicles, the position of a node changes frequently.
- **Unbounded network size**: VANET can be implemented for one city, several cities, or for countries.[9]
- **Frequent exchange of information:** The ad hoc nature of VANET motivates the nodes to gather information from the other vehicles and roadside units.
- **Wireless Communication**: VANET is designed for the wireless environment. Nodes are connected and exchange their information via wireless.
- **Unlimited Battery Power and Storage**: Nodes in VANETs do not suffer power and storage limitation. With the large data processing and storage capacity, complex arithmetic and cryptographic operations can be implemented to ensure the security and proper functioning of these networks.
- **Real-time constraints:** At the time of emergency, delivery of data requires a very short time transmission. This limits the choice of tools and techniques to use during the design of a protocol for VANETs.

- **Exchange of frequent messages**: In VANET networks, vehicles must periodically send beacon messages, which requires frequent data exchange between different vehicles.

1.8 Security and privacy in VANETs:

The fundamental security requirements of VANET should include authentication, integrity, and nonrepudiation. In some specific scenarios, confidentiality should also be provided against attackers. In addition, users' privacy, such as identity and location history, is sensitive information and should be preserved against illegal tracking and user profiling for advertisements. Otherwise, it would cause hesitation for users to welcome the convenience of VANET at the price of their privacy. Nonetheless, law enforcement authorities still need some degree of traceability of vehicles and users for liability issues upon accidents or crimes.

In this section, we present security requirements for VANETs; then we give the types of attacks. Finally, we describe the different categories of attacks against VANETs.

1.8.1 Security requirements for VANETs

This section discusses the proposals that focus on a specific area of VANET security.A security system in VANET should satisfy the following requirements[10]:

- **Integrity Metrics for Content Delivery:** Content delivery is one of the core services of VANET applications. It should provide timely and accurate information for drivers in order to enhance safety and enrich travel experiences. Due to the distributed, wireless and open nature of the vehicular network, its content delivery faces serious security

challenges, and common security metrics are needed to measure the effectiveness of VANET security measures and thusly to assure users confidence in adopting and participating in the network.

- **Authentication**: It imposes that each participating entity should have its credential of communication, as it ensures that the messages are sent by the actual nodes and that recipients can identify their origins.
- **Availability:** It provides an adequate quality of service to access the resources of the vehicle's network.
- **Confidentiality:** When we talk about the confidentiality of information, we are talking about protecting the information from being exposed to an unauthorized party due to a data breach or insider threat. This can be done by using data encryption.
- **Privacy:** This system is intended to hide the identity and geographic location of nodes and other information that endangers the privacy of users.
- **Non repudiation:** In this security-based system, a sender cannot deny the fact of having sent the message.
- **Data verification:** it is used to eliminate misleading messages. This is mainly used for detecting correctness of date and check whether the sender is legitimate or especially between neighboring vehicles
- **Access control**: It ensures that all nodes access the resources according to determined rules and privileges.

1.8.2 Attackers in Vehicular Networks:

Attackers can be classified according to the following three types:

- **Malicious or Rational:** Malicious attackers have no personal benefits to attack. They just harm the functionality of the network. However,

rational attackers have their own personal profit; hence they are predictable.

- **Active or Passive:** The passive attackers simply listen to the data exchanged in the network, while the active attackers intercept the connection and modifies the data

1.8.3 VANETs attacks:

Attacks refer to any malicious activity performed on a system that has an adverse effect on the network. The basic idea behind performing these attacks is to get the secret information in the network or to degrade the systems normal functioning so that it does not work correctly that leads to various threats These attacks fall under [11]:

1. **Availability:** Availability is one of the basic factors for VANET. This assures that useful information is always available when the system is communicating, and the network is functional. It is one of the crucial security requirements for vehicular networks whose aim is to ensure user's lives, and it is the main target for attacks by attackers. Some of the attacks on availability are :

- **DOS:** It is an attack in which the resources and the services are made inaccessible by an attacker to the users in the network and is done by either making the channel busy or by "Sleep Deprivation."
- **Malware:** In this type of attack, an attacker consumes the bandwidth of a network by sending spam messages in the network and increase the latency of data transmission.
- **Broadcast tampering attack and Black Hole attacks:** In a broadcast tampering attack, an attacker tries to provide and send wrong messages as emergency messages in a network that hides the actual safety

messages to authorized users in the network, which can cause accidents and severe effects in a vehicular ad-hoc network.

In VANET networks, a black hole is formed when traffic is redirected to one or more nodes that do not link these packets to their destinations. The intruder, once chosen as a transitional node, drops the packets instead of forwarding them, causing a black hole in the network. This attack is very dangerous because the attacker will have significant control over the network (see figure 1.9). [12]

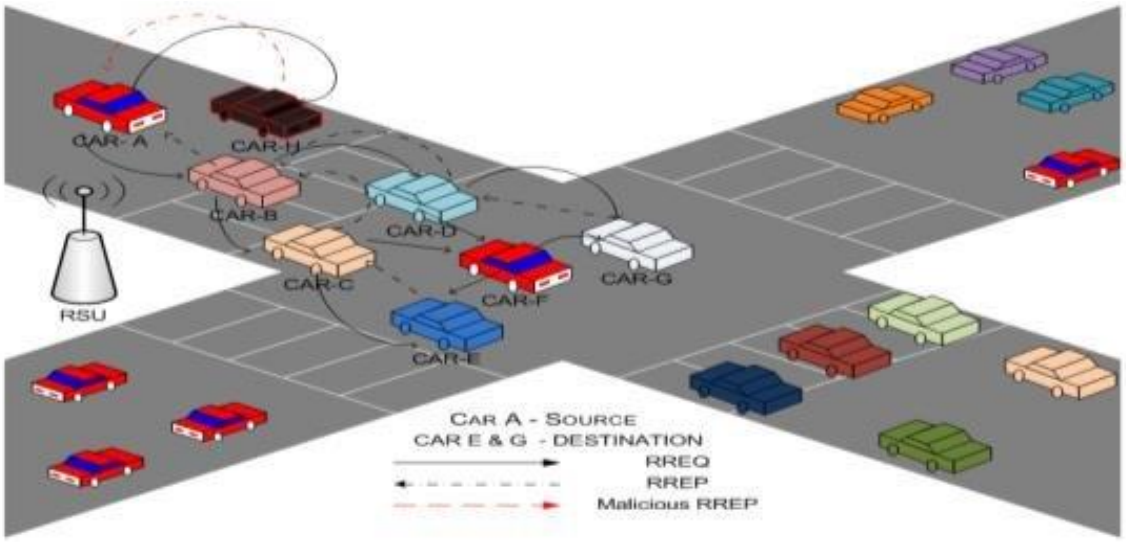

Figure 1.9 Blackhole Attack

2. Authenticity and Identification:

Authentication with other appropriate mechanisms avoids communication with nodes having a false identity, illegitimate retransmission of the message and injection of incorrect information. These attacks include:

- **Sybil Attack:** In this type of attack, an attacker provides an illusion to nodes of many vehicles on the road thus they can change their route for the attackers' goal [13].

- **Relay Attack:** This type of attack involves capturing and replaying the packet to distract the authorities and protect the identity of nodes in an accident.
- **GPS spoofing/position-faking:** Location information is of great importance in the vehicular network,Thus information must be right and authentic. In this type of attack, an attacker provides the neighboring nodes with wrong location information so as to hide its actual position information that is confidential.
- **Tunneling:** This type of attack involves connecting two different parts of the vehicular network by using an additional communication channel such as a tunnel.
- **Key/Certificate Replication:** This attack consist of the use of duplicate keys and certificates, which are used as proof of identification which makes it more difficult for certified authorities to identify a vehicle, particularly in case of accidents.

3. Confidentiality

It contains tow types of attacks :

- **Eavesdropping attack:** This type of attack is against confidentiality. In this attack, an attacker attempts to get useful information in a network such as location, private information of nodes that can be used for tracking vehicles and to perform various attacks[11].
- **Traffic analysis attack:** One of the serious hazards to confidentiality and privacy is the traffic analysis attack in which attackers analyze the collected information and tries to get the useful information as much as possible for its own purpose.

1.9 Type of messages :

In VANETs, network participants can exchange messages that can be categorized into the following main classes:

- **Safety messages :** They are called beacons and are usually generated periodically within T ∈ [100ms, 1000ms].These messages comprise information about speed, geographic position, and the direction of the vehicle. The exchange of such messages between neighboring vehicles allows building a local view of neighbors (Figure 1.10) It will help to anticipate hazardous accidents and other dangerous situations. The beacon messages also provide essential information for building optimized and efficient routing tables.

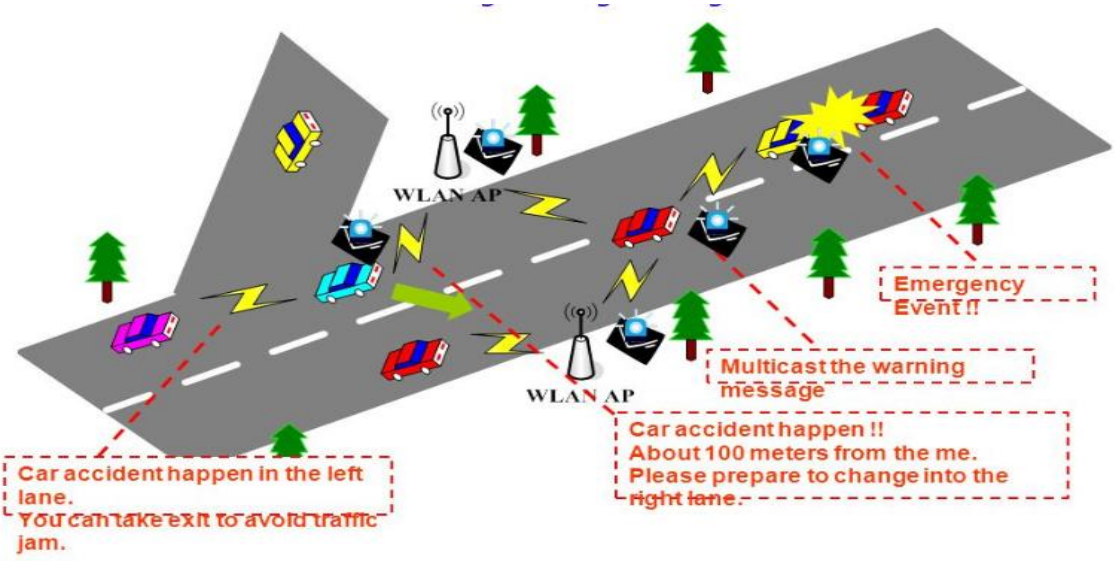

Figure 1.10 Safety message

- **Alert messages:** They are generated each time an event is detected. It can be an accident, an obstacle or even getting an alert message from a neighboring vehicle. These messages are expected to be re-broadcast repeatedly to ensure that all vehicles in the vicinity are aware of the dangerous situation . The size of an alert message is optimized to ensure quick delivery and avoid overwhelming the network

- **Other messages:** They include different messages , control messages, financial transactions, or messages related to infotainment applications.

1.10 Conclusion

VANETs are promising networks with a wide range of applications. Nowadays, vehicular networks are being developed and improved. Several new applications are enabled by this new kind of communication network. However, as those applications have an impact on road traffic safety, security is the main concern of designers due to the importance of the data exchanged. Thus, strong security requirements must be achieved.

Chapter2 Techniques of Pseudonym changing in VANETs

2.1 Introduction

VANET's are expected to be able to store a lot of information including personal data of the vehicle's owners or drivers which has to be considered. Such private information should be protected especially in vehicle communications which must be anonymous, and in security related applications that require authentication of messages and their origins.

Frequently changing pseudonyms is commonly accepted as a solution to protect the privacy in VANETs. The use of pseudonyms involves users acquiring another identity instead of their real identity. Indeed, the identities of the attackers who cause the system to malfunction must be identified for the purpose of revocation and legal proceedings. Thus, it is essential to also have the possibility of correlating the real identity to that used in the VANETs. This requirement is known as ”conditional privacy”. The identity management is a complex problem with the presence of social, ju- ridical, economic constraints and others related to road safety.

A lot of research has been devoted to solve the problems related to this subject. In this chapter, we describe the current operation of vehicle identification. Then we present the problem of privacy in VANETs.

2.2 Protection problems in VANET

When we mention the Vanet network that revolves around the exchange of messages periodically in order to increase the contextual awareness of cars and drivers, But these messages may negatively affect the integrity of the network because they show the identity, location, and privacy information. The path of the target cars can be monitored. This feature is known as "Big Brother Syndrome" [14].

2.3 Pseudonyms privacy:

For privacy-friendly message authentication, a scheme of changing pseudonym short-lived pseudonym certificates, which do not contain any information about their holder,any incoming messages that do not bear a valid signature are discarded. To prevent tracking based on pseudonymous identifiers, pseudonyms are changed "every once in a while", a multitude of different pseudonym systems has been proposed[15].

2.4 The effect of pseudonyms on the safety of privacy in VANET

Digital pseudonyms were used as a public key to verify the signatures made by the owner of the private key in order to conceal the identity of electronic transactions.

So we can conclude that a pseudonym should be used for authentication, but it should not contain any personal information that can be linked to the true identity of the owner of the pseudonym. On the other hand, several pseudonyms can be used to ensure that the identity of the user is not revealed, or a different pseudonym can be used for each procedure(see Figure 2.1)0

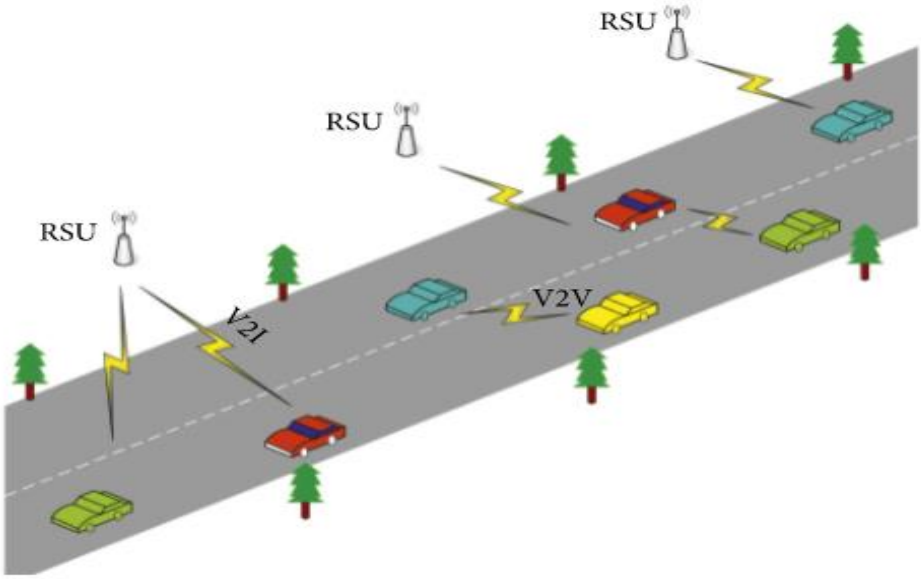

Figure 2.1 Pseudonym Changing Authentication in VANETs

2.5 System model and scenario

We assume an inter-vehicular communication system with the following entities:

1. Participating vehicles Vi equipped with a V2X onboard unit that periodically emits CAM messages while they travel. All messages are signed using pseudonym certificates, which are changed according to the pseudonym change strategy and its parameters. Vehicles start broadcasting messages when they begin their trip and stop when they reach their destination.

2. An adversary that tries to track participants as they travel through the scenario. In particular, his goal is to link their trips' origin and destination (see figure 2.2).

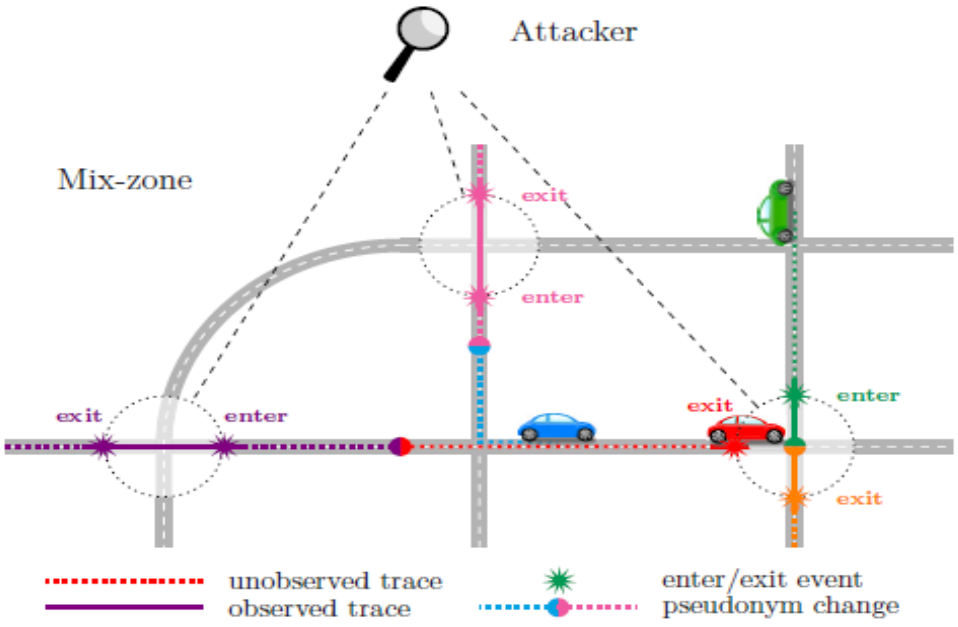

Figure 2.2 Vehicles leaving a trace of messages

2.6 Pseudonym strategies examples

Reusing pseudonyms can be the best option if a vehicle has used up all its pseudonyms and is unable to load fresh ones, e.g., because no cellular

connection is available. However, reusing a small pool of pseudonyms entails the risk that an attacker learns and links all of a participant's pseudonyms, rendering his future changes (using the same pseudonym pool) ineffective [17]. In this work, we investigate a case where the pseudonym pool is so large that pseudonym reuse does not occur, which gives us an upper bound of privacy protection that users can expect.

2.7 Classification of pseudonym systems

There are many basic systems of pseudonyms among them:

2.7.1 Cryptography systems: Is a type of public-key cryptography that allows the use of a public identifier of a user as the user's public key .This allows to avoid exchanging large crypto- graphic information

2.7.2 Pseudonym systems based on group signatures: These systems provide a private key to several groups of vehicles, which requires a signature on their behalf. In addition, we can verify this signature using a corresponding public key.

2.7.3 Symmetric cryptography: These systems are based on the principle of knowing the secret key between the two parties sender and receiver.

2.7.4 Asymmetric cryptography system: It acts as a representation of pseudonyms by means of public keys. A certificate must be sent with a pseudonym with a message to help verify messages directed towards vehicles.

2.8 Modes of action of the attacker

The attacking methods were classified into the following categories:

1. Single Position Attack: The attack depends on the attacker's guess by conducting analysis and methods of the location and identity of the

nodes(Figure 2.3)

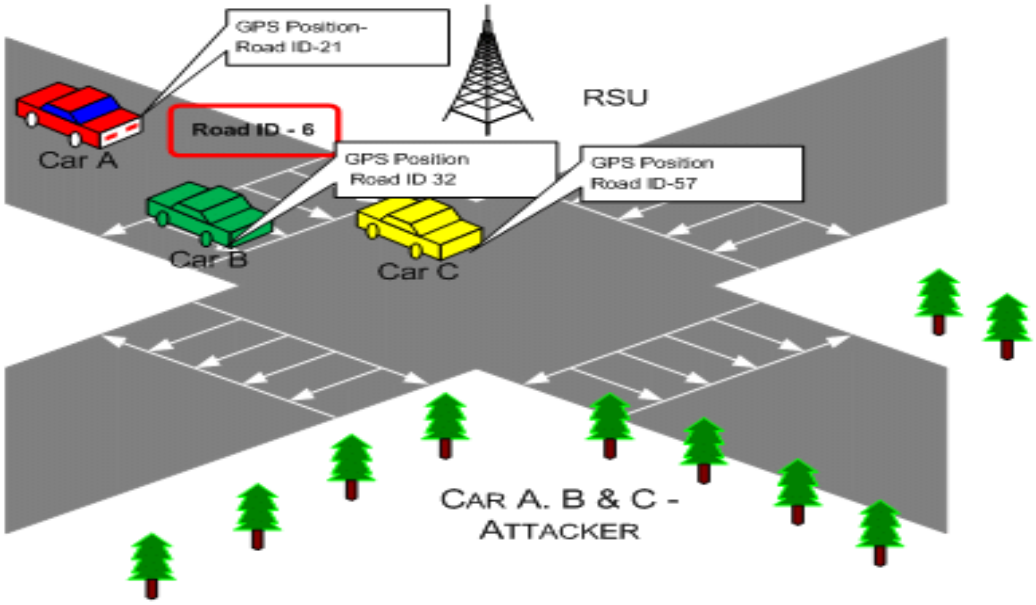

Figure 2.3 Example of single position attack

2. Multiple Position Attack: In this attack, the attacker tries to track and correlate several positions to establish the full path traveled by a node to decrease its privacy.

3. Compromised TTP: If the attacker managed to penetrate the place, he could access and read the user's data, thus affecting the privacy of a network and users of VANET at risk.

4. Context Linking Attack: It works on using the personal information of the user of all kinds in order to create a file containing the user's activity to facilitate the success of the attack.

2.9 The pseudonymity requirements in VANETs:

Protecting the privacy of users in vehicular networks is of major concern Achieving this goal necessitates the following requirements:

- **Minimum disclosure:** The user should only use the necessary information to communicate, not to publish information that might

affect the user's privacy and network safety.

- **Unlikability:** It requires that the relation between two or more pseudonyms should not be found.
- **Conditional anonymity**: This latter is based on not revealing the identity of the sender among a number of senders because the user's identity must be resolved in the event of a conflict problem.
- **Perfect forward privacy:** When performing pseudonymization, consideration must be given to maintaining the confidentiality of other users' information and the real identity of nodes.

To protect privacy, we mention the features that must be provided in the pseudonym:

1- **Determine the life span:**In order to prevent tracking, a pseudonym must have a limited lifetime. This characteristic can be guaranteed in the certificate accompanying the pseudonym.

2- **The Abundance:** In this feature, the new pseudonym must be available for any change that may occur to the pseudonym.

3- **Pseudonym change block:** The ability to block pseudonym change is needed to ensure resilience against attacks and safety levels.

4- **Link to other identifiers:** When a pseudonym is changed, all the other identifiers used by the same vehicle have to be changed as well. For example, in the ETSI Reference Architecture[18], the geonet working identifier is derived from the pseudonym.

2.10 Pseudonym lifecycle

Many pseudonym schemes have been introduced because privacy in the network requires that the main goal of using pseudonyms is to authenticate the sender. The following document refers to the life cycle of the pseudonym.

We can verify this by certifying the sender as the active element in the group. The main stages are summarized in the following figure(Figure2.4).

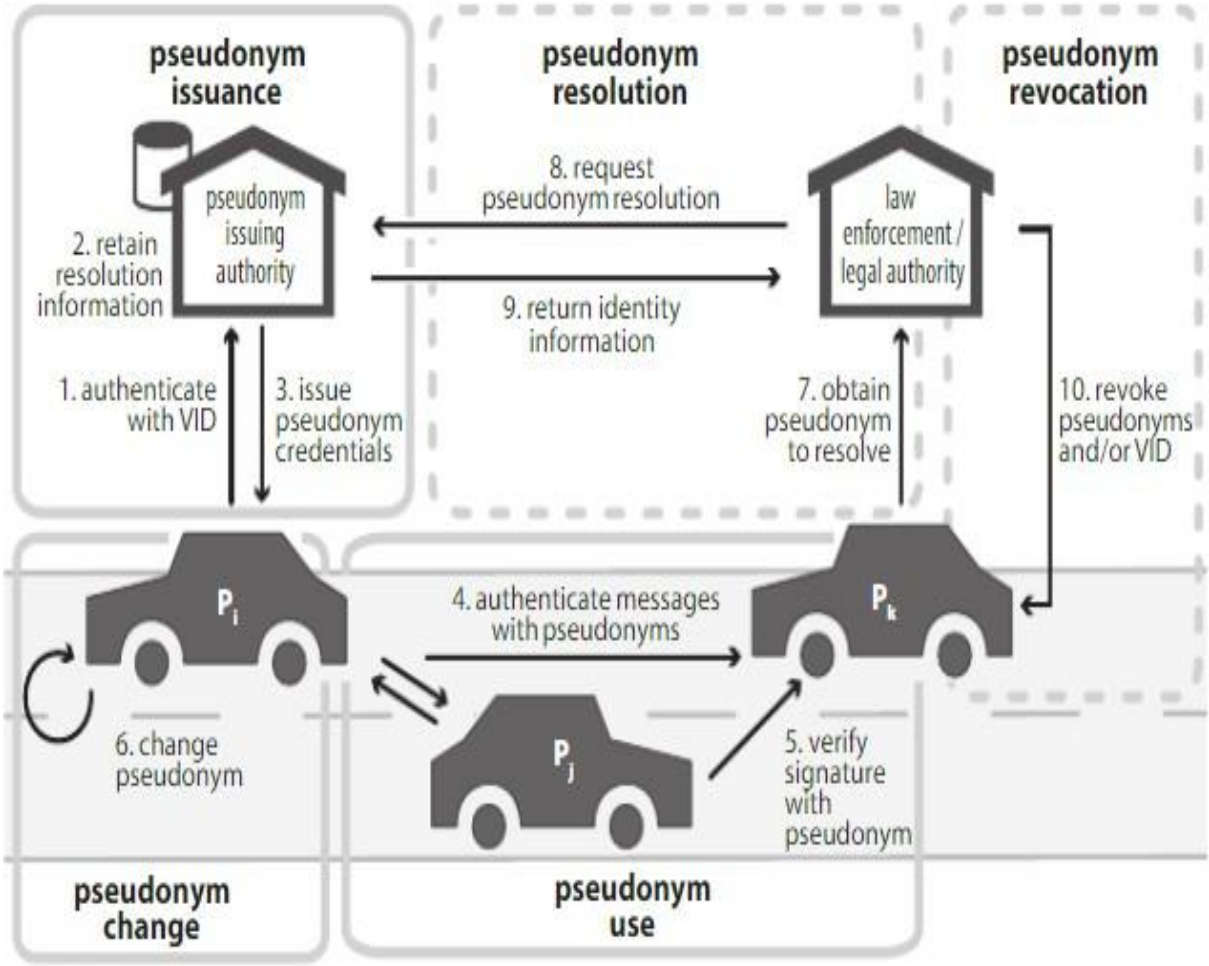

Figure 2.4 Pseudonym life cycle*[18]*

We define and discuss each phase and point out their specific challenges:

1. Pseudonym Issuance: Almost all pseudonymous authentication schemes for vehicular communications assume that a vehicle has a unique digital identifier. This vehicle ID (VID) can be seen as a signed certificate that allows to unambiguously authenticate a vehicle. Similar to the vehicle identification number (VIN), which is embossed onto the vehicle chassis by the manufacturer, the VID is a long-term identifier assumed to be pre-installed in a vehicle's OBU [19]. The VID could be issued alongside the vehicle registration and license plate by a vehicle registration authority, such as the department of motor vehicles (DMV). Therefore, the VID is also referred to as an electronic license plate. Although the VID is required for pseudonym issuance by most pseudonym schemes, the issuance of the VID itself is typically not considered part of the pseudonym scheme or pseudonym lifecycle because they are separable processes.

Pseudonyms are typically assigned an expiry date or validity period. Validity periods or short expiry dates limit the number of pseudonyms available to a vehicle at any given time in order to prevent Sybil attacks. The unlikability property of pseudonyms prevents receivers from knowing that these messages originated from a single node without performing additional plausibility checks, such as position verification. Thus, the adversary could try to propagate a specific viewpoint in the network to obtain an advantage on the road. For example, a greedy driver could simulate congestion on a stretch of road in order to clear the path ahead.

2. Pseudonym Use: It indicates that when the car gets pseudonyms, it can communicate with other vehicles, but the received and outgoing messages must be verified, as they are the most important steps in using the pseudonym. The authentication of the vehicle's own messages allows other nodes to authenticate the sender as a vehicle with valid credentials. Message integrity

must be protected to prevent modification of messages in transit. The message authentication scheme must also provide replay protection. Sender authentications, message integrity, and replay protection essentially corroborate the reliability of received information, which may then be used for safety-critical decision-making [20][21].

3. Pseudonym Change: The basic elements of the network must be changed, such as I.P. and MAC address, because there are no problems between the new and old pseudonym.As shown in Figure 2.5, changing the pseudonym alone is not sufficient for confusing an observer if that observer is able to monitor locations before and after the area in which the pseudonym change occurred (i.e., the observer will be able to link the new pseudonym Z to vehicle A).

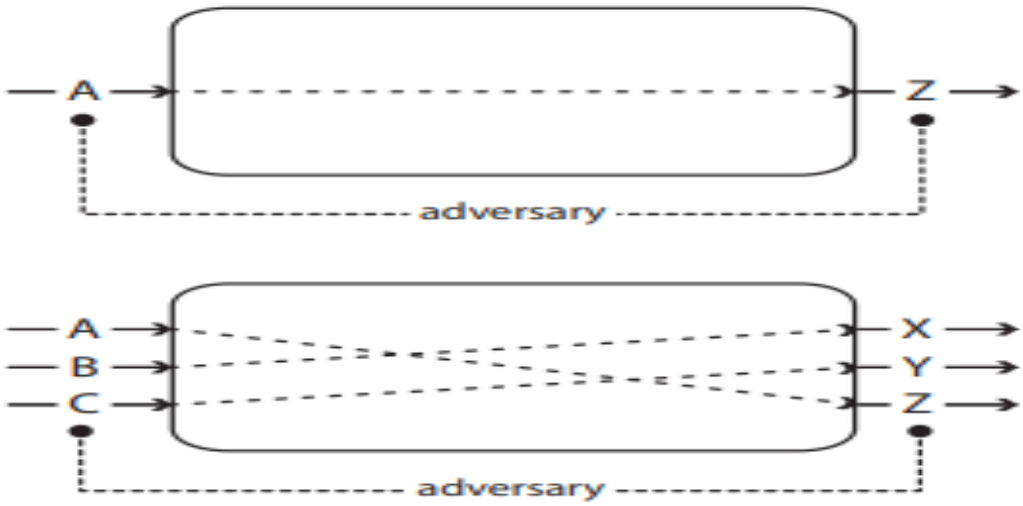

Figure 2.5 Necessary context for effective pseudonym change

4. Pseudonym Resolution (optional): means only relevant for holding malicious nodes accountable. In case of misbehaviour detection, Law enforcement representatives pose a pseudonym resolution request to the pseudonym provider to obtain the pseudonym holder's VID. This is to improve the privacy of VANET users.

5. Pseudonym Revocation: To ensure the safety of the network, it is necessary to cancel the harmful ones, which means revoking the authentication data. If we specify some pseudonyms in order to cancel them, then there are other possible pseudonyms. If we cancel them all, this negatively affects the privacy of the network and leads to its weakness.

2.11 Ways to change the pseudonym

Since changes in the pseudonym are not sufficient to limit tracking for Burmaster and several researchers[22], the car must change its MAC address and IP address. Also, strategies and methods for changing have been proposed, which discusses as follows:

1. Fixed time change (periodic): In this strategy, a vehicle changes its pseudonym according to a fixed, periodic schedule. Using fixed time extension, instead of changing a large number of pseudonyms, each vehicle saves a set of pseudonyms during the period of time, the number of times the last change is determined. The benefit of this technology is that the car always has a pseudonym.

2. Random change: In order to solve the issue of fixed periods, vehicles can change their pseudonym randomly. As a result, an adversary cannot predict the next pseudonym change. However, tracking is still possible if only one or few vehicles change pseudonyms at a specific time because all other neighbors would keep the same identity. Thus, linking of new and old pseudonyms of the vehicle that performed the change is still trivial.

3. Vehicle-centric: It works on focusing on the vehicles, determines the place and time of changing the pseudonym independently. The silent period is based where the cars exchange their pseudonyms and then enter in a random silent period(see Figure 2.6).

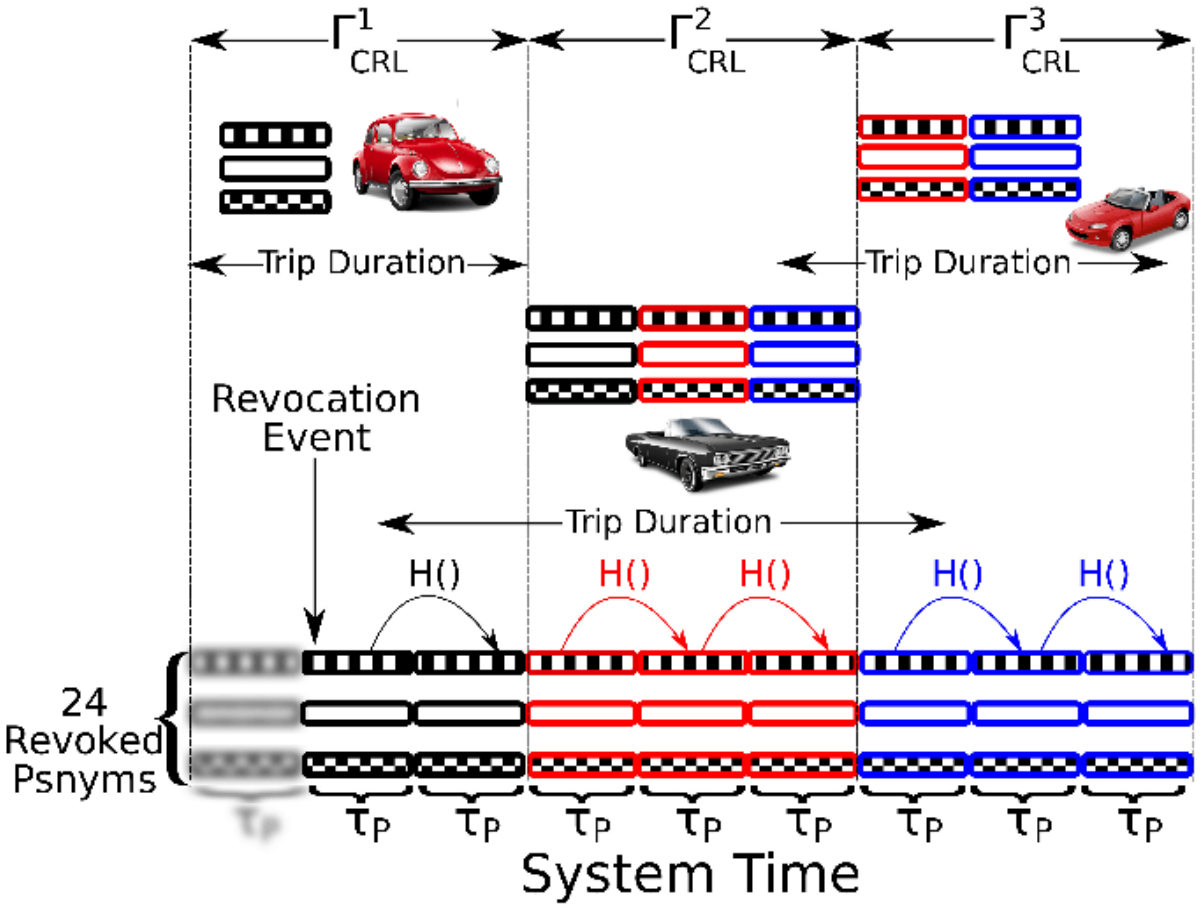

Figure 2.6 Vehicle-centric mechanism*[22]*

4. Density-based: In this strategy, the change of pseudonym depends on the number of current neigh- bors. Therefore, a vehicle can avoid the ineffective pseudonym change.

5. Silent period: In this strategy, the change of pseudonym depends on the number of current neighbors. Therefore, a vehicle can avoid the ineffective pseudonym change. the last one must be made if the size of the set of neighboring vehicles is greater than a determined threshold.

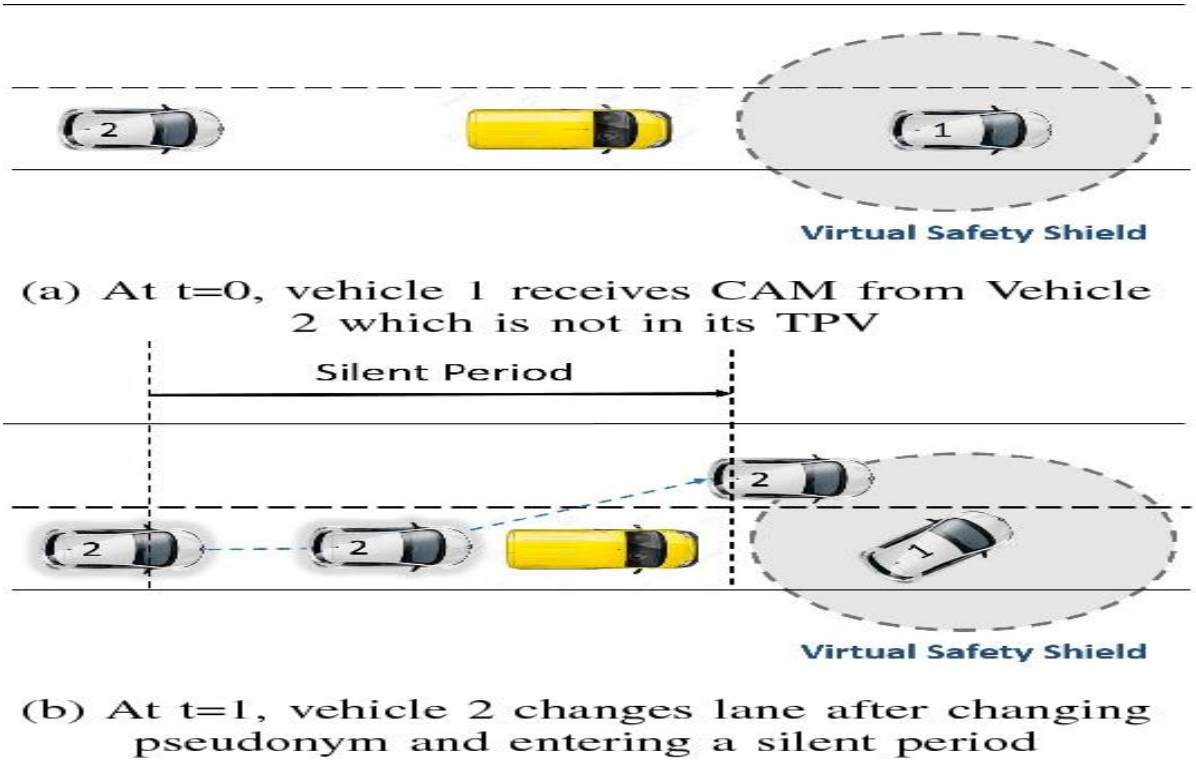

Figure 2.7 Example of the silent period

2.12 Pseudonym revocation systems

As a result of the size of the network, changing or canceling the pseudonym is not an easy thing to mention among the heroes' systems:

1. Passive system:

It works on VID. If the identity is revoked during a large period of time, it is not possible to have a new pseudonym. By revoking the VID, the other vehicle can participate in the network until all the pseudonyms are used up. This process is known as passive cancellation. The life of the pseudonyms can be reduced to solve this problem

2. Self-revocation :

This feature is based on the principle of advance notification, which means sending warnings of a problem detected by the vehicles adjacent to the malicious node. After that, the revocation authority sends an OSR message to the detected vehicle that deletes all the pseudonyms of the malicious cars (see

Figure 2.8)

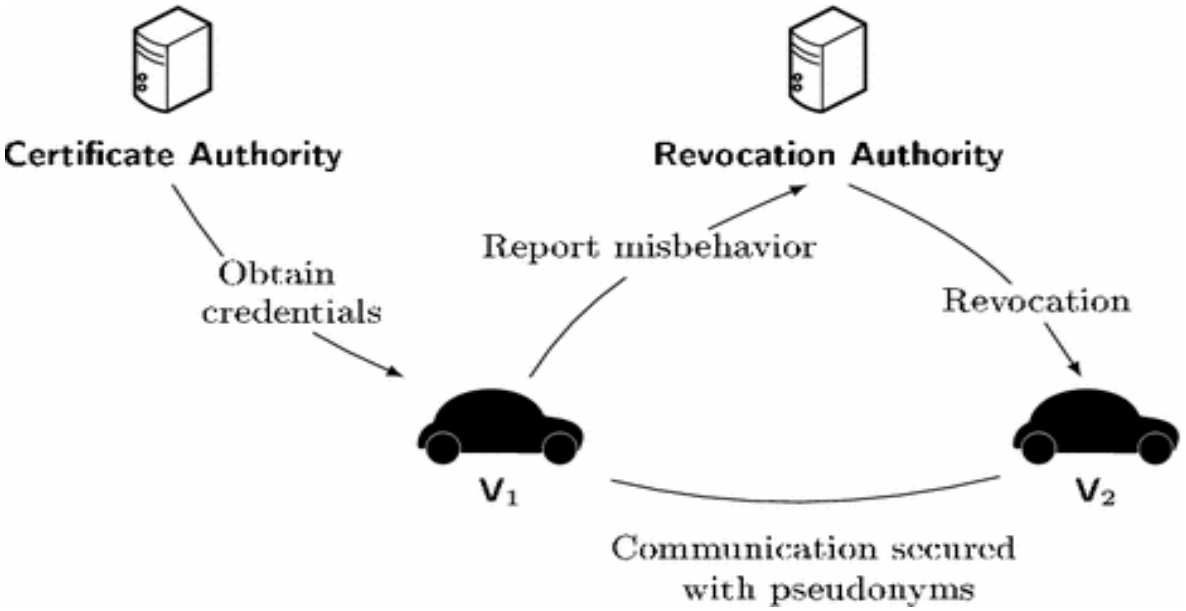

Figure 2.8 Revocation without resolution

3. Threshold based pseudonym revocation:

This technology relies on voting systems by calculating and canceling harmful nodes. This method is characterized by speed, but on the other hand, it may create problems of anonymity because pseudonyms have a life cycle that affects several technologies.

2.13 Conclusion

Safety-critical applications in cooperative vehicular networks require the authentication of nodes and messages. Yet, the privacy of individual vehicles and drivers must be maintained. Pseudonymity can combine security and privacy requirements. Thus, a large body of work emerged in recent years, proposing.

pseudonym solutions tailored to vehicular networks, We provided a comprehensive survey on the complex topic of pseudonymity in vehicular networks. The proposed abstract pseudonym lifecycle is applicable to the majority of pseudonym approaches for vehicular networks and facilitates

comparison and discussion of those approaches.

Chapitre3 Impact of silent period on pseudonym changing

3.1 Introduction

Economic growth and continuous increase in population in the last decades have boosted the number of vehicles on our roads. As a consequence, these roads have known severe traffic congestion and an increasing rate of accidents [23]. Thanks to the current advances in communication technologies and intelligent transportation systems, connected vehicles will enhance road safety by continuously sharing vehicles' location information through periodic messages called beacons [24]. Unfortunately, malicious entities might exploit the shared location information to build trajectories' profiles of the drivers [25]. A possible solution to this problem is to employ pseudonyms as temporal identifiers. Vehicles should change their pseudonyms inadequate situations to confuse trackers. They usually stop sending safety messages for a duration of time called silent periods. Moreover, tracking vehicles can be tricky if enough vehicles with similar contexts enter in silent periods simultaneously.

In general, these schemes provide good performance, according to the authors. However, no study has deeply studied the impact of the silent period on these privacy schemes. The silent period might improve privacy if the selected time intervals high enough. Such an option would negatively affect the network's overall performance (Vehicles are not sending safety nor control messages). Thus, an adequate silent period length should be selected. To that effect, the current study shows the impact of different silent period lengths on known privacy schemes in VANETs. Hence, we will be able to select more efficient silent periods. This study will evaluate the efficiency of different privacy schemes under different silence periods. We will compare the types of silent periods through a simulation that shows the effect of each type.

3.2 PRIVACY SCHEMES AND METRICS

Many privacy schemes exist in VANETs. Most of them use the pseudonym change concept, and they usually employ the silent period technique to create confusion and decrease traceability. In this section, we will present some of the well-known schemes briefly. Then, we present the metrics used for assessing privacy efficiency.

3.2.1 Privacy Schemes

1) **Coordinated Silent Period (CSP):**The CSP has been proposed by Tomandl et al. [27]. In this scheme, privacy actions (pseudonym change and stop beaconing) are all coordinated. Thus, each pseudonym change is performed under high anonymity levels, thanks to the simultaneity of pseudonym change. CSP is not practical due to the overhead required for the coordination, which would increase dramatically in real-world situations.
2) **Context-Aware Privacy Scheme (CAPS) :** in[28], the CAPS protocol has been proposed. The technique requires each vehicle to monitor received beacons using an in-vehicle tracker (An implemented algorithm to track vehicles). If the tracker detects that neighbor has stopped its communication (it is supposed to be in a silent period), it will enter in a silent period as well. The vehicle should select an adequate context to resume communication with neighboring vehicles. It should be stressed that the initial silent period can be triggered by a predefined timer.
3) **Random Silent Period (RSP):**vehicles under this scheme[29] operate independently of each other. When a pseudonym lifetime expires, the vehicle should cease its transmission for a random duration before using another new pseudonym. The main objective of this approach is to increase confusion and reduce the risk of traceability. Unfortunately, this

scheme suffers from the lack of collaboration between vehicles in the pseudonym change process, which will render them vulnerable to pseudonym linking attacks. Thus, it affects the privacy efficiency of the proposed technique.

4) **SLOW:** in SLOW[30],a vehicle ceases broadcasting beacon messages when its speed drops to a predefined threshold (for example, 8 m/s). Then, it should swap to a new pseudonym after a predefined interval of silence period. After that, the vehicle resumes the beaconing process and can send other messages if needed.

3.2.2 Privacy Metrics

In this section, we present some of the known privacy metrics that are used for evaluating the performance of privacy schemes.

1) **The anonymity set:** the anonymity set of a target vehicles is the set of vehicles in which a vehicle v cannot be identified or distinguished regarding its location. Thus, it represents the number of nodes that are indistinguishable from each other. For instance, when n neighboring vehicles switch their pseudonyms simultaneously at a given time t, we can conclude that the anonymity set's size is n. In this situation, the tracker's challenge is to identify the correct position of the vehicle among the locations of n members in the same anonymity set.
2) **Traceability**: it indicates the level of success of tracking attacks. There exist several techniques to measure traceability. Huang et al. [29]proposed solutions to estimate how long an adversary can continuously track a target node. They calculated the MTR (Maximum Tracking Round), representing the number of times a

target node is tracked continuously after the initial pseudonym use. They estimated the maximum tracking time by multiplicating MTR by the lifetime of the pseudonym. Using a different technique, Sampigethaya et al. [31] calculated the maximum tracking time for a given node by summing the periods in which the anonymity set size remains as one.

3.3 SIMULATION SETUP

3.3.1 Simulation environment

In this section, we will discuss the simulation scenario, the density of vehicles, the attacker model, and the simulation parameters used for each privacy scheme. A Simulation environment To perform our study, we have used a libary named PREXT[32]. It's an extension for Veins [33] framework, which runs on top of the network simulator Omnet++ [34]. The simulation scenario uses a map of Munich downtown, Germany as shown in figure 3.1. This map is extracted from the OpenStreetMap project[35]. The mobility of vehicles is generated using the Urbain mobility generator SUMO [36]. More details about the simulation environment are presented in (Table 1).

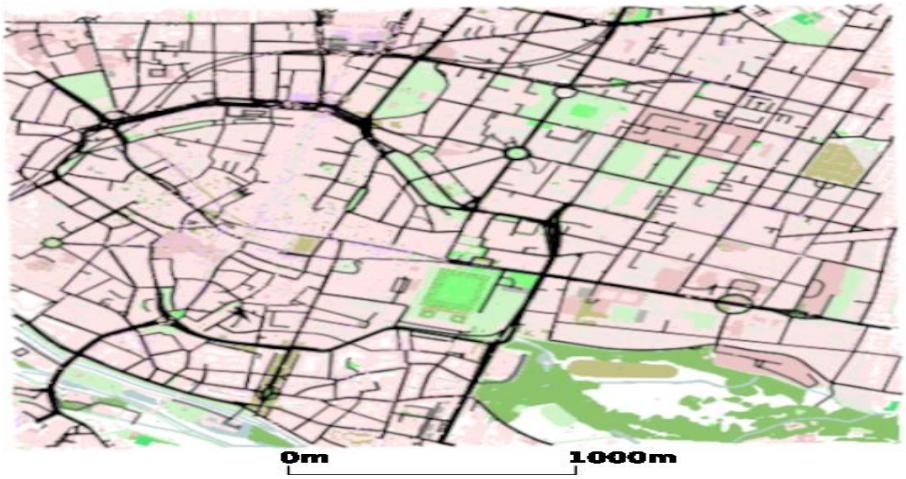

Figure 3.1 Real map of Munich

Parameters	Values
Mobility Generator	SUMO 0.25.0
Network Simulators	OMNET++ 5.2, VEINS 4.5
Vehicle Density	40, 160
Physical Layer	802.11p
Frequency	5.9 GHz
Communication radius	300m
Topologysurface	2900 x 2700 m
Number of eavesdroppers	25
BSM Interval	1 second

Table 1.1 Simulation Parameters

3.3.2 Attacker model

Several studies have shown that the number of attackers and their position affects vehicle tracking efficiency [37][38].To evaluate the considered privacy schemes in worst-case situations, we have considered a global passive adversary. This kind of attack stands on widely placed listening eavesdroppers to collect vehicles' beacons. In our scenario, a group of 25 eavesdroppers is intelligently placed to cover most of the simulation area. The reception range of eavesdroppers is set to 300m the position of eavesdroppers, as well as their coverage range.

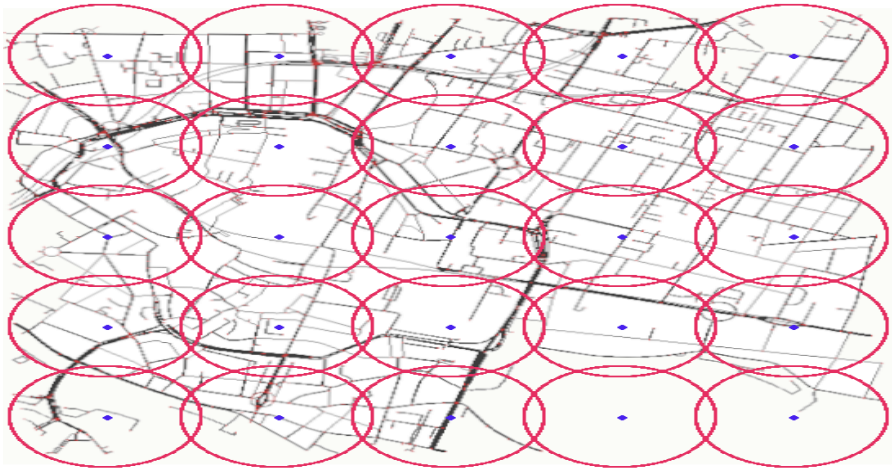

Figure 3.2 Eavesdroppers' placement

3.3.3 Vehicles Density

In order to evaluate the schemes under different density conditions, we have considered the following scenario:

- density: a total of 40 vehicles

The following conditions were considered for both scenarios:

- The average lifetime for each vehicle is around 300 seconds.
- The total simulation duration is 40 seconds.

Due to the fact that vehicles dynamically join and leave the simulation area, the number of vehicles continuously changes during the simulation. The density of vehicles over time, as well as the average density.

3.3.4 Privacy parameters

We have considered the following schemes in our study: CSP, CAPS, RSP, and the SLOW pseudonym change technique. The following metrics are used for privacy evaluation: the average pseudonym change, the anonymity set size, and the normalized traceability.

3.4 Analysis of the results

In this section, we will present the obtained result and then analyze the following schemes based on our simulation

3.4.1 Anonymity set size

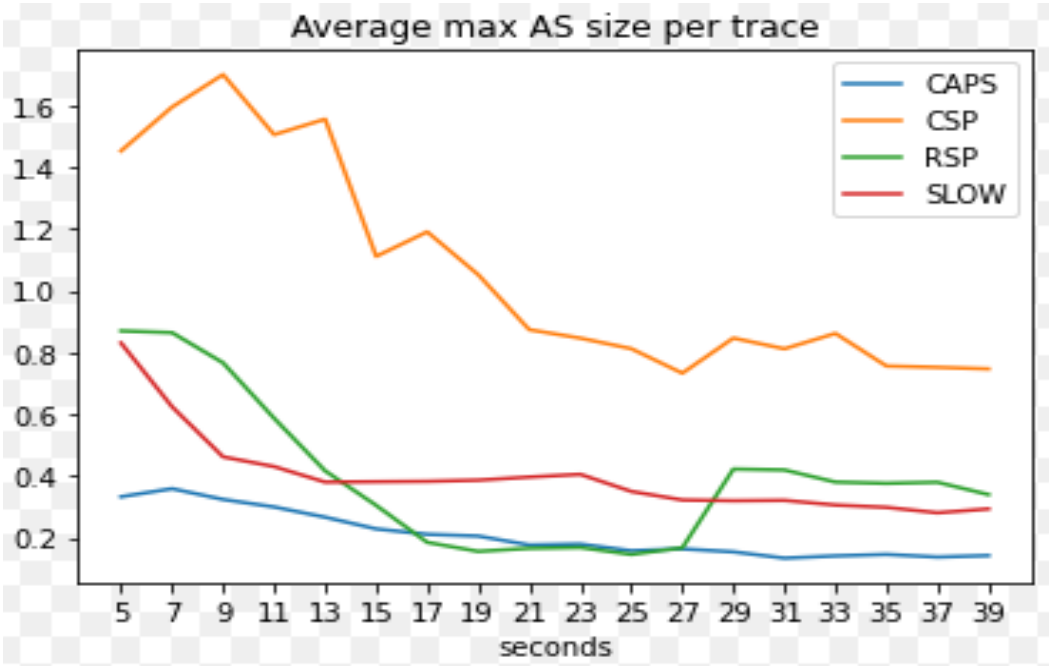

Figure 3.3 Average anonymity set size

The above figure shows the average maximum anonymity in terms of the silent period. This metric indicates the mean number of neighboring vehicles that change their pseudonyms simultaneously with a given vehicle. We note based on the figure that increasing the silent period leads to a decrease in the anonymity set size (with slight increases in the beginning). CSP has the largest value that reached 1.6. This is due to the fact that vehicle synchronize their pseudonym change. The performance of RSP is fluctuating because it depends on randomness of silent period start time, and this explains the rise and fall in performance results. Regarding the slow protocol, it provides average performance results compared to other schemes as it depends on ceasing sending beacon messages when the car speed decreases. Finally, the CAPS protocol provides low performance results.

3.4.2 Normalized Traceability

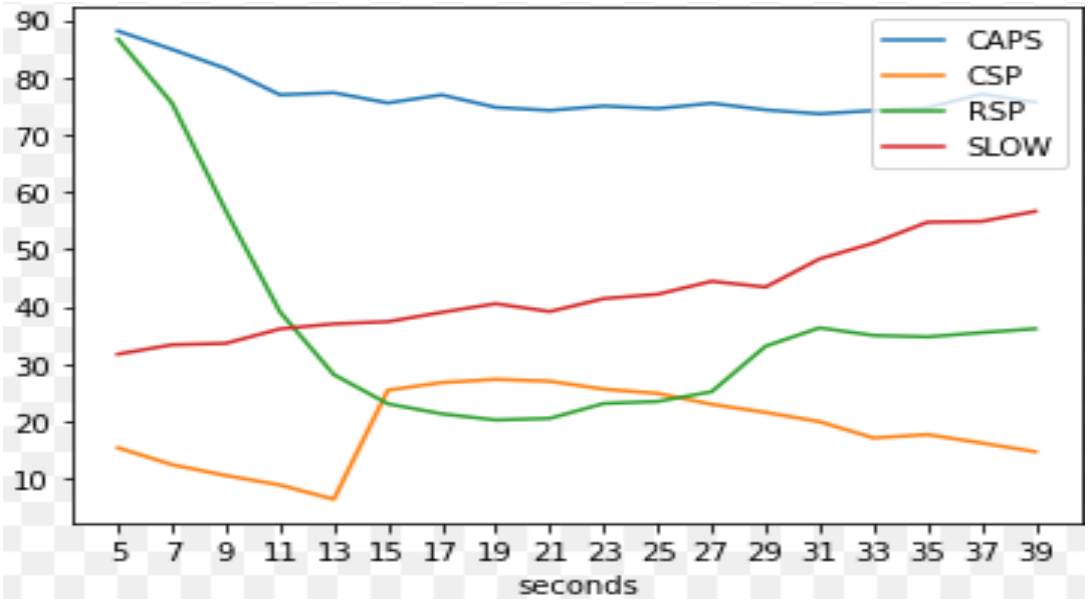

Figure 3.4 Traceability result

The figure above shows the normal traceability for the silent period. It must be stressed that natural tracking ignores compounds that did not change their pseudonym during simulation. We can see that the traceability of CAPS decreases as the silent period increases. The latter has the largest trace value. This can be explained by the fact that silence periods increase the confusion caused by the absence of communication in the shared wireless channel. As for CSP, we notice a decrease in the traceability ratio. With a slight increase in the silent period, it reached the limits of 20. We come to the SLOW protocol. We note the increase in the traceability rate in this technique. This is explained by the stopping of sending messages when a certain speed is reached and thus the ease of tracking. Finally, for the RSP protocol, we notice a decrease in the traceability rates, then an increase and decrease, which reached the limits of 30 by increasing the period. The silence is caused by the randomness of this technique and, therefore, the tracking by values.

3.5 conclusion

After we saw the previous results, we confirmed the right to take the effect of silent period as a solution to protect network privacy, through our simulation, and it was found that the shorter the silent period, the better for privacy and safety such as CSP and SLOW, but this does not cancel the importance of the long silent period such as CAPS,Because each technique has its own characteristics and results depending on the method used.

General conclusion

Our work was inspired by the importance of user privacy in vehicular ad hoc networks, our aim was to find the optimal solution to attain privacy in multiple scenarios through choosing the optimal value of the silent period.

First we gave an introduction on VANETS and we gave a few examples of attacks on them to illustrate the security risks and privacy concerns.Then in the second chapter we defined what a pseudonym is and its importance in the preservation of privacy, then we took a look at the techniques based on the changing of pseudonym .Finally we tested the impact of the silent period on privacy:

we used Prext library to evaluate privacy.This library measures the anonymity and traceability of the vehicles.we tested 4 different protocols:CSP, CAPS, SLOW, RSP We found that RSP, CSP and SLOW need a silent period of 5 seconds to achieve optimal traceability. When it comes to CAPS , it needs at least 15 seconds to achieve optimal traceability but it achieves higher privacy overall.

We surmised that every technique has it’s advantages in certain scenarios depending on the situation.

Bibliography

[1] world health organization. https://www.afro.who.int/health- topics/road-safety. [Accessed: february 08 2020].

[2] Researchgate. https://www.researchgate.net/. [Accessed: february 08 2020].

[3] Selvamuthu, "" Reliability and Survivability of Vehicular Ad hoc Networks". IEEE International Sym- posium on Performance Evaluation of Computer and Telecommunica- tion Systems," D. Selvamuthu, M. Xiaomin, R. Vinayak, K. Trivedi., 2012.

[4] S. Gillani, I. Khan, S. Qureshi, and A. Qayyum,." vehicular ad hoc network(vanet): Enabling secure and efficient transportation system". Tech. J. Univ. Eng. Technol, 2008.

[5] United States Department of Transportation," Decreas in Roadway Fatalities",. https://www.nhtsa.gov/press-releases/roadway-fatalities-2018-fars. [Accessed: february 12,2020].

[6] Anna Maria Vegni, Mauro Biagi and Roberto Cusani. " Smart Vehicles, Technologies and Main Applications in Vehicular Ad hoc Networks". 2013.

[7] A. Vegni, M. Biagi, R. Cusani. " Vehicular Technologies - Deployment and Applications". 2013. vol- Smart Vehicles, Technologies and Main Applications in Vehicular Ad hoc Networks.

[8] S. Salihin, L. Nissirat, R. Noor, I. Ahmedy." vehicular ad hoc network (vanet) handover based on long term evolution advanced (lte-a) using decision technique". Chiew, K.T., et al. (Eds.): PGRES 2017, Kuala Lumpur: Eastin Hotel, FCSIT, 2017: pp 9-17,.

[9] R. S. Raw, M. Kumar, and N. Singh." security challenges, issues and their solutions for vanets". International journal of Network Security and its

Applications, Vol.5, No.5, 2013.

[10] Rizwanul Karim Sakib." security issues in vanet". 2010.

[11] S. Zeadally, R. Hunt, Y. Chen, A. Irwin, A. Hassan." Vehicular ad hoc networks (VANETS): status, results, and challenges". 2010.

[12] M. S. Al-kahtani,." Survey on security attacks in Vehicular Ad hoc Networks (VANETs)". in 2012 6th International Conference on Signal Processing and Communication Systems, 2012. pp. 1-9.

[13] P. Tyagi, D. Dembla." A Taxonomy of Security Attacks and Issues in Vehicular Ad-Hoc Networks (VANETs)". International Journal of Computer Applications, 2014.

[14] Mohamed Watfa." Advances in vehicular ad-hoc networks: developments and challenges". Information science reference USA, 2010.

[15] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym schemes in vehicular networks: A survey", Communications Surveys Tutorials.

[16] SAE International, "On-board system requirements for V2V safety communications",.

[17] C. Troncoso, E. Costa-Montenegro, C. Diaz, and S. Schiffner, "On the difficulty of achieving anonymity for vehicle-2-x communication", Computer Networks, vol. 55, no. 14, pp. 3199–3210, 2011.

[18] ETSI - European Telecommunications Standards Institute, "Intelligent transport systems (ITS); communications architecture," ETSI, European Norm EN 302 665, September 2010.

[19] IEEE, "IEEE 1609.2: Standard for wireless access in vehicular environments (wave) - security services for applications and management messages," Standard, 2013.

[20] F. Schaub, Z. Ma, and F. Kargl, "Privacy Requirements in Vehicular Communication Systems," in Symposium on Secure Computing, IEEE Int.

Conf. on Privacy, Security, Risk, and Trust (PASSAT' 09), Aug. 2009.

[21] T. Leinmuller, E. Schoch, and F. Kargl, "Position Ver- ¨ ification Approaches for Vehicular Ad Hoc Networks," IEEE Wireless Communication Magazine, vol. 13, no. 5, pp. 16–21, 2006.

[22] M. Burmester, E. Magkos, and V. Chrissikopoulos, "Strengthening privacy protection in vanets," in IEEE Int ,Conf,Wireless and Mobile Computing, Networking and Communications (WiMob' 08), Oct. 2008.

[23] S. Bhuvaneswari and R. Saranya, "Internet of vehicle based accident detection and management techniques by using vanet: An empirical study," in 2020 Fourth International Conference on Inventive Systems and Control (ICISC). IEEE, 2020, pp. 237–244.

[24] Y. Zhang, M. Wang, J. Wang, F. Du, Y. Hu, M. Yu, G. Li, and A. Zhan, "Research on adaptive beacon message broadcast- ing cycle based on vehicle driving stability," International Journal of Network Management, p. e2091, 2020.

[25] M. Arif, G. Wang, M. Z. A. Bhuiyan, T. Wang, and J. Chen, "A survey on security attacks in vanets: Communication, applications and challenges," Vehicular Communications, vol. 19, p. 100179, 2019.

[26] J. B. Kenney, "Dedicated short-range communications (dsrc) standards in the united states," Proceedings of the IEEE, vol. 99, no. 7, pp. 1162–1182, 2011.

[27] A. Tomandl, F. Scheuer, and H. Federrath, "Simulation- based evaluation of techniques for privacy protection in vanets," in 2012 IEEE 8th international conference on wire- less and mobile computing, networking and communications (WiMob). IEEE, 2012,.

[28] K. Emara, W. Woerndl, and J. Schlichter, "Caps: Context- aware privacy scheme for vanet safety applications," in Proceedings of the 8th ACM conference on security & privacy in wireless and mobile networks, 2015, pp. 1–12.

Bibliography

[29] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki, "En- hancing wireless location privacy using silent period," in IEEE Wireless Communications and Networking Confer- ence, 2005, vol. 2. IEEE, 2005, pp. 1187–1192.

[30] L. Buttyan, T. Holczer, A. Weimerskirch, and W. Whyte, "Slow: A practical pseudonym changing scheme for location privacy in vanets," in 2009 IEEE Vehicular Networking Conference (VNC). IEEE, 2009, pp. 1–8.

[31] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, "Amoeba: Robust location privacy scheme for vanet," IEEE Journal on Selected Areas in communications, vol. 25, no. 8, pp. 1569–1589, 2007.

[32] K. Emara, "Poster: Prext: Privacy extension for veins vanet simulator," in 2016 IEEE Vehicular Networking Conference (VNC). I.E. @articlesommer2011bidirectionally, author = Sommer, Christoph and German, Reinhard and Dressler, Falko, title = Bidirection.

[33] C. Sommer, R. German, and F. Dressler, "Bidirectionally Coupled Network and Road Traffic Simulation for Improved IVC Analysis," IEEE Transactions on Mobile Computing (TMC), vol. 10, no. 1, pp. 3–15, January 2011.

[34] A. Varga and R. Hornig, "An overview of the omnet++ simulation environment," in Proceedings of the 1st inter- national conference on Simulation tools and techniques for communications, networks and systems & workshops. ICST Institute, 2008, p. 60.

[35] M. Haklay and P. Weber, "Openstreetmap: User-generated street maps," IEEE Pervasive Computing, vol. 7, no. 4, pp. 12–18, 2008.

[36] M. Behrisch, L. Bieker, J. Erdmann, and D. Krajzewicz, "Sumo–simulation of urban mobility: an overview," in Pro- ceedings of SIMUL 2011, The Third International Confer- ence on Advances in System Simulation. ThinkMind, 2011.

[37] I. Saini, B. St Amour, and A. Jaekel, "Intelligent adversary placements for privacy evaluation in vanet," Information, vol. 11, no. 9, p. 443, 2020.

[38] M. Babaghayou, N. Labraoui, A. A. A. Ari, M. A. Ferrag, and L. Maglaras, "The impact of the adversary's eavesdrop- ping stations on the location privacy level in internet of vehicles," in 2020 5th South-East Europe Design Automa- tion, Computer Engin.

Glossary

ITS Intelligent Transport System

DOS Denial Of Service

MANET Mobile Ad-hoc Network

VANETs Vehicular Ad Hoc Network

CA Certificate Authority

OBU On Board Units

OSR Order of Self-Revocation

RSU Road Side Units

TTP Trusted Third Party