الجمهورية الجزائرية الديمقراطية الشعبية

République Algérienne Démocratique et Populaire

وزارة التعليم العالي و البحث العلمي

Ministère de l 'Enseignement Supérieur et de la Recherche Scientifique

جامعة عمار ثليجي الأغواط

UNIVERSITÉ AMAR TELIDJI LAGHOUAT

FACULTE DES SCIENCES

DEPARTEMENT D'INFORMATIQUE

Mémoire de Master

Domaine : Mathématiques et Informatique

Filière : Informatique

Option : Réseaux système et applications réparties

Présenté par : Amal MEDJELLED

THÈME

Privacy aware routing in vehicular ad-hoc networks

Soutenu publiquement le 09/07/2020 devant le jury composé de:

Mr Younes GUELLOUMA	M.C	Président
Mr Omar Sami OUBATTI	M.C	Examinateur
Mr Noureddine CHAIB	M.C	Encadreur

N° d' ordre : ...../Année universitaire 2019/2020

Acknowledgments

First of all, i would thank Allah the Almighty for giving me the courage and the will for the realization of this project and giving me a golden opportunity to fulfill my dream and gain this knowledge.

I would like to express my sincere acknowledgment to my supervisor Mr.Noureddine Chaib for the continuous support, his patience and his immense knowledge. His guidance helped me in all the time of research and in writing this thesis.

To the committee members, i would like to thank them for accepting to be part of the jury and sparing their precious time in order to evaluate my work.

I would also like to take this opportunity to thank all my teachers for their efforts throughout my university studies, my colleagues, and anyone who has helped me from near or far during this experience.

Finally, I would like to express my very profound gratitude to my little family and my best friend. Especially, my parents for providing me with unfailing support and continuous encouragement throughout my years of study and through the process of researching and writing this thesis. This accomplishment would not have been possible without them. Thank you.

Amal

ملخص

الهدف الأساسي من أنظمة إتصالات المركبات VANETs هو تعزيز السلامة المرورية والأمن ، حيث يُمكن المركبات من تبادل المعلومات بطريقة آمنة وكذلك ضمان راحة السائقين والركاب.

أصبحت خصوصية المركبات والسائقين التي تعد عاملاً رئيسياً هدفاً للمهاجمين ، الذين يمكنهم الحصول على هذه المعلومات من البث المتكرر لمعلومات تحديد المواقع في الوقت الفعلي وتبادل البيانات في الشبكة. لذلك حظى هذا الموضوع بإهتمام كبير أدى إلى إنجاز أبحاث خلال السنوات الأخيرة. أقتُرح من خلالها إستخدام أسماء مستعارة لتحديد المركبات وهذا ما يضمن تلبية متطلبات كلاً من الأمان والخصوصية.

في هذه المذكرة، سنتعرف أكثر على شبكة المركبات ثم سنأخذ فكرة حول مختلف التحديات الأمنية وبعض الهجمات التي قد تتعرض لها هذه الشبكات مع الحلول المقترحة التي يمكن تنفيذها ضدها. في الأخير، سنقدم الحل الذي إقترحناه المتمثل في إنشاء بروتوكول توجيه يعتمد على الموقع للمركبة مع إستخدام إستراتجية greedy forwarding، لحل المشاكل التي واجهتها البروتوكولات السابقة التي تستخدم استراتيجية تغيير الاسم المستعار. و سيتم تقييم أداءه وفقاً لنتائج المحاكاة التي تظهر كفاءة الحل الذي إقترحناه.

الكلمات المفتاحية: شبكات المركبات، بروتوكولات التوجيه في شبكات المركبات، تغيير الأسماء المستعارة في شبكات المركبات.

Résumé

L'objectif fondamental des systèmes de communication véhiculaires VANET est l'amélioration de la sécurité et la sûreté du trafic où les véhicules peuvent échanger des données de manière sûre, ainsi que la commodité pour les conducteurs et les passagers.

La confidentialité des véhicules et des conducteurs qui est crucial, est devenue une cible pour les attaquants qui peuvent obtenir ces informations à travers la diffusion fréquente d'informations de positionnement en temps réel et de l'échange de données dans le réseau. Pour cela, un large effectif de chercheurs ont proposer l'utilisation des pseudonymes pour identifier les véhicules, tout en garantissant les exigences de sécurité et de confidentialité.

Dans cet article, nous allons mieux comprendre le réseau véhiculaire. Ensuite nous verrons certains défis de sécurité et quelque attaques majeurs qui peut y être confronté, ainsi que les solutions proposées qui peuvent être mises en œuvre contre eux. Pour atteindre au final la solution dont on a proposé, qui est la création d'un protocole de routage basé sur la position en utilisant la stratégie greedy forwarding, afin de résoudre le problème rencontré dans les protocoles précédents qui utilisent la stratégie de changement de pseudonymes. Or les performances de ce dérnier seront evaluer selon les résultats de la simulation, qui montrent l'efficacité de notre solution.

Mots clés: Réseaux VANETs, Les réseaux véhiculaires, Les protocoles de routages dans VANETs, Le changement de pseudonymes dans VANETs.

Abstract

The fundamental objective of vehicular communication systems VANETs, is the enhancement of traffic safety and security where vehicles can exchange data in a safe manner, as well as convenience to both drivers and passengers.

Privacy of individual vehicles and drivers which is a key factor, became a target to attackers who can obtain this information from the frequent broadcasting of real-time positioning information and the exchange of data in the network. For that a large body of work has emerged during recent years, proposing the use of pseudonyms to identify vehicles, ensuring that pseudonymity can satisfy both security and privacy requirements.

In this thesis, we will learn more about the vehicular networks. Then we will see the various security challenges and some of the major attacks that may be faced. As well as the proposed solutions that can be implemented against them. Finally we will give our proposed solution, Which is the creation of a position-based routing protocol using the greedy forwarding strategy, in order to solve the problem encountered in the other protocols which use the pseudonym change strategy. The performance will be evaluated according to the simulation results which show the efficiency of our solution.

Key words: VANETs, Routing protocols in VANETs, Pseudonym changing in VANETs, Vehicular networks, GPSR, Greedy forwarding based routing protocols, Position-based routing protocols.

Contents

List of Figures

List of Tables

General introduction

Nowadays, road traffic activities are one of the most important daily routines worldwide. But the sheer volume of vehicles affects the safety and efficiency of traffic environment as millions of road accidents each year are the leading causes of death and injury [1].

Road traffic safety has been the challenging issue in traffic management. One possible way is to provide the traffic information to the vehicles so that they can use them to analyse the traffic environment and can detect dangerous situations and broadcast alert messages to warn neighboring vehicles. For this purpose, a new kind of information technology called VANET (Vehicular Ad-hoc NETwork) is being developed.

VANET is an application of mobile ad hoc network. More precisely a self-organised network that can be formed by connecting vehicles aiming to improve driving safety and traffic management and ease traffic congestion. Thus VANETs have a positive impact on the environment and the economy.

These future vehicle networks would be among the largest networks in the world. For this purpose, they would constitute an ideal target for attacks by malicious entities which could aim to degrade their performance, exploit them for their benefit or even commit actions threatening people's life. VANETs are subject to: a highly dynamic topology, high node mobility, changing connectivity, etc. However, communication in VANETs is

done in real time, with vehicles speed up to more than 100km/h connectivity losses are expected and unreliable connections must be handled by protocols.

With the intensive research on VANETs and the emergence of modern cryptography, researchers have proposed solutions to protect the privacy of VANET users. They essentially consist of using pseudonyms to ensure the anonymity of these networks. The anonymity solutions protect privacy on the one hand, and place severe constraints on the detection and identification of malicious nodes, in the other hand.

This thesis consists of three chapters. We present in the first chapter the vehicular networks and its specificities. We detail, more precisely, its future applications, the communication modes, their possible communication architectures, and we give an overview on the security and the possible attacks this network may face. In the second chapter, we focus on the pseudonymity systems in VANETs and the various revocation problems of pseudonyms and the used strategies. In the third chapter, we present the carried out simulations as well as the analysis of the results and we present our proposed solution with the results obtained from the improvements. We conclude this thesis by presenting the conclusions and some perspectives.

Chapter 1

Introduction to VANETs

1.1 Introduction

The emergence of communication technology has encouraged researchers to introduce VANETs to be the core of the ITS (Intelligent Transport System). VANET is a wireless communication between vehicle to vehicle and vehicle to roadside infrastructure, in which vehicles are equipped with dedicated sensors and radio interfaces, exchange information to notify drivers early enough to avoid pile up of vehicles after an accident and various dangerous situations.

One of the major 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.[2]

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 major 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 expense [3].

1.3 What is a VANET network

VANETs are a subset of MANETs (Mobile Ad-hoc NETworks) in which communication nodes are mainly vehicles. The connectivity is done among vehicle to vehicle and vehicle to Road Side Units (RSU) located along the roads (see Figure 1.1). As such,this network is characterized by a great number of highly mobile nodes, eventually dispersed in different roads making the system difficult to design.

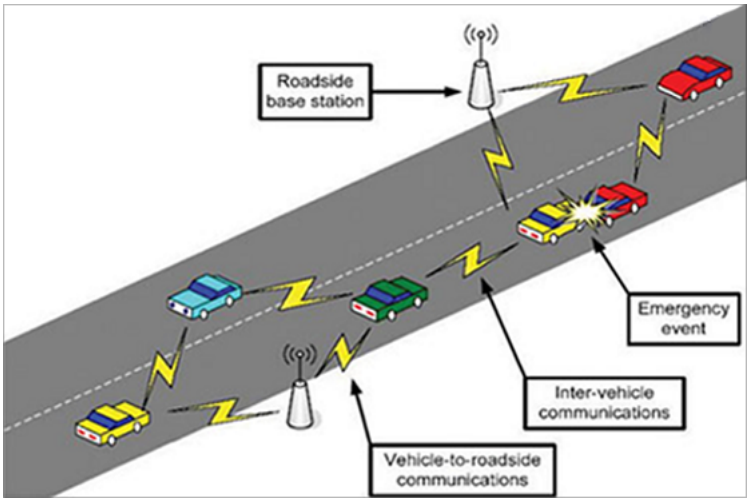


Figure 1.1: Example of a VANET [4]

The implementation of a smart VANET network requires specific electronic equipment (as illustrated in Figure 1.2) such as radars, cameras, the GPS positioning system, a communication platform, etc.

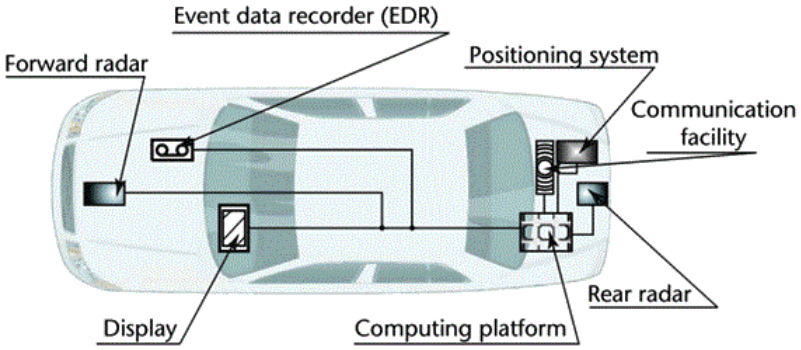


Figure 1.2: Electronic equipment of a smart vehicle

1.4 VANET network applications

For the purpose of illustration, VANET applications may be divided into the following major categories[5]:

1.4.1 Road safety applications

Road safety applications can play an important role in avoiding accidents or at least minimizing their impact. The main objective of VANETs is to provide an intelligent early warning system that can alert the drivers about the road scenario, thus giving him enough time to apply brakes well before arriving the accident place.

According to a study, stating that 60% of roadway collisions could be avoided if the driver was provided a warning at least one-half second be-

fore the collision.[6]

Another study by the US federal road safety agency (called the NHTSA "Abbreviation of National Highway Traffic Safety Administration"), shows in 2008 40% of all car collisions in the United States happen at intersections [7]. But the recent studies in 2018 showed a 2.4% decline in overall fatalities. The number of these accidents is reduced effectively by using more new vehicles that are equipped with advanced technologies that prevent or reduce the severity of crashes [8].

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 [5].

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 travelling 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 intersection.(see Figure 1.3). [9]

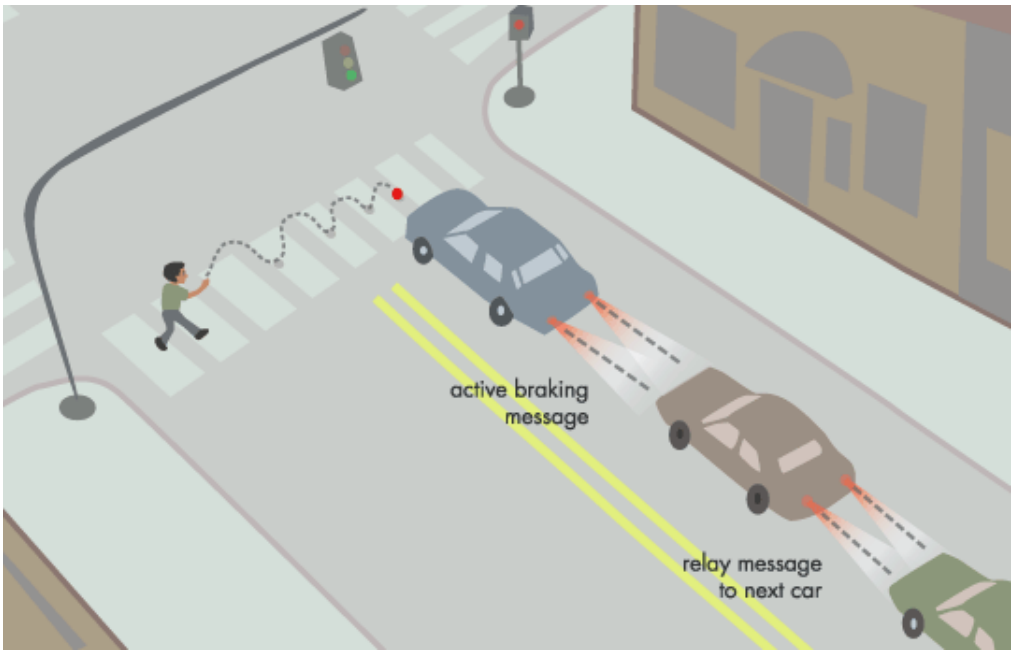


Figure 1.3: Safety application (brake messaging) by using VLC devices [10]

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 on-line gaming, Internet access, using individual terminals next to their seats (see Figure 1.4), Finding the closest fuel station, restaurant...etc can be done effectively using location based service. [9]

Figure 1.4: An example of comfort applications in VANETs [10]

1.5 Communication modes in VANETs

In vehicle networks, several modes of communication can be distinguished, 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:

A. Vehicle-to-Vehicle communication mode (V2V)

This mode of communication is characterized by a decentralized architecture, and represents a particular case of mobile ad hoc networks. It allows the direct vehicular communication without relying on a fixed infrastructure support (see Figure 1.5). According to this mode, if a vehicle is within the radio zone of the other, or via a multi-hop protocol where each vehicle is then a gateway to relay information to other vehicles in the network.

In this mode, the used communication media are characterized by a low latency and a high transmission rate.

B. 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.

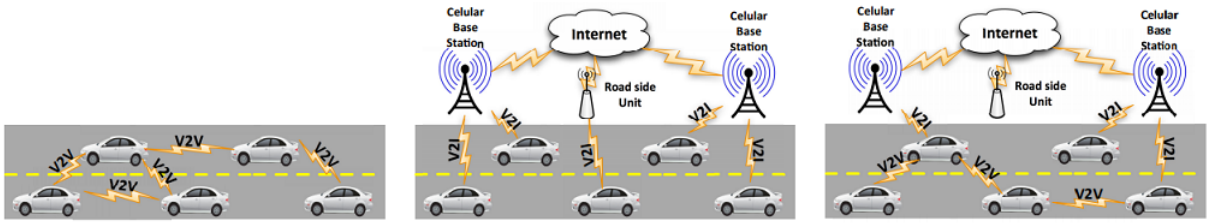
C. Hybrid communication mode (V2I)

It combines both Vehicle-to-Vehicle (V2V) and Vehicle to-Infrastructure (V2I) (see Figure 1.5). 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.

D. 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 smart phones (see Figure 1.3).



(a) Vehicle-to-Vehicle Ad Hoc Network (b) Vehicle-to-Infrastructure Network (c) Hybrid Architecture

Figure 1.5: Communication modes in VANETs [11]

1.6 Beaconing

it's a periodic one-hop link-layer broadcast messages called (Beacons) diffused by each vehicle to other nodes in its radio zone (see Figure 1.6) to inform them about: identity, the geographic position, speed and direction.

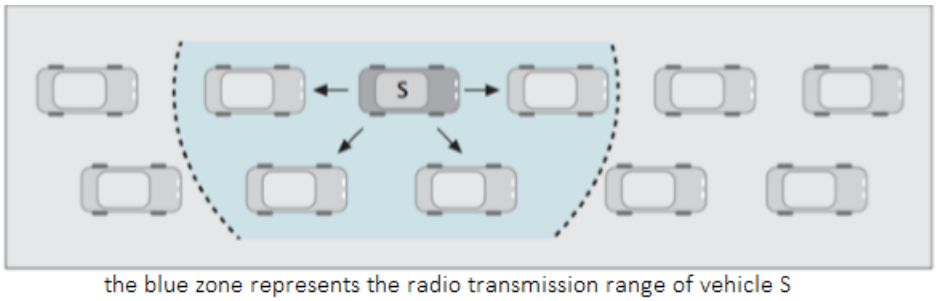


Figure 1.6: Beaconing in VANETs

1.7 Characteristics of VANETs

Vehicle networks have their own characteristics which distinguish them from MANET networks. In this section, we present some properties and constraints concerning this type of network:

- **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.

- **Topology and connectivity:** The high speed of the vehicles along with the very short interaction time between vehicles defines the dynamic topology of VANETs, which complicates the design of efficient systems for VANETs.

- **The mobility model:** in VANET networks, node mobility is extremely high, and can be affected by several factors: type of road, traffic signs, as well as the behavior of drivers and their reactions to the different traffic situations.

- **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.
- **Unbounded network size:** VANET can be implemented for one city, several cities or for countries. This means that network size in VANET is geographically unbounded. [12]

1.8 The challenges in VANETs

The challenges in VANETs can be categorised into two categories [12]:

A. Technical Challenges:

- **Network Management:** Due to high mobility, the network topology and channel condition change rapidly. It is difficult to design an effective communication protocol.
- **Congestion and collision Control:** The traffic load is low in rural areas and at night. Due to this, the network partitions frequently occurs, while in rush hours the traffic load is very high and hence network is congested and collision occurs in the network.
- **Environmental Impact:** VANETs use the electromagnetic waves for communication. These waves are affected by the environment (e.g. due to signal reflection). Hence to deploy the VANET the environmental impact must be considered

- **Security:** The importance of the information exchanged via vehicular communications makes the operation of securing these networks crucial therefore it must be satisfied.

B. Social and Economic Challenges: These challenges should be considered. In fact, it is difficult to convince manufacturers to build a system which does not protect user privacy because a consumer may reject such type of monitoring.

1.9 Security and privacy in VANETs

VANET packets contains life critical information, hence it is necessary to make sure that these packets are not inserted or modified by an attacker who can redirect road traffic, and even cause an accident. 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.

1.9.1 Security requirements for VANETs

VANET must satisfy some security requirements before their deployment. A security system in VANET should satisfy the following requirements [13]:

- **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 vehicles network.

- **Confidentiality:** It is a set of rules to be applied to ensure that only authorized persons can access the resources. This can be done by using data encryption.
- **Non-Repudiation:** In this security based system a sender cannot deny the fact having sent the message.
- **Integrity:** It involves maintaining the consistency, accuracy, and trustworthiness of data that must not be changed in transit.
- **Privacy:** This system is intended to hide the identity and geographic location of nodes, and other information that endangers the privacy of users.
- **Access control:** It ensure that all nodes access the resources according to a determined rules and privilege.

1.9.2 Attackers in Vehicular Networks

Attackers can be classified according to the following three types:

- **Internal or External:** Internal attackers are the authenticated members of the network who have cryptographic keys that allow them to communicate with other nodes in the network, whereas the external attackers are perceived by network members as an intruders, so they are limited in the variety of attacks they can provoke.
- **Malicious or Rational:** Malicious attackers have no personal benefits to attack, they just harm the functionality of the network. How-

ever, 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 intercepts the connection and modifies the data.

1.9.3 Attacks in VANETs

Attacks against VANETs can be classified as follows: [14]

1- **Attacks on availability:** The following attacks against the availability of vehicular communication have been identified:

- **Denial of Service (DoS):** This attack overloads the communication channel or makes its use difficult. It could be performed by compromising enough RSUs, or by making a vehicle to broadcast infinite messages in a period of time.
- **Falsification of disseminated data:** In this attack, the opponent composes a message containing false information on the state of the road or an emergency braking message for example. This falsified information affects the availability of correct data for the driver.
- **Malware:** The injection of malware, such as viruses or worms into VANETs, can cause network disruptions. Malware attacks are more likely to be carried out by internal attackers rather than external ones. Malware can be injected into OBUs (On Board Units), when they receive software updates. In these attacks, the malicious entity may aim to degrade the efficiency of the network.

- **Black Hole attack:** In VANET networks, a black hole is formed when traffic is redirected to one or more nodes which 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 (Figure1.7).

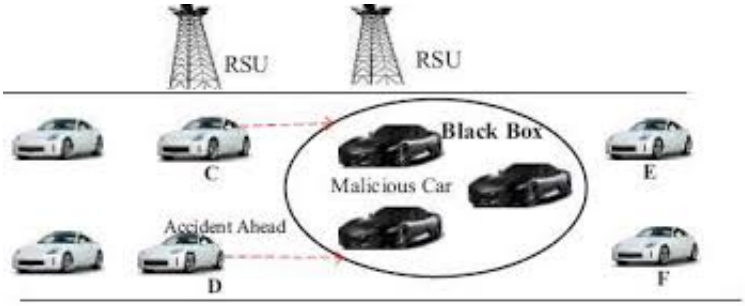


Figure 1.7: Black hole Attack [15]

2- **Attacks on authentication:** Authentication with other appropriate mechanisms avoids communication with nodes having a false identity, illegitimate re-transmission of the message and injection of incorrect information. These attacks include:

- **Spoofing:** It consists in stealing the identity of a node and use it to carry out a malicious action. The attacker can show that he has malicious behaviour under the identities of other nodes in order to degrade their degrees of confidence, and therefore, degrade the network's performance.
- **Replay attack:** In this attack, the attacker re-injects messages already sent by other nodes to cause, for example, the poisoning

of routing tables and neighbours.

- **GPS Spoofing:** This attack consists in using a GPS signal generator which emits stronger signals than those emitted by the satellites, in order to force the victim nodes to inject falsified geographic data.
- **Sybil Attack:** In this type of attack, an attacker use different identities at the same time. This attack is very dangerous since a vehicle can claim to be in different positions at the same time, thereby creating chaos and huge security risks in the network [16].
- **Message Tampering:** An intermediate node can modify the messages exchanged in vehicle-to-vehicle or vehicle-to-roadside unit communication in order to falsify transaction application requests or to forge responses [14].
- **Key and Certificate Replication:** It involves accessing OBU content to retrieve cryptographic data. This attack puts the VANET system at risk, as the malicious entity can generate digital signatures as much as it wants without any possibility of identifying it.

3- **Attacks on confidentiality:** Eavesdropping is the most prominent attack over VANETs against confidentiality. To perform it, attackers can use a controled vehicle or false RSU. Their goal is to illegally get access to confidential data [14], and collect information about road users without their knowledge.

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 impact in 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.

Chapter 2

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 [17]. 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, juridical, 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. Finally, we describe the Pseudonymity solution.

2.2 Identity in VANETs

The identity of an entity is an attribute that uniquely identifies it. Traditionally, license plate numbers were used as the main identifier of a vehicle. In VANETs, a Vehicle Identifier (VID) can be considered as a signed certificate which makes it possible to unambiguously authenticate a vehicle.

The VID is a long-term identifier assumed to be pre-installed in the OBU of a vehicle. The VID could be issued with the vehicle registration and the license plate by a vehicle registration authority, such as the registration service.

2.3 The risks of privacy in VANETs

The periodic exchange of beacon messages is essential in VANETs, because it will play an essential role in increasing the contextual awareness of vehicles.

Unfortunately, these beacon messages contain identity, geographic location and other information that endangers the privacy of users. In fact a global observer can monitor trajectories of targeted vehicles and use this data for a range of purposes or to track their location. The latter scenario is known as ”Big brother syndrome” which is described as the ID disclosure of other vehicles [18] (see Figure 2.1).

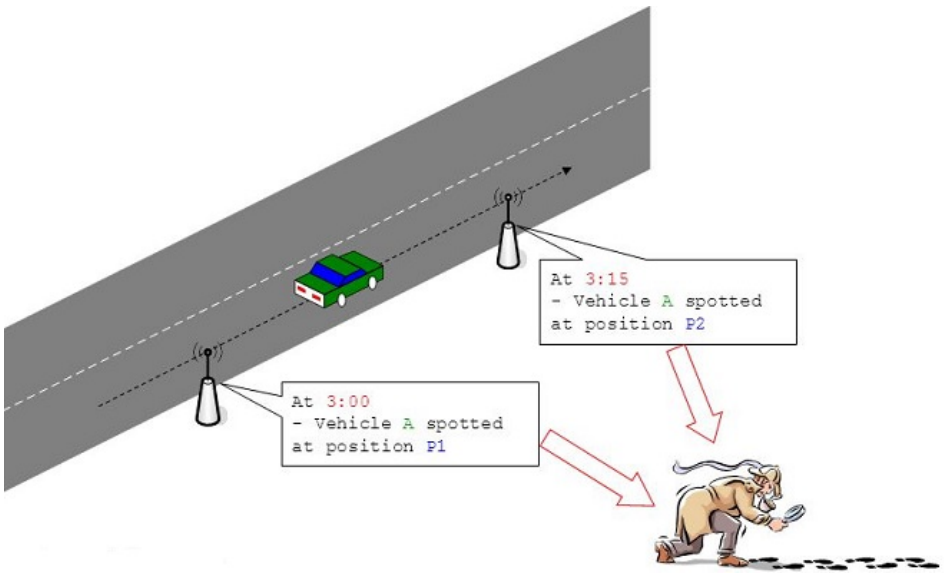


Figure 2.1: Big brother syndrome

2.4 The use of pseudonyms to ensure privacy in VANETs

Chaum [19] has introduced the digital pseudonyms, as a public key used to verify signatures made by the anonymous holder of the corresponding private key, in order to provide anonymity to electronic transactions.
Pfitzmann and Hansen [20], have defined the Digital pseudonyms as a bit string which, is unique as identifier (at least with very high probability). It can be used to authenticate the messages of its holder.
We can conclude that a pseudonym must be used for authentication, but must not contain any personal information which could be linked to the real identity of the holder of the pseudonym. However, the holder may use a set of pseudonyms to ensure his anonymity. An entity in a network can either change the pseudonyms over time to avoid correlating the actions performed over a long period of time, or a different pseudonym could be used for each action.

2.5 Classification of pseudonym systems

By examining the cryptographic mechanisms used for the realization of pseudonym systems, four main categories can be distinguished in the VANETs:

- **Systems based on asymmetric cryptography:** In this category, pseudonyms are represented by public keys. To facilitate the verification of messages received by vehicles, a pseudonym certificate must be sent with the message.

- **Identity-based 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 [21]. This allows to avoid exchanging large cryptographic information.

- **Pseudonym systems based on group signatures:** They introduce a private key for a group of vehicles, which allows an entity of a group to generate a signature on its behalf, the signature can be verified using a corresponding public key. Although these systems generally offer anonymity to signatories within the group.

- **Systems based on symmetric cryptography:** In these systems, a receiver must know the secret key (shared between the transmitter and the receiver) to be able to authenticate the transmitter. They are known for their calculation efficiency.

2.6 Conditional Anonymity

The secret part of the pseudonym (the information which makes it possible to deduce the real identity) must only be known by its holder.
This means guaranteeing the anonymity of an honest vehicle's real identity, unless malicious activities or the suspicion of the presence of malicious behaviour are detected by a specific authority that can determine the corresponding identities. This last operation is called pseudonym resolution. This characteristic makes it possible to satisfy the objective of non-repudiation.

2.7 The adversary model

Wernke et al.[22] have classified attacks on privacy into the following categories:

1. **Single Position Attack :** The general idea of this attack is that the attacker tries to infer the position or the identity of a node by analyzing the content of a query.

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 (see Figure 2.2) to decrease its privacy.
   With the Identity matching method, the attacker can use it to attack several pseudonyms of the same identity.

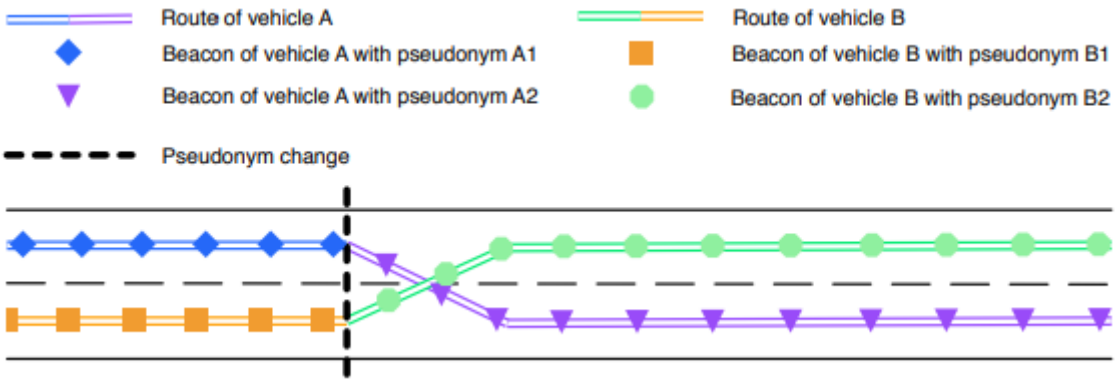


Figure 2.2: vehicle tracking [23]

3. **Context Linking Attack :** It consists in using personal information additionally to spatio-temporal information concerning the victim. Their interest is to establish a user activity profile.

4. **Compromised TTP :** The attack of compromising a trusted third party (TTP). If an attacker succeeds in compromising a TTP, he can

access to the stored user data that allows him to put the privacy of VANET users at risk.

2.8 The pseudonymity requirements in VANETs

The attacks against VANETs define the requirements that must be taken into account by a pseudonym system. The aim is to provide an adequate level of privacy protection for users to remain untraceable and anonymous. In this context Schaub et al. [24] have defined the following requirements:

- **Minimum disclosure:** The amount of information that a user reveals in communication should must be minimal. For example, no more than the necessary information for V2X communication (V2I, V2V or V2P).

- **Conditional anonymity:** A sender of a message should be anonymous among a set of potential senders, this is called the anonymity set of the message. As the identity of the user must be resolved in case of a conflict, anonymity is conditional in VANETs.

- **Unlinkability:** It requires that the relation between two or more items in the network should not be found.

- **Distributed resolution authority:** The identity resolution should be distributed between multiple authorities so that their cooperation is necessary to correlate an anonymous credential to an individual.

- **Perfect forward privacy:** A pseudonym resolution operation for an entity must not lead to revealing any information of other credentials

of the same user and the true identity of the nodes which are not in question.

We give below the characteristics which must be satisfied by a pseudonym to protect privacy:

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

2- **The uniqueness:** In order to avoid having an identity used by more than one vehicle, each pseudonym must be unique. This characteristic is guaranteed by the basic cryptographic system which is used to generate the pseudonyms.

3- **The availability:** A new pseudonym must always be available for a possible change of pseudonym. This characteristic can be guaranteed by storing a very large number of pseudonyms in the OBU.

4- **The abandonment of old identifiers:** Once, a new pseudonym is used, any old identifier in the protocol stack must also be changed in order to prevent tracking.

2.9 Abstract pseudonym life cycle

As there are many privacy requirements in VANETs, many of pseudonym schemes have been proposed. the requirements imposed by vehicular communications lead to an abstract pseudonym life cycle (see Figure 2.3) similar to most pseudonym approaches in vehicle networks. The main purpose of a pseudonym is to authenticate the sender as a valid one. This can

either be accomplished by certifying a sender as a vehicle, or implicitly ensuring that only valid vehicles can perform a certain action such as a group signature.

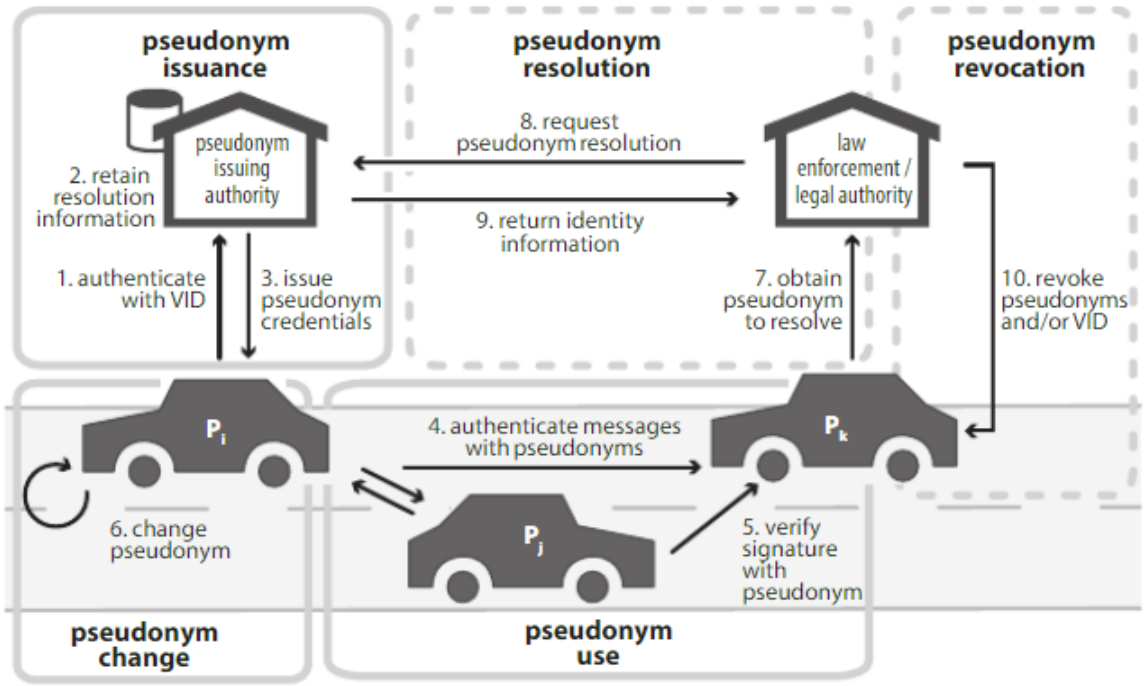


Figure 2.3: Abstract pseudonym lifecycle for vehicular networks [25]

In vehicular networks, pseudonyms pass through a common abstract life cycle resulting from the previous requirements. With some specific pseudonym authentication systems, some of the life cycle phases may diverge from our abstract life cycle model. However, the phases outlined in the following can be found in almost all pseudonym authentication systems.

1- **Pseudonym Issuance:** Almost all pseudonym authentication systems for vehicle communications assume that a vehicle has a unique digital identifier. The VID can be seen as a signed certificate that allows to unambiguously authenticate a vehicle and it is required for the emission of pseudonyms by most of the systems offered.

In the process of issuing pseudonyms, the VID is used to authenticate the vehicle's OBU to ensure that only valid vehicles can obtain pseudonyms and can therefore participate in vehicle communications. For pseudonym issuance, two major based approaches can be distinguished: third-party issuance and self issuance.

- Third-party issuance: This approach is adopted by most systems, whereby pseudonyms are generated by a pseudonym issuing authority. Depending on the system, this entity can be composed of multiple sub-entities: Certificate Authority (CA), Pseudonym Provider (PP), security architecture of ETSI refers to them as registration and authorization authorities.

  The role of the pseudonym issuing authority is commonly assigned to infrastructures managed by ACs and PPs, or by RSUs. In either case, it authenticates the vehicle with its VID, and checks the vehicle's eligibility to obtain pseudonyms (i.e., if the vehicle's VID is valid and has not been revoked).

- Self issuance: the OBU of a vehicle is more autonomous and can generate the pseudonyms it will need. Therefore it is possible to minimize the storage capacity required for the pool pseudonym (the set of pseudonyms available in an OBU). However, sybil attacks are generally more difficult to avoid in these systems due to the level of autonomy.

2- **Pseudonym Use:** Once a vehicle has obtained pseudonyms, it can communicate with other vehicles or infrastructures. Using a pseudonym involves two steps: authentication of outgoing messages and verification of received messages.

In general, pseudonymous authentication systems employ either asymmetric signatures or message authentication codes. Authentication of a message requires verification of the validity of a pseudonym. A valid pseudonym must be generated either by a trustworthy verifiable authority with an accompanying certificate, or independently and can be authenticated with secret parameters.

3- **Pseudonym Change:** Actions performed under one pseudonym can be linked to each other, due to the mentioned characteristics of pseudonyms. Changing a pseudonym affects almost the entire protocol stack.

Network identifiers such as IP and MAC addresses must all be changed simultaneously to avoid trivial linking between old and new pseudonym.

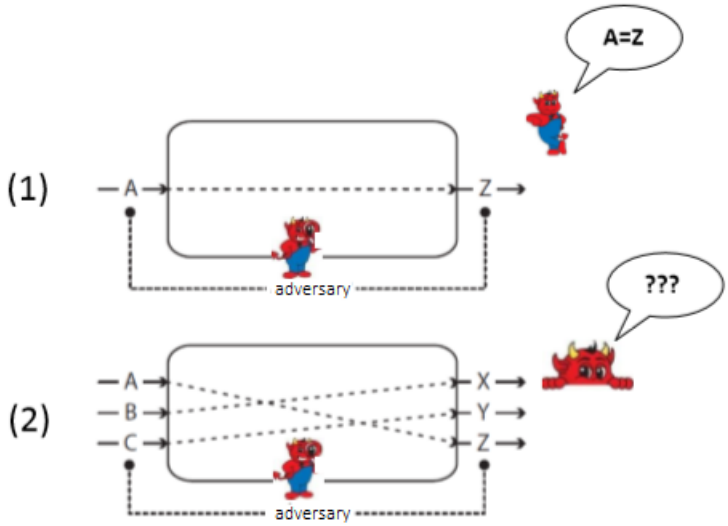


Figure 2.4: The context change of pseudonym [25]

Another important aspect is the necessity of having neighboring vehicles when changing the pseudonym. As shown in Figure 2.4, changing the pseudonym alone is not enough for confusing an observer, by monitoring locations before and after the pseudonym change occurred, it will be easy for the observer to link between two consecutive pseudonyms used by a node. Whereas in the second case in which several nodes change their pseudonyms simultaneously, a possible observer can experience confusion.

Figure 2.5, illustrates a general algorithm for changing the pseudonym in VANETs. In this algorithm, the nodes take into account their contexts (such as the number of neighbors, their directions and their speeds) and can collaborate in order to decide the best time to change their pseudonyms.

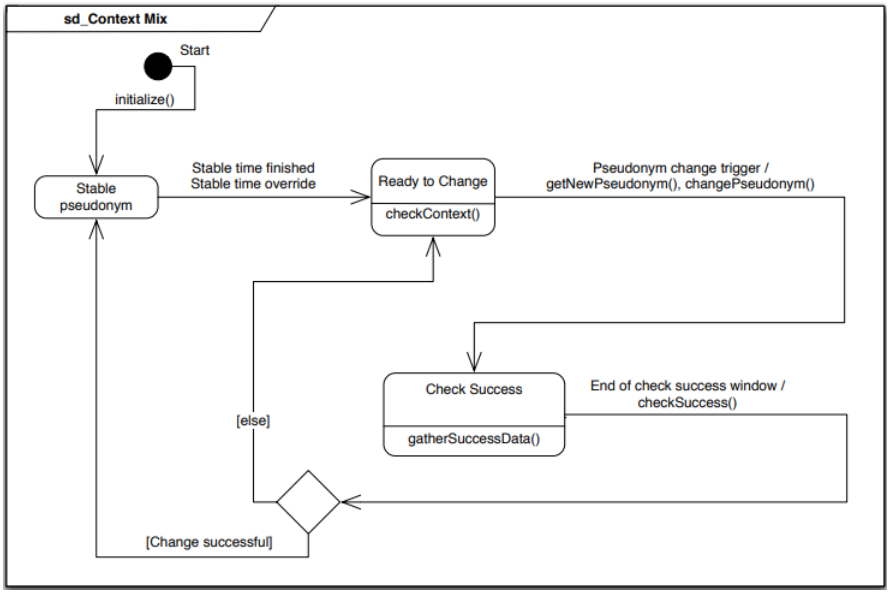


Figure 2.5: General algorithm for pseudonym change [17]

According to this algorithm, the process of managing a pseudonym includes three phases:

- **The stable pseudonym phase:** It is a period in which the vehicle does not change its pseudonym and remains in this phase until having a trigger to pass to the predisposition phase.
- **The predisposition phase:** The vehicle checks its context to choose the right moment to change the pseudonym, some techniques can be used to create confusion and strengthen privacy in this phase.
- **Check pseudonym change success phase:** A vehicle checks whether the change of pseudonym is carried out under good conditions.

4- **Pseudonym Resolution:** It is 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:** Malicious Nodes must be revoked from the vehicle network to ensure its proper functioning. It consists revocation of the node's authentication credentials (pseudonyms, VID, or both). If only specific pseudonyms have been revoked, there will be a possibility that the corresponding vehicle may have other pseudonyms which can be used for future communications. If all the pseudonyms of a node should be revoked, the the necessary information to identify all of its pseudonyms must be implemented. This possibility will considerably weaken the privacy provided by pseudonyms.

2.10 Pseudonym change strategies

An important parameter for pseudonym changes is the rate of change. It influences the communication, the necessary storage memory capacity and the level of privacy. In addition, a simple change of pseudonym is not enough to avoid tracking.

For that purpose, several pseudonym change strategies have been proposed, including:

1- **Periodic change:** In this strategy, a vehicle changes its pseudonym at each predefined time interval (see Figure 2.6), Eckhoff et al.[26] introduced time-slotted pseudonym changes, in order to have the possibility to change the pseudonym even in the absence of pseudonym providers.

Unfortunately, their solution is ineffective once the attacker has known the period used for pseudonyms.

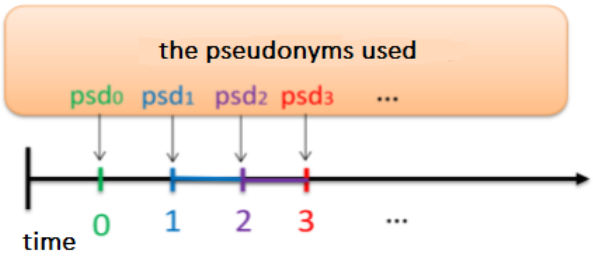


Figure 2.6: Periodic change

2- **Random change:** in order to solve the problem of the fixed change period, vehicles can change theirs according to a random period (see Figure 2.7) [27]. As a result, an attacker cannot predict the next change of pseudonym. However, tracking is still possible, if few vehi-

cles change their pseudonyms at a specific time. In addition, a long-term analysis makes it possible to identify the vehicles which re-use their pseudonyms.

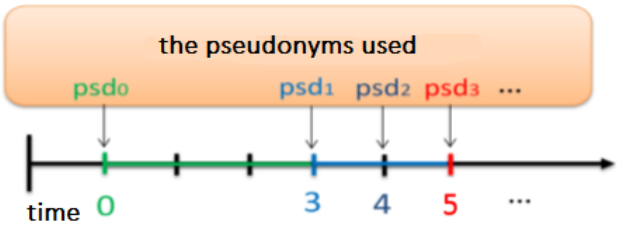


Figure 2.7: Random change

3- **The silent period between pseudonym changes:**

In the CARAVAN change system [28], a vehicle does not access the channel for a certain period (the silent period) before changing its pseudonym. The silent period makes attacks on privacy difficult. If a vehicle uses the silent period strategy in an intersection, it will be difficult to prevent its movement. This strategy consists in making a compromise between privacy and road safety.

4- **Autonomous change:** In this strategy, vehicles independently determine where and when to change their pseudonyms. The two Swing and Swap protocols proposed by Li et al [29] adopt this strategy.

In Swing, vehicles change their pseudonyms when changing speed and direction. Thus, an attacker cannot predict the movement of nodes to establish a correlation between their locations before and after the change of pseudonyms. In Swap, each pair of vehicles exchange their pseudonyms, when changing their pseudonym with a probability 0.5, then enter a random silent period. So they are indistinguishable from

other vehicles. In another protocol called SLOW [30], if a vehicle's speed drops below 30km/h, it enters a silent period and changes its pseudonym.

5- **Density-based change (The CROWD strategy):** In this strategy, the change of pseudonym depends on the number of current neighbors. Therefore, a vehicle can avoid the ineffective pseudonym change (when isolated for example). According to Chaurasia et al.[31][32]. the pseudonym change must be made if the size of the set of neighboring vehicles is greater than a determined threshold.

6- **Collaborative change (synchronous):** When a vehicle changes its pseudonym alone, it easily falls victim to tracking attacks. A better strategy is to change the pseudonym simultaneously with its neighbors. For this, the vehicle broadcasts a message to its neighbors to inform them that it is in the predisposed state [33]. This strategy creates a Mix-zone where vehicles, in the same zone, change their pseudonyms simultaneously which are carefully selected and are generally road intersections [34]. Lu et al.[35] suggest placing Mix-zones in the Social Spots (for example traffic light, parking, etc.) to increase the number of vehicles changing their pseudonyms simultaneously. The Disadvantage of this approach is the weak privacy protection in low vehicle density scenarios.

Although there are many proposed strategies for changing pseudonyms, we cannot know which one is most effective in practice. But, according to the defined objectives of anonymity or metrics such as the speed of processing, the size of messages exchanged, the required storage ca-

pacity, the desired degree of anonymity, the complexity of resolution of pseudonyms, we can determine which one is best suited.

2.11 Pseudonym revocation systems

Given the decentralized nature of vehicle networks and their size, the distribution of the latest revocation information constitutes a major challenge for an effective change of pseudonym and revocation [36]. The classification of revocation system of pseudonyms in VANETs is as follow:

1- **Passive revocation:**

In this category, the pseudonym revocation is limited to the revocation of VID for scalability reasons. If the long-term identity is revoked, no new pseudonym can be obtained. according to [37][38] the distribution of CRL (Certificate Revocation List) to OBUs is not practical, because of the high frequency of messages and the size of CRL which can possibly be large. On the other hand, by revoking only the VID, the corresponding vehicle can continue to participate in the network until all of its pseudonyms have expired, this global revocation approach is known as passive revocation [39]. One solution to this problem is to reduce the lifetime of pseudonyms to a very short time [40].

This approach raises challenges such as changing the pseudonym, reloading it, and protecting privacy.

2- **Self-revocation:**

This category of revocation protocols [41], consists in sending notifications of a detected malicious behavior by vehicles neighboring the malicious node to the revocation authority (see Figure 2.8). Then,

the authority sends an OSR (Order of Self-Revocation) message to the TPD[1] (Tamper Proof Device) of the detected malicious vehicle (the malicious vehicle is black in the figure below) in geocast mode [42] every T_{repeat} seconds until the malicious node's TPD confirms the deletion of all stored pseudonyms. Note that the radius of the geocast region is incremented with each iteration to increase the chances that the TPD of the malicious vehicle will receive the OSR message.

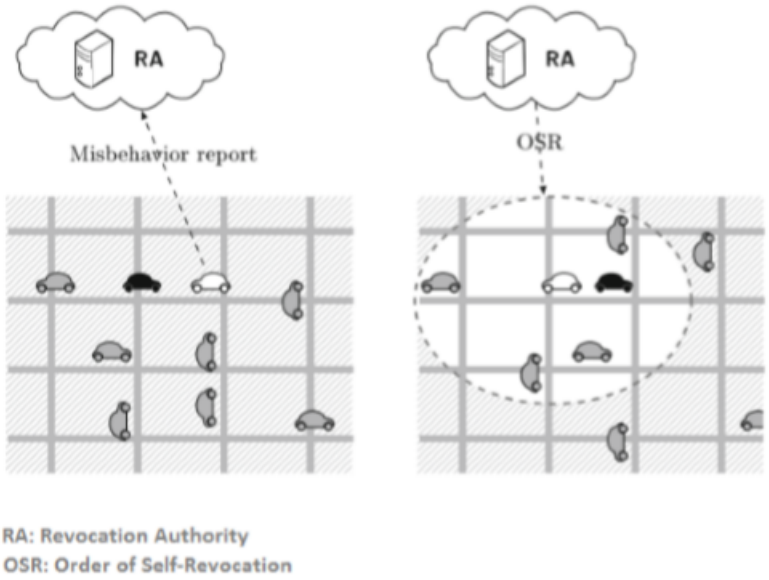


Figure 2.8: The REWIRE revocation protocol [41]

3- **Threshold-based pseudonym revocation:**

Revocation techniques in this category are generally based on voting systems which consists of counting the rate of nodes accusing a malicious node and revoking it if the rate exceeds a predefined threshold. They are necessary to have the distributed aspect of the revocation mechanism.

[1]TPD is a hardware equipment capable of performing cryptographic operations, protect and back up secret data like cryptographic keys, logs of events.

These techniques may be faster, but they present problems related to the use of the anonymity concept. Indeed, the researchers who developed these techniques did not take into account the life cycle of pseudonyms which has a great impact on their techniques. So a new study is needed on the impact of anonymity on this category.

4- **The Proof of Non-Revocation based approach:**

This approach was proposed by Gañán et al.[43] by presenting the EPA technique (Efficient and Privacy-Aware revocation mechanism for vehicular Ad-hoc networks) to minimize the false positive rate.

The main idea of the EPA, it allows each vehicle to prove the validity of its pseudonym and that it has not been revoked recently instead of forcing vehicles to download large revocation lists. These proofs can be obtained by the CA (Certification Authority) by building an MHT (Merkle Hash Tree) which can be obtained from the list of revoked nodes. So the traces of revocation information and the set of revoked pseudonyms can be represented in a single field (the root of MHT). Each time, a node wishing to obtain information which enables it to prove its existence in the network, it must communicate in a secure manner with an RSU. The RSU must use the MHT in order to check the validity (non-revocation) of this node before transmitting the required certification data (see Figure 2.9).

The Disadvantage of this approach is that the nodes must, from time to time, find a way to communicate with the RSUs. So it's hard to define the expiration time of the non-revocation proof.

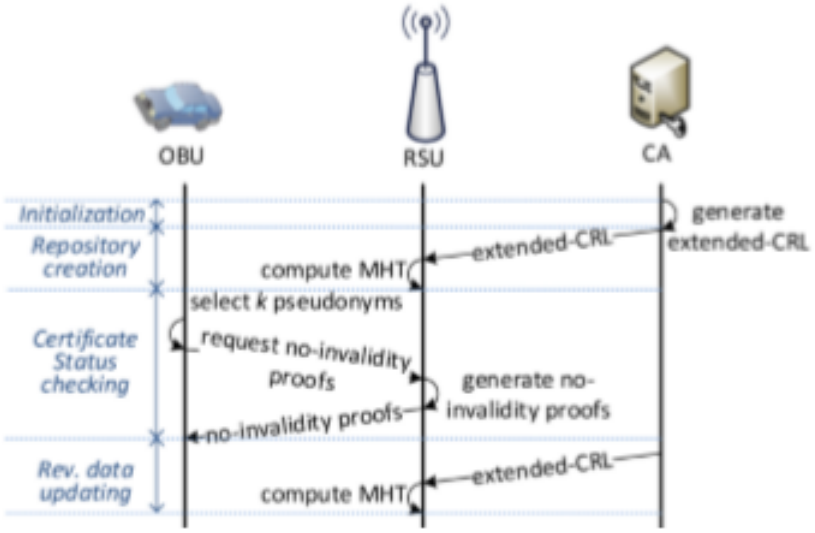


Figure 2.9: The EPA revocation technique scheme [43]

2.12 Conclusion

The anonymity of the future vehicle networks users must be intensively studied and analyzed so that the systems developed over these networks will not violate and satisfy the security and privacy requirements of VANETs. Pseudonymity is the most accepted approach in the research community for this problem. However, there are still some challenges that confront designers.

Chapter 3

Simulation and analysis of results

3.1 Introduction

VANETs rely on periodic broadcast of the vehicles' location. For example, the location of vehicles can be used for detecting and avoiding collisions or geographical routing of data to disseminate warning messages. Whereas, this information can be used to track the users' whereabouts, which was protected by using pseudonyms, but this solution provoked some problems. In this chapter, we will first see the problems encountered while using pseudonyms then will take an idea about some of the routing protocols, to finally introduce our proposed solution where we will be studying the performance of the greedy forwarding protocol and analysing the simulation results based on parameter metrics, i.e. packet delivery ratio and end to end delay.

3.2 Problem statement

We consider the mix-zone strategy where vehicles, in the same zone, change their pseudonyms simultaneously, our study targets vehicles entering intersections (see Figure 3.1).

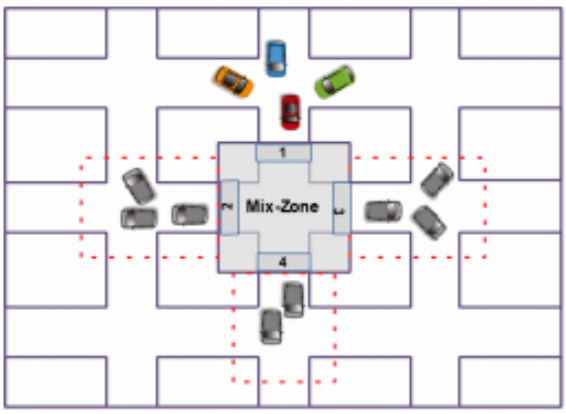


Figure 3.1: Mix-zone concept [44]

Vehicles entering intersections encounter difficulties in sending packets to neighbouring nodes, when the vehicle receives a packet and can not find a neighbour it will end up dropping the packet, because neighbours enters in silent period state after which reduces the network participants pool in the mix-zone area. Thus, they will be considered invisible for the sender (see Figure 3.2).

Another problem can be faced when the node may select a neighbour as a forwarder, when receiving the packet later when it enters in silent period the packet will be dropped.

These two last scenarios will not let the forwarder node send packets.

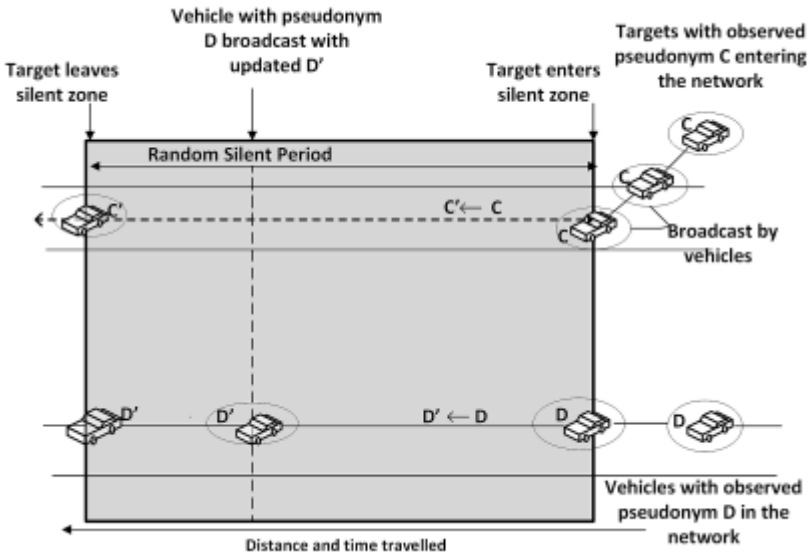


Figure 3.2: Effect of random silent period and peseudonym changing by a vehicle joining the network [45]

A target vehicle entering the network, broadcasts with pseudonym A, and then goes into silence. If a neighboring vehicle updates its pseudonym from B to B' during this silent period, then an adversary can be misled to consider pseudonym B' (and hence, the associated neighbor vehicle's location) to be that of the target vehicle, provided the target vehicle updates to A' before its next broadcast.

3.3 Impact of pseudonym change on routing ad-hoc networks categories

MANET routing protocols are categorized as shown in the Figure 3.3 [46]:

- **Proactive routing protocols (table driven):** In these protocols, each node of the network maintains a single or multiple routing tables that are regularly updated. Each node will send a broadcasting message to all the other nodes in the network in order to detect the changes in their network topology.

- **Reactive routing protocols (on-demand):** In these protocols, each network node discovers its route to destination, on-demand, this on-demand route discovery is done by flooding control messages through global broadcast and once the route is discovered.

These protocols fail to fully address the specific needs of VANETs especially in a city environment (rapid topology changes, fragmented network conditions and frequent disconnection due to nodes distribution), the main reason for the failure of on-demand protocols is if one node enters silent period all the routes built depending in this node will fail.
To address the specific needs of VANET, some routing protocols have been recently proposed. Among them, GPSR (Greedy Perimeter Stateless Routing). GPSR is considered as stateless routing algorithms as each node needs to know about its one hop neighbor's position only to make packet forwarding decisions. GPSR uses greedy forwarding to forward packets to nodes that are always progressively closer to the destination, this category of protocols will be less affected by the degradation of the performance than the

previous ones because the degradation can only be caused by the number of nodes that enter silent period.

In this work, we focus our study on greedy forwarding protocol for vehicular networks in intersections based on a localization system like the GPSR.

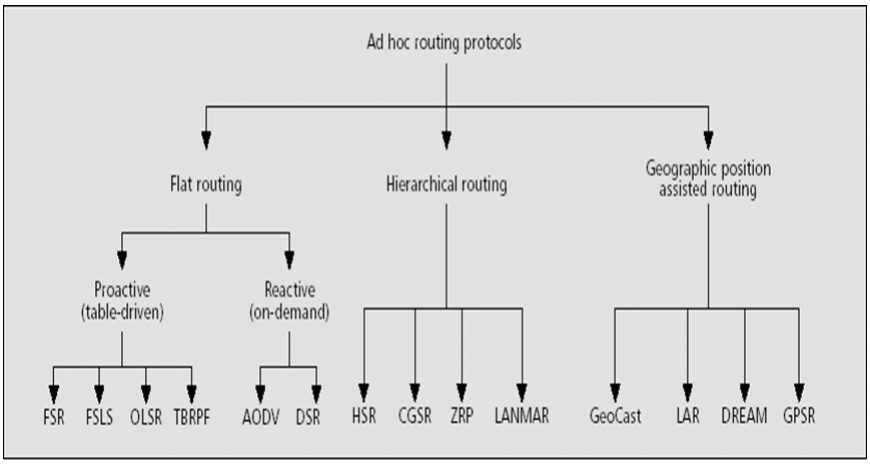


Figure 3.3: Classification of routing protocols [46]

3.4 Proposed solution

In order to solve the problem where the node drops the packet when it enters silent period, we proposed that only some vehicles will sacrifice and risk their privacy with not entering silent period and do the role of a relay to forward packets. These vehicles are chosen randomly with a very small amount of 20% to guarantee that the packets reach their destination.

Before entering intersection a node will first calculate the distance between its position and the intersection to check if the vehicle is approaching the silent period area which is D in the Figure 3.4. Meanwhile the vehicle generates a random value between 0-1 and check it if it is less than 0.2 which is the amount of chosen vehicles, if both conditions are satisfied

then the node will enter silent period, otherwise it is chosen as a forwarder.

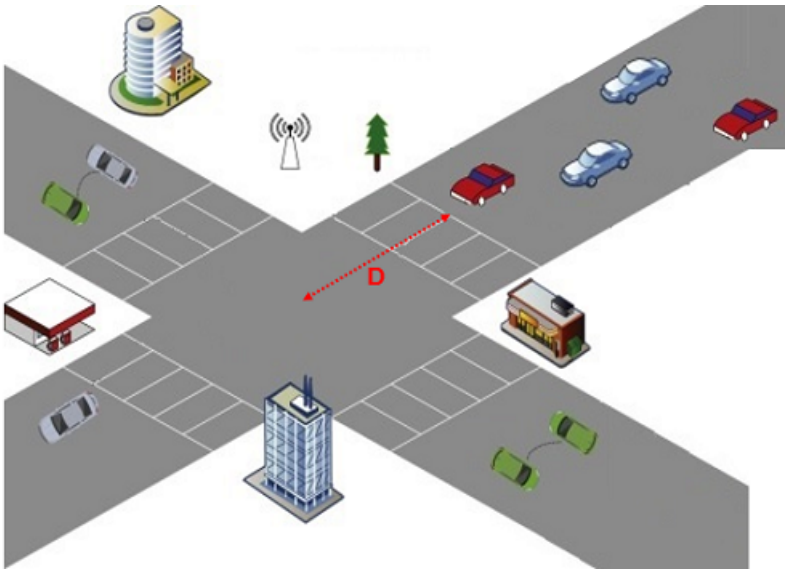


Figure 3.4: The silent period area 'D'

3.5 Simulation environment

In this section, we use the traffic simulator SUMO (Simulation of Urban MObility) in order to generate our mobility model (see Figure 3.5). SUMO allows us to generate trace files for NS2. Our example is on a simple signalized intersection. For the first scenario, we will conduct it without silent period, then we will give a second scenario where we use the silent period to show the performance degradation when vehicles enter intersection and then to finish with the last scenario where we implement our solution.
All the key parameters of our simulation are summarized in the following table:

Parameters	Setting
Simulation time	600 sec
Simulation area	1020m 1013m
Routing protocol	GPSR
Data packet size	512 bytes
Packet sending rate	2 sec
CBR packet rate	10 packets
Number of vehicles	100
Transmission range	40m, 50m, 100m, 250m, 300m
Vehicle velocity	0-22,22 Metres/sec (80Km/hour)
MAC protocol	IEEE 802.11
Traffic type	CBR/UDP

Table 3.1: Simulation Parameters

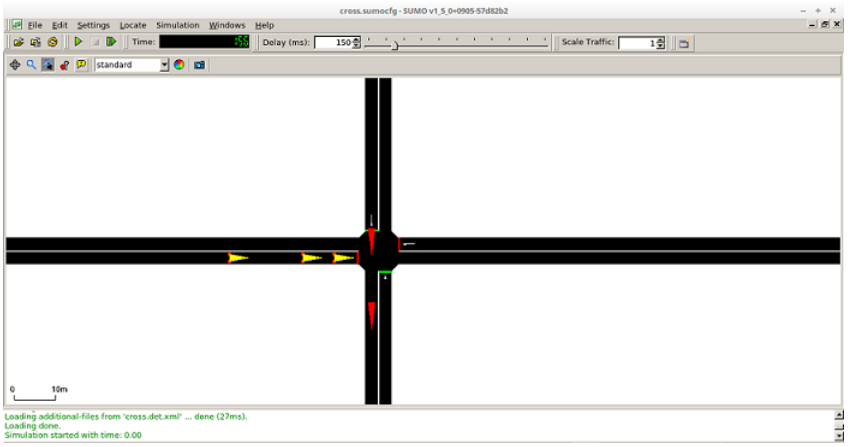


Figure 3.5: Intersection in SUMO

3.5.1 Performance Metrics

Two metrics are measured to understand the performance of our routing protocol.

- **Packet Delivery Ratio:**

  It's the ratio of delivered data packet to the destination.

$$PDR = \frac{\sum Number\,of\,packets\,received}{\sum Number\,of\,packets\,sent} 100$$

- **End-to-End Delay (ms):**

  It refers to the time taken for a packet to be transmitted across a network from source to destination.

$$end - to - end = \frac{\sum (packet\,arrival\,time - send\,time)}{Number\,of\,packets\,received} 1000$$

3.6 Simulation results and analysis

In this section, we provide simulation results.

3.6.1 First scenario without silent period

The graphs below 3.6 and 3.7 show the performance of the greedy forwarding protocol without the use of the silent period.
It is clearly shown that the proposed protocol guarantees a good results. With the increase of the source vehicle's radio range will facilitate the next hop selection for packet forwarding and the number of hops is reduced reasonably by using various transmission ranges which explains the increasing result in the packet delivery ratio. Thus, the time taken to deliver the packet from source to destination (end-to-end delay) is reduced which explains the decreased result in the delay.

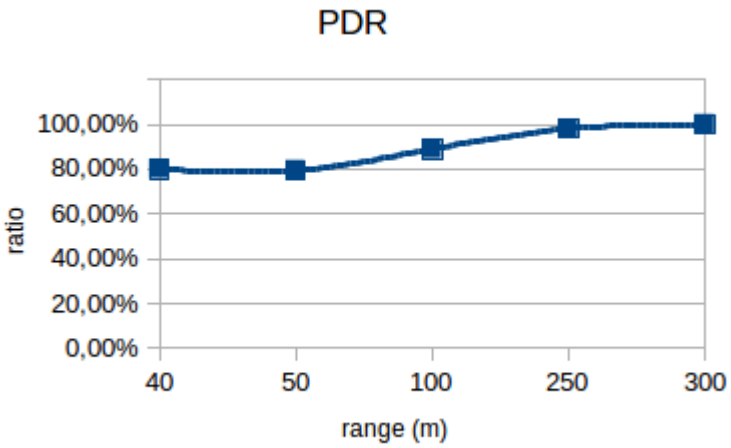


Figure 3.6: Packet delivery ratio vs. range

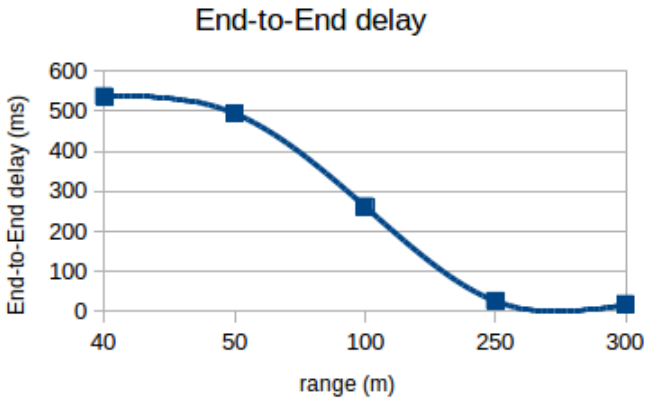


Figure 3.7: End-to-End Delay vs. range

3.6.2 Second scenario with silent period

The graphs below 3.8 and 3.9 show the performance of the greedy forwarding protocol with the use of the silent period.

The performance of the protocol decreased with nearly 20% and that degradation is due to the vehicles entering silent period when approaching intersection, for that the packets will be dropped when the vehicle stops communicating and forwarding and this will affect the delay too causing a

higher results than the previous one. But this didn't affect the fact that when the transmission range increases, the packet delivery ratio initially increases rapidly and the time taken to forward also decreases.

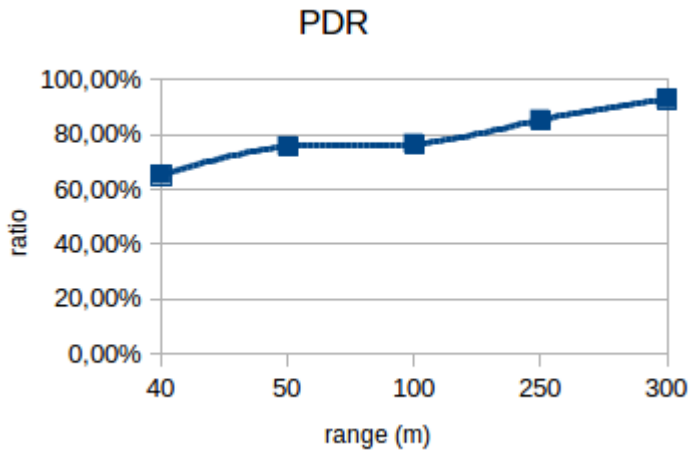


Figure 3.8: Packet delivery ratio vs. range

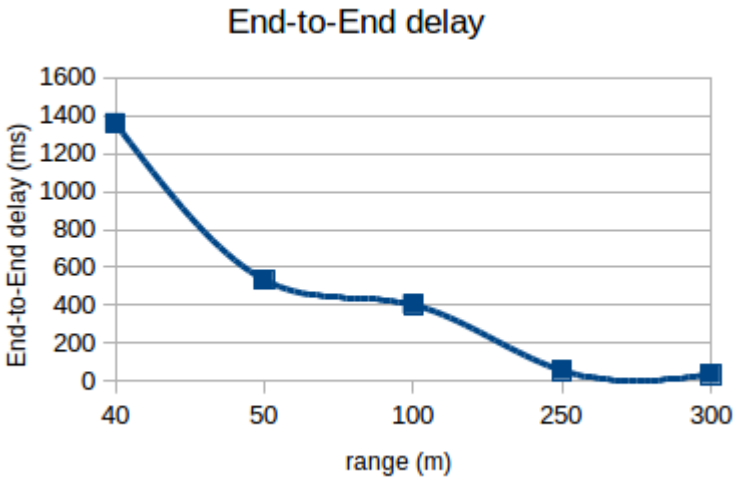


Figure 3.9: End-to-End Delay vs. range

3.6.3 Third scenario with our solution

In order to improve the previous results and get a better performance, we simulated our proposed solution and here are the results obtained.

- **the result and the analysis of our simulation**

  the graphs below 3.10 and 3.11 show the performance of our protocol using the silent period with some conditions.

  We can notice a better results in the PDR from 65% in the previous scenario to 80% of delivered packets and that's due to the reduced number of nodes that enter silent period and the nodes that will take the role of a relay to forward packets, so we can guarantee the packets are successfully delivered to their destination. That perfectly affected in a good way the Delay that decreased to 500ms than the previous one with nearly 1400ms we can say that it improves the time taken for packets to reach their destination as the transmission range increases.

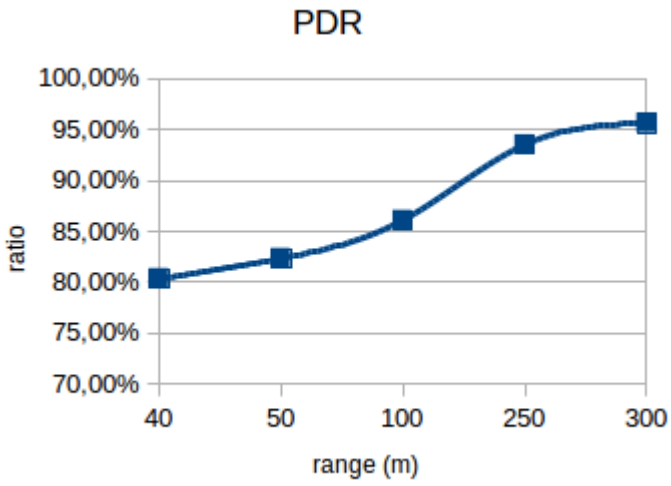


Figure 3.10: Packet delivery ratio vs. range

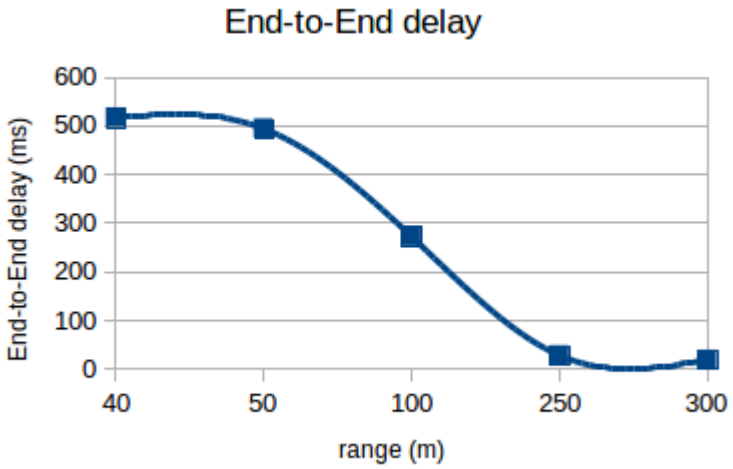


Figure 3.11: End-to-End Delay vs. range

3.7 Conclusion

In this work, we have studied the impact of the frequent change of pseudonyms with the use of the silent period in VANETs and the performance was clear enough to be proven in the first two previous scenarios.

As stated using two of the performance metrics, and according to the results obtained from the simulation of our proposed solution that appear in the third scenario, our routing protocol gives a better performance in terms of packet delivery ratio and end-to-end delay without being affected by the change of the radio range.

Our aim is to have an efficient position based routing protocol, which works well in every traffic scenario.

General conclusion

VANET networks provide a promising applications for saving people's lives and ensuring the comfort of vehicle occupants. These networks can only be deployed after investigation and assurance of their security. Unfortunately, these networks are vulnerable to attacks by malicious entities which can inject messages for malicious purposes.

The protection of the vehicle occupants privacy must be achieved. The most reliable approach to ensure vehicles anonymity is to use pseudonyms. They have a specific life cycle comprising the following phases: generation, transmission, use, revocation and resolution of pseudonyms. These phases can coexist simultaneously, which poses unprecedented challenges for the revocation of these pseudonyms. Indeed, malicious vehicles have enough pseudonyms at a given time and can change them without following the appropriate steps necessary for the operation, and consequently they can cause an attack of succession of charges which allows them to amplify their negative impact on the system performance.

Another faced problems are the location privacy threats that arise in VANET due to tracking of vehicles based on their broadcasts especially in the interurban areas due to the great number of vehicles such as: intersections, congestion, highways, etc. To solve such an issue, we proposed a solution taking into account the mobility, and the application features in

VANETs. Vehicles can be provided with an extended silent period, which in turn enhances their anonymity and impact in first place the communication between vehicles, thus our solution Is to create a position-based routing protocol using the greedy forwarding approach, This protocol will take a place in an intersection, in which some vehicles will sacrifice their privacy with not entering silent period and do the role of a forwarder. Each vehicle entering the intersection will first calculate the distance between its position and the intersection to check if the vehicle is approaching the silent period area. Meanwhile the node generates a random value between 0-1 and check it if it is less than 0.2, if both conditions are satisfied then the node will enter silent period, otherwise it is chosen as a forwarder.
Assuming the global adversary model of VANET, we evaluated the performance achieved by our proposed solution and the results obtained from the simulation, that in the end have shown that our approach allows a better communication method and guarantee the reception of data packets in a reduced time.

As for future works, VANETs are expected to be very attractive in near future, so they need more research which could lead to further improvements. Our aim is to have an efficient position based routing protocol, which works well in every traffic scenario.

Bibliography

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

[2] Al-Sakib Khan Pathan. *"Security of Self-Organizing Networks: MANET, WSN, WMN, VANET"*. CRC press, 2010.

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

[4] D. Selvamuthu, M. Xiaomin, R. Vinayak, K. Trivedi. "Reliability and Survivability of Vehicular Ad hoc Networks". *IEEE International Symposium on Performance Evaluation of Computer and Telecommunication Systems*, 2012.

[5] 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.

[6] C. D.Wang, and J. P. Thompson. "apparatus and method for motion detection and tracking of objects in a region for collision avoidance utilizing a real-time adaptive probabilistic neural network". 1997.

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

[8] The law offices of joel j. kofsky, "intersection accidents". https://www.phillyinjurylawyer.com/intersection-accidents/. [Accessed: february 12,2020].

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

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

[11] 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*, 2017.

[12] 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.

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

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

[15] 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.

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

[17] M. Gerlach and F. Güttler. "Privacy in VANETs using changing pseudonyms - Ideal and real" . *IEEE Veh. Technol. Conf.*, 2007.

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

[19] David L. chaum. "Untraceable electronic mail, return addresses, and digital pseudonyms". *Communications of the ACM*, 24(2), 1981.

[20] A. Pfitzmann, M. Hansen. "A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management". 2010.

[21] L. Yan, C. Rong, G. Zhao. "Strengthen Cloud Computing Security with Federal Identity Management Using Hierarchical Identity-Based Cryptography". 2009.

[22] M. Wernke, P. Skvortsov, F. Dürr, and K. Rothermel. "A Classification of Location Privacy Attacks and Approaches". 2014.

[23] F. Scheuer, K.-P. Fuchs, and H. Federrath. "A Safety-Preserving Mix Zone for VANETs". *in Lecture Notes in Computer Science*, 2011.

[24] F. Schaub, Z. Ma, and F. Kargl. "Privacy requirements in vehicular communication systems". *Proc. - 12th IEEE Int. Conf. Comput. Sci. Eng. CSE 2009,*, 2009. vol. 3, no. March, pp. 139–145.

[25] J. Petit, F. Schaub, M. Feiri, and F. Kargl. "Pseudonym Schemes in Vehicular Networks:A Survey". *IEEE Commun. Surv. Tutorials*, 2015.

[26] D. Eckhoff, C. Sommer, T. Gansen, R. German, and F. Dressler. "Strong and affordable location privacy in VANETs: Identity diffusion using time-slots and swapping". *IEEE Veh. Netw. Conf. VNC 2010*, 2010.

[27] Y. Pan, J. Li, L. Feng, and B. Xu. "An analytical model for random changing pseudonyms scheme in VANETs". *Networks, Software Toolsand Applications*, 2011.

[28] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, K. Sezaki. "CARAVAN: Providing Location Privacy for VANET". 2005.

[29] M. Li, K. Sampigethaya, L. Huang, and R. Poovendran. "Swing & Swap: User-Centric Approaches Towards Maximizing Location Privacy". *WPES*, 2006.

[30] L. Buttyan, T. Holczer, A. Weimerskirch, and W. Whyte. "SLOW: A Practical Pseudonym Changing Schemefor Location Privacy in VANETs". *IEEE Vehicular Networking Conference (VNC)*, 2009.

[31] B. K. Chaurasia and S. Verma. "Optimizing Pseudonym Updation for Anonymity in VANETS". *IEEE Asia-Pacific Services Computing Conference*, 2008.

[32] B. K. Chaurasia, S. Verma, G. S. Tomar, and S. M. Bhaskar. "Pseudonym based mechanism for sustaining privacy in VANETs". *1st Int. Conf. Comput. Intell. Commun. Syst. Networks, CICSYN*, 2009.

[33] D. Eckhoff, C. Sommer, T. Gansen, R. German, and F. Dressler. "Strong and affordable location privacy in VANETs: Identity diffusion using time-slots and swapping". *IEEE Veh. Netw. Conf. VNC*, 2010.

[34] D. Eckhoff, C. Sommer, T. Gansen, R. German, and F. Dressler. "Privacy protection with dynamic pseudonym-based multiple mix-zones over road networks". *China Commun*, 2017.

[35] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen. "Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in VANETs". *IEEE Trans. Veh. Technol*, 2012. vol. 61, no. 1, pp. 86–96.

[36] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J. Hubaux. "Eviction of Misbehaving and Faulty Nodes in Vehicular Networks". *IEEE J. Sel. Areas Commun*, 2007. vol. 25, no. 8, pp. 1557– 1568.

[37] M. E. Nowatkowski and H. L. Owen. "Scalable Certificate Revocation List Distribution in Vehicular Ad Hoc Networks". *IEEE Globecom Work. GC'10*, 2010. pp. 54–58.

[38] Y. Kondareddy, G. Di Crescenzo, and P. Agrawal. "Analysis of Certificate Revocation List Distribution Protocols for Vehicular Networks". *IEEE J. Sel. Areas Commun GLOBECOM - IEEE Glob. Telecommun. Conf*, 2010.

[39] F. Schaub. "Conditional Pseudonymity in Vehicular Ad Hoc Networks". *Ulm University*, 2008.

[40] Z. Ma, F. Kargl, and M. Weber. "Pseudonym-On-Demand: A New Pseudonym Refill Strategy for Vehicular Communications". *IEEE Veh. Technol. Conf*, 2005. pp. 1–5.

[41] D. Förster, H. Löhr, J. Zibuschka, and F. Kargl. "REWIRE – Revocation Without Resolution: A Privacy-Friendly Revocation Mechanism for Vehicular Ad-Hoc Networks". *in Trust and Trustworthy Computing, vol. 9229*, 2015. pp. 193–208.

[42] J. Timpner and L. Wolf. "Query-response geocast for vehicular crowd sensing". *Ad Hoc Networks*, 2016. vol. 36, no. 2, pp. 435–449.

[43] C. Gañán, J. L. Muñoz, O. Esparza, J. Mata-Díaz, and J. Alins. "EPA: an Efficient and Privacy-Aware revocation Mechanism for Vehicular Ad Hoc Networks". *Pervasive Mob. Comput*, 2015. vol. 21, pp. 75–91.

[44] A. Boualouache1, S. Senouci, S. Moussaoui. "A survey on pseudonym changing strategies for Vehicular Ad-Hoc Networks". *IEEE Communications Surveys and Tutorials*, 2017.

[45] P. Asuquo, H. Cruickshank, J. Morley, P. Anyigor Ogah, A. Lei, W. Hathal, S. Bao, and Z. Sun. "Security and Privacy in Location-Based Services for Vehicular and Mobile Communications: An Overview, Challenges and Countermeasures". *IEEE internet of things journal*, 2018.

[46] Krishna Gorantala. "Routing Protocols in Mobile Ad-hoc Networks". *Umea University Department of Computing Science SWEDEN*, 2006.

Glossary

CA Certificate Authority.

CRL Certificate Revocation List.

DOS Denial Of Service.

ITS Intelligent Transport System.

MANET Mobile Ad-hoc NETworks.

NHTSA National Highway Traffic Safety Administration.

OBU On Board Units.

OSR Order of Self-Revocation.

PP Pseudonym Provider.

RSU Road Side Units.

TPD Tamper Proof Device.

TTP Trusted Third Party.

V2I Vehicle to Infrastructure Communication.

V2P Vehicle to Passenger communication.

V2V Vehicle to Vehicle Communication.

VANET Vehicular Ad-hoc NETwork.

VID Vehicle IDentifier.

VLC Visible Lighting Communications.