PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA
وزارة التعـلـيـم الـعـالــي و الـبـحـث الـعـلـمي
MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH
جـامـعـة عمّــار ثـلـيــجــي بالأغــواط
AMAR TELIDJI LAGHOUAT UNIVERSITY
كـلـيــــة الـعـلــــوم
FACULTY OF SCIENCES
DEPARTMENT OF MATHEMATICS AND COMPUTING

Master's thesis

Field: Mathematics and Computer Science

Specialty: Computer Science

Option: Networks, Systems and Distributed Applications

By:
El Hadj Ahmed Menad
Nadir Begouga

THEME

Proposing and designing a new revocation protocol in VANETs

Publicly defended on 06-07-2021 in front of the jury composed of:

Mr Younes GUELLOUMA	*M.C*	*President*
Mr Omar Sami OUBATTI	*M.C*	*Examiner*
Mr Noureddine CHAIB	*M.C*	*Framer*

N◦ : …… / University Year 2020/2021

ACKNOWLEDGEMENT

In the name of Allah, the Most Gracious and the Most Merciful. All praises to Allah and His blessing for the completion of this thesis. We thank God for all the opportunities, trials and strength that have been showered on me to finish writing the thesis. We experienced so much during this process, not only from the academic aspect but also from the aspect of personality. Our humblest gratitude to the holy Prophet Muhammad (Peace be upon him) whose way of life has been a continuous guidance for me.

First and foremost, we would like to sincerely thank my supervisor Mr.Noureddine Chaib for his guidance, understanding, patience and most importantly, he has provided positive encouragement and a warm spirit to finish this thesis. It has been a great pleasure and honor to have him as my supervisor.

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

Our deepest gratitude goes to all of our families members. It would not be possible to write this thesis without support from them.

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

ملخص

تسمح الشبكات المخصصة للمركبات بمشاركة أنواع مختلفة من البيانات بين المركبات بطريقة تعاونية. التي تهدف إلى تعزيز الأمن والسلامة المرورية من خلال تبادل البيانات بطريقة امنة لكل من السائقين والركاب.

أصبحت هاته الشبكات عرضة للمهاجمين الذين بإمكانهم شن هجمات من شأنها أن تلحق اضرارا كبيرة ويمكنها حتى أن تهدد حياة الأشخاص وسلامتهم. لذلك ظهرت مجموعة كبيرة من الأعمال خلال السنوات الأخيرة، تقترح استخدام تقنيات الإلغاء التي يمكن أن تفي بمتطلبات الأمان.

في هذه الأطروحة، سوف نتعلم المزيد عن شبكات المركبات. ثم سنرى التحديات الأمنية المختلفة، وبعض الهجمات الرئيسية التي قد تواجه وتقنيات الكشف عن العقد الخبيثة وإبطالها. سنقوم بتقديم نهج لتحسين الحلول الأمنية الحالية وضمان جودة عالية للخدمة. سيتم تقييم الأداء وفقًا نتائج المحاكاة التي توضح كفاءة الحل الذي نقدمه.

كلمات البحث: شبكات المركبات، إلغاء شبكات المركبات، الكشف نظام كشف التسلل، التحقق.

Résumé

Les réseaux ad hoc de véhicules (VANET) permettent de partager différents types de données entre les véhicules de manière collaborative. Ils visent à renforcer la sûreté et la sécurité du trafic en échangeant des données de manière sûre avec les conducteurs et les passagers.

Ces réseaux sont devenus vulnérables aux attaquants qui peuvent lancer des attaques pouvant causer de gros dégâts ou même menacer la vie et la sécurité des personnes. Ainsi, de nombreux travaux ont vu le jour ces dernières années, proposant l'utilisation de techniques de révocation pouvant répondre aux exigences de sécurité.

Dans ce mémoire, nous en apprendrons davantage sur les réseaux de véhicules. Ensuite, nous verrons les différents défis de sécurité, certaines des attaques majeures qui peuvent être rencontrées et les techniques de détection et de révocation des nœuds malveillants. Nous proposons une approche d'améliorer les solutions de sécurité existantes et assurer une qualité de service élevé. Les performances seront évaluées en fonction des résultats de simulation qui montrent l'efficacité de notre solution.

Mots clés : Révocation, Réseaux VANET, détection, IDS, vérification.

Abstract

Vehicular Ad Hoc Networks (VANETs) allow sharing different kinds of data between vehicles in a collaborative way. which aim enhancement of traffic safety and security by exchanging data in a safe manner to both drivers and passengers.

These networks have become vulnerable to attackers who can launch attacks that can cause great damage or even threaten the life and safety of people. For that a large body of work has emerged during recent years, proposing the use of revocation techniques which can satisfy security requirements.

In this thesis, we will learn more about the vehicular networks. Then we will see the various security challenges, some of the major attacks that may be faced and detection and revocation techniques of malicious nodes. We will provide an approach to improving existing security solutions and ensuring a high quality of service.The performance will be evaluated according to the simulation results which show the efficiency of our solution.

Keywords: Revocation, VANET networks, detection, IDS, verification.

Summary

List of Figures

List of Tables

General introduction

Intelligent Transport Systems (ITS) are applications that provide services in different modes of traffic management and transport. These applications make the use of transport networks safer, more coordinated, smarter and secure.

VANETs (Vehicular Ad hoc Networks) consist in reinforcing road safety and providing our cars and our roads with capacities to make the road safer (information on traffic, accidents, possible deviations, etc.), improve passenger comfort, and make the time spent on the roads more user-friendly (internet access, interactive games between passengers in nearby vehicles, chat service, etc.). VANETs are the typical example of what we call ITS.

The scope of VANETs research is enormous. Researchers have proposed solutions to protect the security of VANETs users. They essentially consist in using revocation techniques. These techniques ensure security protection and constraints on the detection and identification of malicious nodes.

This thesis is organized as follows: In the first chapter, we present the vehicular networks and their specificities. We detail, more precisely, its component, application, communication modes, the architecture, and we give an overview of the security and the possible attacks this network may face. We focus in the second chapter on revocation systems in VANETs and the various revocation problems of it, and the used techniques. We present in the third chapter the simulation, as well as the analysis of the results and wegive 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

VANETs are considered to be a key component of future communication systems. "Intelligent Transportation Systems (ITS)". They represent a promising technology, which, once implemented, will offer the possibility of deploying a wide variety of applications. Some of these applications. Some of these applications aim to improve road safety. Others aim to make the journeys of road users more comfortable.

In this chapter, we have defined the VANETs. Then we present their characteristics, their components, as well as the challenges encountered by VANET networks.

This chapter first presents generally VANETs, and then we provide the different types of services offered by these networks and existing modes of communication and their characteristics.

1.2 Definition of VANETs

VANETs is a new form of Mobile Ad Hoc Networks(MANETs). They make it possible to establish communications between vehicles or with an infrastructure located at the edges of roads. Compared to classic VANETs, VANETs are characterized by high mobility of nodes making the network topology strongly dynamic. It is a particular case of wireless multi-hop network, which has the constraint of fast topology changes due to the high node mobility. When principles of MANETs are applied in the domain of vehicles. Another term used to define VANETs is Inter-Vehicle Communication (IVC). The vehicles are fitted with sensors. The latter interact with the sensors of other vehicles or the infrastructure, certain electronic equipment must be installed within vehicles (see figure 1.1), such as environmental perception devices (radars, cameras), a GPS (Global Positioning System) tracking system, and of course a processing platform. Several technologies can be implemented for establishing communications [1].

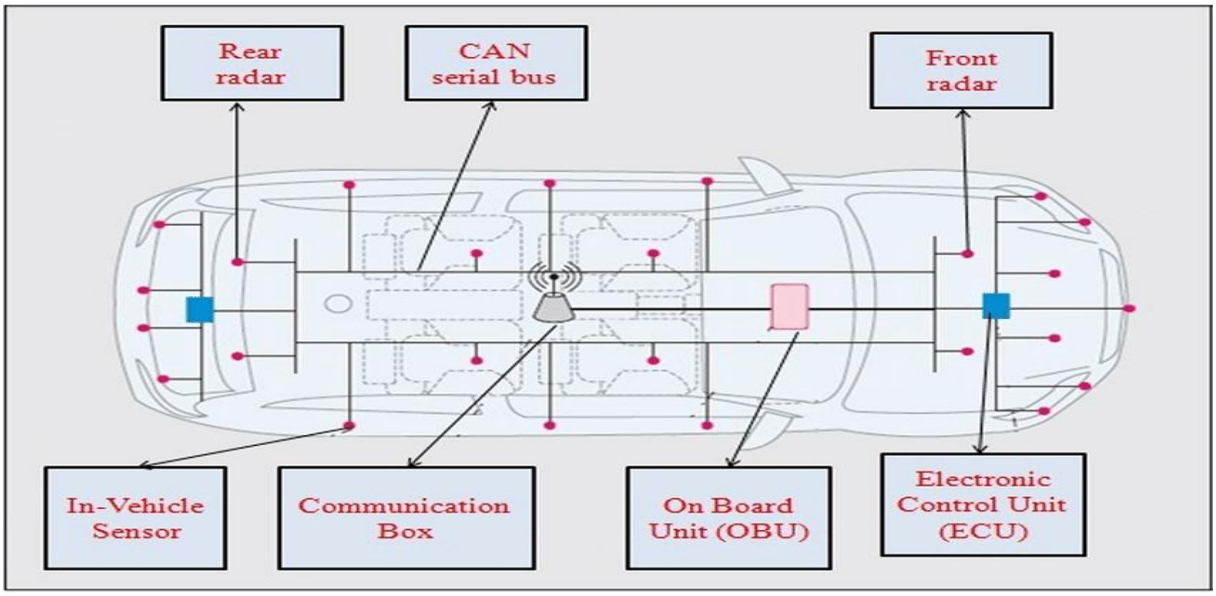

Figure 1.1: The elements constituting the intelligent vehicle [2]

1.3 Components of a vehicular network

A VANET network is made up of three entities:

- Confidence Authority (CA)

CA is a source of the authenticity of the information. It ensures the management and registration of all communicating entities. The CA must know all the real identities of the vehicles. In certain cases, the CA takes care of the delivery and attribution of communication certificates and pseudonyms [3].

- Road-Side Unit (RSU)

RSU serves as a gateway between OBUs and the communications infrastructure. They are the subordinates of the CAs. They are installed by the side of the road [3].

- On-Board Unit (OBUs)

They are units embedded in intelligent vehicles, which bring together a set of high-tech hardware and software components (GPS, radar, and others). They ensure the

location, reception, calculation, storage, and sending of data on the network. These are transceivers that connect the vehicle to the network, as shown in Figure 1.2 below [3].

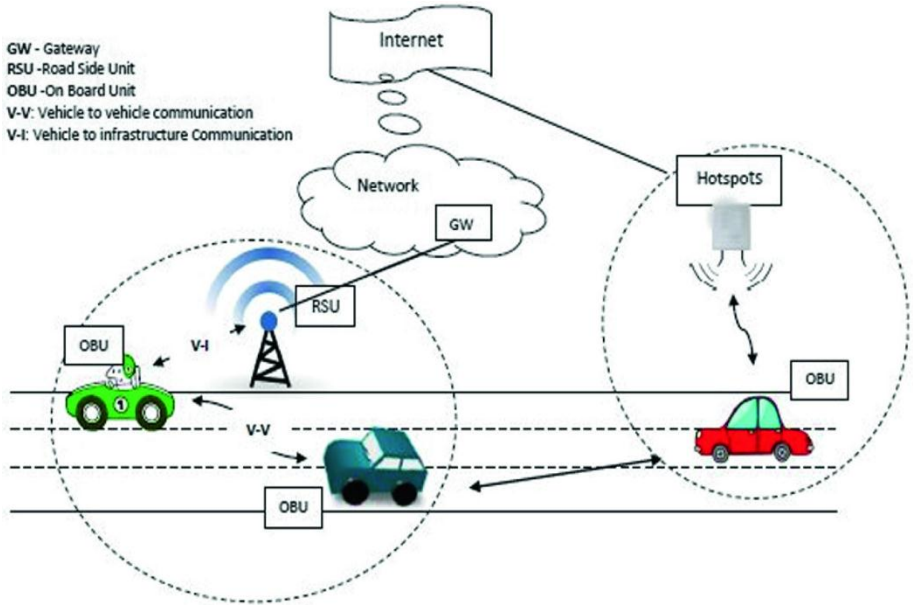

Figure 1.2: Components of a vehicular network [4]

1.4 Applications of VANETs

VANET can be classified into three categories:

1.4.1 Road Traffic management applications

Traffic management applications focus on improving traffic conditions to reduce traffic jams and the risk of accidents (see Figure 1.3). They provide drivers with technical support, enabling them to adapt their route to the road traffic situation. These applications aim to balance the movement of vehicles on the roads for efficient use of the road and intersection capacity, and therefore reducing human losses, duration of trips, and energy consumption [5].

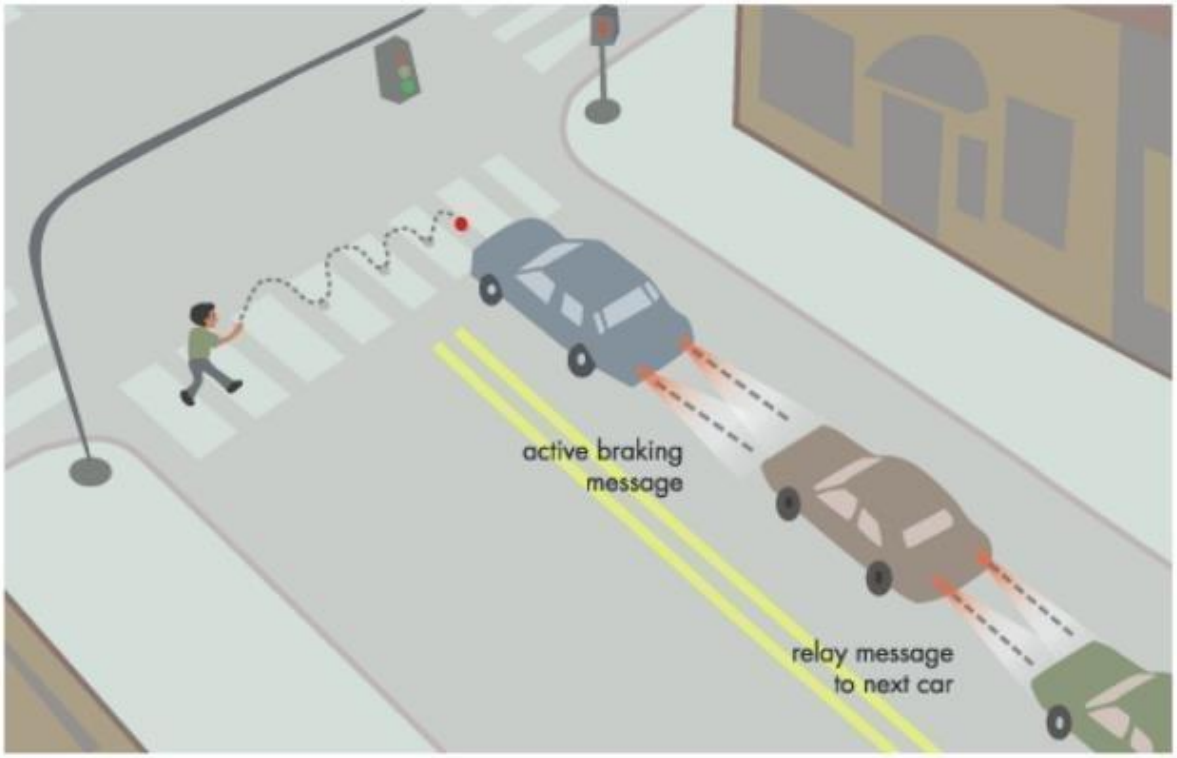

Figure 1.3: Safety application (brake messaging) [6]

1.4.2 Comfort applications

This category includes all the applications that contribute to the driver's comfort and do not fall within the scope of traffic management or road safety (see Figure 1.4). These applications arise, therefore, as services are provided to the driver [6].

Figure 1.4: An example of comfort application in VANETS [6]

1.4.3 Road Traffic safety applications

They aim to improve the safety of passengers on the roads by advising vehicles of any dangerous situation. These applications are generally based on a distribution, periodic or not, informative messages allowing drivers to know about the road conditions and neighboring vehicles. Famous examples of services in this application category are collision warnings, warnings about road conditions, assistance passing and changing lanes, etc. [7].

1.5 VANETs architectures

In VANETs there are three modes of communication: Vehicle to Vehicle (V2V), Vehicle to Infrastructure (V2I), hybrid communication [8][9].

1.5.1 V2V

The V2V architecture includes only opportunistic communications between vehicles (see Figure 1.5). When a vehicle encounters other nearby vehicles (i.e., neighboring nodes), users can then communicate and exchange information during the contact period (send, receive, and retransmit packets)

V2V communication is inexpensive and offers a high transmission rate. On the other hand, this communication model poses challenges such as the infrequent contacts between vehicles in a low-density environment, the short duration of connections due to the speed and quality of the link, and the selection of relay nodes [9].

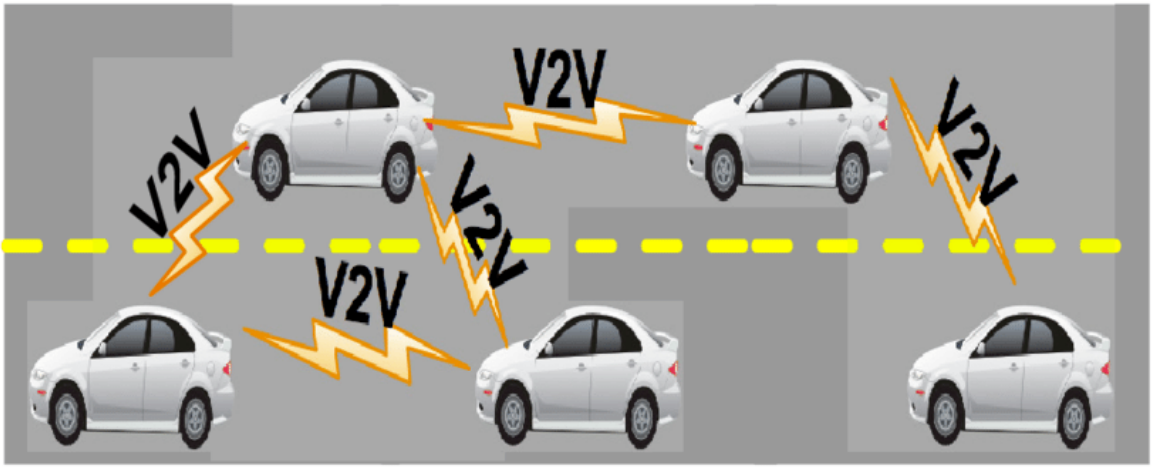

Figure 1.5: Vehicle-to-vehicle communication (V2V) [10]

1.5.2 V2I

The V2I architecture operates under the assumption that users must continually access a centralized server that manages their interactions with other users, even when the vehicles are physically close (see Figure 1.6). In such an architecture, there is no direct interaction between vehicles. In the literature, this communication is known as V2I. Vehicles communicate indirectly through existing infrastructures such as RSUs and cellular networks. Until today, the RSUs are not widely used because of their high cost. In addition, cellular networks are overloaded with the increase in demand and do not cover all areas [9].

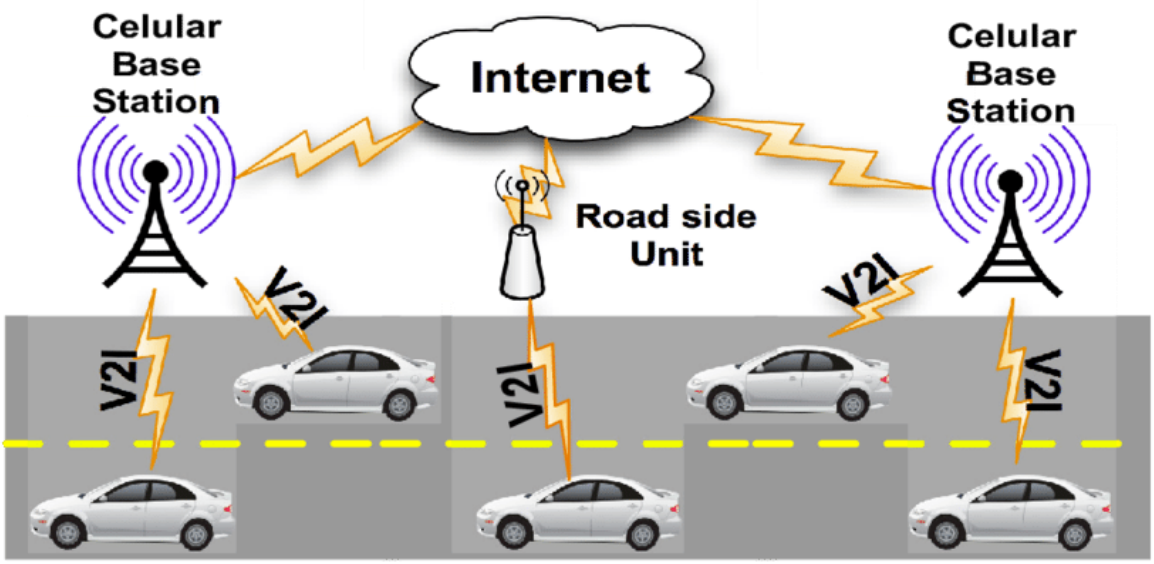

Figure 1.6: Vehicle to infrastructure communication (V2I) [9]

1.5.3 Hybrid Communication

The hybrid Architecture Includes both V2V communications and V2I communications. The infrastructure can be used optionally or when present. In areas with no infrastructure, this architecture serves to extend the logical range of vehicles to reach faraway RSUs as shown in Figure 1.7 below [9].

Figure 1.7: Hybrid communication in a VANET network [10]

1.6 Characteristics of VANETs

VANETs have the particularity of having very high mobility (mobile nodes circulate at very high speed). The dynamic topology causes many reconfigurations (update of routing tables, etc.) [9].

- **Energy and storage capacity:**

  On the contrary of MANETs networks, where the energy constraint represents a challenge for researchers, elements of the VANET network have enough energy that can power the various electronics equipment of an intelligent car. Therefore, the nodes are supposed to have a large data processing and storage capacity [9].

- **Network size**:

  In view of the significant advancements in wireless communications and the low costs of associated equipment, vehicles that already massively integrate systems like GPS devices and Bluetooth equipment can be easily rendered as smart vehicles and will be easily deployed on a large scale [9].

- **Network topology and connectivity:**

  A vehicle can quickly join or leave the network in a very short time, which makes very frequent topology changes. In addition, problems such as frequent network partitioning the second reason for partitioning an inter-vehicular network is that the probability of formation of an uninterrupted chain of vehicles with radio range increases exponentially [9].

- **Security and anonymity:**

  The importance of the information exchanged via vehicular communications makes the operation of securing these networks crucial, which is a prerequisite for the deployment of VANETs [9].

1.7 Beaconing

Beaconing is an operation performed by each vehicle consisting of broadcast periodic messages (called "beacons") to other nodes in their radio area. The purpose of these messages is to allow each vehicle to inform others of its contexts, such as identity, geographic location, speed, and direction. Beacon messages may include beacons Other information needed for various contacts and services in VANETs.

1.8 Security in VANETs

VANETs security is a major problem that must be addressed to ensure the greatest possible adaptability to these networks. Due to the importance of the exchanged information, the overwhelming number of users, dynamic structure, and sporadic connectivity. Malicious entities can tamper with the exchanged data to cause accidents and endanger people's lives. To ensure the proper deployment of these networks, appropriate safety mechanisms must be implemented to prevent this type of attack. In this section, we will specifically address the requirements and challenges related to security and the various security mechanisms in order to secure the information that is exchanged over these networks. We'll also provide a brief description of the benefit of implicit testimonials. Its advantages over explicit certifications are cited. Hence the standard wave DSRC IEEE 1609 focused on security, i.e., IEEE 1609.2 [11].

1.8.1 Security requirements and challenges

In this section, we will also discuss the main requirements and other challenges for security in VANETs. A security system in VANETs should satisfy the following requirements [12]:

a-Confidentiality

Confidentiality identifies the sensitivity of information or assets to unauthorized disclosure. This security requirement makes it possible to guarantee the non-disclosure of data transmitted over the network to unauthorized parties. Only authorized parties can access it through the network, and confidentiality, therefore, consists in preserving vital vehicle information through the application of asymmetric and symmetric cryptography algorithms, which prevents malicious entities from tracking and listening to messages about a targeted vehicle in the network.

b-Integrity

Integrity is the accuracy and completeness of information and assets, as well as the authenticity of transactions. This security requirement ensures that the messages disseminated will not be modified or altered intentionally or accidentally between the transmission and reception phase by unauthorized (malicious) entities. This security requirement thus aims to provide recipients with the power to detect data manipulations carried out during their transmission by malicious entities and to reject the corresponding packets. Integrity can be achieved primarily through the use of hash functions and cryptography on specific fields of the packages.

c-Availability

Availability is the accessibility of an information system or the data it contains, at the appropriate time, to carry out certain processes. This security concept ensures that any authorized entity can access network resources at all times with an adequate Quality of Service (QoS). Indeed, all the participants in the network must have effective and rapid access to the various traffic management services, security and requested comfort applications. To achieve a good level of availability, it is essential to install hardware and implement high-performance security protocols. However, this concept is mainly threatened by Denial of Service (DOS) and black hole attacks, which are very difficult to predict and control.

d-Non-repudiation

Each entity broadcasting a message on the network cannot deny it or retract from having issued it. It helps identify malicious entities that attempt to commit illegal acts, thereby ruling out any possibility of an attacker injecting erroneous data without being immediately identified. In the context of VANETs, the digital signature is used to guarantee the non-repudiation of messages concerning security and traffic management applications.

e-Authentication

This security requirement allows network entities to ensure the correct identity of the entities with which they communicate. Authenticity allows the different entities of the network to trust the data and disseminated messages.

f-revocability

Revocability allows to have the necessary mechanisms to exclude malicious nodes and reveal their true identities.

g-access control

It makes it possible to ensure that the nodes access the resources according to well-defined rules and privileges.

1.8.3 Types of attackers

Attackers can be classified into categories which are [13]:

- **Intern/Extern:** The internal attacker has the cryptographic keys that allow him to communicate with other nodes in the network. Cryptographic techniques alone are not sufficient to defend against this type of attackers. they are limited in the variety of attacks they can provoke.
- **Malicious or Rational:** Malicious attackers have no personal benefits to attack. They use all means to cause the malfunction of the network, whatever the costs and the corresponding consequences.

- **Passive / Active:** The passive attacker listens to the data exchanged in the network, while the active attacker can act on the exchanged data.

1.9 Attacks in VANETs

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

1.9.1 Attacks on availability

The following attacks have been identified:

-Denial of Service (DOS): DOS (Denial of Service) attacks (see Figure 1.8) can be performed by malicious network participants or foreign entities to render a service unavailable to network users through unnecessary flooding of messages. It could be performed by compromising enough RSUs or making a vehicle broadcast infinite messages in a period of time.

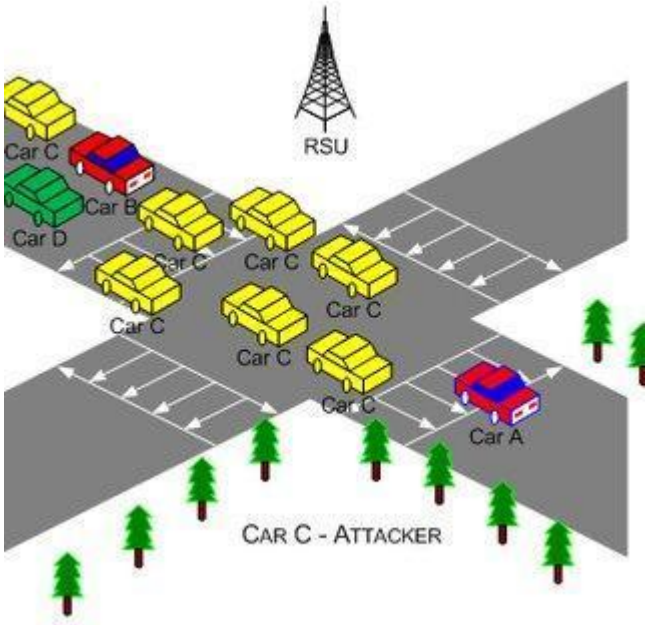

Figure 1.8: DOS Attack [15]

-Falsification of disseminated data: In this attack, the adversary composes a message containing erroneous information on the condition of the road, an emergency braking message, or another on road traffic conditions, for example. This falsified information affects the availability of correct data for driver assistance.

-Malware: The injection of malware, such as viruses or worms in 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 when they receive software updates. In these attacks, the malicious entity may aim to degrade the efficiency of the network.

-Black Hole attack: A blackhole (see Figure 1.9) is formed when traffic is redirected to one or more nodes that do not deliver these packets to their destinations.

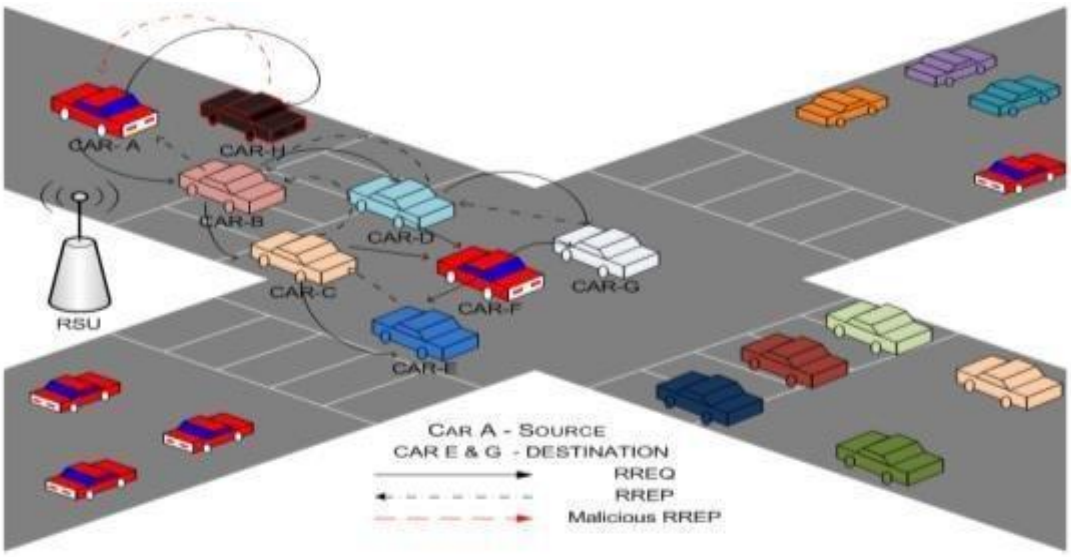

Figure 1.9: Blackhole attack [16]

1.9.2 Attacks on authentication

The following attacks can be distinguished:

- **Spoofing:** In this case, the malicious entity takes on the role or identity of another entity. The spoofing can also relate to any other element making it possible to identify an entity on the network in order to be able to impersonate this entity and act on its behalf, to achieve levels of privilege and unauthorized access, as in the case of police vehicle theft, which is authorized to control network vehicles and therefore access their information and personal data.
- **GPS Spoofing:** GPS spoofing is an attack in which a radio transmitter located near the target is used to interfere with legitimate GPS signals. The attacker can transmit no data at all or could transmit inaccurate coordinates.

1.9.3 Attacks on Confidentiality

Eavesdropping is the most prominent attack over VANETs against confidentiality. Its goal is to illegally access confidential data and collect information about road users without their knowledge.

1.10 Conclusion

This chapter defines the VANET, its architecture, its various characteristics, its application areas. The main purpose of the VANET is to facilitate driving and make the road more pleasant, more comfortable, and more fun for drivers and passengers. It is also a question of clearing up road traffic for the drivers. VANET attacks present a primary danger, as they threaten the security of drivers and passengers. They can also cause accidents and congestion on the road. It is very important to implement the protocols and security mechanisms in order to control the network, to preserve the safety of drivers, passengers, and vehicles, and also allow users to use this technology with confidence. In the next chapter, we present some recent research that has been interested in security.

Chapter 2

Authentication in VANETs

2.1 Introduction

The security of VANETs is a major issue that must be addressed in order to guarantee the well network functioning. Messages related to security can be falsified by malicious entities in order to cause accidents and endanger people's lives. Therefore, to ensure the functioning of these networks, we have to quickly detect the malicious node.

In this chapter, we present the techniques for detecting and revoking nodes.

2.2 The basics of Security in VANETs

In this section, we present the basics of security in VANETs. We present the PKI, the ECDSA algorithm [17].

- **PKI (Public Key infrastructure)**
  The PKI ensures this security through a set of services:
  - Registration of resources (human or computerized).
  - Certificate management, revocation list, and users.

- **ECDSA Algorithm**
  The ECDSA is an Elliptic curve digital signature algorithm [18], this algorithm is for encryption, and it is adopted by IEEE Standard 1609.2. It requires a key of 224 bits for OBUs and 256 bits for RSUs and certificates [19] [20]. The cryptographic element size is in bytes.

2.3 Infrastructure components

The key management infrastructure is based on several components that are essential for its operation. Among these components [21] [22]:

A. Root Certification Authority (CA)

It's an important component of the PKI infrastructure due to its central role in the various kinematics of exchanges within a PKI.

The CA is responsible for issuing and managing the certificates. Indeed, it generates public key certificates and ensures the integrity and authenticity of the information contained by signing them with its private key. To issue certificates, it must first receive certification requests containing the public key of the entity requesting it.

B. Registration Authority (RA)

It acts as an intermediary between the user and CA and depends on the latter. It is responsible for verifying everything concerning the user, his identity, the concordance between private and public keys to certify, and ensuring that he has the necessary rights to request certificates. In summary, the authority's task is to manage the certificate requests it receives from different entities and to design the key pairs that are specific to them.

C. Warehouse Certificate

At the vehicle OBUs level, there is a warehouse of certificates with public keys and their corresponding private keys. They ensure the security of a public key to prevent security failures associated with identity theft and written modification.

D. Certificate Database

It contains the certificate requests, the certificates to be issued, and the certificate revocation list.

2.4 Standardization of secure messages in VANETs

In this section, we present the format of the digital certificate, the format of a secure message in VANETs [18].

2.4.1 The format of the digital certificate

In order to strengthen the concept of digital signature, it should be combined with a digital certificate issued by CA. It should be noted here that certificates are data structures describing digital identities and making it possible to prove the identity of the owner of a public key.

Thanks to asymmetric cryptography, the certificate attests to the authenticity of the public and private key pair and allows vehicles to be uniquely identified.

Figure 2.1 shows the format of the digital certificate, which includes:

- **Version**: this field represents 8 bits of data is what the field is made of and presents the version of the certificate.
- **Signer info**: this field allows checking the validity of the certificate.
- **Subject info**: this field represents the type of the certificate and the context of its use.
- **Subject attributes**: this field is made of 8 bits and refers to information of the previous field.
- **Subject restriction**: this field is referring to the certification validity period and the geographic region.

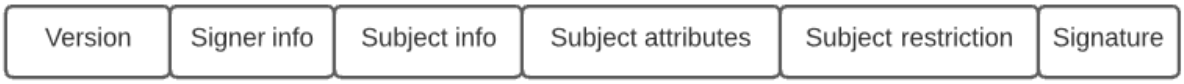

Figure 2.1: Digital certificate format

2.4.2 The format of a secure message in VANETs

Figure 2.2 shows the Simplified format of a secure message in VANETs that refers to the format of signed and encrypted messages. We have the data that we want to authenticate, the digital signature, and the certificate to check the validity of the public key.

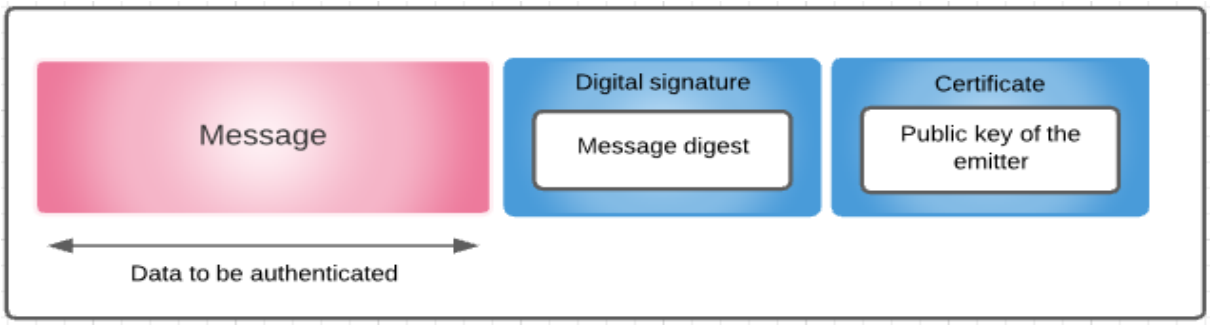

Figure 2.2: Simplified format of a secure message in VANETs

Figure 2.3 format of a secure message according to the 1609.2 standards.

The message header includes the protocol version and the type of message, the signer's information, the data to be signed, and the digital signature calculated according to the ECDSA algorithm.

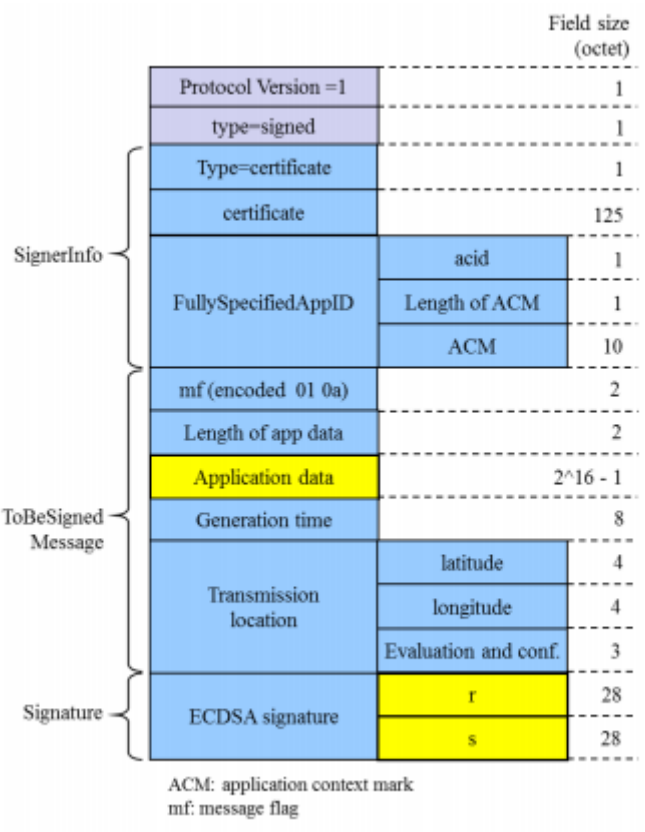

Figure 2.3: Format of a secure message according to the 1609.2 standards [23]

Figure 2.4 presents an example of a secure message following the ETSI standard [24].

Element	Value	Description	Length
SecuredMessage			
protocol_version	0x02		1
header_fields <var>	0x8091	Length: 145 octets	2
type	0x80	=signer_info	1
type	0x02	=certificate	1
certificate	...	certificate of signer	141
type	0x05	=its_aid	1
its_aid	...		1
payload			
type	0x01	=signed	1
data <var>	0x01	Length: 1 octet	1
[data]	...	payload	1
trailer_fields <var>	0x43	Length: 67 octets	1
type	0x01	=signature	1
signature			
algorithm	0x01	=ecdsa_nistp256_with_sha256	1
ecdsasignature			
R			
type	0x00	=x_coordinate_only	1
x	...		32
s	...		32
Total size: 219 bytes			

Figure 2.4: Example of a secure ETSI message [25]

2.5 Problems related to authentication in VANETs

The attackers always aim to inject spoofed information, and that happens according to the IEEE 1609.2 standard that allows the vehicles to broadcast from 1 to 10 beacons to its neighbors, but to face this kind of attacks by using the ECDSA signature by having the vehicles public and private cryptographic keys and certificates managed by CAs which declare that these vehicles are valid participants [18].

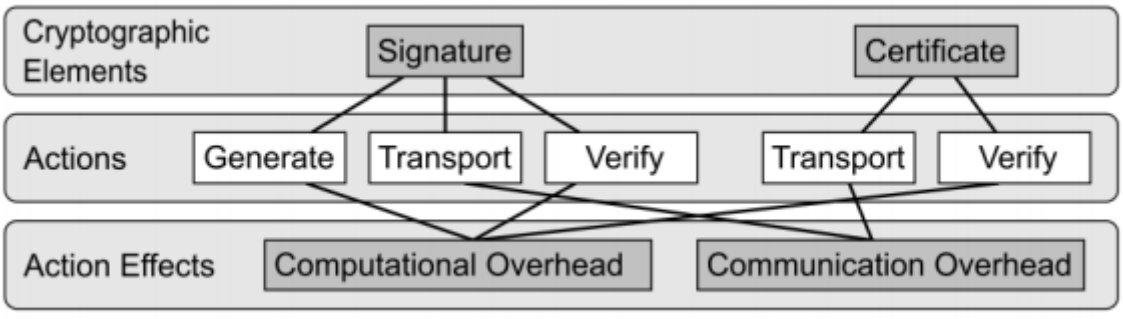

Figure 2.5: The authentication overhead [26]

Figure 2.5 presents the overhead added for security. It increases the bandwidth consumed and the communication delays.

2.6 Certificate revocation

2.6.1 CRL

CRL (Certificate Revocation List) is a list of digital certificates that have been revoked by the issuing CA before their scheduled expiration date and should no longer be trusted. Due Certificates have a period of validity during which nodes are considered legitimate members [27].

We use the mechanism that allows distributing CRL to all the nodes of the network. From this list, we can recognize the nodes that their certificate should be neglected. According to this mechanism, we can decrease the capabilities of attackers who control the corresponding private keys.

Figure 2.6 presents how CRL is divided into N parts where m (M<N) parts are sufficient to reconstruct the CRL.

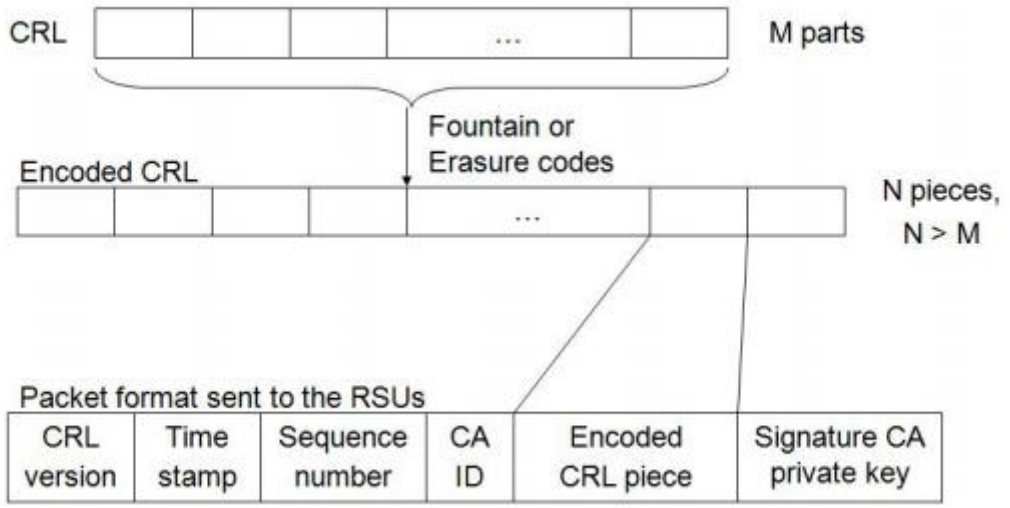

Figure 2.6: Encoding the CRL [27]

2.6.2 Distribution of certificates

To communicate with the RSUs, the vehicles should first download the latest CRL for safe communication as shown in Figure 2.7.

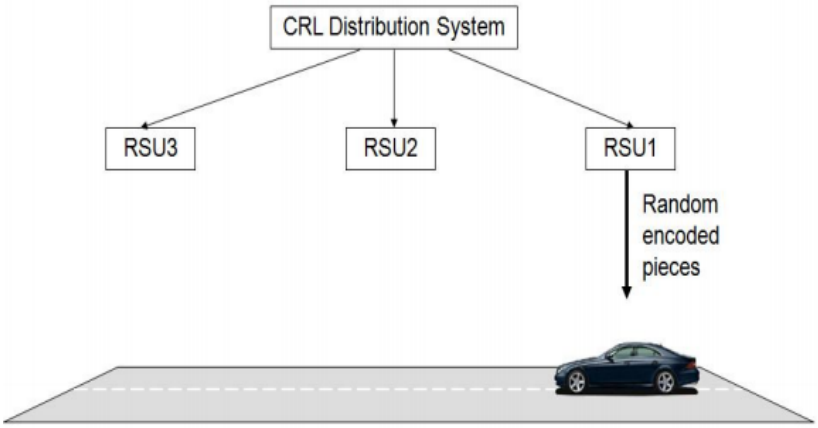

Figure 2.7: A simple certificate distribution system [27]

2.7 Revocation of malicious nodes

The revocation of nodes consists in marking or considering their cryptographic keys invalid: Either via the dissemination of the revocation messages in a limited geographical area. This category of revocation approaches is a local revocation, which is made by a set of nodes that exchange messages of accusation between themselves [28] [29], or via the reception of the CRLs, we call this revocation global or centralized [30] [31].

Local revocation is essential because it allows new neighboring nodes to quickly avoid malicious nodes.

Adding the suspected node to the blacklist comes after receiving a set of accusation messages that should fulfill the revocation condition. It should be stressed that the entity responsible for the detection of malicious nodes is the IDS (Intrusion Detection System).

Figure 2.8 presents an accusation message against a vehicle exchanged between vehicles A, B, and C.

This message of accusation containing the accused nodes' signature that is sent to the CA, which can include the id of M in the next CRL if there are enough accusations against it.

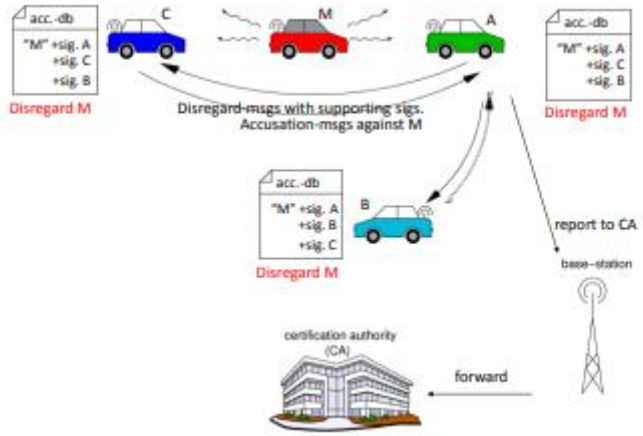

Figure 2.8: Reporting of accusation to CA [27]

2.8 Revocation in VANETs

There are some techniques in revocation of VANETs. In what follows, and we mentioned some of them:

2.8.1 LEAVE revocation system

The leave system (Local Eviction of Attackers by Voting Evaluators), is a system proposed by Raya et al. [32]. This system is dependent on minimizing the weights of the accusations of the nodes according to the number of accusers. These weights are calculated as:

$$W_i = 1 - \frac{A_i}{P_i}$$

Where P_i represents the number of neighbors common to the evaluator and to the evaluated node, and A_i represents the total number of accusations against node i.

The main principle of LEAVE is simple: the neighbors of the misbehaving vehicle temporarily evict it.

The accusation rate is calculated as follows:

$$Q_j = \frac{1}{p_j} \sum_{i=1}^{Pj} W_i . \delta_{i,j}$$

Where $\delta_{i,j}$ =1 if the node i accuses node j, $\delta_{i,j}$= 0 otherwise.

Figure 2.9 shows how the leave revocation technique works:

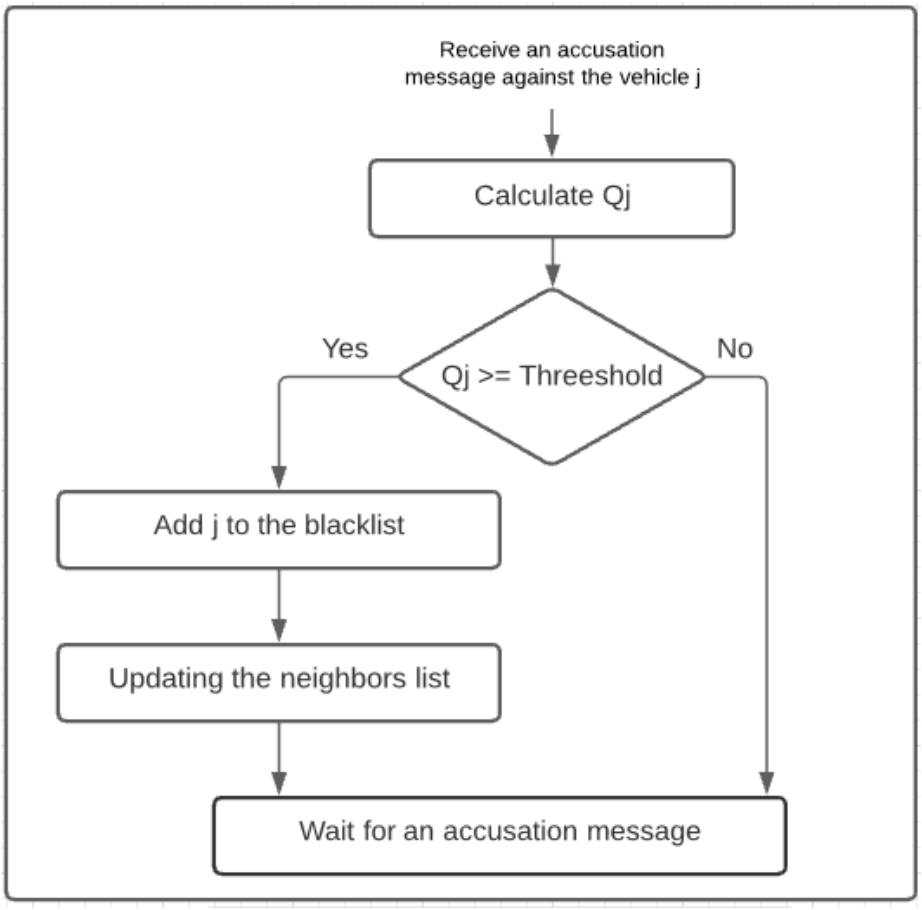

Figure 2.9: Flow chart of LEAVE revocation technique

2.8.2 Stinger system

The stinger system consists of adapting the revocation strategy by suicide attack to the VANET network. In Stinger, the nodes that accus and the accused nodes are penalized only for a limited time in order to defend against attacks from falsified accusations [33].

Figure 2.10 shows the attack of falsified accusation on stinger system, M considers the malicious node who provokes the honest node to issue Sting messages to force the revocation of the honest nodes, then malicious M moves to another region and repeats the same attack scenario to cause the revocation of other honest nodes. But, the temporary revocation mechanism used by Stinger reduces the impact of this attack.

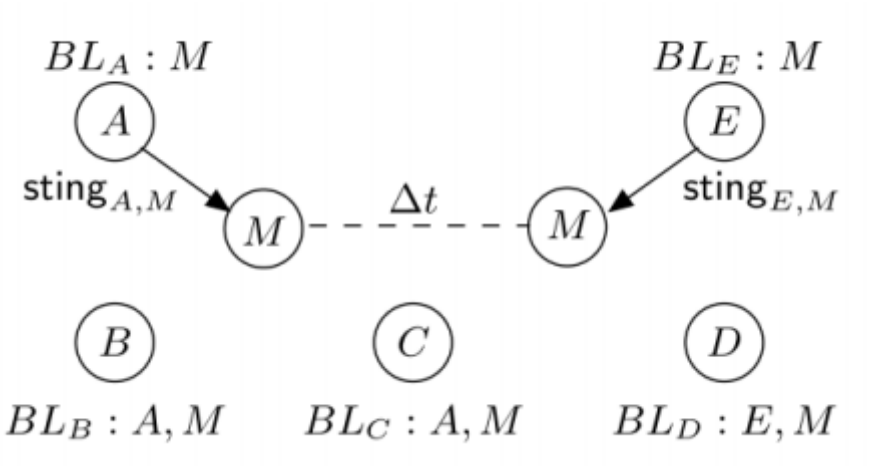

Figure 2.10: Attack on the Stinger System [33]

2.8.3 SLEP system

The SLEP revocation system (Suicide-based Local Eviction Protocol) is a variant suitable for suicide attack revocation system VANETs. In this system, the two nodes accuser and accused are added to the blacklist. There are two ways in the SLEP system for one node in VANETs to be aware of the misbehaving node:

- In the detection range of the misbehaving node and detect the misbehavior directly.

- It has received the suicide message accusing against the misbehaving node. We let every node maintain an updated local blacklist to record the misbehaving history, the format [34].

Figure 2.11 shows the message format of this system. It contains the public keys of the accuser and the accused, the time of the accusation, the cause, and the digital signature.

PID of accused node	PID of accuser	Time	Reason	Signature of accuser

Figure 2.11: Format of the local blacklist [35]

2.9 Comparative analysis

The performance of LEAVE, STINGER, and SLEP systems must be carried out according to certain criteria. In this analysis, the degradation of one of these criteria may influence.

Table 2.1 summarizes the performance of previous revocation techniques in terms of these criteria:

1. The processing and overhead of accusation messages

There are two main aspects in studying performance, the number of clock cycles and the bandwidth consumed. With three possibilities: high, medium, and low, they are given as follows:

High: This indicates a high number of the clock cycle.

Medium: The consumption bandwidth is high.

Low: The consumption bandwidth is low.

2. NNMA (the Necessary Number of Charging Messages for Revocation)

There are many revocation techniques, and each of them has its method to send the suspected node to the blacklist.

According to this method, to revoke a node who has suspicious actions be according to a number of accusation messages.

3. The impact of the FAM attack (Falsification of accusation Messages)

Malicious colluding nodes can spoof accusation messages in order to degrade performance by causing honest nodes to be revoked.

It is small if there are strong mechanisms to filter malicious accusation messages. However, the impact is medium if there are mechanisms to reduce the weight associated with accusation messages.

4. The revocation strategy

It can be performed according to the following approaches:

- **The Voting System (VS):** The voting system is made to calculate the rate of the node that accuses another node and, depending on this rate, accuse the node that is malicious and revoke it if the rate exceeds a predefined threshold.
- **The Accusations Weighted**: The rate of accusation is the weighted average of the accusation of the nodes.
- **Suicide attack:** The suicide attack allows the accusing to eliminate the accused node

5. The revocation architecture

There are two types of centralized and decentralized architecture:

- **Centralized:** The revocation requires communication with a predefined entity.
- **Decentralized:** The revocation requires one or more nodes that can revoke a node without the intervention of any predefined entity.

	Overhead	NNMA	FMA impact	Revocation strategy	Revocation architecture
LEAVE	High	High	Low	Accusations Weighted	Decentralized
STINGER	Low	Low	High	Suicide Attack	Decentralized
SLEP	Low	Low	medium	Suicide Attack	Decentralized

Table 2.1: Comparative study of revocation protocols in VANETs

Table 2.1 presents a comparative study between the revocation protocols in the VANETs.

The accusation message in the LEAVE revocation system uses the digital signature, which causes a high overhead for processing and bandwidth consumed in the event of an attack. The advantage of LEAVE is the use of a very effective weighting system against falsification of accusation messages.

The STINGER revocation system is based on a suicide attack. Furthermore, nodes broadcast Sting messages only for a limited time.

The SLEP revocation system is a variant of a suicide attack. It looks like a STINGER. But, SLEP uses the backoff mechanism. It helps reduce the false positive rate on the one hand and increases the detection time on the other.

2.10 Conclusion

In this chapter, we have presented the basics of security in VANETs, Problems related to authentication in VANETs and different techniques for detecting and revoking malicious nodes. Finally, we presented a comparative study of the different malicious node revocation techniques

Chapter3

The CBRP revocation system

3.1 Introduction

To ensure the correct flow of data and the quick detection of malicious nodes, we have proposed a VANET network revocation system CBRP (Category Based Revocation Protocol). CBRP is designed to improve the security of communication protocols in VANETs. We ensure that our protocol takes into consideration the mobility model and the routing requirements in this environment including the quickness of detection as well as the availability of the network.

In this chapter, we provide a comprehensive description of the adversary model. Next, we present our CBRP protocol. Finally, we analyze its performance with different simulations.

3.2 Adversary model

The main goal of our proposed system is to exclude malicious nodes from the process routing in VANET. By analyzing the traffic and determining the classes of malicious nodes according to the misbehavior and its impact degree. Malicious nodes can be considered as nodes controlled by malicious entities, or nodes with failed equipment. We assume that there are several attackers in the network with their own certificates, they can communicate with other members of the network and send messages.

Also, we assume that the purpose of the malicious nodes is to send false messages about their locations or alerts that may threaten people's lives, they can also target the network by sending various attacks, such as a Denial-of-service attack, or trying to consume a higher share of the bandwidth. In our CBRP system, we will capture the traffic and identify the attacks so that these attacks can be categorized into categories which we will discuss subsequently.
Honest nodes monitor the activities of the neighbors, and each time they detect a malicious behavior they should inform the neighbors by sending an accusation message against them.

In the network, a set of nodes can be separated into two subsets honest and malicious nodes. Figure 3.1 presents the types of accusations in an accusation graph, the red nodes representing

malicious nodes and the green nodes represent honest nodes. From the accusation graph we can distinguish the following types of accusations:

1- The honest nodes accuse the malicious node if detected by IDS.

2- The malicious nodes accuse the honest nodes, and this can be considered as an attack against the revocation protocol to cause a denial of service. To succeed in this attack, attackers need a set of colluding malicious nodes.

Finally, identifying all malicious nodes from the accusation graph is not easy. To exclude a high number of honest nodes from the network, attackers can use any combination of accusations and thus reduce the chances of correctly delivering security messages.

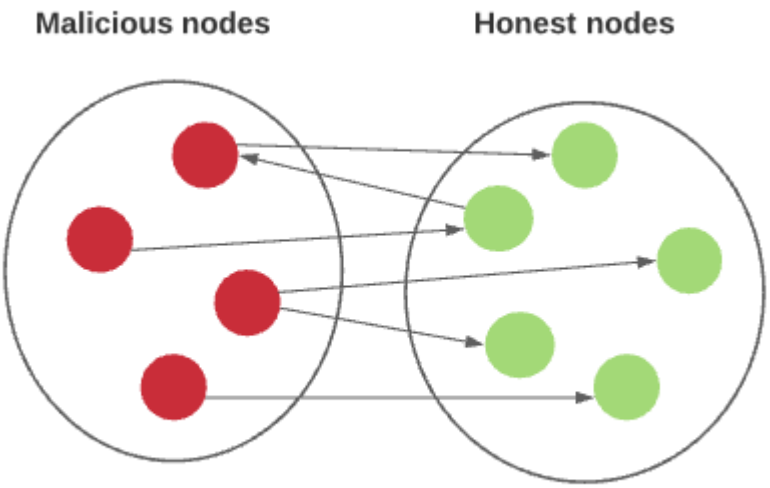

Figure 3.1: The types of accusations in an accusation graph

3.3 The CBRP Protocol (Category Based Revocation Protocol)

Unlike the classical revocation protocols that block all malicious nodes that have been detected. The CBRP is a system proposed to improve both the security of routing protocols and network traffic quality in VANETs. To this end, we ensure that our protocol does not block malicious nodes permanently, except if their actions threaten people's lives. This process is carried out by filtering the nodes after classifying them according to the degree of severity, and this is what we will address next.

3.3.1 Attacker model

In our attacker model, we have considered a classification of attacks depending on the severity degree. In reality, the categories that can be distinguished are very large, However, we have concentrated on these three categories:

- Category 1: It consists of selfish attacks that target any behavior targeting the availability of services and information.
- Category 2: It consists of attacks that target the honest nodes such as sending accusation messages against them.
- Category 3: In this category, the impact is dangerous and includes the transmission of false information that threatens people's lives. For example, sending a false report of an accident.

3.3.2 Description of the system

Our system consists of three modules: IDS, Protection Module, Alert Advertise Module.

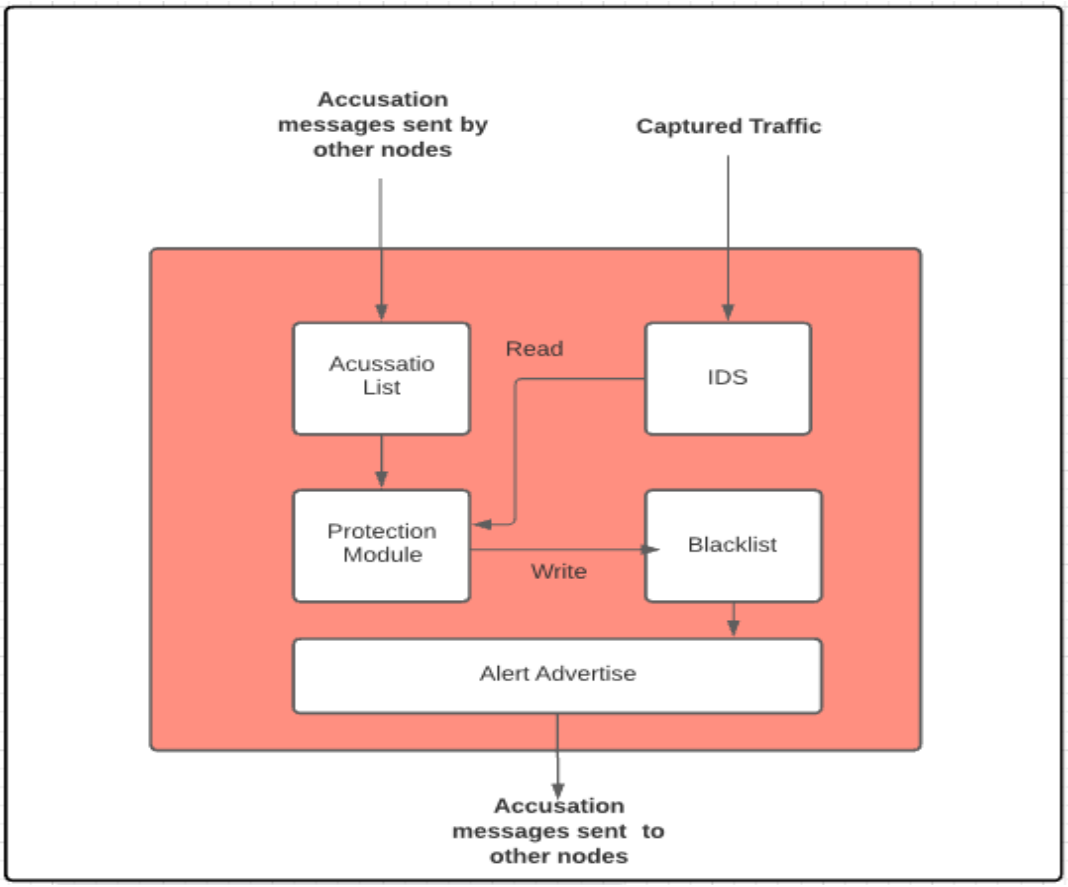

Figure 3.2: Overview of CBRP

Figure 3.2 represents the modules of the system and their interactions. The IDS analyzes the activities of all nodes and detects malicious nodes. Each node must activate promiscuous mode in order to capture the packets sent by its neighbors, and analyze them and gather the observation of the nodes.

The protection module implements the punishment mechanism of misbehavior actions, it receives the accusation list sent by other nodes and reads what was captured from the IDS module. This module begins by classifying the malicious nodes and determining the punishment period.

In this case, if the malicious node is completely blocked, the protection module will add it in the blacklist and then pass it to the alert advertise module, which in turn informs the other nodes by sending accusation messages.

The purpose of this last operation is to avoid dealing with this malicious node, which poses a danger in the event that it manages to infiltrate again into the network.

The punishment period is given according to each category as follows:

- Category 1: In general, we block the nodes of this category for a limited time. We propose the initial punishment period to be 30 seconds due to the fact that it cannot be considered dangerous. Each time the node repeats the suspicious action we will duplicate the time of the punishment.

  It should be stressed that the punishment time for this category can be formulated as follows:

  $$PT=PT*n$$

  Where PT is the punishment time interval, and n is the number of rounds in which the malicious node repeats its malicious activities.

- Category 2: In this category the malicious nodes are detected locally and endorsed by accusation messages from honest nodes. In this case, we increase the punishment period to three minutes. If the punishment period expires and we discover another misbehaving node from the malicious accused node, our system will ban it permanently.

- Category 3: This category also comprises malicious nodes detected based on a signature of a dangerous attack. Thus the confidence about this attack is very high, that's why the CBRP system will block this type of malicious node permanently.

The nodes use the Watchdog mechanism. This mechanism consists of activating the Promiscuous mode, which allows nodes to capture packets that are not theirs[36].

3.4 Simulation

3.4.1 The simulation environment

We used the NS2 tool, which is an open-source simulator used in searches related to computer communication networks. The parameters used in the simulations for our proposed system are summarized in the following table:

Parameters	Setting
Simulator	NS-2 version 2.30
Simulation time	10 minutes
The number of nodes	300
The mobility generator	IMPORTANT
MAC protocol	IEEE 802.11
Forwarding strategy	Greedy
Malicious node rate	30%
The nature of the antennas	Omnidirectional

Table 3.1: Simulation environment

3.4.2 Performance metrics

We use the two following metrics EED (End-to-End Delay) and PDR (Packet delivery ratio) to understand and evaluate the performance of our CBRP (category based revocation protocol) protocol:

- **PDR (Packet Delivery Ratio):**

  It represents the ratio between the number of data packets successfully delivered to the destination:

$$\mathbf{PDR} = \frac{\sum \boldsymbol{Number\ of\ packet\ received}}{\sum \boldsymbol{number\ of\ packet\ sent}} \boldsymbol{X100}$$

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

  It represents the sum of taken time from the source to the destination for a packet to reach:

$$\mathbf{EED} = \frac{\sum(\boldsymbol{packet\ arrival\ time - send\ time})}{\boldsymbol{number\ of\ packet\ received}} \boldsymbol{X100}$$

3.4.3 Simulation results and analysis

A. Simulation Scenarios

In this section, we represent the two scenarios which are:

1. **First scenario without attack and without CBRP**

   This represents the normal execution of the protocol without any attack or CBRP. We set this scenario to see the difference that may arise after evaluating our proposed protocol in terms of the EED and PDR.

2. **Second scenario with attack**

   We divided this scenario into two parts:

   - With the implementation of the classical revocation protocol, which blocks all malicious nodes, regardless of the type of behavior they performed. We set this

scenario to compare with our protocol and see if our protocol is better in terms of EED and PDR.

- With the implementation of our proposed protocol CBRP, which is unlike the previous protocol, it makes classifications and gives different punishments duration according to the type of malicious behavior.

B. Simulation results

In this section, we provide the obtained results which measures the impact of malicious nodes rate in terms of EED and PDR:

1. First scenario

This scenario does not contain any malicious nodes. It indicates that there are no changes in terms of PDR and EED. The PDR is about 92% and the EED is nearly 18ms.

2. Second scenario

- The Classical revocation protocol:

As shown in Figure 3.3, the PDR drops to 60% for the percentage of malicious nodes that does not exceed 15%, while it has reached 22% with the percentage of 30% malicious nodes.

It can also be noticed in Figure 3.4, that the EED has risen from 18ms to the highest period of 66 ms with a ratio of malicious nodes of 100%.

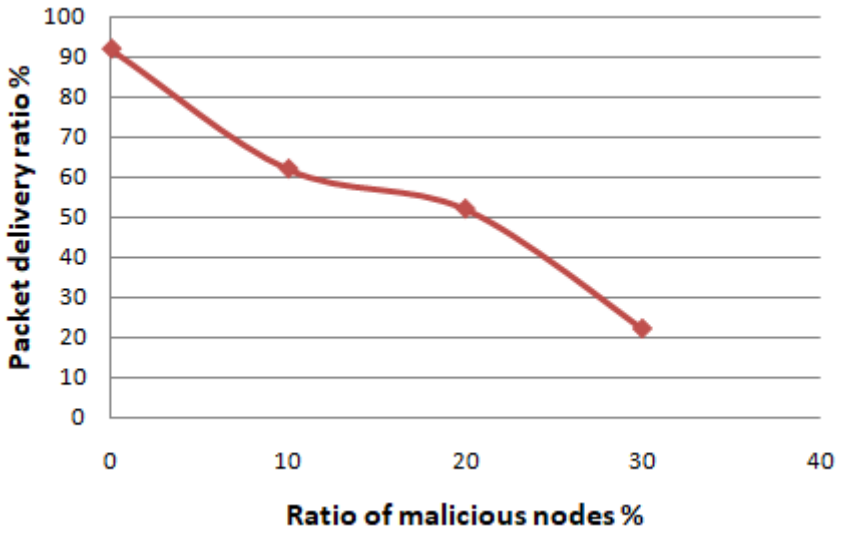

Figure 3.3: PDR (Classical revocation protocol)

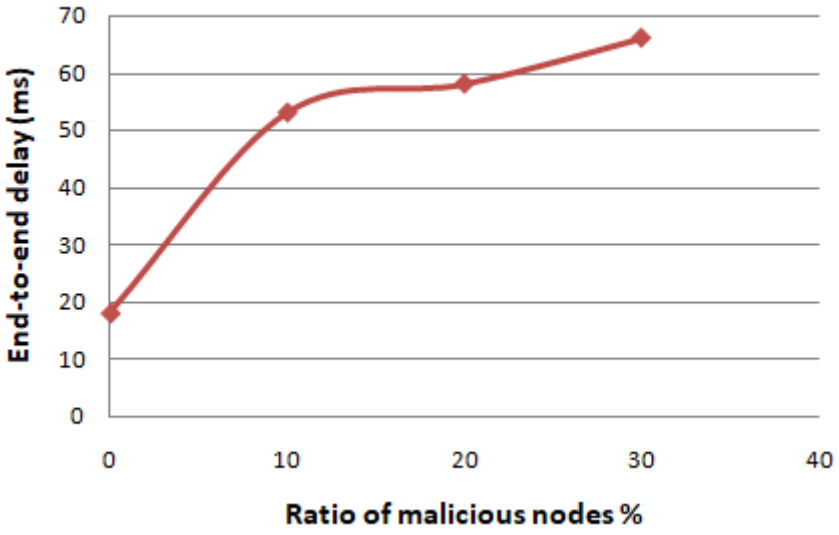

Figure 3.4: EED (Classical revocation protocol)

- CBRP:

As shown in Figure 3.5 that represents the CBRP system, it is clear that the PDR drops to 79% for the proportion of malicious nodes that does not exceed 20%, while it has reached 45% with 30% of malicious nodes.

It can also be noticed from Figure 3.6 which represents the scenario of our proposed, the EED has reached a value of 63 ms.

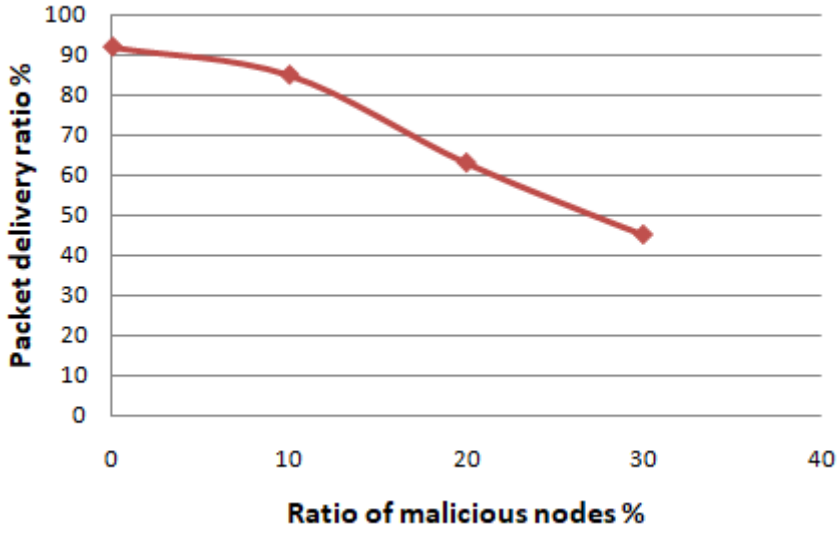

Figure 3.5: PDR (CBRP)

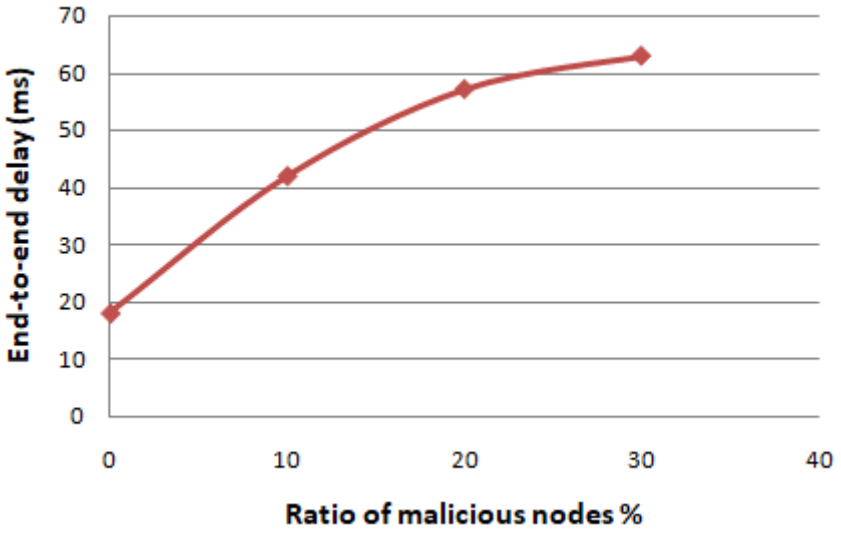

Figure 3.6: EED (CBRP)

The apparent high jump of the EED value from 18ms to 66s for the classical revocation protocol and from 18ms to 63ms for our CBRP protocol can be explained due to the deletion of the malicious nodes which represent the short path to the destination while the rest of honest nodes are representing the long path to the destination and that's what explains the jumping of the EED. While the reason for the decrease in PDR is the erasure of the packets of malicious nodes.

By comparing the classical revocation protocol with our proposed CBRP system, it can be noticed clearly that our protocol is better in terms of EED and PDR, and this indicates that our proposed CBRP system has improved the quality of service.

3.5 Conclusion

The malicious nodes can attack VANETs which cause them dangerous impacts and others don't. To take advantage of the classification of attackers, we have proposed a CBRP category-based revocation protocol.

According to the two metrics, the simulation results showed that CBRP has a better performance compared to the classical approach in terms of EED and PDR.

General conclusion

VANETs are vulnerable to attacks by malicious entities and cause threats to people's lives by injecting messages for malicious purposes, so these networks can only be deployed after investigation and assurance of their security.

The classic model of revocation protocol can detect malicious nodes even before interacting with them. It is immediately blocking the malicious nodes permanently and considering all the attacks the same, regardless of their impact and their categories.

In this work, we have proposed a new approach for certificate revocation called the CBRP system. It aims to improve both the security of routing protocols and the quality of service in VANETs and classify the attack into categories to distinguish the different impacts of the network.

We evaluated the performance of our solution, and simulation results showed that CBRP outperforms others, which shows that it provides high PDR and Low latency in presence of a high rate of attackers.

In the future, we aspire to improve the CBRP system by adding other categories that will further improve the security and quality of service in the VANETs. These classifications depend on the type, degree, and impact of network attacks. Also, we will conduct continuous studies to make this system more effective.

Bibliography

[1] R.Mazot, W.Meslem, M. Layouni, and A. Tran, “Communication inter vehicular”. PhD thesis, Arles Avignon, 2013.

[2] https://www.researchgate.net/figure/Components-of-smart-and-Intelligent-vehicle_fig1_344142721. [Accessed: 2 june 2021].

[3] Busanelli, S., Ferrari, G., & Veltri, L. Short-lived key management for secure communications in VANETs. 2011 11th International Conference on ITS Telecommunications, 2011.

[4] https://link.springer.com/book/10.1007/978-981-15-7907-3. [Accessed: 6 june 2021].

[5] Gillani, S., Khan, I., Qureshi, S., & Qayyum, A. Vehicular ad hoc network (VANET): enabling secure and efficient transportation system. Technical Journal, University of Engineering and Technology, Taxila, 13. 2008.

[6]Vegni, Anna Maria, Mauro Biagi, and Roberto Cusani. "Smart vehicles, technologies and main applications in vehicular ad hoc networks." Vehicular technologies-deployment and applications (2013): 3-20, 2013.

[7] Wang, C. David, and James 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." U.S. Patent No. 5,613,039. 18 Mar. 1997.

[8] Moghraoui, Kahina. Gestion de l'anonymat des communications dans les réseaux véhiculaires Ad hoc sans fil (VANETs). Diss. Université du Québec à Trois-Rivières, 2015.

[9] Bektache, Djamel. "Application et Modélisation d’un protocole de communication pour la sécurité routière." thèse de doctorat de l'université badi mokhtar annaba, 2014.

[10] ResearchGate. https://www.researchgate.net/figure/Vehicle-to-Vehicle-V2V. communication_fig26_309546589. [Accessed: 7 june 2021].

[11] Sakib, Rizwanul Karim, and Bisway Reza. Security issues in vanet. Diss. Department of Electronics and Communication Engineering, BRAC University, 2010.

[12] Zeadally, Sherali, et al. "Vehicular ad hoc networks (VANETS): status, results, and challenges." Telecommunication Systems 50.4 (2012): 217-241, 2012.

[13] Johnson, D., Menezes, A., & Vanstone, S. (2001). The elliptic curve digital signature algorithm (ECDSA). International journal of information security, 1(1), 36-63, 2001.

[14] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "VANet security challenges and solutions: A survey", Veh. Commun., vol. 7, pp. 7–20, 2017.2016_fig2_309546589

[15] https://www.researchgate.net/figure/Hybrid-communication-CUNHA-et-al 2016_ fig2_309546589. [Accessed: 9 june2021].

[16] ResearchGate. https://www.researchgate.net/figure/Black-Hole-attack-in VANET_fig11_325414699. [Accessed: 9 june2021].

[17] I. Transportation, S. Committee, I. Vehicular, and T. Society, IEEE Standard for Wireless Access in Vehicular Environments — Security Services for Applications and Management Messages IEEE Vehicular Technology Society, vol. 2013, no. April.2013.

[18] J. H. Zhang, M. Xu, and X. N. Su, "An Efficient and Provably Secure Digital Signature Scheme Based on Elliptic Curve", Int. J. Comput. Appl. Math., vol. 12, no. 1, pp. 45–52, 2017.

[19] Petit, J. (2009, December). Analysis of ecdsa authentication processing in vanets. In 2009 3rd International Conference on New Technologies, Mobility and Security (pp. 1-5). IEEE, 2009.

[20] Nowatkowski, Michael E. Certificate revocation list distribution in vehicular ad hoc networks. Georgia Institute of Technology, 2010.

[21] Coronado-Garcia, L. C., Hernandez-Lopez, C., & Perez-Leguizamo, C. (2009, June). Autonomous decentralized root certification authority system. In 2009 29th IEEE International Conference on Distributed Computing Systems Workshops (pp. 257-262). IEEE, 2009.

[22] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "VANet security challenges and solutions: A survey", Veh. Commun., vol. 7, pp. 7–20, 2017.

[23] J. Kang, S. Ok, J. Y. Kim, and E. Kim, "Software Implementation of WAVE Security Algorithms", J. Korea Acad., vol. 15, no. 3, pp. 1691–1699, 2014.

[24] ETSI (European Telecommunications Standards Institute), “ETSI TS 103 097 - Intelligent Transport Systems (ITS). Security. Security header and certificate formats”, 2013.

[25] Lonc, B., & Cincilla, P. (2016, June). Cooperative its security framework: Standards and implementations progress in europe. In 2016 IEEE 17th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM) (pp. 1-6). IEEE, 2016.

[26] Schoch, E., & Kargl, F. (2010, March). On the efficiency of secure beaconing in vanets. In Proceedings of the third ACM conference on Wireless network security (pp. 111-116), 2010.

[27] M. Raya, M. Raya, J. Hubaux, and J. Hubaux, “Securing vehicular ad hoc networks,” J. Comput. Secur., vol. 15, pp. 39–68, 2007.

[28] C. Caballero-Gil, J. Molina-Gil, J. Hernández-Serrano, O. León, and M. Soriano-Ibañez,“Providing k-anonymity and revocation in ubiquitous VANETs,” Ad Hoc Networks, vol. 36, pp. 482–494, 2016.

[29] J. R. Singh, A. Kumar, D. Singh, and R. K. Dewang, "A Single-Hop Based Fast Certificate Revocation Protocol in VANET", in 2016 2nd International Conference on Computational Intelligence and Networks (CINE), pp. 23–28, 2016.

[30] M. N. Mejri and J. Ben-Othman, "GDVAN: A New Greedy Behavior Attack Detection Algorithm for VANETs", IEEE Trans. Mob. Comput., vol. 16, no. 3, pp. 759–771, Mar. 2017.

[31] P. Maheshwaran and S. Rajagopal, "A scheme for detecting the types of misbehaviour and identifying the attacks using reputation mechanism in a mobile ad-hoc network", in 2016 International Conference on Communication and Electronics Systems (ICCES), pp. 1–6, 2016.

[32] 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., vol. 25, no. 8, pp. 1557– 1568, Oct. 2007.

[33] T. Moore, M. Raya, J. Clulow, P. Papadimitratos, R. Anderson, and J.-P. Hubaux", Fast Exclusion of Errant Devices from Vehicular Networks", 2008 5th Annu. IEEE Commun. Soc. Conf. Sensor, Mesh Ad Hoc Commun. Networks, pp. 135–143, Jun. 2008.

[34] ACM Press the 12th ACM International Conference - Tenerife, Canary Islands, Spain (2009.10.26-2009.10.29)] Actes de la 12e conférence internationale ACM sur la modélisation,

l'analyse et la simulation des systèmes sans fil et mobiles - MSWiM '09 - Suppression de les initiés qui se comportent mal dans les VANET anonymes, 2009.

[35] X. Zhuo, J. Hao, D. Liu, and Y. Dai, “Removal of misbehaving insiders in anonymous VANETs,”in Proceedings of the 12th ACM international conference on Modeling, analysis and simulation of wireless and mobile systems - MSWiM ’09, p. 106, 2009.

[36] N. Rafique, M. A. Khan, N. A. Saqib, F. Bashir, C. Beard, and Z. Li, “Black Hole Prevention in VANETs Using Trust Management and Fuzzy Logic Analyzer,” Int. J. Comput. Sci. Inf. Secur., vol. 14, no. 9, p. 1226, 2016.

Glossary

CA **Certificate Authority.**

CRL **Certificate Revocation List.**

CBRP **Category-based revocation protocol.**

IDS **Intrusion Detection System.**

LEAVE **Local Eviction of Attackers by Voting Evaluators**

MANETs **Mobile Ad Hoc Networks.**

OBU **On Board Units.**

RSU **Road Side Units.**

SLEP **Suicide-based Local Eviction Protocol.**

V2I **Vehicle to Infrastructure Communication.**

V2P **Vehicle to Passenger communication.**

V2V **Vehicle to Vehicle Communication.**

VANETs **Vehicular Ad-hoc Networks.**