Securing Vehicular Networks Against Denial of Service Attacks

Mohamed Nidhal Mejri





N° Assigned by the Library

Thesis

by

MOHAMED NIDHAL MEJRI

Securing Vehicular Networks Against Denial of Service Attacks

A thesis submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy in ≺ Telecommunication and Computer security ≻

Committee

Pr. Paul Mühlethaler	Research Director, INRIA	Examiner
Pr. Emmanuel Viennet	Paris 13 university	Examiner
Pr. Sidi-Mohammed Senouci	Bourgogne university	Reviewer
Pr. Nabil Tabbane	Sup'Com Tunisia	Reviewer
Pr. Anne Canteaut	Research Director, INRIA	Invited
Dr. Nadjib Achir	Paris 13 university	PhD advisor
Dr. Mohamed Hamdi	Sup'Com Tunisia	PhD advisor

May 19, 2016

Declaration of Authorship

I, *Mohamed Nidhal MEJRI*, declare that this thesis report titled, *"Securing vehicular Networks against denial of service attacks"* and the work presented in it are my own. I confirm that:

- This work was done wholly or mainly while in candidature for a research degree at this University.
- Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated.
- Where I have consulted the published work of others, this is always clearly attributed.
- Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work.
- I have acknowledged all main sources of help.

Signed: _____

Date: _____

Résumé

Dans cette étude nous nous sommes interéssés à sécuriser les réseaux véhiculaires Ad hoc (VANETs) contre les attaques de déni de service (DoS) jugées comme étant les attaques les plus dangereuses pour ces types de réseaux. Notre travail peut être subdivisé en trois grandes parties.

Dans un premier temps, nous avons étudié les différentes vulérabilités auxquelles sont exposés les VANETs et spécialement les attaques DoS. Vu notre expertise en matière de la cryptographie, nous avons etudié, dégagé et classifié des solutions possibles à une grande panoplie de bréches de sécurité VANETs. En effet, nous avons montré que la cryptographie avec ses primitives et outils assez puissants permet de résoudre un grand nombre de problèmes de sécurité. Notre premire contribution dans ce sens est un algorithme de génération de clés de groupe pour les convois de véhicules.

Dans notre deuxième contribution nous avons conçu deux nouvelles techniques de détection des attaques DoS dans les VANETs caractérisés essentiellement par la forte mobilité et les déconnexions fréquentes ce qui complique considérablement la phase de détection par rapport d'autres réseaux plus lent. Notre premier algorithme de détection est basé sur la regression linéaire, la logique floue ainsi que trois nouvelles métriques de détection spécifiques VANETs. Dans notre deuxième algorithme nous avons défini le "Packet entropy" comme nouvelle métrique que nous avons introduit pour la première fois pour détecter les DoS dans les VANETs.

Notre troisième contribution est relative à la réaction contre les attaques détéctées et pour celà nous avons eu recourt aux techniques offertes par la théorie des jeux. Nous avons proposé deux jeux de réaction non coopératifs sous forme stratéqique et extensive. Pour chacune des phases de détection et de réaction, les expérimentations ont été faites essentiellement pour les attaques greedy et jamming. Nos algorithmes proposés présentent l'avantage de la rapidité, d'être exécutés par n'importe quel nœud du réseau et ne nécessitent aucune modification du protocole IEEE 802.11p de la couche MAC, utilisée comme standard pour les VANETs.

Au courant de ce travail nous avons pu participer à la sécurisation des résaux VANETs. Cependant nous jugeons qu'il reste beaucoup de travail à faire. A savoir par exemple, l'étude des solutions cryptographiques que nous avons menée, qui nous a permis de découvrir á quel point l'usage de la cryptographie pour la sécurité des VANETs est un sujet assez vaste et qui nécessite d'être encore mieux exploré. Ceci consituera pour nous une ouverture assez prometteuse.

Mots clés: `Réseaux véhiculaires Ad hoc (VANETs), Déni de service (DoS), Sécurité, Cryptographie, Attaques, IEEE 802.11p.`

Abstract

In this thesis we are interested in securing Vehicular Ad hoc NETworks (VANETs) against Denial of Service (DoS) attacks judged to be the most dangerous attacks to such networks. Our work can be divided into three main parts.

First, we studied all the various possible existing vulnerabilities to which are exposed VANETs, we focused especially on denial of service attacks. Given our expertise in cryptography, we explored, identified and classified the possible solutions to a wide range of VANET security breaches from a cryptographic point of view. Indeed, we showed that cryptography with its primitives and fairly powerful tools solves many security problems. Our first contribution in this direction is a secure Group key generation algorithm for VANET platoons.

In our second contribution, we have developed two new techniques to detect denial of service attacks in VANET networks mainly characterized by the high mobility and frequent disconnections which considerably complicates the detection. Our first detection algorithm is based on the linear regression mathematical concept, fuzzy logic and three newly defined VANET appropriate. In our second algorithm we defined a new Shannon Entropy based metric that we introduced for the first time to detect DoS attacks in VANET.

Our third contribution was devoted to the reaction against the detected attacks. For that we used the techniques offered by game theory. We have proposed two non-cooperative strategic and extensive form reaction games. For both detection and reaction proposed schemes, experiments were made essentially for the greedy behavior and jamming attacks. All our proposed algorithms present the advantage of rapidity, to be executed by any node of the network and does not require any modification of the 802.11p MAC layer protocol used as a standard for VANETs.

Aware of this work we have participated in securing VANETs, however we believe that much remains to be done. Namely, for example the study of cryptographic solutions we have conducted, allowed us to discover how the use of cryptography for VANET security is a fairly broad topic which needs to be better explored. This will be for us a very promising opening.

KeyWords: `Vehicular Ad hoc Networks (VANETs), Denial of Service (DoS), Security, Cryptography, Attacks, IEEE 802.11p.`

Acknowledgments

This work has been carried out under a co-supervision contract between the national Tunisian engineering school (ENIT), and Paris 13 university. The research works were done alternately in L2TI, the academic research lab of the Galilee institute and the SysCom lab of ENIT. This work was done under the direction of Mr Mohamed Hamdi from ENIT and respectively Mr Jalel Mr Ben-Othman and Mr Nadjib Achir from Paris 13.

I would like to thank everyone in both labs for this opportunity and for providing the environment and tools that allowed this work to come to life.

I would like to extend my greatest appreciation and gratitude to all my advisers Dr. Mohamed Hamdi and Dr Nadjib Achir for their guidance, understanding and patience.

I would like to thank Prof. Sidi-Mohammed Senouci and Prof. Nabil Tabbane for kindly accepting to review my work. I also extend a special thanks to Prof. Paul Mühlethaler, Prof. Emmanuel Viennet and Prof. Anne Canteaut for agreeing to serve on my committee. Their valuable comments and feedback will help to improve my future work.

I also would like to thank the following gentlemen: Junling BU and Mathieu LACAGE for the long and valuable exchanges that we have had to correct and improve the ns-3 simulator to make it more effective for VANETs.

Finally and most importantly, I would like to thank my parents, my family and especially my wife and my children for their encouragement and for supporting my absence during three years.

Dedication

To my parents for their unconditional love and support throughout my hole live,

To my wife and my children for their continuous encouragement.

Contents

CHAPTER 1

INTRODUCTION

Contents

1.1 Context

One of the major features that have shaped the vehicular industry during the last years is the integration of embedded components whose main role is the improvement of driver safety. To disseminate the information gathered and processed by these components, wireless communication infrastructures have been used. Such Intelligent Transportation Systems Intelligent Transportation System (ITS) that have been initially developed for safety purposes have then been extended to cover driving efficiency as well as the provision of value-added services, including infotainment and commercial applications. In the near future, it is expected that vehicles which increasingly become an intelligent systems will be equipped with radio communications interfaces. Automakers have realized the potential of the interconnection of their vehicles. In order to expand the perception of event recognition which can not be detected by local sensors or by the driver, on-board sensors have been introduced. Thus, critical driving conditions can be detected, and important information can be shared with nearby vehicles. To exchange such information, the vehicles form a spontaneous networks, and they are commonly known as VANETs using a direct communication between vehicles known as Inter-Vehicle Communications (IVC). Using this system, vehicles can respond by themselves to avoid accidents by preventing vehicles in close proximity and it transparently to the driver.

There are two communication types in a VANET network: Vehicle to Vehicle (V2V) where vehicles communicate directly and Vehicle to Infrastructure (V2I) which also refers in the literature the I2V communications, where vehicles communicate with existing infrastructure, such as GSM, UMTS, WiMAX networks and WiFi via fixed equipment placed on the road sides.

VANETs are a use case of mobile ad hoc networks where cars are the mobile nodes. In addition to the on board entertainment services, the essential purpose of VANETs is to improve road safety and enhance driving conditions. Thus, the life of users is one of the most important involved factors, hence the paramount importance of securing VANETs against any type of attack they can undergo. The VANET networks are actually a special case of Mobile Ad hoc NETworks (MANETs) and as they exhibit several unique features such as the high mobility of nodes, short connection times, etc. conventional security mechanisms are not always effective. More specifically, under the mentioned conditions, different types of conventional attacks under which operate mobile networks in ad hoc mode are valid

for VANET. However, the behavior of VANETs towards these attacks, and the proposed solutions are not usually the same.

Given the variety of attacks and vulnerabilities that may exist in VANET, several techniques and mechanisms exist either to completely avoid or to minimize the effects desired by the attacker. However, this area is not well explored in the literature. It is therefore necessary to find solutions to these existing security breaches in VANETs, basically the DoS attacks. This thesis was proposed in this context.

1.2 Thesis objectives

In a VANET environment, both V2V or V2I communication modes are exposed to different kinds of attacks. However, in this work we focus on:

- *V2V communications*: Which is the most difficult case to configure compared to V2I communications.
- *Denial of Services attacks*: Judged to have the most disastrous and dangerous effects on the network.

Our goal is to *analysis*, *design* and *evaluate* new methods for securing vehicular networks based on IEEE 802.11p standard. More precisely, we provide both ***detection*** and ***reaction*** algorithms to more secure VANETs against DoS attacks.

Analysis refers to qualitatively evaluate existent related works and their effectiveness in a VANET context with high mobility. Based on this background, *design* relates to introducing new proposals in order to enhance both detection and reaction phases against attacks. Finally, the term *evaluate* is used to denote the assessment of the performance of our proposals by a series of experimental results and comparison with existing approaches coming from literature.

1.3 Summary of contributions

The major contributions of our dissertation are basically based on both cryptographic solutions for DoS attacks in VANETs and on detection and reaction methods against these

kind of vulnerabilities. We contribute also by providing a recent sate of art study in this context. These contributions are summarized in the following:

- **Recent advances in VANETs**
  This work was done in order to provide the latest recent advances in vehicular networks, and more specifically the works related to the security of these networks. We studied the physical and the MAC layer protocols, as well as related standards. We also classified the VANETs vulnerabilities and attacks, from a cryptographic point of view depending on the affected service.

- **Possible cryptographic solutions for VANET security challenges**
  The previous classification, allowed us to study the possible cryptographic solutions for each family of attacks. The various known attacks and their feasible solutions have been studied one by one. We have demonstrated that cryptography can solve a wide range of VANET security challenges and much remains to be done in this direction.

- **Group key generation proposal**
  We addressed in this contribution, the secure group communications problem in VANETs. By generating a secret group key that can be used by the vehicles of a VANET platoon to guarantee secure communication between them. To address this need, we propose a new secure *Diffie-Hellman* based variant algorithm for groups, that we fortified by a pre-shared secret to withstand the famous *Man in the Middle* attack. As necessary, our proposal can be used by several types of authentication and encryption VANET applications.

- **Linear regression and fuzzy logic based detection scheme**
  As explainedabove, detecting DoS attacks in ITS is an important part of our dissertation. With respect to this issue, we proposed a new linear regression and fuzzy logic based detection scheme. The objective of this scheme divided into suspicion and decision phases is to detect if the VANET network is under DoS attack or not. For this effect we have defined three new metrics and we have focused especially on greedy behavior attack.

- **Entropy based detection scheme**
  In the same axis, we have proposed a new Shannon Entropy based scheme for VANETs DoS attack detection. We define "Packets entropy" as a new metric to

measure the entropy of chosen family of exchanged packets in VANET network. In fact, the idea is simple: the entropy of normal network (not under attack) is too different (higher) from the entropy of network under DoS attack. Based on this principle, our method is generic (not related to the type a attack), presented the advantages of rapidity and does not require any MAC protocol modification.

- **Game theory based reaction methods**
  For the latest part of this dissertation related to the reaction against VANETs DoS attacks, we have proposed a game theory based scheme. In fact, game theory becomes increasingly a powerful reaction design tool. Basically, a network under attack can be considered as game between honest nodes and attackers nodes. Using this principle we have designed two non-cooperative security games which allowed to avoid and mitigate attack effects.

1.4 Publications

Based on the findings of the current research, some papers have been published to the international journals and conferences as following:

1. MEJRI, Mohamed Nidhal, BEN-OTHMAN, Jalel, and HAMDI, Mohamed. GDVAN: A New Greedy Behavior Attack Detection Algorithm For VANETs. Accepted in IEEE transaction on mobile computing journal (5-year impact factor 3.01)

2. MEJRI, Mohamed Nidhal, BEN-OTHMAN, Jalel, and HAMDI, Mohamed. Survey on VANET security challenges and possible cryptographic solutions. Vehicular Communications, Elsevier, 2014, vol. 1, no 2, p. 53-66.

3. MEJRI, Mohamed Nidhal and BEN-OTHMAN, Jalel. Entropy as a new metric for denial of service attack detection in vehicular ad-hoc networks. In : Proceedings of the 17th ACM international conference on Modeling, analysis and simulation of wireless and mobile systems. ACM, 2014. p. 73-79.

4. MEJRI, Mohamed Nidhal and BEN-OTHMAN, Jalel. Detecting greedy behavior by linear regression and watchdog in vehicular ad hoc networks. In : Global Communications Conference (GLOBECOM), 2014 IEEE. IEEE, 2014. p. 5032-5037.

5. MEJRI, Mohamed Nidhal and HAMDI, Mohamed. Recent advances in cryptographic solutions for vehicular networks. In : Networks, Computers and Communications (ISNCC), 2015 International Symposium on. IEEE, 2015. p. 1-7.

6. MEJRI, Mohamed Nidhal, ACHIR Nadjib and HAMDI, Mohamed. A New Group Diffie-Hellman Key Generation Proposal for Secure VANET Communications. 2016 13th IEEE Annual Consumer Communications Networking Conference (CCNC).

7. MEJRI, Mohamed Nidhal, ACHIR Nadjib and HAMDI, Mohamed. A New Security Games Based Reaction Algorithm Against DoS Attacks in VANETs. 2016 13th IEEE Annual Consumer Communications Networking Conference (CCNC).

8. MEJRI, Mohamed Nidhal, HAMDI, Mohamed and BEN-OTHMAN, Jalel. A New Information Theory Based Proposal For VANET Security. Submitted to Elsevier Computers & systems Journal (impact factor 1.32)

9. MEJRI, Mohamed Nidhal, ACHIR Nadjib and HAMDI, Mohamed. Game Theory based proposal for Vehicular Networks Security. (in progress)

1.5 Thesis outline

The remainder of the report is organized as follows:

- **Chapter 2** presents the recent state of art advances of VANETs and identifies all the existing security problems in VANETs with a wide variety of studied examples in such identified family of attacks especially for DoS attacks.

- **Chapter 3** evaluates what cryptography which is a securing tool set can solves among all the existing identified VANET vulnerabilities and security challenges. From this point of view, we present our proposal to solve the problem of secure key generation for a VANET platoon.

- **Chapter 4** details our contribution about the detection against DoS attacks in VANETs using the linear regression, watchdog and fuzzy logic concepts. We confirm the efficiency of our proposed detection algorithm by simulating the greedy behavior which is a dangerous DoS attack.

- **Chapter 5** continues in the same direction as chapter 4 and present our second contribution about DoS detection. We define "Packets entropy" as a new metric to be used to distinguish easily and rapidly between a normal VANET and a VANET under DOS attack. Jamming and greedy behavior attacks has been used as DoS attacks simulations examples.

- **Chapter 6** is devoted to our contribution about the reaction methods against DoS attacks. We proposed two non-cooperative security game algorithms based on game theory allowing to avoid and mitigate the DoS attack effects. Some experimental results are carried out in order to evaluate our approach with existing methods. Compared to similar existing methods, this proposal seems to be wide efficient.

- **Chapter 7** summarizes the results of the current research and points out several lines of future work.

The bibliography is given at last.

⁂ ⁂ ⁂ ⁂ ⁂

CHAPTER 2

VANET STATE OF ART

Contents

In this chapter we provide in a first part a detailed review of the recent advances of the state of art of Vehicular Ad hoc networks commonly known as VANETs. In addition to the communication architecture, standards and routing protocols we detailed also the most known projects and applications of VANETs. In a second part, we focus on the privacy and security challenges that need to be overcome to make such networks safety usable in practice. All the existing security problems in VANETs have been identified and classified. A wide variety of examples in such identified family of attacks has been studied.

2.1 Introduction

In recent years, the development of ITS [1] has made a big step. In addition to entertainment services on board, the main aim is to improve road safety and driving conditions. The automakers have realized the potential of the interconnection of their vehicles. To broaden the perception of recognition events that cannot be detected by traditional sensors or by the conductor, embedded sensors were introduced. Critical driving conditions can be detected and the information may be shared with nearby vehicles. To share this information, vehicles establish a spontaneous network, known as Vehicular Ad hoc NETwork (VANETs), using a direct mode of communication between vehicles called IVC [2]. Using this communication method, the vehicle can react by itself to avoid accidents by preventing other vehicles in its neighborhood in a transparent way to the driver. There are two types of communication in a VANET network [3] : V2V where vehicles communicate directly and V2I which also refers in the literature as I2V communications where vehicles communicate directly with existing infrastructure, such as GSM, UMTS or WiMAX network via fixed equipment located on the road.

The architecture of vehicular ad hoc networks involves various hardware and software components. In a VANET network, vehicles are equipped with a unit called On Board Unit (OBU), mounted in the vehicle. On roads, units of infrastructure communication are called Road Side Unit (RSU) [4].

Besides the warning security applications and driver assistance, which form the essential purpose for which the VANET has emerged, there are applications for passenger comfort

and online entertainment. Despite the facilities it offers, the wireless medium used in intelligent vehicular networks has some drawbacks that leave it vulnerable to different types of attacks that target this type of transmission medium, namely jamming, eavesdropping, interference, etc. [5]. In addition, and given the architecture of vehicular networks which involve almost the seven layers of the Open System Interconnection (OSI) reference model, attacks and vulnerabilities exist almost at all levels, stretched from the physical to the application layer. Techniques and tools to deal with VANET security attacks are numerous. Among others, cryptography is one of the ways that solve, by some primitives, a lot of VANET systems security issues.

This chapter is organized into five sections. After the introduction, section 2 is devoted to related work especially of VANET security challenges. In section 3 we present the recent advances of VANET state of the art. Section 4 discusses challenges and security in VANETs. Finally, section 5 concludes the chapter.

2.2 Literature review

The major motivation that led us to carry out this work is to provide in the same chapter a recent summary about VANET state of art and a study about VANETs security challenges and their possible related solutions. Unlike other studies, we classify and evaluates all recent existing vulnerabilities for VANETs, which have been proposed separately in other studies. To the best of our knowledge, most research works on the VANETs security domain were either papers that address a specific problem or general surveys. However, some papers that are considered to be among the first works in the field have especially treated also some security issues. Among these papers, we quote [2], in which Blum and Eskandarian were interested in the problem of intentionally collusion which can be caused between smart vehicles. Maxim Raya et al. [1, 6] have been interested in the classification of attacks, the presentation of the attacker model. They presented also some attacks for the first time such as hidden vehicle, tunnel, wormhole, Bush Telegraph. In theirs works they defined the requirements that must be respected to secure messages exchange in Vehicular networks. Group communications Security issues were also discussed.

In the survey papers [7, 5, 8] respectively of B. Mishra, A. Dhamgaye and S. Zeadally and their co-authors, they presented the state of the art and reviewed some security challenges and general proposals for VANETs security. M.S Al-Kahtani and Irshad Ahmed

Sumra and their co-authors presented succinctly in [9, 10] some VANETs possible attacks and their proposed related solutions. In the same direction, Maria Elsa Mathew et al. and Also, A. Rawat et al. have presented respectively in [11] and [12] a recent classification of VANETs attacks and a category set of their possible solutions. Jose Maria Fuentes et al. glance in [13] some works which cover safety and privacy aspects of VANETs. Some of these mentioned works study the security issues with a cryptographic primitives point of view without going into details or presenting solutions to mentioned problems.

Among works related to the security of Vehicular networks, but focused on a specific issue, we quote: [14] of Bin Xiao et al. reserved for the detection and localization of Sybil attack in VANET nodes. [15] of P. Golle et al. which treat correcting malicious data entered in VANETs. In [16], Irshad Ahmed Sumra et al. have been interested into "timing attacks". [17] of Seyed Mohammad Safi et al. focused into avoiding the wormhole attack. In [18, 19] and [20] respectively of RoselinMary, Li He and Adil Mudasir Malla and their co-authors have detailed the DoS attack in a VANET environment. [21] of Sapna S. Kaushik, was reserved to privacy protection issues in VANETs. In [22], L. Gollan et al. were interested into the use of digital signatures as a means of authentication between cars.

Research in the field of VANETs is currently very active and varied as it touches on several axis at the same time, namely: wireless communications, protocols for physical and MAC layers, routing protocols and security. The following section will detail the state of the art and recent advances of all these aspects.

2.3 Recent advances in VANET State of art

2.3.1 Overview

The large and rapid changes that know all the domains in the world not excluded the transport sector. Today, the fleet is growing, the roads are becoming more dangerous by the effect of congestion and increase the likelihood of collusion. According to the statistics of the National French Inter-ministerial Road Safety Observatory, published in 2013 annual report [24], there were 65,556 accidents (bodily injury) in 2012 against 65,024 in 2011. Therefore, Securing traffic becomes not only a necessity but also an obligation. It is necessary to satisfy this requirement and others that ITS appeared. The Intelligent Transportation Systems aim to provide solutions to road safety of passengers and the

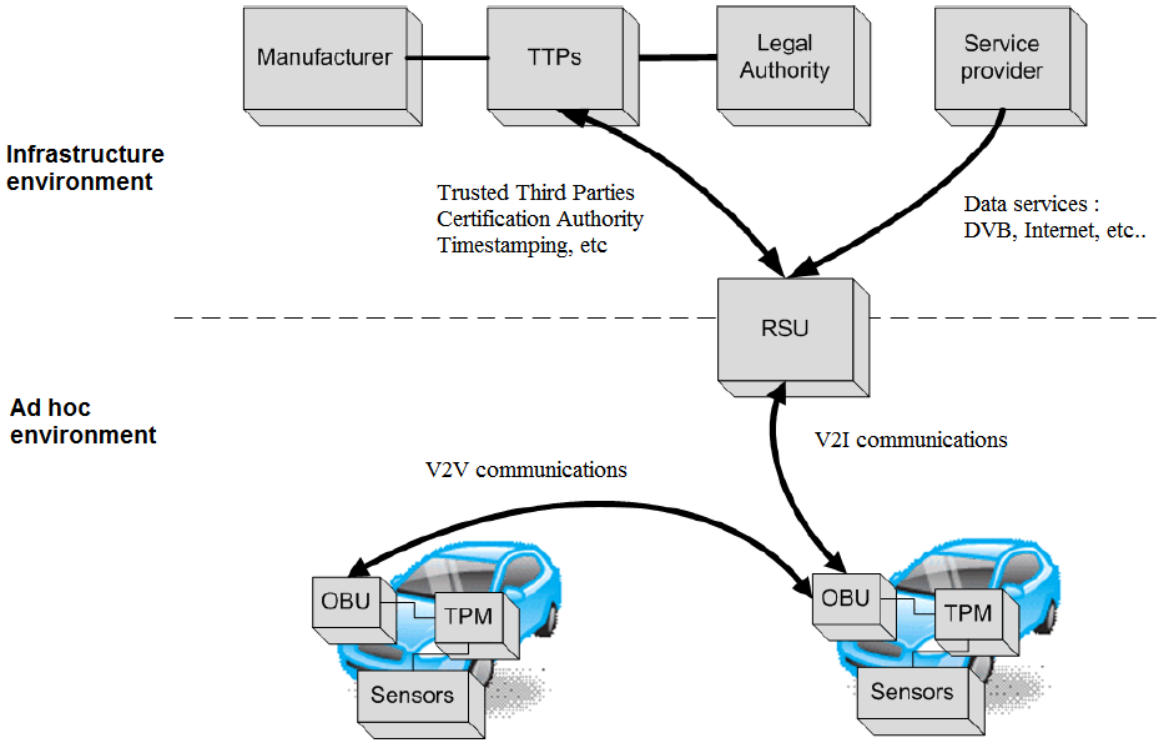


Figure 2.1. VANET components [23]

traffic congestion problems. They improved also comfort and driving conditions by integrating information technology in transport systems. We distinguish two possible types of communications:

1. *Vehicle To Vehicle (V2V)*: are communications between vehicles in ad hoc mode [21]. In this mode, a vehicle can receive, transmit or exchange valuable traffic information such as traffic conditions and road accidents with other vehicles.

2. *Vehicle To Infrastructure (V2I)*: used to broadcast between the network infrastructure and vehicles, and for the exchange of useful information about road conditions and safety measures to be taken into account [21]. In this mode, a vehicle establishes a connection with the RSU to connect and communicate with external networks such as the Internet. V2I links are less vulnerable to attacks and require more bandwidth than V2V links.

In ITS, a node can be a vehicle equipped with a radio system operating in the wireless short range, reserved for ad hoc network, it can be also a road equipment to communicate

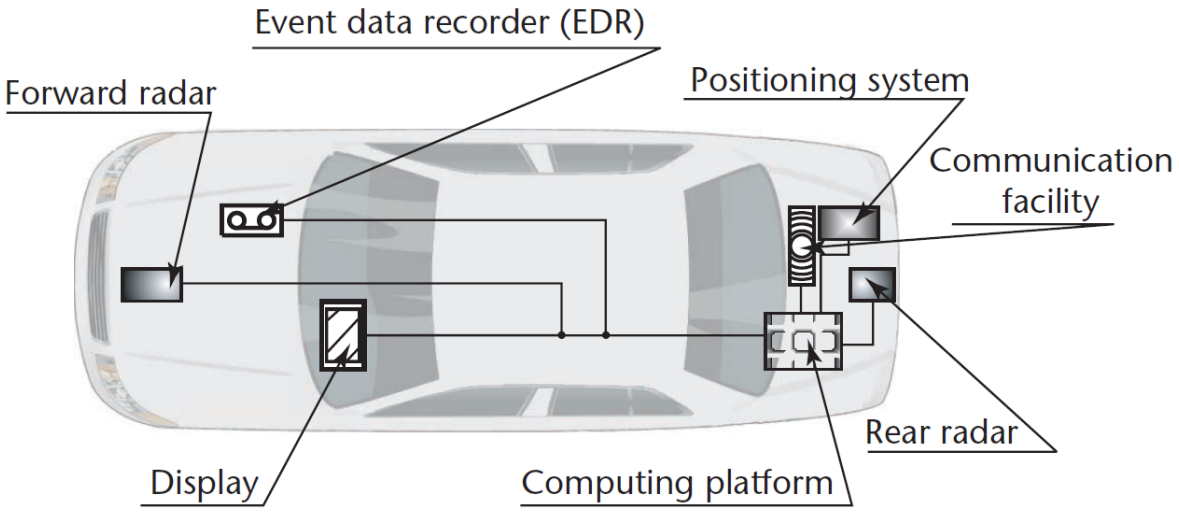


Figure 2.2. Smart vehicle [23].

with mobile ad hoc nodes, and connect them to network infrastructure [8]. The integrated unit in the vehicle is named OBU (On Board Unit) and the roadside unit is named RSU (Road Side Unit). Fig.2.1 describes the infrastructure and Ad hoc environments which form a simplified VANET network. The Ad hoc part is mainly composed of vehicles equipped with sensors, the OBU and Trusted Platform Module (TPM) [1], where the infrastructure part includes the manufacturer, the Third Units: Trusted Third Party (TTP), service providers on board and legal authorities. In the infrastructure part, the RSU acts as a bridge between ad hoc and infrastructure parts.

2.3.2 Smart vehicle

An intelligent vehicle as it was designed in [25], incorporates basically a set of sensors (front radar, reversing radar, etc.) that receive useful environmental information that generally the driver alone is unable to perceive . We find also a positioning system such as Global Positioning System (GPS) for example, which is essential for locating and driving assistance. A smart vehicle is obviously equipped with a communication system (can be multi-interface), a computing system, an event recording device which is a device whose functioning is similar to the black box of an aircraft.

Mainly, and for security measures, Hubaux et al. propose in [25] that a smart vehicle must be equipped with an Electronic License Plate (ELP) or with Electronic Chassis Number (ECN) which represent the electronic identity of the vehicle instead of the conventional

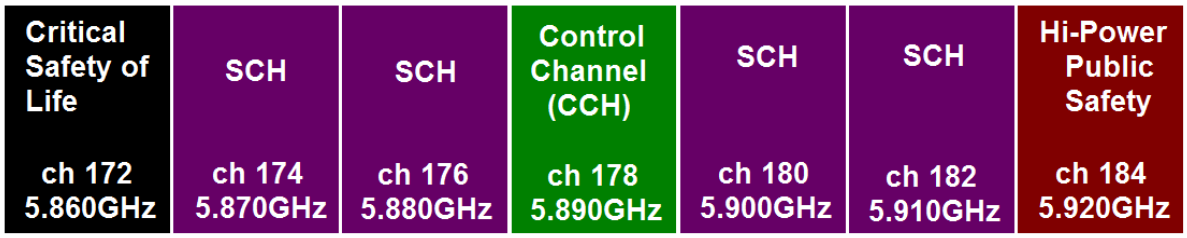


Figure 2.3. DSRC in USA, 7 channels of 10 MHz.

identification by license plates. The ITS current terminology includes some features such as transceiving, display and interactivity with the driver in a single unit called OBU. The Fig.2.2 shows the different components that can be integrated in a smart vehicle.

2.3.3 VANETs Standards

In addition to the facility of the production process, and the reduction of costs and the time to market, normalization and standardization in communications and information technology help also to ensure the interoperability and the rapid implementation of new technologies. For VANETs, standardization affects virtually all the different layers of the OSI (Open System Interconnection) model which is a communication system integrating all the features from the physical to the application layer. It should be noted that in the literature, often Dedicated Short Range Communications (DSRC) [26], Wireless Access in Vehicular Environments (WAVE) or even IEEE 802.11p [27] are used to designate the entire protocol stack of standards dealing with VANETs.

2.3.3.1 DSRC

For maximum of interoperability and for the purpose of standardization of frequencies with which the VANETs work, the U.S. government represented by the Federal Communication Commission (FCC) attributed the band 5.850 to 5.925 GHz, (75 MHz band wide). This band is known as Dedicated Short Range Communications (DSRC). The use of the DSRC band is not subject to a license, but rather to strict rules of use. According to [26], the DSRC band is divided into seven channels of 10 MHz, respectively numbered 178, 172, 174, 176, 180, 182, 184. The channel 178 is the Control CHannel (CCH). The other six are Service CHannels (SCH). Service channels 172 and 184 are respectively reserved to High Availability and Low Latency (HALL), and for high power and public safety (Fig.2.3). In Europe the DSRC band is regulated by the European Telecommunications Standards

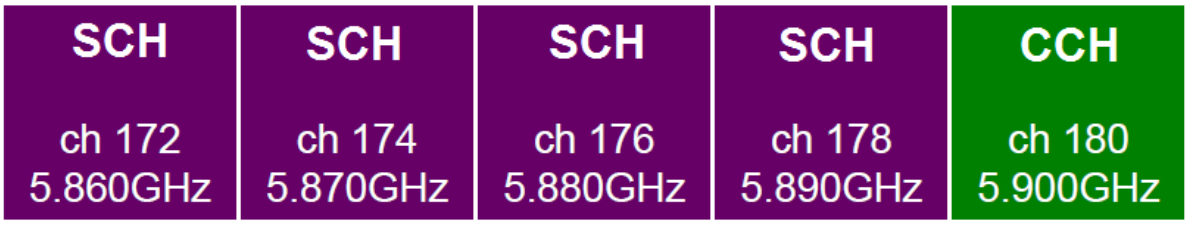


Figure 2.4. DSRC in Europe, 5 channels of 10 MHz.

Institute (ETSI) [28], and only the channels 180 of CCH and 172, 174, 176, 178 of SCH are used (Fig.2.4).

2.3.3.2 WAVE

According to the latest ITS standards fact sheets of IEEE published in [29], the WAVE IEEE 1609 family (Standard for Wireless Access in Vehicular Environments) defines an architecture and a complementary set of standardized protocols, services and interfaces that allow all WAVE stations to operate in a VANET environment and establish Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) communications. The WAVE architecture defines also the security of exchanged messages. WAVE Standards form together the basis for the implementation of a wide set of applications in the transportation domain, they include vehicles safety, automatic tolls, improved navigation, traffic management and many other applications. The WAVE IEEE 1609 standards family is organized as follows:

IEEE P1609.0: This draft is the definition guide for the Architecture of Wireless Access in Vehicular Environments (WAVE). It defines how IEEE 1609 standards family work together and the necessary services for the multi-channel DSRC devices to be able to communicate in a high mobile environment.

IEEE P1609.1 (Resource Manager): This Standard defines data flows and resources, it describes the basic components of the WAVE system architecture. It defines also the command messages and storage data formats. IEEE 1609.1 specifies also the device types that can be supported by the On Board Unit.

IEEE Std 1609.2 (Security Services for Applications and Management Messages): Defines the processing method and the formats of secure messages used within WAVE and DSRC system. This Standard describes some methods for securing WAVE application

messages and management messages, It describes also the functions necessary to support security of messages and the anonymity and privacy of the vehicle.

IEEE Std 1609.3 (Networking Services): This standard describes services for the network and transport layers, these services include routing and addressing with the support of WAVE secure data exchange. It describes also the WAVE Short Messages (WSM) protocol. It provides an efficient alternative specific to WAVE architecture to directly support IP applications. In addition, IEEE 1609.3 standard defines the Management Information Base (MIB) for WAVE protocols family.

IEEE Std 1609.4 (Multi-Channel Operations): This standard is an enhancement to 802.11 MAC to be able to support WAVE. It describes wireless multi-channel radio operations which use the IEEE 802.11p protocol (medium access control and physical layers) for WAVE architecture. It specifies interval timers, priority access parameters, control channel and service channel operations. It defines also management services, channel routing and switching parameters.

Draft IEEE P1609.5 (Layer Management): This draft is under work, it will describe communication management services for Vehicle to Vehicle (V2V) and for Vehicle to Infrastructure (V2I) communications for the WAVE Environment.

Draft IEEE P1609.6 (Remote Management Services): This draft is under work too, it will provide the management of inter-operable services. It includes a remote management and identification services for WAVE devices (OBU and RSU), using WAVE management services of IEEE Std 1609.3 and also identification services with the WSM (WAVE Short Message) protocol defined by IEEE Std 1609.3. Thus, it offers an additional middle layer between application and transport layer for more additional facilities.

IEEE Std 1609.11 (Over-the-Air Data Exchange Protocol for Intelligent Transportation Systems (ITS)): Defines services and secure messages required for the use of secure electronic payment formats.

IEEE Std 1609.12 (Provider Service Identifier Allocations (*PSID*)): This document specifies the identifier values that have been allocated for use by the WAVE systems.

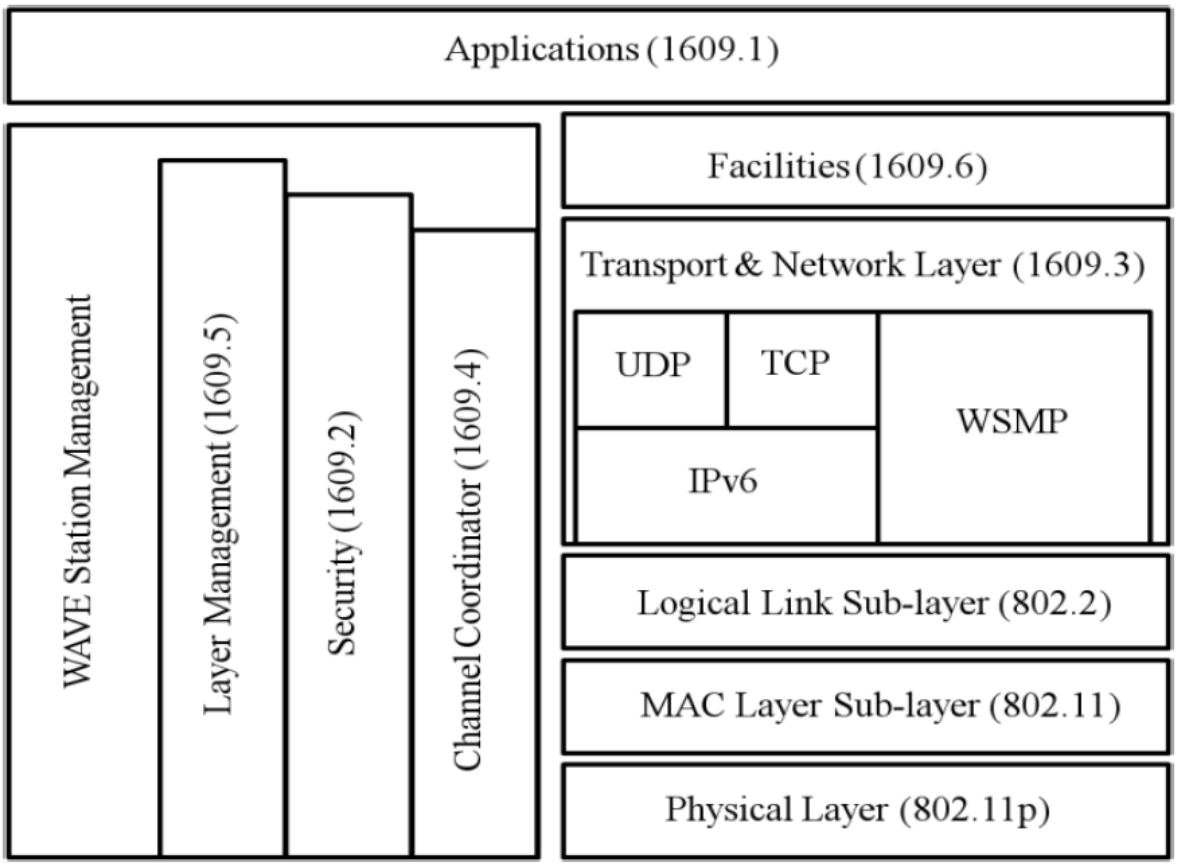


Figure 2.5. WAVE architecture [23].

The different standards of the 1609 WAVE architecture and their integration with the *OSI* reference model are summarized in Fig.2.5.

2.3.3.3 IEEE 802.11p

In addition to the IEEE 1609 standards, IEEE has expanded its family of IEEE 802.11 protocols by adding 802.11p to accommodate vehicular networks, in accordance with the DSRC band. The definitions of the physical and medium access layers for VANETs are specified by the standard IEEE 802.11p - 2010 [27], who adapted PHY and MAC layers of the IEEE 802.11-2007 [30] to be suitable for vehicular networks. IEEE 802.11p is specially based on the IEEE 802.11a for the definition of the PHY layer and on IEEE802.11e for the definition of the QoS [31].

IEEE 802.11p PHY:
The IEEE 802.11p PHY is based on the Orthogonal Frequency Division Multiplexing (OFDM) with flow rates of 3, 4, 5, 6, 9, 12, 18, 24 and 27 Mbps, and a channel width of 10 MHz. Litters transmissions can reach 1000 m [32]. A WAVE equipment in a VANET switches between CCH and SCH channels 10 times per second (10 Hz).

IEEE 802.11p MAC:
The MAC layer of IEEE 802.11p uses Enhanced Distributed Channel Access (EDCA) which is an improvement of the former Distributed Coordination Function (DCF), used in most of the IEEE Std 802.11 standards [33]. To ensure more chance to safety messages so they can be transmitted within a reasonable time, the EDCA introduces the management of QoS concept through the notion of Access category (AC). IEEE 802.11p defines four access categories according to the type of traffic: Background traffic (AC0 or BK), Best Effort traffic (AC1 or BE), Video traffic (AC3 or VI) and Voice traffic (AC3 or VO). Access category AC3 is the highest. (see Fig.2.6)

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) is the method used by EDCA to access the channel. In EDCA [31, 4], with a simplified manner and without going into too much detail, if a node is ready to transmit, it senses the medium, if the later is free for an Arbitration Inter-Frame Space (AIFS) period, the node must defer transmission by selecting a random backoff time. The backoff procedure of 802.11p EDCA will be detailed in chapter 4.

2.3.4 Characteristics of VANETs

VANETs are a wireless networks where nodes are a a fixed road units or a highly mobile vehicles. Nodes communicate with each other in ad hoc mode and communicate with fixed equipment on the roads in infrastructure mode. Thus, the characteristics of VANETs are basically a mixture of wireless medium characteristics and the characteristics of the different topologies in ad hoc and infrastructure modes. these characteristics are:

- *High mobility*: The high mobility of VANET nodes is one of the most important features. In normal operation of the network, nodes move all the time with different speeds and directions. According to [5, 8], the high mobility of nodes reduces the mesh in the network (fewer routes between nodes). Compared to MANET, VANET mobility is relatively high. In the literature, quite researches such as [34, 35, 36, 37]

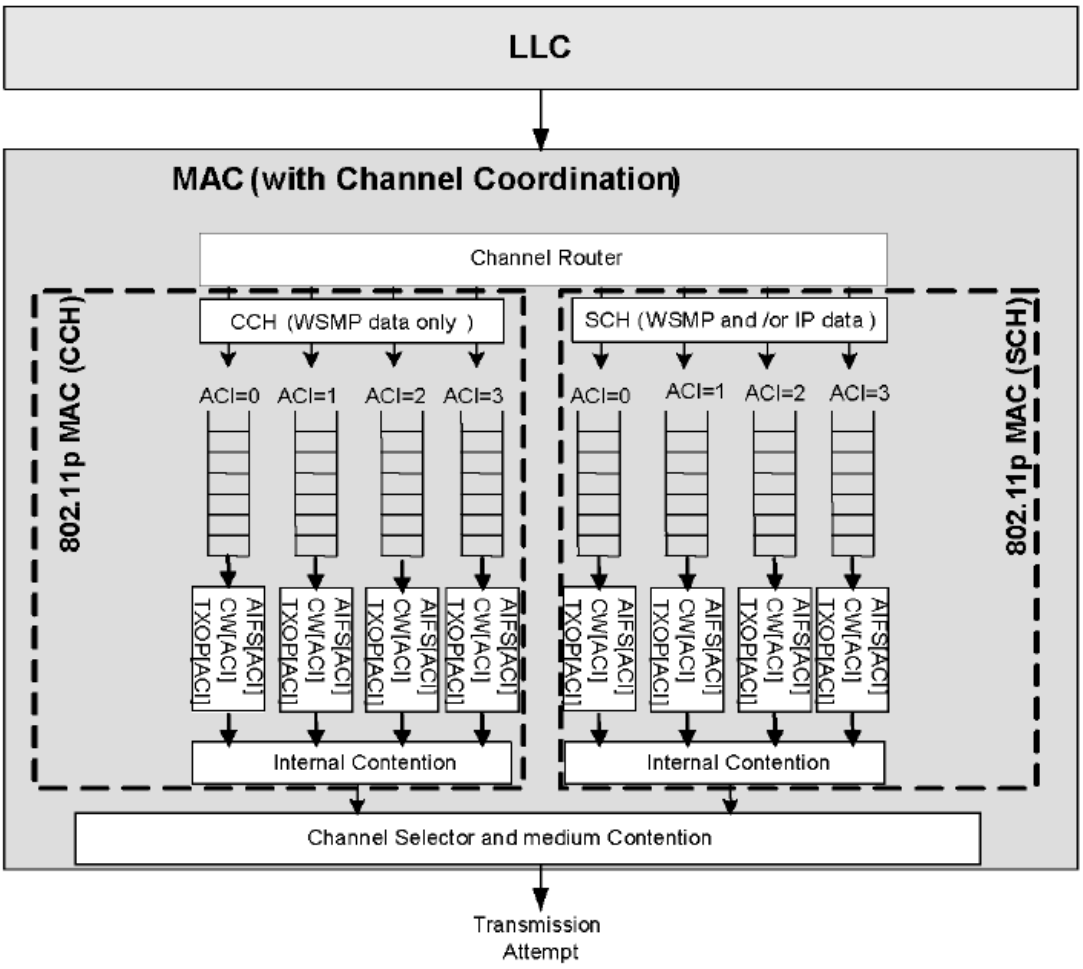


Figure 2.6. Access categories in EDCA [27].

have been specially devoted to study the impact of mobility factor in ad hoc networks and especially for vehicular networks.

- *Dynamic topology*: Given the high mobility, VANET topology is changing rapidly, it is therefore dynamic and unpredictable. The connection times are short especially between nodes moving in opposite directions. This topology facilitates the attack of the entire network, and makes difficult the detection of malfunction.

- *Frequent disconnections*: The dynamic topology and the high mobility of nodes as well as other conditions such as climate, the density of traffic cause frequent disconnections of vehicles from the network.

- *Availability of the transmission medium*: The air is the transmission medium of

VANETs. Although the universal availability of this wireless transmission medium which is one of the great advantages in IVC, becomes the origin of some security issues, related to both the nature of transmission in wireless environment and to the security of communications using an open support.

- *Anonymity of the support*: Data transmission using a wireless medium is generally anonymous. If we leave aside the restrictions and regulations of use, anyone equipped with a transmitter operating in the same frequency band can transmit and hold the band [2].

- *Limited bandwidth*: The standardized DSRC band (5.850-5.925 GHz) for VANET can be considered as limited, the width of the entire band is only 75 MHz. Restrictions of use in some countries suggest that these 75 MHz are not all allowed. The maximum theoretical throughput is 27 Mbps.

- *Attenuations*: DSRC band has also transmission problems related to digital transmission with such frequencies, such as reflection, diffraction, dispersion, different types of fading, Doppler effect, losses and propagation delays due to multi-path reflections.

- *Limited transmission power*: The transmission power is limited in the WAVE architecture, which limits the distance that data can reach. This distance is up to 1000 m. However, in certain specific cases such as emergency and public safety, it is allowed to transmit with a higher power [26].

- *Energy storage and computing*: Unlike other types of mobile networks, VANETs do not suffer from problems of energy, computing capacity or storage failure. However, real-time processing requirement of large amount of information is a challenge to keep in mind.

2.3.5 Routing protocols in VANETs

Routing protocols aim to ensure the selection of the best route for packets from source to destination in a timely manner [5]. The flow of data in a wireless environment, infrastructureless (especially V2V communications) and with high mobility is a difficult task to solve. In fact, routing is considered as one of the difficult problems of VANETs. According to [5], there are two main methods of routing in VANETs: hop by hop routing and source routing. Basically, all existing MANET's routing protocols can be optimized to be used for IVC [38, 39], taking into account the specific characteristics of vehicular networks.

VANETs routing protocols can be classified into the following six main categories [39, 40]. For each category, some examples of VANETs routing protocols are given.

2.3.5.1 Topology Based routing protocols

In this family we use information of the links (roads) to route packets. Protocols discover routes and prepare routing tables before sending packets. Generally, topology based protocols do not function properly for networks which exceed one hundred nodes [40]. In this family we distinguish 3 types of protocols:

- Proactive routing protocols: In these protocols, also called "table-driven", each node maintains one or more tables containing routing information for all destinations [41]. To keep routing tables updated, this class requires a periodic exchange of control packets between nodes.

- Reactive / On-demand routing protocols: In this family also known as "on-demand driven", the path computation is done only on request. Then the routing operation consists of two phases: the route discovery phase to route data and the updating phase executed when the network topology changes.

- Hybrid routing protocols: Hybrid protocols combine the mechanisms of proactive and reactive protocols. They use the technique of proactive protocols just for the neighbors discovery phase. For the rest of the nodes they act as reactive protocols.

Several "topology based protocols" exist in the literature, such as OLSR [42], TBRPF, FSR [39] and DSDV [43] as proactive protocols. DSR [42] and AODV [44] as reactive protocols. ZRP and HARP as hybrid protocols [39].

2.3.5.2 Position based geographic routing protocols

To select the next hop destination these protocols use data provided by positioning systems (e.g. GPS). So, no overall routes between sources and destinations must be created and updated [45]. In this category we find: VGPR, GPSR and MIBR [39].

2.3.5.3 Cluster-Based Routing protocols

In this category, the neighbors vehicles form a cluster. Each cluster has a "cluster-head", which is responsible of management functions intra- and inter-cluster. The training of the cluster and cluster-head selection are a critical required steps for the proper functioning

of the network. For VANETs, and due to the "high mobility", cluster management is considered as a greedy process. In this category we find: CBLR, CBR, HCB and CBDRP [39].

2.3.5.4 Broadcast Routing protocols

In this class of protocols, a flooding mechanism is used, where each node broadcasts messages to all its neighbors except the original sender. The flooding mechanism ensures that the message will reach every node in the network. This protocol category is suitable for a small number of mobiles. Its performance drops rapidly with the increase of the network size. "Broadcast Routing protocols" is a routing method frequently used in VANETs, to share the traffic, weather, emergency messages, information between vehicles, and to provide advertisements and announcements. In this category we cited: EAEP, DV-CAST and SRB [39].

2.3.5.5 Geocast Routing protocols

The basic principle of these protocols is to send messages to all vehicles in a specific geographic area [46]. The use of these protocols is very useful in the case of informational VANETs applications, connected to a given region. Research in this area is booming. As examples of such routing protocols we cite: DTSG [47], ROVER and DTSG [39].

2.3.5.6 Infrastructure based routing protocols

The "Infrastructure based routing protocols" are protocols including routing mechanism based on methods designed primarily for infra-structured networks, and after they have been adapted to VANETs use case. This category refers RAR and SADV [39], which use a static network node as a relay.

2.3.6 VANETs projects

The main motivations for launching national or continental VANET projects are reaching a reasonable road safety and well manage the transport sector, while ensuring accidents reduction and minimizing the waiting times in traffic. Several research and industrial ITS projects are active throughout the world. VANET protocols research project, affect various international organizations such as IEEE, IETF, ETSI, ISO, SAE, ASTM. As already shown, the IEEE developed the WAVE protocol stack, containing the IEEE 1609 standards family and including an extension of the famous 802.11 for ITS applications. On the other

hand, the IETF is working on extensions of Internet Protocol (IP) (IPv6, Mobile IP) and auto-configuration for VANETs. ISO also develops CALM standard for vehicle networks. The C2C-CC (Car-to-Car consortium) [48] develop and test VANETs protocols. In Europe, ETSI is working on the adaptation of ISO, IETF standards essentially. Interoperability and integration of these projects are the subject of intense discussions and studies. Among VANETs industrial projects [6, 49] we cite: VII, CICAS and IVBSS in the USA; CVIS, SafeSPOT, CARAVAN [50], COOPERS, PReVENT, GST, DRiVE, HIGHWAY, FleetNet, SeVeCom[48] and GeoNet in Europe; PREDIT in France; NoW in Allemagne; SmartWay and VIC in Japan; and ITSIndia in India.

Most of the mentioned projects include the integration of *V2V* and *V2I* communications [49]. For example, PReVENT helps the driver to avoid accidents or mitigate their impacts. GST (Global System for Telematics) focuses on the creation of an open standard for on-board telematic services. The CVIS (Cooperative Vehicle Infrastructure Systems) project focuses on road safety and integrates V2V and V2I communications. The DRiVE project (Dynamic Radio for IP Services in Vehicular Environments) focuses on the exclusive use of existing infrastructure for the implementation of the IVC system, it is the convergence of different cell technologies and high-speed UMTS networks, DVB-T and DAB develop innovative IP services to vehicles [51].

2.3.7 VANETs applications

ITS applications include basically applications for coordination of driving systems, cooperation for collision avoidance, notifications danger of the road. Comfort applications for travelers are also an innovative ITS applications category, they include the provision of mobile internet access, a variety of on-board services. VANET applications can be classified into Several family of classifications. These classifications range from two to several categories according to the degree of accuracy.

In [52], they classify applications into only two categories: Safety and Infotainment. In [1] VANET applications are also classified into Safety related applications and Other applications. In [31] they extended the classification into: Road safety applications, Traffic efficiency applications, and Value added applications. In [49] the classification is according to the involved element: driver, vehicle, passenger and infrastructure. Thus, we distinguish four families of ITS applications:

- Driver-oriented applications : to help drivers make better use of the road if it receives information about the dangers ahead, traffic, etc..
- Vehicle-oriented applications : Allowing to provide information to their vehicles to increase automation and improve road safety.
- Passenger-oriented applications : For the comfort of the user with new on-board services (e.g. infotainment, Internet access).
- Infrastructure-oriented applications : In order to make better use of highway infrastructure.

In general, we conclude that most of the research papers in VANET are practically in agreement that the main applications dedicated for vehicular networks can be grouped into three categories:

1. *Applications for road safety*: In order to improve travel safety and reduce road accidents, VANET applications provide collision avoidance and road work, detection of mobile and fixed obstacles and dissemination of weather information. In this category of applications, we find e.g: Slow / Stop Vehicle Advisor, Emergency Electronic Brake Light [7], Post Crash Notification, "Road Hazard Control Notification" Cooperate Collision Warning.

2. *Applications for driver assistance*: They aim to facilitate driving and assist the driver in specific situations such as overtaking vehicles, prevention of channel outputs, detection and warning of traffic congestion, warning of potential traffic jams etc.. In this category we find e.g: Congested Road Notification, Parking availability notification, Toll booth collections [7].

3. *Applications of passengers comfort*: These applications are for the comfort of the driver and passengers, they essentially provide services such as mobile Internet access, messaging, discussion between vehicles, collaborative network games, etc.. In the remainder of this section we limit ourselves to the description of some services and examples of applications of vehicle-to-vehicle communication systems.

Given their importance, it is absolutely essential to secure VANETs against all attacks that may occur. In the next sections we study the most existing VANETs security challenges and their possible cryptographic solutions.

2.4 VANETs security challenges

In their article "Threat of Intelligent Collisions" [2], Jeremy Blum and Azim Eskandarian ask an important question: A wireless network of intelligent vehicles can make a highway travel safer and faster. But can hackers use the system to cause accidents? . By this question they mark the importance that automakers must give to VANETs security. Safety in VANETs is crucial because it affects the life of people. It is essential e.g. that the vital information cannot be modified or deleted by an attacker. Securing VANETs systems must be able also to determine the responsibility of drivers while maintaining their privacy [8]. Communications passing through a vehicular network as well as information about the vehicles and their drivers must be secured and protected to ensure the smooth functioning of intelligent transportation systems [51].

The consequences of a security breach in VANETs are critical and dangerous. In fact, with a highly dynamic environment characterized by frequently instantaneous cars arrival and departure, and short connection durations, the deployment of a complete security solution is practically hard, it faces constraints and specific configurations. Although, the need for secure data transmission solutions in VANETs has been tipped as they appear, it is recently that this issue has aroused great interest and some solutions have been proposed.

In addition to the high mobility, the dynamic network topology and the use of the wireless medium which constitute the origin of the most important security breaches, other factors are also involved.

2.4.1 Involved entities in VANETs security

From security point of view, the entities directly involved in the security of VANETs are:

1. *The driver*:
   The driver is the most important element in the VANET safety chain because it is ubiquitous and he has to make vital decisions. In addition, all used cases currently scheduled for VANET applications make the driver as an interactive component with the driving assistance systems.

2. *The vehicle (OBU)*:
   Although it does not reflect the reality, The OBU refers to both the driver and the vehicle in the literature. In a VANET network, we can distinguish two kind of vehicles: the normal vehicles that exist among network nodes and operate in a normal way, and the malicious vehicles.

3. *Road Side Unit (RSU)*:
   As in the case of the OBU, we can distinguish normal RSU terminals, which operate in a normal way, and malicious RSU terminals.

4. *Third Parties*:
   We denote by third parties (may be trusted or semi-trusted), all digital equivalents of stakeholders in a direct way in intelligent transportation system. Among these third parties, we quote: the regulator of transport, vehicle manufacturers, traffic police, and judges. They all have their respective secrets / public key pairs. These public keys can be integrated for example into the OBU which is supposed an inviolable device.

5. *The Attacker*:
   In the context of VANET security, the attacker is one (or more) compromise entity that wants to violate successfully the security of honest vehicles by using several techniques to achieve his goal. An attacker can also be a group of vehicles that cooperate together. It may be internal (an authentic vehicle of the VANET network) or an external vehicle. It can also be classified as rational (the attacker follows a rational strategy in which the cost of the attack should not be more than the expected benefit) or irrational (a suicide bomber is an example of irrational strategy) [1, 53]. An attacker can be either active and made his attack with an exposed manner or passive and his actions cannot be detected.

2.4.2 Classification of VANETs attacks

As like any other communication and data processing systems, VANETs are exposed to various types of threats and attacks. The absence of the energy problem and the ability of an OBU to accommodate dozens of microprocessors give the vehicle an important capacity of processing and computing. Compared to a regular ad hoc network [8], this represents two significant benefits for VANET nodes. Due to the high mobility in VANETs, the two mentioned advantages affect the feasibility of attacks. Thus, there are possible attacks in

an ad hoc network that will be impossible for VANETs and vice versa.

Given the diversity of VANETs possible threats and attacks, and in the interests of clarity and simplification, it is necessary to classify them. Several classifications have been proposed in the literature [54, 5]. In this chapter we propose the use of a cryptographic related classification, which suite the better the presentation of the rest of our work (next chapter): cryptographic solutions of VANETs security issues. This classification is as follows:

2.4.2.1 Attacks on availability

Availability is a very important factor for VANETs. It guarantees that the network is functional, and useful information is available at any functioning time. This critical security requirement for VANETs, which main purpose is to ensure the users' lives, is an important target for most of the attackers. Several attacks are in this category, the most famous are the DoS.

2.4.2.2 Attacks on authenticity and identification

Authenticity is a major challenge of VANETs security. All existing stations in the network must authenticate before accessing available services. Any violation or attack involving the process of identification or authentication exposes all the network to a serious consequences. Ensure authenticity in a vehicular network is to protect the authentic nodes from outside or inside attackers infiltrating the network using a falsified identity [8]. The importance of identification-authentication process comes from the fact that it is frequently used whenever a vehicle needs to join the network or a service. There are several types of attacks in this category.

2.4.2.3 Attacks on confidentiality

Confidentiality is an important security requirement for VANETs communications, it ensures that data are only read by authorized parties [5]. In the absence of a mechanism to ensure the confidentiality of the exchanged data between nodes in a vehicular network, exchanged messages are particularly vulnerable to attacks such as the improper collection of clear information [8]. In these cases, the attacker can gather information on the location of the vehicle and its routes, on users privacy, etc.

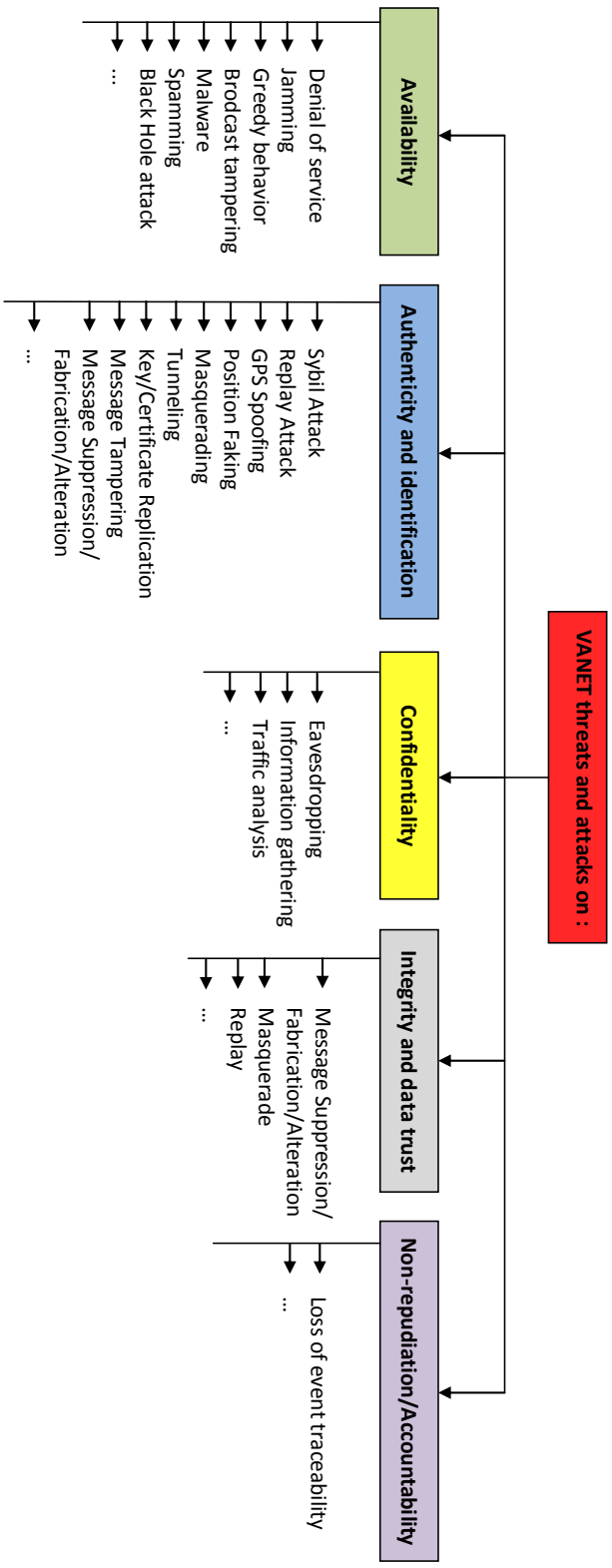


Figure 2.7. Examples of VANET threats and attacks

The information collected in the absence of a confidentiality mechanism may affect the privacy of individuals, knowing that it is difficult to detect this kind of attack, since it is virtually passive and user currently is not aware of the collection. However, in the case where the exchanged messages do not contain any sensitive information, Raya and Hubaux state in [1] that confidentiality is not necessary.

2.4.2.4 Attacks on integrity and data trust

The integrity of exchanged data in a system is to ensure that these data have not been altered in transit. Integrity mechanisms help therefore to protect information against modification, deletion or addition attacks. In the case of VANETs, this category targets mainly V2V communications compared to V2I communications because of their fragility. One of the possible techniques which facilitate this kind of attacks is the manipulation of in-vehicle sensors [13].

2.4.2.5 Attacks on non-repudiation and accountability

Non-repudiation in computer security means the ability to verify that the sender and the receiver are the entities who claim to have respectively sent or received the message [55]. Otherwise, the non-repudiation of data origin proves that data has been sent, non-repudiation of arrival proves that they were received. In a VANET context and since the manipulated data related to the safety and privacy of the users, it should be always possible to verify all hardware and software changes of security settings and applications (update, modification, addition, etc...) [56].

2.4.3 Examples of attacks

As it has been summarized in Fig.2.7 and already mentioned in the previous paragraph, there are several varieties of possible attacks in a vehicular network. In the following sections, we detailed the most existing attacks and vulnerabilities, which were presented separately in [5, 8, 9, 12, 13, 17, 18]. The possible potential solutions from a cryptographic point of view will be presented later in this study.

2.4.3.1 Attacks on availability

- ***Denial of service attacks***: The DoS attacks actually include a family of attacks targeting the availability of network services, which can have serious consequences

especially for VANETs applications. Because of their impacts, DoS attacks are classified as a dangerous class of attacks. They can be performed by internal or external malicious nodes to the network [8]. In these attacks, the attacker tries to block the principal means of communication and aims to interrupt services, so they will not be available to legitimate users [5]. As an example, flooding the control channel with high volumes of messages generated by intentionally manufacturing [18]. The network nodes (OBU and RSU) will not be able to handle the huge amount of received data. DDoS attack (Distributed Denial of Service) is a variant of DoS attacks [57], it is a distributed attack ordered by a main attacker who plays the role of "attack manager" with other agents who may be also victims unknowingly. The action methods of DDoS attacks are in most cases flooding the network and the results are always disastrous. Jamming, greedy behavior, blackhole attack, are examples of DoS attacks.

- ***Jamming attack***: The jamming attack, is a physical level of Denial of Service attack. Jamming in its basic definition is the transmission of a signal to disrupt the communications channel, it is usually intentional [58]. This lowers the signal to noise ratio (SNR: Signal to Noise Ratio) for the receiver. Unintentional interference is called "interference" and occurs when a transmission is made in a frequency band that is already in use and operational.

  For a successful adaptive jamming attack, the jammer must act at the same time that the activity of the useful signal to jam. It must also choose the most effective signal transmission model that merges the best the receiver. In a VANET network, and as shown in Figure 2.8, jamming once successful, can have inevitable consequences. Some research works such as [32, 58] have looked for some techniques to reduce the effect of jamming for mobile ad hoc networks.

- ***Greedy behavior attack***: The Greedy attack is an attack on the functionality of the MAC layer according to the architecture of the OSI model. The greedy node does not respect the channel access method and always tries to connect to the media. The main purpose is to prohibit other nodes to use the support and services. According to [59], a greedy behavior node tries also to minimize its waiting time for faster access to the channel and penalize other non-compromised nodes. Greedy behavior causes overload and collision problems on the transmission medium, which produces delays in authorized users services. Greedy behavior is independent and hidden to upper

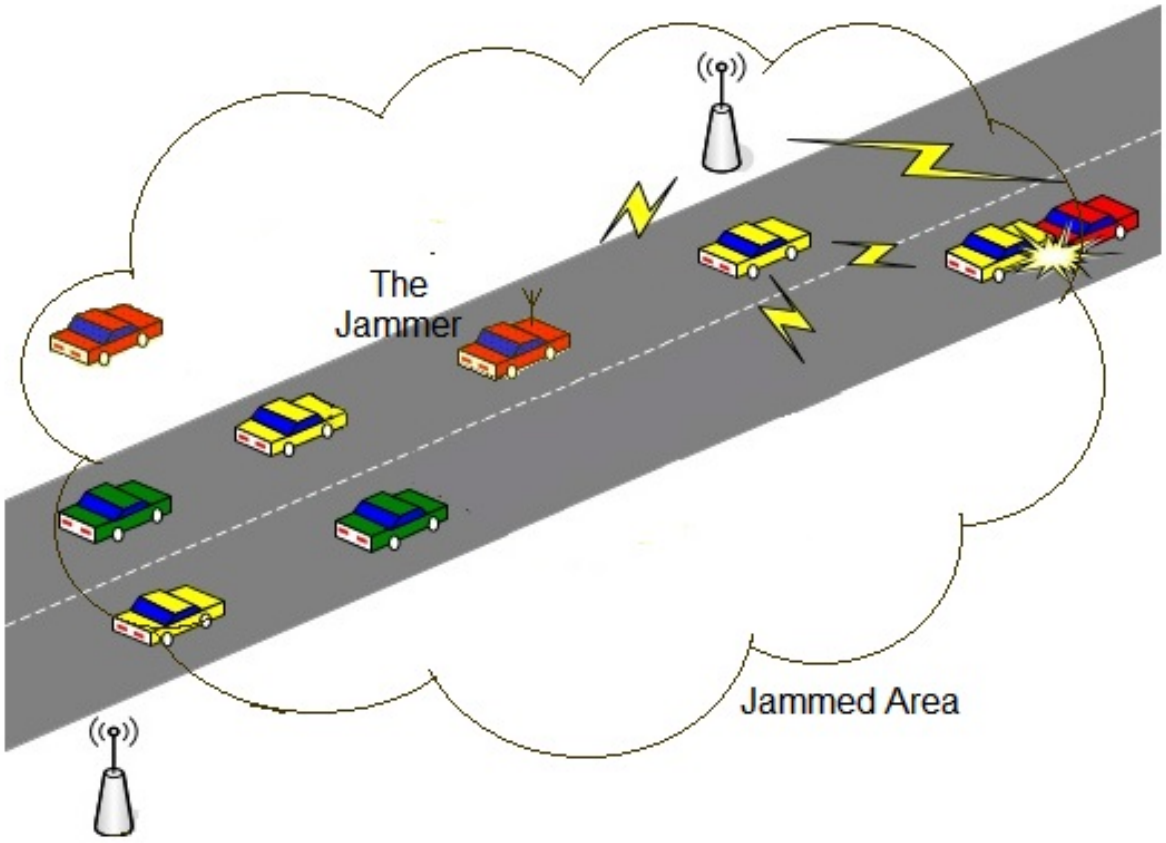


Figure 2.8. Jamming attack in a VANET environment.

layers, then it cannot be detected by mechanism designed for those layers.

- ***Blackhole attack***: The Blackhole attack is a conventional attack against the availability in ad hoc networks, it exists also for VANETs. In Blackhole attack, the malicious node receives packets from the network, but it refuses to participate in the operations of routing data. This disrupts the routing tables and prevents the arrival of vital data to recipients mainly because the malicious node always declares being part of the network and able to participate, which is not the case practically [8, 9].

  The effect of this type of attacks is more dangerous for VANETs than other mobile networks. A Blackhole node can e.g. redirect the traffic that receives to a specific node which does not exist in fact and this causes data loss [5]. Blackhole attack can also be used as a first phase of a man in the middle attack that we detailed later.

- ***Grayhole attack***: This attack consists in removing only the data packets of certain applications that are vulnerable to packets loss [60]. GrayHole is considered as a

Blackhole attack variant.

- ***Sinkhole attack***: This attack consists that the malicious node attracts neighboring nodes so their packets go through it, this helps to eliminate or modify the received packets before re-transmitting them eventually. The Sinkhole attack can be used to mount other attacks as Grayhole and Blackhole [61].

- ***Wormhole attack***: Wormhole is a denial of service attack, it requires the participation of at least two nodes. It simply consists that an attacker A sends a message to an attacker B geographically far from him, that B broadcasts completely. This message suggests to neighboring nodes of B, that A is their neighbor [62]. This attack allows two or more legitimate nodes and non-neighbors (their radio transmission areas do not overlap) to exchange control packets between them [17], to create non-existent roads.

- ***Malware attack***: Given the existence of a software components to operate the OBU and RSU, the possibility of infiltration of malware (malicious software) is possible in the network during the software update of VANET units [5, 9]. The effect of a malware is similar to the effect of viruses and worms in an ordinary computer network, except that in a VANET network, disruption of normal functionality is always followed by serious consequences.

- ***Broadcast tampering attack***: In this type of attack, the attacker tries to make and inject fake security alert messages in the network. This may hide the true safety messages to legitimate users,it can cause also accidents and seriously affect the overall network security [8]. In general this type of attack is possible for a legitimate node.

- ***Spamming attack***: As in a web environment, the spam messages such as advertisements e.g. have no utility for users. In a VANET network which is a mobile radio environment, this type of attack aims to consume bandwidth and cause voluntary collisions. Given the lack of a centralized management of the transmission medium, this makes more difficult the control of such attacks [5, 8].

2.4.3.2 Attacks on authenticity and identification

- ***Sybil attack***: The idea of the sybil attack as presented for the first time in [63] is that a malicious entity can present multiple identities at once. One of the direct means by which two entities can convince a third that they are distinct is to run,

at the same time, some tasks that one entity cannot do it alone. To ensure the identity of a node, several techniques have been proposed such as testing resources based on computational, storage and communication challenges. The Sybil attack is a dangerous attack in a VANET environment, given the disastrous consequences it can cause.

- ***GPS spoofing / Position faking attack***: In a VANET, the position information is of crucial importance, it must be accurate and authentic [5]. This attack consists on providing neighbors node a false location information. The exact location information can easily be obtained from a system such as GPS, whence the name of the attack: GPS spoofing. Each vehicle of a VANET is equipped with a positioning system (receiver), then the attack can be achieved using a transmitter generating localization signals stronger than those generated by the real satellites [9]. Successful GPS spoofing attack can facilitates other attacks such as attacks against applications which use the position of the node as an identification method.

- ***Node Impersonation attack***: Every vehicle has a network ID which allows to distinguish it among the other node of the VANET [9]. This identifier becomes especially important in case of problems. In the impersonation attack, the attacker obtains a valid ID and passes for another legitimate vehicle in the network. This constitute a violation of authentication process in the network.

- ***Tunnelling attack***: The tunneling attack is almost similar to the wormhole attack [8]. In this attack, attackers use the same network to establish a private connection (tunnel), while in the Wormhole the attackers (assumed to be external), use a different radio channel for the exchange of packets. The Tunneling attack connects two distant parts of the vehicular network by using an additional communication channel such as a tunnel [12]. Thus, the victims of two distant parts of the network can communicate as neighbors.

- ***Key and /or Certificate Replication attack***: The attack consists in the use of duplicate keys and or certificates which used as proof of identification and to create ambiguity which make more difficult to authorities to identify a vehicle, especially in the case of dispute.

2.4.3.3 Attacks on confidentiality

- ***Eavesdropping attack***: In wireless networks such as VANETs, listening to the media is an attack easy to carry out. In addition, it is passive and the victim is not aware of the collection. Eavesdropping attack is against confidentiality, it is without imminent impact on the network [5]. Through this attack, several types of useful information can be collected such as location data that can be used for tracking vehicles.

- ***Traffic analysis attack***: In a VANET, the traffic analysis attack is a passive serious threat against confidentiality and privacy of the users. The attacker analyzes collected information after a phase of listening to the network, it tries to extract the maximum of useful information for its own purposes.

2.4.3.4 Attacks on integrity and data trust

- ***Masquerading attack***: In this attack, the attacker is hidden using a valid identity (called a mask), and tries to form a Blackhole or produce false messages that have the appearance of coming from an authentic node. For example, to slow down the speed of a vehicle or require it a lane change. A malicious node attempts to act as an emergency vehicle e.g and thus cheat the other vehicles.

- ***Replay attack***: This is a classic attack, it consists in replaying (broadcast) a message already sent to take the benefit of the message at the moment of its submission. Therefore, the attacker injects it again in the network packets previously received. This attack can be used e.g. to replay beacons frames [64], so the attacker can manipulate the location and the nodes routing tables. Unlike other attacks, replay attack can be performed by non-legitimate users.

- ***Message tampering /suppression /fabrication /alteration***: As its name implies, this attack is against integrity it consists in modifying, deleting, constructing or altering existing data. It can occur by modifying a specific part of the message to be sent [12]. For example, the attacker falsifies received data indicating that the route is congested, and changes them to deceive users, so it indicates that there is no congestion and traffic on the road is normal. In this attack, the attacker can also delete a part of the message, alter or make new messages which help him achieving its intended purpose of the attack.

- ***Illusion Attack***: A direct application of the fabrication of messages attack is the Illusion attack, which is an attack against integrity and data trust. It consists in placing voluntarily sensors which generate false data [11]. These data can move normally in the network and require drivers interaction to make decisions. Authentication mechanisms are not able to detect this attack, because the attacker connects to the network in an authentic way.

Masquerading, Replay, Tampering, deleting, manufacturing, alteration, and illusion of messages can be also considered as attacks against the authenticity and identification.

2.4.3.5 Attacks on non-repudiation and accountability

- ***Loss of events traceability***: Despite its importance, we have not seen any document that addresses this attack that we find quite feasible in a VANET environment. In fact, this non-repudiation attacks consists of taking action, allowing subsequently an attacker to deny having made one or more actions. This kind of attack is essentially based on the erasure of actions traces and creating confusion for the audit entity. Some attacks can serve as preliminary to non-repudiation attack such as Sybil attack and duplication of keys and certificates.

2.4.3.6 Other attacks

- ***Attacks on privacy***: These attacks represent a major violation of privacy of drivers and VANET users. Several studies in the literature [21, 5] classify the attacks of privacy as a separate category for VANETs. As a practical example we find:
  - Tracking: The pursuit of a vehicle during its journey.
  - Social Engineering: Known e.g. whether a vehicle at a definite moment is in the garage or in circulation.

- ***Timing attack***: The timing attack is to delay the transmission of messages with high requirements on propagation delay, and transmit them e.g. after adding time preventing their treatment in a normal way. Some classifications such as in [16, 9], consider also this category as a separate family of attacks.

- ***Brute force attack***: The Brute force attack can be against the confidentiality of exchanged messages or the encryption keys. It can be also against the identification or authentication process. This attack can be performed e.g. while trying to find the

network ID of the vehicle by dictionary researching process. In a VANET environment where connection times are relatively short, Brute force attack is not easy to conduct, since it is time consuming and resource intensive.

- ***Man in the middle attack***: The man in the middle attack can be achieved in several contexts. As its name indicates, the attacker is inserted between the transmitter and the receiver. In the case of VANETs, the attacker is a vehicle which is inserted between two vehicles that communicate. The attacker controls the communication between the two victims [9], while they believe that they are in direct communication with each other. In the literature, the man in the middle attack is used to violate the authentication and or the integrity and non-repudiation mechanisms.

2.5 Conclusion

Vehicular Ad hoc NETworks (VANETs) are becoming popular in Intelligent Transportation Systems, they have been designed to provide road safety and services for passengers comfort. Given their importance related to the safety of humans' lives, VANETs attract attackers and represent a favorite target for several types of attacks which consequences vary from negligible to severe. Therefore, securing VANETs poses a great challenge.

In this chapter, and after reviewing the various recent aspects of VANETs sate of art such as standardization, routing protocols, projects and applications, we identify all existing security issues in VANETs and classify them from a cryptographic point of view. Also, we regroup and study a wide number of the most possible VANET attacks famous examples. For a sake of clarity, this approach facilitates for us to study in the next chapter the possible cryptographic solutions against VANET attacks in general and especially DoS attacks.

⁎ ⁎ ⁎ ⁎ ⁎

CHAPTER 3

CRYPTOGRAPHIC BASED SOLUTIONS

Contents

In this chapter, we illustrate the ability of cryptography as an efficient tool to implement security policies aiming to solve some VANETs security issues. We provide also our contribution about the problem VANETs secure group communications. By generating a secret key that can be used to encrypt or authenticate, the members of a VANET platoon can thus guarantee secure communication between them. To address this need, we propose a new secure variant of the Diffie-Hellman *algorithm for groups. This variant allows the generation of a group key fortified by a pre-shared secret to withstand the famous Man in the Middle (MiM) attack.*

3.1 Introduction

During the last years, vehicles have become increasingly reliable and comfortable. This need for reliability and comfort is accompanied by several security requirements. Unfortunately, the proliferation of VANET applications is severely affected by the potential attacks that may alter the services provided across vehicular networks. As detailed in the previous chapter, such threats, ranging from denial-of-service (DoS) to identity spoofing, might have disastrous effects since they can lead to the partial or total loss of control on the vehicle. A plethora of cryptographic solutions have been proposed in the literature to thwart the aforementioned attacks. However Due to the specific features of vehicular communication channels, existing security solutions are often inapplicable to thwart the aforementioned threats. A security solution for VANETs has to account for the contention-based opportunistic communication medium, the ad hoc group formation strategies between vehicles, the ease of eavesdropping and capturing the data exchange, the high mobility of the network nodes, and the crucial need for privacy and anonymity.

Cryptographic protocols have often been presented as potential solutions to cover the vulnerabilities of VANETs and improve their robustness to the malicious events characterizing the hazardous environment in which they operate. Despite the abundance of literature surveys related to the security of VANETS [5],[9] and[65] none of these surveys was specifically focused on cryptographic protocols. In this chapter, we provide a description of the most relevant cryptographic schemes that have been proposed for vehicular ad hoc networks. We begin by providing an overview on the communication architecture used in the

VANET context. Then, we underline the specific network security challenges associated to vehicular communication. An overview of the researches that have been published to propose cryptographic solutions for VANETs is also given with some insights on the future development issues.

3.2 Literature review

Cryptography presents the advantage to address and solve multiple VANET security breaches at once [23]. For example, deploying a central Validation Authority (VA) or a Vehicular PKI (VPKI) [2][56] for the authentication between vehicles and for signing warning messages solve security weakness such as *sybil*, *replay* and *illusion* attacks. Also, the use of strong encryption and key generation algorithms helps to avoid several attacks such as *traffic analysis*, *brute force* and *eavesdropping*.

Basically, we focus in this literature review on existing work related to key generation for secure group communications which is the subject of our contribution in this direction and based on the Group Diffie-Hellman (GDH) key generation algorithm that can be used to encrypt or authenticate exchanged information. This alternative can solve simultaneously several security problems and prohibit for example an intruder to eavesdrop or communicate with a group of a vehicles [21][53]. The lack of such technical proposals in the literature for VANETs was our main motivation to propose our contribution detailed later. To the best of our knowledge, no previous work was focused on the use of *GDH* for VANETs. Indeed, most of the developed works are specifically related to group key generation and group key management in its general context.

Boyd presents in [66] an example of the distributed approach that uses concepts of asymmetric cryptography. A group conference key is to be generated from the contributions of all members. This group key is set to $f(C_1, C_2, ..., C_n)$ where f is a function and C_i is the contribution of the participant i. Apart from the group leader, group members send their contributions in plain to the whole group. The leader of the group encrypted his contribution with the public key of each participant, and sends the compounds messages to the whole group. All group members can then deduce the group key.

Based on the Diffie-Hellman key exchange system, Steiner et al. proposed an extension adapted to user groups [67]. This protocol, called *GDH* for Generic or Group DH has

also been the subject of several versions, *GDH-1*, *GDH-2* and *GDH-3*. The most common is *GDH-2* which is the original version of the *CLIQUES* system [68]. In this system, Steiner et al. describe suitable protocols for dynamic groups. Indeed, they present a protocol for the initial key generation called *IKA* (Initial Key Agreement) and protocols for key regeneration and management for dynamic groups called *AKA* (Auxiliary Key Agreement). *CLIQUES* has served for many recently developed solutions for collaborative keys exchange.

To cope with the famous keys management problems in VANETs, such as the limited connectivity and the sensitive communication with a central certification authority, Busanelli et al. [69] proposed a novel key management approach to secure VANET communications. Especially, they provide a framework for group key multicast. Their framework is designated to a VANET specific communication scenario. In fact, they have proposed a scheme for generating a series of short-lived secret keys, shared by all the subscribers of a specific service. The application targets the *V2V* communications and consists in securely disseminating information owned by a small number of privileged users to a larger number of unprivileged users.

We have already classified in chapter 2 the VANET security challenges and attacks into attacks on : availability, integrity and data trust, authenticity, confidentiality and non repudiation. We study in the two next sections the most possible cryptographic solutions for each given attack and vulnerability. It is in order to provide a practical contribution to this kind of problems using cryptographic tools that our contribution detailed in section 5 has been carried out. For a sake of clarity,the basic and most known cryptographic tools and primitives are presented in the next section.

3.3 Cryptographic primitives and tools

3.3.1 Cryptographic primitives

We denote by cryptographic primitives, all the security services that cryptography provides. Modern cryptography offers several security techniques such as confidentiality, authentication, integrity, non-repudiation, secret sharing, etc. To satisfy these security services, cryptography uses methods such as encryption / decryption algorithms, Keys generation and exchange protocols, hash functions, digital signature and a lot of other

techniques. In the following we mainly rely on the famous reference [55] of Bruce Schneier for the presentation of the different cryptographic primitives.

- *Confidentiality*: It is the first problem that has been posed to cryptography. Confidentiality is to ensure that messages can only be read by those who are authorized. In a VANET, the information exchanged is mostly public, except those related to the privacy of users.

- *Authentication*: It allows the receiver to verify the origin of the data, and if the issuer is the one who claims to be. A VANET user should not be able to pass for someone else. The digital signature is one of the most used solutions for authentication problems.

- *Integrity*: It means that the receiver is able to ensure that the received message is the message that has been issued and it has not been altered in transit. An attacker should not be able to modify messages. One way hash functions form the basis solutions set for integrity problems. It should be noted that in the literature, the term "authenticity" means both authentication and integrity, and it is often confused in use with authentication.

- *Non-repudiation*: It is to ensure that a player cannot deny having done an action. In a VANET context, a vehicle should not be able to deny sending a warning e.g. or having done an attack.

3.3.2 Encryption/Decryption

The principle of encryption and decryption of a message, described schematically in Fig.3.1, is as follows:

- An algorithm for encryption / decryption, which is a set of information operations processing based on mathematical functions, receives as input a clear message and an encryption key, then as a result it outputs an encrypted message.

- The encryption / decryption algorithm receives as input an encrypted message and a decryption key, then as a result it outputs the corresponding clear message.

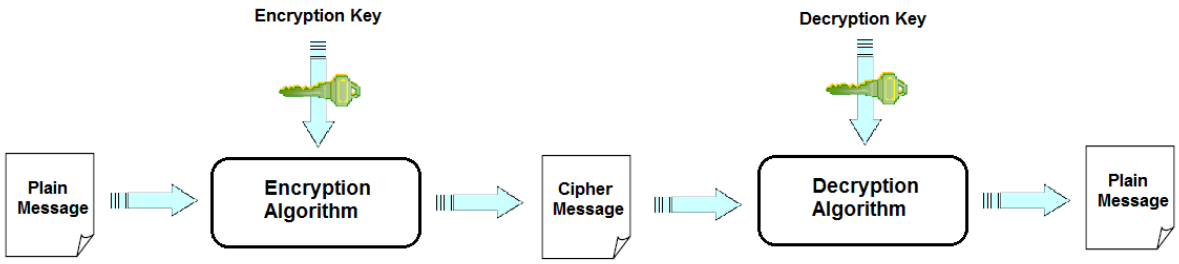


Figure 3.1. The principle of encryption decryption

3.3.3 Symmetric cryptography

Also called secret key cryptography. For this technique, the decryption key can be easily calculated from the encryption key, in practice it takes the same. Security in symmetric cryptography is based on the ability to keep the key secret between communicating parties. If the key is revealed the system is compromised. The requirement that both parties have access to the secret key is one of the main drawbacks of symmetric cryptography in comparison to asymmetric one.

3.3.4 Asymmetric cryptography

Also known as public key cryptography. The principle of Functioning is as follows:

- Each user has a pair of keys, one private key that he must keep secret, and the other public key that he must make it available to the public.

- If we encrypt with the public key, only the private key can decrypt and vice versa.

- It is practically impossible (time and resources) to determine e.g. the private key knowing the public one and vice versa.

Asymmetric cryptography can also be used in encryption, but compared to symmetric algorithms it is usually slower. It is mainly used in the key exchange procedures and in digital signature authentication tool through digital certificates. The public key cryptography solves several problems which secret key cryptography does not succeed.

Several proposed public key cryptography based solutions for some security issues in VANETs will be discussed later.

3.3.5 PKI, digital certificates and timestamping

The management of private and public keys for a large number of users requires the establishment of a PKI: Public Key Infrastructure, which is a set of software, hardware and procedures components [70]. A PKI can provide several security services, the most important is to be a trust third party between digital counterparts. PKI ensures that role through the certification authority (CA), so it signed, delivers and keep up to date digital certificates which represent a digital ID for an entity.

In fact, a certificate is an electronic file (can be stored in many forms), which binds together a public key with an identity with the guarantee of the certification authority. A certificate allows to authenticate and sign (signing certificates) and also encrypt messages (encryption certificates). Timestamping is also among the services that PKI can provide. It certify that an event (send /receive / signing a message, ...) happens at a given time. The timestamping faces basically to authentication and non-repudiation attacks.

In a VANET context, several solutions e.g. propose the creation of a PKI related to VANETs named VPKI (Vehicular Public Key Infrastructure) [6, 13], and propose the use of digital certificates as a method of rapid authentication in a vehicular network. This proposed solution will be discussed later for some related attacks.

3.4 VANETs security challenges versus cryptographic solutions

A plethora of cryptographic solutions have been proposed in the literature to bypass or mitigate the aforementioned attacks. Table 3.1 gives a summary of the contribution of these cryptographic schemes with regard to the basic protection requirements for VANETS. A solution that has been proposed by [1, 23] consists in deploying a central authority validation, which validates entities in real time. Validation can be direct or indirect. In direct validation, the entity that requires access to the network gets directly connected to the validation authority. In the indirect method, an entity already enabled can accept an incoming entity. To limit the drawbacks of this delegation functionality (as shown in Figure 3.2), the validation authority can use such temporary certificates [71].

In the case of presence of authentic and secure links with trusted nodes, [14] proposes

Cryptographic solutions	Provided security requirement					
	Auth.	Avail.	Conf.	Integrity	Non Repudiation	Privacy and Anonymity
Raya et al. [1]	x	x	x	x		
Xiao et al. [14]	x	x				
RoselinMary et al. [18]	x	x				
He et al. [19]	x	x				
Rawat et al. [12]			x			
Malla et al. [20]		x				
Zeldaaly et al. [8]	x		x	x	x	
Blum et al. [2]	x		x	x	x	
Kaushik et al. [21]	x		x	x	x	x
Gollan et al. [72]	x					
Singelée et al. [56]	x			x	x	
Mejri et al. [73]	x		x	x	x	x

Table 3.1. Overview on cryptographic approaches for VANETs.

to reduce the effect of the Sybil attack by validating the unknown nodes through secure location verification. Roselin Mary et al. [18] also proposes a PKI-based technique to achieve this goal. Changing the transmission channel and using the frequency hopping technique (FHSS: Frequency Hopping Spread Spectrum) has also been proposed as a secure solution. It involves cryptographic algorithms for generating pseudo-random numbers. This proposal [19][12] requires a modification of the standard that currently allows only the use of OFDM. In [20], a digital signature-based authentication mechanism has been proposed to reduce the impact of certain DoS attacks. A timestamp-based technique has been proposed in [8] to enforce strong authentication policies in VANETs.

The use of specific PKIs to guarantee authentication between communication peers and to sign the exchanged messages has been discussed in [1]. For example, establishing group communications [2][21] will allow the secure exchange of cryptographic keys being managed by a system of Group Key Management (GKM). This prevents an intruder from communicating with the group at the moment of the establishment of the group key. Pres-shared secrets may also be used to discard attackers during the negotiation phase. However, this technique is hardly applicable in VANETs due to the rapid changes in the network topology.

Only a few trust models have been proposed for enforcing accurate information sharing in vehicular networks. Two typical entity-oriented trust models are the sociological trust model proposed by Gerlach [75] and the multi-faceted trust management model proposed

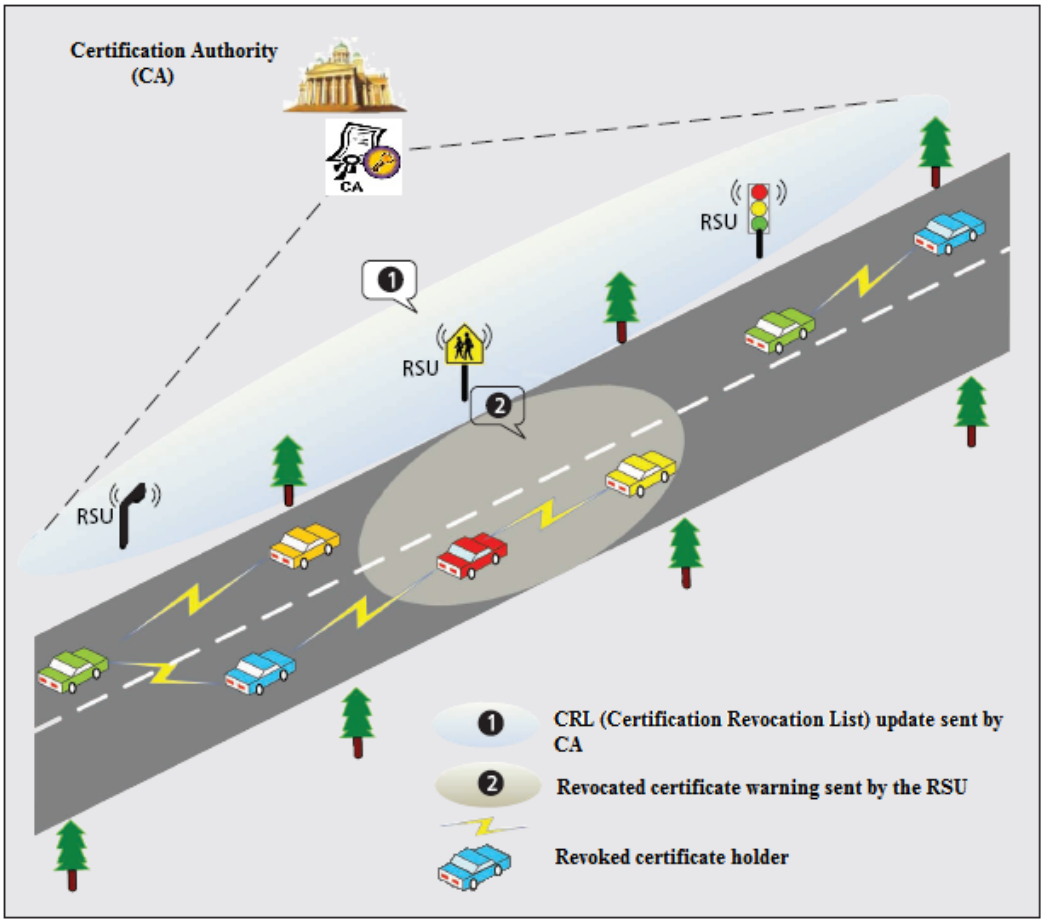


Figure 3.2. Possible VANET drawback with classic PKI implementation ([74, 71].)

by Minhas et al. [76]. The sociological trust model is proposed based on the principle of trust and confidence tagging. Raya et al. [77] propose that data-oriented trust may be more appropriate in the domain of Ephemeral Ad-hoc Networks such as VANETs. Data-centric trust establishment deals with evaluating the trustworthiness of the data reported by other entities rather than trust of the entities themselves.

The main question that should be addressed at this level is: what security problems among those existing in VANETs can cryptography and its strong primitives and services solve? We summarize in Table 3.2 all recent existing attacks for VANETs. For each attack, we define the affected services and we describe the related possible cryptographic solutions. The solutions are proposed without going into details of the advantages and disadvantages of each solution. We detailed only both the technical aspect of each solution.

Attacks	Compromised services	Cryptographic solutions
DOS	Availability	- Use bit commitment and signature based authentication mechanisms [19], which reduces the impact of almost of DOS attacks.
Jamming	Availability	- Switch the transmission channel and use the frequency hopping technique FHSS (Frequency Hopping Spread Spectrum) which involves cryptographic algorithms to generate pseudo-random numbers for the hopping algorithm. This proposal requires a modification of the used standard which currently allows only the OFDM [20].
Eavesdropping	Confidentiality	- Encrypt only data which has paramount importance and which manipulation puts in risk the privacy of the driver (positioning data, vehicle identification data, ...).
Traffic analysis	Confidentiality	- Same proposition as eavesdropping. - Use algorithms such as VIPER for V2I communications [12].
Replay	Authentication Integrity	- Use timestamping technique for packets which their replay is dangerous [8]. For this proposition, we encountered the problem of time synchronization between entities.
Brute force	Confidentiality	- Use strong encryption and key generation algorithms unbreakable within a reasonable running time [8]. This prohibits access to information to those who are not allowed.
Timing attack	Availability	- Use the timestamping mechanism for packets of delay-sensitive applications. For this proposition, we encountered the problem of time synchronization between the entities.
Man in the middle attack	Authentication Confidentiality Integrity	- Use a strong authentication methods such as digital certificates and zero-knowledge.
Sybil attack	Authentication Availability	- Deploy a central Validation Authority (VA), which validates entities in real time. Validation process can be direct or indirect. In direct validation, the node which wants to authenticate, establish a direct connection with the VA. In the indirect method, an entity already enabled can accept an incoming entity. The VA can use temporary certificates [9]. The use of the validation technique makes the VA a privileged target of attacks. - In the case of the presence of authentic and secure links with trusted nodes, [14] proposes to reduce the effect of the sybil attack by validating unknown nodes with the method of secure location verification. For this method, [6] proposes the use of approved certification. - Strengthening the authentication mechanism by the use of distance bounding protocols based on cryptographic techniques such as bit commitment and zero-knowledge [25, 78, 56, 79].

Attacks	Compromised services	Cryptographic solutions
Message tampering/ suppression/ fabrication/ alteration	Availability Integrity Non-repudiation	- Use a vehicular PKI (VPKI) or a zero-knowledge techniques for the authentication between vehicles and for signing warning messages [2, 56, 53]. - Establish group communications [21, 53]. Keys can be managed by a Group Key Management system (GKM). This causes that an intruder could not be able to communicate with the group.
Broadcast Tampering	Integrity	- Given that this attack can be performed by a legitimate node of the network, cryptographic primitives are enable to prevent it. However, a non-repudiation mechanism may exist.
Key and /or Certificate Replication	Confidentiality Authentication	- Use certified and disposable keys. - Check the validity of digital certificates in real time via CRL (Certificate Revocation List) [1], which represents a real hard problem in VANETs. - Use cross certification between the different certification authorities involved in VANETs security scheme [6].
Loss of event traceability	Non-repudiation	- Same proposition as illusion Attack.
Tracking / Social engineering	Privacy	- Use always variables MAC and IP addresses to separate the addresses from the identities of vehicles and drivers [1]. MAC and IP addresses allocation must be managed by robust algorithms.
Illusion Attack	Authentication Integrity	- The hardware equipment and the software must be accessible only by authorized. - Updates or reading operations from the sensors must be authenticated and verified e.g by a challenge/response mechanism. - Use trusted hardware for which it is piratically impossible to change existing protocols and values, except by authorized [56].
GPS spoofing/ Position faking	Authentication Privacy	- Use bit commitment and signature based mechanisms with positioning systems to accept only authentic location data [19, 79, 25].
Node Impersonation	Integrity Authentication Non-repudiation	- Use variables MAC and IP addresses for V2V and V2I communications [6]. - Authenticate via digital certificates [9]. - Strengthening the authentication mechanism using distance bounding protocols based on cryptographic techniques such as bit commitment and zero-knowledge [25, 78, 56, 79]

Attacks	Compromised services	Cryptographic solutions
Greedy Blackhole Grayhole Sinkhole Wormhole Malware Masquerading Spamming Tunneling	Availability Authentication Integrity Confidentiality Non-repudiation	- For these attacks, cryptography does not offer real solutions, but certain suggested actions can reduce disastrous effects, such as digital signature of software and sensors. - Use trusted hardware for which it is piratically impossible to change existing protocols and values, except by authorized [56].

Table 3.2. Cryptographic solutions for VANETs attacks and vulnerabilities.

3.5 Contribution: A new group Diffie-Hellman key generation proposal

3.5.1 Proposal context

The first objective of our proposal is to solve or avoid a wide numbre of VANET security challenges, for which cryptography can provide adequate solutions i.e. data confidentiality and user's authentication. In fact, the security of encryption and authentication methods is based on the confidentiality of the generated keys. We must therefore ensure that the generated and used session keys are only known by who are authorized (members). In this case, Group Key Managment Protocol (GKMP) ensures management and security of keys.

In the literature, many solutions were proposed for secure generation and exchange of group keys. These solutions differ by a certain number of characteristics such as fault tolerance, collaboration, decentralization, dynamic and hierarchy. It should be noted that quite systems are based on the adoption of an existing Pair-Wise Key Management (Designed for only two users). For example, protocols Cliques [80] [81] and [68] are an extensions of the *Diffie-Hellman* [82] algorithm to get it working for groups. In dynamic groups, it is important to manage this dynamism. When a new member joins the group, it must have a group key enabling him to exchange data since the time he received it. In this case, the key management responsible entity should replace the old group key by a new one in order to prevent a new member to access the old traffic. The generation and distribution of a key to any member who has the right of access reflect the use of group key in practice. Basically, group key management protocols use a key for each session; this session key is derived from a master key. At the end of a session and all traces of the session key must be removed. Furthermore, the concept of session key is used to create communication

independence between different sessions and applications. Thus, add and remove of users can be considered as the begin of a new session. According to [83][84], there are several GKMP classifications. The three most important are:

- ***Centralized:*** In this approach a single entity chooses the group key and transfers it securely to other group members. This entity is called Group Controller, denoted GC [85][86]. In addition to the management difficulties encountered by the GC when the group expands, it represents a prime target for attacks. Once the GC has a problem, the whole group is therefore affected. The group will be vulnerable since the keys are neither generated nor distributed. The major challenge of using the centralized approach is to ensure the protection of the key during the transfer phase.

- ***Collaborative:*** A system is called collaborative when all group members are involved in the key generation phase. The absence of a head within the group, make the system decentralized. Multiple controllers of subgroups called clusters ensure group key management then. The benefit is to reduce the effect of a change in the composition of the group's key, such as when adding or removing a member. Indeed, adding a member to a subgroup does not affect the entire group but only the cluster to which is added this member. The subdivision into clusters has the advantage of increasing fault tolerance of the entire system.

- ***Distributed:*** Called also collaborative/decentralized approach. In this approach, the group's key is derived using key agreement protocol concepts. According to [87], a key agreement protocol is a protocol that allows a group of participants to generate a key whose value is based on all their contributions. Each participant should not be able to predict the resulting value of the key that will be generated. The generation of this key is carried out by simple network messages exchange. These messages contain members' contributions. In addition, the obtained key is only known by group members [66].

In VANET environment it is clear that the distributed approach is the most suitable. In fact, this approach has the advantage of not needing secure channels between vehicles. However, since the group key is based on the contributions of all members. However, the key generation required more computations since the number of contributions becomes important. For VANETs, this is not a problem given the significant computational capabilities embedded in a smart vehicle.

Therefore, our contribution is to study and implement our variant of the distributed group key management algorithm *GDH* (Generic or Group Diffie-Hellman) to be used for VANETs. In our proposal, and in addition to the exponents used in the original algorithm, we propose the use of pre-shared secret as an additional protection to withstand the famous *Man in the Middle* attack. This proposed solution is more suitable for secure communications in a platoon of vehicles whose members know beforehand.

3.5.2 Background

3.5.2.1 Diffie-Hellman algorithm overview

Diffie-Hellman is a powerful algorithm for securely exchanging cryptographic keys over an insecure channels. It is one of the first public key algorithms, originally conceptualized by Ralph Merkle [88] and designed in its actual version by Diffie and Hellman [82]. The DiffieHellman key exchange method allows two participants, which have no prior knowledge of each other to establish together a common secret key over an insecure channel. Thus, this key can be used to encrypt further communications. *DH* is a simple algorithm and is based mathematically on the discrete logarithm problem from which the practical impossibility of breaking it.

Basically, the original implementation of the algorithm used the cyclic multiplicative group of integers modulo p, where p is prime, and g is a primitive root modulo p, ($g \in \mathbb{Z}_p^*$). According to Kirchhoff principle, g and p are not secret and assumed to be known by attackers. In a cyclic multiplicative group $\mathbb{Z}_p^*$ we have the main property:

$$(g^a)^b mod(p) = (g^b)^a mod(p).$$

Alice and *Bob* want to communicate securely without they know each other in advance, they agree on a large prime p and a generator g for $\mathbb{Z}_p^*$. *Alice* and *Bob* agree on a secret key as follows:

- *Alice* randomly picks a number $a < p - 1$, computes $X = g^a mod(p) \in \mathbb{Z}_p^*$ and sends X to *Bob*.
- *Bob* randomly picks a number $b < p - 1$, computes $Y = g^b mod(p) \in \mathbb{Z}_p^*$ and sends Y to *Alice*.

- Both *Alice* and *Bob* can now compute respectively the key: $K = Y^a mod(p) = X^b mod(p) \in \mathbb{Z}_p^*$

In no time, *Alice* and *Bob* have exchanged their secret values a and b. Thus, for an adversary who knows g and p and can have $g^a mod(p)$, or $g^b mod(p)$, it will be practically impossible for him to deduce the secret key $K = g^{ab} mod(p)$. This is the discrete log problem on which the security of the DH algorithm is based. Successfully attacking the Diffie-Hellman algorithm is mathematically equivalent to solve the discrete log problem, which is: *"Given a prime number p, a generator g of* $\mathbb{Z}_p^*$ *and two numbers* $X = g^x and Y = g^y, compute K = g^{xy}$*"*.

There are several techniques of attacks against the discrete logarithm problem, which are more efficient than exhaustive attack, but there is no known polynomial time attack. For large primes, this problem is believed to be practically intractable [89][90].

The prime number p in Diffie-Hellman should nowadays be chosen to be at least *1024 bits*. For long term security, *2048 bits* is recommended(which is not the case for VANETs exchanged messages). For example a values of a and b of at least *70 digits* long is quite sufficient for VANETs. It is very important to note that g does not need at all to be large, in practice it is usually a small integer.

As we need to manipulate large exponents, it is essential to detail the various existing techniques to calculate a *modular exponentiation* rapidly and with minimal cost (time / memory). In fact, in a VANET environment the time challenge is more important than memory one.

3.5.2.2 Modular exponentiation

In modular arithmetic, modular exponentiation is exponentiation modulo an integer. For large numbers, it is mainly used in cryptography. Typically, the variables in an exponentiation are: a given base b, an exponent e, an integer p. We want to compute:

$$C \equiv b^e mod(p). \tag{3.1}$$

The modular exponentiation calculations are considered easy to do for small numbers. However, if the numbers to manipulate are large, calculating an exponentiation becomes a

real challenge. The time required to perform a modular exponentiation depends essentially on the exponentiation technique and on processor capacities. To perform this kind of treatment, there are substantially 3 methods. The brief overview of the first two methods will justify our choice for the third one:

- *Direct*: This method consist on the computation of b^e directly and then take this number modulo p. Unfortunately, this method involves a significant computing time and a large memory utilization since it does not take advantage of the commutative ring structure of integers modulo p. However, this structure allows the computation to be made directly in this ring without passing by the integers. The advantage is to manipulate data whose size does not exceed that of p.

- *Less memory*: This method requires more operations than the direct method. The operations take less time despite the requirement less memory, since there is less exchanges between volatile and swapping memories. Thus, this method is a bit faster. As the first method, this requires $O(\sqrt{e})$ of computing time.

- *Square And Multiply (SAM)*: Given the shortcomings of each of the previous methods, we choose the "Square And Multiply" method *(SAM)* [87], which is a smart and fast method of modular exponentiation computation. It is composed by a series of squaring and multiplication, which significantly reduces the number of calculations to do and the necessary storage space. It is a combination of the method *Less memory* and a technique called *Binary exponentiation* or *Exponentiation per square*. Obviously, the numbers will be manipulated in binary format. The exponent e is converted to binary notation is written as:

$$e = \sum_{i=0}^{n-1} e_i 2^i. \tag{3.2}$$

By definition, $e_{n-1} = 1$, the other e_i can take 0 or 1 for $i \in 0 \leq i \leq p-1$. Thus, b^e is written:

$$b^e = b^{(\sum_{i=0}^{n-1} e_i 2^i)} = \prod_{i=0}^{n-1} (b^{2^i})^{e_i}. \tag{3.3}$$

Then, the equation (3.1) $C \equiv b^e mod(p)$ becomes:

$$C \equiv \prod_{i=0}^{n-1} (b^{2^i})^{e_i} mod(p). \tag{3.4}$$

This method is implemented for modular exponentiation computation in our proposed *GDH* algorithm that we describe next section.

3.5.3 Proposed solution: Analysis and design

Our contribution is essentially to propose, design and implement a new *DH* algorithm to be used for secure VANET applications. In its original proposal *DH* was designed as a pair-wise algorithm. To understand how we will use it for group communications, we detailed in the next subsection its functioning for 3 nodes.

3.5.3.1 GDH enhanced algorithm

Figure 3.3 illustrates the execution the *DH* protocol for three vehicles A, B and C. a, b and c respectively designate their secret contributions. So, the group key is g^{abc}. This key is generated respectively by each vehicle using the exponentiation of neighbors received message by their own secret a, b or c. Our detailed generation algorithm is as following:

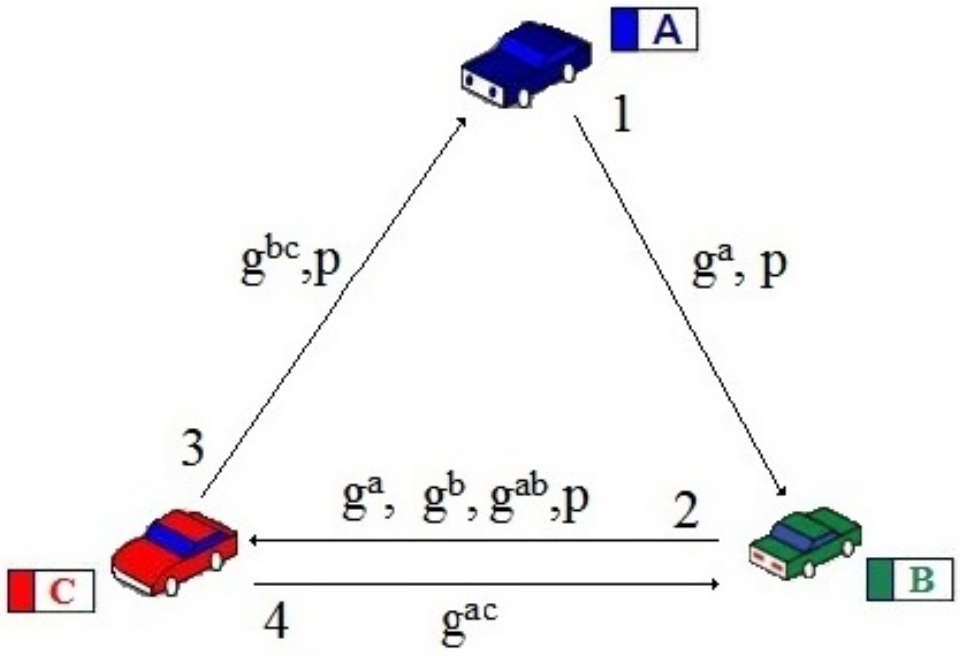


Figure 3.3. GDH exchanged messages for 3 vehicles.

- A chooses (or has in advance) a number generator g of a cyclic group, p a public prime and generates a random secret a.
- A calculate $g^a mod(p)$.
- A send to B : g, p, $g^a mod(p)$.
- B generate a random secret b.
- B calculate $g^b mod(p)$ and $g^{ab} mod(p)$.
- B send to C : g, p, $g^b mod(p)$, $g^a mod(p)$ et $g^{ab} mod(p)$.
- C generate a random secret c.
- C calculate $g^{bc} mod(p)$ and $g^{ac} mod(p)$.
- C calculate the group key $K = g^{abc} mod(p)$.
- C send to A : $g^{bc} mod(p)$
- C send to B : $g^{ac} mod(p)$
- A calculate the group key $K = g^{abc} mod(p)$.
- B calculate the group key $K = g^{abc} mod(p)$.

In Fig.3.4, we consider the same protocol when a fourth vehicle D joins the conversation. In this case, the vehicle C uses the last message it has received during the generation of the key and multiply the components of this message with a new contribution c', and sends the message to the new member D. The fourth vehicle D adds its contribution, and sends back the result to the rest of the group, which will be capable to generate the new group key whose value is $g^{abc'd}$. For additional users, the same process can be applied again.

We have already demonstrated that the major difficulty in the use of the *DH* algorithm lies in the calculation of the modular exponentiation. We have also shown that the best method for this type of calculation, (best *time/memory* compromise) is the already detailed *SAM* method. We detailed in algorithm 1, inspired from [87] our *SAM* implementation technique for the modular exponentiation calculation. The running time of this algorithm is $O(\log e)$. Although, the *SAM* algorithm is simple at first glance, but the main difficulty is the implementation of large numbers optimum manipulation class. For a *64*

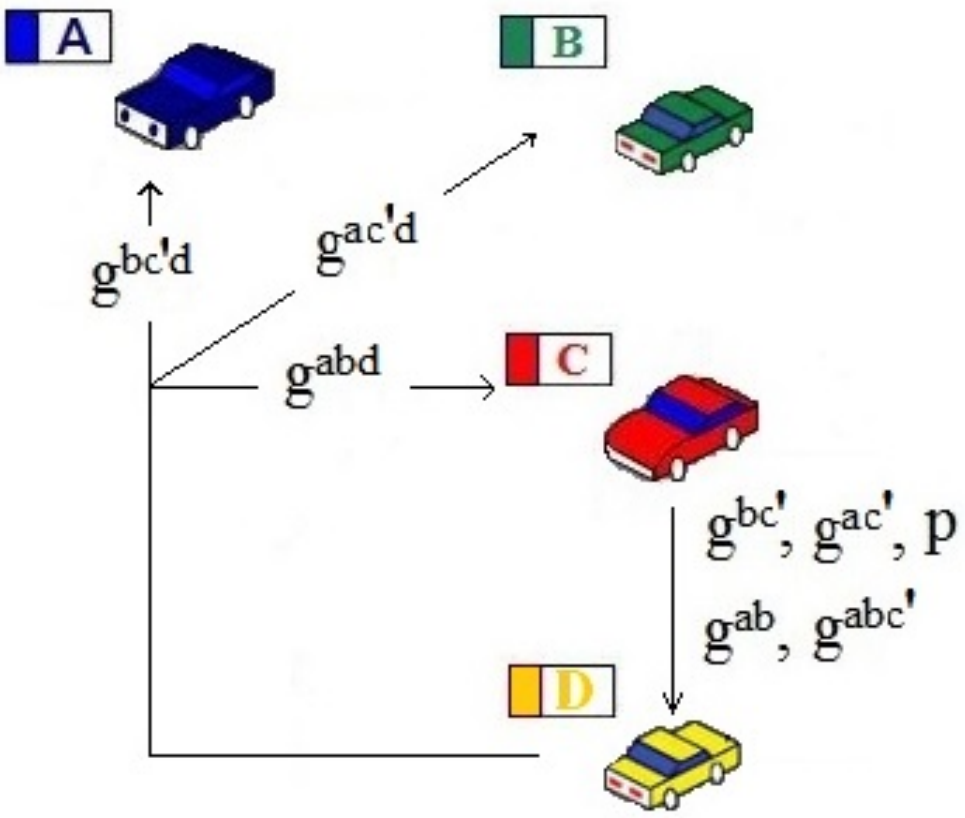


Figure 3.4. GDH exchanged messages for the addition of a fourth vehicle.

bits OBU (On Board Unit) for example, we can just perform operations at most of the order of $2^{64}(\approx 10^{20})$, without having to make a special treatment. However, once the numbers to handle exceed this threshold, it is essential to decompose them into blocks similar in size to microprocessor registers, and specify by programming the meaning of each block of bits that constitute the large number.

3.5.3.2 Countermeasures against the Man In Middle attack

Despite its cryptographic robustness the *DH* algorithm is vulnerable to the Man in the Middle attack (*MIM*). In this attack, given the absence of a specific authentication mechanism, the attacker *Charlie* stands between *Alice* and *Bob*, he pretends to *Alice*, that he is *Bob* and vice versa as illustrated in figure **??**. This attack once achieved, allows the attacker to have the same key as *Alice* and *Bob*[91]. Although it is too difficult to achieve for more than two communicants, we decided to secure our proposal against this attack.

Algorithm 1: Binary Modular Exponentiation using the *SAM* method

INPUT : $a \in \mathbb{Z}_p^*$,
p,
$e = \sum_{i=0}^{t} e_i 2^i$ $(e : 0 \leq e \leq p-1)$
OUTPUT: $b = a^e mod(p)$

begin
1. $b \leftarrow 1$ **if** $(e = 0)$ **then**
   $return(b)$
end
2. $A \leftarrow a$
3. **if** $(e_0 = 1)$ **then**
   $b \leftarrow a$
end
4. **for** *(*$i = 1$ *to* t*)* **do**
   $A \leftarrow A^2 mod(p)$
   if $e_i = 1$ **then**
      $b \leftarrow A * b \ mod(p)$
   end
end
5. Return (b);

end

Given that the solution we offer is essentially the generation of a group key for securing communications between members of a platoon of vehicles who know each other in advance, our chosen solution to deal with the attack *MIM* is the use of a secret S shared in advance between the members of the platoon. The pre-shared secret S admits a bits length which is assumed to be higher than the bits length n of the generated group key K.

We denote by $[S]_n$, the truncation of the secret S into n bits, we denote also by $\oplus$ the XOR bitwise operator between two variables of the same bit length. $[S]_n$ and K have the same bit length, thus, we can calculate the new group key $K_G = K \oplus [S]_n$. For example, and according to the truth table of the XOR operator the K_G is calculated as detailed in Fig.3.6.

The new group key K_G present the advantage to be computed and known only by the group members. It is also very rapid in computation and this is due to the rapidity of the XOR bitwise operator. To the best of our knowledge, our proposed countermeasure is the

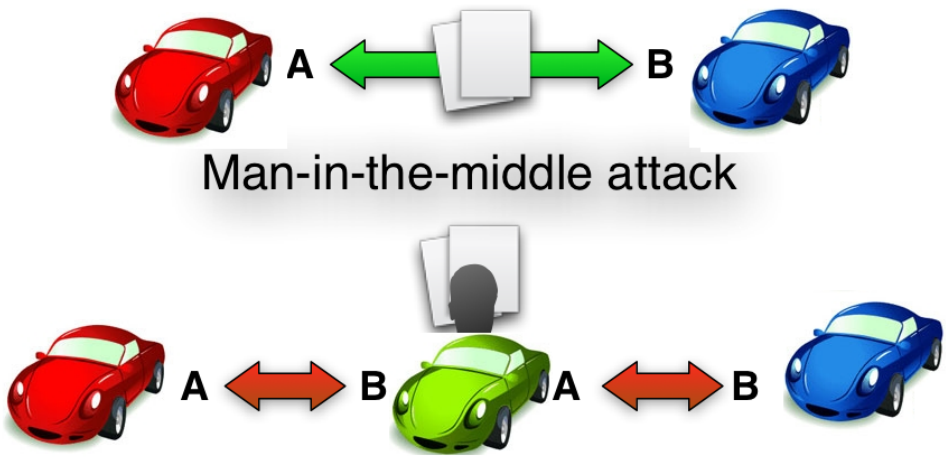


Figure 3.5. The man in the middle attack in VANET context.

first proposal in literature for securing the *GDH* algorithm against *MIM* attack using a pre-shared secret in a VANET environment.

3.5.4 Performance evaluation

To evaluate the performance of our proposed algorithm, we have simulate a network of 40 vehicles in a highway environment using Network Simulator 3 (ns-3) [92] as a protocol simulator and *SUMO* [93] as a mobility simulator. Our simulation chain is summarized in Fig.3.7. Among these 40 vehicles, we have a platoon of *5* vehicles which pre-shared a secret S beforehand. The simulation parameters are detailed in Table 3.3. The *GDH* has been implemented in the OBU (On-Board Unit) of each vehicle using the Square And Multiply *(SAM)* technical method detailed before.

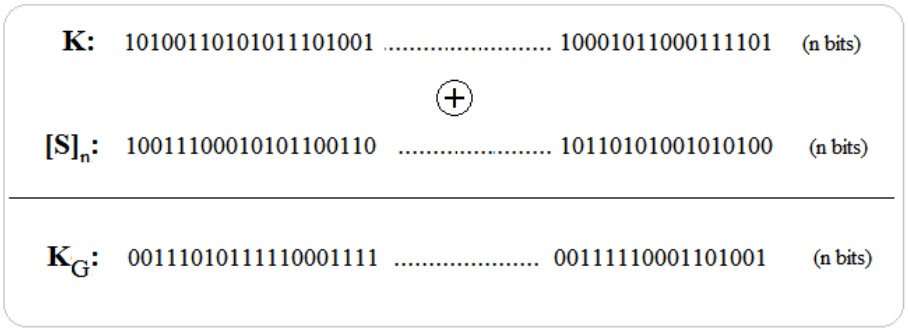


Figure 3.6. Example of K_G computation using the bitwise XOR operator.

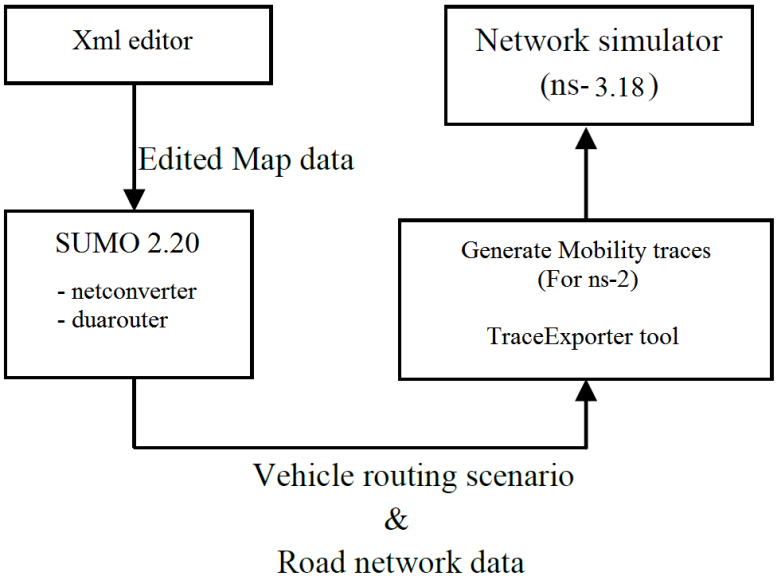


Figure 3.7. Simulation chain and the combination use of SUMO, ns-2 and ns-3.

Parameter	**Value**
Protocol	*IEEE 802.11p*
Transmission rate	*OfdmRate6MbpsBW10MHz*
Environment	*Highway*
Highway size	*5000m x 15m*
Number of lanes	*3 lanes (5m for each)*
Average speed	*70 Km/h (≈ 20m/s)*
Max speed	*90 Km/h (≈ 25m/s)*
Execution time	*300s*
Packet size	*1400 bytes*
Channel	*CCH (Control Channel)*
Routing protocol	*OLSR*
Mobility simulator	*SUMO*
Number of vehicles	*40 vehicles*

Table 3.3. Simulation parameters.

According the last considerations, we have simulate our key generation and exchange between a platoon of respectively 3, 4 and 5 vehicles simultaneously. In addition, we consider two scenarios, with an average speed of *70 km/h* for the first scenario and an average speed of *90 km/h* for the second one. Each scenario has been repeated 5 times. Finally, we specifically focus on the time needed for the group to generate and establish a secure

group key K_G in order to secure communications between platoon members.

Operation	**Average duration**
Modular exponentiation ($e \approx 78$ decimal digits)	$\approx 40ms$
Random number generation (≈ 78 decimal digits)	$\approx 3ms$
Big numbers native multiplication	$\approx 1ms$

Table 3.4. Average of execution times.

It is clear that the period necessary for group key generation and establishment is strongly related to the time required to perform all mathematical operations in addition of the number of cars involved in the process. In this case, we add to the total time all the computation time necessary for these basic operations. For example, if we consider 3 vehicles we need to generate a prime number p, 3 random numbers (a, b and c) and 9 modular exponentiation. And a fourth vehicle join the platoon we need to generate 2 random numbers (c', and d) and 11 modular exponentiation. We summarize in Table 3.4, the measured times for the elementary executed operations such as the modular exponentiation, the large number random generation and the large number native multiplication.

We plot in Figure 3.8 the average of the total times needed for the platoon members to generate and exchange the group Key K_G. As we can see, increase the vehicle speed increases only slightly the time required for establishing and sharing the key. However, when we increase the number of involved vehicles the delay is more significantly increased. This is justified by the fact that delay depends mainly on the computation capacities of the *OBU* (On-Board Unit) and the number of basic operations needed to the computation time for key generation. Only a small portion of that period is due to the communications environment and to the high mobility of nodes. As mentioned before, and to the best of our knowledge, there are no previous existent similar work for VANETs (high mobility) which simulate the generation of a group Key based on the *GDH* algorithm and using a fortification method against the Man in the middle attack. Given this lack, we have not compared our work to other existing ones. Thus, we hope that our obtained results may serve as comparison basis for eventual future studies.

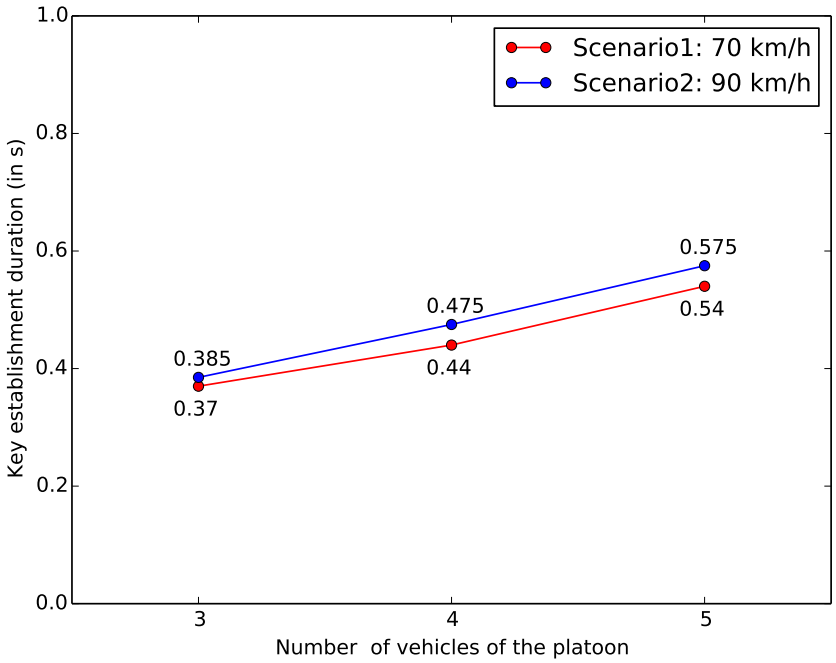


Figure 3.8. Average of the Group key establishment duration for two scenarios.

3.6 Conclusion

In the first part of this chapter, and after proofing the capacities of cryptographic tools to solve or mitigate a large number of existing attacks and vulnerabilities in VANETs, we regroup, study and compare the various cryptographic solutions that have been separately proposed for these attacks and evaluate their efficiency.

In the second part, we detailed our contribution related to a wide number of security problems in VANETs, which can be solved by the generation and the use of secure cryptographic keys to encrypt or authenticate private VANET communications. We have proposed and enhanced the Group Diffie-Hellman algorithm *GDH* for group key generation in VANETs. This proposal allows securing group communications especially between the members of a platoon of vehicles. We have also fortified our proposal against the famous Man in the Middle attack by calculating the final group key as an *XOR* bitwise between the initial calculated group key and a pre-shared secret only known by the group members. The actual proposed solution is dedicated to a small number of participants. thus, it will be very useful to study its extension for a large group using an appropriate clustering

scheme.

However, in addition to cryptographic solutions, which are specifically dedicated for securing the application level, we thought, to secure VANETs against attacks targeting both the physical and MAC layers. For this, it is first necessary to detect these attacks, which is the subject of our next contribution.

⁂ ⁂ ⁂ ⁂ ⁂

CHAPTER 4

LINEAR REGRESSION AND FUZZY LOGIC BASED DETECTION SCHEME

Contents

In this chapter we detailed our second contribution and the first one related to the detection of DoS attack in VANETs. We focus especially on the greedy behavior which has been well studied for Wireless LAN (WLAN) and for Mobile Ad hoc Networks (MANETs). However, this attack is less studied for VANETs. Indeed, the detection of a greedy behavior is much more difficult for high mobility networks such as VANETs. Thus, we propose our Greedy Detection for VANETs (GDVAN)*: a new detection algorithm for greedy behavior attacks. Our method is roughly divided into suspicion and decision phases. The suspicion phase is based on linear regression mathematical concept while decision phase is based on a fuzzy logic decision scheme. The proposed algorithm distinguishes the existence or not of a greedy behavior and suspects the compromised nodes using three new defined appropriate metrics. In addition to be passive, it can be executed by any node of the network and does not require any modification of the IEEE 802.11p standard.*

4.1 Introduction

Intelligent Transportation Systems (ITSs) are being developed in order to provide innovative and distributed services ranging from the broadcast of traffic data to the transmission of infotainment data. Due to the criticality of an important proportion of the services offered through VANET architectures, real-time is becoming one of the major concerns in vehicular communication systems. In fact, the VANET may not guarantee timely detection of dangerous road conditions or maintain communication connectivity when the network density is low (e.g., in rural highways). This may introduce substantial and important threats to the safety of the driver and the passengers. More specifically, some applications require real-time information about the speed and the position of vehicles in order to predict dangerous situations before they occur, and warn drivers accordingly while some other applications require more accurate data, such as multimedia streams. Therefore, considering the modeling, engineering, and security aspects in the roadside components of VANETs turns out to be a must.

VANETs is an important use case of mobile networks in ad hoc mode. In this type of architecture, nodes connect automatically without the need of a preexisting infrastructure. Compared to MANETs, VANETs present many other constraints such as the high mobility of nodes, the network topology changing and the short times of connection. These

constraints require that different types of conventional attacks to which they are exposed ad hoc mobile networks are valid for VANET, but the behavior of VANETs against these attacks is not the same.

As proposed in [23, 74], attacks and vulnerabilities against VANETs can be classified into attacks on availability, integrity and data trust, authenticity, confidentiality and non repudiation. Attacks on availability are mainly formed by DoS attacks family [8, 5]. These attacks have catastrophic effects since they can lead to the partial or total loss of vital information. Their impact is generally measured by the proportion of the needed time to recover the VANET system to its normal status. DOS attacks can be achieved by external or internal malicious nodes to the network [8]. Generally, the attacker aims to interrupt services for legitimate users. Thus, these services will be more available to him. In other cases, the purpose of conducting a DOS attack is just a challenge. Avoiding DOS attacks is a critical security requirement for VANETs, whose main objective is to ensure the live of drivers and road users.

Multiple techniques can be used by malicious users/drivers to make the VANET experience service interruptions. In this study, we focus on greedy behavior which is a common DoS attack. It targets the operation of the MAC layer and exploits the weaknesses of the medium access method. A greedy node aims to minimize its waiting time for a faster access to the channel and therefore penalize the other honest nodes [59]. Then, it does not respect restrictions of the channel access method and tries always to connect to the medium and maintains it for its own use. The major problem of such attacks is that they can be performed by an authenticated user which makes the detection more complicated.

The achievement of a greedy behavior in VANETs exploits the weakness of the MAC layer. There are several techniques to carry out this attack such as backoff manipulation, Request To Send (RTS) and Clear To Send (CTS) frames scrambling, oversized Network Allocation Vector (NAV) and DATA frames manipulation, etc. Due to the high mobility of VANETs and also to the short connection duration times, the manipulation of the backoff mechanism is proved as the best technique to use [94]. It allows the attacker to reduce considerably his waiting time [5]. Therefore, it is necessary to overview, in what follows, the IEEE 802.p standard and how it can be exploited to perform a greedy denial of service attack.

The MAC layer of IEEE 802.11p [27] uses EDCA (Enhanced Distributed Channel Access), which is an improvement of the former distributed coordination function DCF (Distributed Coordination Function) used in most of the standard IEEE Std 802.11[30]. To ensure more likely to highly relevant safety messages, so they can be transmitted within a reasonable time in a VANET, the EDCA introduces in [95] the concept of management of QoS through the notion of access categories (AC: Access category). Four categories are defined according to the type of traffic: Background traffic (or AC0 BK), Best Effort traffic (BE or AC1), Video traffic (VI or AC2) and Voice traffic (VO or AC3). AC3 is considered with the highest priority.

EDCA uses CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) method as access channel method. In EDCA [96, 4], if a node is ready to transmit, it senses the medium. If the latter is free during an $AIFS$ (Arbitration Inter-Frame Space) period, the node must defer transmission by selecting a random backoff time. The EDCA 802.11p backoff procedure works as follows:

(i) The node that wants to transmit selects a backoff value uniformly distributed in the interval $[0, CW]$, where the initial value of CW(contention window) is equal to CW_{min},

(ii) The value of CW increases (double + 1), if the transmission attempt fails, until the CW reaches CW_{max} value, the maximum number of retry attempts is set to 7 (Table 4.1),

(iii) The backoff value will be reduced when the channel is idle,

(iv) If the value of backoff reaches 0, the node will send immediately.

The waiting time $AIFS_k$ for a category of access k is calculated as follows:

$$AIFS_k = SIFS + AIFSN_k * t_{slot}$$

where $t_{slot} = 13\mu s$ represent the time slot and $SIFS = 32\mu s$ represent the Short Inter Frame Space for IEEE 802.11p PHY OFDM ($10MHz$) as defined in [27].

Different $AIFSN$ (Arbitration Inter-Frame Space Number) and CW values are selected for different types of access ACs for each use case with the CCH and SCH, respectively Control and services channels. Table 4.2 presents all of these values, which are calculated with the formulas given in [97]. It is easy to understand now that a greedy node can greatly increase its chances of access to the channel by reducing its backoff time. This is done by manipulating the CW_{max}, CW_{min} and $AIFSN$ values. There are other techniques to achieve a greedy behavior, but in a high mobility environment, manipulation of backoff parameters remains feasible but more difficult to detect.

It should be noted that in the literature, and in several studies [31, 96, 4], there is a confusion about the value of CW_{max}. As based on the IEEE 802.11p and for the OFDM PHY layer with $10MHz$, the value of CW_{max} is 1023. While the IEEE 1609.4 specification standard [95] indicated that the value of CW_{max} to use is 511.

Obviously, handling backoff parameters allows easily a greedy attack. A malicious node can, for example, choose a low value of backoff instead of random one. It can even choose zero and increases considerably its chances to access to the medium. To detect this kind of attack, we have developed an algorithm based on *linear regression* concept [98] for the suspicion phase and on a *watchdog supervision software* using *fuzzy logic* design for the decision phase. The proposed algorithm is able to suspect a greedy behavior in VANET and suspect the responsible nodes.

The rest of the chapter is organized as follows. Section 2 runs through literature review. Our detection algorithm is described in Section 3. Section 4 presents the simulation environment and the the simulations for each phase. Section 5 discuses the obtained results. Finally, Section 6 concludes the chapter and gives directions for future work.

Retry	**BK**	**BE**	**VI**	**VO**
0	15	7	3	3
1	31	15	7	7
2	63	15	7	7
3	127	15	7	7
4	255	15	7	7
5	511	15	7	7
6	511	15	7	7
7	511	15	7	7

Table 4.1. Contention Windows values used for CCH [95]

	CCH			SCH		
AC	CW_{min}	CW_{max}	AIFSN	CW_{min}	CW_{max}	AIFSN
BK	15	511	9	15	511	7
BE	7	15	6	15	511	3
VI	3	7	3	7	15	2
VO	3	7	2	3	7	2

Table 4.2. EDCA parameters set used on CCH and SCH WAVE channels

4.2 Literature review

The problem addressed by this contribution is related to several research axis such as DoS attacks, Medium Access Control (MAC) layer misbehavior, appropriate detection metrics, fuzzy logic design, ad hoc networks and also greedy behavior attack especially for VANETs characterized by their high mobility and the short connection durations of nodes. To the best of our knowledge there are no actual work for MAC greedy behavior detection in Vehicular Ad hoc Networks based IEEE 802.11p protocol. Most of the developed works are specifically related to MANETs based on IEEE 802.11 protocol and not on 802.11p, whereas many solutions have been proposed for MAC greedy behavior in wireless networks, for MANETs and Wireless Mesh Networks (WMNs). The proposed solutions can be classified into three families:

- New MAC design based solutions (backoff algorithm modification): for this category, a new MAC layer is proposed to avoid backoff algorithm weakness against greedy attacks. Examples of this category can be found in [99] and [100].

- Monitoring-based solutions: an additional component is added to detect greedy nodes, without any modification of the MAC layer. The proposed solution in [59] is an example of this category.

- Game theory-based solutions: in this category, honest and malicious nodes are supposed adversaries in a fictitious game. Detection and reaction solutions against attacks are based on game theory. Examples of this category can be found in [101] and [102].

Raya et al. proposed in [94] a greedy behavior detection scheme called DOMINO, for infrastructured networks (IEEE 802.11 hotspots). DOMINO is a software system for detection of greedy behavior in IEEE 802.11 MAC layer for public networks. It is to be installed in the Access Point (AP), it can identify and detect greedy stations, without

any required modification of the standard protocol at the AP. It has the advantage to be transparent to network users. Given the lack of mobility, DOMINO can detect many kinds of manipulation techniques, such as the reduction of backoff time, CTS and ACK delay and increase the NAV (Network Allocation Vector) time.

Buchegger et al. [103] have studied several misbehavior detection and reputation systems that have been proposed for mobile ad-hoc networks and based on direct observation mechanisms of the network behavior so-called watchdogs. They have been interested in the capabilities of the watchdog detection component in a real network and they presented their test-bed implementation of misbehavior detection.

Buchegger also with Le Boudec proposed CONFIDANT [104]: a protocol called CONFIDANT for mobile ad hoc networks (MANETs) which is based on selective altruism and utilitarianism. It detects and isolates misbehaving nodes which refuse to cooperate with the other honest nodes of the network. CONFIDENT built routing decisions and trust relationships based on observation, experience, and reports on behavior of the other cooperate nodes. The proposed system can detect several types of attacks and thus honest nodes have the possibility to isolate misbehaved one from the network. Decisions are based on a reputation system. In fact, nodes have reputation records for first-hand and trusted second-hand observations.

Hamieh et al. [59], used the linear regression mathematical concept to detect MAC greedy nodes in an IEEE 802.11 based-protocol network (MANET). This method is based on the observation that successive access times of nodes are highly correlated. It was possible to represent the behavior of nodes in a network linearly. The calculated slope of the linear regression straight is used to assess the presence or absence of a greedy behavior. This proposition does not require any modification of the MAC layer of the protocol IEEE 802.11. In our algorithm, we have adopted a similar concept to distinguish between a normal VANET and a VANET under attack.

FLSAC (Fuzzy Logic based Scheme to Struggle Against Adaptative Cheaters) has been proposed Djahel et al [105]. FLASAC is an Enhancement of DOMINO scheme [94] but adapted to wireless mesh networks (WMNs). FLSAC focus the detection of greedy behaving or selfish nodes which aim to violate the proper use of the CSMA/CA protocol rules in

order to increase their bandwidth at the expense of the well-behaving nodes. The proposed scheme can be implemented in such gateways or Mesh Routers to supervise attached wireless nodes behavior and also report any deviation from the proper use of the MAC protocol.

As already mentioned, there are no greedy behavior detection scheme for VANETs and this lack is our essential motivation to perform the present contribution. Basically, we propose a new detection algorithm which distinguishes the presence of a greedy behavior and suspects the compromised nodes using as input a short periodic traffic traces. The design and the functional description of the proposed algorithm, which is roughly divided into respectively *suspicion* and *decision* phases, are detailed in what follows.

4.3 Proposed detection algorithm: *GDVAN*(Greedy Detection for VANETs)

4.3.1 Algorithm overview

The main goal of our algorithm introduced in [106] and shown in Fig. 4.1, is to supervise the VANET. If a greedy behavior is suspected, the watchdog software determines the responsible nodes using three newly defined metrics. We define these metrics to be suitable to greedy behavior in VANETs and after a depth study of the 802.11p MAC layer. In fact, according to several studies related to MANETs (Mobile Ad hoc Networks) [94] and [59], the metrics packet delivery ratio, queue length, throughput and backoff supervision can be used. However, these metrics are only efficient in the case of infrastructured or low mobile networks. For VANETs, and especially due to the high mobility of nodes and their short periods of connection, we have proven by simulation in [106] that it is not practical to use the mentioned metrics. We have chosen to supervise:

- *The number of connection attempts*,
- *The average node of connection duration*,
- *The average of waiting times between connections*.

In fact, a VANET greedy node has not enough time to perform adaptive manipulation of backoff parameters. It tries to connect to the network more often than honest nodes, also it maintains the medium much more time for its own profit and of course it has to reduce its waiting time between connections. In this context, a connection means the necessary

time for a node to achieve its transmission and another node can transmit.

Thus, our main contribution is the design of *GDVAN*: a new greedy behavior detection algorithm for VANETs. *GDVAN* combines and enhances both linear regression and watchdog concepts to be suitable for VANETs. These two techniques have been used separately only for MANETs. Due to the high mobility in VANETs, we proved later that linear regression method is not totally suitable for VANETs. It can be only used for the distinction between a normal network behavior and a network under attack (suspicion phase). In *GDVAN*, the decision scheme uses the strength of design tools provided by the fuzzy logic theory to determine if a node is either greedy or it is honest. This way decreases the rates of both false positive and false negative. We detail in what follows the various components and the operation mode of respectively the suspicion and decision phases.

4.3.2 GDVAN suspicion phase

In a VANET, the nodes of the same Wave Independent Basic Service Set (WIBSS) share access to the transmission medium with respect to CSMA/CA access method managed by the MAC layer protocol which guaranteed a fairness access to all connected nodes. It was observed in [59] that for MANET, the access times of active nodes are highly correlated. In a normal behavior of the network (without greedy nodes), if the node N_i connects to the support, the node N_{i+1} has to wait and cannot connect until N_i ends its transmission. Statistically, the nodes have almost the same average connection time. Thus, the connection time of the node N_{i+1} linearly depends on connection time of the node N_i. The presence of one or more greedy nodes in the network violates this important access regulation rule.

To mathematically model the problem, we denote by t_i the connection time of the node N_i, and by t_{i+1} the connection time of the node N_{i+1}, that connects to the media just after N_i. We also denote by $\{ x_i \}$ the set of values taken by t_i and $\{ y_i \}$ the set of values taken by t_{i+1}.

The calculation of correlation coefficient is used to determine the dependence degree between the times of nodes connection. Statistically, this coefficient measures the dependence between two random variables [98]. In our case, we compute this coefficient for two random variables X and Y taking their values respectively in $\{ x_i \}$ and $\{ y_i \}$. The correlation coefficient takes values in the interval $[-1, 1]$. The values -1 and 1 indicate a strong

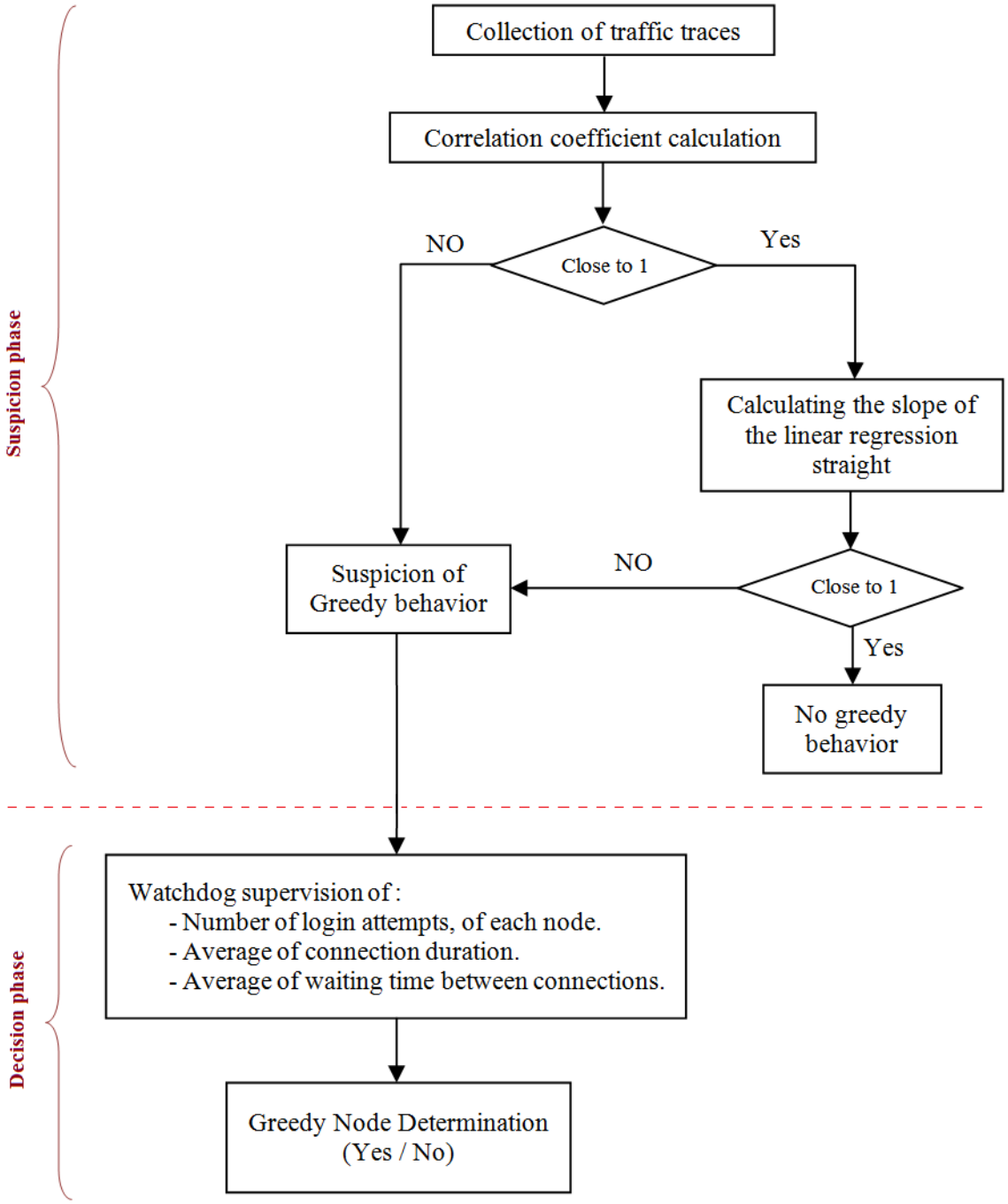


Figure 4.1. The proposed detection algorithm.

correlation, thus more we move away from these two values more the dependency decreases. For MANET, it has been proved in [59] that in the case of existence of strong correlation, the relationship between the connection times can be expressed in a linear way for both normal or greedy behavior. However, the correlation coefficient is always close to 1. Also, the slope of the estimated linear regression straight is close to 1 for a normal network and more greater in the case of greedy behavior. Thus, calculating the slope of the estimated linear regression straight can determine whether or not the existence of a greedy behavior. Contrary for VANETs, we confirm the previous result only in the absence of greedy attack. Otherwise, this technique is no longer valid and the relationship between the connection times is rather random. In fact, due to their high mobility and short connection times, VANET greedy nodes have to access rapidly to support and maintain it as long as possible for their own use. Thus, connection times are never more correlated contrary to the case of MANETs. To solve this problem we have introduced the watchdog technique to monitor our newly defined metrics in order to report possible greedy attacks.

Thus, the *GDVAN* suspicion phase works as detailed in Algorithm 2:

As we need to compute the correlation coefficient in *GDVAN*, the method is detailed bellow.

4.3.2.1 Correlation coefficient

The correlation coefficient ρ measures statistical relationships between two random variables or observed data values [98]. It is defined as the covariance of the variables X and Y divided by the product of their standard deviations (cf. 4.1).

$$\rho = \frac{Cov(X,Y)}{\sigma_x \sigma_y} \qquad \rho \in [-1,1] \tag{4.1}$$

To calculate ρ, and by definition, it is assumed that the values taken by connection times are random. Statistically, we define the two random variables X and Y as follows: If a node connects to the network at time t_n the next connects to time t_{n+1}. Thus X takes values in the set $\{ x_i \}$ of the connection times t_i of any network node, while Y in the set $\{ y_i \}$ of the connection times t_{i+1}. In the case of presence of correlation, the variables x_i and y_i represent respectively t_i and t_{i+1}, which can be connected by a linear relationship. Therefore we have : $t_{i+1} = at_i + b$. The application of the method of linear regression can approach the values of the slope a, and b.

Algorithm 2: Suspicion phase

INPUT : T : Monitoring period, State_Greedy = FALSE.
OUTPUT: Annonce_Greedy(State_Greedy)

begin
  repeat
    1) Collect traffic traces during T,
    2) Calculate the correlation coefficient ρ
    if ρ *is close to* 1 **then**
      goto (3);
    else
      goto (4);
    end
    3) Calculate the slope of the linear regression straight,
    if *the slope is close to* 1 **then**
      State_Greedy = FALSE;
    else
      run (4);
    end
    4) A greedy behavior is suspected: Return and run the watchdog supervision tool.
    Return; Annonce_Greedy(State_Greedy)
  until *No existing communication*;
end

If the calculated correlation coefficient is close 1, we need to calculate the slope $'a'$ of the linear regression straight. An overview on the mathematical foundations and the method of calculating the linear regression parameters are detailed in the following.

4.3.2.2 The linear regression concept

The linear regression mathematical concept is a statistical method for finding functional linear relationship between two random variables X and Y. This functional relationship is a linear function of approximation.

Provided when X is given, Y is not completely determined. Y takes values around a certain average one. When X varies, the values of Y describe a curve called the regression straight of Y with respect to X. Mathematically, the desired function is $f(x) = E(Y/X = x)$.

Therefore, we have samples of n pairs of observations (x_i, y_i) that can be represented on a graph in the plane, where each point i, which is a couple of observations with x_i on the x-axis and y_i on the y-axis. In practice, the samples formed a cloud of points (Fig.4.2). We looked for a straight line $y^* = ax + b$, which describes well the trend of the observed cloud. We have: $y_i = ax_i + b + e_i$, where e_i is the error approximation called residues (Fig.4.3), e_i is added to the value $y_i^* = ax_i + b$.

For a better approximation of the straight line $y* = ax + b$, we use the least squares method, that consists to minimize the sum of square residuals e_i:

$$S = \sum_{i=1}^{n} e_i^2 = \sum_{i=1}^{n} (y_i - ax_i - b)^2 \tag{4.2}$$

S is minimal if the partials derivatives with respect to a and b are zero:

$$\frac{\partial S}{\partial a} = -2 \sum_{i=1}^{n} x_i (y_i - ax_i - b) = -2 \sum_{i=1}^{n} x_i e_i = 0 \tag{4.3}$$

$$\frac{\partial S}{\partial b} = -2 \sum_{i=1}^{n} (y_i - ax_i - b) = -2 \sum_{i=1}^{n} e_i = 0 \tag{4.4}$$

The processing of equations 4.3 and 4.4, is used to calculate the values of a and b. In our algorithm, we are just interested in the calculation of the slope:

$$a = \frac{Cov(X, Y)}{Var(X)} \tag{4.5}$$

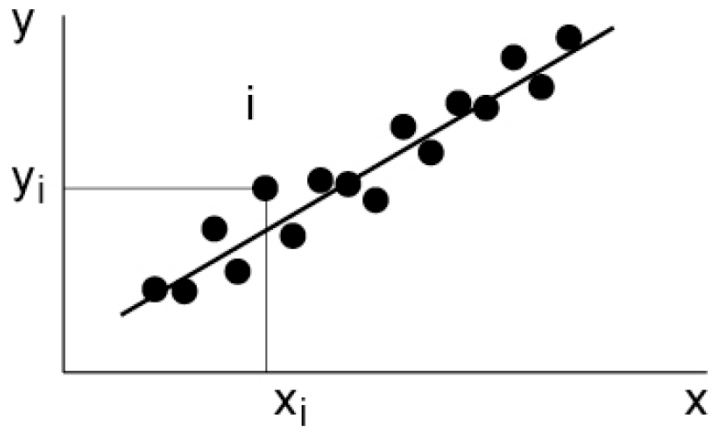


Figure 4.2. Cloud of linear regression points.

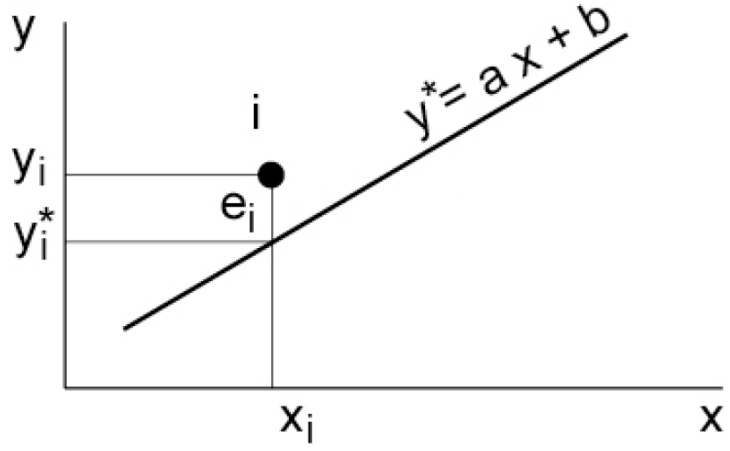


Figure 4.3. Approximated linear regression straight.

Whenever the calculated correlation coefficient or the slope of the linear regression straight is not close to 1 (with appropriate authorized slight deviation), we run the watchdog monitoring tool based on fuzzy logic decision scheme, which functioning is described below.

4.3.2.3 Watchdog supervision tool

In a network security context, and as defined in [103], watchdogs mean several misbehavior detection and reputation systems that have been proposed for mobile ad-hoc networks, relying on direct network observation mechanisms. In our case, we supervise the greedy behavior in a VANET network. For this behavior, nodes do not respect MAC layer access method requirements by manipulating several parameters such as CW_{min}, CW_{max}, $AIFSN$ etc. Using these manipulations, an attacker is able to increase his chances of access to the support and penalize the other nodes.

In *GDVAN*, we suspect the existence of a greedy behavior in the two following cases:

1. The correlation coefficient is not close to 1.
2. The correlation coefficient is close to 1 and the slope of the linear regression straight is not close to 1.

VANETs are characterized by high mobility and relatively short connection times compared to ordinary ad hoc networks. Thus, the most effective way for a greedy behavior attacker is to disregard the backoff time and quickly try to connect before the other nodes.

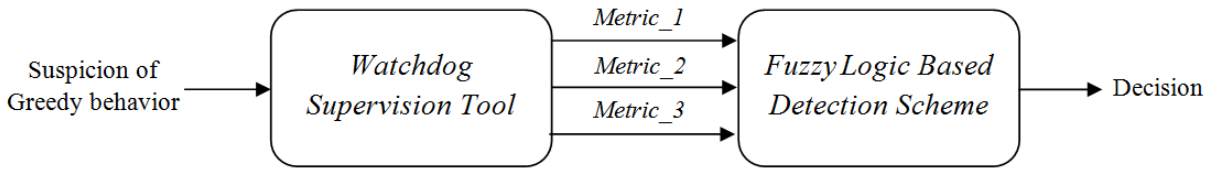


Figure 4.4. Fuzzy logic based decision scheme

In addition, a greedy node tries to establish a high number of connections, with an occupation time of the support higher than a normal node. Thus, our software monitors the following parameters:

1. The duration between two successive transmissions: The waiting time of a greedy node is almost close to zero.
2. Transmission time: a greedy node occupies the medium more than other normal nodes.
3. Connection attempts number of a node: a greedy node tries much more than the other nodes to connect to the network.

Other parameters can be monitored, but for a high efficiency, rapidity and in order to simplify the watchdog supervision tool, we have only maintained these parameters. Once a suspicious behavior of a node has been suspected, we need to decide if it is a real one or not: this is the goal of the *decision phase*.

4.3.3 GDVAN decision phase

For decision making systems, where the membership of an element (node in our case) to a class (honest or greedy) remains proportional, fuzzy logic can be an efficient tool for design. In this contribution, we propose a new decision scheme for detecting greedy behavior suitable for VANETs. This scheme detects nodes which aim to violate the proper use of the CSMA/CA protocol rules in order to increase their bandwidth at the expense of the well-behaving nodes. As shown in Fig. 4.4, it used newly defined metrics which best convenient to highly mobile networks and can be used during short monitoring periods.

Design details are given in the following.

As already explained, in our watchdog detection software, we have to supervise the following 3 newly defined metrics for each node in the VANET:

- The number of connection attempts,

- The average of connection duration,

- The average of waiting times between connections.

From a fuzzy logic point of view, and for each parameter, we begin to suspect the existence of a greedy behavior from a certain value of the parameter (first threshold). Reaching a certain value of the parameter (second threshold) makes suspicion high enough. Between these two threshold values suspicion is gradual. So, our idea is based on the use of the tools provided by the fuzzy logic theory which help to solve this kind of problems.

Before detailing our scheme and the use of the three monitoring parameters, we introduce some basic facts about the fuzzy logic. It helps to understand some basics such as inputs, fuzzy sets, membership functions, inference and defuzzification (for more details refer to [107] and [108]).

4.3.3.1 Inputs, fuzzy sets and membership functions

As any system of data processing, our fuzzy logic-based scheme requires inputs to be processed to get results. We use the three inputs already described and supervised by the watchdog software after short collection periods. In a high mobility environment such as VANET, we have approved that these tree variables are the best appropriate for suspecting a greedy behavior, unlike other parameters used for MANET networks for example.

In the classical theory of sets, an element belongs or does not belong to a set. However, this basic concept does not satisfy some simple situations frequently encountered. By contrast, fuzzy set theory permits the gradual assessment of the membership of elements in a set. In this theory, each element belongs partially and gradually to defined fuzzy sets. The contours of each fuzzy set are not "net", but "fuzzy" or "gradual". This can be described with membership function which takes values in the interval $[0, 1]$, while the indicator of classical function sets takes only 0 or 1. The fuzzy set theory is widely used in a domain

where information is incomplete or imprecise.

The designer of a fuzzy logic based system has to clearly define his fuzzy sets. A fuzzy set is defined by its "membership function", which corresponds to the notion of "characteristic function" in classical logic theory.

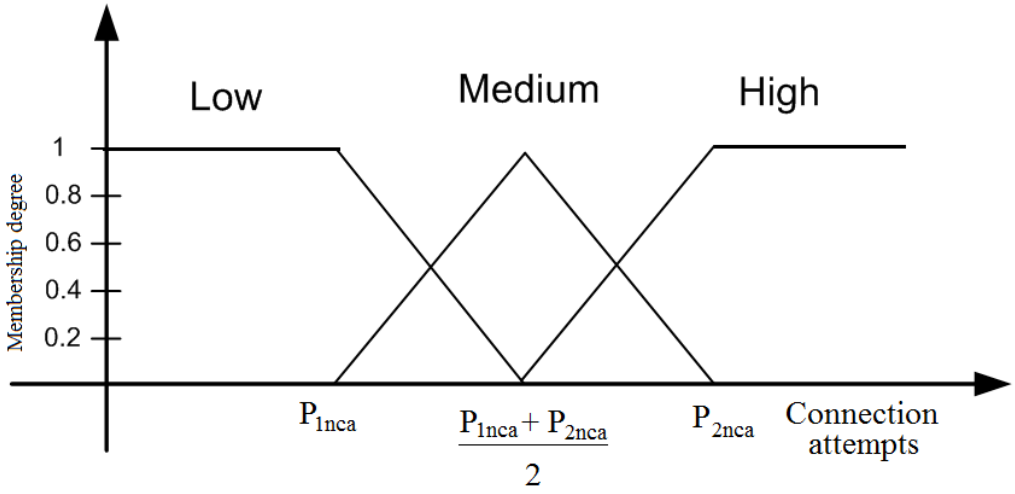


Figure 4.5. Membership function of the number of connection attempts parameter.

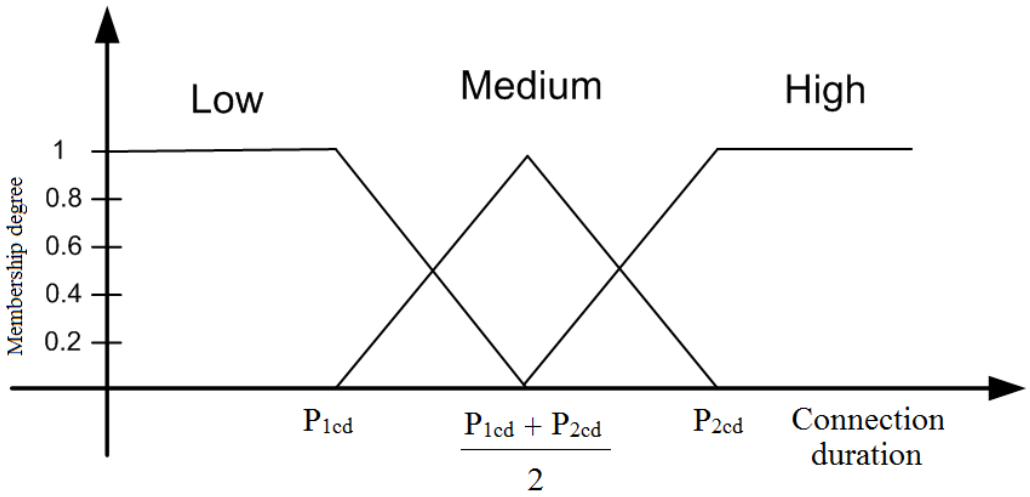


Figure 4.6. Membership function of connection durations parameter.

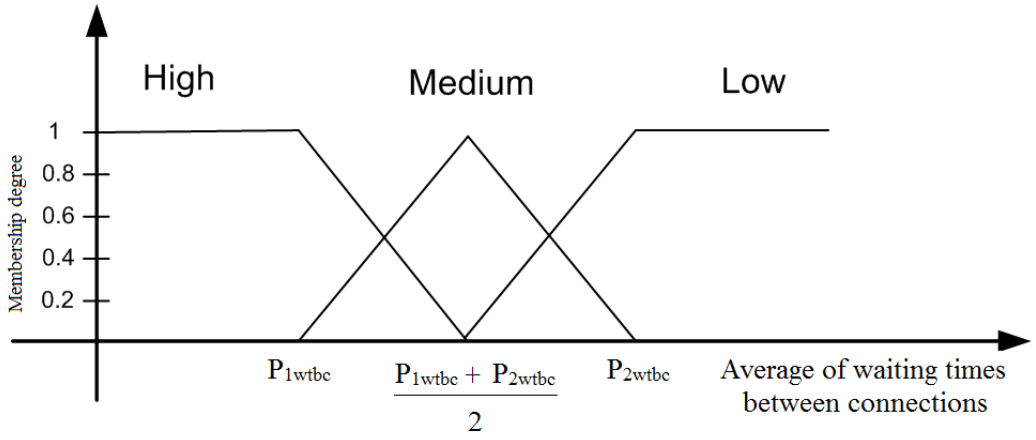


Figure 4.7. Membership function of average of waiting times between connections parameter.

4.3.3.2 Fuzzification and membership degree

Fuzzification step or the determination of the degree of membership, is used to switch from real to fuzzy domain. It consists in determining the degree of membership of a input value (measured for example) to a fuzzy set. In our system, for each value of an input variable, we define its membership to one of the following chosen fuzzy sets "Low", "$Medium$" and "$High$", respectively denoted by L, M and H.

Mathematically, a fuzzy set S of an universe U, can be defined by the membership function [109]:

$$M_S : U \longrightarrow [0, 1]$$

The degree of membership to the fuzzy set S is given by $M_S(e)$, for each element e of U. For our fuzzy scheme design, we choose the use of the trapezoidal method [108] for membership functions which is often used in such cases and is well appropriate for our conception, given that we use the three fuzzy sets "Low", "$Medium$" and "$High$". Our designed membership functions are given in Figures. 4.5, 4.6 and 4.7.

Parameter	Description
T	Monitoring period
N	Total number of vehicles. (we suppose that it is constant during the monitoring period).
T_{CA}	Number of total connections attempts during T.
T_{CD}	Total connections duration of all vehicles during T.
P_{1nca}	Threshold of connection attempts from which we begin to suspect greedy behavior.
P_{2nca}	Threshold of connection attempts from which we have a high suspected greedy behavior.
P_{1cd}	Threshold of connection duration from which we begin to suspect greedy behavior.
P_{2cd}	Threshold of connection duration from which we have a high suspected greedy behavior.
P_{1wtbc}	Threshold of waiting times between connections average from which we begin to suspect greedy behavior.
P_{2wtbc}	Threshold of waiting times between connections average from which have no suspected greedy behavior.
V_1	Number of connections attempts.
V_2	Connection duration.
V_3	Average of waiting times between connections.

Table 4.3. Description of the model parameters.

Furthermore, we need to define the parameters mentioned in Table 4.3 and used especially to specify the first and the second threshold for each supervised metric. More precisely, these parameters are defined as follows:

- $P_{1nca} = \frac{T_{CA}}{N}$: is the threshold from which we begin to suspect greedy behavior. If the number of connection attempts of a controlled node exceeds the the average $\frac{T_{CA}}{N}$ then the node is suspected.
- $P_{2nca} = 0.7T_{CA}$: is the threshold from which we classify the controlled node as greedy. We determine statistically in our simulations that if a node reaches 70% of the total number of connections, then it is suspected as greedy.
- $P_{1cd} = \frac{T_{CD}}{N}$: is the threshold from which we begin to suspect greedy behavior. If the average of the total connections duration of a controlled node exceeds the total average of all nodes $\frac{T_{CD}}{N}$ then the node is suspected.
- $P_{2cd} = 0.6T_{CD}$: is the threshold from which we classify the controlled node as greedy. We determined statistically in our simulations that if a node reaches 60% of the total duration of connections, then it is suspected greedy.
- $P_{1wtbc} = min(AIFS_K)$: if the average of waiting times between connections of a controlled node is lower than $AIFS_K$ threshold, the node is greedy.

- $P_{2wtbc} = max(AIFS_K + CW_{max}.t_{slot})$: If the average of waiting times between connections of a controlled node reaches the maximum allowed waiting period for IEEE 802.11p which equal to $max(AIFS_K + CW_{max}.t_{slot})$, then the node is not suspected greedy.

4.3.3.3 Decision rules

In this step, we define the decision rules, what will determine the system outputs. A fuzzy rule allows to connect the inputs with the outputs. By the established rules, we classify the behavior of vehicles in one of the three classes: *Normal*, *Suspected* and *Greedy* respectively denoted by N, S and G.

The rules are formulated using the algorithmic formalism: *IF*(*condition*), *THEN*(*conclusion*). The condition part uses the membership of each input to a fuzzy set, and the conclusion part is the desired classification of vehicle behavior.

To compute the truth value of a condition (called also a predicate), of the form C is S, the membership function is used and the truth degree T_d of an attribute e is given by $T_d = M_S(e)$.

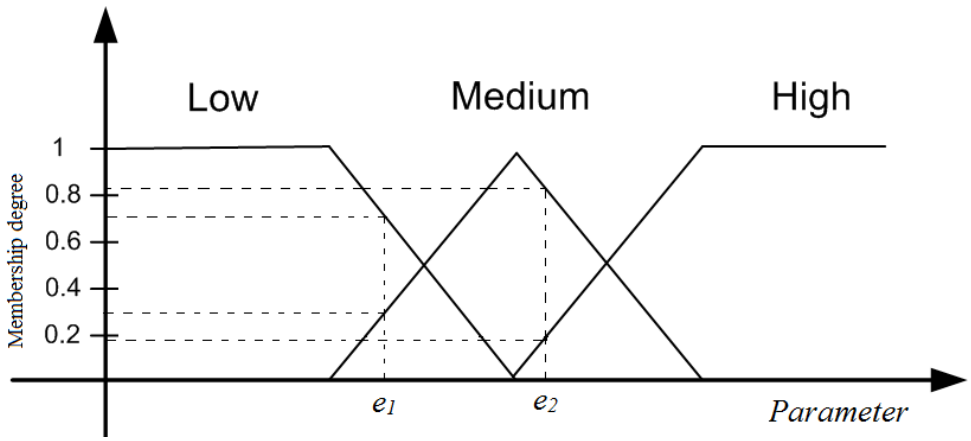


Figure 4.8. Membership function illustration example.

To better illustrate these concepts, we give the example shown in Fig. 4.8 which is similar to our membership functions (trapezoidal representation). The truth degrees of the values related to e_1 and e_2 are given in Table. 4.4. In this example, e_1 belongs to the class *Low* with a membership degree equal to 0.7 (70%), to the class *Medium* with a membership degree equal to 0.3 (30%) and to the class *High* with a membership degree equal to 0 (0%).

	L	M	H
e_1	0.7	0.3	0
e_2	0	0.81	0.19

Table 4.4. Degree of truth values of the illustration example

For two truth degrees T_{d1} and T_{d2}, Zadeh [107] has redefined the classical logical operators AND and OR to be suitable for fuzzy logic theory. Thus, the truth values can be calculated as following:

$$T_{d1} \ \ AND \ \ T_{d2} = min(T_{d1}, T_{d2})$$
$$T_{d1} \ \ OR \ \ T_{d2} = max(T_{d1}, T_{d2})$$

There are other definitions of AND and OR operators, but Zadeh definition [107] is the most widely used one. In our case, at the end of each monitoring period, the three variables V_1, V_2 and V_3 mentioned above, are selected for processing in order to define the final affiliation of a vehicle to one of the classes N, S and G. For each vehicle of the network, these variables are computed as follows:

$$CLASS = (V_1 \ AND \ V_2) \ OR \ V_3$$

This gives:

$$CLASS = \max[\min(V_1, V_2), V_3]$$

The following tables summarize our classification rules. Table.4.5 summarizes the fuzzy rules of the formula: $CLASS1 = min(V_1, V_2)$ and Table.4.6 summarizes the fuzzy rules of the final formula $CLASS = max(CLASS1, V_3)$.

	V_1 :	L	M	H
V_2				
L		N	N	S
M		N	S	S
H		S	G	G

Table 4.5. Fuzzy rules of CLASS1 formula

	CLASS1:	N	S	G
V_3				
L		N	S	G
M		N	S	G
H		S	G	G

Table 4.6. Fuzzy rules of CLASS formula

4.3.3.4 Defuzzification

At the end of the inference, the fuzzy outputs are determined, but they are not directly usable. It is necessary to move from "fuzzy world" to the "real world", it is the defuzzification step. Defuzzification is to provide an exact final value as a result of the end of treatment to help make a decision, this value is called Crisp value [108]. Several defuzzification techniques exist, the most used one is the method of center of gravity. With this method, the value of Crisp is calculated from the values of the area center of each fuzzy set. This value is given by the formula:

$$Crisp = \frac{\int cL(c)d_c}{\int L(c)d_c} \tag{4.6}$$

In the discrete domain, and in the case of our system the formula 4.6 can be written as :

$$Crisp = \frac{\sum_{i=1}^{3} c_i L(c_i)}{\sum_{i=1}^{3} L(c_i)} \tag{4.7}$$

where:

- c_i: is the center of the area corresponding to the class i of node behavior (we have 3 nodes behavior classes).

- $L(c_i)$: is the node behavior membership level to the class i.

The development of the formula 4.7 gives:

$$Crisp = \frac{c_N L(c_N)+c_S L(c_S)+c_G L(c_G)}{L(c_N)+L(c_S)+L(c_G)}$$

Thus algorithm 3 implement our rules for the decision phase. In what follows, we detailed the simulations steps for both suspicion and decision phases.

Algorithm 3: Decision phase

INPUT : T: Monitoring period;
File: Collected_Trafic_File;
State_Class $\in \{N, S, G\}$
OUTPUT: Annonce_Decision(V_ID, State_Class)

begin
  Extract Vehicle_IDs existing in File during the T period, N;
  Calculate: T_{CD}, P_{1cd}, P_{2cd}, P_{1wtbc}, P_{2wtbc};
  foreach *Vehicle* $\in$ {*Vehicle_IDs*} **do**
    Calculate: T_{CA}, P_{1nca}, P_{1nca};
    Calculate: V_1, V_2, V_3;
    Calculate: $Crisp$;
    if $Crisp > 50\%$ *for the class* G **then**
      V_ID is G
    else
      if $Crisp > 50\%$ *for the class* S **then**
        V_ID is S
      else
        V_ID is N
      end
    end
    Return: Annonce_Decision(V_ID, State_Class)
  end
end

4.4 Performance evaluation

4.4.1 Simulation environment and mobility model

To evaluate the performance of both *suspicion* and *decision* phases which form the proposed algorithm, we used the ns-3 [92] as network simulator and Simulation of Urban Mobility (SUMO) [93] as a mobility simulator. We simulate a VANET composed of 40 nodes. For a high level of real simulation, the selected traffic model is Constant Bit Rate (CBR). Any node of the network can transmit at any time at a constant rate, which is often the case in practice. The generated traffic is of type Wave Short Message Protocol (WSMP) and in accordance with the requirements of standards [110] and [95].

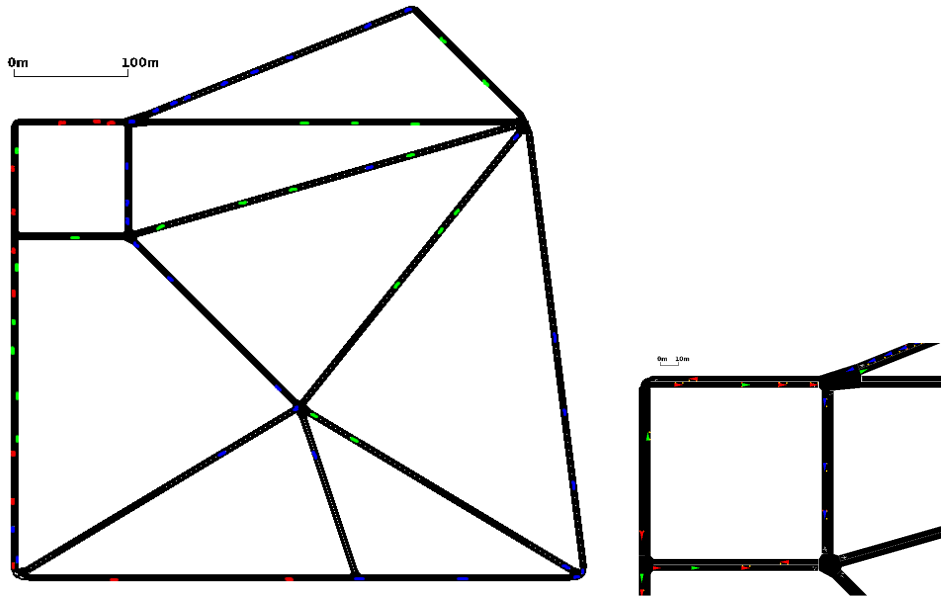
Parameter	Value
Environment	Dense urban
Network size	500m x 500 m
Node count	40
Average speed	36 Km/h ($\approx$ 10m/s)
Max speed	50 Km/h ($\approx$ 14m/s)
Execution time	From 10s to 40s
Sending capacity	6 Mbps
Packet size	Variable (max 1400 bytes)
Traffic model	CBR
Channel	CCH
Routing protocol	OLSR
Mobility simulator	SUMO
Traffic flow	40 $vehicles/s$
Traffic density	160 $vehicles/Km^2$
Correlation coefficient deviation	$\pm 10^{-4}$
Slope deviation	$\pm 10^{-1}$

Table 4.7. Simulation parameters.

The parameters of the simulation environment are described in Table 4.7. To ensure a maximum degree of efficiency of the statistical results we have repeated each simulation case about twenty times.

According to the several studies [111], [36] and [112] the mobility model chosen for the simulation of a VANET network plays an important role in the accuracy of results. To the best of our knowledge and according to [111], there are no current open source simulator which can be used simultaneously to simulate IEEE 802.11p protocol with a real mobility model (using real vehicle motion and road map). However, there are combining solutions of simulators such as proposed in [113], where a mobility simulator such as SUMO and a protocol network simulator can be used together. This kind of solutions presents in addition to the slow, the downside of the long procedure of data processing, which is no longer in real time.

To avoid this disadvantage and for each simulated scenario, we generate our mobility traces file using SUMO simulator and we use them directly with ns-3. Based on a real city map with signs and traffic lights designed for this purpose, shown in Figures 4.9 (a) and (b), the mobility files contained the coordinates and the speeds of all the nodes at each instant. This technique is used instead of the predefined mobility model of ns-3 originally designed for MANETs, it allow of course a real simulation environment. The traffic flow expressed in $vehicles/s$ [38], which define the rate of vehicles insertion into the network is



(a) (b)

Figure 4.9. (a) The map of the urban area of simulation, (b) Zoom on a part of the urban area of simulation.

fixed to 40 vehicles, that mean all vehicles exist allover the simulation. The traffic density expressed in $vehicles/Km^2$ is 160 which is a normal value for a dense urban environment.

4.4.2 Simulation of the suspicion phase

First we have simulated a normal behavior of network nodes in a dense urban environment. We confirmed the application of the linear regression method for the detection of normal behavior (absence of greedy nodes). Fig.4.10 shows the correspondent obtained straight. The choice of the correlation coefficient and slope deviations are fixed respectively to 10^{-4} and 10^{-1}. These parameters have been chosen based on statistical observations of the different simulations cases. We showed in Fig.4.11 that nodes had almost the same chance to access the media and the maximum connection duration for one node connection has not exceeded $6ms$.

Among the several techniques developed to achieve greedy behavior in the MAC layer, the manipulation of backoff parameters is known as having the best effect [94] particularly for VANETs characterized by short connection duration where nodes have not enough time to perform adaptive manipulation. Then, in a second step, we have simulated the

injection of respectively one, two, three and four greedy vehicles ($CW_{max} = CW_{min} = 0$). In fact, In a VANET and due to very short connection duration between nodes, it is not beneficial to perform a complicated attack. We suppose of course that normal nodes are majority, which is a realistic assumption. Contrary to the network normal behavior, we observed that the connection times are never more correlated, the correlation coefficient varies for all performed simulations in the interval $[-0.29; 0.29]$. The effects of the greedy nodes injection in the network and for all different simulated cases are shown in Table 4.8. The effects of greedy behavior on the total transmission time for the different simulated scenarios are shown in Table.4.8. Figures 4.12 and 4.13 respectively for one and two injected greedy nodes show that the connections duration of these nodes were very high. For example, one fully greedy vehicle uses approximately 66% of the total transmission time of the entire network, while four vehicles can reach together 75%. For these suspected nodes and according to our proposed algorithm 2, if a greedy behavior is suspected, the algorithm 3 must be performed to determine the accuracy of suspicion, and the nodes whom they are responsible.

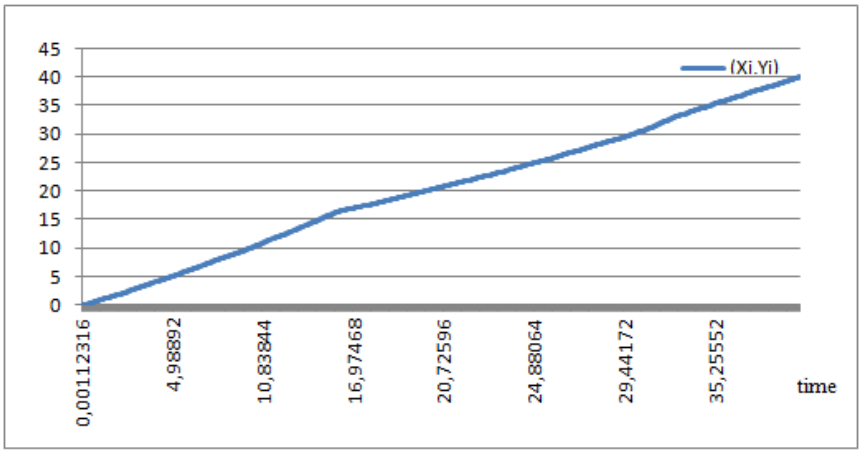


Figure 4.10. Linear regression straight of a normal behavior without greedy nodes.

Number of injected greedy nodes	Occupation percentage of the total transmission time
1	66%
2	69%
3	73%
4	75%

Table 4.8. Time occupation percentage and established connection number of greedy nodes.

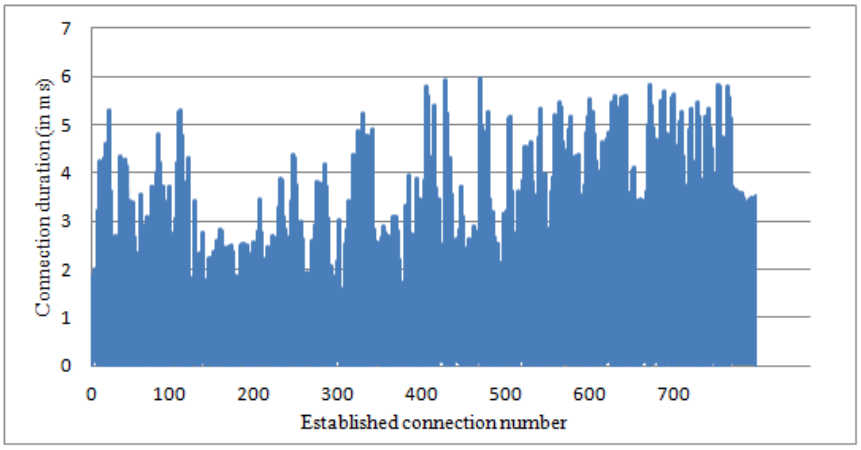


Figure 4.11. Connection durations in a normal network (without greedy nodes)

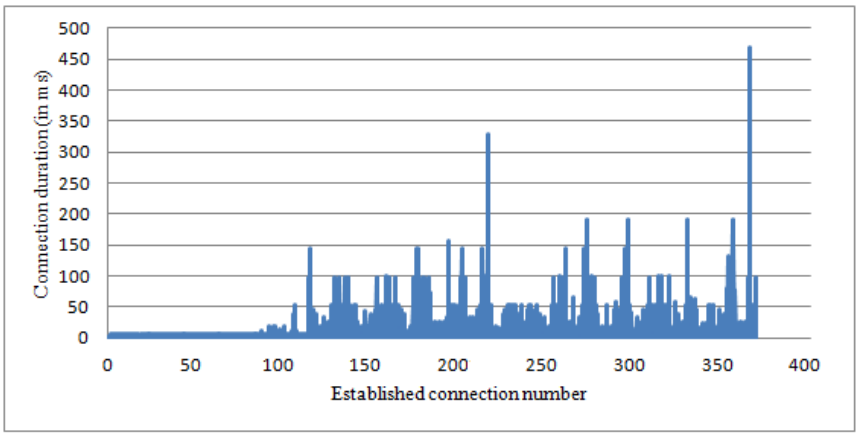


Figure 4.12. Connection durations in a VANET with one greedy node.

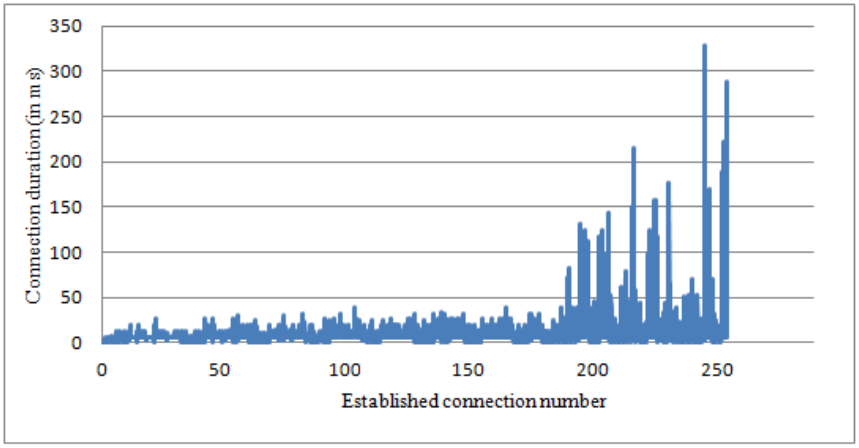


Figure 4.13. Connection durations in a VANET with two greedy nodes.

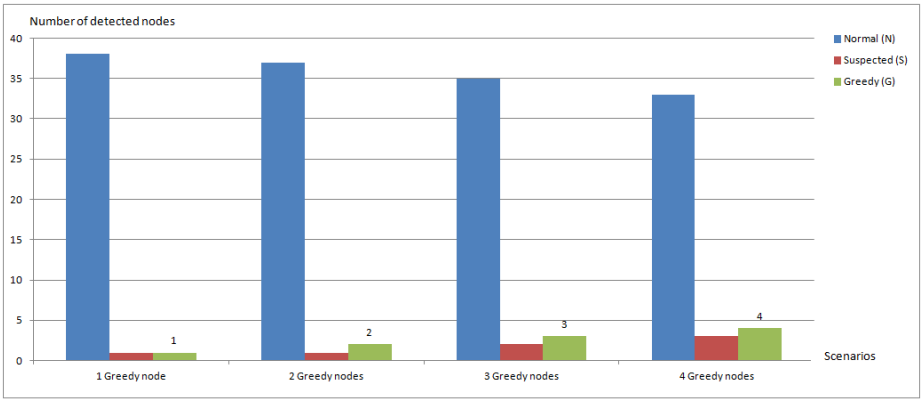


Figure 4.14. Detection results for the four scenarios.

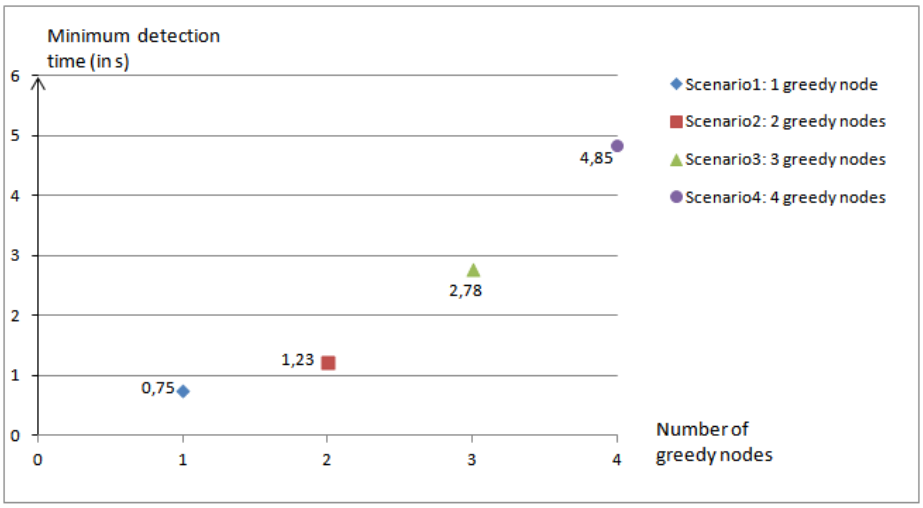


Figure 4.15. Minimum detection times for the four simulation scenarios with 40 vehicles.

4.4.3 Simulation of the decision phase

To evaluate the performance of the fuzzy logic based decision phase as detailed in the algorithm 3, we used also the same parameters and conditions as in the simulation of the suspicion phase. Using the collected traffic traces file and using our designed watchdog tool, which can be implemented in any network vehicle, we supervise the behavior of the other vehicles. Our fuzzy logic based decision scheme implementation is added to the watchdog tool and we supervised results for the effective injecting of respectively 1, 2, 3 and 4 greedy nodes. Simulation parameters are the same provided in Table 4.7. Obtained results are given and discussed in the following.

Our fuzzy logic based decision scheme for greedy behavior provided results as a percentage of belonging of a node to one of the Normal (N), Suspected (S) and Greedy (G) classes.

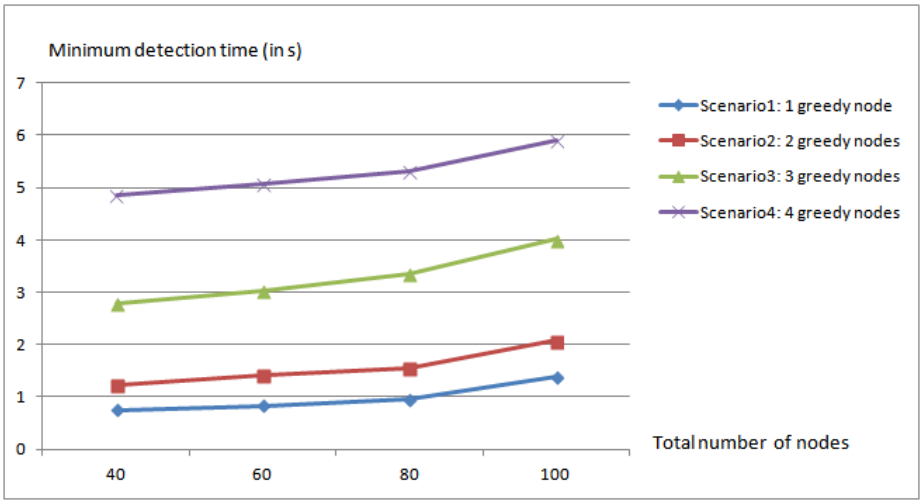


Figure 4.16. Minimum detection times for the four simulation scenarios with 40, 60, 80 and 100 vehicles.

In all performed simulations, the greedy nodes belong to the class G with a percentage greater than 95%. Fig. 4.14 shows the results of the distribution of the 40 vehicles to the classes N, S and G respectively for the four greedy injected nodes. Table 4.9 summarizes all the simulation cases. For each scenario, figure 4.15 illustrates the minimum detection time required by the scheme to fully detect all the existing greedy nodes in the network.

	Final decision:	N	S	G
Greedy nodes				
1		38	1	1
2		37	1	2
3		35	2	3
4		33	3	4

Table 4.9. Final decision results

4.5 Discussion

Compared to normal VANET, A vehicular network which contain a greedy node is easily distinguishable using our proposed algorithm. At first, the suspicion scheme is able to distinguish if the network behavior is normal or not. If a greedy behavior is suspected, the fuzzy logic decision scheme can affirm the suspicion (if it really exist), and determine the responsible nodes using our monitoring defined metrics already mentioned.

By realistic simulations we have confirmed the proper functioning of our proposed algorithm. In fact, we used the concept of linear regression to distinguish between a normal VANET, and a VANET under attack. Once the existence of a probable attack is confirmed, the three defined metrics are used to determine perfectly the nodes that exceeded the normal operating thresholds. In our model and for a dense urban environment, and for 40 vehicles for example, the minimum required detection times are $0.75s$, $1.23s$, $2.78s$ and $4.85s$ respectively for one, two, three and four greedy nodes.

It can be observed form these four simulations scenarios that all the existing greedy nodes have been entirely detected. Furthermore, some other nodes have been classified in the intermediate class S. According to our decision rules, these nodes have momentarily exceed at least one of the fixed thresholds and they have to be supervised in the next monitoring period. Thus, it can be concluded from these results that for a VANET of 100 vehicles, a monitoring period of only 8 seconds is widely sufficient if we consider that greedy nodes are not majority which is a realistic assumption. Moreover, the results confirm that our approach is very efficient and it was able to detect all greedy existing vehicles with a very high probability.

Given the absence of a similar algorithm to the greedy attack in VANETs, we have not been able to compare our numerical results to an existing similar model, but compared to result of detecting greedy attack in MANETs obtained in [59] our results are much more better.

4.6 Conclusion

Although the IEEE 802.11p MAC layer has been enhanced to fit VANETs requirements and despite all the advantages it offers, the IEEE 802.11p protocol, which is the VANET standard, remains vulnerable to many DOS attacks especially the greedy behavior. This denial of service attack is practically easy to achieve by simple manipulation of the backoff parameters. It can easily paralyzes a VANET and endangers the lives of road users. To deal with, we have proposed in this chapter a new algorithm for detecting greedy behavior in VANETs. The proposed algorithm used three newly defined metrics which were proved to be well appropriate for greedy detection in a high mobile network such as VANET, where connections are short and nodes have not enough time to perform adaptive manipulation of backoff parameters. It is composed of both suspicion and decision phases respectively based on enhanced linear regression and fuzzy logic concepts. By monitoring network traffic traces, the algorithm is able to affirm the existence or not of a greedy behavior. In the

affirmative case, monitoring the new mentioned metrics is used to determine responsible nodes.

GDVAN has the advantages of being passive, non-resource-intensive and does not require changes in MAC layer. It has the advantage also to be transparent to users and it can be executed by any node of the network. The simulation results of the different parts of the algorithm are quite promising and they confirmed the correctness of our choices of the metrics and the decision method design. However, the proposed detection method remains specific for greedy attack (and probably for jamming). Thus, our objective was also to develop a more generic DoS attack detection method in order to eliminate or reduce their serious impacts. The new proposed method is the subject of the next chapter.

⁂ ⁂ ⁂ ⁂ ⁂

CHAPTER 5

ENTROPY BASED DETECTION SCHEME

Contents

In this chapter, we detailed our second contribution related to the DoS detection in VANETs. The proposed method is based on Shannon's entropy concept. In fact, we define "Packets entropy" as a new metric of detection. Using "Packets entropy", the proposed method is able to detect DoS attacks by the supervision of traffic traces during short monitoring periods. We measure the entropy of chosen family of exchanged packets in VANET network. The idea is simple: the entropy of normal network (not under attack) is too different (higher) from the entropy of network under DoS attack which allow the distinction between a normal VANET and a VANET under attack. In addition to be generic (not related to the type of attack), this method presents the advantage of rapidity, to be executed by any node of the VANET network and does not require any modification of the 802.11p MAC. Simulations and detection results for both greedy behavior and jamming attacks show its high efficiency.

5.1 Introduction

Given their critical importance, VANETs are exposed to severe attacks, basically due to the weakness of the IEEE 802.11p MAC layer protocol and also to the vulnerabilities of the wireless medium [5, 23] which can be used to attack the entire network and expose users' lives to danger. Among VANET attacks, we distinguish especially the Denial of Service which is a dangerous family of attacks that target services availability and can have bad consequences on the whole network functioning. The attacker, who can be an internal or an external node to the VANET [8], aims to lock available services to legitimate users. Thus, he increases his chances of access to these services. A successful DoS attack can be achieved e.g by a greedy behavior, jamming attack, black-hole attack etc. Since these attacks mislead the critical network services, a high-level security requirement is mandatory for the right deployment of such technology.

In addition to the wireless medium vulnerability which facilitates attacks, VANETs are also characterized by frequent disconnections, a rapid change of topology and a high mobility of nodes. These characteristics make the detection of DoS attacks more difficult. To avoid such attacks it is essential to ensure regular protocols enhancement to reduce prospective exploitation of any existing vulnerabilities. It is also important to design at-

tacks detection tools to prevent and escape the serious consequences that may arise.

In this chapter we focus essentially on both greedy behavior and jamming as an examples of DoS attacks. Thus, we design a new detection method based on a the definition of a new metric named "Packets entropy". It is used to distinguish between a the normal network behavior and the network behavior when it is under DoS attack. Based on the new defined metric, the new proposed detection method is able to supervise traffic traces during short monitoring periods and warns driver in the case of attack detection [114].

Thus, The major contributions of this part of work are:

- The definition of "Packets entropy" as a new detection metric based on the concept of Shannon entropy. To the best of our knowledge this concept have never been used before for network attack detection.
- A novel rapid denial of service attack detection algorithm based on our newly defined metric.
- The application of our algorithm for attack detection in VANET.

The rest of the chapter is organized as follows : Section 2 runs through some backgrounds, essential to introduce the proposed idea. Section 3 overviews the related work in the domain of DoS attacks detection in MANETs and VANETs. We describe in section 4 our new defined metric and our proposed detection method which is based on. Some experimental results are given in section 5 followed by a discussion of the obtained results in section 6 and finally section 7 concludes the chapter and gives direction for future work.

5.2 Background

Our proposed method is based on a new defined metric using entropy concept. This metric is used to distinguish between the behavior of a network in normal operation and the behavior of a network under DoS attack. In this study we focus basically on both greedy behavior and jamming as examples of DoS attacks. To facilitate the understanding of the rest of the chapter, we provide in the following a brief introduction of the Greedy behavior and the techniques that can be used to perform this attack in the case of VANET. We provide a brief description of the jamming attack especially for VANET environment. We study also the mathematical basis of the entropy notion which is an information measurement parameter that we tamed for detecting attacks.

5.2.1 VANET DoS attack: The greedy behavior

As it has been detailed before, the greedy behavior is a well known DoS attack, it specially targets the MAC layer operation and tries to exploit the medium access method weakness. Generally, a greedy node aims to decrease its waiting time, therefore it can access more quickly the medium and penalizes the other existing honest nodes. A greedy node violates restrictions of the MAC layer access method, It always tries to connect to the support and maintains it for its proper use. Several techniques are possible to achieve a greedy behavior attack in a VANET environment, among them we quote: backoff parameters manipulation, scrambling RTS/CTS frames, manipulation and/or over-sizing NAV and DATA frames [94]. Due to VANET nodes' high mobility and short connection duration, the manipulation of backoff parameters is the most useful technique to achieve greedy attack [59]. The attacker can greatly reduce his waiting time and access to the support more rapidly than other nodes. In our simulation we have performed greedy attack using this method.

5.2.2 VANET DoS attack: The jamming

The jamming attack, is a physical level of Denial of Service attack. Due to their affects, jamming attack is considered as a serious Denial of service attack for VANETs. Jamming in its basic definition is the transmission of a signal to disrupt the communications channel, it is usually intentional [58]. This lowers the signal to noise ratio (SNR: Signal to Noise Ratio) for the receiver. Unintentional interference is called "interference" and occurs when a transmission is made in a frequency band that is already in use and operational.

The Jamming can be done in several ways, it can be general (the entire used band is jammed) or selective (only certain transmission sequences are jammed). Despite its ease of implementation, the jamming is difficult to detect. In fact, it is necessary to differentiate jamming from others similar conditions and scenarios such as frequently communication interruption due to the high mobility of vehicles and traffic congestion especially in main intersections. In this attack, the jammer sends signals repeatedly to deny the use of the transmission medium for vehicles and affect communications between them. The channel seems to be busy to the victim. Thus, it cannot receive or send signals in the jammed area.

To evaluate the jamming effect, several parameters can be measured. The most useful among these parameters we find:

- Signal to Noise Ratio:

$$SNR = \frac{Power_{signal}}{Power_{noise}}$$

- Frame Error Rate:

$$FER = \frac{Numberofunsuccessfulframes}{Totalnumberoftransmittedframes}$$

- Jammer to Signal power Ratio:

$$JSR = \frac{Averagejammerpower}{Averagesignalpower}$$

With an effective jamming, legitimate communication are practically blocked. The sender vehicle doesn't detect any idle channel to be able to transmit its packets. Even in the case of a successful sending of the transmitter and in the presence of a jammer, it will be difficult for the receiver to receive correctly what has been transmitted. For a successful adaptive jamming attack, the jammer must act at the same time that the activity of the useful signal to jam. It must also choose the most effective signal transmission model that merges the best the receiver. In a VANET network, jamming once successful, can have inevitable consequences. Some research works such as [32, 58] have looked for some techniques to reduce the effect of jamming for mobile ad hoc networks.

5.2.3 The Shannon entropy

The entropy (also known as the Shannon entropy in the field of information theory) is a mathematical function that intuitively corresponds to the amount of information measured at a destination, and is present or is issued by an information source. The source of information can be a transmitter (such as a radio or network card), a text written in a given language, an electrical signal or any computer file (collection of bytes).

Thus, the entropy measures the uncertainty on the information sent by the source. The more data sent by the source are variable, the more entropy is high. That is to say, if a source is deemed to always send the same information, for example the word 'OK', then its entropy is zero. A source whose next transmitted information is unpredictable admits a maximum entropy. In the absence of specific constraints, the entropy is maximum for a source whose symbols are equiprobable. In particular, the more redundant the source is, the less it contains information.

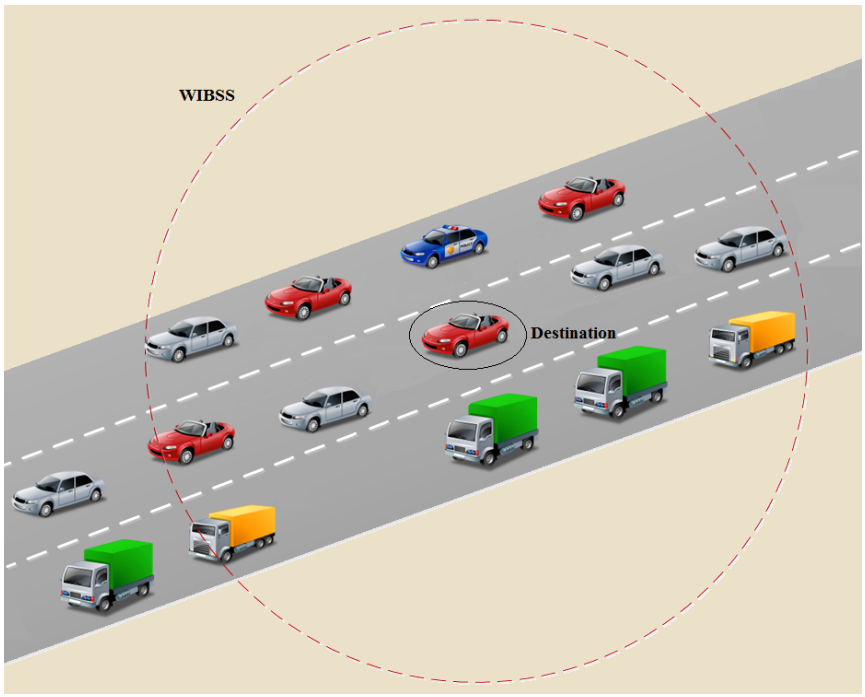


Figure 5.1. VANET decomposition according to information theory requirement.

Entropy is the primary metric in information theory, which is a theory to qualify and quantify the concept of content information on a data set. Mathematically and as defined in [115], the entropy of a source which emits n symbols, the source can be considered as a discrete random variable X having n symbols, each symbol x_i has a probability P_i to appear. Thus, the entropy H of the source X is defined as:

$$H(X) = E[\log_b P(X = x_i)] = \sum_{i=1}^{n} P_i \log_b \frac{1}{P_i} \tag{5.1}$$

where E denotes the mathematical expectation and log_b the logarithm to the base b. In general a base 2 logarithm is used and the entropy uses $bit/symbol$ as a unit. The symbols represent the possible realizations of the random variable X. In this case, the entropy $H(X)$ can be interpreted as the amount of information in bits that the source must provide to the receiver to determine the values of X unambiguously. Then, in base 2 equation (5.1) can be written as:

$$H(X) = -\sum_{i=1}^{n} P_i \log_2 P_i \tag{5.2}$$

The system we design to be used for simulation is composed of several nodes (vehicles) which Form a WIBSS (Wave Independent Basic Service Set). In this architecture, any node can act as a receiver to which the other nodes send data. In this system, the symbols will be transmitted packets, each packet has a probability of occurrence. According to this decomposition shown in Fig.5.1, the receiving node (destination) can therefore measure the entropy of the system according to the formula given by the equation (5.2).

It is important to note that the entropy function can divergent to $+\infty$ when the number of vehicles tends to $+\infty$ (see proof later). In fact, given that we measure our metric in the case of the same WIBSS the number of vehicles is always limited and the value of entropy for any type of data is easily measurable.

- **Proof in the case of equiprobability:**

The object of this proof is to demonstrate that the entropy function can diverge when the number of vehicle became infinite (which is a not practical assumption). We study the case of equiporbability of transmission chances between N nodes. We know that:

$$\lim_{N\mapsto+\infty} H(X) = \lim_{N\mapsto+\infty} \sum_{i=1}^{N} P_i \log \frac{1}{P_i}$$

Or in the case of equiprobability we have:

$$P_i = \frac{1}{N}; \qquad Then$$

$$\begin{aligned} \lim_{N\mapsto+\infty} \sum_{i=1}^{N} P_i \log \frac{1}{P_i} &= \lim_{N\mapsto+\infty} \sum_{i=1}^{N} \frac{1}{N} \log(N) \\ &= \lim_{N\mapsto+\infty} \log(N) \\ &= +\infty \end{aligned}$$

5.3 Literature review

The Attack detection in VANET networks, is so complicated and highly diversified. It cover simultaneously several fields such as the vulnerabilities of the communication protocols, which facilitate the implementation of the attacks. We quote especially the

vulnerabilities of MAC and physical layers protocols. The problem affects also attacks detection techniques in ad hoc networks, which are becoming more and more difficult in practice due to the high mobility and quick change of VANET topology and also the choice of appropriate metrics for the detection. To the best of our knowledge our proposed solution is the first to use the concept of entropy as metric to detect DoS attacks in VANETs, but it is important to look at other related works in the same research axis as our study.

Kyasanur and respectively Cardenas and their co-authors presented in [99, 100], two newly MAC design based solutions both based on a modification of the backoff algorithm of the MAC layer. In general, for this category of solution, a new MAC layer is proposed to avoid backoff algorithm weakness against Denial of service attacks. Hasbullah et al. [51] presented several kinds of possible DoS attacks in VANET. They developed also a model to secure VANETs from DoS attacks and to cope with these dangerous attacks. They demonstrate that Denial of service attacks can be performed using three levels. In the first level, the attacker denies the VANET communication between nodes by keeping the communication state busy for a long time. In a second level, an attacker jams a chosen channel, therefore the other users cannot access the VANET network in the jammed area. Finally, The third level is the Distributed DoS (DDoS), in this level, an attacker run his attack using different agents placed in different locations. To mitigate DoS attacks, the proposed solution in this paper is essentially based on Channel Switching, Technology Switching, Frequency Hopping Spread Spectrum (FHSS) and Multiple Radio Transceivers.

Hamieth et al. proposed in [32] a new detection model of a special class of jamming attack. In this attack, the jammer transmits only when an effective radio activity is detected. In order to detect the presence of jamming attack in VANETs, the proposed detection model is based on the measurement of the error distribution, on the measure of correlation between errors and the correct reception times. They used the correlation coefficient which is a statistical value used to measure the correlation between two series of values (the realization of two random variables). A vehicle calculates the probability of error ($P.E$) then compares with the correlation coefficient ($C.C$). The VANET is considered under jamming attack when the ($C.C$) is greater than the ($P.E$).

In the thesis [58] Tilal and Minhas studied the different types of jamming that can hinder the right operation of IEEE 802.1p based system. They checked the IEEE 802.11p

physical layer resilience of transceivers against several kinds of jamming signals and they evaluated the performance of the system under jamming effects, basically for VANETs environments. They studied both unintentional (interference) and intentional jamming. They have simulated different cases of jamming attacks in order to put the 802.11p protocol to the hardest vulnerability check and improvements tests.

Thamilarasu et al. have focused in [116] on jamming as a type of DoS attack in the IEEE 802.11 based networks. They studied the jamming effects at the PHY and MAC layers in a wireless ad hoc network and they proposed a cross layer suitable detection algorithm. They proved that jamming caused collisions are similar to those caused by the hidden terminal or network congestion. The usage of the channel utilization metric allowed to the detection algorithm to mesure the state of the network congestion and evaluate whether the detected collusion is due to the network traffic conditions or to real intentional jamming. In fact, by relating the use collision detection metric and the cross-layer given information, they distinguished attack scenarios from the non malicious collision scenarios.

In [117] Nguyen et al. have studied the jamming attack as a denial of service attack in vehicular networks and they have proposed a detection method based on the detection of the changes of the Packets Delivery Ratio (PDR) values. The decrease of the PDR compared to a predefined threshold value indicates the presence of a jammer in the supervised area. The proposed solution have been simulated with a fixed jammer and authors claimed that it has fast detection time. For the jamming attack, Muraleedharan and Osadciw proposed in [118] a defense algorithm based on a novel approach in detecting the DoS attack and this to enhance the physical layer security of sensor networks against jamming. Several metrics such as Signal Noise Ratio (SNR), hops, Bit Error Rate (BER), energy, packet loss, packet delivery and distance were used to make anti-jamming decision. They formulate a jammer classification under various scenarios. They analyzed also their proposed method for a variety of scenarios which helps in achieving a high reliability on DoS and improving the Wireless Sensor Networks (WSN) Quality of Service.

Cerasoli generalizes in [119] the use of Shannon's entropy for MANETs by the definition of two new metrics "Relative motion entropy" and "Energy entropy" respectively used for the characterizing of MANET node motion predictability and the efficient use of the energy by cluster-heads communicating to cluster members. The paper shows that "Energy

entropy" is a very useful metric to use in spite of "Relative motion entropy" which lacks the features to be helpful for node motion prediction.

To the best of our knowledge there is no previous existing work for Denial of service attacks detection for VANETs which is based on the Entropy as metric of detection. Existing solutions are mainly interested in MANET and Wireless Mesh Networks (WMN) and used other detection techniques. In this work, we generalize the notion of "Shannon's entropy" by the definition of the "Packets entropy" as a new metric to be used to make decision and define efficiently the membership of vehicle to one of honest or attacker classes. The proposed solution has been tested in the cases of greedy behavior and jamming attacks and it was able to detect the violation of the proper use of the network. The mathematical details of the design and the operating principle of the proposed detection method are given in the next section.

5.4 Method description

5.4.1 New metric description

In the case of mobile wireless network working with a variant of the IEEE 802.11 protocol such as VANET network, we can divide the circulating packets between nodes into four main categories which are: DATA, ACK, RTS and CTS packets family. These packets may be transmitted by any network node. To model this choice, we define the random variable X where sent packets represent the possible realizations of this variable. Thus, mathematically we can write:

$$\sum_{i=1}^{n} P(X = x_i) = 1 \tag{5.3}$$

In terms of packet categories, the equation (5.3) can be written as:

$$P(Data) + P(Ack) + P(RTS) + P(CTS) = 1 \tag{5.4}$$

Where $P(Data)$, $P(Ack)$, $P(RTS)$ and $P(CTS)$ are the respective probabilities that the transmitted packet is of type Data, Ack, RTS and CTS respectively. It is assumed that any packet is in one of the mentioned types. For N nodes in the network, any kind of packet can be transmitted by any node. Thus, for Data packets type for example, we find packets that issue from node n_1, n_2,... ,n_i. It is the same for the other types of packets.

For ease of notation, a packet is characterized by its issuer node n_i and its type {Data, Ack, RTS, CTS}. Thus, we note e.g $Packet(n_i, Data)$, the packet issued from the node n_i and of type Data.

In a VANET the possible transmitted packets are in the following sets: $\{Packet(n_i, Data)\} \cup \{Packet(n_i, Ack)\} \cup \{Packet(n_i, RTS)\} \cup \{Packet(n_i, CTS)\}$, where $i \in N$.

In the following, we note:

- $P(n_i \setminus Data)$: the probability that the received packet is issued from the node i, knowing that is a Data packet.
- $P(n_i \setminus Ack)$: the probability that the received packet is issued from the node i, knowing that is an Ack packet.
- $P(n_i \setminus RTS)$: the probability that the received packet is issued from the node i, knowing that is an RTS packet.
- $P(n_i \setminus CTS)$: the probability that the received packet is issued from the node i, knowing that is a CTS packet.

Whatever the behavior of nodes in the network, we have always:

$$\sum_{i=1}^{N} P(n_i \setminus TYPE) = 1 \tag{5.5}$$

However, for normal operation of a VANET, the event: "the transmitted packet comes from node i" has the same probability for all the nodes, they are called equipossible or to be "equally likely", then we can write:

$$P(n_i \setminus TYPE) = \frac{1}{N} \tag{5.6}$$

where $TYPE \in \{Data, Ack, RTS, CTS\}$

5.4.2 Related detection method description

The detection idea that we propose in this study is based on the supervision of the entropy of a chosen type of transmitted packets in the network. To calculate this entropy we supervise and determine the packets emission probabilities for the chosen type of packets (e.g Data and Ack). Given that the probability of emission of packets changes, then the

entropy change, and the distinction between a normal network and a network under attack can be performed by the calculation of the packets entropy in each case. In fact, a greedy node for example emits more data packets, since it occupies the support for much more time than other vehicles. Thus, the events: "the transmitted packet comes from node i" are never more equipossible.

Then for a greedy node n_G, using Data packets e.g and contrary to the equation (5.6), it is logical to have:

$$P(n_G \setminus Data) \gg \frac{1}{N}.$$

Based on what we have already explained, we defined our newly "Packets entropy" metric for the four types of packets exchanged in a VANET network based on IEEE 802.11p protocol. Thus, we define the four following packets entropy denoted H_{Data}, H_{Ack}, H_{RTS} and H_{CTS} respectively for Data, Ack, RTS and CTS entropy. Then we can write:

- $H_{Data}(X) = -\sum_{i=1}^{N} P(n_i \setminus Data) \log_2 P(n_i \setminus Data)$
- $H_{Ack}(X) = -\sum_{i=1}^{N} P(n_i \setminus Ack) \log_2 P(n_i \setminus Ack)$
- $H_{RTS}(X) = -\sum_{i=1}^{N} P(n_i \setminus RTS) \log_2 P(n_i \setminus RTS)$
- $H_{CTS}(X) = -\sum_{i=1}^{N} P(n_i \setminus CTS) \log_2 P(n_i \setminus CTS)$

To calculate $P(n_i \setminus TYPE)$, we know that mathematically and for two events A and B we have:

$$P(A \setminus B) = \frac{P(A \cap B)}{P(B)} \tag{5.7}$$

where $TYPE \in \{Data, Ack, RTS, CTS\}$

Then $P(n_i \setminus TYPE\}$ become:

$$P(n_i \setminus TYPE) = \frac{P(n_i \cap TYPE)}{P(TYPE)} \tag{5.8}$$

Using the formula given by the equation (5.8), we are able to calculate the packets entropy metric for each chosen type among $\{Data, Ack, RTS, CTS\}$ set of packets types. Given

that Data and Ack packets are the most exchanged in a VANET network and given that the RTS/CTS mechanism is enabled in the IEEE 802.11p protocol only for large packets, we performed our simulations with Data and Ack type packets. By the following described simulations we test in a realistic scenarios the effectiveness of our theoretical designed detection method. For these simulations we used the algorithm 4 which described the steps of the detection phase. To be sure of the existing of a real attack, we chose to report an attack warning when the practical obtained packets entropy is equal or less than the half of the theoretical packets entropy. This threshold can be modified according to the desired accuracy.

Algorithm 4: Entropy based DoS attack detection algorithm

INPUT : T : Short_Monitoring_Period,
State_Attack = False,
$Type \in \{Data, ACK, RTS, CTS\}$
D : Threshold deviation = 50 %
OUTPUT: Annonce_State (State_Attack)

begin
  repeat
    1) Collect traffic traces during T,
    2) Calculate the number N of communicating vehicles
    3) Calculate Theoretical $H_T(Type)$
    4) Calculate Practical $H_P(Type)$
    if $H_P(Type) \leq D.H_T(Type)$ **then**
      State_Attack = True
    end
    Return; Annonce_State (State_Attack)
  until *No existing communication*;
end

5.5 Performance evaluation

To evaluate the performance of our proposed DoS attack detection method, we used the ns-3 simulator [92], to simulate traffic and communications between vehicles (nodes) in a VANET based on IEEE 802.11p protocol. We have simulated two different scenarios using respectively 40, 70 and 100 vehicles. The two scenarios consist on testing respectively the behavior of a normal VANET network and a VANET under DoS attack (greedy behavior). To achieve the greedy attack we manipulate back-off parameters to minimize the waiting

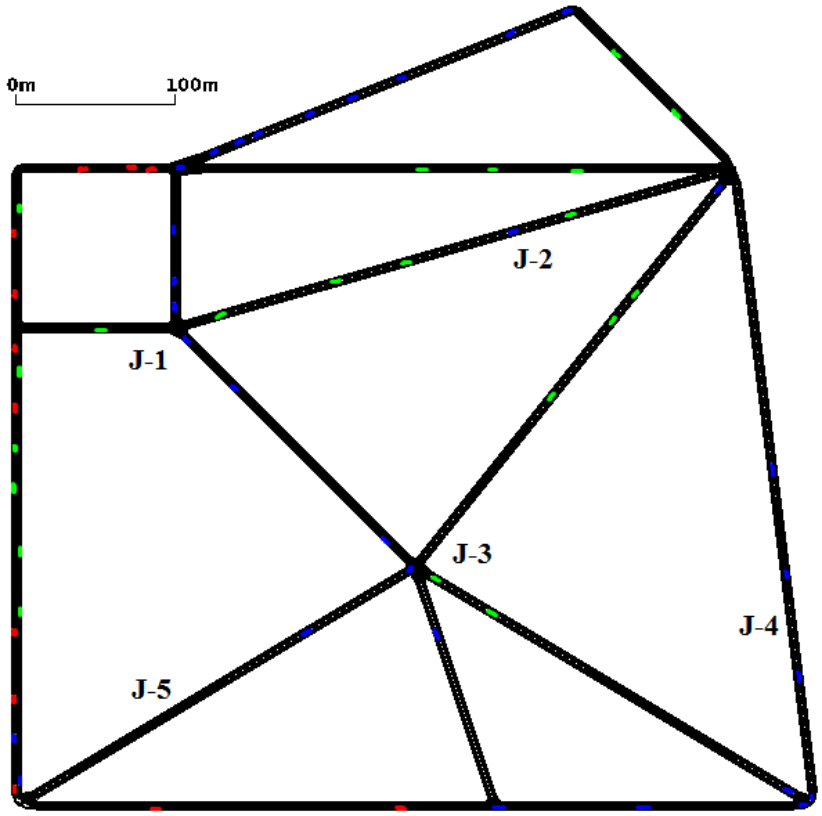


Figure 5.2. Simulation map and jammer's locations.

time of the greedy nodes. We suppose also that honest nodes are majority which is a realistic assumption. In each scenario we calculate the related Data and Ack packets entropy. For greater efficiency, and to approach realistic results, each scenario was repeated 50 times with new random initial conditions at each time. According to the requirements of standards [110] and [95], The generated traffic was of type: WSMP (Wave Short Message Protocol). To simulate nodes mobility, and as shown in 5.2, we use a real city map with signs and traffic lights designed for this purpose under the mobility simulator SUMO [93]. Using SUMO, we generate a mobility traces file for each simulated scenario which can be used directly under ns-3. Each mobility file contains the coordinates and the speeds of all the nodes at each instant. This technique allows a real simulation environment and it is used instead of the predefined ns-3 mobility models especially designed for MANETs. We provided in table 5.1 our used simulation parameters.

Simulation parameters	
Transmission rate	OfdmRate6MbpsBW10MHz
Protocol	802.11p
Simulation time (s)	30
Packets size (bytes)	variable: 1000-1400
Access class	AC_VO
Speed (Km/h)	Variable: 30-60
Network size	600m x 500m
Node count	40 / 70 / 100
Routing protocol	OLSR
Greedy technique	CW_{min} and CW_{max} manipulation
Jamming technique	PBNJ
Jammer count	5
Jammer type	Fixed
Mobility simulator	SUMO

Table 5.1. Simulation parameters

In our simulations, we choose a node to act as a listener (destination) for all the other transmitting nodes. All the nodes are in the same WIBSS. Thus, the chosen node listen to the support and collect traffic traces for short periods. Using these short traffic traces, the destination node can calculate rapidly and easily the packets entropy H_{Data} or H_{Ack}. We choose our simulation scenarios as follows:

- Scenario 1: Normal VANET behavior.
- Scenario 2: VANET under the attack of one greedy node.
- Scenario 3: VANET under the attack of three greedy nodes.
- Scenario 4: VANET under the attack of five fixed jammer.

Each scenario was simulated 50 times with 40, 70 and 100 vehicles. In what follows, we represent in the given figures the average value of the obtained entropy for the 50 performed experiments for each scenario.

5.5.1 Simulation of a normal VANET behavior

In a normal behavior of the network (Scenario 1), and during the monitoring period, we can practically assume (without loss of generality) that all the nodes have the same probabilities to send a Data packet. For example, in the case of $N = 40, 70$ and 100 vehicles, the theoretical H_{Data} can be respectively calculated as follows:

$$H_{Data} = -\sum_{i=1}^{40} \frac{1}{40} \log_2(\frac{1}{40}) = \log_2(400) \approx 5.32$$

$$H_{Data} = -\sum_{i=1}^{70} \frac{1}{70} \log_2(\frac{1}{70}) = \log_2(70) \approx 6.13$$

$$H_{Data} = -\sum_{i=1}^{100} \frac{1}{100} \log_2(\frac{1}{100}) = \log_2(100) \approx 6.64$$

As shown in Figures 5.3 and 5.4, the measured H_{Data} and H_{Ack} for scenario 1 are slightly lower than the theoretical results which is correct because the theoretical entropy measured in the case of equiprobable transmission between nodes, is the highest entropy that can be detected according to the information theory facts. We observe also that measured values for H_{Ack} are slightly smaller than H_{Data} values because that not all the nodes can sent an acknowledgment packet due to the frequent disconnection and to the high mobility in the VANET.

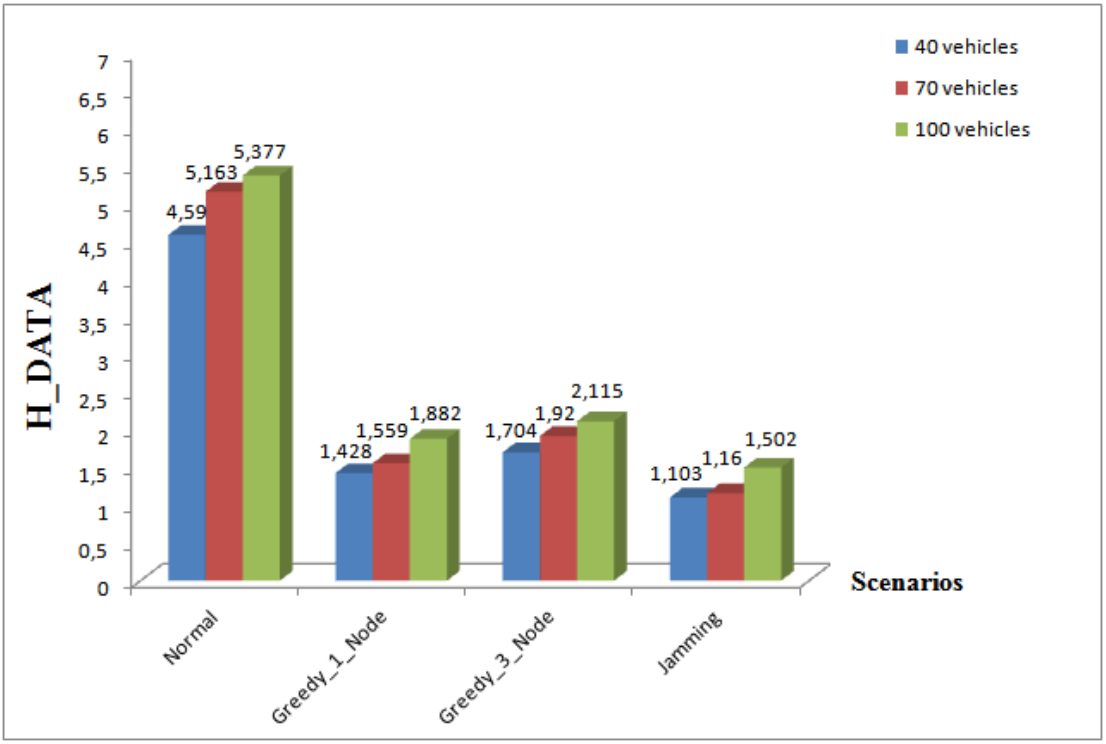


Figure 5.3. Data Packets entropy for the four simulated scenarios (Normal, Greedy_1_Node, Greedy_3_Nodes and Jamming).

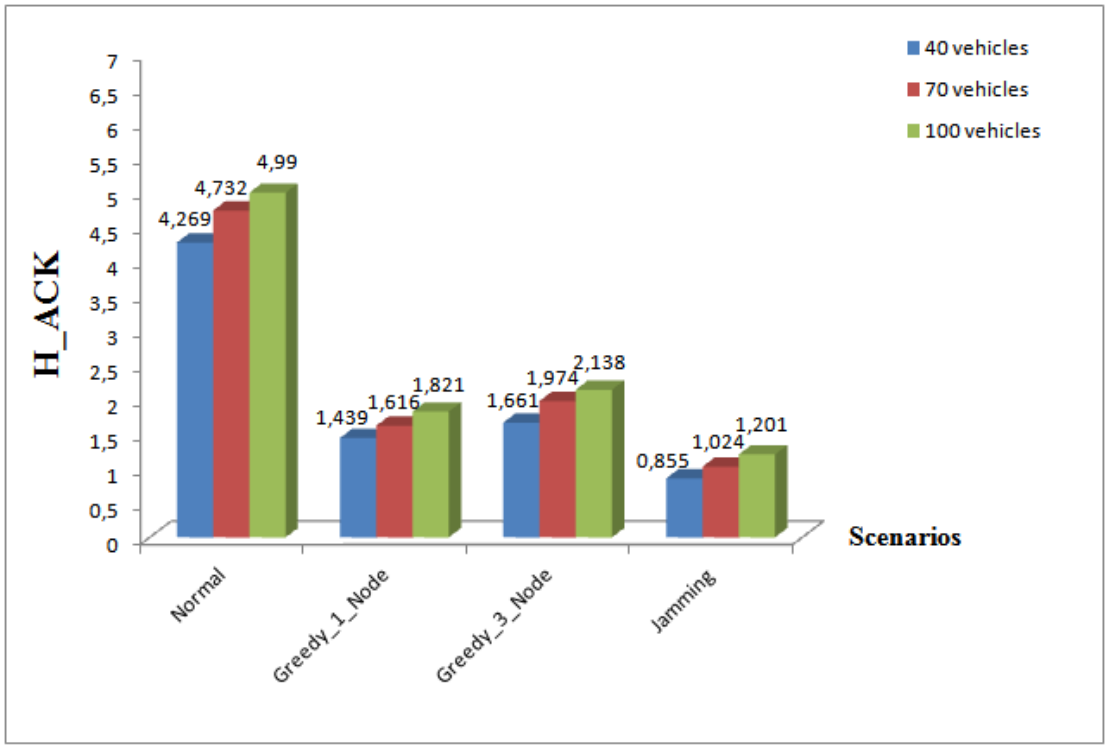


Figure 5.4. ACK Packets entropy for the four simulated scenarios (Normal, Greedy_1_Node, Greedy_3_Nodes and Jamming).

5.5.2 Simulation of a VANET under DoS attack: Greedy behavior

When the network is under DoS attack such as the greedy attack, we have confirmed by simulations that e.g one or two greedy nodes can consume alone about two third ($\frac{2}{3}$) of the hole transmitted data. The consumption of three or four greedy nodes can reach also three quarters ($\frac{3}{4}$) of all transmitted data. We suppose that the other nodes (honest nodes) have the same probabilities to send a Data packet. In the following part we present results for one and three greedy nodes (scenarios 2 and 3) because no significant variations have been seen between one and two or between three and four greedy nodes.The theoretical H_{Data} can be calculated respectively for $N = 40, 70$ and 100 vehicles as follows:

- For one greedy node we have:

$$H_{Data} = -\frac{2}{3}\log_2(\frac{2}{3}) - \sum_{i=1}^{39}\frac{1}{3*39}\log_2(\frac{1}{3*39}) \approx 2.68$$

$$H_{Data} = -\frac{2}{3}\log_2(\frac{2}{3}) - \sum_{i=1}^{69}\frac{1}{3*69}\log_2(\frac{1}{3*69}) \approx 2.95$$

$$H_{Data} = -\frac{2}{3}\log_2(\frac{2}{3}) - \sum_{i=1}^{99}\frac{1}{3*99}\log_2(\frac{1}{3*99}) \approx 3.12$$

- For three greedy nodes we have:

$$H_{Data} = -\frac{3}{4}\log_2(\frac{1}{4}) - \sum_{i=1}^{37}\frac{1}{4*37}\log_2(\frac{1}{4*37}) \approx 3.30$$

$$H_{Data} = -\frac{3}{4}\log_2(\frac{1}{4}) - \sum_{i=1}^{67}\frac{1}{4*67}\log_2(\frac{1}{4*67}) \approx 3.51$$

$$H_{Data} = -\frac{3}{4}\log_2(\frac{1}{4}) - \sum_{i=1}^{97}\frac{1}{4*97}\log_2(\frac{1}{4*97}) \approx 3.63$$

Under greedy attack, (Scenario 2 and 3) and as expected, the obtained packets entropy values for both Data and Ack packets shown in Figures 5.3 and 5.4 were relatively decreased compared to the normal VANET scenario. Also, and as it was observed in the case of a normal VANET, the measured H_{Data} and H_{Ack} for one and three greedy nodes are also slightly lower than the theoretical results for the same previously detailed reasons in the case of a normal network.

In the next section we discussed all the obtained results for a normal behavior, a greedy behavior attack and a jamming attack.

5.5.3 Simulation of a VANET under DoS attack: Jamming

To simulate the jamming attack (Scenario 4), we placed five jammers distributed throughout the action area as shown in Fig. 5.2. From a simulation point of view, these are fixed node equipped with a high power IEEE 802.11p transceiver configured to be able to jam an entire chosen band. In fact, we had the choice between several locations of jammers that allow us to cover the whole desired area. In this case, we assume that we have a total covering jamming attack that covers the entire area. For a maximum jamming efficiency, and as proved in [58], we choose to use the variant PBNJ (Partial Band Noise Jammer)

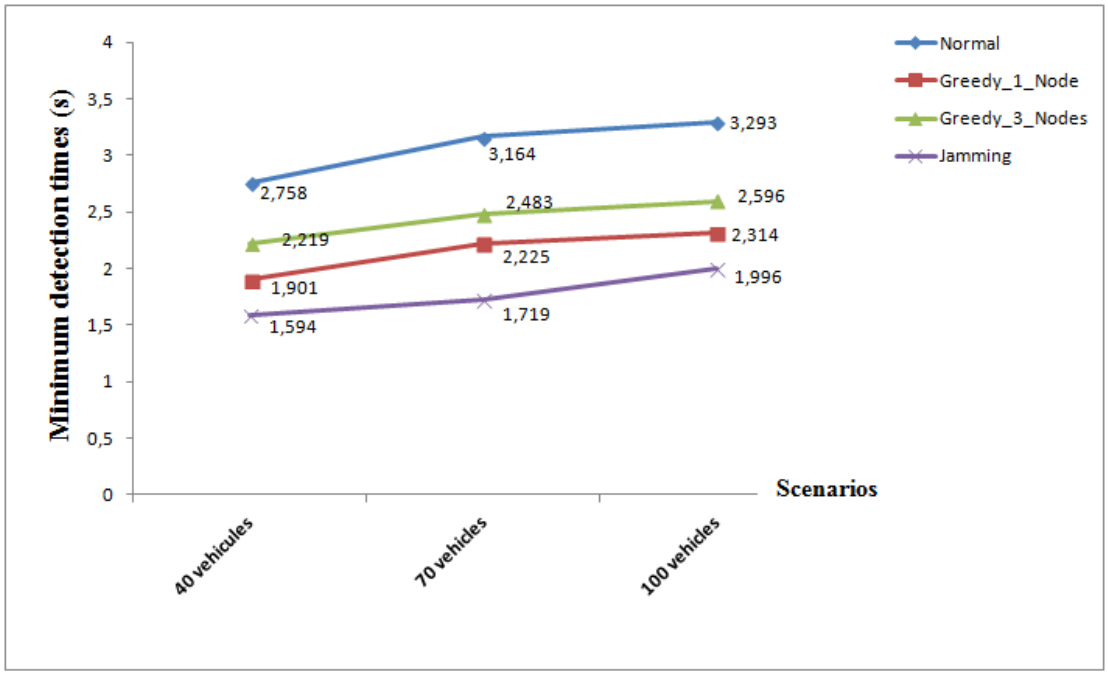


Figure 5.5. Mimimum detection times for the four simulated scenarios (Normal, Greedy_1_Node, Greedy_3_Nodes and Jamming).

of the noise jamming technique proved to be the most fatal to the system. Each jammer sends a confusing signal immediately when it detects a useful signal emitted by any vehicle and this in the operation band of the WIBSS (Wave Independent Basic Service Set) of the VANET.

Under this total covering jamming attack and as expected, the obtained packets entropy values for both Data and Ack packets shown in Figures 5.3 and 5.4 were relatively decreased compared to the normal VANET scenario. We observed also that the H_{Data} and H_{Ack} obtained values for the jamming scenario are slightly lower compared to greedy scenarios, in fact it was only enough to jam a part of packet to guarantee that it is not received correctly.

5.6 Discusion

By the simulations we carried out, the obtained results were significant. For each performed scenario for both greedy and jamming attacks, the practical results were close to the theoretical ones. The two observed metrics H_{Data} and H_{Ack} behaved in the same way.

By these results, it has also been proved that the entropy is maximum for an information source where emitted symbols are equiprobable that mean: the more data sent by the source is variable, the more entropy is high. In fact, this is the case of a normal VANET where all the nodes have the same probability to transmit, contrary to a VANET under attack where some nodes (attackers) behaved with a completely different way.

Thus, it is normal to have a high packets entropy for a normal VANET behavior contrary to a VANET under attack. This difference allows our scheme to distinguish easily between a normal VANET and a VANET under attack by a simple fixed threshold. In our case for example, a H_{Data} lower than 3 indicate a very suspicious network behavior. In our algorithm 4, we suspect an attack when the measured packets entropy is less than the half of the theoretical that must be obtained if the network was not under attack.

To make a comparison with the best obtained detection times of other techniques and to the best of our knowledge there are no existing similar work for the greedy behavior or jamming detection which gave its best minimum detection times. Using our new Packets entropy defined metric, we give in Fig.5.5 our best minimum obtained detection times to serve as a reference for future comparison with other methods. Thus, Fig.5.5 detailed the minimum detection times for each simulated scenario. We observe that the jamming attack is the fastest to be detected with is logic because in the case of total jamming scenario, the number of correct received packets by the most existing nodes is very limited, and this is detectable more quickly than other scenario. We observed also that the detection of the non existence of possible attack (normal VANET) takes more time than the other scenario. In fact, it is more rapid to detect a network dysfunction than to assert that it does not exist.

5.7 Conclusion

In this chapter, we defined "Packets entropy" as a new metric to be used for VANET denial of service attack detection. Based on this metric, we proposed also a new DoS attack detection scheme for VANET. The proposed scheme has been verified for both greedy and jamming attacks using collected traffic traces during short monitoring periods. It presents the advantage of rapidity of computation, to be executed by any vehicle of the VANET network and does not require any modification of the 802.11p MAC layer protocol used as a standard for VANETs. Performed simulations show the high efficiency of the newly

defined metric and the related proposed detection method. As a future work, we expect verify the efficiency of our defined metric for other DoS attack such as blackhole. We expect also the design of a new reaction method against these attacks, which the subject of our next and final contribution for this dissertation.

⁂ ⁂ ⁂ ⁂ ⁂

CHAPTER 6

GAME THEORY BASED REACTION SCHEME

Contents

In this chapter, we propose a reaction method against DoS attacks in VANET. In this method we have the choice between two proposed reaction games. Design methodology and defined metrics are inspired from game theory models. Recently, some detection methods have been validated. However, for the reaction, the problem is much more complicated especially in the case of vehicle to vehicle communication. In this direction, game theory applied to the security of wireless networks (also known as security games) can be a good way of modeling. The main advantage of game-based models is their ability to implement adaptive strategies that take into consideration the changes occurring in the contexts in which VANETs are deployed. To the best of our knowledge, such games have not been proposed in the literature. The simulations showed the efficacy of our proposal measured by the performance of the obtained results.

6.1 Introduction

Denial of service attacks family is considered as one of the most dangerous family of attacks for vehicular networks. Basically, an attacker tries for example to block the communication using a jamming approach. These attacks can have serious consequences especially for VANET applications. The literature is rich of several proposals dealing with detection and reaction algorithms against DoS attacks for MANETs. However, for VANETs there is much less algorithms. The majority of existing works are mainly dealing with attacks detection [120, 74].

After two DoS attack detection methods presented in the previous chapters, we focus, in this chapter on VANET reaction against DOS attacks and we propose two newly security games theory-based approaches since it seems to be a good way of design for our problem. Indeed, in a game there are generally two kind of players. When a player makes an action the other responds with a reaction. According to the general principle of game theory, each player tries to maximize his gain and/or reduce his loss. From formal modeling perspective, the gain or the loss can be obtained by cost estimation functions commonly known as *payoff function*. To maximize their profits, players act according to their chosen strategies. A *strategy* of a player can be a single movement or a set of successive movements during the game. Throughout the game, a player can sometimes win or lose. Thus, the

total cost of a given player can be computed as the sum of gains/losses for each step of the game. Game theory classifies games according to several criteria including: *Cooperative* vs *Non-cooperative*, *Static* (single-stage) vs *Dynamic* (repeated), *Strategic-form* vs *Extensive-form*, *Perfect* vs *Imperfect* information and finally *Complete* vs *Incomplete* information. The choice of one of these criteria depends mainly on the formalism of the game itself and also on its conditions.

Basically, there are two main families of games approaches: cooperative games and non-cooperative games. The cooperative games require a prior arrangement between users; they require also an additional signaling. This assumption may be more difficult to achieve especially in a highly mobile and heterogeneous environment such as VANET. However, in a non-cooperative game, decision makers are the players themselves, everyone decides for himself without the need for any kind of cooperation, which is more appropriate in our case. Thus, the major contributions of this study are:

- Provide a new theory game based formalism for denial of services attacks in VANETs.
- Propose two possible non-cooperative games for DOS attack under realistic assumptions and the use of real mobility models based on real map.

The rest of the chapter is organized as follows. In Section 2 we provide the state of the art. Our security game based reaction algorithms are described in Section 3. Simulation environment, simulation parameters, metrics and the performance evaluation results are presented in Section 4. Finally, Section 5 concludes the chapter.

6.2 Literature review

To the best of our knowledge there are no actual game theory based reaction algorithm against DoS attacks in Vehicular Ad hoc Networks based on IEEE 802.11p protocol. Most of the existing developed works are based on IEEE 802.11 protocol especially related to MANETs which are less mobile than VANETs. However, some interesting works about attacks modelization in wireless networks and based on game theory concepts have been proposed.

Felegyhazi and Hubaux demonstrate in [121] the wide possibilities of the use of game theory as a modeling tool for wireless networks attacks. In fact, in wireless networks, the behavior of an attacker node can modify the behavior of a honest node. Thus, these behaviors can be modeled as an attack/defense game. In their work, they used four simple examples to introduce the most basic concepts of the theory of non-cooperative games. They tried to connect the four proposed games: *Forwarder's Dilemma game*, *Joint Packet Forwarding game*, *Multiple Access game* and *jamming game* to the different possible attacks according to the OSI model. They presented several notions and concepts of game theory such as static games, dynamic games, Nash equilibrium, zero-sum games, games with complete and incomplete information and the representation of games in strategic and extensive form.
According to the authors, this will allow researchers to have the necessary techniques to analyze and model the different use cases without the need to read books of this theory which are generally economy oriented. However, modelization that has been done for the four games was with only two players.

The most important VANETs security aspects from game theory point of view have been discussed in [122] by Alpcan and Buchegger. They provided a framework to take defensive and optimized measures against threats posed by malicious users. The provided models and solutions were generic to maximize their applicability for further systems. Proposed security games for VANETs take as inputs some metrics called centrality measures. These measures are calculated using road maps and vehicles distribution. Authors claimed their proposed methods and strategies allowed optimal infrastructure development of traffic control and security for Road Side Unit (RSU) and On-Board Unit (OBU). Multiple types of security games such as classical zero-sum games, fictitious play and fuzzy game have been studied under varying information availability assumptions for the players. Some simulation cases were given such as evolution of attack and defense strategies for each type of studied game. Nash equilibrium probabilities have been also evaluated. We noted that the simulations for this work were made with a private simulator that is not recognized for VANET simulations. It was mainly developed and used for mesh networks.

Cagalj et al. have addressed in [123] the cheating problem in CSMA/CA MAC based networks. They proposed a new game-theoretical model to investigate the selfish behavior problem of nodes and verified it by appropriate simulations. The main contribution of

their work is the proposed new formalism for the rational cheating. The paper studied also the cases of single and several cheaters acting without restraint and demonstrates how to obtain a Nash equilibrium. The paper demonstrates also that the Nash equilibrium can be collectively obtained by smart cheaters.

Recently, Sedjelmaci et al. designed and implemented a new game theory based intrusion prevention schema for VANET [124]. It has the ability to predict a possible future malicious behavior of an attacker. They used the game theory concept to predict the future behavior of the monitored node and categorize it into one of four possible classes, according to its predicted attack severity. Despite that their method is preventive and ours is for reaction, we compared the generated overhead of their schema to ours.

Thus, we notice very diverse possibilities of using game theory to solve some security challenges of wireless networks and especially of vehicular networks. Unfortunately this latter aspect is not sufficiently addressed in the literature. We hope participate to reduce this gap by our present work detailed in the next section.

6.3 Proposed Reaction games

6.3.1 Overview

This section provides our mathematical designed model for the context in which vehicles operate. The communication model is governed by the requirements and constraints of the standard IEEE 802.11p [27]. We design a VANET with variable speeds nodes. Among these nodes we may have some nodes acting as attackers. To guarantee consistency with the requirements of game theory, we assume that players are rational: That is mean they either seek to reduce their loss or to maximize their profit. The choice between maximizing profit or reducing loss depends strongly on the nature of the payoff functions. Throughout the game, a player can sometimes win or lose. Loss and gain values are estimated by the $utilityfunctions$ that we detailed thereafter and the total cost of the game for each player P_i is calculated using the formula:

$$TC(P_i) = \sum_{t=1}^{t=S} W_t(P_i) - \sum_{t=1}^{t=S} L_t(P_i) \tag{6.1}$$

Where:

- $TC(P_i)$: the total cost of the game for the player i.
- $W_t(P_i)$: the winning of player P_i at step s of the game.
- $L_t(P_i)$: the losses of player P_i at step s of the game.
- S: the total number of game steps.

In fact, we proposed two different possible reaction games. For these games and due to several theoretical and practical reasons (heterogeneity and high mobility of the VANET environment which induces frequently disconnections and often topology changes), we considered non-cooperative games where each player plays for his own account. For our proposed reaction games, we used the following generic game formalism: $\mathcal{G} = (\mathcal{P}, \mathcal{S}, \mathcal{U})$ as proposed in [121], where:

- $\mathcal{P}$ is the set of players (honest and attacker),
- $\mathcal{S}$ is the strategies set (possible movements),
- $\mathcal{U}$ is the utility functions set (payoff functions).

The main idea of our reaction games is to try to avoid driving through attacked areas. Figure 6.2 show an example of road change to avoid jammed area. The blue path indicate the normal road to flow, while the red one indicate an other road to flow in the case of attack detection. In a VANET context and given the variety of attacks that can take place, we assume that escaping the attacked areas and malicious nodes (while maintaining unchangeable final destination) increases the efficiency for a VANET user in terms of data rate.

We assume that the targeted area is subdivided into a matrix of $l \times r$ cells, as shown in Fig.6.1, which is considered as the same for all the vehicles. We limit the attack effects to the cell where the attacker is belonging. We also consider that each player, P_i, travels from a starting point s_i to a destination point d_i, that it does not change but it can be reached by making different choices (different paths). Moreover, we subdivide the traveling time in several periods. Each period, noted as T, represent one state/step of the game. This period is estimated as the crossing time of one cell. In our case, we chose two values for T corresponding to the urban and rural portions of the targeted area. We consider also that the action of a player, at any step, is quantified by a pair of values representing his gain

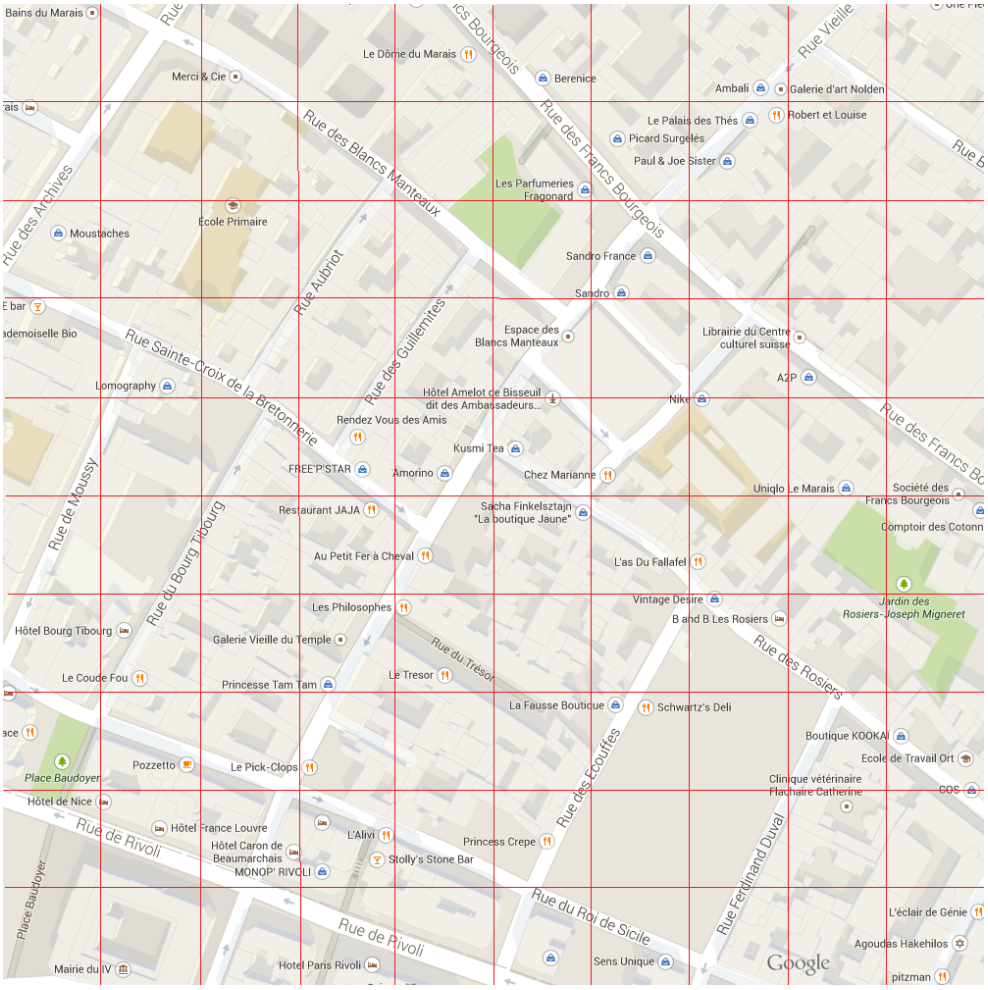


Figure 6.1. Example of the subdivision of the action area.

and the gain of his adversary for this step. These values are computed using our proposed algorithms that we will describe later and they define what a player may lose or win if he chooses to cross a given cell. These values depend on the player type (honest or attacker). Indeed, for a honest vehicle, a congested or jammed cell is not recommended to cross and will have a high value of loss. However, a vehicle carrying a jamming attack may attribute to this same cell a high value of gain.

In this study, we propose two games. The first one is a *strategic* game, where the second one is an *extensive* game. Both games are detailed in the next subsections.

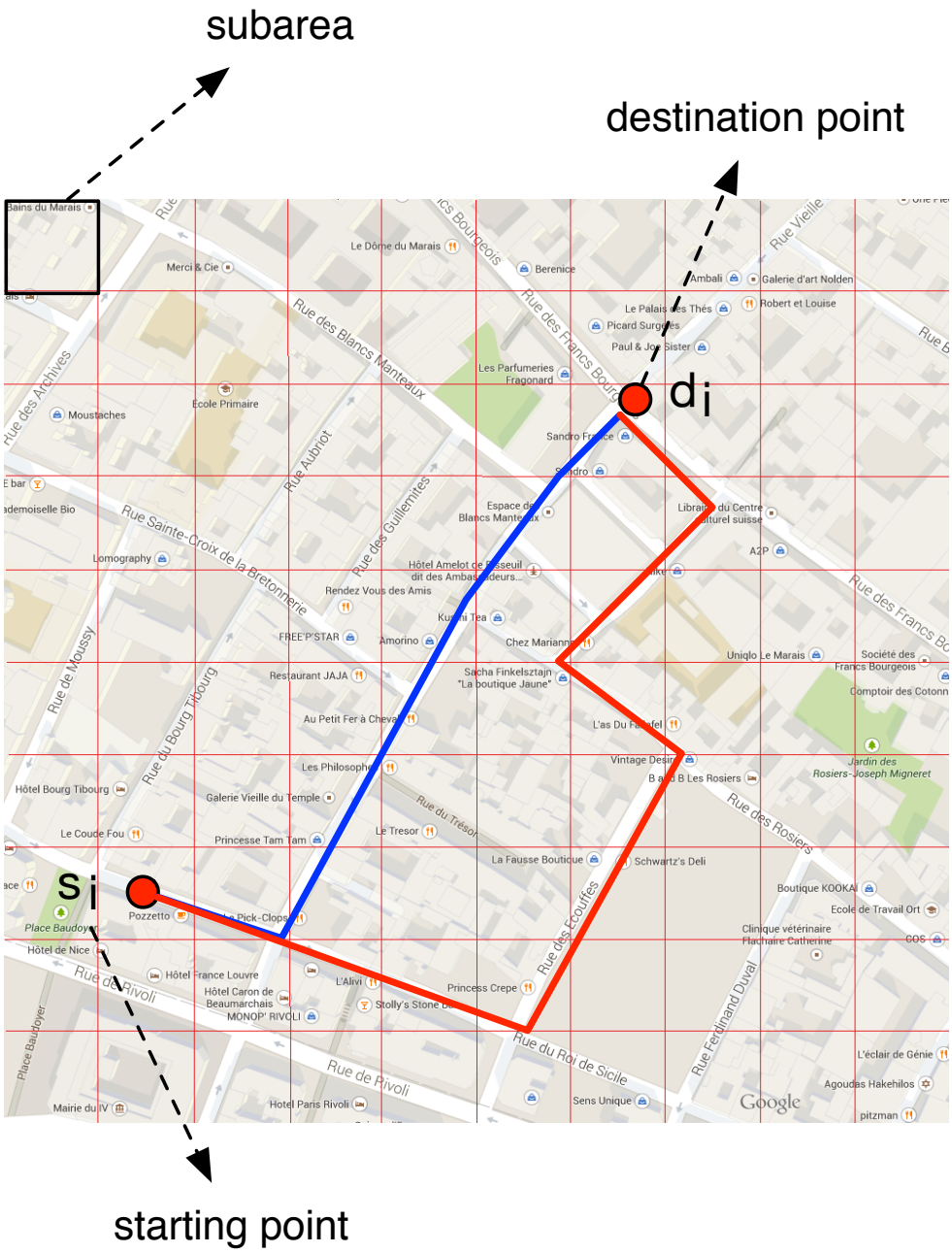


Figure 6.2. Example of road change to avoid jammed area.

6.3.2 Game 1: Description, strategic form representation and payoff matrix

Our first game is a *zero-sum strategic* game with *perfect information*. A perfect information game is a game in which each player is aware of the moves of all other players

that have already taken place [125]. In this game players make decisions simultaneously. Players are defined as honest (noted H) vehicle or attacker (noted A) vehicle. In this case, the set $\mathcal{P}$ of players is equal to $\{H_1, H_2, ..., H_n, A_1, A_2, ..., A_m\}$, and the total number of vehicles is equal to $n + m$. We assume that the number of honest vehicles is much more important than the number of attacker ones ($m \ll n$). As a strategies, we propose $\mathcal{S} = \{\text{Attack, Stop}\}$ for attacker vehicle and $\mathcal{S} = \{\text{Continue, Change direction}\}$ for honest vehicle. Basically, attacker has two options: It can either maintain or stop its attack. On the other hand, honest vehicle can either continue driving on the current cell, or it can change its direction in order to move away from the attacker. It is clear that both the players must have certain information of their environment. They must know the time, location, actions, strategies and payoff functions of the other player on real time basis. In the following table (Tab. 6.1) we summarize the payoff function that we propose for this first game.

	Attacker vehicle	Attack	Stop
Honest vehicle			
Continue		(H_{11}, A_{11})	(H_{12}, A_{12})
Change direction		(H_{21}, A_{21})	(H_{22}, A_{22})

Table 6.1. Game 1 Payoff matrix

where:

- $H_{11} = A_{12} = -2$
- $H_{12} = A_{11} = +2$
- $H_{21} = A_{21} = +1$
- $H_{22} = A_{22} = -1$

It is worth noting that with these payoff values our game is a zero-sum game. For example when the attacker choice is to attack, he obtain a payoff equal to $A_{11} = +2$ when the honest vehicle continue its direction to an attacked zone. In this case, the honest vehicle receive a payoff equal to $H_{11} = -2$. Moreover, when the attacker choice is to stop attack he loses ($A_{12} = -2$) when the honest vehicle continue its direction to the attacked zone. In this case, the later one owns $H_{12} = +2$. According to the last considerations and following the Nash theorem:

Theorem 1. ***(Nash 1950)***
Every finite strategic-form game has a mixed-strategy Nash equilibrium.

our game admit a *Nash equilibrium* (NE). In fact, the NE of this game is obtained when the attacker vehicle continue to attack and the honest vehicle change its direction, which is a logic result in this kind of simulated attack (jamming).

6.3.3 Game 2: Description, extensive form representation and payoff algorithms

In our second game we use the *extensive-form* game with perfect information called also dynamic game [125]. The *extensive-form* representation is recommended for finite sequential games, when players play one after the other during a finite number of steps. In order to illustrate an *extensive-form* game, let consider a game with two players P_1 and P_2. As shown in figure 6.3, the player P_1 has 3 possibles strategies ($S_1(P_1)$, $S_2(P_1)$ and $S_3(P_1)$), while the player P_2 has 2 possibles strategies for each P_1 strategy (($S_1(P_2)$, $S_2(P_2)$); ($S'_1(P_2)$, $S'_2(P_2)$) and ($S''_1(P_2)$, $S''_2(P_2)$)). P_1 starts the game, then the P_2, and so on. α_{12} and β_{12} represent the payoff pair of P_1 and P_2 when they chose respectively strategies 1 then 2. The sets of possible strategies that can be played by each player can be different.

As in our first game, we define for the second game the same set of player. We also consider the same possible strategies for the attacker vehicle $\mathcal{S} = \{\text{Attack, Stop}\}$. However, we add a new *stop* strategy for the honest vehicle, $\mathcal{S} = \{\text{Continue, Stop, Change direction}\}$. In this case, in addition of continue driving or change direction, a honest player can also stop in order to wait for the attacker to move away from its cell. Finally, for assessing the payoff values for each player, we take into account if a crossed cell is under attack or not, and also the density of vehicles in that cell. Based on our realistic assumption that escaping the attacked areas and malicious nodes (while maintaining unchangeable final destination) increases the efficiency for a VANET user. Thus, the main idea for this second game is also to avoid, if possible, both attacked and congested cells (where and when attackers operate). Algorithm 5 and Algorithm 6 present our payoff values, noted as:

- α_{ij} = honest vehicle payoff when he choose i strategy and attacker chosse j strategy.
- β_{ij} = attacker payoff when he choose j strategy and honest vehicle chosse i strategy.

Algorithm 5: Payoff calculation for honest vehicles

INPUT : (c_x, c_y) : Position of the current cell,
(d_x, d_y) : Position of the destination cell,
$\{A(x_i, y_i)\}$: Set of attacked areas positions.
OUTPUT: α_{11}; α_{12};
α_{21}; α_{22};
α_{31}; α_{32}

begin
Compute $\{P(x_i, y_i)\}$: The set of positions of the cells belonging to the shortest paths from (c_x, c_y) to (d_x, d_y).
Extract the position of the next cell (n_x, n_y).

if $(n_x, n_y) \in \{A(x_i, y_i)\}$ **then**
$\alpha_{11} = -2$; $\alpha_{12} = +2$;
$\alpha_{21} = 0$; $\alpha_{22} = -2$;
$\alpha_{31} = +1$; $\alpha_{32} = -2$
else
$\alpha_{11} = +3$; $\alpha_{12} = +3$;
$\alpha_{21} = -2$; $\alpha_{22} = -2$;
$\alpha_{31} = -2$; $\alpha_{32} = -3$
Return: α_{11}, α_{12}; α_{21}; α_{22}; α_{31}; α_{32}

Algorithm 6: Payoff calculation for attacking vehicles

INPUT : $\{V(c_x, c_y)\}$: The set of existing vehicles positions in the cell (c_x, c_y), where an attacker is present
OUTPUT: β_{11}; β_{12};
β_{21}; β_{22};
β_{31}; β_{32}

begin
if $\{V(i, j)\}$ *is empty* **then**
$\beta_{11} = -2$; $\beta_{12} = +2$;
$\beta_{21} = -2$; $\beta_{22} = +2$;
$\beta_{31} = -2$; $\beta_{32} = +2$
else
$\beta_{11} = +3$; $\beta_{12} = -3$;
$\beta_{21} = +2$; $\beta_{22} = -2$;
$\beta_{31} = +1$; $\beta_{32} = -1$
Return: β_{11}; β_{12}; β_{21}; β_{22}; β_{31}; β_{32}

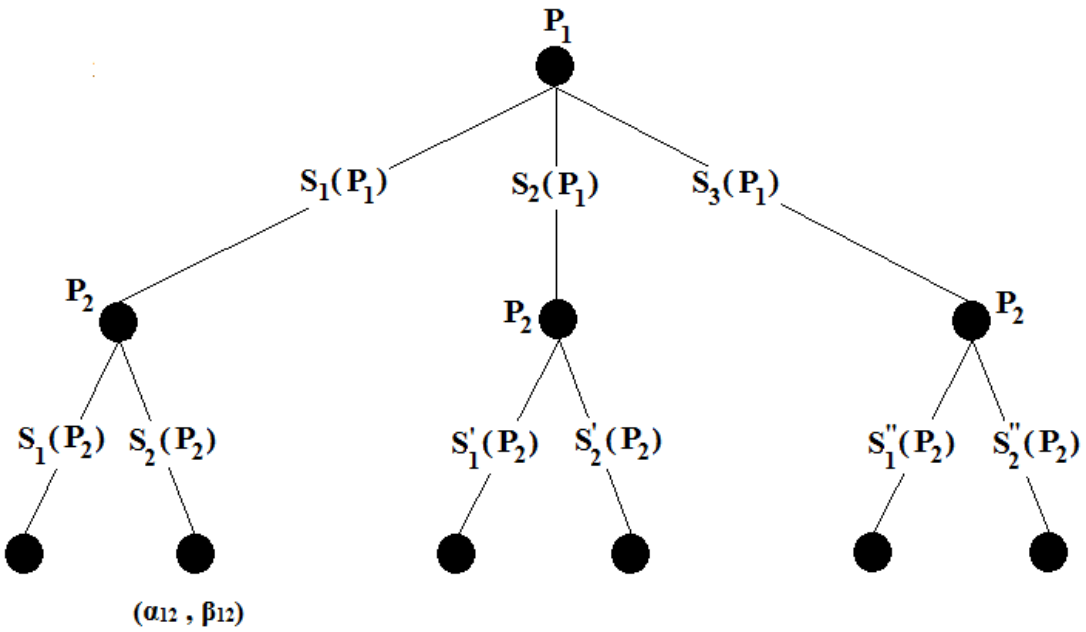


Figure 6.3. The extensive form representation of a game

According to the last considerations and following the Kuhn theorem:

Theorem 2. ***(Kuhn 1953)***
Every finite extensive-form game of a perfect information has a pure strategy Nash equilibrium.

our game admit a *Nash equilibrium (NE)*. In fact, the *NE* of this game is obtained when the attacker vehicle continue to attack and the honest vehicle momentously stops (until the attacker live the zone) or change its direction, which seems to be a logic result for the jamming attack that we discuss later.

6.4 Performance evaluation

In this section we numerically evaluate the performances of our security game solutions using realistic simulation data obtained from a traffic engineering simulations systems. We used the ns-3 network simulator [92] as network simulator and SUMO [93] as a mobility simulator. For the simulations setup, we considered VANET composed of maximum 250 nodes in which we vary the number of attackers from 1 to 3 attackers (jamming attack).

All the nodes are following IEEE 802.11p standard with a channel capacity of 6 Mb/s. Our simulation map is shown in Figure 6.4. This map has both urban and rural areas. The traffic model is CBR (Constant Bit Rate). The generated traffic respect the requirements of the WSMP (Wave Short Message Protocol) and standards [126] and [95]. In addition, we assume that all the players have prior knowledge of the attacks and congestion areas. This assumption could be easily considered, if we assume that the player use one of the algorithms of detection attacks proposed in [106] or [114]. We also consider that the probabilities that an attacker vehicle turns to honest one and that of a honest one becomes attacker vehicle are negligible.

Parameter	**Value**
Protocol	*IEEE 802.11p*
Transmission rate	*OfdmRate6MbpsBW10MHz*
Environment	Mixed (urbain and rural)
Network size	1000m x 1000 m
Urbain average speed	36 Km/h ($\approx$ 10m/s)
Rural average speed	70 Km/h ($\approx$ 20m/s)
Max speed	90 Km/h ($\approx$ 25m/s)
Execution time	From 200s to 300s
Packet size	Variable (max 1400 bytes)
Traffic model	CBR
Channel	CCH
Routing protocol	OLSR
Mobility simulator	SUMO
Maximum allowed traffic density	250 $vehicles/Km^2$

Table 6.2. Simulation parameters.

The fading effect existing in real wireless channels has been taken into account. We carried out all our simulation using the shadowing channel model, represented by the following equation:

$$\left[\frac{P_r(d)}{P_r(d_0)}\right]_{dB} = -10\xi log(\frac{d}{d_0}) + X_{dB}$$

where d_0 is the reference distance, $P_r(d)$ is the mean received power at the distance d, ξ is the path loss exponent and X_{dB} is a Gaussian random variable with zero as mean and standard deviation σ_{dB}. We used $\sigma_{dB} = 4$ and $\xi = 2$ (free space propagation). Finally, we assume that the energy and computation capacities of each vehicle are high which is a

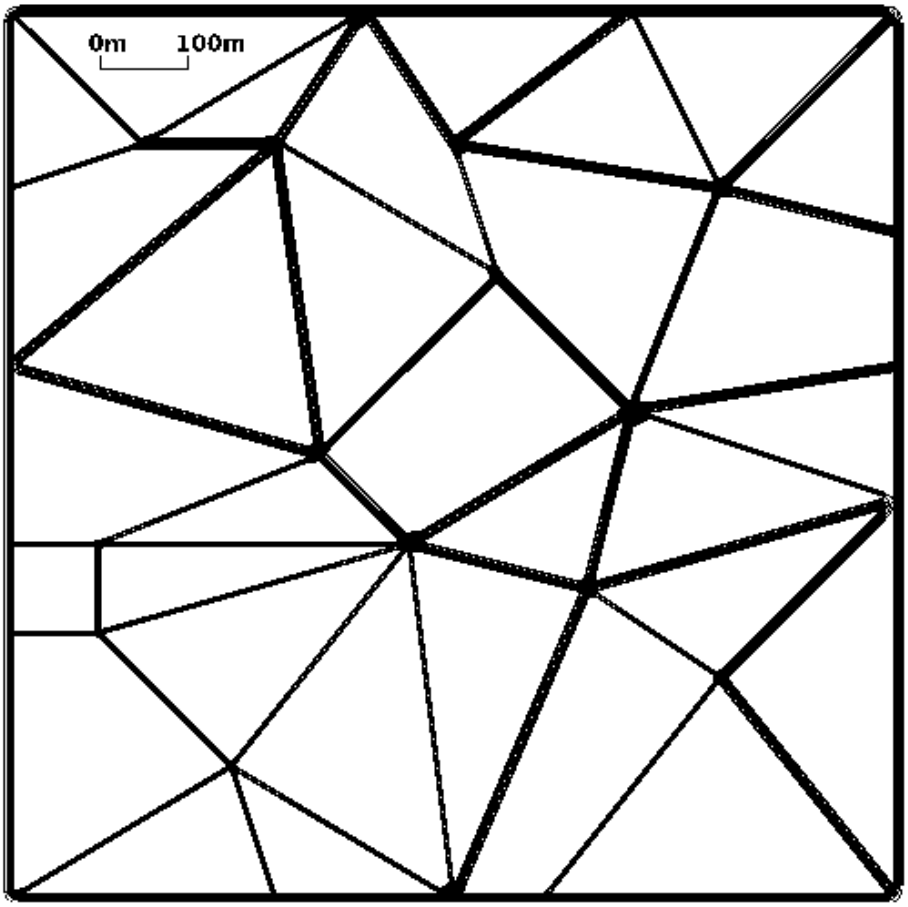


Figure 6.4. The map of the simulation zone.

common VANET assumption. The parameters of the simulation environment are described in Table 6.2.

To evaluate the efficiency of our reaction games, we used the following metrics:

- *Packet Delivery Ratio (PDR)*: The fraction of original data packets sent by the source application layer and are successfully delivered to the application layer of the desired destination.

- *Packet Overhead (POV)*: The total count of overhead packets, other than the data packets. In each original or forwarding transmission, an overhead packet is counted once.

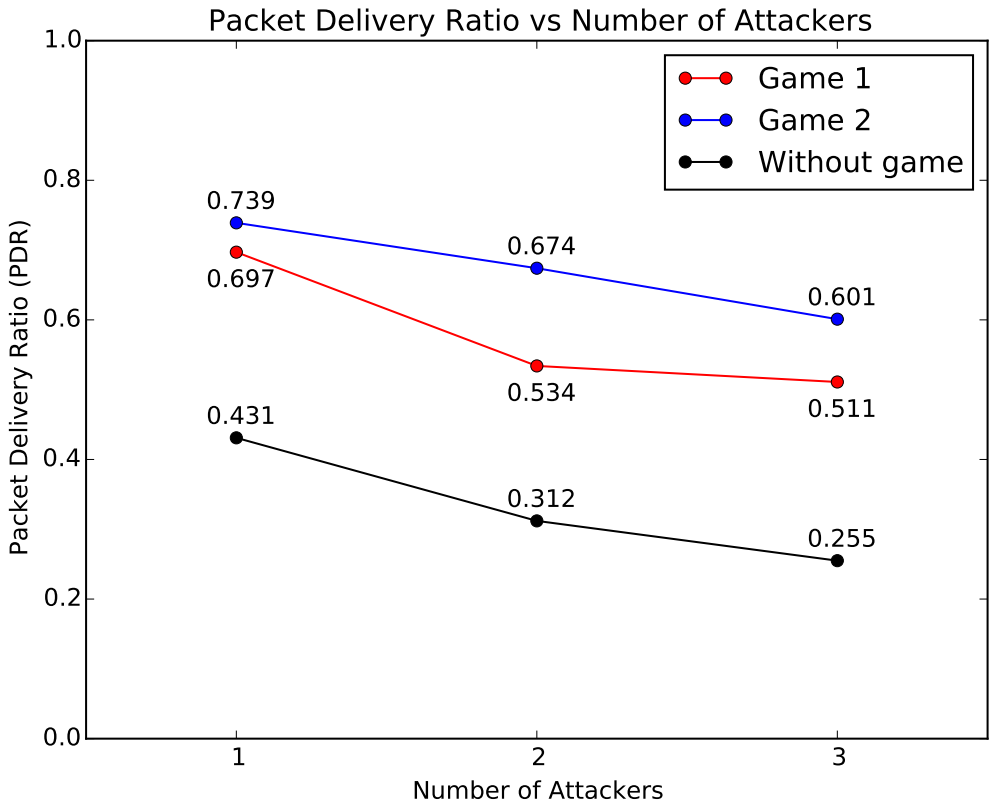


Figure 6.5. The Packet Delivery Ratio (PDR)

Obtained results for the two simulated games are summarized in figures 6.5 and 6.6. Both *PDR* and *POV* are a network performance metrics and they allow us to evaluate the accuracy of the reaction scheme. Our results are based on averaging the measurements obtained from 10 simulation runs.

In Figure 6.5, we plot the packet delivery ratio obtained when using game 1 or game 2 as a reaction strategy to the case where no reaction strategy is used. At the same time, we vary the number of attackers from 1 to 3. We can clearly observe that increasing the number of attackers leads to reduce the packet delivery ratio. However, the most interesting observation is that both our reaction games outperform the case where no reaction strategy is adopted. Finally, we note also that the game 2 is slightly better than game one. This is due to the fact that in the game 2 the honest vehicles have more response strategies than the honest vehicles in game 1. This will offer them more chance to govern and have more opportunity to achieve maximum payoff.

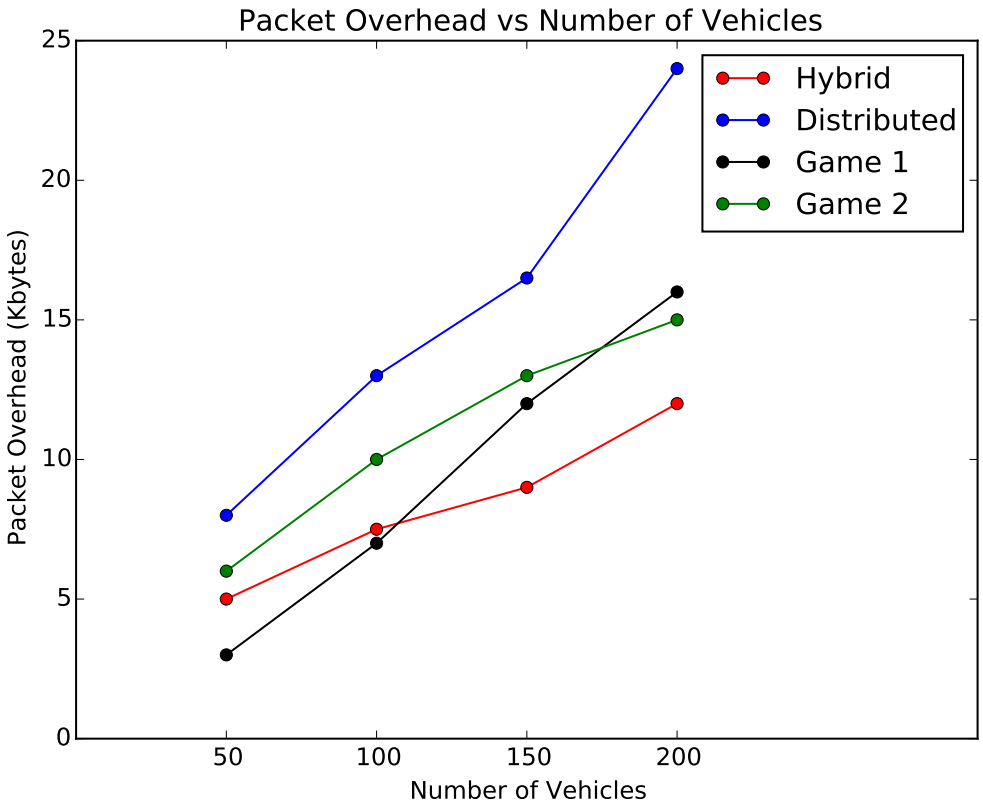


Figure 6.6. The Packet Overhead (POV)

In Figure 6.6 we compare the Packet Overhead of our games to the scheme proposed in [124]. To the best of our knowledge, it is the best one to which we can compare. We notice that for similar comparison conditions (i.e. the same number of vehicles), the packet overhead of our two reaction schemes outperform their distribution scheme and underperform their hybrid scheme. It should be noted that the schemes to which we compare are preventive games and not a pure reaction strategies.

6.5 Conclusion

In this chapter we have addressed the denial of service attack reaction problem in vehicular networks. For this purpose, we have proposed a new security games based model and verified our proposal by various appropriate simulations. Our contributions are: First, we

have provided a new security games formalism for Denial of service attacks in VANETs. Second, we have designed two possible games' scenarii: (*i*) *strategic-form game* (simultaneous decisions) and (*ii*) *extensive-form game* (consecutive decisions). Third, we have studied the DOS attack under realistic assumptions such as the use of real mobility models based on realistic map. Finally, we evaluated our proposed games by simulations. We believe these contributions to be very useful for solving the denial of service attack reaction problem in vehicular networks. As a future work, we intend to study the possibility to design a new reaction algorithm against DOS attacks in VANET based on a cooperative game, which is considered as a challenging problem.

⁂ ⁂ ⁂ ⁂ ⁂

CHAPTER 7

CONCLUSION AND PERSPECTIVES

Contents

7.1 Conclusion

The goal of the current research was to devise, analyze, and evaluate security solutions for DoS attacks conducted against VANETs. The major outcomes consisted in the design of both *detection* and *reaction* algorithms against these attacks.

A review study was achieved in order to provide the latest recent advances in vehicular networks, and more specifically the works related to their security. We studied the physical and the MAC layer protocols, as well as related standards. We also classified the VANETs vulnerabilities and attacks, from a cryptographic point of view depending on the affected service. This classification allowed us to provide and evaluate the possible cryptographic solutions for each family of threats. We approved that a wide range of VANET security challenges can be solved by cryptography. In the same direction, we addressed in our first contribution the problem of secure group communications in VANETs. Our proposal was a new secure *Diffie-Hellman* based variant algorithm for groups key generation that we fortified by a pre-shared secret to withstand the famous *Man in the Middle* attack. As necessary, our proposal can be used by several types of authentication and encryption VANET applications.

Our Denial of service attack detection proposed methods have been presented respectively in chapter 4 and 5. First, we have proposed a new linear regression and fuzzy logic based detection scheme. This scheme divided into suspicion and decision phases, is able to detect if the VANET network is under DoS attack or not. For this effect we have defined three new metrics and we have focused especially on greedy behavior attack. Second, In the same axis, we have proposed a new Shannon Entropy based scheme for VANETs DoS attack detection. We define "Packets entropy" as a new metric to measure the entropy of chosen family of exchanged packets in VANET network. In fact, the entropy of normal network (not under attack) is too different (higher) from the entropy of network under DoS attack. Based on this principle, our method is not related to the type a attack (generic). The both proposed algorithms presented the advantages of rapidity and does not require any MAC protocol modification.

Finally, the latest contribution of this dissertation related to the reaction against VANETs DoS attacks, have been proposed in 6. We have proposed a game theory based reaction scheme. Basically, a network under attack can be considered as game between hon-

est nodes and attackers nodes. Using this principle we have designed two non-cooperative security games which allowed to avoid and mitigate attack effects.

In conclusion, the current research has *Studied*, *evaluated* and *proposed* several solutions for the denial of service (DoS) attacks in vehicular networks. We believe these contributions to be very useful to solve or mitigate the mentioned problem. A series of experimental results and comparison with existing approaches coming from literature are performed and it showed an impressed result for our proposals.

7.2 Future work

In the course of the research carried out for this thesis a number of possible directions for further possible research directions have been identified. Relating to different parts of this thesis, they can be divided into two separate sections.

For cryptographic solutions Even though an important interest has been given by the research community to this topic, it is noteworthy that the use of new cryptographic concepts, including homomorphic encryption and ID-based cryptography, has to be more efficiently exploited in other future works to cover the weaknesses of the existing schemes and adapt to the intrinsic features of vehicular communication. Thus, our research serves as one step closer towards the design and development of effective security schemes to support the protection of critical services based on VANETs.

For detection and reaction algorithms First, work in these research axis are very few. Secondly, we also noticed that practically the proposed solutions are dependent on types of attacks that we have tried to overcome by our "entropy" based scheme. Complexity is the enemy of security. If for each type of attack, we must develop an independent algorithm: a complete solution for securing a VANET network will be quite complicated to implement. Further work should be focused on finding a metric that does not depend on the type of attack. Identifying these deficiencies would make space for further improvements.

⁂ ⁂ ⁂ ⁂ ⁂

Acronyms

List of Acronyms

AC Access category

AC0 or BK Background traffic

AC1 or BE Best Effort traffic

AC3 or VI Video traffic

AC3 or VO Voice traffic

AIFS Arbitration Inter-Frame Space

BER Bit Error Rate

CBR Constant Bit Rate

CCH Control CHannel

CSMA/CA Carrier Sense Multiple Access with Collision Avoidance

CTS Clear To Send

DCF Distributed Coordination Function

DSRC Dedicated Short Range Communications

DoS Denial of Service

DSRC Dedicated Short Range Communications

ECN Electronic Chassis Number

EDCA Enhanced Distributed Channel Access

ELP Electronic License Plate

ETSI European Telecommunications Standards Institute

FCC Federal Communication Commission

GDH Group Diffie-Hellman

GDVAN Greedy Detection for VANETs

GKMP Group Key Managment Protocol

GPS Global Positioning System

IP Internet Protocol

ITS Intelligent Transportation System

IVC Inter-Vehicle Communications

MAC Medium Access Control

MANETs Mobile Ad hoc NETworks

MiM Man in the Middle

NAV Network Allocation Vector

ns-3 Network Simulator 3

OBU On Board Unit

OFDM Orthogonal Frequency Division Multiplexing

OSI Open System Interconnection

PDR Packets Delivery Ratio

RSU Road Side Unit

RTS Request To Send

SCH Service CHannels

SNR Signal Noise Ratio

SUMO Simulation of Urban Mobility

TPM Trusted Platform Module

TTP Trusted Third Party

V2V Vehicle to Vehicle

V2I Vehicle to Infrastructure

VA Validation Authority

VANETs Vehicular Ad hoc NETworks

WAVE Wireless Access in Vehicular Environments

WIBSS Wave Independent Basic Service Set

WLAN Wireless LAN

WMN Wireless Mesh Networks

WSMP Wave Short Message Protocol

WSN Wireless Sensor Networks

List of Tables

List of Figures

Bibliography

[1] Maxim Raya and Jean-Pierre Hubaux. Securing vehicular ad hoc networks. *Journal of Computer Security*, 15(1):39–68, 2007.

[2] Jeremy Blum and Azim Eskandarian. The threat of intelligent collisions. *IT professional*, 6(1):24–29, 2004.

[3] O Trullols, Marco Fiore, Claudio Casetti, Carla-Fabiana Chiasserini, and José M Barcelo Ordinas. Planning roadside infrastructure for information dissemination in intelligent transportation systems. *Computer Communications*, 33(4):432–442, 2010.

[4] Subir Biswas, Jelena Misic, and Vojislav Misic. Ddos attack on wave-enabled vanet through synchronization. In *Global Communications Conference (GLOBECOM), 2012 IEEE*, pages 1079–1084. IEEE, 2012.

[5] Anup Dhamgaye and Nekita Chavhan. Survey on security challenges in vanet. *International Journal of Computer Science*, 2, 2013.

[6] Maxim Raya, Panos Papadimitratos, and J-P Hubaux. Securing vehicular communications. *Wireless Communications, IEEE*, 13(5):8–15, 2006.

[7] Bharati Mishra, Priyadarshini Nayak, Subhashree Behera, and Debasish Jena. Security in vehicular adhoc networks: a survey. In *Proceedings of the 2011 International Conference on Communication, Computing & Security*, pages 590–595. ACM, 2011.

[8] Sherali Zeadally, Ray Hunt, Yuh-Shyan Chen, Angela Irwin, and Aamir Hassan. Vehicular ad hoc networks (vanets): status, results, and challenges. *Telecommunication Systems*, 50(4):217–241, 2012.

[9] Mohammed Saeed Al-kahtani. Survey on security attacks in vehicular ad hoc networks (vanets). In *Signal Processing and Communication Systems (ICSPCS), 2012 6th International Conference on*, pages 1–9. IEEE, 2012.

[10] Irshad Ahmed Sumra, Iftikhar Ahmad, Halabi Hasbullah, and J-L bin Ab Manan. Behavior of attacker and some new possible attacks in vehicular ad hoc network (vanet). In *Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2011 3rd International Congress on*, pages 1–8. IEEE, 2011.

[11] Maria Elsa Mathew and Arun Raj Kumar P. Threat analysis and defence mechanisms in vanet. *International Journal of Advanced Research in Computer Science and Software Engineering*, 3(1), 2013.

[12] Ajay Rawat, Santosh Sharma, and Rama Sushil. Vanet: Security attacks and its possible solutions. *Journal of Information and Operations Management*, 3(1):301–304, 2012.

[13] José María de Fuentes, Ana Isabel González-Tablas, and Arturo Ribagorda. Overview of security issues in vehicular ad-hoc networks. 2010.

[14] Bin Xiao, Bo Yu, and Chuanshan Gao. Detection and localization of sybil nodes in vanets. In *Proceedings of the 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks*, pages 1–8. ACM, 2006.

[15] Philippe Golle, Dan Greene, and Jessica Staddon. Detecting and correcting malicious data in vanets. In *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*, pages 29–37. ACM, 2004.

[16] Irshad Ahmed Sumra, JAMALUL-LAIL AB MANAN, and Halabi Hasbullah. Timing attack in vehicular network. In *Proceedings of the 15th WSEAS international conference on Computers*, pages 151–155. World Scientific and Engineering Academy and Society (WSEAS), 2011.

[17] Seyed Mohammad Safi, Ali Movaghar, and Misagh Mohammadizadeh. A novel approach for avoiding wormhole attacks in vanet. In *Internet, 2009. AH-ICI 2009. First Asian Himalayas International Conference on*, pages 1–6. IEEE, 2009.

[18] S RoselinMary, M Maheshwari, and M Thamaraiselvan. Early detection of dos attacks in vanet using attacked packet detection algorithm (apda). In *Information Communication and Embedded Systems (ICICES), 2013 International Conference on*, pages 237–240. IEEE, 2013.

[19] Li He and Wen Tao Zhu. Mitigating dos attacks against signature-based authentication in vanets. In *Computer Science and Automation Engineering (CSAE), 2012 IEEE International Conference on*, volume 3, pages 261–265. IEEE, 2012.

[20] Adil Mudasir Malla and Ravi Kant Sahu. Security attacks with an effective solution for dos attacks in vanet. *International Journal of Computer Applications*, 66(22), 2013.

[21] Sapna S Kaushik. Review of different approaches for privacy scheme in vanets. *International Journal*, 5, 2013.

[22] Lutz Gollan, Iur Lutz Gollan, and Christoph Meinel. Digital signatures for automobiles. In *in Systemics, Cybernetics and Informatics (SCI.* Citeseer, 2002.

[23] Mohamed Nidhal Mejri, Jalel Ben-Othman, and Mohamed Hamdi. Survey on vanet security challenges and possible cryptographic solutions. *Vehicular Communications*, 1(2):53–66, 2014.

[24] ONISR. Onisr-bilan provisoire 2012, http://www.securite-routiere.gouv.fr/. 2013.

[25] Jean-Pierre Hubaux, Srdjan Capkun, and Jun Luo. The security and privacy of smart vehicles. *Security & Privacy, IEEE*, 2(3):49–55, 2004.

[26] DSRC. Dsrc, http://grouper.ieee.org/groups/scc32/dsrc/. 2013.

[27] 802.11p-2010 - ieee standard for information technology - local and metropolitan area networks - specific requirements - part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications amendment 6: Wireless access in vehicular environments. 11 June 2010.

[28] ETSI. European telecommunications standards institute (etsi)), http://www.etsi.org. 2013.

[29] ITS. Its standars fact sheets of ieee, http://www.standards.its.dot.gov/factsheets/factsheet/80 seen october 19 2013. 2013.

[30] 802.11-2007 - ieee standard for information technology - telecommunications and information exchange between systems - local and metropolitan area networks - specific requirements - part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications. IEEE STANDARD, 12 June 2007.

[31] Lusheng Miao, Karim Djouani, Barend J van Wyk, and Yskandar Hamam. Evaluation and enhancement of ieee 802.11 p standard: A survey. *Mobile Computing*, 2012.

[32] Ali Hamieh, Jalel Ben-Othman, and Lynda Mokdad. Detection of radio interference attacks in vanet. In *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE*, pages 1–5. IEEE, 2009.

[33] Jihene Rezgui, Soumaya Cherkaoui, and Omar Chakroun. Deterministic access for dsrc/802.11 p vehicular safety communication. In *Wireless Communications and Mobile Computing Conference (IWCMC), 2011 7th International*, pages 595–600. IEEE, 2011.

[34] Md Shohrab Hossain and Mohammed Atiquzzaman. Stochastic properties and application of city section mobility model. In *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE*, pages 1–6. IEEE, 2009.

[35] Tracy Camp, Jeff Boleng, and Vanessa Davies. A survey of mobility models for ad hoc network research. *Wireless communications and mobile computing*, 2(5):483–502, 2002.

[36] Atulya Mahajan, Niranjan Potnis, Kartik Gopalan, and Andy Wang. Urban mobility models for vanets. In *2nd IEEE International Workshop on Next Generation Wireless Networks*, 2006.

[37] David R Choffnes and Fabián E Bustamante. An integrated mobility and traffic model for vehicular wireless networks. In *Proceedings of the 2nd ACM international workshop on Vehicular ad hoc networks*, pages 69–78. ACM, 2005.

[38] Jun Luo and Jean-Pierre Hubaux. A survey of inter-vehicle communication. *EPFL, Lausanne, Switzerland, Tech. Rep*, 2004.

[39] Jagadeesh Kakarla, S Siva Sathya, B Govinda Laxmi, and B Ramesh Babu. A survey on routing protocols and its issues in vanet. *International Journal of Computer Applications*, 28(4), 2011.

[40] Liana Khamis Qabajeh, Miss Laiha Mat Kiah, and Mohammad Moustafa Qabajeh. A scalable and secure position-based routing protocols for ad-hoc networks. *Malaysian Journal of Computer Science*, 22(2):99–120, 2009.

[41] Angeline G Dludla, Ntsibane Ntlatlapa, T Nyandeni, and Matthew Adigun. Towards designing energy-efficient routing protocol for wireless mesh networks. 2009.

[42] Floriano De Rango, Juan-Carlos Cano, Marco Fotino, Carlos Calafate, Pietro Manzoni, and Salvatore Marano. Olsr vs dsr: A comparative analysis of proactive and reactive mechanisms from an energetic point of view in wireless ad hoc networks. *Computer Communications*, 31(16):3843–3854, 2008.

[43] Thomas Clausen, Philippe Jacquet, Cédric Adjih, Anis Laouiti, Pascale Minet, Paul Muhlethaler, Amir Qayyum, Laurent Viennot, et al. Optimized link state routing protocol (olsr). 2003.

[44] Mazlan Osman. The performance of AODV routing protocol based on dropped packet and throughput metrics: A simulation and comparative study for VANET. *International Journal of Management & Information Technology*, 4(2):265–279, 2013.

[45] Zhigang Wang, Lichuan Liu, MengChu Zhou, and Nirwan Ansari. A position-based clustering technique for ad hoc intervehicle communication. *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on*, 38(2):201–208, 2008.

[46] Rahul Jain, Anuj Puri, and Raja Sengupta. Geographical routing using partial information for wireless ad hoc networks. *Personal Communications, IEEE*, 8(1): 48–57, 2001.

[47] Hamidreza Rahbar, Kshirasagar Naik, and Amiya Nayak. Dtsg: Dynamic time-stable geocast routing in vehicular ad hoc networks. In *Ad Hoc Networking Workshop (Med-Hoc-Net), 2010 The 9th IFIP Annual Mediterranean*, pages 1–7. IEEE, 2010.

[48] C2C-CC. Car2car project, http://www.car-2-car.org/. 2013.

[49] Bertrand Ducourthial, Farah El Ali, et al. Architecture pour communication véhicules-infrastructure. In *CFIP'2009*, 2009.

[50] Krishna Sampigethaya, Leping Huang, Mingyan Li, Radha Poovendran, Kanta Matsuura, and Kaoru Sezaki. Caravan: Providing location privacy for vanet. Technical report, DTIC Document, 2005.

[51] Halabi Hasbullah, Irshad Ahmed Soomro, and Jamalul-lail Ab Manan. Denial of service (dos) attack and its possible solutions in vanet. *World Academy of Science, Engineering and Technology (WASET)*, 65:411–415, 2010.

[52] Shie-Yuan Wang, Chih-Che Lin, Kuang-Che Liu, and Wei-Jyun Hong. On multi-hop forwarding over wbss-based ieee 802.11 (p)/1609 networks. In *Personal, Indoor and Mobile Radio Communications, 2009 IEEE 20th International Symposium on*, pages 3040–3044. IEEE, 2009.

[53] Josep Domingo-Ferrer and Qianhong Wu. Safety and privacy in vehicular communications. In *Privacy in Location-Based Applications*, pages 173–189. Springer, 2009.

[54] ETSI. Intelligent transport systems (its), security, threat, vulnerability and risk analysis(tvra). *ETSI TR 102 893 V1.1.1 (2010-03), Technical Report*, 2010.

[55] Brouce Schneier. *Applied cryptography. Protocols, Algorithms, and Source Code in C.* John Wiley & Sons, Inc, 1996.

[56] Dave Singelee and Bart Preneel. Location verification using secure distance bounding protocols. In *Mobile Adhoc and Sensor Systems Conference, 2005. IEEE International Conference on*, pages 7–pp. IEEE, 2005.

[57] Levente Buttyan and Jean-Pierre Hubaux. *Security and cooperation in wireless networks: thwarting malicious and selfish behavior in the age of ubiquitous computing.* Cambridge University Press, 2008.

[58] Rashid Minhas and Muhammas Tilal. Effects of jamming on ieee 802.11 p systems. 2010.

[59] Ali Hamieh, Jalel Ben-Othman, Abdelhak Gueroui, and Farid Naït-Abdesselam. Detecting greedy behaviors by linear regression in wireless ad hoc networks. In *Communications, 2009. ICC'09. IEEE International Conference on*, pages 1–6. IEEE, 2009.

[60] Michele Nogueira Lima, Helber Wagner da Silva, Aldri Luiz dos Santos, and Guy Pujolle. A security management architecture for supporting routing services on wanets.

[61] Adam Burg. Ad hoc network specific attacks. In *Seminar Ad hoc networking: Concepts, Applications, and Security. Technische Universitat Munchen,2003*, 2003.

[62] Waldir Ribeiro Pires Jr, Thiago H de Paula Figueiredo, Hao Chi Wong, and Antonio Alfredo Ferreira Loureiro. Malicious node detection in wireless sensor networks. In *Parallel and Distributed Processing Symposium, 2004. Proceedings. 18th International*, page 24. IEEE, 2004.

[63] John R Douceur. The sybil attack. In *Peer-to-peer Systems*, pages 251–260. Springer, 2002.

[64] Bryan Parno and Adrian Perrig. Challenges in securing vehicular networks. In *Workshop on hot topics in networks (HotNets-IV)*, pages 1–6, 2005.

[65] Saira Gillani, Farrukh Shahzad, Amir Qayyum, and Rashid Mehmood. A survey on security in vehicular ad hoc networks. In *Communication Technologies for Vehicles*, pages 59–74. Springer, 2013.

[66] Colin Boyd. On key agreement and conference key agreement. In *Information Security and Privacy*, pages 294–302. Springer, 1997.

[67] Michael Steiner, Gene Tsudik, and Michael Waidner. Diffie-hellman key distribution extended to group communication. In *Proceedings of the 3rd ACM conference on Computer and communications security*, pages 31–37. ACM, 1996.

[68] Michael Steiner, Michael Waidner, and Gene Tsudik. Cliques: A new approach to group key agreement. In *2013 IEEE 33rd International Conference on Distributed Computing Systems*, pages 380–380. IEEE Computer Society, 1998.

[69] Stefano Busanelli, Gianluigi Ferrari, and Luca Veltri. Short-lived key management for secure communications in vanets. In *ITS Telecommunications (ITST), 2011 11th International Conference on*, pages 613–618. IEEE, 2011.

[70] Suranjan Choudhury, Kartik Bhatnagar, and Wasim Haque. *Public key infrastructure implementation and design.* John Wiley & Sons, Inc., 2002.

[71] Mahmoud Al-Qutayri, Chan Yeun, and Faisal Al-Hawi. Security and privacy of intelligent vanets. 2010.

[72] Lutz Gollan, Iur Lutz Gollan, and Christoph Meinel. Digital signatures for automobiles?! In *in Systemics, Cybernetics and Informatics (SCI.* Citeseer, 2002.

[73] M. N. Mejri, N. Achir, and M. Hamdi. A new group diffie-hellman key generation proposal for secure VANET communications. In *2016 13th IEEE Annual Consumer Communications Networking Conference (CCNC)*, pages 992–995, Jan 2016. doi: 10.1109/CCNC.2016.7444925.

[74] Mohamed Nidhal Mejri and Mohamed Hamdi. Recent advances in cryptographic solutions for vehicular networks. In *Networks, Computers and Communications (ISNCC), 2015 International Symposium on*, pages 1–7. IEEE, 2015.

[75] Philipp Wex, Jochen Breuer, Albert Held, T Leinmuller, and Luca Delgrossi. Trust issues for vehicular ad hoc networks. In *Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE*, pages 2800–2804. IEEE, 2008.

[76] Matthias Gerlach. Trust for vehicular applications. In *Autonomous Decentralized Systems, 2007. ISADS'07. Eighth International Symposium on*, pages 295–304. IEEE, 2007.

[77] Umar Farooq Minhas, Jie Zhang, Thomas Tran, and Robin Cohen. Towards expanded trust management for agents in vehicular ad-hoc networks. *International Journal of Computational Intelligence Theory and Practice (IJCITP)*, 5(1), 2010.

[78] Stefan Brands and David Chaum. Distance-bounding protocols. In *Advances in CryptologyEUROCRYPT93*, pages 344–359. Springer, 1994.

[79] Marko Wolf. Vehicular security mechanisms. In *Security Engineering for Vehicular IT Systems*, pages 121–165. Springer, 2009.

[80] Giuseppe Ateniese, Michael Steiner, and Gene Tsudik. New multiparty authentication services and key agreement protocols. *Selected Areas in Communications, IEEE Journal on*, 18(4):628–639, 2000.

[81] Giuseppe Ateniese, Michael Steiner, and Gene TsudiK. Authenticated group key agreement and friends. In *Proceedings of the 5th ACM conference on Computer and communications security*, pages 17–26. ACM, 1998.

[82] Whitfield Diffie and Martin E Hellman. New directions in cryptography. *Information Theory, IEEE Transactions on*, 22(6):644–654, 1976.

[83] Mark Manulis. Survey on security requirements and models for group key exchange. *IACR Cryptology ePrint Archive*, 2006:388, 2006.

[84] Sandro Rafaeli and David Hutchison. A survey of key management for secure group communication. *ACM Computing Surveys (CSUR)*, 35(3):309–329, 2003.

[85] T HARDJONO and B WLIS. Rfc 3740. *The multicast group security architecture*, 2004.

[86] Mark Baugher, Ran Canetti, L Dondeti, and Fredrik Lindholm. Multicast security (msec) group key management architecture. *Internet Engineering Task Force, RFC*, 4046, 2005.

[87] Alfred J Menezes, Paul C Van Oorschot, and Scott A Vanstone. *Handbook of applied cryptography*. CRC press, 1996.

[88] Ralph C Merkle. Secure communications over insecure channels. *Communications of the ACM*, 21(4):294–299, 1978.

[89] Ueli M Maurer and Stefan Wolf. The relationship between breaking the diffie–hellman protocol and computing discrete logarithms. *SIAM Journal on Computing*, 28(5): 1689–1721, 1999.

[90] Douglas R Stinson. *Cryptography: theory and practice*. CRC press, 2005.

[91] Aaron C Geary. Analysis of a man-in-the-middle attack on the diffie-hellman key exchange protocol. Technical report, DTIC Document, 2009.

[92] NS-3. ns-3, http:// www.nsnam.org/. 2013.

[93] Simulation of urban mobility, http:// sumo.sourceforge.net/. 2013.

[94] Maxim Raya, Jean-Pierre Hubaux, and Imad Aad. Domino: a system to detect greedy behavior in ieee 802.11 hotspots. In *Proceedings of the 2nd international conference on Mobile systems, applications, and services*, pages 84–97. ACM, 2004.

[95] 1609.4-2010 - ieee standard for wireless access in vehicular environments (wave)–multi-channel operation (revision of ieee std 1609.4-2006). 7 February 2011.

[96] Yi Wang, Akram Ahmed, Bhaskar Krishnamachari, and Konstantinos Psounis. Ieee 802.11 p performance evaluation and protocol enhancement. In *Vehicular Electronics and Safety, 2008. ICVES 2008. IEEE International Conference on*, pages 317–322. IEEE, 2008.

[97] 1609.4-2006 - ieee trial-use standard for wireless access in vehicular environments (wave)multi-channel operation. 29 November 2006.

[98] Pierre-andre Cornillon and Éric Matzner-Løber. *Régression: théorie et applications*. Springer, 2006.

[99] Pradeep Kyasanur and Nitin H Vaidya. Detection and handling of mac layer misbehavior in wireless networks. In *DSN*, pages 173–182. Citeseer, 2003.

[100] Alvaro A Cardenas, Svetlana Radosavac, and John S Baras. Detection and prevention of mac layer misbehavior in ad hoc networks. In *Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks*, pages 17–22. ACM, 2004.

[101] Jerzy Konorski. Multiple access in ad-hoc wireless lans with noncooperative stations. In *NETWORKING*, pages 1141–1146. Springer, 2002.

[102] Allen B MacKenzie and Stephen B Wicker. Stability of multipacket slotted aloha with selfish users and perfect information. In *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, volume 3, pages 1583–1590. IEEE, 2003.

[103] Sonja Buchegger, Cedric Tissieres, and Jean-Yves Le Boudec. A test-bed for misbehavior detection in mobile ad-hoc networks-how much can watchdogs really do? In *Mobile Computing Systems and Applications, 2004. WMCSA 2004. Sixth IEEE Workshop on*, pages 102–111. IEEE, 2004.

[104] Sonja Buchegger and Jean-Yves Le Boudec. Performance analysis of the confidant protocol. In *Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing*, pages 226–236. ACM, 2002.

[105] Soufiene Djahel and Farid Naït-Abdesselam. Flsac: A new scheme to defend against greedy behavior in wireless mesh networks. *International Journal of Communication Systems*, 22(10):1245–1266, 2009.

[106] Mohamed Nidhal Mejri and Jalel Ben-Othman. Detecting greedy behavior by linear regression and watchdog in vehicular ad hoc networks. In *Global Communications Conference (GLOBECOM), 2014 IEEE*, pages 5032–5037. IEEE, 2014.

[107] Lotfi A Zadeh. Fuzzy sets. *Information and control*, 8(3):338–353, 1965.

[108] KLIR GEORGE J and Yuan Bo. Fuzzy sets and fuzzy logic, theory and applications. -, 2008.

[109] Kevin M Passino and Stephen Yurkovich. *Fuzzy control*, volume 42. Citeseer, 1998.

[110] 1609.3-2010 - ieee standard for wireless access in vehicular environments (wave)networking services (revision of ieee std 1609.3-2007). 30 December 2010.

[111] Francisco J Martinez, Chai Keong Toh, Juan-Carlos Cano, Carlos T Calafate, and Pietro Manzoni. A survey and comparative study of simulators for vehicular ad hoc networks (vanets). *Wireless Communications and Mobile Computing*, 11(7):813–828, 2011.

[112] Amit Kumar Saha and David B Johnson. Modeling mobility for vehicular ad-hoc networks. In *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*, pages 91–92. ACM, 2004.

[113] Feliz K Karnadi, Zhi Hai Mo, and Kun-chan Lan. Rapid generation of realistic mobility models for vanet. In *Wireless Communications and Networking Conference, 2007. WCNC 2007. IEEE*, pages 2506–2511. IEEE, 2007.

[114] Mohamed Nidhal Mejri and Jalel Ben-Othman. Entropy as a new metric for denial of service attack detection in vehicular ad-hoc networks. In *Proceedings of the 17th ACM international conference on Modeling, analysis and simulation of wireless and mobile systems*, pages 73–79. ACM, 2014.

[115] Claude E Shannon and Warren Weaver. The mathematical theory of communication (urbana, il. *University of Illinois Press*, 19(7):1, 1949.

[116] Geethapriya Thamilarasu, Sumita Mishra, and Ramalingam Sridhar. Improving reliability of jamming attack detection in ad hoc networks. *International Journal of Communication Networks & Information Security*, 3(1), 2011.

[117] Anh Tuan Nguyen, Lynda Mokdad, and Jalel Ben Othman. Solution of detecting jamming attacks in vehicle ad hoc networks. In *Proceedings of the 16th ACM international conference on Modeling, analysis & simulation of wireless and mobile systems*, pages 405–410. ACM, 2013.

[118] Rajani Muraleedharan and Lisa A Osadciw. Jamming attack detection and countermeasures in wireless sensor network using ant system. pages 62480G–62480G, 2006.

[119] Carmen Cerasoli and James Dimarogonas. The generalization of information entropy to manet metrics. In *Military Communications Conference, 2008. MILCOM 2008. IEEE*, pages 1–9. IEEE, 2008.

[120] M. N. Mejri, N. Achir, and M. Hamdi. A new security games based reaction algorithm against DoS attacks in VANETs. In *2016 13th IEEE Annual Consumer Communications Networking Conference (CCNC)*, pages 837–840, Jan 2016. doi: 10.1109/CCNC.2016.7444896.

[121] Mark Felegyhazi and Jean-Pierre Hubaux. Game theory in wireless networks: A tutorial. Technical report, 2006.

[122] Tansu Alpcan and Sonja Buchegger. Security games for vehicular networks. *Mobile Computing, IEEE Transactions on*, 10(2):280–290, 2011.

[123] Mario Cagalj, Saurabh Ganeriwal, Imad Aad, and J-P Hubaux. On selfish behavior in csma/ca networks. In *INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE*, volume 4, pages 2513–2524. IEEE, 2005.

[124] Hichem Sedjelmaci, Tarek Bouali, and Sidi Mohammed Senouci. Detection and prevention from misbehaving intruders in vehicular networks. In *Global Communications Conference (GLOBECOM), 2014 IEEE*, pages 39–44. IEEE, 2014.

[125] Sankardas Roy, Charles Ellis, Sajjan Shiva, Dipankar Dasgupta, Vivek Shandilya, and Qishi Wu. A survey of game theory as applied to network security. In *System Sciences (HICSS), 2010 43rd Hawaii International Conference on*, pages 1–10. IEEE, 2010.

[126] IEEE. 1609.2-2013 - ieee standard for wireless access in vehicular environments security services for applications and management messages. 2013.