الجمهورية الجزائرية الديمقراطية الشعبية

Ministry of Higher Education and Scientific Research

UNIVERSITY YAHIA FARES OF MEDEA

Faculty of Science

Department of Mathematics and Computer Science



Trustworthy in Vehicular Social Networks (VSNs)

Approach for the optimal exploration of the Vehicular Social Network (VSN).

THESIS OF MASTER ISTW 2019/2020

Presented by:

Abdelhak ZOUBIRI

Under the direction of:

M. Abdellah KACI

&

M. Redha MAZARI

Yahia Fares university, computer science

Specialization in systems engineering and web technologies

Abstarct

Vehicular transportation is an essential part of modern cities. With the integration of the Internet of Vehicles and social networks, vehicular social networks (VSNs) are promising to make traffic management easier for commuters, and with wireless technology available on each car, it is expected that huge amounts of information will be exchanged between vehicles or between vehicles and roadside infrastructure or passengers. The issue is that it becomes harder for commuters to distinguish between trusty and nontrusty commuters especially with the sranger ones, so to increase the safety it is necessary to build a trustworthy system.

The aim of the study is to study and understand the vehicular social network and the trustworthy in VSN, the aim was to shed the light on a new reliable system model with a new methode that makes it easier to establish the trustwothy in the Vehicular Social Network VSN. The results of this study showed that the problem of achieving an indirect trust model mentioned in a previous study is in fact feasible.

In this report before we talk about the main concept of the work we need first to present the VSNs, the start of the VSN and describe it's architecure and applications, furthermore, we cover the part of the trust management in the VSNs and the recent research progress in measuring and modeling indirect trust in vehicular social networks.

Keywords: Vehicular transportation, Internet of vehicles, Social networks, vehicular social networks (VSNs), Trust.

Résumé

Le transport routier est un élément essentiel des villes modernes. Et avec l'intégration de l'Internet des véhicules et des réseaux sociaux, les réseaux sociaux véhiculaires (VSN) promettent de faciliter la gestion du trafic pour les navetteurs, et avec la technologie sans fil disponible sur chaque voiture, il est prévu que d'énormes quantités d'informations seront échangées entre véhicules ou entre les véhicules et les infrastructures routières ou les passagers. le problème est qu'il devient plus difficile pour les navetteurs de faire la distinction entre les navetteurs de confiance et ceux qui ne font pas confiance, en particulier avec les étrangers, donc pour augmenter la sécurité, il est nécessaire de construire un système de confiance.

Le but de l'étude est d'étudier et de comprendre le réseau social véhiculaire et les dignes de confiance dans VSN, l'objectif était de mettre en lumière un nouveau modèle de système fiable avec une nouvelle méthode qui facilite l'établissement du digne de confiance dans le réseau social des véhicules. VSN, Les résultats de cette étude ont montré que le problème de la réalisation d'un modèle de confiance indirecte mentionné dans une étude précédente est en fait faisable.

Dans ce rapport, avant de parler du concept principal du travail, nous devons d'abord présenter les VSN, le début du VSN et décrire son architecture et ses applications.En outre, nous couvrons la partie de la gestion de la confiance dans les VSN et les recherches récentes progrès dans la mesure et la modélisation de la confiance indirecte dans les réseaux sociaux véhiculaires.

الملخص

النقل بالسيارات جزء أساسي من المدن الحديثة. ومع تكامل إنترنت المركبات والشبكات الاجتماعية، تبشر شبكات التواصل الاجتماعي الخاصة بالمركبات بتسهيل إدارة حركة المرور للركاب ، ومع توفر التكنولوجيا اللاسلكية في كل سيارة ، من المتوقع أن يتم تبادل كميات هائلة من المعلومات بين المركبات أو بين المركبات والبنية التحتية على جانب الطريق أو الركاب.المسألة هي أنه يصبح من الصعب على الركاب التمييز بين الركاب المؤتمنين وغير الموثوق بهم خاصة مع أولئك الذين لا يثقون بهم ، لذلك لزيادة السلامة لا بد من بناء نظام جدير بالثقة.

الهدف من الدراسة هو دراسة وفهم الشبكة الاجتماعية للمركبات والجديرة بالثقة في الشبكات الاجتماعية للمركبات، وكان الهدف هو إلقاء الضوء على نموذج نظام جديد موثوق به مع طريقة جديدة تجعل من السهل إنشاء الثقة في الشبكة الاجتماعية للسيارات أظهرت نتائج هذه الدراسة أن مشكلة تحقيق نموذج الثقة غير المباشرة المذكورة في دراسة سابقة أنها ممكنة في الواقع.

في هذا التقرير قبل أن نتحدث عن المفهوم الرئيسي للعمل ، نحتاج أولاً إلى تقديم الشبكات الاجتماعية للمركبة ، وبداية الشبكة الاجتماعية للمركبة ووصف هيكلها وتطبيقاتها ، علاوة على ذلك ، نغطي جزء من إدارة الثقة في السيارة الشبكات الاجتماعية والتقدم البحثي الأخير في قياس ونمذجة الثقة غير المباشرة في الشبكات الاجتماعية للمركبات.

Acknowledgments

First and foremost, praises and thanks to the God, the Almighty, for His showers of blessing throught my research work to complete the research successfully.

I am over helmed in all humbleness and gratefulness to acknowledge my depth to all those who have helped me to put these ideas, I would like to express my deep and sincere gratitude to my research supervisor Mr.Kaci Abdellah and Mr.Redha Mazari for giving me the opportunity to do research and providing invaluable guidance throughout this research. which also helped me in doing a lot of Research and i came to know about so many new things I am really thankful to them.

I would like to express a special thanks of gratitude to Mr. Mohamed El amine Badjara and my friends Ramzi and Abdelrahmen that helped me a lot during my journey and without them I would never be able to do this work.

Finally, I would like to thank my friends and family for all their love and support during this time. I hope others will enjoy reading my work and hope it is interesting.

Table of contents

Abstract……2

Acknowledgement……5

Table of contents……6

Table of figures……9

List of tables……11

Abbreviations……12

Introduction……13

1. Introducion into the Vehicular Social Networks VSNs

1.1. Introduction……16
1.2. Internet of things (IoT)……16
1.2.1. What is the internet of things……16
1.2.2. History of IoT……17
1.2.3. IoT applications and domains……18
1.3. Vehicular Ad-hoc Networks (VANETs)…… 19
1.3.1. Definition……19
1.3.2. Smart vehicles……20
1.3.3. Applications in vehicular ad-hoc networks……21
1.4. The online social networks (OSN)……22
1.4.1. What is social networking……22
1.4.2. Social network history……23
1.4.3. How online social networking works……23
1.5. The Start of VSNs……24
1.5.1. From IoVs to VSNs……25
1.6. The vehciular social networks……26

2. Study of VSNs and it's architecture and applications

2.1. Introduction……28
2.2. VSNs architecture……28
2.2.1. The components of VSNs……28
2.2.2. The interaction between VSNs components……29
2.2.3. VSNs architecture's classification……30
2.2.4. VSN layer's……32
2.2.5. The architecture……34
2.3. The characteristics of VSNs……36
2.3.1. Between IoVs and VSNs……36
2.3.2. Between VSNs and OSNs……37
2.4. The applications of VSNs……38
2.5. Social connection between vehicles……40

3. Trust management in VSN

3.1. Introduction……44
3.2. Definition of trust management in VSN……44
3.3. Trust types in VSN……45
3.3.1. Direct trust in VSN……45
3.3.2. Indirect trust in VSN……45
3.4. The social connection tree (SCT)……46
3.5. The trust factors……48
3.6. Existing trust models……52
3.6.1. The Qing Yang and Honggang Wang study……53
3.6.2. The trust on the ratee system……54
3.6.3. The authenticated RFID security mechanism……56
3.6.4. Trust Management of service-oriented IoT Systems……57
3.7. Conclusion……58

4. The concept of the new trust model

4.1. Introduction……60
4.2. The network presentation……60
4.3. Intro into graph theory……60
4.3.1. Directed graph……61
4.4. Mathematical presentation of the problem……62
4.5. The system model……63
4.5.1. The Dijkstra's algorithm……63
4.5.2. The Recommended method for solving the problem……64
4.6. The mythodology……70
4.7. The presetnation of the software program……72
4.8. Conclusion……76

Conclusion and prequisites……77
Perspective……78
Personal review……79

Bibliography…… 80

Webography……81

Table of figures

Figure 1 IoT objects

Figure 2 VANETs' architecture

Figure 3 Online Social Networks OSNs

Figure 4 Physical communication between vehicles and RSUs

Figure 5 Physical communication architecture of VSNs

Figure 6 Centralized VSNs communication

Figure 7 Distributed VSNs applications

Figure 8 VSN's layers

Figure 9 Schematic diagram of VSNs

Figure 10 Applications of VSN categorized by physical and social distances

Figure 11 Illustration of a distributed vehicular social network construction

Figure 12 Trust factors for vehicular social networks

Figure 13 Scheme of Ratee-based Trust Management system

Figure 14 A directed graph with 10 vertices (or nodes) and 13 edges.

Figure 15 Graph of vehicular network

Figure 16 Dijkstra's algorithm implemented

Figure 17 Phase 0

Figure 18 Phase 1

Figure 19 Phase 3

Figure 20 Network example to apply the new formula

Figure 21 Dataset sample

Figure 22 User's input

Figure 23 The generated network

Figure 24 results of the input

Figure 25 Trust chart

List of tables

Table 1 Key features of IoV and VSN

Table 2 Difference between VSNs and MSNs.

Abbreviations

VSNs : Vehicular Social Networks

SIoVs : Social Internet of Vehicles

IoT : Internat of Things

VANET : Vehicular Ad-hoc NETwork

OSN : Online Social Networks

IoVs : Inetrnet of vehicles

V2V : Vehicle to Vehicle

RSU : Road Side Units

I. Introduction :

In the upcoming years, IoT-based technology will offer advanced levels of services and practically change the way people lead their daily lives. This new revolutionary concept integrated the transportation section which gives us a new term called the vehicular social networks (VSNs).

The transportation section is of great significance due to the rapidly increasing number of vehicles in big cities, which makes traffic management for smart cities rather challenging, With the rapid growth of smart devices and advent of advanced communication and computing capabilities, and while the VSN field is growing up every year, it will become popular within families and between close friends and makes it possible for drivers and passengers to communicate and socialize with other commuters on the roads.

With VSNs various information are exchanged between cars, including traffic jam, road constructions, incidents/crashes, road conditions and weather alerts, so it's important for a vehicle/driver to distinguish trustworthy from untrustworthy data. Vehicles sharing factual information with others are considered to be trustful, while those sending false information are distrustful.
It is possible for legitimate vehicles to send untrustworthy information due to defective sensors, computer viruses, and even for malicious reasons. Untrustworthy information sent by distrustful vehicles have the potential to become the most harmful data within a vehicular network. So the discovery of trustworthy services is the key to a secure and reliable VSN.

The authors Qing Yang and Honggang Wang in [4] faced a problem achieving a trsustworthy model and finding all the possible paths between two vehicles, Therefore, an interesting questions : What is trustworthy in vehicular social networks VSNs ? Is it possible to achieve a trustworthy vehicular social network model ? Is it possible to compute the trust value of the strangers vehicles ? Is it possible to find the most appropriate path (the one we obtain the trust value from it) between two strange vehicles ?

In this report, we aim to capture a clear image about the new concept applied to achieve a reliable system model in the Vehicular Soicia Network VSN.

This document, summarizing the work carried out, consists of four chapters. A first chapter, used to present a little introduction to the Vehicular Social Networks. A second chapter dedicated to define very clearly the VSN and describe it's architecture and applications. A third chapter focuses on the VSN trustworthy and it's types, also it shows the factors managing the trust, and presents an overview of exiting trust management models available in the literature. A fourth chapter, which present the new concept to calculate and distnguish between the trustworthy and non trustworthy vehicles by applying a reliable model. Finally we conclude our work with a general conclusion and a personal review.

Chapter 1

Introduction into the Vehicular Social Networks VSNs

1.1. Introduction :

A Vehicular Social Network (VSN) is a sub domain of the internet of things (IoT) and the social internet of things, VSN is an emerging field of communication where relevant concepts are being borrowed from two different disciplines vehicular ad-hoc networks (VANETs) and online social networks (OSNs) [1].
In this chapter we will talk about the very start of the VSN, we'll talk on each of the domains related to VSN such as the IoT, VANET and OSN, and the convergence from the internet of vehicles into the VSN.

1.2. Internet of things (IoT) :

1.2.1. What is the Internet of Things :

Definitions for the Internet of Things vary. According to McKinsey: "Sensors and actuators embedded in physical objects are linked through wired and wireless networks, often using the same Internet Protocol (IP) that connects the Internet. " [14].

The idea is that not only your computer and your smartphone can talk to each other, but also all the things around you. From connected homes and cities to connected cars and machines to devices that track an individual's behavior and use the data collected for new kind of services.

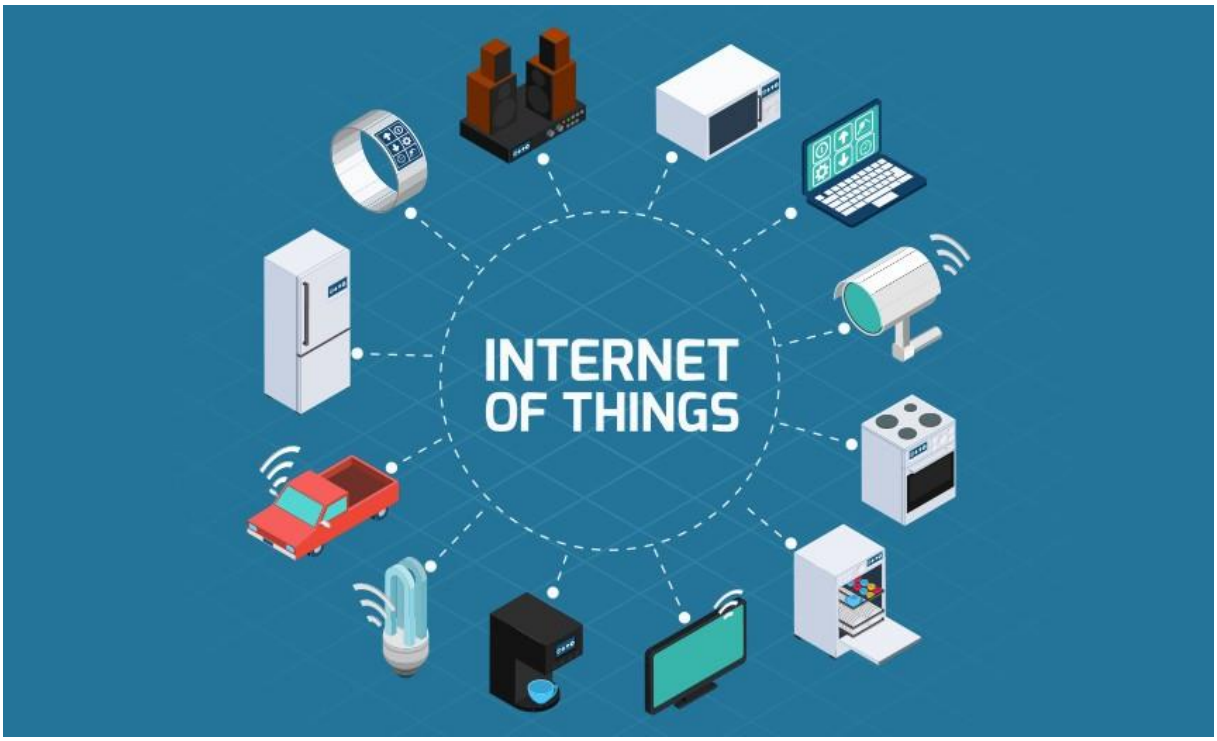


Figure 1: IoT objects.

According to Intel's report "Rise of the Embedded Internet" the Internet of things will involve a massive build-out of connected devices and sensors woven into the fabric of our lives and businesses. Devices deeply embedded in public and private places will recognize us and adapt to our requirements for comfort, safety, streamlined commerce, entertainment, education, resource conservation, operational efficiency and personal well-being.

1.2.2. History of IoT :

The term Internet of Things is 16 years old. But the actual idea of connected devices had been around longer, at least since the 70s. Back then, the idea was often called "embedded internet" or "pervasive computing". But the actual term "Internet of Things" was coined by Kevin Ashton in 1999 during his work at Procter&Gamble. Ashton who was working in supply chain optimization, wanted to attract senior management's attention to a new exciting technology called RFID.

Because the internet was the hottest new trend in 1999 and because it somehow made sense, he called his presentation “Internet of Things”.

Even though Kevin grabbed the interest of some P&G executives, the term Internet of Things did not get widespread attention for the next 10 years.

The concept of IoT started to gain some popularity in the summer of 2010. Information leaked that Google’s StreetView service had not only made 360 degree pictures but had also stored tons of data of people’s Wifi networks. People were debating whether this was the start of a new Google strategy to not only index the internet but also index the physical world.

The same year, the Chinese government announced it would make the Internet of Things a strategic priority in their Five-Year-Plan.

In 2011, Gartner, the market research company that invented the famous “hype-cycle for emerging technologies” included a new emerging phenomenon on their list: “The Internet of Things”.

The next year the theme of Europe’s biggest Internet conference the Web was the “Internet of Things”. At the same time popular tech-focused like Forbes, Fast Company, and Wired starting using IoT as their vocabulary to describe the phenomenon.

The term Internet of Things reached mass market awareness when in January 2014 Google announced to buy Nest for $3.2bn. At the same time the Consumer Electronics Show (CES) in Las Vegas was held under the theme of IoT.

1.2.3. IoT applications and domains :

To the public, IoT currently appears to be a mixture of smart home applications, wearables and an industrial IoT component. But actually it has the potential to have a much wider reach. When the connected

world becomes reality, the Internet of Things will transform nearly all major segments – from homes to hospitals and from cars to cities.

The extensive set of applications for IoT devices is often divided into many domains such as smart city , smart home, smart grids, medical and health care, manufacturing, agriculture,...etc

One of these domains is the transportation segment and the connected cars.

1.3. Vehicular Ad_hoc Networks (VANETs) :

1.3.1. Definition :

VANET is a type of networks that is created from the concept of establishing a network of cars for a specific need or situation. Vehicular ad-hoc networks have now been established as reliable networks that moving vehicles use for communication purpose on highways or urban environments.

A vehicle can communicate with another vehicle directly which is called Vehicle to Vehicle (V2V) communication, or a vehicle can communicate to an infrastructure such as a Road Side Unit (RSU), known as Vehicle-to-Infrastructure (V2I) [12].

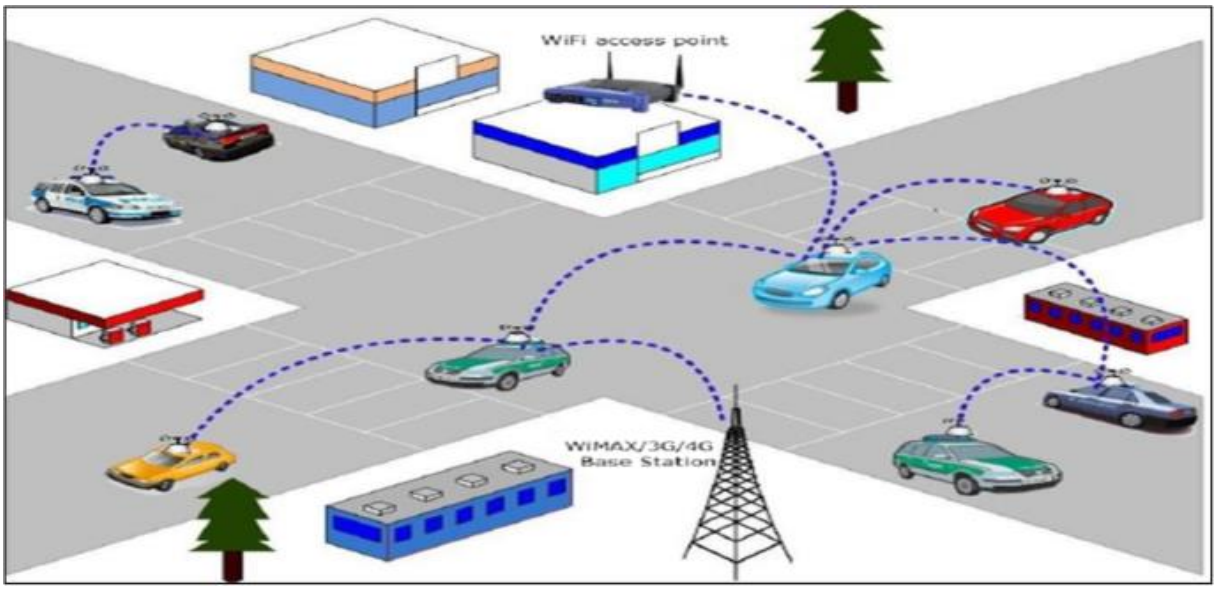


Figure 2: VANETs' architecture.

1.3.2. Smart vehicles :

Vehicles are equipped with multi interface cards, as well as sensors, both on board and externally. With an increasing number of vehicles equipped with on-board wireless devices (*e.g.*, UMTS, IEEE 802.11*p*, Bluetooth, etc.) and sensors (*e.g*., radar, ladar, etc.), efficient transport and management applications are focusing on optimizing flows of vehicles by reducing the travel time and avoiding any traffic congestions. As an instance, the on-board vehicle radar could be used to sense traffic congestions and automatically slow the vehicle. In other accident warning systems, sensors are used to determine that a crash occurred if air bags were deployed, this information is then relayed via V2V or V2I within the vehicular network.

In the next few years we will drive *smart —intelligent— vehicles*, with a set of novel functionalities (*e.g.*, data communications and sharing, sensor equipment, etc.). It is then necessary that for specific applications (*i.e.*, safety messages and alerts, gossip-based applications, etc.) the majority of mobile vehicles within a vehicular network be equipped with *on-board* wireless device, namely On-Board eqUipment (OBU).

Commonly, a smart vehicle is equipped with the following devices and technologies: (*i*) a Central Processing Unit (CPU) that implements the applications and communication protocols; (*ii*) a wireless transceiver for data transmissions among vehicles (V2V) and from vehicles to RSUs (V2I); (*iii*) a Global Positioning Service (GPS) receiver for positioning and navigation services; (*iv*) different sensors laying inside and outside the vehicle to measure various parameters (*i.e.*, speed, acceleration, distance from neighboring vehicles, etc.); (*v*) an input/output interface for human interaction with the system.

The basic idea of *smart vehicles* is addressed to safety issues, and then by a proper combination of functionalities like *control*, *communications*, and *computing* technologies, it will be possible to assist driver decisions, and also prevent wrong driver's behaviors.

.13.3. Applications in Vehicular Ad hoc Networks :

Vehicular applications are typically classified in three caregories

- active road *safety* applications,
- traffic efficiency and *management* applications,
- *comfort* and *infotainment* applications

The first category aims to avoid the risk of car accidents and make safer driving by distributing information about hazards and obstacles. The basic idea is to broaden the driver's range of perception, allowing him/her to react much quicker, thanks to alerts reception through wireless communications. The second category focus on optimizing flows of vehicles by reducing travel time and avoiding traffic jam situations. Applications like enhanced route guidance/navigation, traffic light optimal scheduling, and lane merging assistance, are intended to optimize routes, while also providing a reduction of gas emissions and fuel consumption.

Finally, although the primary purpose of VANETs is to enable safety applications, non-safety applications are expected to create commercial opportunities by increasing the number of vehicles equipped with *on-board* wireless devices. Comfort and infotainment applications aim to provide the road traveler with information support and entertainment to make the journey more pleasant. In the next subsections we will describe the main aspects of *safety* and *entertainment* applications for VANETs.

The applications regarding *safety* are strictly tied to the main purpose of vehicles: moving from a point till to destination.
Car collisions are currently one of the most frequent dead causes, this leads to a great business opportunity for infotainment, traffic advisory service, and car assistance.

Safety applications are always paramount to significantly reduce the number of accidents, the main focus of which is to avoid accidents from happening in the first place. For example, TrafficView and StreetSmart inform drivers through vehicular communications of the traffic conditions in their close proximity and farther down the road.
Vehicle platooning is another way to improve road safety. By eliminating the hassle of changing lane and/or adjusting speed, platooning allows vehicles to travel closely yet safely together.
Together with adaptive cruise control assisted by V2V communications, the problem of vehicle crashes due to human error can be alleviated.

❖ Some of the most requested applications by polls :

- Post Crash Notification (PCN).
- Congestion Road Notification (CRN).
- Lane Change Assistance (LCA).
- Cooperative Collision Warning (CCW).

1.4. The online social network (OSN) :

1.4.1. What is social networking :

Social networking is the use of Internet-based social media sites to stay connected with friends, family, colleagues, customers, or clients. Social networking can have a social purpose, a business purpose, or both, through sites such as Facebook, Twitter, LinkedIn, and Instagram, among others. Social networking has become a significant base for marketers seeking to engage customers [15].

For many users, online social networks are not only a way to keep in touch, but a way of life.



Figure 3: Online Social Networks OSNs.

1.4.2. Social Networks History :

In the early 1930s, a self-published psychologist named Dr. Jacob Levi Moreno introduced the sociogram, the first formal attempt to map out the relationships within a group of people. Moreno's sociogram -- a cluster of individual points, or "nodes," connected by straight lines -- became a powerful tool for identifying social leaders, outsiders, and what he called the "sociometric star," the person to whom all others are connected.

In 1954, anthropologist J. A. Barnes used the phrase "social network" to describe the complex relationships in a Norwegian fishing village.

1.4.3. How online social networking works :

Each online social network has different rules and methods. But Several features of online social networks are common to each of the more than 300 social networking sites currently in existence. The most basic feature is the ability to create and share a personal profile. This profile page typically includes a photo, some basic personal information (name, age,

sex, location) and extra space for listing your favorite bands, books, TV shows, movies, hobbies and Web sites.

The most important feature of online social networks is the ability to find and make friends with other site members. These friends also appear as links on your profile page so visitors can easily browse your online friend network and each online social network has different rules and methods for searching out and contacting potential friends.

And some of the famous online social networks are Facebook, Instagram, LinkedIn,…….

1.5. The start of the VSNs :

The Internet of things (IoT) is a revolutionary concept that is being materialized with the integration of numerous smart objects. Latest communication technologies have empowered remote devices and networks to become a dynamic part of the Internet.

The concept of Internet of vehicles IoVs is derived from vehicular ad hoc networks (VANETs) that have been around for decades. In VANETs, vehicles establish a network by communicating with each other referred to as vehicle to vehicle (V2V) and with infrastructure referred to as vehicle to infrastructure (V2I). VANETs enable various applications to ensure road safety by managing traffic.

Advent in technology transmutes the concept of VANETs to IoV that unleashes possibilities of developing unique applications. In IoVs, each vehicle and road-side units (RSU) are Internet enabled and also capable of communicating with each other using dedicated short-range communication (DSRC). This approach enhances the capabilities of the

nodes (vehicles, RSUs, etc.) to communicate with each other on a local network and with other networks globally through the Internet [5].

1.5.1. From IoVs to VSNs :

The cognizance of IoV has set a foundation for special forms of vehicular networks called Social Internet of Vehicles (SIoV) or the Vehicular Social Networks (VSN). That has evolved from its parent domain Social Internet of Things (SIoT).

SIoT enables the smart objects to create and manage social relationships between them based on the constraints set by their owners. This way, VSNs is a sub-domain of the SIoT where the vehicles are considered smart objects.
This ability of socializing empowers these vehicles to solve many problems as service discovery (SD) in a network of heterogeneous vehicles to provide trustworthy services to the vehicles.

Consequently, this helps realizing diverse applications that can significantly improve the safety on roads, enhance the driver experience, share common interests, and so on.

In VSNs, a cluster of vehicles may have a communal interest or need that might assist by socializing with each other. For example, a group of vehicles going to a community fair can socialize with each other by sharing information of traffic in the area, vacant car parking slots, alternate routes, accident warnings, and emergency exits. All these examples depict socializing of vehicles based on their common interest, context, category, and various other aspects like intent for socializing, achieving goals, and enhancing social relationships and environmental factors.
So in brief VSNs is an enhanced form of IoV that provides all the benefits of IoV along with providing socializing in vehicular networks.

1.6. The Vehicular Social Networks (VSNs):

At the different interval of day/week, the commuters along the roads encounter other commuters with the same routine, social behaviors, social interests and facing similar traffic conditions along their routes. People tend to use the same routes to travel to and from specific destinations with predictable and regular patterns and form virtual communities on roads with unique features inherited from social networks, i.e., centrality, similarity, common interests, friendship and professional relationships.

Vehicular social networking is the concept of incorporating possible social behavior of these commuters in vehicular environments.

VSNs incorporate social networking to communicate based on social properties, similar interests, social behaviors and objectives in the virtual community of vehicles, RSUs, drivers', passengers' and pedestrians' smart devices.

So a VSNs could be defined in a broader sense as the network of physically or virtually connected vehicles which are interested in sharing information for a common purpose or benefits, offering safety and convenience and entertainement for commuters and passengers on the road [4].

Chapter 2

Study of VSNs and it's architecture and applications.

2.1. Introduction :

In order to build a reliable trust model in the vehicular social network, we need to explore every side of the VSN, so in this chapter we will define the VSN very clearly, we will talk about everything about the architecture of VSN, it's characteristics and applications.

2.1. VSNs Architecture :

2.1.1. The components of VSNs :

The major components of VSNs are participants, smart devices that can be embedded into On Board Units (OBUs), and network infrastructure or Road Side Units (RSUs) that have tranceivers and trnsponders [1].

In VSNs, not only drivers, but also passengers, pedestrians, and OBUs participate in the communication. The integrated smart devices in vehicles, drivers', passengers' and pedestrians' smart devices can detect proximity with other devices and may share contents. Each user can be a publisher, a subscriber or both at the same time.

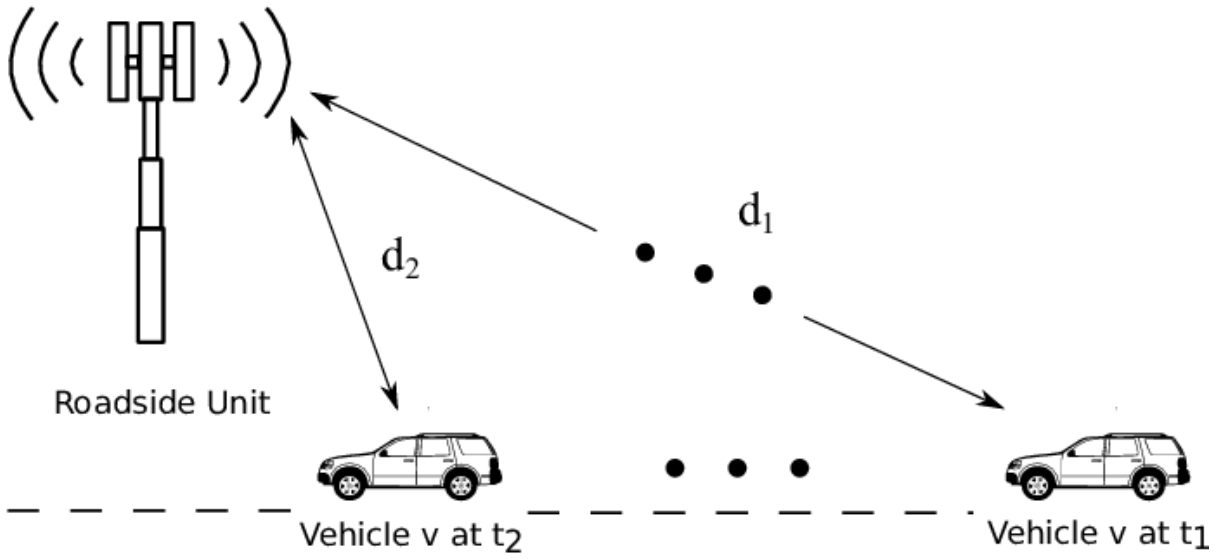


Figure 4: Physical Communication between vehicule and RSUs.

2.1.2. The interaction between VSNs components :

The way in which these devices can communicate depends on the underlying communication architecture. The communication of these devices/users can be classified as :

- Humans to Humans (H2H) communication.
- Humans to Machines (H2M) communication.
- Machines to Machines (M2M) communication.

The physical communication architecture of VSN depends on upon the network infrastructure of a vehicular network and software platform [2]. As shown on figure 5.

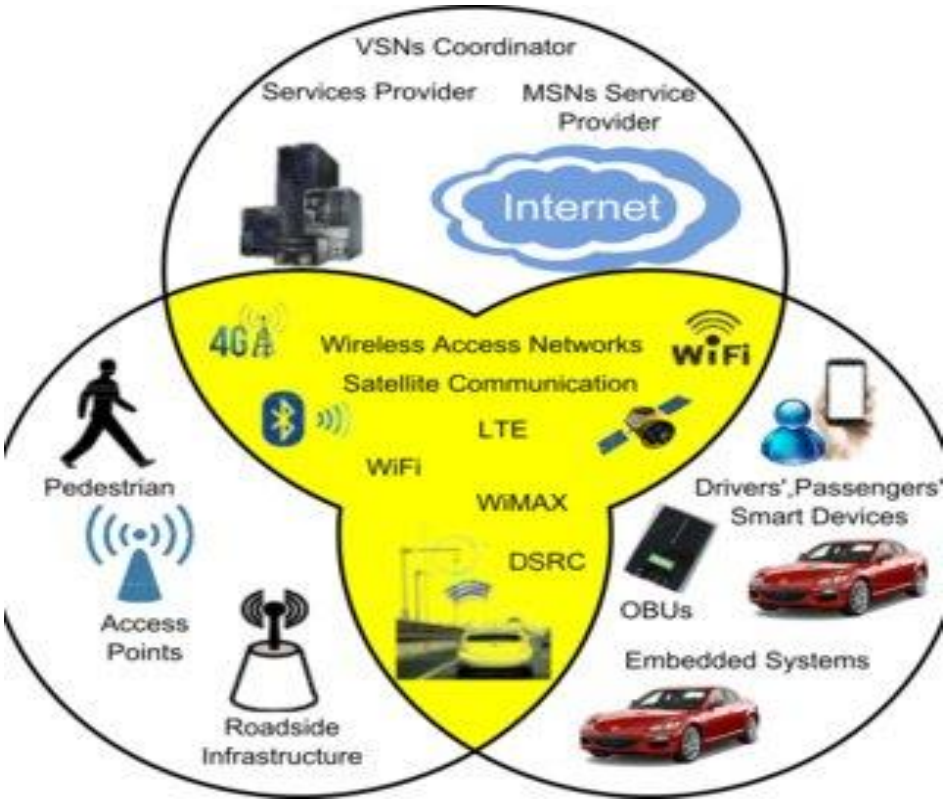


Figure 5: Physical Communication Architecture of VSNs.

2.1.3. VSNs architecture's classification :

The architecture of VSNs is flexible, VSNs are classified into three types based on communication architecture: Centralized VSNs, distribute VSNs and hybrid VSNs [1].

Centralized VSNs : In centralized VSNs, all devices/users communicate with centralized services providers such as Intelligent Traffic Control Systems (ITCS), web-based social network services providers, or a centralized server which continuously monitors and manages their interaction. In such a centralized communication architecture, the commuters can not communicate directly, and all the information concerning the members of VSNs are stored at a remote server.

A centralized coordination unit works as a bridge between two users to communicate. End users/devices communicate with infrastructure units,

E.g. RSUs resulting in Vehicle-to-Infrastructure (V2I) communication.

- **Advantages :** The centralized architecture of VSNs provides an opportunity to each user to maintain his profile on the server and may update his profile or interest list at any time. Also, a centralized system is less sensitive to traffic density on roads and can operate over larger geographic area enabling VSNs user to communicate even they are not close to each other.
- **Inconvenients :** centralized communication cost, Besides, centralized system architecture may cause inefficient communication between end users, low capacity for content storage in RSUs, and traffic load on RSUs in the highly dense area.

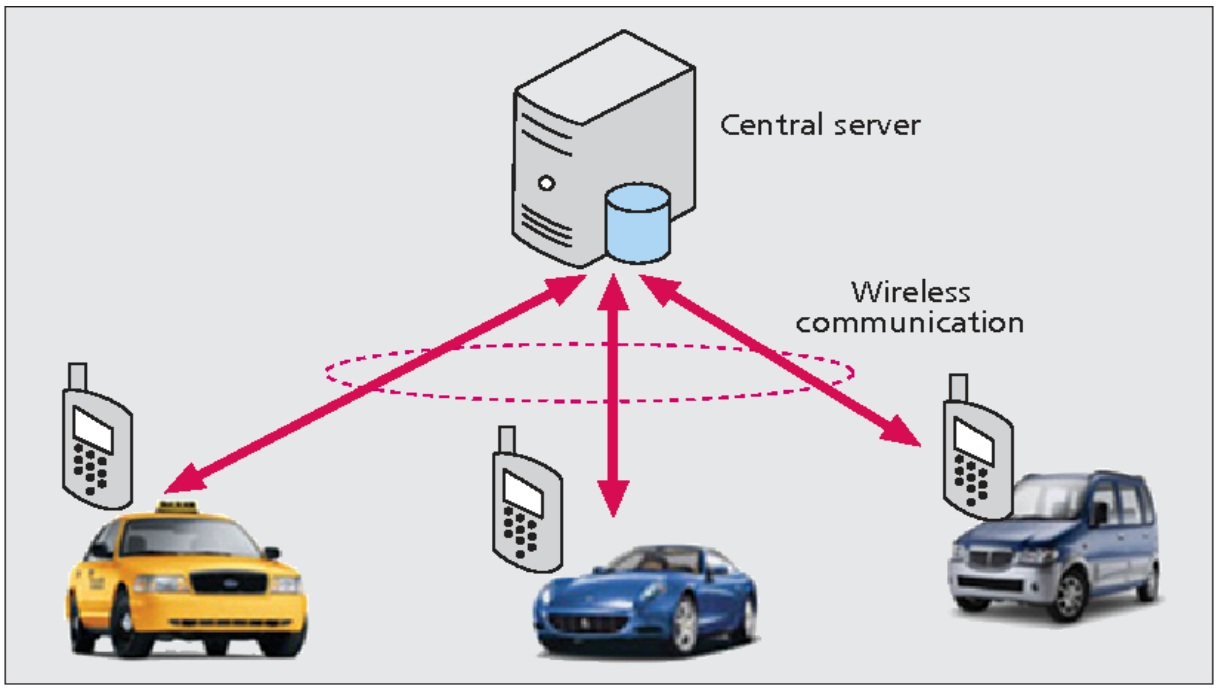


Figure 6: Centralized VSNs communication.

Distributed or decentralized VSNs : In distributed or decentralized VSNs, vehicles/commuters communicate with each other independently and collaborate in an ad-hoc manner without any centralized server to cooperate or regulate the communication. Vehicles/commuters communicate without any centralized infrastructure to facilitate opportunistic data delivery and forwarding using Vehicle-to-Vehicle (V2V) contact. The intermediate nodes store the contextual and social data packets until the destination node is found.

However, this does not mean at all that infrastructure does not exist. Road Side Unites (RSUs), or cellular network can be used to provide connectivity between two nodes.

- **Advantages :** Temporary communities are established on roads to share data of common interests based on user proximity. Distributed communication architecture is more efficient than centralize to provide direct communication among vehicles and reduce traffic load on RSUs.

- **Inconvenients :** Data dissemination in distributed VSNs is a challenging task since it demands cooperative communication and processing without the aid of a centralized system. Moreover, data forwarding and dissemination in distributed VSNs is vulnerable to malicious behavior of relay nodes. Interoperability of devices/applications, network protocol design, and communication overhead are other challenges in distributed VSNs. limited to a geographic area with challenges in communication in sparse situations.

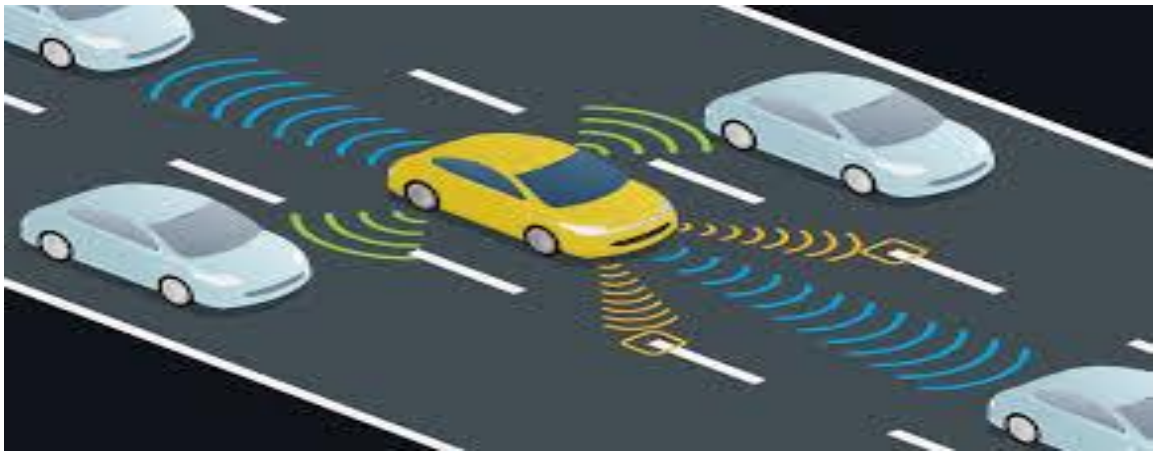


Figure 7: Distributed VSNs communication.

Hybrid VSNs : The vehicles can communicate directly using V2V communication or indirectly with V2I communication in a hybrid VSN, enabling a diverse range of applications, such as improved vehicle traffic efficiency and infotainment on the roads.

2.1.4. VSNs layers :

The architecture of VSN is not standardized and is subject to vague comprehensions that are inspired by the existing IoT architecture. The IoT architecture is simplified for sensing, network, and application layers, which have functions of data acquisition, data transfer, and offering middleware services, respectively.

However, VSN is far more complex because of the inclusion of social interactions between vehicles and its dynamics [5].

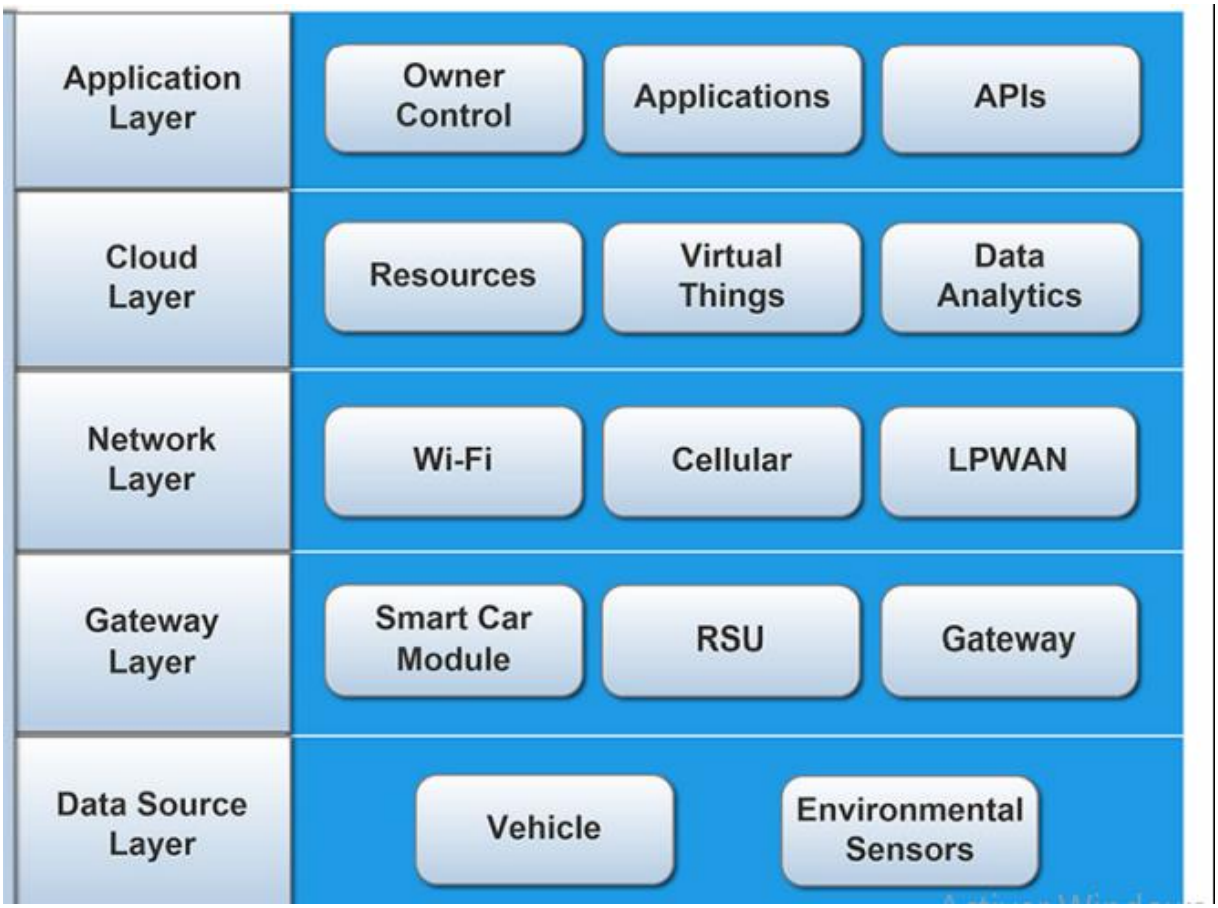


Figure 8: VSNs layers.

Data source layer : This layer collects dynamic data from the vehicle's owner, sensors deployed in a vehicle, and other available environmental sensors. In VSNs, the owner of a vehicle may want to share specific information about him or his journey based on the trust-based relationships, The in-vehicle sensors provide data to sense the environment of the vehicle around it to help improving a journey and driving experience by providing auto-pilot and other auxiliary systems [5].

Gateway layer : This layer consists of different gateway units such as a smart car module, RSU, and other gateways to enable the vehicles and

other environmental sensors to send their sensed data for further processing.

Network layer : Network layer integrates the gateway layer to the cloud using different communication protocols. The smart car modules, because of their mobility, can use cellular 3G/4G networks or low-power wide area networks (LPWAN) to send their data to the cloud.

Cloud layer : The cloud layer provides the required computing and storage for VSNs to process and analyze the data to offer trustworthy services.

Application layer : The application layer consists of all VSN-based applications that are based on consuming different cloud services. These applications offer their own application programming interfaces (API) to offer their services to customers. A vehicle owner can get information and can remotely configure the vehicle's level of openness and willingness.

2.1.5. The architecture :

As we have already mentioned that the VSN is an emerging field of communication where relevant concepts are being borrowed from the Internet of vehicles (IoVs) and the online social networks (OSNs) we can illustrate the architecture of the VSNs in this schema :

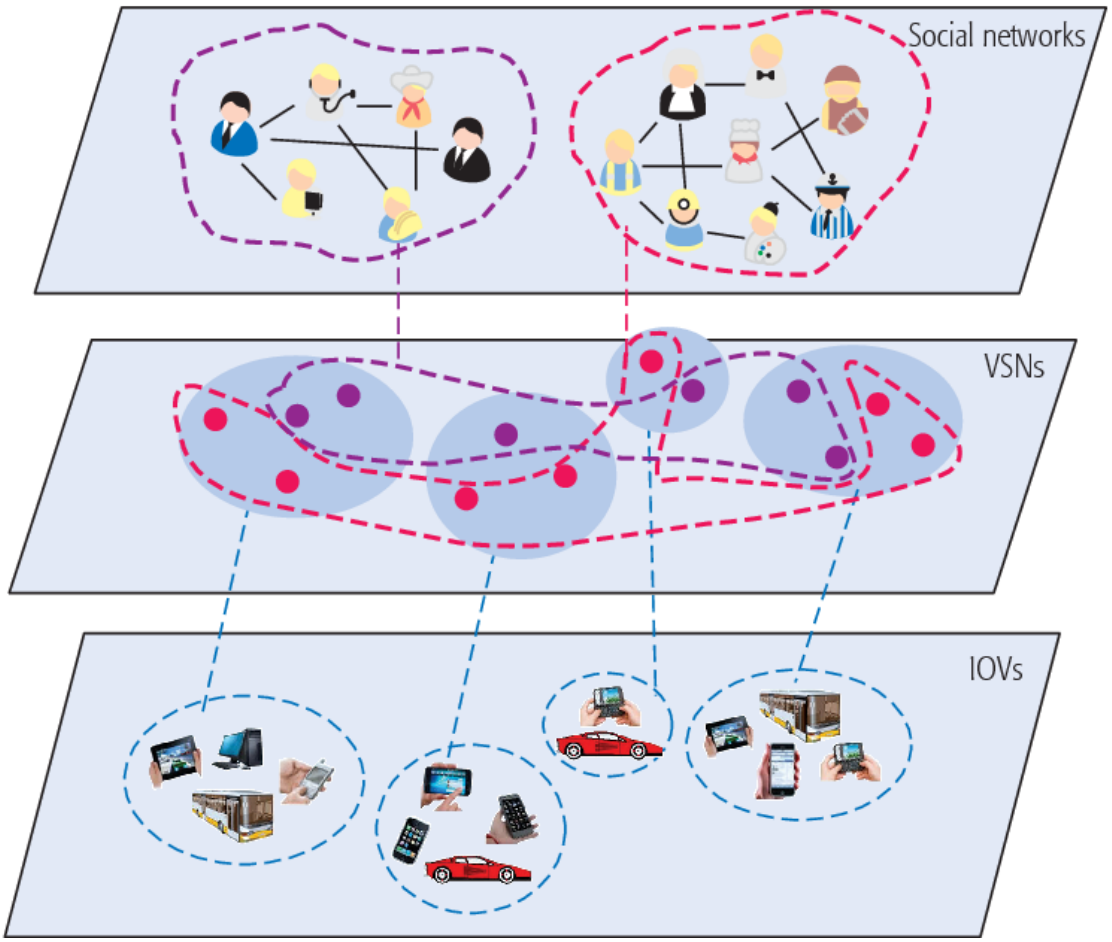


Figure 9: Schematic diagram of VSNs.

- The bottom level embraces the communication networks among vehicles and smart terminals, and can be viewed as a social network including physical communities.
- Meanwhile on the upper level the virtual social networks are constructed by mobile users in light of their inherent social ties.
- For the middle level we can illustrate VSNs as the fusion of the IoVs and the MSNs that can be embedded into on board units (OBUs) and road side units (RSUs).

2.2. The characteristics of VSNs :

VSNs could be broadly leveraged in smart cities since they can obtain individuals' social relationships through network analysis, and extend users' social activities in IoVs by providing data services. The main intrinsic features in VSNs can be summarized from the social and mobile aspects. Compared with online social networks (OSNs) and Internet of vehicles (IoVs).

2.2.1. Between IoVs and VSNs :

VSN is an enhanced form of IoV that provides all the benefits of IoV along with providing socializing in vehicular networks [5].

In order to provide these extra features, VSN requires additional resources like better communication technologies, enhanced security and privacy, more storage space, and high processing power. Table 1 illustrates the key features of IoV and VSN and presents the major differences between the two.

Features	Internet of vehicles (IoVs)	Vehicular social networks (VSNs)
• Dynamicity	✓ .	✓ .
• Mobility management	✓ .	✓ .
• Reputation		✓ .
• Contextualization	✓ .	✓ .
• Security and privacy	✓ .	✓ .
• Mutual interests		✓ .
• Social relationships		✓ .
• Data analysis	✓ .	✓ .
• Reliability	✓ .	✓ .
• Quality of service QOS	✓ .	✓ .
• Trust management		✓ .
• Data integrity	✓ .	✓ .
• Decentralization	✓ .	✓ .
• Profiling		✓ .
• Relationship management	✓ .	✓ .

Table 1: Key features of IoV and VSN.

N.B : Some of these features are common between both IoV and VSN, for example, dynamicity and mobility management, as vehicles are expected to be highly mobile in nature and capable of forming dynamic network topologies.

However, in some cases, VSN is expected to provide features that are not of much interest in a traditional IoV system, for example, social relationship and their management is of key interest to SIoV system as it sets the foundation for developing social apps for VSN network.

2.2.2. Between VSN and OSN :

VSNs consolidate relevant features and concepts from two different fields namely VANETs and social networks, and as VSNs incorporate social networking to communicate based on social properties, similar interests, and social behaviors and objectives in the virtual community of vehicles which is likely similar to mobile social network.

Table 2 illustrate the main differences between VSN and MSN.

	Mobile Social Networks (MSN)	Vehicular social Network (VSN)
Mobility	Random.	Restricted to roads and streets.
Network topology	Slow nodes mobility.	Highly dynamic due to vehicular speed and mobility requirements.
Social contributions	Real life, friends.	Human to human, human to machine, machine to machine, contact frequency, similarity.
Network architecture	Opportunistic and the internet	Internet and vanets or (IoVs).

Time sensitivity	Normal and acceptable.	Application dependent, real-time requirements for safety applications.
Energy constrains	High.	Not sensitive.
Mobility modeling	Random and easy.	Complicated and large scale.

Table 2 : Difference between VSNs and OSNs.

2.3. The applications of VSNs :

Any transportation-related information could be facilitated by VSN applications. It is projected that the concept of VSNs can be broadly used to enhance commuters' communication along the roads for different applications. Users can obtain traffic information from central providers and share these information with nearby users, or they can sense surrounding traffic condition and construct a global view based on contributed sensing data from multiple nearby users.

These applications can be widely categorized into four categories :

- Safety-based applications.
- Convenience-based applications.
- Comfort-based applications.
- Entertainement-based applications.

Safety-based applications : The Safety-based applications are of great importance and are primarily employed to enhance the safety on roads to decrease the probability of traffic accidents.

The safety-based applications can ensure the sharing of information such as vehicle's position, speed, direction, distance heading, and calculated

collision position to avoid accidents. This information can be shared among vehicles or RSUs. Safety-based applications are delay sensitive as the drivers need to be notified promptly to avoid accidents.

These applications include warning for intersection collision, overtaking vehicles, rear end collisions, emergency vehicles, pre-crash sensing, traffic conditions, and signal violation.

Convenience-based applications : The convenience-based applications primarily help to improve traffic flow, avoid congestion, and reduce commuters' travel time. As an instance, the commuters on the road may form virtual community to share real-time traffic information with user of mutual interests, which can be exploited to select or change the route to avoid traffic congestions.

Comfort-based applications : The Comfort-based applications allow commuters to communicate either with other commuters or with Internet hosts so as to improve commuters comfort.

For example, VSNs provide Internet connectivity to commuters along the roads so that they can access other networks to share and download information. These communication capabilities can be used to enhance commuters comfort with a diverse range of applications which include payment of tolls for bridges/roads, parking payments, repair and maintenance records of vehicles, finding free space for parking, finding fuel stations and recreation centers along their trajectories.

Entertainement-based applications : Entertainment-based applications facilitate commuters while driving to share/download music, video, photos or play games. sharing or downloading of location-dependent data, VSNs will facilitate the commuters to gain access to various available information of diverse interests such as advertisements, multimedia contents, and recreational facilities along the roads.

Due to road congestion during rush hours, commuters spend more time in comparison to normal traffic conditions, in such a case, these applications of VSNs will play an important role to provide entertainment sources to commuters.

2.4. Social connection between vehicles :

To understand how and why stranger vehicles are socially connected in a VSN, we first revisit the lifecycle of relationships among humans in traditional social networks.

The lifespan of such a relationship can be broken into three stages:

1. A weak connection is created.
2. A weak connection is cultivated and becomes a strong one.
3. A strong connection is maintained and a weak connecyion is terminated.

At each stage, a connection could be created, cultivated, and maintained only when two people both have the desire to further their relationship.

In a VSN, it is evident that drivers desire to share information with each other, which has been demonstrated in the Waze.com, one of the world's largest community-based traffic and navigation system. However, it is unclear whether this desire leads to a social network among vehicles. Therefore, it is necessary to investigate the lifecycle of relations in traditional social networks and compare them to the counterparts in a VSN.

At the first stage, weak connections in traditional social networks are created from communities or existing social networks, if two persons share a common community (e.g., a sport club), the likelihood that they create a connection becomes significantly large.

Another way of building new connections is through a person's existing social network, e.g., your friend might introduce you to one of his friends.

In VSNs, a car could connect with another if :

1. It encounter (within the communication range) others on the road.
2. It Have the common interest about shared information.

While vehicles exchanging messages, their local social connections could also be shared, so it is highly possible for a vehicle to create virtual connections to its “friends’ friends.”

At the second stage, a weak connection becomes a strong connection when people in tradition social networks have the chance to interact with each other and cultivate their relationship.

In VSNs, two vehicles frequently encountering and sharing information with each other (e.g, parking in the same parking lot) have the chance to build a weak connection into a strong one.

At the third stage, strong connections in traditional social network are maintained while weak connections are terminated.

In the context of VSNs, strong connections are maintained if and only if two vehicles keep sharing mutually beneficial information.

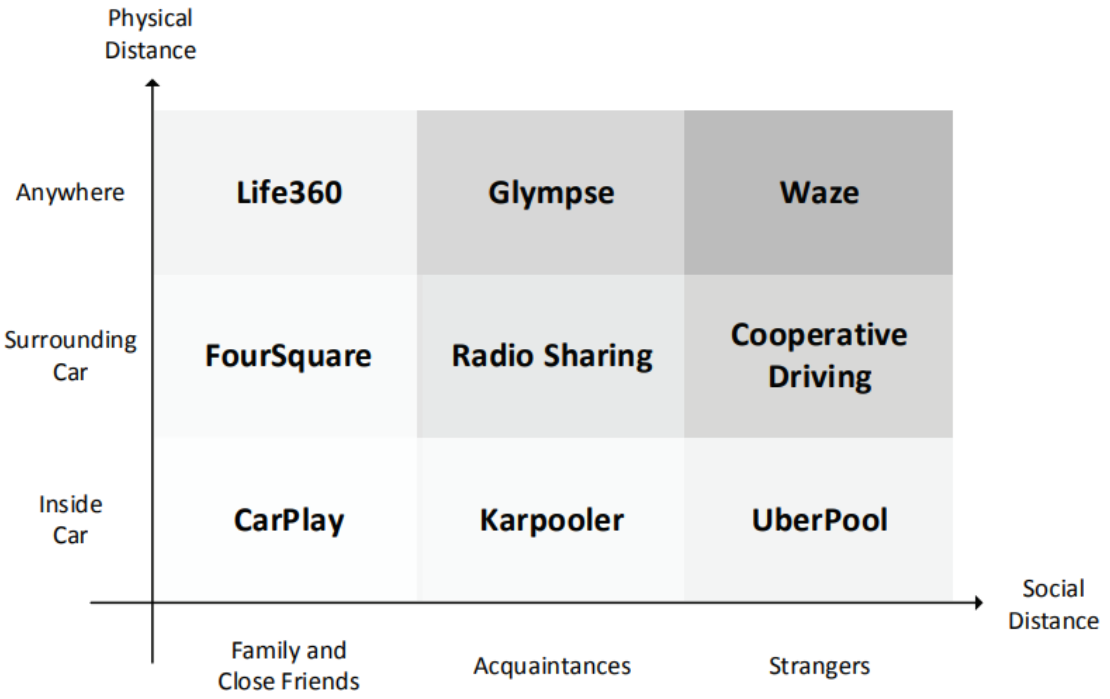


Figure 10 : Applications of VSN categorized by physical and social distances.

Chapter 3

Trust management in VSNs

3.1. Introduction :

The benefit of sharing common interest among vehicle drivers can be brought into VSNs. Thanks to the technological advances of wireless networks, drivers in populated locales are connected to form a tightly coupled and ad-hoc mobile vehicular social network (VSN). Within such a mobile social network, trustworthiness between temporarily connected vehicles could be mined from their interactions and applied within a VSN to achieve trustworthy information sharing among vehicles, In this section, we start with the definition of the trust management in VSN and the current research on direct and indirect trust in VSN. Finally, we will provide some of the most existing trust models in the Vehicular Social Networks (VSNs).

3.2. Definition of trust management in VSN :

Trust management in VSN Trust management is a mechanism of establishing a trust relationship between entities [5].

It can be conceptualized in two forms: a process of making an entity trustworthy for other entities and a process of assessing trustworthiness of other entities from the perspective of a specific entity.

Trust is considered an integral part of socializing, especially in VSN where socializing vehicles are mostly foreign to each other. Establishing a trustworthy relationship between the vehicles can significantly reduce the discernment of risk and uncertainty. Trust is normally based on the context, and value of trust might vary in different situations even if participating vehicles are the same [5].

3.3. Trust types in VSN :

3.3.1. Direct Trust in VSN :

A study on direct trust in OSN reveals that it is possible to compute or mine direct trust from driver interest similarities and direct interactions in VSNs.

The user interest similarity between vehicles should be re-defined because it's differ from the similarity in OSN meanwhile the only product in VSNs are messages exchanged between vehicles.

Messages are exchanged only when two vehicles with a common interest encounter each other, the trust computed from vehicle interactions is considered direct trust as vehicles are directly connected to each other. To determine whether a received message is trustworthy or not, each vehicle must have an information discrimination system. Vehicles could rely on their own sensors to evaluate the trustworthiness of received messages. In addition, they can upload received messages to Cloud to conduct information discrimination.

Information shared between vehicles should be classified into different categories and a driver's interest profile vector should be built from ratings of all categories.

The rating of a category can be modeled as the user's estimate about the trustworthiness of received information in that category [4].

3.3.2. Indirect Trust in VSN:

While direct trust could be obtained from vehicles' similarity and interactions, indirect trust is derived from other vehicles' recommendations, which describes the trust relations of vehicles that never physically meet.

The indirect trust from a trustor vehicle to a trustee vehicle highly depends on how strongly they are connected, which is affected by many factors such as the social distance, connection strengths and social network topology between them.

In summary, a vehicle could evaluate the direct trust of another vehicle based on their past interactions, and infer indirect trust by investigating how closely they are socially connected. This approach is different from traditional ones that focus on securing or authenticating vehicles based on the public key infrastructure (PKI). While PKI builds the first line of defense, it guarantees only the identification of legitimate vehicles but not the trustworthiness of vehicles [4].

3.4. The social connection tree (SCT) :

As mentioned previously A VSN can be constructed in centralized or distributed ways. In the centralized solution, a social connection between two vehicles is uploaded to Cloud via existing cellular technologies, e.g., 3G or 4G. After collecting these social connections, a social network among vehicles could be built and downloaded by vehicles.

In the distributed solution, each vehicle shares its social connections with nearby vehicles via DSRC technology [1]. By exchanging social connections with others, a vehicle can incrementally construct its vehicular social network.

A social connection in VSN initiates when two vehicles encounter and share information with each other. Such connection information will be either uploaded to Cloud or saved by these two vehicles. In this thesis we will focus on the social connection tree constructed in a distributed manner.

In the distributed solution, each vehicle maintains a local social connection tree (SCT). The root of a local SCT is the vehicle that maintains this SCT, the edges in the SCT are the (direct or indirect) social connections of the vehicle.

As shown in Fig. 7, a vehicle (e.g., n0) keeps tracking the interactions between itself and nearby vehicles. If it receives a message, e.g., road condition from

vehicle n2, it first checks whether n2 is in its local SCT. If not, a node n2 is created and inserted into its local SCT.

Otherwise, the weight of the edge between n0 and n2 is updated based on the new interaction. The more the positive interactions, the stronger (heavier) the connection (edge).

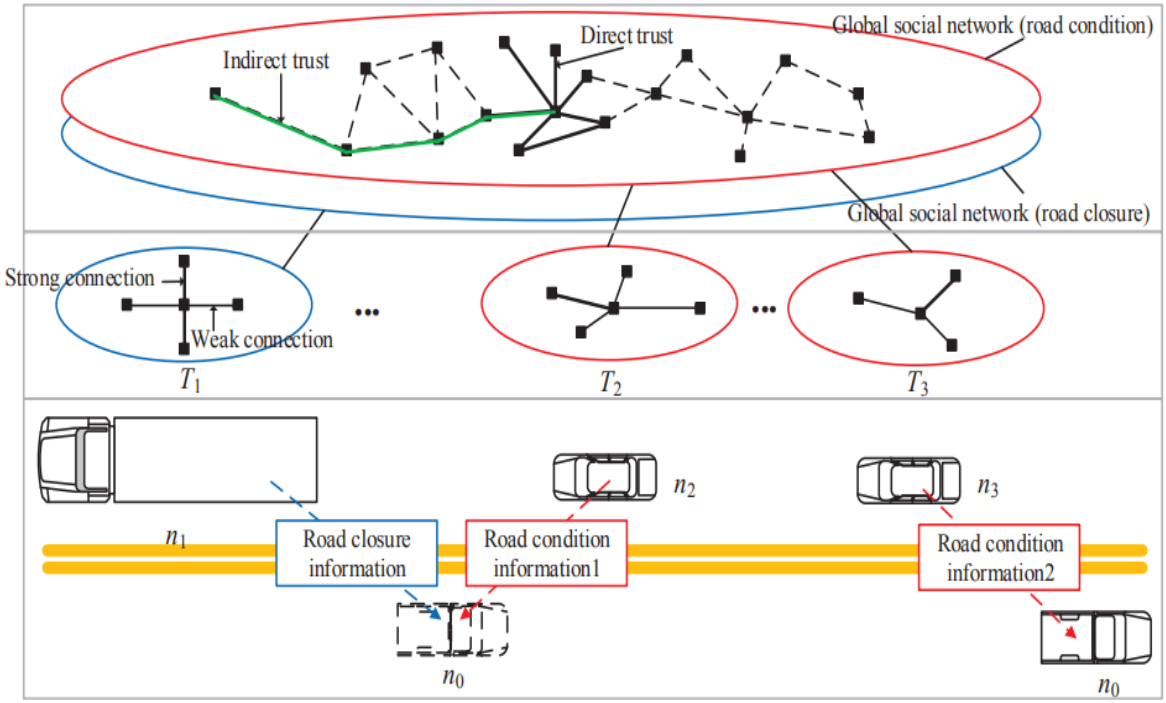


Figure 11: Illustration of a distributed vehicular social network construction

When two vehicles encounter each other on the road, they could also share their local SCTs. With the SCTs received from others, a vehicle can incrementally build its global social network. Knowing more vehicles with the common interests and receiving more relevant information motivates vehicles to share its local SCT with others.

For instance, when vehicle n0 receives road closure information from truck n1, the connection between n0 and n1 is created in n0's local SCT dedicated to road closure. Later on, when it receives local SCTs about road conditions from

n2 and n3, these SCTs are integrated into n0's global road-condition social network.

If a social network structure exists in a vehicular network, it is possible to study the trustworthiness among vehicles by a social network approach. For example, if two vehicles have a weak connection, it probably means the trustworthiness between them is low. At least, there is a lack of positive evidences indicating a trustful connection between them. Later on, if they exchange lots of useful information, the weak connection may become a strong one, indicating high trustworthiness between them. So how to classify messages into different categories is a tradeoff issue where more categories (contexts) increase the processing time and storage while fewer categories yield inaccurate trust estimations [4].

3.5. The trust Factors :

Trust in VSN depends on several factors like reputation, context, environment, goals, user expectations, social relationships and willingness [5], as illustrated in the next figure.

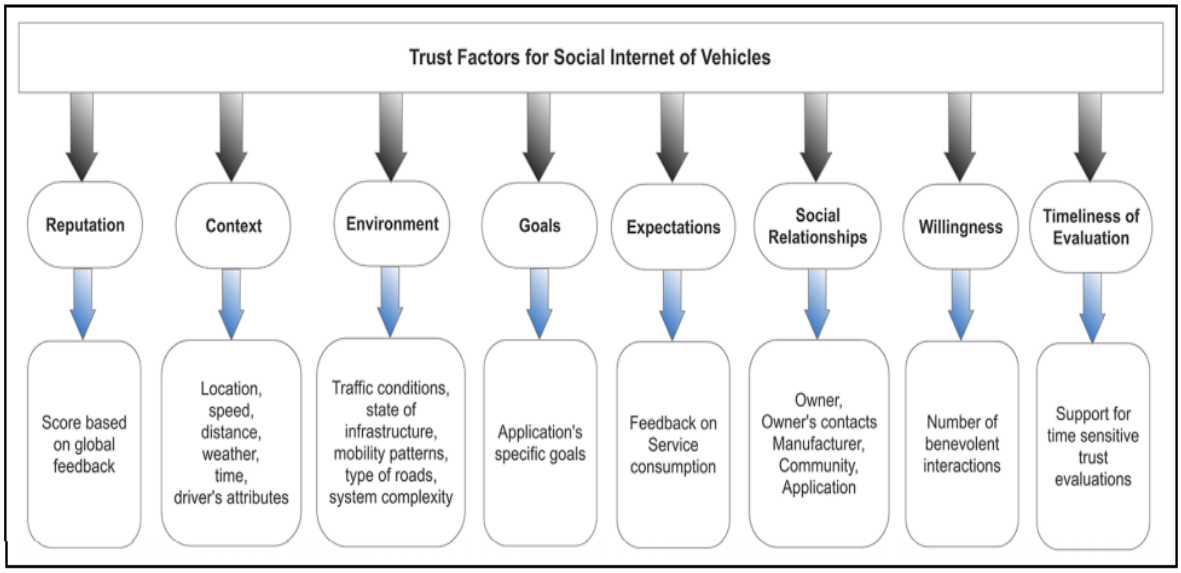


Figure 12: Trust factors for vehicular social networks

Each factor plays a significant role in the design of an efficient and reliable trust model that can be implemented in a highly dynamic and scalable environment like VSN, in this section we will define briefly each of the factors mentioned above.

- **Reputation :** Reputation is an opinion held by an object (human or machine) about another object.
  In VSN systems, trust among vehicles is highly dependent on how the vehicles are handling the information (received from sensors and on-board unit (OBU) and sent to other entities of the system).
  Reputation is used to create trust among vehicles that have no prior knowledge of each other (no previous contact) and hence use their experience from previous encounters along with the feedback from peers to evaluate the trustworthiness of the vehicles in the network, the system is expected to be responsible for calculating the reputation score for each entity based on its behavior. The reputation score is based on the information sthat the vehicle or the driver deliver whetеher it's generally true or false, the more the vehicle offer a real (true) informations the higher the reputation score it will gain.

- **Context :** Context is the occurrence of an event or an idea that helps in fully understanding the situation.
  In VSN a vehicle can't trust another vehicle in the network depending on the informations it gets from the other vehicle whether it's reasonable or not depending on the situation. For example, information sharing like ''school crossing ahead'' from one vehicle to another might be acceptable in urban areas but might not be considered valid information on highways. Similarly, providing speed limit of highways at urban areas might be out of context and can cause serious inconvenience for the drivers and the authorities.

So in brief in VSN vehicles are expected to trust other vehicles if they get contextual information based on their previous interactions.

- **Enivronment :** Environment is an external factor that can affect the trust process between vehicles in VSN.
  Environment can create an uncertainty in the trust mechanism due to several varying factors like traffic conditions, state of infrastructure, mobility patterns, type of roads, system complexity, scalability, and kind of communication. For example, information sharing between vehicles can be disrupted by loss of communication that results in receiving incomplete information at recipient vehicle. Due to receiving incomplete information, the recipient might not be able to interpret the information as required that might give an impression to the recipient that sender is not sending the right information which would spoil the reputation of the sender vehicle and ultimately the trust.
  Another example is the growin number of vehicles on road escalates associated parameters with each entity of the system, and trust and reputation score in a highly dense vehicular environment requires complex computations and fast processing which can cause a delay in sharing informations.

- **Goals :** Goals are aims or desired results expected to be achieved by the objects.
  Goals in VSN can be accomplishment of anticipated results by sharing information. Vehicles having mutual goals in SIoV can significantly improve the trust between them. For example, a common goal of vehicles in SIoV can be to share the information regarding traffic congestions on the roads to avoid traffic jams. Similarly, another goal can be finding vacant car parking slots in a shopping mall. Achieving this goal can improve the reputation of the vehicles and eventually the trust between them in a V2V communication.

- **Expectations :** expecation is a feeling or belief about how successful, good, someone or something (information) will be.
  In VSN receiving the expected information will increase the trust between vehicles, the trust is influenced by a node's subjective expectation to predict another node's behavior.
  For example, a smart parking application requesting information of vacant parking slots on a roadside from other vehicles is expecting to receive this information instead of receiving discount coupons of a nearby restaurant.
  The trust score of an entity can drastically change if expectations of other entities are not met, system plays a vital role in keeping the trust score of each entity when it comes to setting expectations from the entities and delivery of expectations. Therefore, a highly efficient mechanism is required to calculate the trust score based on the expectations of the entities.

- **Social relationships** : The social relationships and past social interactions between vehicles, their drivers, passengers and infrastructure impact the trust between vehicles.
  A vehicle will trust other vehicle more if they had past collaboration to satisfy some application requirements. The past successful social interaction builds strong relationships between objects. And the trustworthiness in VSN is also positively affected by social relationships between their drivers.
  For example, if the driver's social contact list shows that it contains the current driver of other vehicle, then the information provided by the other vehicle will be more trustworthy compared to other vehicles that are being driven by strangers.

The best way to acquire the social information of drivers and passengers is that they share their social relationship information directly with the trust manager.

- **Willingness :** The willingness in VSN is how much a vehicle is ready in the contribution of sharing useful informations in the network.
  The willingness attribute highlights the behavior of a vehicle regarding sharing information. This aspect explains the past active contributions of a vehicle to help other vehicles to meet their application requirements.
  Willingness helps improving the trustworthiness in system, For example, if a vehicle is actively contributing to the provision of services in a VSN environment, then applications will rely more on the information provided by the vehicle compared to other vehicles.

- **Timeliness of evaluation :** The vehicles in a VSN environment need to evaluate the trustworthiness of each other in a reasonable time to fulfill requirements of different applications by consuming shared information. The evaluation of trust can be done at different times with the available information and the requirements of applications.
  The evaluation process consists of two stages: pre-evaluation, vehicles assess the trustworthiness of each other based on the available context information and their experience, the post-evaluation is based on the results of the task performed and the environment.

3.6. Existing trust models :

Though Currently, not many trust models are available in the literature that are specifically proposed for the VSN networks. We try in this setion to

mention some of the existing trust models that have a decent realization for VSN networks.

3.6.1. The Qing Yang and Honggang Wang study :

The study by Qing Yang and Honggang Wang in [4]. proposes a distributed and indirected trust management model that focused on computing the trustworthiness between vehicles and finding all the possible paths between two vehicles.
Their study contained four pricipals steps in order to achieve trustworthiness :

1. **information classification and discrimination :** in order to achieve the context-aware trust evaluation, they've distinguished between the messages exchanged between commuter on the road and classified it into different categories based on their content.
2. **Resource-Aware Information Discrimination :** it can benefit from a complementary notification system that can help by reducing the amount of messages recieved by sending notifications about the non reliable vehicles.
3. **The indirect trust model :** the indirect trust model can be represented in a graph with nodes representing vehicles and edges representing the connection between'em.
4. **The efficient algorithm on computing trust :** the authors assumed that they have already the trust model in place, they were in need for an an efficient indirect trust computation algorithm, also they had a problem finding all the possible paths because finding all possible paths between two vehicles in a global social network is NP-Hard.

So our work is based on this study and we try to come up with new solutions for the problem mentionned by Yang and Honggang Wang in their article.

3.6.2. The trust on the ratee system :

The authors in Gai et al [8]. Proposed a Ratee-based Trust Management (RTM) system, where each entity of the system keeps its own reputation score collected from other entities during the previous interactions. Different from traditional vehicular trust models, RTM is ratee-based, where each node stores a limited amount of information about how much other users trust them. Furthermore, the authors have proposed a reliable Certification Authority server to ensure fairness and robustness of the trust information.

The presented model utilizes the relationships between the diverse entities of VSN and calculates the reputation score of the entity at the ratee level instead of rater level to enhance the reliability of the trustworthiness.

The results of their experiments exhibit high-speed information propagation and success rate as compared to raterbased technique. Furthermore, timely evaluation while calculating trustworthiness for the proposed model meets the demand of vehicular networks.

The Ratee-based Trust Management (RTM) system is composed of four components: *CA server*, *Cookies*, *Relationship Management*, and *Local Trust Management*. The schematic diagram of the RTM architecture is depicted in Figure 8. The major procedure of one transaction can be described as follows.

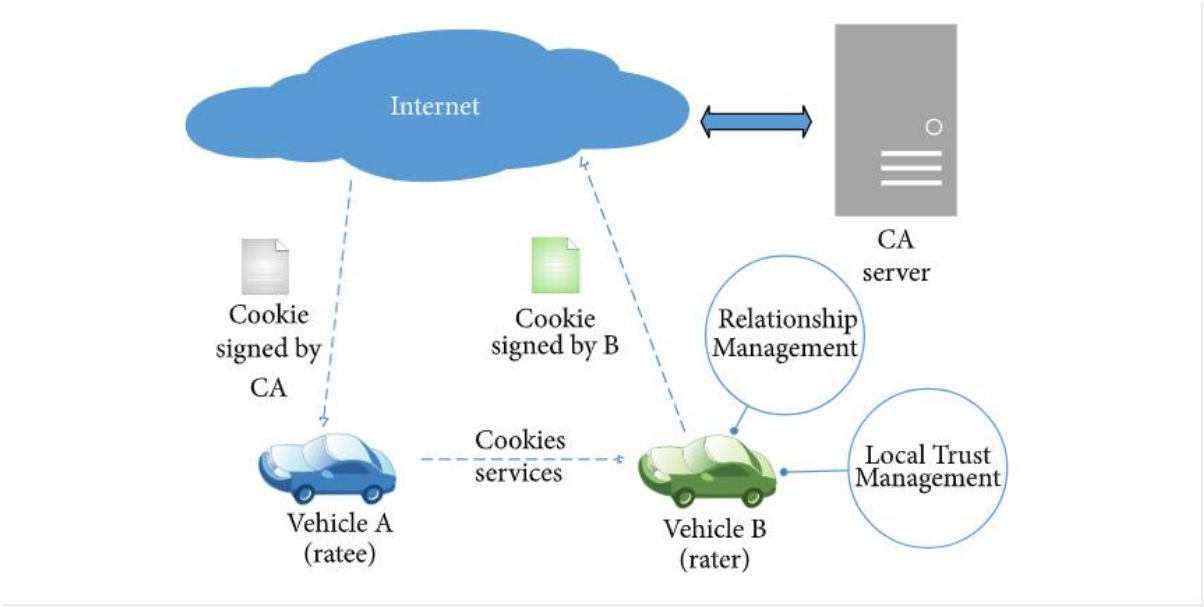


Figure 13: Scheme of Ratee-based Trust Management system.

For example, vehicle B is asking for congestion information, and vehicle A is willing to provide the information. To show its trustiness, A sends its *Cookies* which accumulate during past interactions along with the congestion information to B. Note that *Cookie* here is different from the cookie in HTTP that is to identify users. It is a feedback about a transaction generated by the requester and is used to evaluate trust value to the service provider.

After receiving the *Cookies* and congestion information, B first checks if the *Cookies* are signed by CA. If so, it computes trust value with these *Cookies* to decide whether to trust A or not.

If A can be trusted, then the congestion information will be sent to the application, and after that, a *Cookie* which contains a feedback about this transaction will be generated and sent to the CA Server with a sign from B through the Internet. Then after being verified and signed by CA, the *Cookie* will be sent to A when A connects to the Internet.

However, this model does not take into consideration the contextual information which is significant to highly mobile environment like VSN as context changes rapidly in such environment.

Furthermore, privacy aspect has not been addressed in this model which is considered imperative when it comes to sharing personal information like driver details, vehicle details, and passenger details for calculating trust.

3.6.3. The authenticated RFID security mechanism :

Kamesh and Priya [9] have proposed a trust management scheme for identity anonymous vehicular networks to assure privacy. In order to evaluate the trustworthiness of the received data, the proposed scheme detects false location and time information provided by the entities of the network.

The schemes operates in three phases :

Phase1 : In the first phase, the entities calculate the confidence score of the message received from other entities about specific events.

Phase2 : In the second phase, trust score for each received message for a particular event is calculated.

Phase3 : in the last phase, the decision to accept a message with highest trust value is taken.

The proposed scheme takes into consideration the context and complexity of the system to provide an efficient way of calculating the trust score for the entities.

Though the proposed model does not consider the memory, processing, storage, and energy limitations of vehicular networks. The authors have proposed their model keeping these factors constant which is not the case in real-time vehicular networks. Similarly, the authors have not taken into consideration the security and privacy factors.

3.6.4. Trust Management of Service-Oriented IoT Systems :

The study by Chen et al [10]. proposes a distributed trust management model that focused on minimizing computation and convergence time and maximizing application performance.
The model consider service-oriented IoT environments with no centralized trusted authority. Each IoT device has its unique identity which can be achieved through standard techniques such as publik key infrastructure (PKI).
A device communicates with other devices through the overlay social network protocols, or the underlying standard communication network protocols (wired or wireless).
Their social IoT model is based on social relationships among humans who are owners of IoT devices.
Every IoT device has an owner who could have many IoT devices.
Social relationships between owners is translated into social relationships between IoT devices as follows:

- Each owner has a list of friends (i.e., other owners), representing its social relationships.
- This friendship list varies dynamically as an owner makes or denies other owners as friends.
- If the owners of two nodes are friends, then it is likely they will be cooperative with each other.
- A device may be carried or operated by its owner in certain community-interest environments (e.g., work vs. home or a social club).
- Nodes belonging to a similar set of communities likely share similar interests or capabilities (2 paper title)

The authors also simulated trust-based SC with and without constraints to assess the gains of the adaptive behavior. However, this model lacks the integration of reputation and willingness trust factors that are crucial to deal with advanced trust-based attacks.

3.7. Conclusion :

The trust management in VSN is a very vaste domain, in this chapter we tried to highlight only the most needed points for the study.

We've defined the trustworthy in the vehicular social network VSN, we mentioned the two types of trust existed in the VSN, we've show how vehicles maintain their previous interaction by exploring the social connection tree (SCT), we've discussed the factors affecting the trust in VSN, also we've talked about some existing trust models and specifically the study of Qing Yang and Honggang Wang which we'll try to find a solution for their problem in chapter four.

Chapter 4

The Concept of the new trust model

4.1. Introduction :

As we've mentioned before the authors in [4] faced an issue achieving a reliable indirect trust model, the problem was finding an efficient algorithm for trust compute between vehicles based on the trust values shared by other vehicles, also finding all possible paths between two vehicles was an another issue, in this section we present the solution for the problems mentioned above by achieving a reliable trust model.

4.2. The network representation :

In mathematics, networks are often referred to as graphs so a VSN can be considered a dynamic graph where nodes represent vehicles and time-varying edges indicate connections between connected vehicles.

4.3. Intro into graph theory :

Before we start talking about our work concept we want to present a general definition of graph theory and it's different uses.
In mathematics, graph theory is the study of *graphs*, which are mathematical structures used to model pairwise relations between objects. A graph in this context is made up of *vertices* (also called *nodes* or *points*) which are connected by *edges* (also called *links* or *lines*).
Though graphs may look very theoretical, many practical problems can be represented by graphs. They are often used to model problems or situations in physics, biology, psychology and above all in computer science.
In computer science, graphs are used to represent networks of communication, data organization, computational devices, the flow of computation, In the latter case, they are used to represent the data

organisation, like the file system of an operating system, or communication networks.
The link structure of websites can be seen as a graph as well, i.e. a directed graph, because a link is a directed edge or an arc.

4.3.1. Directed graph definition :

A directed graph is graph, i.e., a set of objects (called vertices or nodes) that are connected together, where all the edges are directed from one vertex to another. A directed graph is sometimes called a digraph or a directed network.

One can formally define a directed graph as **G = (N, E)**, consisting of the set **N** of nodes and the set **E** of edges, which are ordered pairs of elements of **N**.

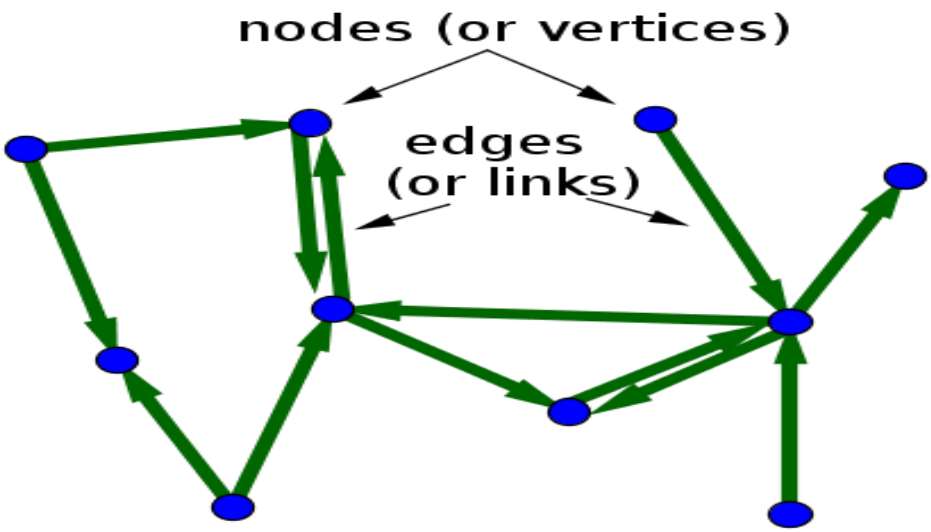


Figure 14: A directed graph with 10 vertices (or nodes) and 13 edges.

4.4. Mathematical presentation of the problem :

In a vehicular social network (VSN) vehicles exchange a lot of informations between'em, so the problem is to distinguish between trustworthy cars and the non trustworthy ones. In other words the dilemma is how to calculate the trustworthy of a vehicle that the commuter has no previous direct interactions with it.

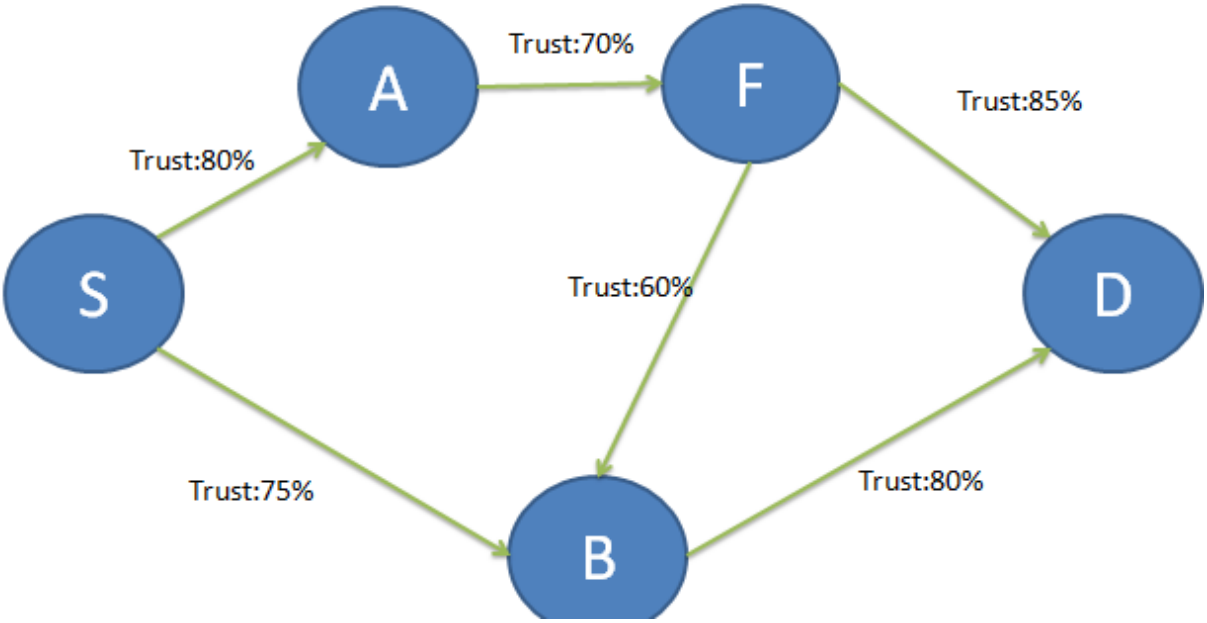


Figure 15: graph of a vehicular network

For example in Figure 15, we have an oriented (directed) graph that represents a vehicular network, the network consist of 5 vehicles (nodes), 6 edges that ties between the vehicles (the edges represent that the vehicles tied together have at least one previous interaction between'em), with a trust value between the connected nodes (the trust value shows how much a vehicle trust the other vehicle).

The problem : vehicle **S** and vehicle **D** don't have a previous interaction between'em, the commuter in vehicle D shares an information to vehicle S , naturally the commuter in vehicle S wants to know how much the informations are trustworthy.

The question : how to calculate trustworthy between **S** and **D** ?.

4.5. The system model :

As already mentioned not many trust models are proposed for the VSN networks, so we present a new concept or a new formula that allows us to calculate or estimate the trustworthy between two completely foreign nodes that have no idea about each other (no previous interactions). And also allows us to find the most trustful path we've passed through.

4.5.1. The Dijkstra's algorithm :

Our model or our algorithm is inspired by the Dijkstra's algorithm so before we talk and implement our algorithm we first present and demonstrate the Dijkstra's algorithm.

Dijkstra's algorithm (or Dijkstra's Shortest Path First algorithm, **SPF** algorithm), is an algorithm for finding the shortest path between nodes in a graph. which may represent, for example, road networks.

The algorithm exists in many variants. Dijkstra's original algorithm found the shortest path between two given nodes, but a more common variant fixes a single node as the "source" node and finds shortest paths from the source to all other nodes in the graph, producing a shortest-path tree.

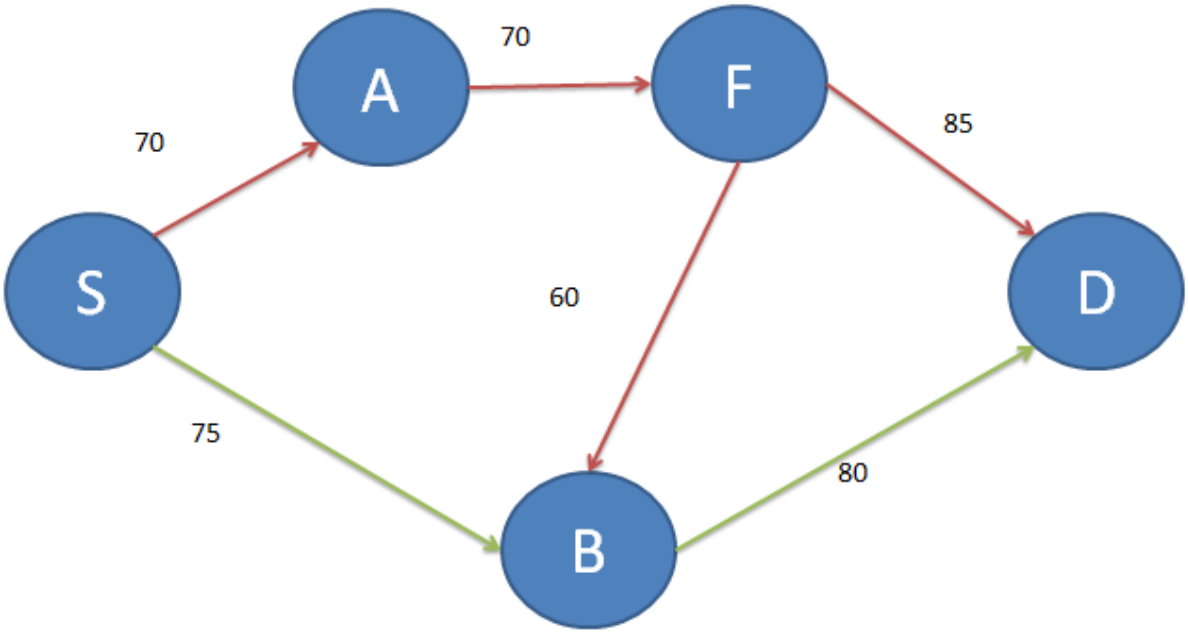


Figure 16: Dijkstra's algorithm implemented.

We consider the source node is **S** and the destination node is **D.**

In Figure 16 we can see that the shortest path between S and D is the path : **S** ⟶ **B** ⟶ **D**, with a value of **155**.

The algorithm :

1. we put $\delta = \{S\}$; $\pi(S) = 0$; $X = \{all\ THE\ nodes)$;

$$\pi_i = \begin{Bmatrix} d(u); if\ u = Sx_i\ is\ an\ arc \\ +\infty; if\ not \end{Bmatrix}$$

2. While $\delta \neq X$, choose $x_i \in X \backslash \delta\ of\ minimal\ \pi_i$, we put : $\delta = \delta \cup \{x_i\}$
   A. For all $x_j \in X \backslash \delta \cap \Gamma^+(x_i)$, we put :

$$\pi_j = min\{\pi_i + d(x_i, x_j),\ \pi_j\}$$

N.B.

- The source node is **S**.
- $d(u)$: The distance between the starting node and his neighbours.
- π_i: the new distance.
- $\Gamma^+(x_i)$: successors of the node x_i .

4.5.2. The Recommended method for solving the problem :

Objective : The objective of the new concept is :

1. calculate the trustworthiness between two vehicles (nodes) in a network based on the trustworthiness the other vehicles mention from their previous interactions.
2. Find the trustworthy path between the two stranger nodes.

The method : as mentioned above this new concept has been inspired by the djikstra's algorithm, before we talk about the algorithm we start make clear these points :

- **Trust type :** since we try to calculate trust between two vehicles with no past interaction we classify this new method in the column of Indirect trust.
- **Architecture :** the model is about vehicles/commuters communicating with each other independently without any centralized server to cooperate or regulate the communication, hence we classify our model as a distributed/decentralized architecture.
- **Concept :** the idea of the new concept is to developpe an efficient algorithm and to apply a new mathematical formula to calculate the trustworthy between two vehicles. We will explain the formula with an example.

<u>The Efficient Algorithm on Computing Trust:</u>

1. we put $\delta = \{S\};\ \pi(S) = 100; X = \{all\ the\ nodes\};$
$$\pi_j = \begin{Bmatrix} trust(u); if\ u = Sx_i\ is\ an\ arc \\ -1; if\ not \end{Bmatrix}$$
2. While $\delta \neq X$, choose $x_i \in X \backslash \delta\ of\ maximal\ \pi_i$, we put : $\delta = \delta \cup \{x_i\}$
   A. For all $x_j \in X \backslash \delta \cap \Gamma^+(x_i)$, we put :
$$\pi_j = \max\{\pi_j,\ min\{\pi_i\ ;\ trust(x_i, x_j)\}$$

N.B.

- The source node is **S**.
- $trust(x_i, x_j)$:The trust value between the starting node and his neighbours.
- π_i: the trust value of the previous node i .
- Γ^+: successors of the node.

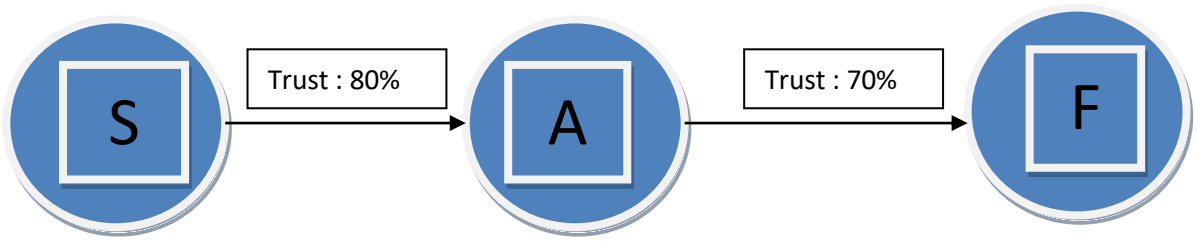


Figure 17 : Phase 0

PHASE 1 :

- As a start we give the **S** the value 100.
- And since the **A** is directly connected with **S** we give him the actual value of trust which is 80.
- **F** is not connected directly with **S** so we give it the value -1.

The graph becomes :

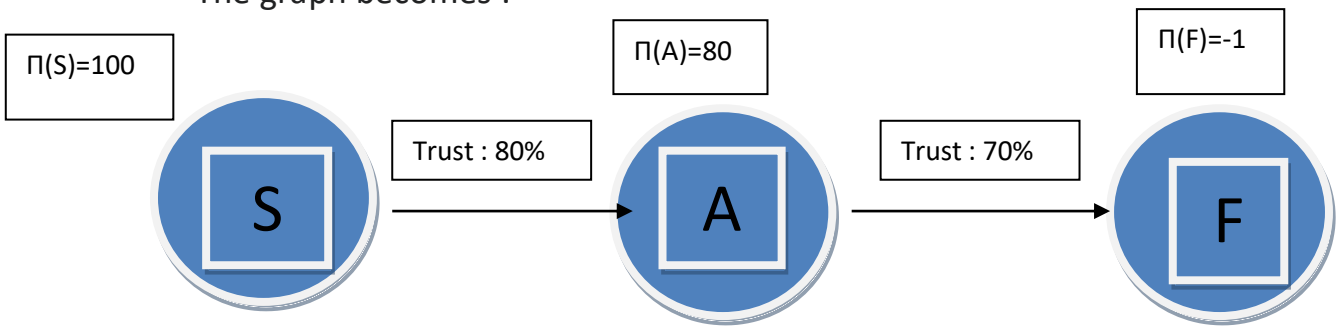


Figure 18 : Phase 1

PHASE 2 : the formula :

$$\pi(F) = \max\{\ \pi(F), min\ \{\pi(A)\ , trust(A, F)\}\}.$$

PHASE 3: applying the formula :

$$\pi(F) = \max\{\ -1, min\ \{80\ ,70\}\}.$$

Which means the value of trust between **S** and **D** is 70%. As shown in Figure 19.

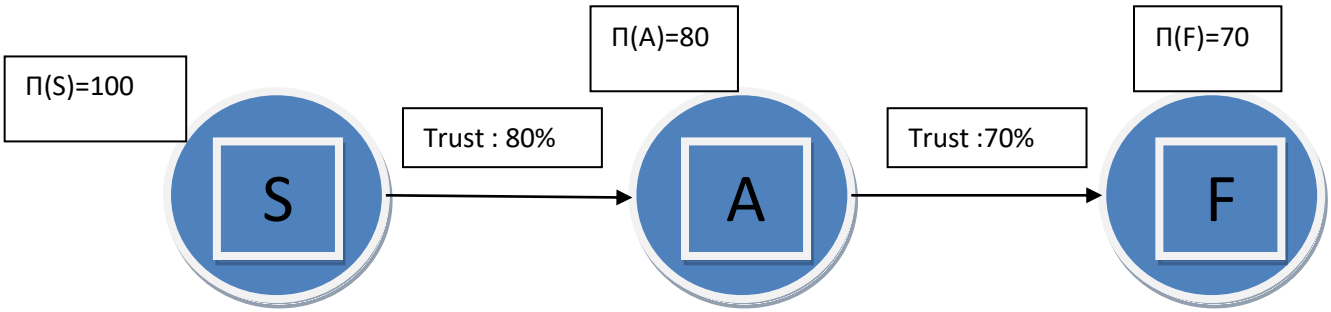


Figure 19 : Phase 3

The detailed algorithme :

Function Calculate_Nodes_Values **#Recursive Function**

Input : G, n

If n has no neighbor : **return**

For each $n_{neighbor}$ of n :

New_neighbor_value <- max (min (Value(n) , trust(n, $n_{neighbor}$)), Value($n_{neighbor}$))

If Value($n_{neighbor}$) >= New_neighbor_value: **return**

Value($n_{neighbor}$) <- New_neighbor_value

Calculate_Nodes_Values(G, neighbor)

Function Select_path **#Recursive Function**

Input : G, n_{begin} , n_{end}

If (n_{begin} = n_{end}) : **return** n_{begin}

Else if n_{begin} has no neighbor : return

Put all neighbors nodes and it's trust values in the list L with descendant order.

Result = ''

While True :

Try :

Select then$n_{neigHbour}$ and it's value of the first element

Result <- select_path(G, $n_{neigHbour}$, n_{end})

Exit the while loop

except IndexError :

return ''

except :

delete the first element in L #to make to the second edge in the list the first one.

return n_{begin} + '->' + Result

Function Main

Input : G(N,E,T) # a Direct graph with **N**odes , **E**dges and the **T**rust represent the **W**eight of the edge.

T[n] <- -1 #assigning -1 for each node

T[n_{begin}] <- 100 # assigning the value 100 which means total confident

Calculate_Nodes_Values(G, n_{begin}) #Calculate all nodes values starting from the node (n_{begin})

Select_path (G, n_{begin} , n_{end}) #select the most trustful path

Applying the algorithme on a network : We will apply this algorithm on a bigger network to demonstrate the iterations step by step.

Let's take the next figure as a network example to apply the algorithme.

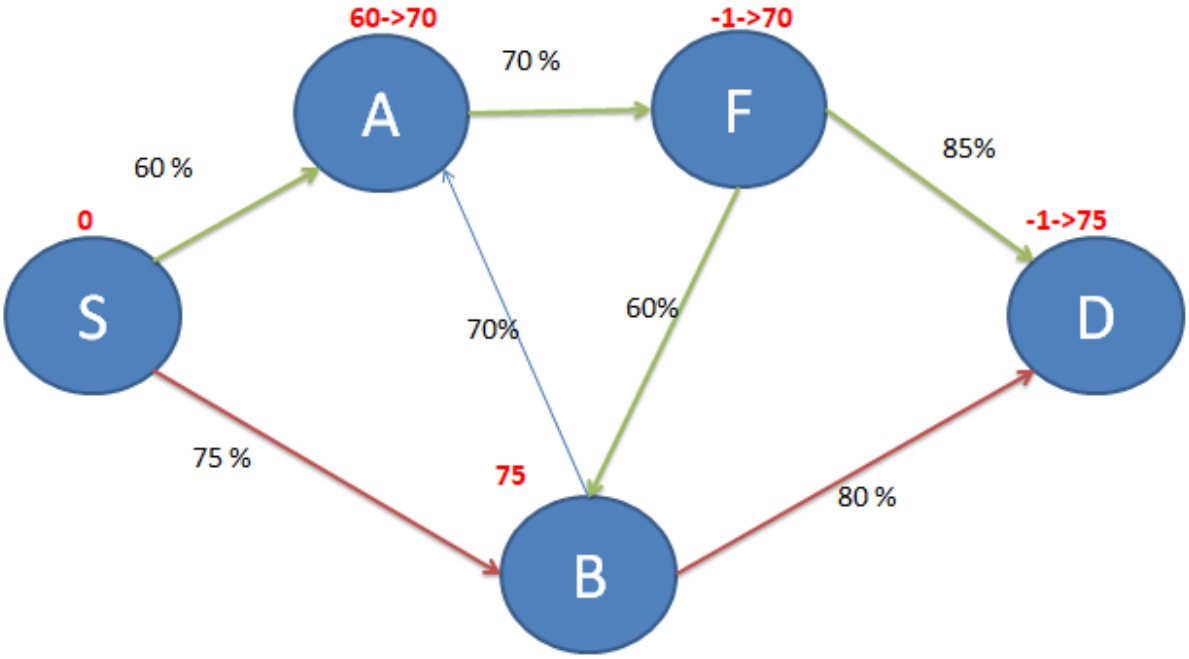


Figure 20 : Network example to apply the new formula.

- **The goal :** starting node S, destination node D.
- **The iterations :**
  1. $X = \{S, A, B, F, D\}$. $\delta = \{S\}$
  2. $\delta = \{S, B\}$

     $\pi(A) = \max\{60, min\{75, 70\}\}$

     $\pi(A) = 70.$

     $\pi(D) = \max\{-1, min\{75, 80\}\}.$

     $\pi(D) = 75.$
  3. $\delta = \{S, B, D, A\}$
  4. $\pi(F) = \max\{-1, min\{70, 70\}\}.$

     $\pi(F) = 70.$
  5. The path is : **S** → **B** → **D**, with a trust value of 75%.

4.6. The methodology :

The dataset : A dataset is a collection of data. In other words, a dataset corresponds to the contents of a single database table, or a single statistical data matrix, where every column of the table represents a particular variable, and each row corresponds to a given member of the dataset in question.

We conducted our study on a multi-label data set which contains:

-The nodes (or the vehicle number), the source nodes (vehicle), the destinated node (vehicle), the value of trust between the two nodes (vehicles).

The figure 21 represents a sample of the data set we used to apply the algorithme above.

	A	B	C
1	source	dest	conf
2	0	1	80
3	0	2	55
4	1	3	70
5	2	1	70
6	3	2	80
7	3	4	85
8	2	4	80

Figure 21 : Dataset sample.

The preprocessing :

1. **Generating the dataset :**
   Generation of different types of datasets which means differnt types of graphs for a better experiment.

2. **Importing all the crucial libraries:**
   Before mentioning the imported libraries used in the program we should mention that our work was done by the python language,

Python is a high-level programming language designed to be easy to read and simple to implement. It is open source, which means it is free to use, even for commercial applications. Python can run on Mac, Windows, and Unix systems and has also been ported to Java and .NET virtual machines.

- **NetworkX :**
  NetworkX is a Python package for the creation, manipulation, and study of the structure, dynamics, and functions of complex networks. NetworkX is suitable for operation on large real-world graphs: e.g. graphs in excess of 10 million nodes and 100 million edges. Due to its dependence on a pure-Python "dictionary of dictionary" data structure, NetworkX is a reasonably efficient, very scalable, highly portable framework for network and social network analysis.

- **Pandas :**
  Pandas is a python package provides rich data structures and functions designed to make working with structured data fast, easy, and expressive. It is one of the critical ingredients enabling Python to be a powerful and productive data analysis environment.
  Pandas aims to be the fundamental high-level building block for doing practical, real world data analysis in Python. Additionally, it has the broader goal of becoming the most powerful and flexible open source data analysis / manipulation tool available in any language.

- **Matplotlib:**
  Matplotlib is a comprehensive library for creating static, animated, and interactive visualizations in Python.

3. **Reading the dataset :**
   In this step we read the data set given which contains the source node and the destination and the trust value between'em.

4. **Creating the network :**
   In this step we transform the content of the data to a graph (a network) that contains source nodes, destination nodes, and edges which represents the connection between the nodes representing the network to study.

5. **Apply the algorithm :**
   As we explained above, we apply the algorithm and the new formula to the network generated from the dataset so we can obtain the new trust values calculated of each of the nodes we've passed through the operation.

6. **Selecting the path :**
   In this step we save the nodes we pass through to generates the maximum trust value of the destination node which gives us the most confident path.

7. **Display the data :**
   The final step is displaying all what we have done, we will display the network generated, display the new trust values, and display the confident path, and finally we display a chart that represents trust chart that contains the nodes and the trust values.

4.7. The presetnation of the software program :

1. **The dataset :** For this example we've used the dataset shown in Figure 21 (p.71).
   This datasets is composed of 5 nodes (vehicles), and 7 arcs between the nodes represent a previous intercation, each arc has a trust value given.

2. **User's inputs :** First the user is going to enter the csv file path to get the results, after that the user got to enter the value of the source node which represents himself and the destination node as shown in Figure 22.

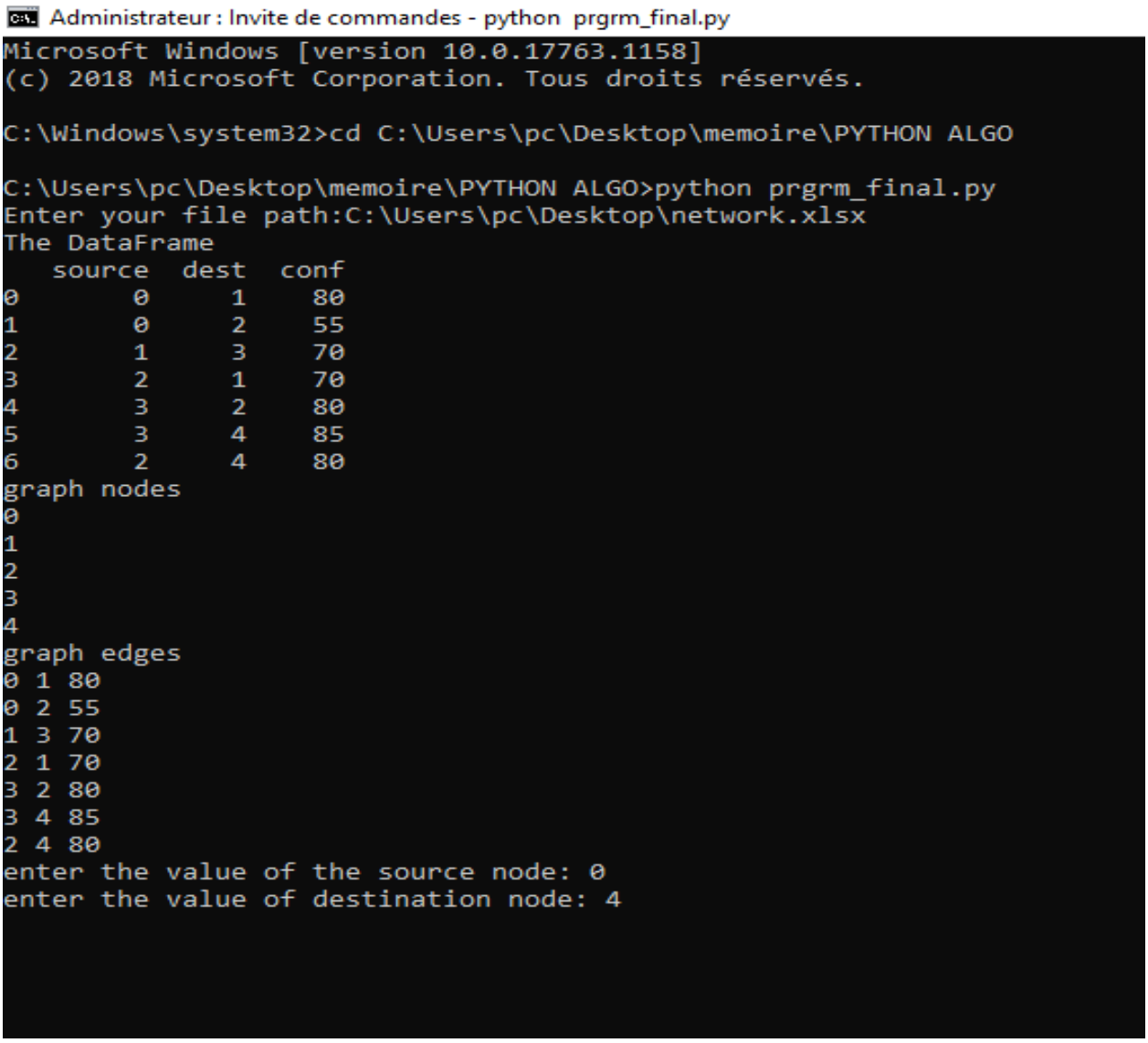


Figure 22 : User's input.

3. **The generated network :** after the user enters his inputs, the network got generated as shown in Fig 23.

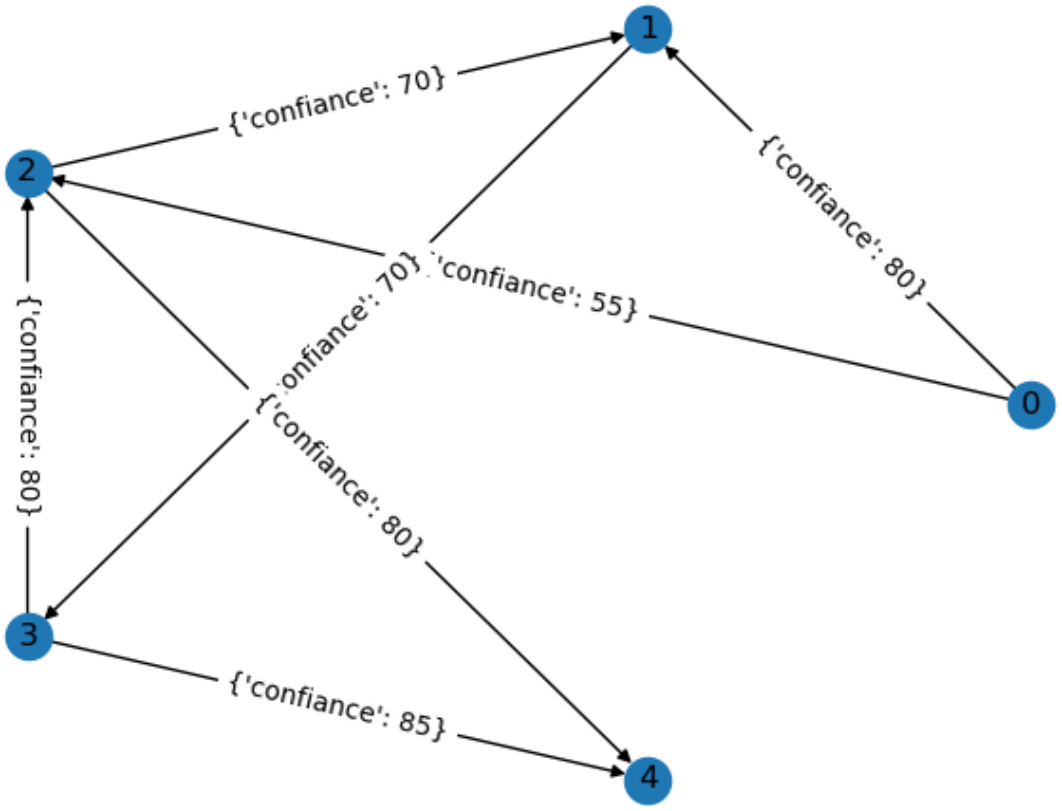


Figure 23 : The generated network.

4. **The trust values and the confident (appropriate) path :**
   The users got the result of the trust values and the confident path he is looking for in a text file. As shown in fig 24.

```
the confident values of the nodes:
[(0, {'valeur': 100}), (1, {'valeur': 80}), (2, {'valeur': 70}), (3, {'valeur': 70}), (4, {'valeur': 70})]
the most confident path
0->1->3->4
```

Figure 24 : Results of the input.

5. **The results in a chart :**

   As shown in figure 25, for a better view of result, we got the result in a chart called trust chart, in the x_axis we have the nodes of our network, and in the y_label we got the trust values.

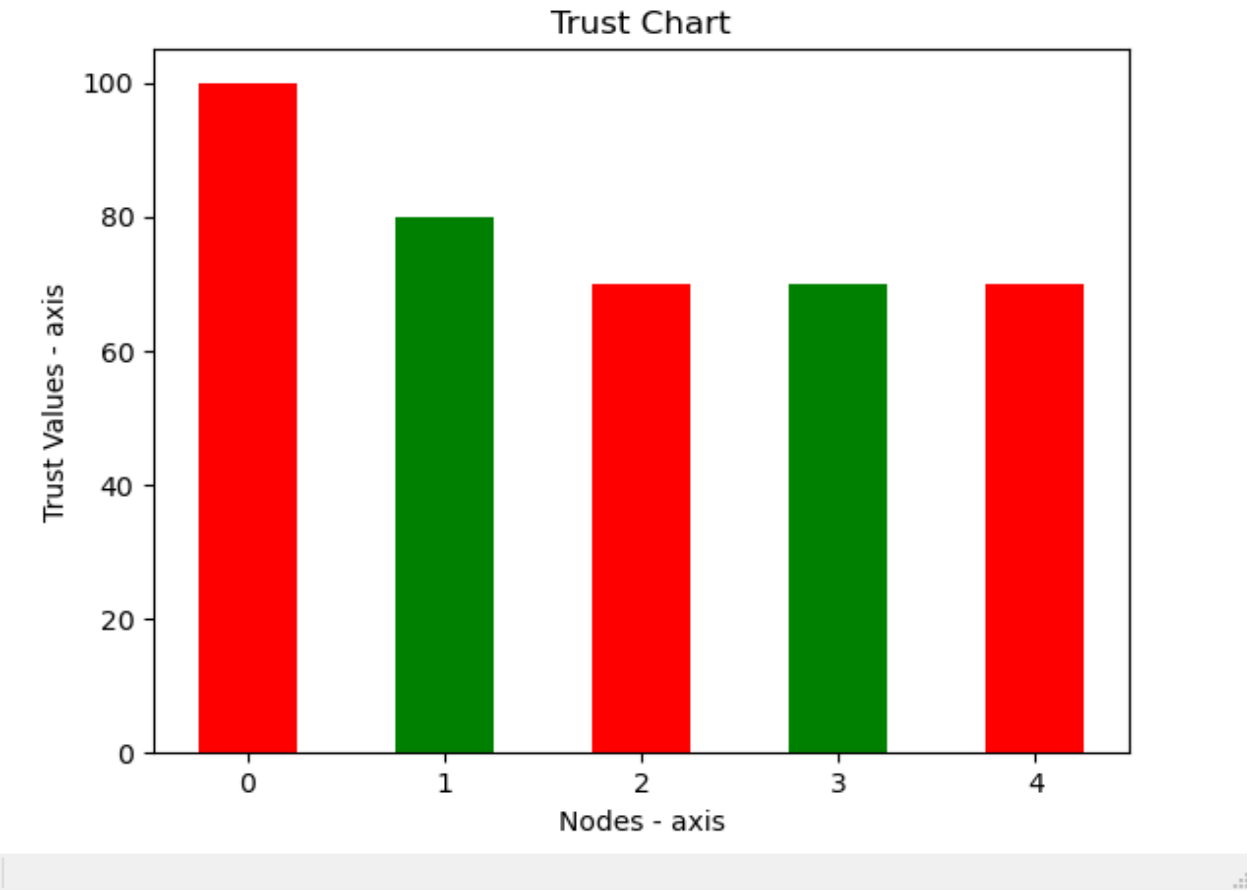


Figure 25 : Trust chart.

4.8. Conclusion :

In this chapter we've concluded the object of our work which is achieving a reliable trust model. The developpement of an efficient algorithm applied in the indirect trust type was achieved , finding the solution to find the only one path that is the most trustful path between two vehicules, the one we obtained our result from.

This new concept of a reliable trust mode makes it easier to compute trustworthy between stranger vehicles. Makes it easier for cummuters to communicating with comfort.

Conclusion and prequisites:

The vehicular social networks (VSNs) is a brand-new communication paradigm that have attracted the research community and it's going to be an essential part in the modern cities, in its early age of research, VSN has various unexplored areas, and trust model is one of them. Trustworthy between commuters will play a vital role in VSNs, commuters need to trust each other in order to communicate and share informations between'em, so the objective of our work was to apply a reliable trust model and calculate trustworthy between vehicles.

In this paper, we can resume our work to :

- VSN introduction and architectures.
- Trust management in VSN.
- The new concept provided for the trust management.

First, we presented VSN as a sub domain of IoT and IoV and it's a merge between OSN and VANET. Then, the architecture of VSN was clarified, Further, we discussed the trust management in VSN including the trust types and factors beside talking about existing trust models.

Finally, the core of our work was to find a solution and an algorithm to solve the problem of fnding all the possible paths between two vehicles in a global social network and computing trust value between two stranger vehicules, so we've created the new concept and method to develop an efficient and reliable trust model for VSN and we came up with an efficient algorithm to compute the trustworthy, and also we've provided a solution to only provide the appropriate path between two vehicles without finding all the other paths.

This new system is adaptable in the small and the large networks, networks where the commuters share their previous trust values about others.

The new idea has offered a new rsolutions in order to improve trustworthy between strangers, this new concept of trust makes it easier for strangers to communicate and share informations with no fear of the other side to offer a non reliable informations.

Perspective :

VSN is one of the recently emerged communication networks and it's going to have a big impact on our life in the futur, and so on the trustworthy will become indispensable in the VSN architecture, after reviewing currently efforts made in this direction and the effort we've made, based on our analysis, we highlight a few of these issues for future research :

The OMNeT++ simulation :

In VSNs, the design of such interesting environment is very complex and cost a lot, in this case the simulation become the only possible choice to validate newly designed architectures and for applying the new trustworthy system model, so the best way is to apply the simulation in the OMNeT++ simulator.

NB. OMNeT++ is an extensible, modular, component-based C++ simulation library and framework, primarily for building network simulators.

Set up a scientific article for publication :

As the indirect trustworthy is one of the major issues in VSN, and by proposing the solution explained in this thesis, one of our future objectives is to come up with a scientific article for publication .

Proposing new solutions and new future researches:

Our future objective is try to find new robust and strong algorithms in order to offer a reliable vehicular network. Also trustworthy in VSN rely on drivers's informations, and it connot be widely acepted by the public, so in our futere research directions we wil touch on the security and privacy issue in VSN.

Personal review :

During my researches and my work for the project I encountered many difficulties, the main challenges that I've faced during my work are the following :

- Accelerate skills training on project issues. Indeed, the projects are often short, which require to quickly understand the problem faced and the main objective of the project.

- Reconcile the time constraint and the high level of quality expected by adopting a methodological approach, adapting quickly and working efficiently... and when that is not enough, all that remains is to decouple efforts and surpass oneself to succeed !

On the other hand, working on this project gave me the opportunity to make the link between my academic knowledge and the professional world.

It allowed me to develop my technical skills, deepen my theoretical and practical knowledge and simulate my creativity.

And also the work allowed me to improve my knowledge and my rigor and to strengthen my professionalism.

Finally, this experience strengthened my motivation, my determination and my ambitions as a project professional.

Bibliography

1. A. Rahim, X. Kong, F. Xia, Z. Ning, N. Ullah, J. Wang, S.K. Das, Vehicular Social Networks: A survey, Pervasive and Mobile Computing (2017), https://doi.org/10.1016/j.pmcj.2017.12.004.
2. [Ning et al, 2017] Vehicular Social Networks - Enabling Smart Mobility.
3. Hongyu Jin, Mohammad Khodaei and Panos Papadimitratos Networked Systems Security Group, KTH Royal Institute of Technology, Sweden, Security and Privacy in Vehicular Social Networks arXiv:2001.08014v1 [cs.CR] 22 Jan 2020.
4. Q. Yang and H. Wang. "Towards Trustworthy Vehicular Social Networks, IEEE Communication Magazine, June, 2015, Volume: 53, Issue: 8 pp. 42-47.
5. Razi Iqbal1, Talal Ashraf Butt1, Muhammad Afzaal1 and Khaled Salah2, Trust management in social Internet of vehicles: Factors, challenges, blockchain, and fog solutions [2018].
6. S. Smaldone, L. Han, P. Shankar, L. Iftode, RoadSpeak: enabling voice chat on roadways using vehicular social networks, in: Proceedings of the 1st Workshop on Social Network Systems, ACM, 2008, pp. 43–48.
7. Rasheed Hussain1, Waqas Nawaz1, JooYoung Lee1, Junggab Son2, and Jung Taek Seo3, A Hybrid Trust Management Framework for Vehicular Social Networks.
8. Gai F, Zhang J, Zhu P, et al. Trust on the ratee: a trust management system for social Internet of vehicles. Wirel Commun Mob Comput 2017; 2017: 7089259.
9. Kamesh S and Priya S. Security enhancement of authenticated RFID generation. Int J Appl Eng Res 2014; 9(22): 5968–5974.
10. Chen R, Guo J and Bao F. Trust management for SOAbased IoT and its application to service composition. IEEE T Serv Comput 2016; 9(3): 482–495.

Webography

11. **https://www.sciencedirect.com/topics/computer-science/vehicular-ad-hoc-network.**
12. **https://www.intechopen.com/books/vehicular-technologies-deployment-and-applications/smart-vehicles-technologies-and-main-applications-in-vehicular-ad-hoc-networks.**
13. **https://socialnetworking.lovetoknow.com/about-social-networking/definition-online-social-networking.**
14. **https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT.**
15. **https://money.howstuffworks.com/business-communications/how-social-networks-work.htm.**
16. **https://money.howstuffworks.com/business-communications/how-social-networks-work.htm.**
17. **https://en.wikipedia.org/wiki/Graph_theory#:~:text=In%20mathematics%2C%20graph%20theory%20is,also%20called%20links%20or%20lines).**
18. **https://www.python-course.eu/graphs_python.php.**