PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA

MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH

MOHAMED BOUDIAF UNIVERSITY - M'SILA

FACULTY OF MATHEMATICS AND COMPUTER SCIENCE

DEPARTEMENT OF COMPUTER SCIENCE

N°:……..

FIELD:MATHEMATICS AND COMPUTER SCIENCE

BRANCH: COMPUTER SCIENCE

OPTION:NETWORK AND INFORMATION AND COMMUNICATION TECHNOLOGY

Thesis submitted for obtaining
From the Academic Master's degree

By: Ammari Aya

Bensalem Amani

Titled

Fault tolerance and VANET

(Vehicular Ad-Hoc Network)

Defended before the jury composed of:

Ouldmohamedi Nedjib	M'sila University	President
Bahache Mohamed	M'sila University	Rapporteur
Guesmia Salah	M'sila University	Reviewer

Academic year: 2021/ 2022

Dedication

For all those people who answered the call and never hesitated

For those who were there with their support.

For them all go our gratitude and credit, and to them all

We dedicate this modest work.

Acknowledgments

We are pleased to describe our deepest gratitude to our supervisor Dr. Ould Mohamedi Nedjib for his invaluable feedback that has shaped and assembled this study.

We would like to express our sincere thanks to the members of the jury who have red, evaluated, and discussed the dissertation, as well as all the teachers who have ever enlightened us with their wisdom and knowledge along our study pathway.

We expand our gratitude to our parents, families, and friends for their unconditional care, support, and inspiration. Above all, our gratitude goes to Allah (SWT) who showered us his blessings in our everyday lives, especially for the strength, patience, and guidance in realization of this work.

Table of contents

List of tables

List of figures

Abbreviations

AODV	Ad-Hoc on-Demand Distance Vector
DDOS	Distributed Denial of Service
DOS	Denial of Service
DSDV	Destination Sequenced Distance vector
DSR	Dynamic Source Routing
DSRC	Dedicated Short Range Communication
EDR	Event Data Recorder
FSR	Fisheye State Routing
GPS	Global Positioning System
GPSR	Greedy Perimeter Stateless Routing
GYTAR	Greedy Traffic Aware Routing
HARP	Home Agent Redundancy Protocol
I2I	Infrastructure to Infrastructure
Manet	Mobile Ad-hoc Networks
MIBR	Mobile Infrastructure Based VANET Routing
OBE	On -Board Equipment
OBU	On -Board Unit
OLSR	Optimized Link State Routing
OM	Oral Messages
QOS	Quality Of Service
RDMAR	Relative Distance Micro-discovery Ad-hoc Routing
RpCQ	Reply Channel queue
RqCQ	Request Channel queue
RSE	Road-Side Equipment
RSU	Road-Side Unit

TA	Trusted Authority
TBRPF	Topology Dissemination Based on Reverse-Path Forwarding
TORA	Temporarily Ordered Routing Algorithm
VANET	Vehicular Ad-hoc Networks
V2I	Vehicle-to-Infrastructure
V2V	Vehicle to Vehicle
VGPR	Vertex-Based Predictive Greedy Routing
WAVE	Wireless Access in the Vehicle Environment
ZRP	Zone Routing Protocol

General Introduction

In the last decade, the world witnessed a remarkable technological development, especially in the field of wireless networks, which touched many areas, including cars that were in the past only a preserve of mechanical engineers, but with the progress made especially in the field of its industry, it started to include many network engineers.

These wireless networks are known in the field of cars as VANET, and they were established in order to improve transportation systems and provide security and safety on the roads. Indeed, it was specified for the road users as they provide many services and applications due to the existing communication between its components.

However, like the other networks, this network is exposed to malfunctions and attacks that hinder its work. Accordingly, this prompts us to use fault tolerance strategies, which is the main topic of this research.

In this study, we will propose a tolerance strategy for the problem of RSU being exposed to a spoofing attack that makes it faulty, This strategy is based on Oral Messages algorithm which works to detect faulty nodes.

The study at hands is arranged as follows:

In the first chapter, we talked about forgiving mistakes in general by mentioning its objective, techniques and work methodology.

In the second chapter, we gave an overview of the VANET network (Components, Applications , characteristics ,challenges …).

In the third chapter, we mentioned the various faults that can occur in the vanet and its components, we also discussed the various attacks in this network as one of the causes of those faults.

In the last chapter, we proposed a strategy that tolerate one type of attacks which is spoofing attack using oral message algorithm (OM).

CHAPTER 1

FAULT TOLERANCE IN GENERAL

1.1 Introduction:

Recently, the field of technology has witnessed a remarkable development in wireless networks. With this development, these networks have become more and more complex, and ensuring their safety and continuity of operation has become among the challenges that must be faced. In order to overcome these challenges and to provide better services, fault tolerance techniques were used. In this chapter we will examine fault tolerance in general.

1.2 The Dependability:[1]

dependability of a system is the ability to avoid service failures that are more frequent and more severe than is acceptable. It consists of three parts: the threats to, the attributes of, and the means by which dependability is attained. They are shown in **Figure 1.1**

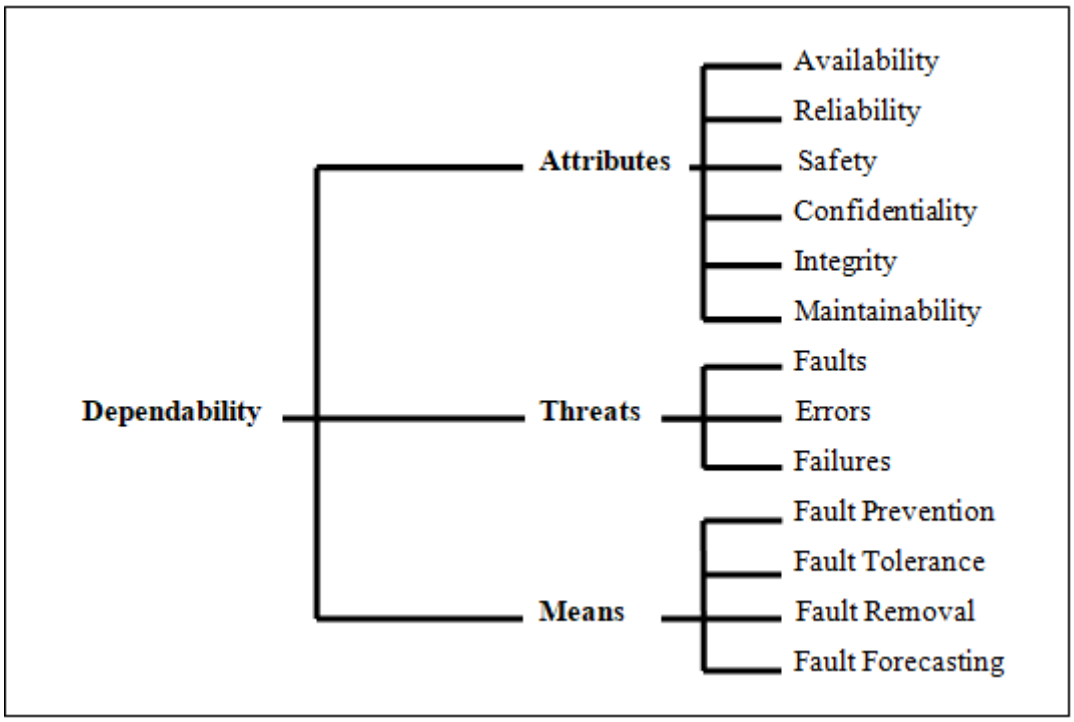

Figure 1.1 The dependability tree

1.2.1 The Attributes:

The dependability integrates the following attributes that are considered as the qualitative and quantitative measures of system dependability [1][2]:

- **availability:** means that the system is ready to provide the service when the user asked it.
- **reliability:** means that the system can continue to execute its services correctly without any failure.
- **safety:** absence of catastrophic consequences on the user(s) and the environment.
- **confidentiality:** absence of unauthorized disclosure of information.
- **integrity:** absence of improper system alterations.
- **maintainability:** ability to undergo, modifications, and repairs.

1.2.2 Threats:

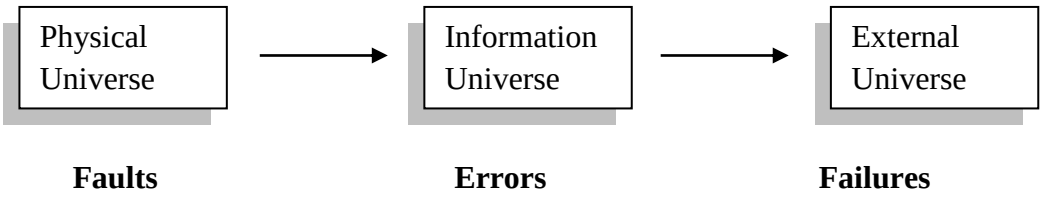

Figure 1.2 The Three-universe model.

- **Fault:** abnormal state that can cause a system component to fail.
- **Error:** is a consequence of a fault and state not tolerated by the system specifications.
- Failure: occurs when an error reaches the service interface and alters the service[1].

1.2.3 Means:

Combination of following means is used for development of a safe system [2]:

- **Fault prevention:** how to prevent the occurrence or introduction of faults.
- **Fault tolerance:** how to deliver correct service in the presence of faults.
- **Fault removal:** how to reduce the number or severity of faults.
- **Fault forecasting:** how to estimate the present number, the future incidence, and the likely consequences of faults.

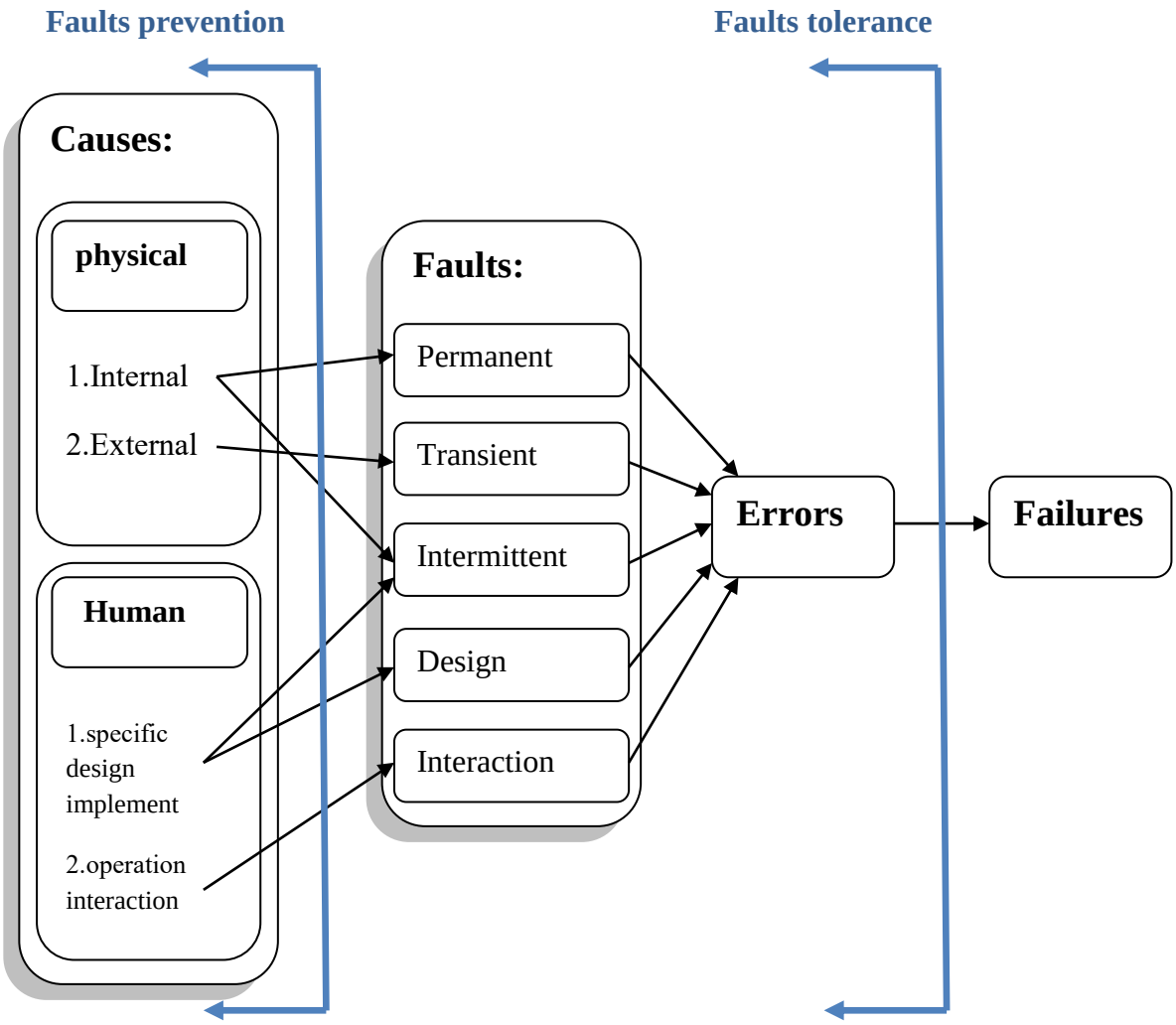

Figure 1.3 The design barriers of fault prevention and tolerance to improve dependability.

1.3 fault tolerance:

Fault tolerance is a design method that allows a system to remain functional, possibly in a reduced way, instead of breaking down completely and remaining more or less operational when one of its components no longer works correctly with a reduction in the throughput or an increase in response time.

1.4 Faults Classification:

There are different types of faults that canoccur in a system Dependingon certain criteria. In what follows, a classification of faults according to three criteria is presented:

- Fault origin.
- Fault nature.
- Fault duration.
- Fault effect.

1.4.1 Faults according to the origin:

This category includes the following types of faults:

- **Hardware faults:** This type of fault occur when the specified hardware for the given software does not work properly. It is also known as Physical Fault.
- **Software faults:** they can occur due to design faults. They can be classified according to their creation phases: development faults or operational faults**.**

1.4.2 Faults according to the nature:

- **Accidental faults:** they occur accidentally, either by executing erroneous code or by installing a badly configured or less conforming component.
- **Intentional faults :**they are the set of malicious actions that constitute the risk for a system to break down, like viruses.

1.4.3 Faults according to the duration:

- **Transient faults:** faults disappear automatically after a certain period of time.
- **Permanent faults:** faults of unlimited duration, It only disappears with an external intervention.
- **Intermittent faults:** may this type of failure occurs randomly, that is mean stops and resumes at an irregular interval.

1.4.4 Faults according to the effect:

We can classify failures based on how they are perceived by the rest of the system into 5 failures types, which are:

- **Timing (performance failure):** this failure means that the node no longer provides its service on time (the result is late or too early). it deliver a response correctly, but this response is outside the expected time interval.
- **Omission failure:** is a failure where a the node response never appears to be sent (taking an infinitely late amount of time to respond), so this fault is considered as temporal of infinite duration. It is used to represent network faults. It comes in two forms:

  Send Omission**:** a node fails to send response.

  Receive Omission: a node fails to receive another node response .

- **Crash(frank failure):**is a permanent failure, so once the component is in frank failure, it ceases immediately and indefinitely to respond to any solicitation or to generate new requests.
- **Response failure:** the node provides incorrect or inaccurate response. this may be caused by software and/or hardware failures, corrupted messages or by malicious nodes generating incorrect values. It comes in two forms too:
  Value failure: the value of the response is wrong.
  State-transition failure: Deviates from the correct flow of control.
- **Byzantine (Arbitrary failure):**They simply correspond to an arbitrary type offault, and are therefore the most malicious breakdowns possible.

1.5 General fault tolerance procedure:

The number of phases configured for fault tolerance varies with different systems; however, some general steps are implemented in most systems and are shown in **Figure 1.3**

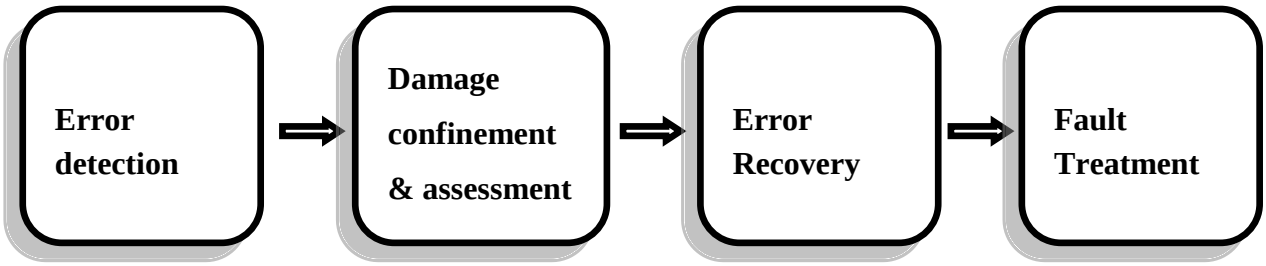

Figure 1.4: General fault tolerance procedure

1.5.1 Error detection:

This is the usual first step for fault tolerance techniques. To detect errors there are many detection techniques, among the techniques used, we have:

- **Replication checks:** The system uses multiple replicas of component working in the same time and any difference in their outputs is an indication of an error.
- **Diagnostic checks:** the diagnostic checks establish whether a component is working properly through the applying of known inputs with a known outputs.

- **Timing checks:** In order to detect timing errors, the time checks approach is utilized. A timer is used for each operation of the component to detect if the time to finish an operation is longer than the expected time.

1.5.2 Damage confinement and assessment:

Because of the time lag between the occurrence of a fault and the detection of it, invalid information may have spread from the faulty component to others, resulting in other faults that have not yet been discovered. thus, in this case the damage confinement procedure is used to determine and isolate the components where the error occurred.

1.5.3 Error Recovery:

Following error detection and damage assessment comes error recovery, which is the most important phase of any fault tolerance technique.

This procedure will used to convert the current erroneous system state into a well-defined and error-free state. There are two general approaches to achieving this, forward-error recovery and backward-error recovery.

Forward-Error Recovery: In the forward error recovery the system is moved to a new valid state following a precise detection and isolation of the fault that caused the error [15].

- **Backward -Error Recovery:** periodically take checkpoints to save a correct computation state. When error is detected, roll back to a previous checkpoint, restore the correct state and resume execution.

1.5.4 Fault Treatment:

In the previous phase the system was returned to an error-free state, but the error might repeat, so in this phase the system is repaired by removing or isolating the faulty components which are thereafter replaced by another functional components (standby components).

The integration of the standby components into the system is a difficult process in which the state of the standby components should be synchronized with the rest of the system. There are three general types of standby schemes [15]:

- **Cold standby:** In the cold standby approach the standby component is not operational, and a synchronization of it state is necessary during its initialization, a process that requires additional time for the complete system recovery.
- **Warm standby:** In warm standby, the standby components keep the last valid state of the operational component (checkpoints) and when the principal component fails, the standby components are integrated in the system with the last checkpoint state.
- **Hot standby:** The hot standby practice requires the standby component to be fully active, duplicating the function of the primary component. Therefore, in the case that an error occurs, recovery can be practically instantaneous.

1.6 Fault Tolerance techniques:

There are many fault tolerance techniques that depend on redundancy, so we can say that fault tolerance is based on it.

Redundancy: Providing multiple identical instances of the same system and switching to one of the remaining instances in case of a failure (failover).. It can be: hardware, software, time or information redundancy.

2 **Hardware redundancy:** Based on the use of multiple physical components to avoid hardware.

3 **Software Redundancy:** based on the use of programs that support fault tolerance (Recovery blocks).

4 **Time (execution) redundancy:** Based on multiple executions of some instructions in different times (Check pointing and rollback recovery).

5 **Information Redundancy**: Based on coding data in such a way that a certain number of bit errors can be detected and/or corrected.

We can classify the fault tolerance techniques as follows:

1.6.1 Proactive techniques :

aims to identify faults ahead of time and replace suspicious components with proper replacements, thus eliminating error recovery. The techniques based on this policy are:

- **Process migration:**

  is the act of transferring a process between two machines. Migration improves the

fault resilience of a system on abnormal and unstable situations e.g. a partially failed node, or in the case of long-running applications when failures of different kinds (network, devices) are probable [15]. In some articles they classify it in Reactive techniques, both classifications are correct.

- **Active Redundancy (Replication):**
  Providing multiple identical component in the network and directing tasks or requests to all of them in parallel making it possible to get a result even though one or component node has failed. multi-route routing (characterized by the presence of many possible paths to route a message) is an example of this redundancy.

1.6.2 Reactive techniques :

When a fault occurs, this policy is used to eliminate the effects of it and to restore the system. The techniques based on this policy are:

- **Checkpoint:**
  The system state is saved periodically to avoid losing everything in the event of a failure. When a malfunction is detected, it returns to the last checkpoint in order to continue the failed task from the point of failure 15

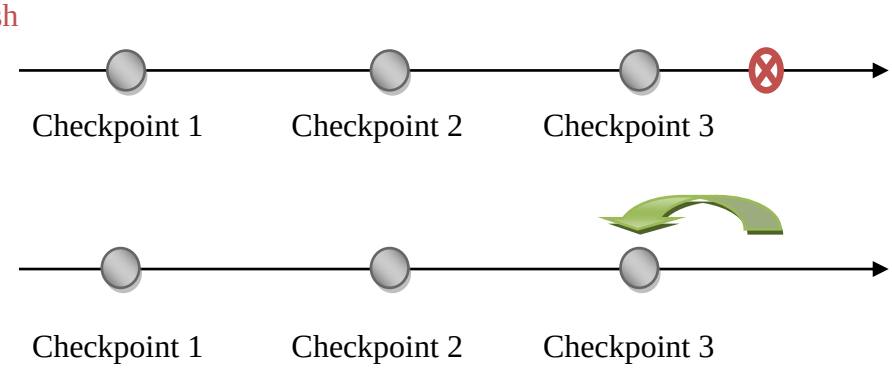

Figure 1.5: Checkpoint technique

- **Passive Redundancy :**
  Only the active component (original component) processes requests. Moving to the spare components happens only when the active component fails. It is therefore necessary to maintain a certain consistency between the spare components and this component by periodically transferring the state and information of requests from the original component to the spare components.

1.7 Conclusion:

In this chapter, we have discussed dependability and its main concepts in addition to faults and their types in wireless networks. Then, we addressed fault tolerance as one of the mechanisms for achieving reliability and ensuring operational safety, which makes it an indispensable part of wireless networks.

CHAPTER 2

General information on VANETs

2.1 Introduction:

Recently, the world has seen a significant technological advancement which affected many fields including wireless networks that's undergoing a massive development. With the increase of population and the expansion of roads, traffic increased dreadfully with an uncountable number of victims. Therefore ،a technology designed to reduce accidents must be used and the assistance of commuters have to be provided. A new ad hoc mobile network appeared, it's known as VANET (Vehicular Ad-hoc Networks) which is a certain type of MANET (Mobile Ad-hoc Networks). In VANET every vehicle acting as node behaves like a router to exchange data between different nodes in the network. Thus, we'll know more about this technique in this chapter.

2.2 wireless networks:

It is a network that is not connected by cables of any kind. Communication in it is done over the air, the basis of wireless systems is radio waves. it has two types : networks with infrastructure and without infrastructure (ad- hoc).

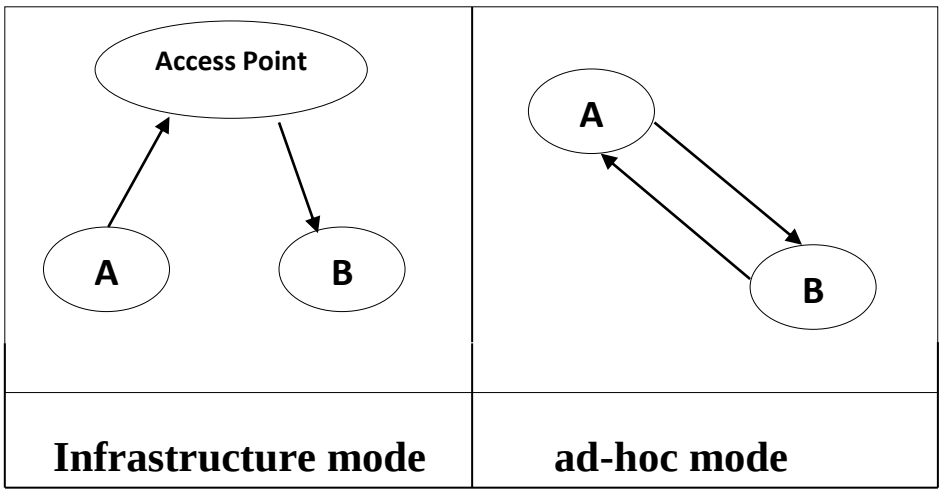

Figure 2.1 Types of wireless networks

2.3 Ad-hoc vehicular networks (VANETs):

2.3.1 Definition of ad-hoc network:

An ad hoc network is a (possibly mobile) collection of communications devices (nodes) that wish to communicate, but have no fixed infrastructure available, and have no pre-determined organization of available links. This individual nodes are responsible for dynamically discovering which other nodes they can directly communicate with [11] .

2.3.2 Definition of VANET:

It is a subtype of mobile ad hoc network (MANET). Nodes in network are vehicles (smart vehicles) and road side unit (RSU) deployed along road side. It is highly dynamic network as the vehicles are moving with a speed of 40–200 km/h [16] .**Figure 2.2** models a smart vehicle.

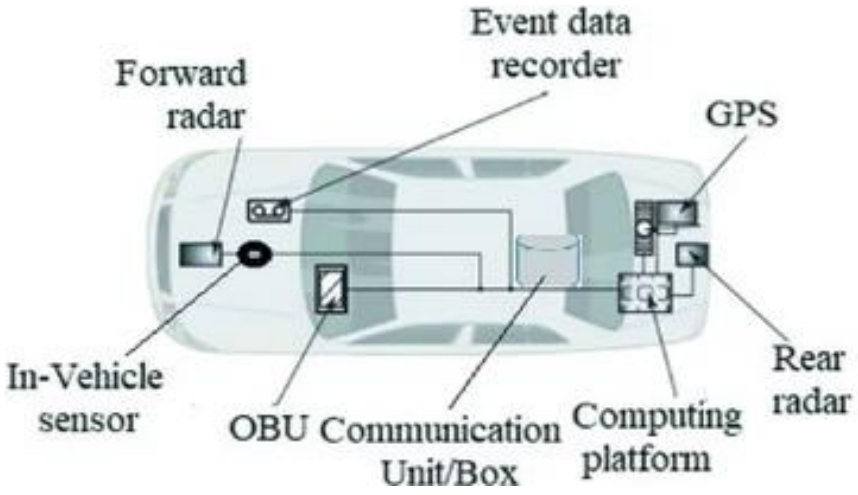

Figure 2.2 Smart Vehicle

2.3.3 The domains of VANET[7].:

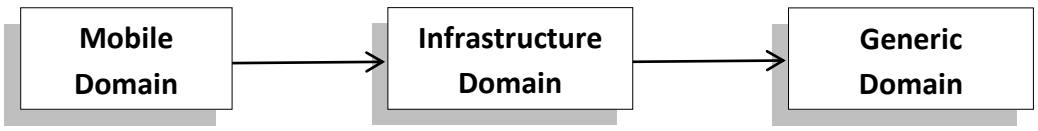

Figure 2.3 Domains of VANET

- Mobile domain: This domain communicates and exchanges data with the Infrastructure domain. It is divided into vehicle domain such as buses, cars and mobile device domain such as laptop, GPS .
- Infrastructure domain: Its includes traffic lights etc. after the exchanges of data with the first domain it start to analyze data and share it with the generic domain.
- Generic domain: it includes different nodes and servers that is working directly or indirectly with VANET.

2.3.4 Components of VANETs:

VANET consists of [12]:

a- **Road Side Unit or Equipment (RSU/RSE):** A roadside unit is a device that is permanently installed alongside a road or in a specific location and is used to give local connectivity to passing vehicles.

Figure 2.4 Road Side Unit

RSU's Function: RSUs are deployed on the roadside where they help to network performance in a VANET. The following are some roles of RSUs [16]:

- Message delivery to vehicles.
- Forwarding message to other vehicles.
- Internet access to vehicles.
- Interface between vehicle and trusted authority (TA).

RSU architectures components [16]:

Request channel queue: Whenever an RSU receives packets from vehicles, it first moves to RqCQ, and as per priority, it gets processed by the RSU.

Reply channel queue: Reply packets are getting stored in RpCQ, and as per priority, they are forwarded to other vehicles or RSUs.

Network: To communicate between vehicles, other RSUs, and TASs.

Memory: To store data.

Module for making decisions: It receives the packets, and processes the data and takes decisions that suit applications.

Scheduler: This helps a VANET to manage packet priority.

b- **On -Board Unit or Equipment (OBU/OBE):** Is a GPS-based tracking device found in vehicles in order to share their information with RSUs and other OBUs , it is characterized by the presence of sensors.

Figure 2.5 On-Board Unit

c- **Trusted Authority (TA):** is responsible for managing VANET. it works to identify and register any device or person that has a relation with VANET. Its task is to find out everything that is happening in the system as well as to identify any attack.

d- **Event Data Recorder (EDR):**It is a device on vehicle which keeps the track of communications sent to or received from other vehicles [16].

Figure 2.6 Event Data Recorder

e- **Global Positioning System (GPS):** It is a device that provides the facility of map and also keeps the track of location of a vehicle.

2.3.5 Types of messages in VANET:

Messages in VANET are divided into two types:

Service Messages: Means the messages used when requesting or responding to a service we find two types:

- Safety Messages :It works to help road users by giving alerts, for example, in the event of congestion or an accident (beacons).
- Non safety Messages :These types of messages are less priority than the first type, but they have an important role in making driving more comfortable as they provide helpful information.

Control Messages: This type of message is used to control the network for example Network setup, Authentication, Network policy update.

2.3.6 VANET communication types:

It is characterized into 5 sections which are illustrated in **Figure 2.7**:

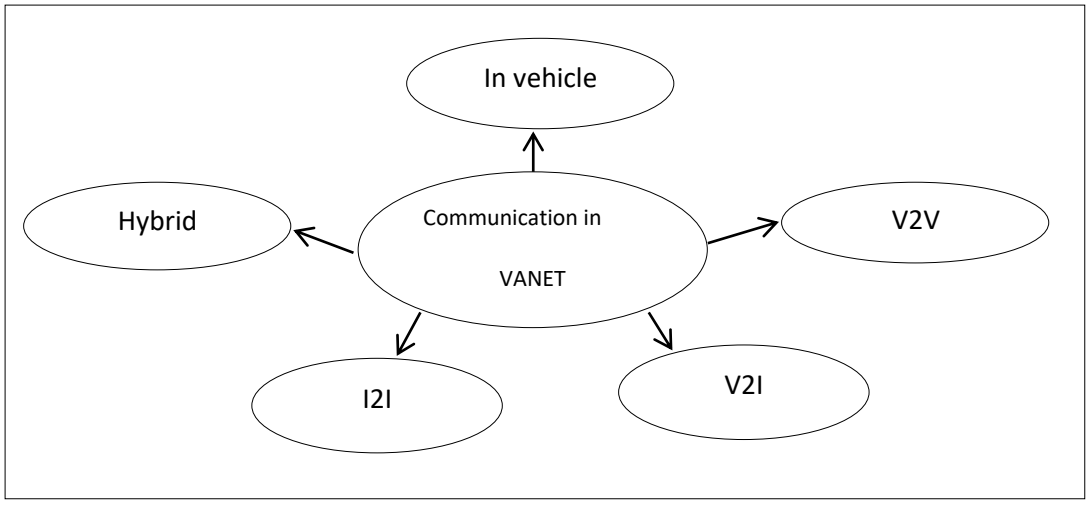

Figure 2.7VANET Communication Types

1-**In vehicle communication:** it's specialized in detecting vehicle system data and all driver's related factors such as fatigue [5].

2-**Vehicle to Vehicle communication (V2V):** It refers to inter vehicle communication in which the data exchange between vehicles in order to help the drivers by alerting them about warnings and other critical information [5].

Advantages of V2V communication[13]:

- Less cost.
- It does not need any roadside infrastructure.
- Improve vehicle safety by protecting them from potential road dangers.

Disadvantages of V2V communication:

- Problems in long range communication
- Problems in broadcasting messages in high traffic .

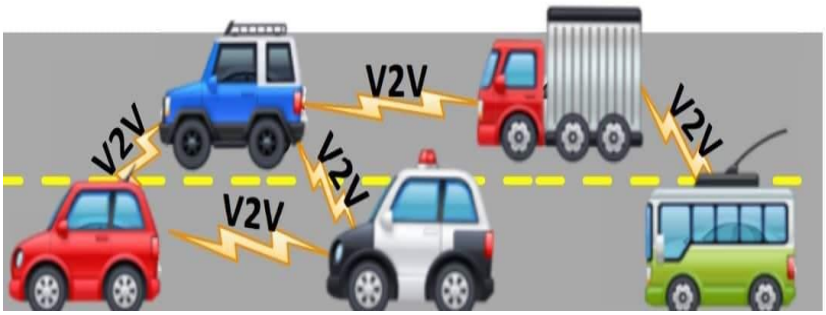

Figure 2.8 Vehicle to Vehicle communication (V2V)

3-**Vehicle-to-Infrastructure communication (V2I):** It is the communication between vehicles and roadside fixed infrastructure so as to collect data .It is essential to provide the latest updates such as real time traffic update or weather update.

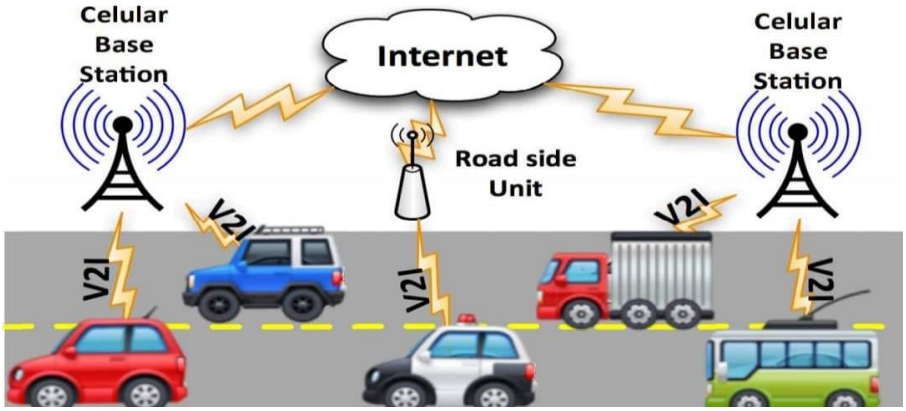

Figure 2.9 Vehicle to Infrastructure communication (V2I)

4-**Infrastructure to Infrastructure Communication(I2I):** the communication between RSUs in the network define with purely a static network as there are no moving nodes .we use this type of communication for various purposes such as to pass emergency information about bad weather, to cross-check log of vehicles, to intimate about accident etc. The RSU in this network communicates with the other RSU through either a wired or wireless medium [16].

5-Hybrid Communication: It combines both Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) , It allows for long distance connection to the Internet or to vehicles that are far away [6].

Figure 2.10 Hybrid Communication

2.3.7 Application of VANET:

The communications in VANET enable for the development of a huge number of apps and can give drivers and travelers with a wide range of information. The following applications are listed [9]:

- Safety Applications: These applications have been developed for several purposes, including providing traffic safety, reducing accidents and thus saving human lives as the majority of accidents and loss of life occur due to collisions or lack of safety while driving. Three main applications are explained as follows[14]:
  - ✓ Collision avoidance: specially the accidents in junction so when an accident occurs, a signal is generated and is transmitted to other vehicles. That's mean the other vehicles stay away from that place and does not create chaos in the emergency area. This information can be in form of vehicle speed, direction and route.
  - ✓ Traffic optimization: By collecting data from vehicles. When critical situations arise, a warning signal can be deployed to drivers in remote locations so that they do not reach the same place and cause more congestion. By warning vehicles of such situations it can improve traffic.
  - ✓ Cooperative driving: It lies in exchanging and sharing road information between drivers to avoid all embarrassing situations and have an improved journey.
- Commercial Applications: we see that this type provides drivers with entertainment services, such as using the web for online shopping.
- Convenience Applications: the main aim of these application is to make the driver during the trip feel comfort. By providing the nearby restaurant, gas station, the available parking, weather and traffic information.

2.3.8 Characteristics of VANETs:

VANET networks are a branch of MANET networks so we note that they are involved in many things but there are some characteristics that make VANET a different network, including [5]:

- Unrestrained network size: This means that the geographical area of application of this network is wide and unlimited. As we can implement it for one city or several cities or countries.
- Network topology: mobility and erratic vehicle speeds lead to the frequent change of nodes As a result, the topology of VANET networks is constantly changing.
- Security and anonymity: the importance of information exchanged via communications vehicles makes the operation of securing these networks necessary and important.
- No problem with power and storage: Nodes in VANET do not suffer from power and storage limitation as in sensor networks.
- On board sensors: The sensors can read data relating to vehicle speed, direction and can communicate with the data center.

2.3.9 Challenges and Future Research Directions:

We can consider the challenges as future research that needs further progress. Here are some of these challenges [7] [14] [10] [3]:

1. High Mobility : The mobility of nodes in a VANET is quite high because vehicles come and go in a matter of seconds. As a result, it is an open research topic that requires further development.
2. Quality Of Service (Qos): nodes in a VANET are in perpetual motion. That's why node position, topology, the distance between nodes, connection ,etc. differ. thus the service of routing protocols reduce. As a result, it is both a problem that has to be solved and an open research issue.
3. Volatility: The connections between vehicles in VANETs may be lost or stay active, it makes difficult to ensure personal security in VANETs .Therefore, it needs to develop to make the network more secure.
4. Support of network intelligence: In future VANETs, vehicles will be equipped with a huge number of sensors, and the edge cloud will gather and preprocess the data before sharing it with other portions of the network.
5. Security and privacy: The issue of security is one of the most important issues in VANET networks due to the nature of the latter and its use of air as a medium for transmission. It is an open network that allows any node to join the network and transfer data. Therefore, it is

necessary to improve and develop strong security models to ensure security and privacy in VANET.

2.3.10 Routing in VANETs:

2.3.10.1 Definition:

Routing is the process of determining the best route from source to destination.High mobility of nodes and rapid changes of topology are the main factors that influence the need of generating an efficient routing protocol which can deliver a packet in minimum period of time [7].

2.3.10.2 Routing protocols in VANETS networks:

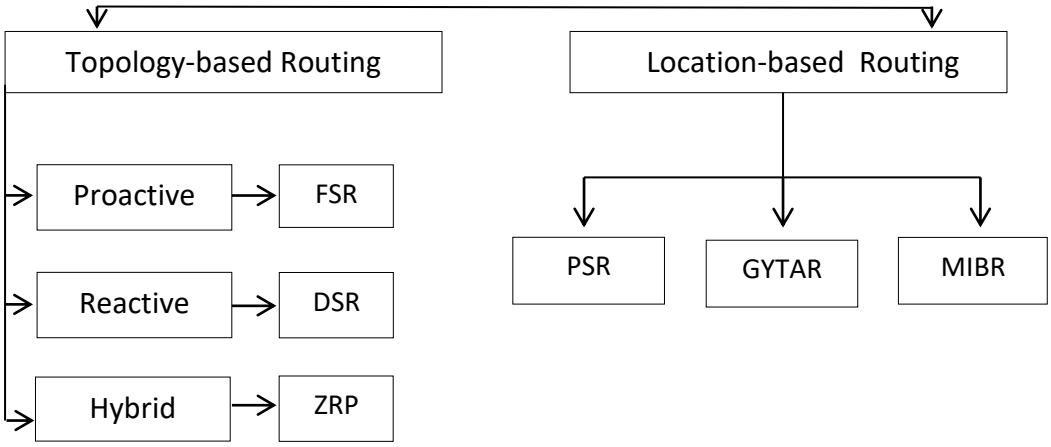

Figure 2.11 Routing protocols

Generally, routing protocols can be categorized into two types which are [4] :

1. **Topology-based Routing:** These routing protocols use link information that exists between nodes to route packets. They are classified into 3 types which areproactive, reactive and hybrid.

- Proactive: In this protocol, nodes information is stored in the form of tables. Whenever any change occurs in the Network, the tables are updated accordingly (constantly maintain updated routes). Nodes exchange topology information so that they always have route information. When looking for a new route, there is no route discovery delay. Here are some examples of protocols:
    - ✓ FSR (Fisheye State Routing) .
    - ✓ OLSR (Optimized Link State Routing).
    - ✓ DSDV (Destination Sequenced-Distance –vector routing protocol).

- ✓ TBRPF (Topology Dissemination Based on Reverse-Path Forwarding).

- Reactive: In Reactive Protocols routes are discovered only when a source node requests a route and expires after some time. When a node wants to send a packet, it starts searching for the desired path. If a node receives this packet and does not know the destination, it also broadcasts a path-finding message. Here are some examples of protocols:
  - ✓ AODV (Ad-Hoc on-Demand Distance-Vector Routing Protocol).
  - ✓ DSR (Dynamic Source Routing).
  - ✓ RDMAR (Relative Distance Micro discovery Ad Hoc Routing).
- Hybrid: Hybrid protocols combine the benefits of proactive and reactive protocols, their advantage is that they adapt to large networks. Some examples of protocols:
  - ✓ ZRP (Zone Routing Protocol).
  - ✓ TORA (Temporarily Ordered Routing Algorithm).
  - ✓ HARP (Home Agent Redundancy Protocol).

2. **location-based Routing:** These protocols are based on the idea that the source sends a message to the geographical location of the destination instead of using the network address we can define this types :

   GPSR (Greedy Perimeter Stateless Routing).

   GYTAR (Greedy Traffic Aware Routing protocol).

   MIBR (Mobile Infrastructure Based VANET Routing).

2.4 Communication standards used in networks:

DSRC (Dedicated Short Range Communication): A short range communication system designed for safety and entertainment applications to be used in V2V and V2I communication environments it is the only technology that offers several advantages, including:

- High speed of establishing the connection.
- Minimum Delay Time: In safety applications, the vehicle must be able to recognize another vehicle and communicate with it in a very short time.

- Security and privacy.
- High reliability: That is why DSRC works with high speed vehicles and in severe weather conditions.

IEEE 802.11p:it is an upgraded version of the IEEE 11.802 standard for adding wireless access in the vehicle environment (WAVE).

IEEE 1609: a higher-layer standard based on IEEE 802.11p .it is a set of standards to support safety applications in vehicular networks.

2.5 Conclusion:

In this chapter, we talked about the VANET starting with concepts about networks to give an overview of the topic. Then, we got to know the Components, communication types, applications, characteristics, and routing of the VANET. We saw that VANET is very diverse which is what made it gain these characteristics. Then we gave some challenges and future research that needs to be developed to make this network more effective.

Chapter 3

Faults in VANET

3.1 Introduction:

The interest in vehicular ad-hoc network has increased in recent years due to the privileges and services they offer, especially for road users. But this does not mean that the network is secure because of the possibility of malfunctions and attacks that may affect some important elements in the network, thus losing their effective function and detracting from the security of the network. We'll see in this chapter some of the security requirements that the network needs to operate safely, we will also learn about the sources of faults that can affect wireless networks in general and VANET network in particular.

3.2 VANET Security :

The security services increase the security of processing and data exchange in VANET. The security requirements explained below [16]:

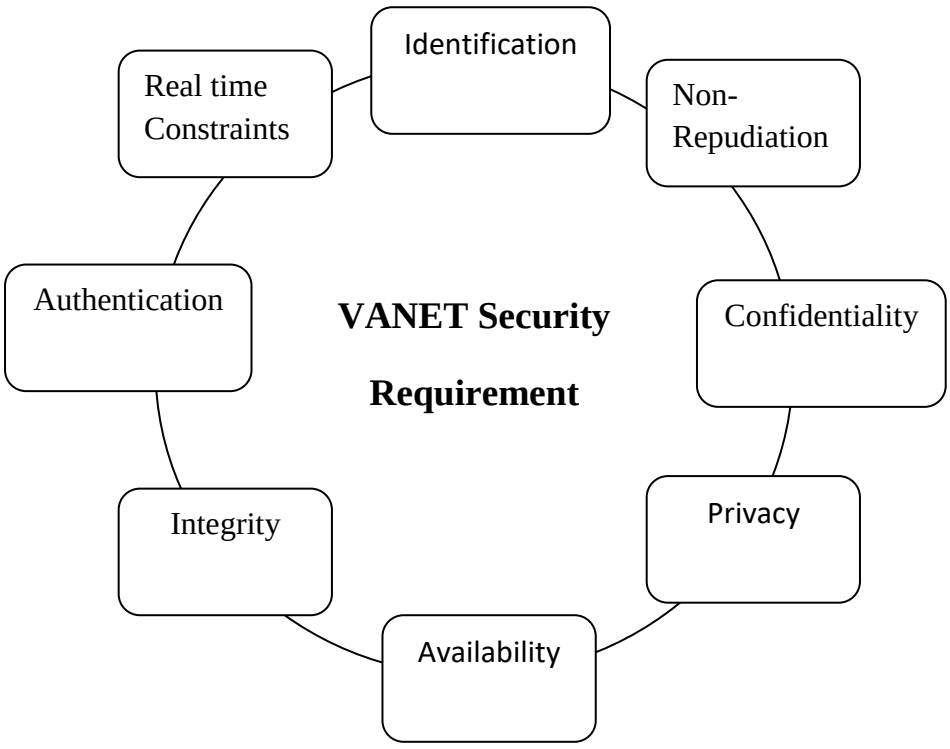

Figure 3.1 VANET Security Requirement

Identification: it means identifying valid users.

Authentication: confirms that the message was sent by a real user. Receiver will only trust on data which are coming from the authenticated source.

Privacy: the main goal of security is privacy. it aims to maintain information on any node in VANET, such as the speed and destination of vehicles.

Non-Repudiation: prevents the sender or receiver from denying the sending or receiving of messages.

Real time constraints: time guarantee is a very important aspect in VANET. Since the mobility is very high, the delay in response leads to catastrophe occurs.

Availability, Integrity and Confidentiality are explained in the first chapter.

3.3 Faults Sources:

We can classify these errors according to the propagation of the fault into:

3.3.1 Nodes Faults:

The nodes can be exposed to faults, whether in its hardware components or software components (generally a hardware fault always leads to a software fault). The following are some of the causes of these faults in general:

- Node software bugs.
- Nodes get exposed to external accidents such as shocks.
- Environmental conditions such as vibrations.

Now, we will tackle the nodes faults specifically through mentioning some expected faults for each node and its effect on the work of this node as well as on the network in general.

On-Board Unit (OBU):

The on-board unit faults can occur for several reasons, including:

1. trying to remove the On-Board Unit from the vehicle or modify it in any way without the assistance of the competent authorities.
2. trying to connect any additional devices to the OBU.

3. Splitting the speedometer signal, used for the automatic toll system, also can cause faults or failure of the On-Board Unit.
4. Also, as vehicles in roads are managed by a driver, the behavior of this latter can damage the system.
5. Faults that are resulted from an incomplete concept such as faults in the OBU formal design (hardware and/or software design fault) or in its integration into the system by the competent authorities.
6. Faults during maintenance.

as a result for those faults:

- causes wrong functionality and failures conducting to offline services and applications.
- sending a fault result to the rest of OBUs and RSUs. Thus, the fault information spreads across the network.
- Or isolating the vehicle from the rest of the network (The OBU lose connection with other OBUs and RSUs). This result is considered the least harmful among the results because in this case the vehicle becomes ineffective for the network.

7. We know that the OBU collect data from various inbuilt sensors; such as traffic data And mobility data and provide decisions after processing to various applications[16], but what if one of these sensors is a faulty one (providing incorrect readings); this will cause the OBU to process faulty data which coming from the faulty sensor and pass it to the application layer where various applications use this faulty data to accomplish objectives of different applications. This can change the behavior of users, especially if these data are sensitive data.
8. Also the OBU use wireless sensors to forward the data to various VANET nodes [16] and any faults in these wireless sensors will lead to a failure in data forwarding.

these faults can belong to more than one category as shown in **Table 3.1 .**

		Fault N° 1	Fault N° 2	Fault N° 3	Fault N° 4	Fault N° 5	Fault N° 6	Fault N° 7
Phase of creation	Development faults				✓	✓		
	Operational faults						✓	✓
System boundaries	Internal faults				✓	✓	✓	✓
	External faults							
Phenomeno-Logical cause	Natural faults						✓	✓
	Human made faults	✓	✓	✓				
Dimension	Hardware faults				✓		✓	✓
	Software faults	✓	✓	✓	✓	✓		
Capability	Accidental faults						✓	✓
	Incompetence faults				✓	✓		

Table 3.1 OBU Faults Classification

Roadside Unit (RSU) :

Including the reasons that cause faults in RSU:

1. An error during the installation of RSU that leads to no contact with the infrastructure.
2. Deployment faults, such as installing an RSU in an inappropriate location due to the existence of walls, buildings and other objects can be an obstacle to exchanging messages with this RSU. Faults of this kind lead to the loss of many messages, whether the sent one or the received one by this node.
3. Misinterpretation of data by the sscheduler can occur by considering emergency messages as normal messages and thus retreating the priority of dealing with them, and this can lead to hazardous situation in the network.

		Fault N° 1	Fault N° 2	Fault N° 3
Phase of creation	Development faults			
	Operational faults	✓	✓	✓
System boundaries	Internal faults	✓		✓
	External faults		✓	
Phenomeno Logical cause	Natural faults			✓
	Human made faults	✓	✓	
Dimension	Hardware faults	✓		
	Software faults		✓	✓
Capability	Accidental faults			✓
	Incompetence faults	✓	✓	

Table 3.2 RSU Faults Classification

These two nodes (OBU and RSU) also can be exposed to malicious faults. We can shorten these faults in attacks of all kinds, whether the attacker is internal or external one (In general, an internal attacker is more dangerous than an external attacker (In general, an internal attacker is more dangerous than an external attacker).

The OBU/ RSU can be exposed to attacks such as DOS, DDos, Spoofing and Sybil these attacks can cause:

- The node to be isolated from the rest of the network.
- Spread misinformation in the network.
- Exploit node data especially sensitive data.

Trusted Authority (TA):

A software failure as a result of an attack that has changed the identity of the nodes which belong to the network and therefore, when these nodes try to communicate the TA will consider them as intruders.

3.3.2 Network faults:

When we talk about the network in VANET, we must talk about routing as one of the most important aspects of it, as it is necessary for the communication between the different nodes, and any fault in it can lead to communication failure and loss of messages.

Among the possible causes of fault of this type:

1. The high mobility in VANETs causes high topology changes and in turn leads to excessive control overhead messages and frequent link failures.
2. As nodes moves in different speeds, they connect and disconnect frequently. Disconnection of nodes causes an interruption in communication. Thus, it requires retransmission of data. Disconnection may cause data loss and time delay in sending data at the receiver end.
3. Congestion of data because there are a lot of vehicles belonging to the network which leads to a large exchange of messages.
4. Presence of bugs in the routing function.
5. Poor selection of the appropriate routing protocol for the applications used.
6. The limitation of the radio band.

7. The physical obstructions made by the continuous atmospheric changes and solid structures (building, trees, tunnel ...etc.) also may prevent wireless signals to reach the desired coverage area.
8. A faulty important node entering the routing mechanism will lead to fault at the network (Eg: faulty node in the cluster head).

3.4 VANET Attacks:

The network faces many challenges due to the nature of the wireless medium, the size of the network, the speed of the vehicles, which makes it vulnerable to various malicious acts such as wireless attacks.

There are several types of attacks that are categorized according to the layer they are attacking (physical layer, network layer, application layer).Below we will mention some types of attacks in two different layers:

3.4.1 Application Layer Attacks:

In attacks of this type, the attacker's goal is to use applications for personal advantage by changing their content. Among these attacks, we mention:

- **Bogus Information Attack:**

The attacker sends false and fake information in the network, that information affects the behaviour of users in this network.

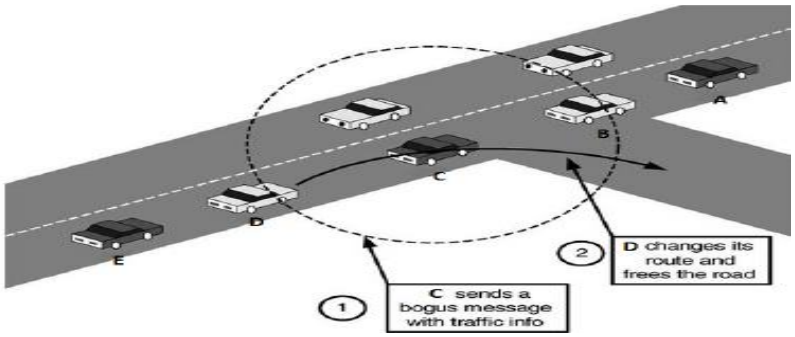

Figure 3.2 :Bogus Information Attack

3.4.2 Network Layer Attacks:

It is the layer most vulnerable to attacks, the attack can be on vehicles or on the network as a whole. Among these attacks:

- **Denial of Service Attack (DOS):**

The basic goal of a DOS attack is to prevent authorized users from accessing services. In a DOS attack, the attacker sends many phony messages to the network in attempt to attract attention, gain network privileges, or degrade the network's efficiency.

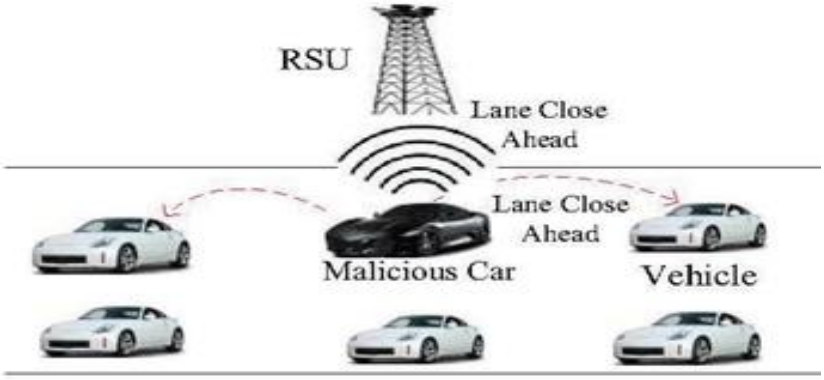

Figure 3.3 :DOS Attack

- **Distributed Denial of Service (DDOS) Attack:**

In DDOS attack multiple malicious vehicles launch attack on a legitimate vehicle from different locations and they may use different time slots for sending those messages. That’s why it very difficult to prevent or trace this attack.

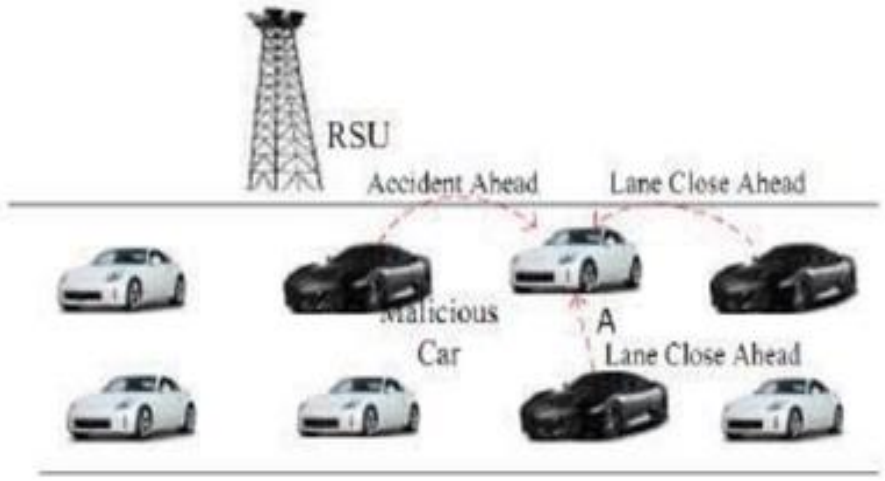

Figure 3.4 :DDOS Attack

- **Sybil attack:**

The Sybil attack occurs when a hacked node declares itself as several nodes and sends fake information to neighbor nodes. I.e. the vehicle announces its various positions at the same time which leads to create confusion and security risk in network.

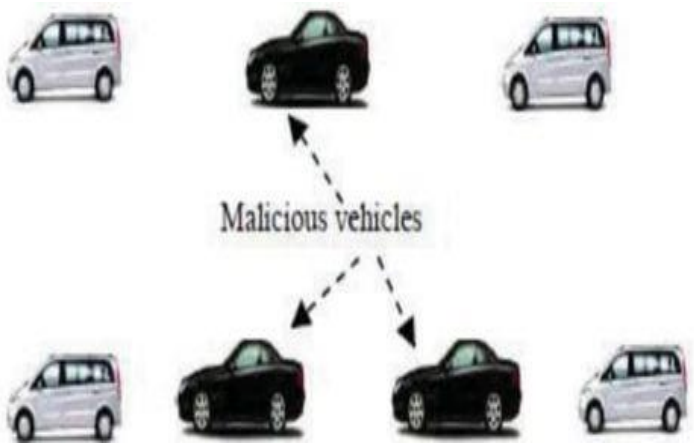

Figure 3.5 :Sybil Attack

- **Spoofing Attack:**

It is intended to impersonate another node using its identity, so we find the attacker identifies himself using the identity of a legitimate node and thus he can communicate with the rest of the nodes without refusing.

We try to categorize the attacks with which types of security issue. Here we are considering issues

	Identification	Authentication	Confidentiality	Availability	Integrity
Denial of service				✓	
Sybil attack	✓	✓	✓	✓	
Spoofing attack	✓	✓			✓
Bogus Information Attack			✓		✓

Table 3.3 the impact of attacks on security requirements

3.5 Conclusion:

In this chapter, we discussed the necessary security requirements in the VANET network, and then we identified some faults and security attacks that can occur in this network and its components, and the negative consequences it has. This is what prompts the creation of tolerance strategies for these faults and attacks, which is what we will address in the next chapter, where we chose to implement a tolerance strategy for the spoofing attack as it is one of the worst attacks in terms of its consequences.

Chapter 4

Fault Tolerance Strategy for Spoofing Attack

4.1 Introduction:

In this chapter, we want to put a strategy which aim to find a appropriate solution to the problem shown in the following case, in which we assume that we have a group of RSU located on the side of the road, and one of these RSU falls into the hands of a bad person through implements one of the attacks that we knew previously on it. In our case, we are talking about a spoofing attack that involves stealing the identity of a legitimate node and works to distort the results in order to obstruct the good functioning of the studied environment.

4.2 Oral Messages Algorithm:

The above problem is a trust problem between nodes and this describes completely the Byzantine failure. So we will try to solve this problem by Byzantine consensus algorithm specifically using oral messages solution. We chose this algorithm because its hypotheses are similar to our network conditions.

4.3 The objective of the algorithm:

We will use this algorithm to check if there is a harmful node in the network in order to detect it and get it isolated from the network.

4.3.1 General principle of this Algorithm[8]:

This algorithm is a solution works for n= 3m + 1 or more generalsin the presence of at most m traitors. Each general is supposed to execute some algorithm that involves sending messages to the other generals OM(m), and we assume that the loyal general correctly executes his algorithm. The definition of an oral message is embodied in the following assumptions which we make for the generals' message system:

A1. Every message that is sent is delivered correctly.

A2. The receiver of a message knows who sent it.

A3. The absence of a message can be detected.

Assumptions A1 and A2 prevent a traitor from interfering with the communication between two other generals, since by A1 he cannot interfere with the messages they do send, and by A2 he cannot confuse their intercourse by introducing spurious messages. Assumption A3 will foil a traitor who tries to prevent a decision by simply not sending messages.

Also we have:

- The algorithms require that each general be able to send messages directly to every other general.
- A traitorous commander may decide not to send any order. Since the lieutenants must obey some order, they need some default order to obey in this case. We let RETREAT be this default order.
- the Oral Message algorithms OM(m) is define for all nonnegative integers m, by which a commander sends an order to n - 1 lieutenants.
- The algorithm assumes a function majority with the property that if a majority of the values vi equal v, then majority (vl,..., v n-1) equals v. There are two natural choices for the value of majority(v1, ..., v,-1):
    1. The majority value among the vi if it exists, otherwise the value RETREAT.
    2. The median of the vi, assuming that they come from an ordered set.

The Algorithm:

Algorithm OM(m), m >0.

(1) The commander sends his value to every lieutenant.

(2) For each i, let vi be the value Lieutenant i receives from the commander, or else be RETREAT if he receives no value. Lieutenant i acts as the commander in Algorithm OM(m - 1) to send the value vi to each of the n - 2 other lieutenants.

(3) For each i, and each j ≠i, let vj be the value Lieutenant i received from Lieutenant j in step (2) (using Algorithm OM(m - 1)), or else RETREAT if he received no such value. Lieutenant i uses the value majority (vl, ... ,v n-1).

4.4 Network Environment:

Network environment diagram is as shown in figure 4.1, which contains the Trusted Authority and four Road Side Units (R1, R2, R3, R4). Every RSU can communicate with other RSUs and with TA (sending and receiving packets).

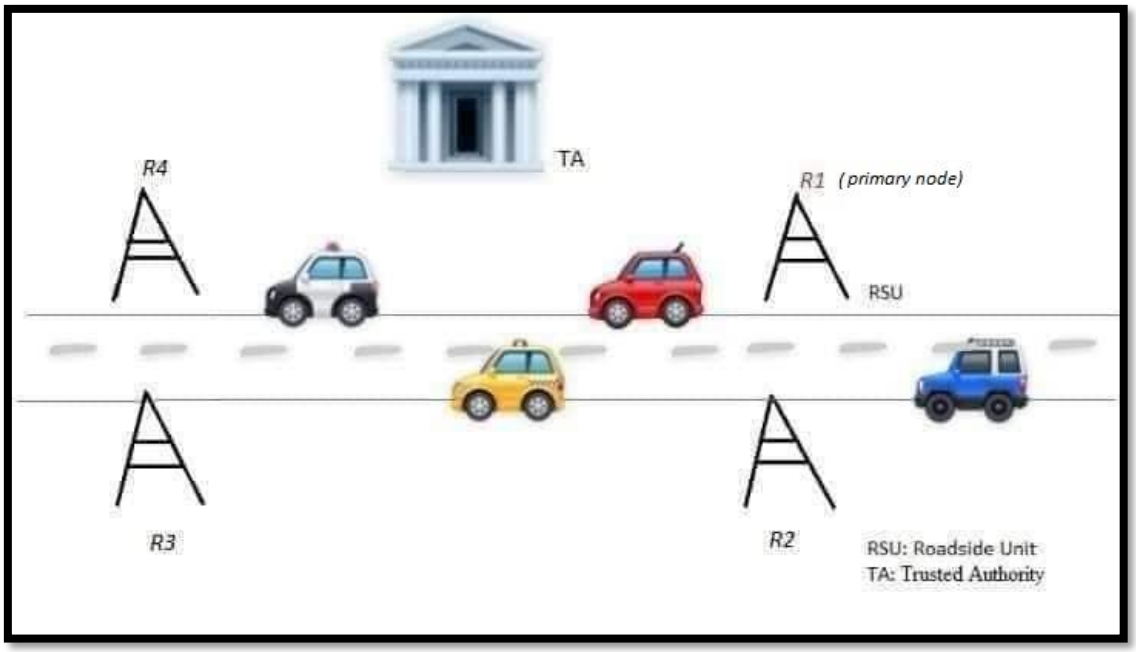

Figure 4.1 Network environment

We assume that R1 is the primary node, and R2, R3, R4 are the secondary nodes, and we also assume that one of those roadside units has become a malicious node due to being subjected to a spoofing attack. Now we need to applying the oral messages algorithm on this network for detect the malicious node and isolate it from the rest of the network components.

When we match the data in the algorithm on our network, we find:

- The traitors(m) is the malicious RSUs and in this case there is only one malicious RSU, which means m=1.
- The generals is the Roadside units (R1, R2, R3 and R4) , in this case they equal 4 (n=4).
- The commander is the primary roadside unit (R1).
- The Lieutenants are the secondary roadside unit (R1, R2 and R3).
- OM(m) in this case is a message containing keyword.

4.5 The proposed strategy Algorithm:

We will implement the algorithm below in the network at the nodes level when a new user joins the network, or when the network identifies a vehicle that connects to the network several times from a location close to one of the units at a specific time

Début

tantque (i<n-1) faire

primary_RSU send (keyword);

tantque (i<n-1) faire {

Si (secondary_RSUi receive (keywordi)) alors

Tantque (j<n-1 et j≠i) faire

secondary_RSUi send (keyword i);

else

secondary_RSUi RETREAT();

}

secondary_RSU followMajority();

fin

When we execute the algorithm in the normal case(no malicious node)on this network we find the communication between the RSUs as shown in Figure 4.2

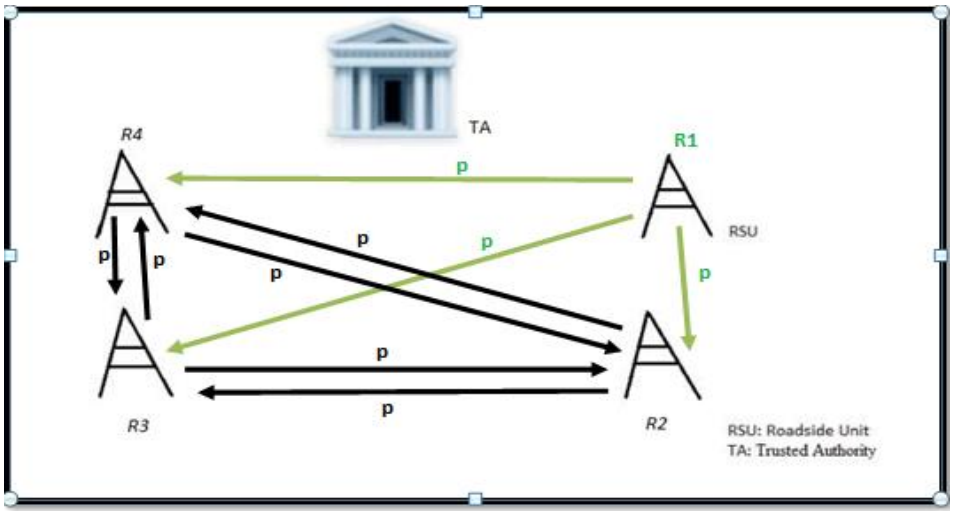

Figure 4.3 Algorithm OM(0)

And when we execute the algorithm in our case (there is a malicious node) and let us consider that one of the secondary RSUs is the malicious one.

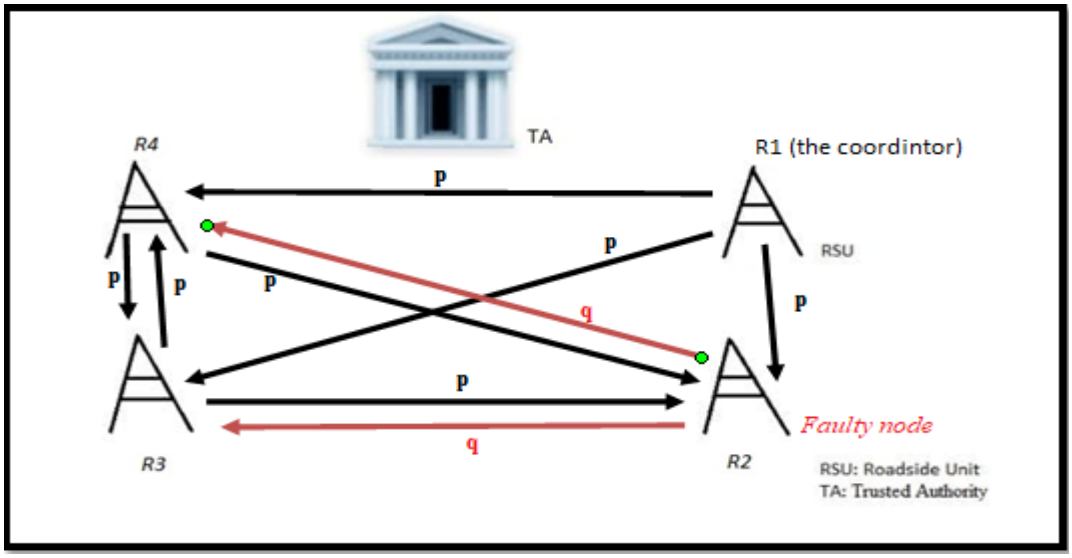

Figure 4.4 Algorithm OM(1)with a malicious secondary

4.6 Conclusion

In this chapter, we propose a tolerance strategy with RSU spoofing attack that uses Oral Messages Algorithm to detect the malicious RSU. Although this algorithm is effective in certain cases, but we encountered a case where a non-malicious node is detected as a malicious one (in case of primary RSU is the malicious one). This case is shown in Figure 4.4

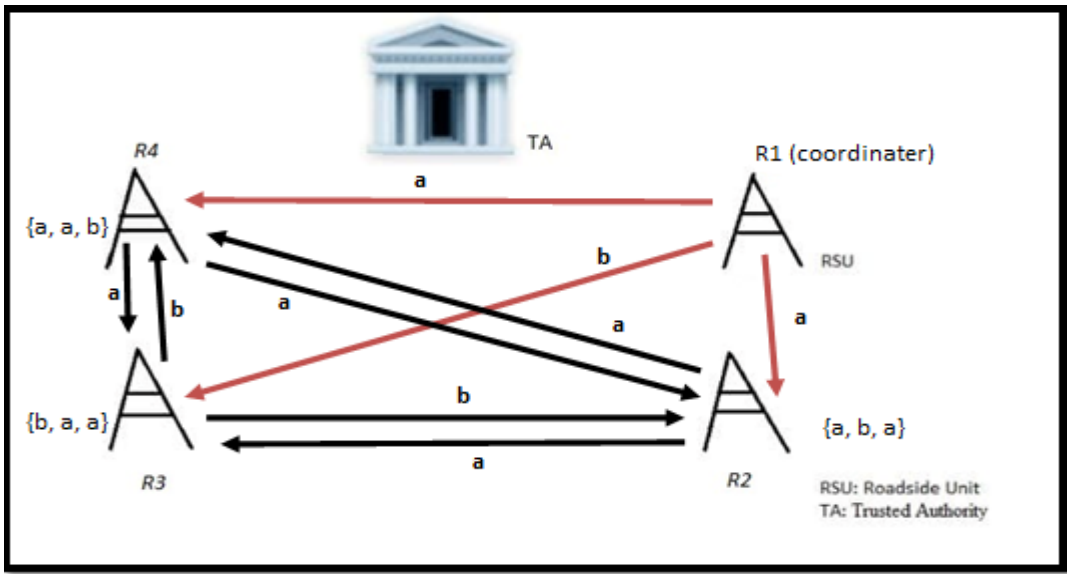

Figure 4.4 Algorithm OM(1) with a malicious primary

Also this strategy is invalid in case of the attacker is an external. Therefore, it is necessary to continue working to improve it.

General Conclusion

The VANET network is among the modern technologies that still require research in many aspects, especially in the field of fault tolerance due to its great importance in systems.

This work has allowed us to know many new topics that we were ignorant of. However, with this research, we were able to learn a lot, mostly in networks or possible faults in this network.

We have proposed a tolerance strategy for the Roadside Unit (RSU) spoofing attacks by discovering malicious RSU in the network, using an algorithm called Oral Messages, but we encountered a problem when we applied in some cases, for example in the Case of a primary malicious RSU. Also, this strategy works only in the case that the attacker was internal, and therefore we can say that this strategy needs to be improved in a sereval aspect, especially since the VANET network is among the networks that will have a great use in the future.

Bibliography

Articl:

[1]Algirdas Avizienis, Fellow, IEEE, Jean-Claude Laprie, Brian Randell, Carl Landwehr, Basic Concepts and Taxonomy of Dependable and Secure Computing

[2]Algirdas Avizienis, Jean-Claud Laprie, Brian Randell, Fundamental Concepts of Dependability

[3]Challenges_of_Future_VANET_and_Cloud_Based Approaches

[4]CHOUHAN[1], Piyush, KAUSHAL, Girish, et PRAJAPATI, Urmila. Comparative Study MANET and VANET.

[5]Dr. Pankaj Dadhich, Priyanka Vyas, "Vehicular Ad Hoc Network(VANETs): A Brief Overview", Journal of Advanced Computing andCommunication Technologies (ISSN: 2347 - 2804), Volume No.5 IssueNo.3, June 2017.

[6]Felipe Domingos da Cunha, AzzedineBoukerche, Leandro Villas, Aline CarneiroViana, Antonio A. F. Loureiro,Data Communication in VANETs: A Survey, Challenges and Applications

[7]KUGALI, S. et KADADEVAR, Sneha. Vehicular ADHOC Network (VANET): A Brief Knowledge. International Journal of Engineering and Technical Research, 2020, no 9, p. 6.

[8]LESLIE LAMPORT, ROBERT SHOSTAK, MARSHALL PEASE, The Byzantine Generals Problem

[9]Navyshree H M Tanuja .K SushmaT.M VEHICULAR_AD_HOC_NETWORK_VANET , International Journal of Engineering Research & Technology (IJERT) (ISSN: 2278-0181)

[10]QAMAR, Mehreen, KHAN, Sowaiba, MEHMOOD, Aneela, et al. MANet vs VANet-The Applications & Challenges. Lahore Garrison University Research Journal of Computer Science and Information Technology, 2019, vol. 3, no 3, p. 34-38.

[11] RAMANATHAN, Ram et REDI, Jason. A brief overview of ad hoc networks: challenges and directions. IEEE communications Magazine, 2002, vol. 40, no 5, p. 20-22.

[12]Sameer Sheikh , and Jun LiangA Comprehensive Survey on VANET Security Services in Traffic Management System Muhammad 2013

[13]TanujaK ,Sushma T M , Bharathi M ,Arun K H A Survey on VANET Technologies. International Journal of Computer Applications ,july 2015

[14]TOMAR, Ravi, PRATEEK, Manish, et SASTRY, G. H. Vehicular adhoc network (vanet)-an introduction. International Journal of Control Theory and Applications, 2016, vol. 9, no 18, p. 8883-8888.

Books:

[15]Dimosthenis P. Kyriazis, Theodora A. Varvarigou, Kleopatra G. Konstanteli, Achieving Real-Time in Distributed Computing

[16] Sonali P. Botkar, Sachin P. Godse, Parikshit N. Mahalle, Gitanjali R. Shinde(Intelligent Signal Processing and Data Analysis) - VANET_ Challenges and Opportunities-CRC Press (2021).

ملخص

تعتبر شبكة السيارات اللاسلكية من الشبكات التي سيكون لها استعمال كبير في المستقبل خاصة وأنها توفر العديد من الخدمات والتطبيقات التي تساعد مستعملي الطرقات. لكن كغيرها من الشبكات تتعرض للعديد من الأعطال. وللتغلب على هذه الأعطال وجب استعمال مختلف استراتيجيات التسامح مع الخطأ. في هذه الورقة سنتحدث عن بعض الأعطال الموجودة في هذه الشبكة وعن التسامح مع الأخطاء مع تقديم إستراتيجية للتسامح مع الخطأ في هذه الشبكة.

كلمات مفتاحية: شبكة السيارات اللاسلكية، الأعطال، التسامح مع الخطأ، إستراتيجية.

Abstract

VANET is considered one of the networks that will have a great use in the future, especially as it provides many services and applications that help road users. But like other networks, it suffers from many faults. To overcome these faults, various fault tolerance strategies must be used. In this paper we will talk about some of the faults in the VANET and fault tolerance also we will present a fault tolerance strategy in this network.

Keywords: VANET, fault, fault tolerance, strategy.

Résumé

VANET est considéré comme l'un des réseaux qui aura une grande utilité à l'avenir, d'autant plus qu'il fournit de nombreux services et applications qui aident les usagers de la route. Mais comme les autres réseaux, il souffre de nombreux défauts. Pour surmonter ces défauts, diverses stratégies de tolérance aux pannes doivent être utilisées. Dans cet article, nous parlerons de certains des défauts du VANET et de la tolérance aux pannes. Nous présenterons également une stratégie de tolérance aux pannes dans ce réseau.

Mots clés: VANET, panne, tolérance aux fautes, stratégie.