Attacks against security in the vehicular network and the impact of Sybil attack and Blackhole attack on the vehicular network performances: average Throughput as a study of case

Ayoub Toubi, Tomader, Mazri
National School of Applied Sciences - IBN TOFAIL University – Morocco
aytoubi@gmail.com, tomader20@gmail.com

Abstract—
Vehicular Ad-Hoc Network presents a revolution for SMART CITY. Vehicular Ad-Hoc Network uses two modes of communication V2V and V2I. Wireless vehicle communication presents vulnerabilities and threats to vehicles and to RSU. The Communication between vehicles and infrastructure presents a significant security challenge to protect the confidentiality and integrity of data. For this reason, we must understand the types of attacks and their classifications, and make simulations to study their impact on the environment and performance of the vehicular network. In this work we will discuss the challenges security in Vehicular network and we simulate two types of attacks, Blackhole attack and Sybil attack and their impact on the vehicular network performances: average Throughput as a study of case.

Index Terms— Vehicule to infrastructure; RSU; end to end security; 5G Architecture; Vehicular Ad hoc Networks; Blackhole attack; Sybil attack; Network simulator.

INTRODUCTION

Vehicular Ad hoc Networks (VANETs) are a new form of mobile ad hoc networks (MANETs). They enable communications between vehicles or between a roadside infrastructure. The vehicular networks are threatened by attacks either internally or externally which can be a great cause for the degradation of the performances of the vehicular network, Compared to a conventional ad hoc network, vehicular networks are characterized by a high mobility of nodes making the topology of the network highly dynamic. For the establishment of such a network, certain electronic simulate, the fourth section is about the simulation and the Impact of the Blackhole attack on the performance of vehicular networks, in the last section we will analyze the simulation results and we will show the impact of the Sybil attack on the performance of vehicular networks. Vehicular Ad hoc Networks (VANETs) are a new form of mobile ad hoc networks (MANETs). They enable communications between vehicles or between a roadside infrastructure. The vehicular networks are threatened by attacks either internally or externally which can be a great cause for the degradation of the performances of the vehicular network, Compared to a conventional ad hoc network, vehicular networks are characterized by a high mobility of nodes making the topology of the network highly dynamic. For the establishment of such a network, certain electronic equipment must be installed within vehicles such as environmental perception devices (radar, cameras), a GPS tracking system, and of course a processing platform, the set will compose what is called a connected car.

The first section of this paper will talk about the 5G infrastructure and data communication in vehicular networks, in the second we will define the classification of attacks, inter-vehicle attacks and intra-vehicle attacks, in the third section we will explain the types of attacks that we will simulate, the fourth section is about the simulation and the Impact of the Blackhole attack on the performance of vehicular networks, in the last section we will analyze the simulation results and we will show the impact of the Sybil attack on the performance of vehicular networks.

RELATED WORK

Douceur [1] describes and formalizes Sybil attacks in the context of peer-to-peer networks. It can easily defeat reputation and threshold protocols intended to protect against it. In a distributed system such as VANET, most applications assume that each participating entity has exactly one identity. If this assumption is satisfied, there is no risk of identity spoofing attacks. Raya and Hubaux [2] discuss a number of unique challenges in VANETs. They describe how adversaries use safety applications to create various attacks and lead to security issues. Various types of attacks on an inter-vehicle communication system are presented in [3]. They analyze how an attacker can manipulate the input of an on board unit (OBU) and sensor readings. Hortelano et al. [4] evaluate the protocol independent watch- dog mechanism [5] in VANETs. Daeinabi et al. [4] propose an algorithm which utilizes vehicles monitoring each other in order to detect vehicles explicitly drop or duplicate packets.

I. 5G INFRASTRUCTURE AND DATA COMMUNICATION IN VEHICULAR NETWORK

A. 5G infrastructure

This new generation [Figure 1] is still in the testing stage. To make this standard effective, the allocation of new frequencies following the MWC World Congress 2015 (Mobile World Congress) was requested and granted: the release of the band 3.4 - 3.6 GHz will ensure upgradability never reached until today, but also VHF band (400 - 700 MHz) for a better spectral occupation of the network.

Massive use of the millimeter bands will not only enable the mobile terminals to connect to the base stations, but also connect them to the collection networks and overcome the

significant costs of installing fiber optics: Access points will use the V band (57-66 GHz) but also the W (71-86 GHz) and E (94 GHz) bands.[6]
Based on 5G techniques such as Massive-Multiple-Input Multiple Output (MIMO) and LDPC / Polar, the base station can create up to 20 Gbit / s, 20 times that offered by a 4G network. [7] These UHD (Ultra High Definition) television transmissions will be realizable live, virtual reality (VR) and augmented reality (AR) experiments, as well as the viewing of auto-stereoscopic images.

The 2G band focuses on the 900 and 1800 MHz bands. Some operators also operate 4G on the 1800 MHz. 3G is used on the 900 and 2100 MHz bands. The 4G operates on the 800, 1800 and 2600 MHz bands and more recently on the 700 band. The arrival of the 5G in the next few years will be based on the 700 and 3500 MHz bands at first.

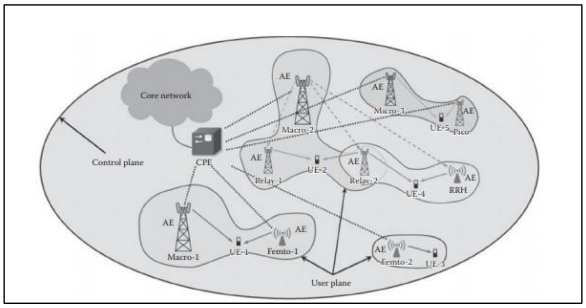


Figure 1: backbone network of the 5G generation

Software Network Controller (SDN) and Network Function Virtualization (NFV): These two features go beyond the strict framework of 5G networks; they are part of the general process of evolution of current networks and are already available in 4G technology (4.9G).

The purpose of the Software Defined Network (SDN) is to dissociate the control part of a network from its operational part, these two parts being traditionally linked and distributed (fixedly) in the network.
The control of the network, previously devolved to specialized and non-evolving hardware components, is centralized in the form of software on more powerful servers and freed (in theory) from the specifications of the equipment manufacturers. This allows the deployment of high added value services (load balancing, intelligent routing, dynamic configuration ...) in heterogeneous environments.

The NFV, complementary to the SDN, aims to virtualize, that is to say replace by software on a server, specialized hardware equipment in some key functions of the network (firewall, core network, interfaces between different systems ...), in order to speed up deployments and enable rapid changes.

CloudRAN: This feature, also known as centralized-RAN, involves very different network architecture from what is currently done. This is an evolution of the SDN: the signal processing units of the base stations, currently located at the station itself, are deported to the cloud and centralized; they communicate with the head ends, located closest to the antenna, via a fiber optic network (Radio over fiber technology). This centralization provides an overview of all deployed stations and coordinates signal processing and interference management between cells and terminals.

B. The protocol stack for vehicular networks

The protocol stack for vehicular networks must handle communication between neighboring vehicles, and between the infrastructure itself and the fixed road equipment.

- The physical layer

Physical layer protocols must take into account multipath signal attenuation and frequency changes caused by fast vehicle movements. Experimental V2V communications use radio and infrared waves, as well as very high frequency waves are examples of radio waves that are used for V2V communications.

Infrared and millimeter waves are suitable for line-of-sight communications only, while VHF and microwave provide broadcast communications [8].

- Dedicated Short-Range Communication:

DSRC (Dedicated Short-Range Communication) is a defined system for vehicular networks which is a short and medium range communication technology operating in the 5.9 GHz band [9] for the use of private and security applications.

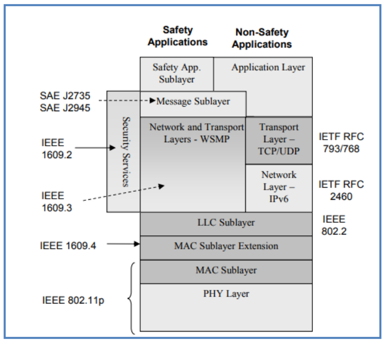


Figure 2: ITS protocol stack: DSRC-WAVE according to the FCC-US [10]

DSRC is known as IEEE 802.11p WAVE (Wireless Ac-cess in Vehicular Environments), designed based on earlier standards for Wireless LANs [9]. DSRC technology can be used in the communication mode (V2V) or in the vehicle-to-infrastructure (V2I) communication mode.
The DSRC system supports a speed of up to 200 km / h, a range of 300 m up to 1000 m and a default speed of 6 Mbps (up to 27 Mbps). [Figure 2] presents the protocol stack for intelligent telecommunication systems: DSRC - WAVE and associated layer specifications, as well as standards applied in the United States.

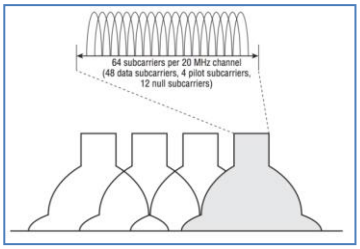

64 subcarriers per 20 MHz channel
(48 data subcarriers, 4 pilot subcarriers,
12 null subcarriers)

Figure 3: OFDM modulation with 64 subcarriers.

The protocol stack security applications are based on the WAVE (1609.x) specifications and not on the IP applications. IP headers contain general bits that can cause channel congestion, this is not tolerable in a security application and it leads to the creation of WAVE specifications that can reduce the number of overload bits.

- The IEEE 802.11p standard of the physical layer

In this section we will discuss the modifications made to the 802.11p standard with the OFDM modulation of the physical layer[11][12]. The 802.11a standard uses the full clocked mode with a bandwidth of 20 MHz while the 802.11p uses the half-clocked mode with a bandwidth of 10 MHz. Regardless of the bandwidth, the FFT size is 64 subcarriers [Figure 3], with 48 data subcarriers and 4 pilot subcarriers the remaining twelve subcarriers are not considered.

There are two important changes to TX and RX specifications to support the 802.11p standard, transmitters and receivers must have a much stricter spectrum mask and stricter adjacent and non-adjacent channel rejection requirements [Figure 4].

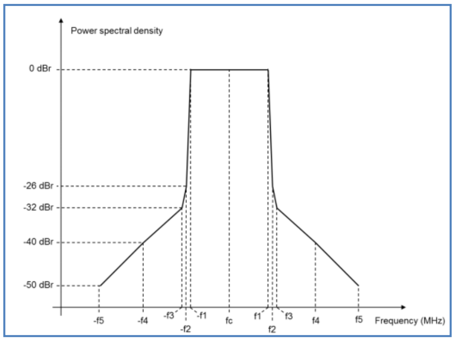


Figure 4: Class C spectrum emission mask for the 802.11p standard.

C. Communication

The communication block establishes the communication between autonomous vehicles and remote servers. Communication protocols typically work in the data link layer, network layer, transport layer, and application layer of the OSI model. Communication protocols are the backbone of IoT systems and provide network connectivity and application coupling. Protocols define data exchange formats, data encoding, addressing schemes for devices, and routing packets from source to destination.

- 802.11 WIFI

IEEE 802.11 is a set of communication standards for wireless local area networks (WLANs). For example, 802.11a operates in the 5 GHz band, 802.11b and 802.11 g in the 2.4 GHz band, 802.11n in the 2.4 / 5 GHz bands, 802.11ac in the band 5 GHz and 802.11ad in the 60 GHz band [13].

These standards provide speeds ranging from 1 Mb / s to 6.75 Gb / s. Wi-Fi provides a communication range of around 20m [indoor] to 100m [outdoor].

- 802.16 WiMax

IEEE 802.16 is a set of wireless broadband standards. WiMAX (Global Interoperability for Microwave Access) standards provide data rates between 1.5 Mb / s and 1 Gb / s.

The recent update (802.16 m) provides a data rate of 100 Mb / s for mobile stations and 1 Gb / s for fixed stations. Mobility must be supported on the IEEE 802.16m network. The IEEE 802.16m standard needs to be optimized for low speeds such as stationary pedestrian mobility classes and offers high performance for higher mobility classes [13].

Performance must be degraded gracefully to greater mobility. In addition, the IEEE 802.16m must maintain the connection to the highest supported speed.

Vehicle speeds above 350 km / h and above 500 km / h may be taken into account depending on the frequency band and deployment. The IEEE 802.16m standard must define the minimum antenna specifications for the base station and mobile station.

For the base station, a minimum of two transmit antennas and two receive antennas must be supported. For the mobile station, at least one transmitting antenna and two received antennas must be supported.

The IEEE 802.16m standard must support MIMO technology, beamforming, or other advanced antenna techniques. The IEEE 802.16m standard must also support single-user and multi-user MIMO techniques.

- 802.15.1 - BlueTooth

Bluetooth is based on the IEEE 802.15.1 standard. It is a low-power wireless communication technology that is suitable for transmitting data between mobile devices for a short distance (8 to 10 m).

The Bluetooth standard defines a PAN (Personal Area Network) communication. It operates in the 2.4 GHz band. The data rate in different versions of Bluetooth varies from 1 Mb / s to 24 Mb / s. The ultra-low-power, low-cost version of this standard is called Bluetooth Low Energy (BLE or Bluetooth Smart). Previously, in 2010, BLE had merged with the Bluetooth v4.0 standard [13].

D. - Architecture of VANET networks and their characteristics.

The VANET architecture [Figure 5] can be divided into three categories: cellular architectures and wireless LAN, ad hoc architectures and hybrid architectures [14], if the infrastructure consists of a cellular gateway or a d-point. WLAN access, the network will be considered a pure cellular-WLAN network.

When no infrastructure is available, the nodes must communicate with each other without depending on an infrastructure, this set up a pure ad hoc architecture.
Sometimes, various access points, such as cellular gateways, will be available for communication, in which case the nodes can communicate with these infrastructures or communicate directly with each other [Figure 5] this is the principle of the hybrid architecture.

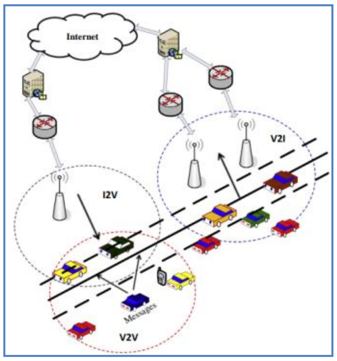


Figure 5: VANET architecture

VANET networks have several features that are unique, such as the channel feature that we have discussed previously, the DSRC system that is based on the 802.11p standard, and other features, such as the hardware features installed in vehicles to ensure communication with the infrastructure and other vehicles, this depends on the mode of communication chosen.

The equipment installed in the vehicles makes them intelligent and gives them the means to communicate. Among these equipments:

- A data and event recorder (EDR) [15 - 16]: records transmissions and receives messages and all events that occurred in the vehicle environment during the movement.

- Global Positioning System (GPS) receiver: provides information on geographic location, speed, direction of movement, and vehicle acceleration at specific time intervals.

- Radars and sensors are also used to detect obstacles in the vehicle environment.

- An electronic license plate (ELP) is installed on each new vehicle of the factory [17], it provides an identification number used by the police or any other official order.

E. Modes of communication in vehicular networks

Vehicle-to-Vehicle (V2V) communication mode [18]: allows direct communication with vehicles without relying on fixed infrastructure support, this mode of communication can be mainly used for safety, security and broadcasting applications, [Figure 6].

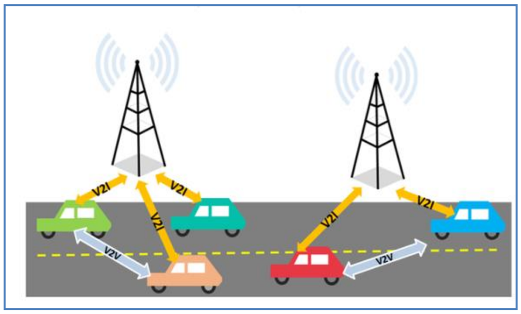


Figure 6: The different modes of communication in vehicular networks

Vehicle-to-Infrastructure (V2I) communication mode [18]: allows a vehicle to communicate with the road infrastructure, for information gathering applications and for authentication.

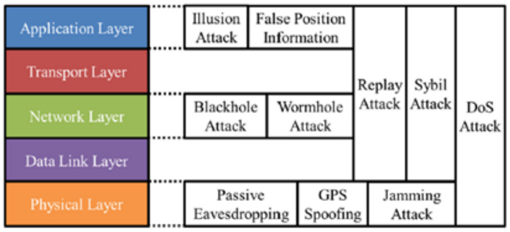
Hybrid architecture: combines V2V mode and V2I mode, in this scenario, a vehicle can communicate with the road infrastructure either with one jump or with several jumps, depending on the distance.

II. Attacks classification

Attacks in the vehicular network are classified either by layer [Figure 7] or by type. [19]:

Inter-Vehicle Attacks: Malicious nodes may send falsified data in order to free up traffic or other undesirable applications such as loss of life or loss of energy and money.

Intra-vehicle attacks: Intra-vehicle communication describes communications in a vehicle. Intra-vehicular attacks consist in launching attacks on sensors connected within the vehicle to damage the vehicle and the environment, these sensors consists in checking the state of the road, the distance of the vehicle, the detection of obstacles, fire detection and detection of speed, etc.



Application Layer	Illusion Attack	False Position Information	Replay Attack	Sybil Attack	DoS Attack
Transport Layer					
Network Layer	Blackhole Attack	Wormhole Attack			
Data Link Layer					
Physical Layer	Passive Eavesdropping	GPS Spoofing	Jamming Attack		

Figure 7: Attacks classification by layer [19].

A. Attack types:

Memory overflows attack: A buffer overflow condition exists when a program tries to put more data in a buffer than it can hold, or when a program tries to put data into a memory area beyond one buffer, in this case, a buffer is a sequential section of memory allocated to contain anything, from a string of characters to an array of integers. Writing outside the limits of an allocated memory block can corrupt data, block the program, or cause malicious code to run.

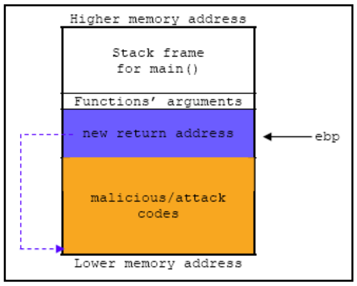


Figure 8: Buffer overflow vulnerability.

Buffer overflows are not easy to discover, and even when one of them is discovered, it is usually extremely difficult to exploit. However, attackers have been able to identify buffer overflows in an impressive number of products and components.

In a classic exploit, the hacker sends data to a program that it stores in a buffer stack that is too small. The result is that call stack information is overwritten, including the return pointer of the function. The data sets the value of the return pointer so that when the function returns, it transfers the control to the malicious code contained in the attacker's data [Figure 8]. Although this type of stack buffer overflow is still common on some platforms and in some development communities, there are various other types of buffer overflows, including the Heap buffer overflow and the Offset error.

Another very similar class of defects is known as an attack by a format string. In the next section we will propose our approach based on the dynamic adaptability aspect to solve the memory buffer overflow problem.

Sybil attacks*:* The Sybil attack [Figure 9] can be classified as one of the most dangerous and most difficult attacks to detect in the vehicular networks, the attack consists that a vehicle can claim several identities.

In other words, other vehicles in the network are unable to distinguish if the information comes from one or more vehicles, the main objective of the attacker is to shape the networks according to his objectives, and for example, an attacker could manipulate the behavior of other vehicles by forcing them to take a different route from their intended route [20].

If the vehicular networks use geographic routing, the Sybil attack poses a threat to the other vehicles because the trigger of the attack claims that the vehicle is in several positions by sending incorrect information on its exact position [19].

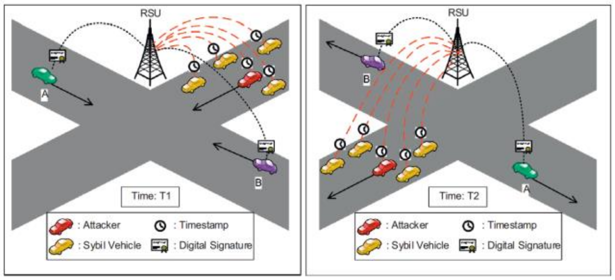


Figure 9: Sybil attack [19].

Another type of attack can be considered a Sybil attack is called node impersonation attack.

In VANET networks, each vehicle in the network has a unique identity and the vehicles use their identity while communicating with other vehicles in the network. However, if a vehicle changes identity without informing the RSU, it could be a different vehicle than a Sybil attack.

For example, a vehicle involved in a traffic accident, could change its identity to appear as a moving vehicle in the network, Then the malicious vehicle could send incorrect information on road conditions to the RSUs that are in its coverage area. Among the operations that an attacker Sybil can cause in a vehicular network:

Deleting packets: deleting alert packets in the event of an accident.

Insert erroneous information or modify existing packages: an attacker can create the illusion of a traffic jam before selecting another route to his advantage.

Replay packets: An attacker can fraudulently repeat or delay the transmission of data.

Sybil attack classification: An attack Sybil can be classified in three categories [21, 22] according to the following three orthogonal dimensions: the type of communication - the mode of acquisition of the identity Sybil - the participation in the network.

Attack by type of communication: The communication mode between the Sybil identities created by an attacker can be of two types: Direct and Indirect. In direct communication, the Sybil nodes created by an attacker communicate directly with a legitimate vehicle.

This process is feasible in a scenario where an attacker impersonates an actual vehicle. Usually, Sybil nodes and legitimate nodes communicate indirectly in cases where an attacker uses falsified identities. A vehicle in the network communicates with a vehicle Sybil in this case the attacker receives the data transmitted by the vehicle without realizing it.

This scenario represents an example of indirect communication where the legitimate nodes reach the Sybil nodes via a malicious node.

Attack by Identity Acquisition Mode Sybil: A Sybil node can have two types of identity.

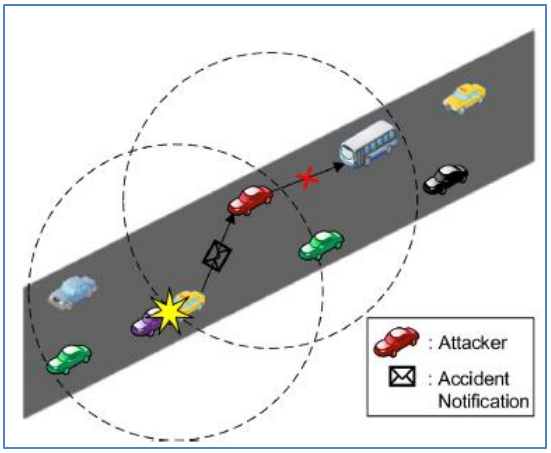


Figure 10: Blackhole attack [6]

Fabricated Identity: If the vehicular network ignores the restriction on the number of allocated identities, the attacker can generate a random number of identity.

Usurped identity: if the vehicular network limits the number of allocated identities in the network and detects the false identities, the attacker can assign legitimate identities to the Sybil nodes by usurping the identity of one of the neighbors.

Attack by type of participation: Multiple Sybil identities created by malicious nodes can simultaneously participate in an attack or the attacker can use multiple Sybil identities one at a time, while a particular identity can be used at any time and can also leave or join the network several times. Attackers can periodically coordinate identity change to make the detection process more difficult.

Blackhole attack: In vehicular networks, an attacker could exploit routing protocols such as claiming that it has the best path for the destination vehicle / RSU or that it is in the best position to forward packets.

By spreading false routing information, other vehicles prefer to send their packets by the path proposed by the attacker.
After the victim vehicles send their packets to the attacker, he usually just rejects all the packets and as a result, packet losses occur in the network [Figure 10].

B. *The objectives of security*

Before addressing security issues in VANET networks, it is essential to meet the requirements that the system must meet for the proper functioning of the network, as a result of the importance of the information exchanged and the huge number of users. The environment of vehicular networks will be increasingly vulnerable and threatened by attacks that can lead to very serious consequences.

The main objectives of security are: authentication, integrity, confidentiality, non-repudiation, availability, access control, real-time constraint and privacy protection.
Most of these goals are related to general security issues and some are specific to VANETs.

-Authentication

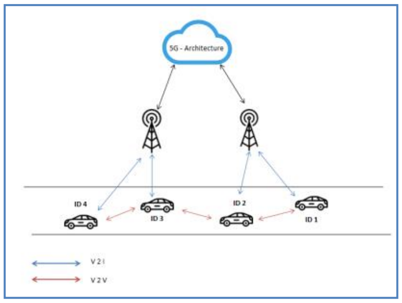


Figure 11: Authentication by ID

Powerful authentications provide legal evidence using external mechanisms, such as traditional law enforcement authorities to detect attacks [23]. In VANET networks, it is very important to identify the sender of the message in order to have some information about the transmitting vehicle as well as its location, for this there are some types of authentication [24]:
Authentication by ID: allows a node to identify the sender of a message in a unique way. This authentication also allows a node to be a member of the network. When ID authentication is set, it is easy to avoid certain attacks such as identity theft [Figure 11].

Entity Authentication: Determines which type of entity communicates, whether a car, RSU, or other type of equipment.
Location Authentication - authenticates the position of the node when a location application is involved.

- Integrity

Integrity protects against unauthorized destruction or modification of data [25]. If a corrupted message is accepted, the integrity property is violated and the protocol is considered defective [Figure 12], this can cause serious traffic problems.

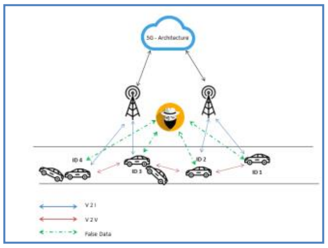


Figure 12: Changing data in VANET networks

-Confidentiality

This security goal ensures that only authorized parties can access data transmitted across the network. These data may relate to the application layer or the lower layers.

-The availability

This security goal is to ensure that authorized entities have access to network resources with adequate quality of service.

Security in VANET networks is a prerequisite because the life of users is put at risk if an attack and launch. For this, the vehicles must have a secure link to stay in communication with the infrastructure, we talk about security in the V2I communication mode that is to say we must seek to find optimal solutions, robust and complicated to end to meet the objectives of security.

The use of honypot in vehicular networks makes it possible to collect information on the behavior of unauthorized users and the techniques that use to put the vehicular network in danger.
This information about the behavior of unauthorized users, we will use it to build a database to prevent and detect intrusions before they enter the system. In our case we are talking about IDS and IPS who will use the information collected through the honeypots for trigger alerts in the case of an attack or the appearance of a vulnerability in the system.

The use of encryption algorithms and shorthand is a great way to ensure the integrity and confidentiality of messages.
The use of very large encryption keys does not present a latency problem if the infrastructure connected to the vehicle uses 5G frequencies because the fifth generation cellular network is processing data rates that are too high.

Another point is the use of firewalls to limit access to the databases of the infrastructure according to the rights of users: VLR (Visitor Location Register) - HLR (Home Location Register) ... etc, and trigger alerts systems in the opposite case.

The air is a sharing environment, anyone can intercept the messages and even if these messages are encrypted, the attacker can look for algorithms to break the encryption key, and sometimes the attacker can launch a DOS attack to stop any type of communication between the vehicle and the infrastructure.

III. Simulation Blackhole attack and Sybil attack.

The blackhole attack aims to reject the packets transmitted by the vehicles, it generates losses of packets.

In this section we will treat the impact of the blackhole attack on the vehicular network, and more precisely we will study the variation of the average flow during the time of the simulation.

A. *Blackhole attack: Simulation parameters setup.*

In this simulation we used NETWORK SIMULATOR (NS2) as a simulator with and TCL language which allowed us to program the scenario of the blackhole attack [Figure 13], for that we based on the Simulation parameters setup:

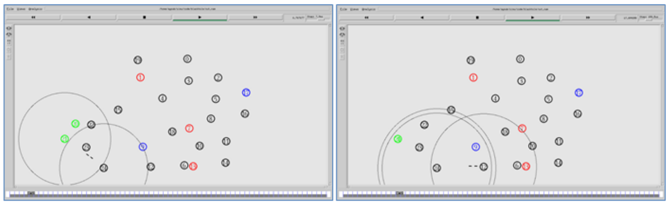


Figure 13: Blackhole attack simulation.

The table below [Table 1] presents the various parameters of the simulation, the type of channel that we chose during this simulation is a wireless channel since we treat the adhoc vehicular networks, for this we have chosen the two-ray ground reflection model as a wave propagation model, the ground reflection model is a model of radio wave propagation that predicts path losses between a transmitting antenna and a receiving antenna when they are in motion Live visibility [Line of sight].

For the antenna type an omnidirectional antenna was chosen because it radiates in all directions of the horizontal plane. For the data link type we used the layer link control of the OSI model.
In the case where the vehicles exchange packets with one another, the AODV protocol has been used as a routing protocol.

B. *Blackhole attack: Scenario of the simulation.*

In order to simulate the Blackhole attack [Figure 13] we have proposed the following scenario:

The vehicles in green present the victims, the vehicles in red present the attackers, the circles present the RSUs in this attack the communication occurs in unconnected mode using the UDP flows.

The attacker exploits the AODV routing protocol as he claims that he has the best way to communicate with either the vehicle or the RSUs, where he claims that he is in the best position to forward packets.

C. *Sybil attack: Simulation parameters setup.*

We also brought this simulation using NETWORK SIMULATOR (NS2) with the TCL language which allowed us to program the scenario of the Sybil attack [Figure 15], for that we based on the Simulation parameters setup.

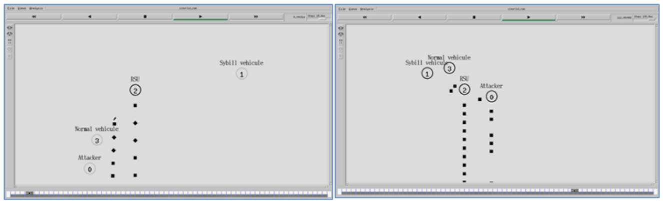


Figure 15: Sybil attack simulation.

The table below [Table 1] presents the various parameters of the simulation, the type of channel that we also chose during this simulation is a wireless channel and also we chose the ground reflection model with two radii as wave propagation model, that we already explained its role.

For the type of antenna also we chose an omnidirectional antenna because it radiates in all directions of the horizontal plane. For the type of data link, the data link sublayer of the OSI model was used.

In the case where the vehicles exchange packets with one another, the AODV protocol has been used as a routing protocol.

Parameters of Blackhole attack simulation	
Simulation parameters	Configuration
Channel type	Channel/WirelessChannel
Radio-propagation model	Propagation/TwoRayGround
Network interface type	Phy/WirelessPhy
Mac Type	Mac/802_11
Interface queue type	Queue/DropTail/PriQueue
Link Layer type	LL
Antenna model	Antenna/OmniAntenna
Max packet in ifq	50
Number of mobile nodes and RSU	23 vehicles, 2 RSU
Routing protocol	AODV
Time of smiluation end	100 secondes
Parameters of Sybil attack simulation	
Simulation parameters	Configuration
Channel type	Channel/WirelessChannel
Radio-propagation model	Propagation/TwoRayGround
Network interface type	Phy/WirelessPhy
Mac Type	Mac/802_11
Interface queue type	Queue/DropTail/PriQueue
Link Layer type	LL
Antenna model	Antenna/OmniAntenna
Max packet in ifq	50
Number of mobile nodes and RSU	3 vehicles, 1 RSU
Routing protocol	AODV
Time of smiluation end	100 secondes

Table 1: attack simulation parameters

D. *Sybil attack: Scenario of the simulation.*

In order to simulate the Sybil attack [Figure 15] we have proposed the following scenario: a vehicle involved in a traffic accident, could change its identity to appear as a moving vehicle in the network, Then the malicious vehicle could send incorrect information on road conditions to the RSUs that are in its coverage area, this information will be send in two mode, connected mode using the TCP stream and in offline mode using the UDP stream.

IV. DISCUSSION

A. *The impact of the Blackhole attack on vehicular network performances.*

After running the simulation a trace file that contains the results of the simulation was generated. After analyzing and interpreting this file we found the following result:

The graph below [Figure 14] shows the impact of the blackhole attack on the average Throughput in the vehicular network. There is an exponential degradation during the execution time of the simulation; the impact of the blackhole attack is remarkable between the periods [5 - 20]. This leads us to double efforts to find optimal solutions to limit performance degradation in vehicular networks.

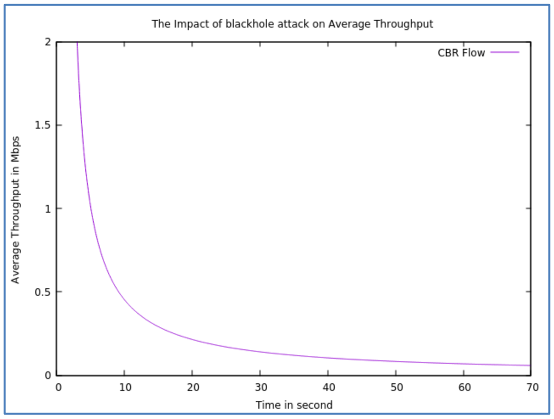


Figure 14: The impact of the Blackhole attack on average Throughput.

B. *The impact of the Sybil attack on vehicular network performances.*

After running the simulation a trace file that contains the results of the simulation was generated.
After the analysis and the interpretation of this file we found the following result: The graph [Figure 16] presents the impact of the Sybil attack on the average Throughput in the vehicular network.

Exponential degradation is observed during the execution time of the simulation, the impact of the Sybil attack is remarkable between the period [21 - 60] for the TCP stream and [2 - 40] for the UDP stream. Note that using the unconnected mode degrades the performance over the connected mode.

To decide which mode of communication is desirable to launch a Sybil attack without being detected, a study was made on the energy level of the vehicles during the attack in the connected TCP mode and the non-connected UDP mode, the graph below [Figure 16] presents the result of the analysis:
Note that in the case where the attack is launched with the TCP connected mode, the energy level of the vehicles is periodically increased by cons in the unconnected mode vehicles do not consume too much energy.

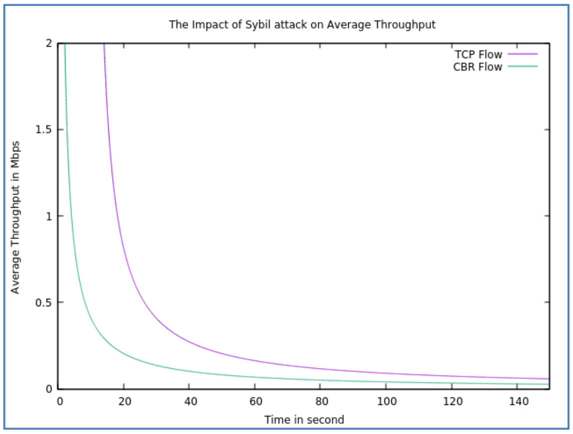


Figure 16: The impact of Sybil attack on average Throughput.

To decide which mode of communication is desirable to launch a Sybil attack without being detected, a study was made on the energy level of the vehicles during the attack in the connected TCP mode and the non-connected UDP mode, the graph below [Figure 17] presents the result of the analysis:
Note that in the case where the attack is launched with the TCP connected mode, the energy level of the vehicles is periodically increased by cons in the unconnected mode vehicles do not consume too much energy.

From this analysis it is deduced that the Sybil attack with the unconnected mode allows the attacker not to be detected by the detectors that rely on the calculation of the signal power.

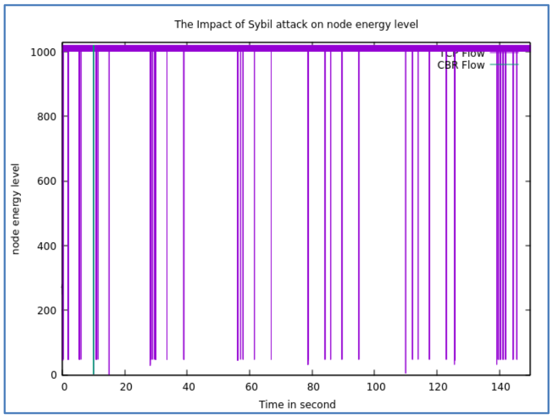


Figure 17: The impact of Sybil attack on node energy level.

The graph below [Figure 18] shows the impact of the blackhole attack and the Sybil attack on the average Throughput in the vehicular network. There is an exponential degradation during the execution time of the simulation, the impact of the blackhole attack and the Sybil attack is remarkable between the period [5 - 60]. This leads us to double efforts to find optimal solutions to limit performance degradation in vehicular networks.

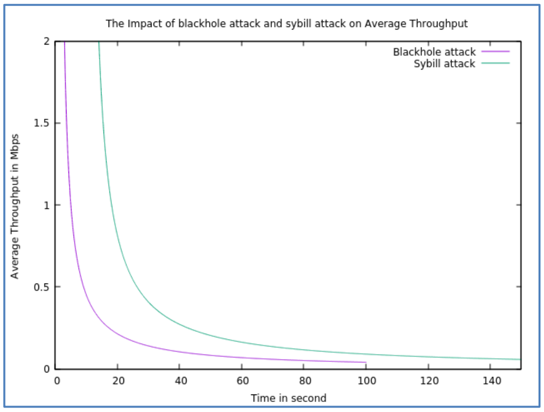


Figure 18: The impact of blackhole attack and Sybil attack on Average Throughput.

CONCLUSION

To conclude the security in the V2I communication mode is a very important aspect that presents vulnerabilities at the interfaces of 5G infrastructure and vehicles. Sybil attack can be classified as one of the most dangerous and most difficult attacks to detect in the vehicular networks, the attack consists that a vehicle can claim several identities. The blackhole attack aims to reject the packets transmitted by the vehicles, it generates losses of packets.

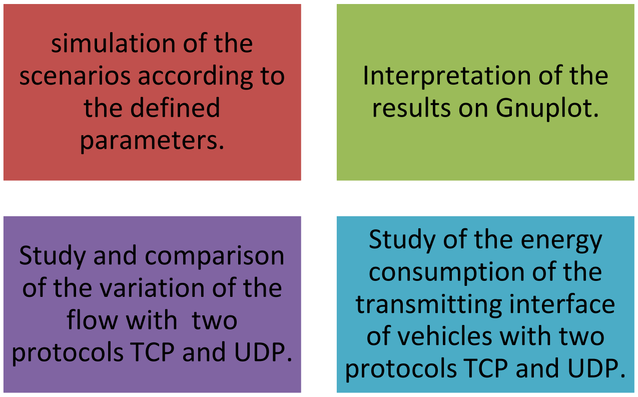

simulation of the scenarios according to the defined parameters.
Interpretation of the results on Gnuplot.
Study and comparison of the variation of the flow with two protocols TCP and UDP.
Study of the energy consumption of the transmitting interface of vehicles with two protocols TCP and UDP.

Figure 18: summary of the simulation and result.

The vehicular network suffers from physical interface attacks because of the nodes that use 802.11p wireless communication. In this paper we have shown the impact of Sybil attacks and blackhole attack on performance of vehicular network as well as the energy consumption of the nodes with different modes of communication, we see that this study helps to find approaches and methods detection of these types of attacks in vehicular networks.

References

[1] J.R. Douceur, The Sybil Attack, IPTPS ’01: Revised Papers from the First International Workshop on Peer-to-Peer Systems, Springer-Verlag, London, UK, 251–260, 2002.

[2] M. Raya, J.P. Hubaux, Securing vehicular ad hoc networks, JCS 15(1), 39–68, 2007

[3] A. Aijaz, B. Bochow, F. Dötzer, A. Festag, M. Gerlach, R. Kroh, T. Leinmüller, Attacks on Inter Vehicle Communication Systems - an Analysis, Proc. WIT, 189–194, 2006.

[4] J. Hortelano , J.C. Ruiz , P. Manzoni , Evaluating the usefulness of watchdogs for intrusion detection in vanets, in: 2010 IEEE International Conference on Com- munications Workshops, 2010, pp. 1–5 .

[5] S. Marti , T.J. Giuli , K. Lai , M. Baker , Mitigating routing misbehavior in mobile ad hoc networks, in: Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, 20 0 0, pp. 255–265 .

[6] Loïc Martin. Design of a compact base station antenna for cellular networks. Electronic. UNIVERSITY OF NANTES, 2017. French. p 23

[7] Loïc Martin. Design of a compact base station antenna for cellular networks. Electronic. UNIVERSITY OF NANTES, 2017. French. p 25

[8] P. Papadimitratos , A. De La Fortelle , K. Evenssen , R. Brignolo , S. Cosenza , Vehicular communication systems: Enabling technolo-gies, applications, and future outlook on intelligent transportation, Comm. Mag. 47 (11) (2009) 84–95 .

[9] J. Kenney , Dedicated short-range communications (dsrc) standards in the united states, Proc. IEEE 99 (7) (2011) 1162–1182 .

[10] J. Kenney, "Dedicated Short Range Communication (DSRC) Applications Tutorial, IEEE 802.11-13/0541r1," 14 May 2013. [Online]. Available: https://mentor.ieee.org/802.11/dcn/13/11-13-0541-01-0wng-dsrc-applications-tutorial.pptx. [Accessed 29 August 2013].

[11] M. Weiss, "WLAN Tests According to Standard 802.11a / b / g," 28 July 2004. [Online]. Available: http://cdn.rohdeschwarz.com/dl_downloads/dl_application/application_notes/1ma69/1MA69_1e_WLAN_tests_80211abg.pdf.

[12] IEEE Std 802.11TM-2012, "IEEE Standard for Local and Metropolitan Area Networks: Wireless MAC LAN and PHY Specifications," [Online]. Available: http://standards.ieee.org/getieee802/download/802.11-2012.pdf.

[13] P.P.Ray. Journal of King Saud University ‑ Computer and Information Sciences (2018) 30, p.297.

[14] Y. Wang, F. Li, Vehicular Ad Hoc Networks, Springer-Verlag, London, 2009.

[15] M. Raya, J.P. Hubaux, The security of vehicular ad hoc networks, in: Security in Ad Hoc and Sensor Networks (SASN), 2005.

[16] G. Yan, B.B. Bista, D.B. Rawat, E.F. Shaner, General active position detectors protect VANET security, in: Broadband and Wireless Computing, Communication and Applications (BWCCA), 2011, pp. 11–17.

[17] C. Wei, Y. Jianding, L. Xiangjun, The design of electronic license plate recognition terminal system based on nRF24LE1, in: 2012 Fifth International Symposium on Computational Intelligence and Design (ISCID), 2012, pp. 127–129.

[18] F. Cunha, L. Villas, A. Boukerche, G. Maia, A. Viana , R. Mini, A. Loureiro, Data communication in VANETs: Protocols, applications and challenges. Ad Hoc Networks 44 (2016) 90–103 , p 2.

[19] Fatih Sakiz, Sevil Sen,A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV,Ad Hoc Networks,Volume 61,2017,Pages 33-50.

[20] I.A. Sumra , I. Ahmad , H. Hasbullah , others , “Classes of attacks in VANET, in: Electronics, Communications and Photonics Conference (SIECPC), 2011 Saudi International, 2011, pp. 1–5 .

[21] P. Golle, D. Greene, J. Staddon, Detecting and correctingmalicious data in VANETs, VANET ’04: Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks, ACM, Philadelphia, PA, USA, 29–37, 2004

[22] S. Pal, A.K. Mukhopadhyay, P.P. Bhattacharya,Defending Mechanisms Against Sybil Attack in Next Generation Mobile Ad Hoc Networks, IEEE Technical Review 25(4), 209–214, 2004

[23] B. Parno, A. Perrig, Challenges in securing vehicular networks, in: Workshop on Hot Topics in Networks (HotNets-IV), 2005.

[24] F. Kargl, Z. Ma, E. Schoch, Security engineering for VANETs, in: 4th Workshop on Embedded Security in Cars, 2006.

[25] M. Raya, J.-P. Hubaux, Securing vehicular ad hoc networks, J. Comput. Secur. 15 (2007) 39–68.

[26] A. Toubi, M. Tomader Security challenges in V2I architectures and proposed solutions.In: 5TH EDITION INTERNATIONAL IEEE CONGRESS on INFORMATION SCIENCE and TECHNOLOGY, Marrakech, Morocco. PP 1-6,2018