SECURITY STUDY OF ROUTING ATTACKS IN VEHICULAR AD-HOC NETWORKS (AUTONOMOUS CAR)

Sara LAHDYA[1], Tomader MAZRI[2]

[1]University Ibn Tofail, National School of Applied Sciences Kenitra, Morocco - sara.lahdya@uit.ac.ma
[2]University Ibn Tofail, National School of Applied Sciences Kenitra, Morocco - tomader.mazri@uit.ac.ma

KEY WORDS: Security, VANET, Autonomous Car, DoS, Spoofing, Sniffing etc.

ABSTRACT:

For the past twenty years, the automotive industry and research organizations have been aiming to put fully autonomous cars on the road. These cars which can be driven without the intervention of a driver, use several sensors and artificial intelligence technologies simultaneously, which allow them to detect the environment in order to merge the information obtained to analyze it, decide on an action, and to implement it. Thus, we are at the dawn of a revolution in the world of transport and mobility, which leads us to ensure the movement of the autonomous car in a safe manner. In this paper, we examine certain attacks on autonomous cars such as the denial of service attack, as well as the impact of these attacks on the last two levels of vehicle autonomy.

1. INTRODUCTION

Self-driving cars have symbolized the future of the automobile, but these vehicles are not immune to cyberattacks.

Cybercrime doesn't just target computers, servers or web data. It can also attack much more unusual objects, such as self-driving cars, to hijack artificial intelligence technologies. Knowing that the number of autonomous vehicles could well exceed half a million in just a few years (according to the industrial analysis company Gartner), they are therefore becoming targets of great interest for the most malicious hackers.(Billois, 2016)

2. INTRODUCTION TO VANETS

2.1 Definition of an Ad-hoc network:

Ad-hoc networks are wireless networks capable of spontaneously and autonomously organizing themselves in the environment in which they are deployed without a previously defined infrastructure.

Ad hoc networks, in their mobile configuration, are known as MANETs.

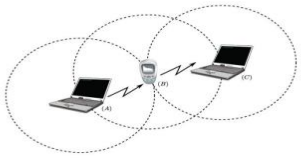

Figure 1. Example of a message transmission in an ad-hoc network

2.2 Definition of a VANET network:

VANETs (Vehicular Ad Hoc Networks) is a new emerging technology of Mobile Ad Hoc Networks (MANETs), where the mobile nodes are intelligent vehicles, equipped with very high technology hardware (Computers, radars, geolocation systems (GPS), different types of sensors, and network peripherals).(Ouiza and Ouiza, 2017)

2.3 VANET communication entities:

On Board Unit: These are on-board units in intelligent vehicles; they include a group of high-tech hardware and software components.(Moghraoui, 2015)

Trusted Authority: it is a storage and transaction server, which is trusted by all network entities. It provides services and applications to all users.

Road Side Unit: they refer to entities located and installed at the roadside. These entities have network access points, and are deployed along the road.

2.4 The VANET communication modes

2.4.1 Vehicle-to-Vehicle (V2V) communication mode:

- Operates on a decentralized architecture.(Marzak, 2017)
- Based on simple inter-vehicle communication that does not require an infrastructure.
- A vehicle can communicate directly with another vehicle, if it is located in its radio zone or through a multi-hop protocol.
- The communication media used are characterized by a low latency and a high transmission rate.
- Very efficient for the transfer of information concerning road safety services.

2.4.2 Vehicle to Infrastructure (V2I) communication mode:

- Allows a better use of shared resources and multiplies the services provided.(Marzak, 2017)
- Thanks to RSU (Road Side Units) access points deployed at the roadside, this mode is inadequate for road safety applications because infrastructure networks are not efficient in terms of routing delays.

2.5 Characteristics of vehicular networks

Energy capacity and storage: The VANET elements have enough energy that can power the various electronic devices of a

smart car. Therefore, the nodes are expected to have a large data processing and storage capacity.(Chaib, 2011)

Topology and connectivity: like Mobile Ad Hoc Networks, VANETs are characterized by sporadic connectivity, as a vehicle (node) can join or leave a group of vehicles in a very short time, thus, leading us to have a very dynamic topology consisting of several separate islands.

Mobility model: Several factors can affect mobility in these networks such as road infrastructure, for example: road, highway, and traffic signs. Moreover, mobility in VANETs is directly related to the behavior of drivers and their reactions to obstacles or different and complex situations encountered, such as traffic jams, accidents... etc.

Security and anonymity: the importance of the information exchanged via vehicular communications makes the operation of securing these networks crucial and a prerequisite for the deployment of VANETs.

2.6 The services offered by VANET networks

Services related to road safety: These services concern applications that have a direct impact on the safety of people and property, i.e. applications that reduce the number of road accidents and improve traffic conditions.(Amar Bensaber et al., 2020)

Services related to comfort: VANETs will not only offer services related to the safety of vehicles and their occupants, but will also ensure the comfort of the latter during their trips.

3. INTRODUCTION TO AUTONOMOUS CARS

3.1 History of the autonomous car

The idea of the autonomous car is not new. It made its first appearance at the General Motors Futurama exhibition at the World's Fair in New York.(Biglia, 2015)

In 1950, Ford and General Motors presented their prototype of the autonomous car. Some independent attempts were also made in Japan and Europe in the 1960s to 1980s. These first attempts at self-driving cars were made on test tracks, but never in real traffic conditions.

The real breakthrough came in 2004 with the creation of the DARPA Challenge. It brings together universities, car manufacturers and innovators with the mission of creating an autonomous vehicle for military use. This challenge takes place in the desert where it is required that the autonomous vehicle travels 150 miles (240 kilometers). While the first edition was a failure, the second was a success with five vehicles crossing the finish line.(Forrest and Konca, 2017)

In 2007, a new challenge was launched. The challenge was to drive 60 miles (97 kilometers) in an urban area while respecting traffic regulations and the obstacles that a driver faces on a daily basis. As a result of this success, many car manufacturers and some participants such as Google embark on the research and development of the autonomous car.

3.2 Definition of the concepts used

Autonomous car concept:

A vehicle is said to be autonomous, when it does not require human intervention to evolve on the road in real traffic conditions.

The concept aims to develop and produce vehicles that can actually drive on public roads among other vehicles.

Concept of applied artificial intelligence:
All the information collected by an autonomous vehicle through its sensors is processed by algorithms and artificial intelligence programs dedicated to its piloting.

Thus, the role that artificial intelligence must play in the autonomous car is very clear: act like a real driver of knowing how to observe and understand its environment.

OEMs concept:
The role of the automotive suppliers is to be specialized in the manufacturing of various components specific to a car.
The automotive suppliers can have a leverage effect on the whole industry regarding its new equipment to be produced.

3.3 The levels of empowerment

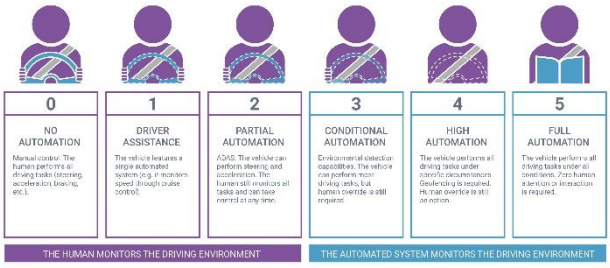

Figure 2. ©Levels of driving automation Copyright 2019, MELISSA KIRSCHNER

3.4 Advantages and disadvantages of autonomous cars

3.4.1 Advantages

- Reduce stress during a journey
- Easier to park
- More economical driving
- Towards more autonomy for people with disabilities

3.4.2 Disadvantages

- A technology that has yet to be perfected
- The risks of computer interference
- Administrative formalities in case of an accident
- The cost

3.5 The different networks of an autonomous car

- The internal network of on-board computers, accessible via the OBD.(Studnia, 2016)
- The vehicle is also interconnected with mobile equipment, such as a smartphone or a tablet.
- The vehicle can be connected to the Internet via mobile networks (2/3/4/5G) and access different services.
- In terms of V2X communications, there are two levels:

- ✓ Locally, the vehicle communicates with other automobiles.
- ✓ The vehicle also communicates with a dismounted infrastructure (roadside), which itself constitutes a network in its own right.

- Finally, the vehicle receives data via satellite (GPS).

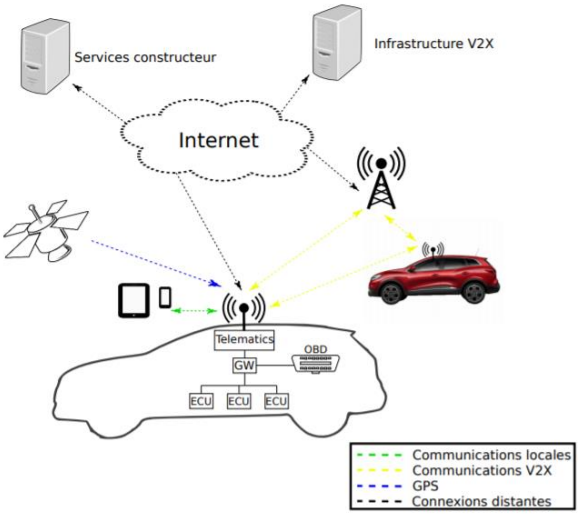

Figure 3. The different networks of an autonomous car.

3.6 The local components of an autonomous car

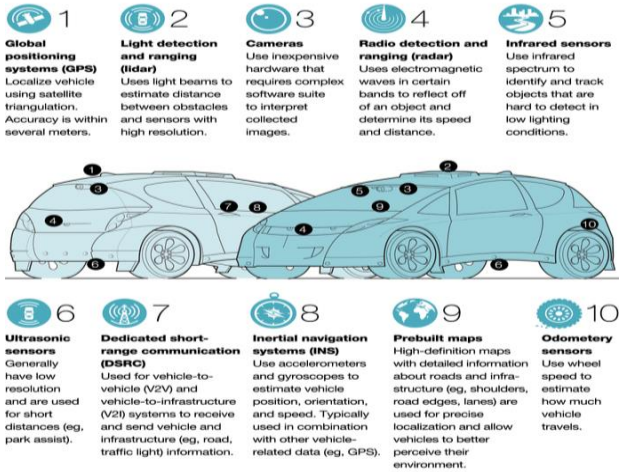

Figure 4. ©The local components of an autonomous car
Copyright 2019 ,McKinsey&Company

4. AUTONOMOUS CAR APPLICATIONS

Services for drivers and passengers:
The exchange of data between the vehicle and its environment allows the development of new services such as the payment of parking lots or tolls, the reception of information on energy consumption, the broadcasting of entertainment, etc.

Commercial offers:
Data sent from a VA to servers could form the basis for many services: predictive maintenance, maintenance or tire change scheduling, etc. Therefore, the market will be very creative in proposing new insurance modalities (towards individualization according to the type of driving) or other administrative or commercial services.

Navigation assistance and driving optimization:
The data received by the vehicle allows it to take into account the traffic situation in a dynamic way in order to avoid traffic jams, for example. For the comfort of passengers, automated driving profiles (speeds, driving styles, etc.) adapt to the topology of the terrain, the state of the traffic, and the driving habits of other road users.

Cooperative and coordinated driving:
Coordination between vehicles allows better management of lane occupancy, optimal traffic light management and avoidance of bottlenecks. The construction of dynamic local maps becomes possible thanks to the sharing of information captured by each vehicle.

5. SECURITY CONCEPTS AND MECHANISMS

5.1 Security in VANETs

The security of wireless networks, like wired networks, aims at guaranteeing essentially the confidentiality, integrity and availability of services. This is a difficult task, especially in a context of increasing connectivity, which is the case of Mobile Ad Hoc Networks.(Gouty, 2020)

5.2 Security features

- A shared transmission medium
- Multi-hop communications
- Dissemination of location information
- Autonomous operations(Kornwitz, 2017)

5.3 Security threats

Denial of Service:
One of the most dangerous threats is the threat of Denial of Service attacks, often abbreviated to DOS. It consists in temporarily paralyzing services and resources in the network, so that they cannot be used and accessed. The purpose of such an attack is not to recover or alter data. It is usually provoked as a consequence of other attacks on energy resources or bandwidth. This can prevent the exchange of alert messages and consequently cancel security services in the networks.(Dede et al., 2021)

Sniffing: Eavesdropping on communications:
In this type of threat, the attack is not active, because the malicious entity only listens to the conversations exchanged in the network and copies all the messages transmitted, to extract the data that interests the malicious entity. Although eavesdropping is considered a passive threat. Nevertheless, in most cases, it is not without consequences. Because the attacker can then use the data collected for personal use or serve other attackers who need this information for the success of their attack plans.

Spoofing: Identity and role impersonation:
In this case, the malicious entity takes the role or identity of another entity. Spoofing can also involve any other element that identifies an entity on the network, in order to impersonate that entity and act on its behalf, to achieve unauthorized privilege levels and access. Such as the case of impersonating a police

vehicle, which is authorized to control vehicles on the network and thus access their personal information and data.

The injection of erroneous messages:
In this type of threat, the attack can cause very serious consequences in VANETs, which can even endanger human life. Indeed, malicious entities broadcast erroneous messages and information in order to influence the behavior of vehicle drivers or to modify their trajectories. This attack can cause the network to malfunction and leads to road accidents.

Privacy Threats:
This type of threat affects very sensitive information in the network. The malicious entity collects information related to the privacy of a vehicle, such as its identity and location to track its path. The purpose of such a threat is very diverse and depends on the intention of the malicious entity towards its target. For him/her may use the information gathered for a later attack, he may pass it on to other entities that have hired him, or he may simply disclosed it to other entities in the network. To remedy this kind of threat, the use of communication pseudonyms is very useful. However, it is not enough. It is necessary to change them periodically in order to avoid that the malicious vehicle can link each entity (vehicle) to its private pseudonym. This way, each vehicle can keep its anonymity in the network.

5.4 Security requirements

Attacks threaten users of vehicular wireless networks. In order to detect and prevent these attacks and improve the security of systems, security services exist. These services include integrity, authentication, non-repudiation, confidentiality, availability, privacy management and access control.

- **Integrity:** guarantee that the data is what it is believed to be.
- **Authentication:** to ensure that only authorized persons have access to resources.
- **Non-repudiation:** ensuring that a transaction cannot be denied.
- **Confidentiality**: Confidentiality protects information transmitted over the network against attacks by malicious entities or entities not authorized to have it (Spoofing attack, for example).
- **Availability:** to maintain the proper functioning of the information system.
- **Privacy management:** It is very important to keep drivers' personal information (real identity, travel path, speed) away from unauthorized observers. To preserve the privacy of drivers, an anonymity management protocol must be in place using communication pseudonyms, which must be changed frequently.
- **Access control:** The role of access control is to define which entities are allowed to connect to the network and to block unauthorized users. This access control is very important so that some applications can distinguish the different levels of access depending on the entity. For example, allowing police and emergency services to exchange information with traffic lights to control traffic.

5.5 Basic security mechanisms

Cryptography:
The technology used for the protection of transmitting data, which contained the messages of different communications.

Cryptography mainly uses keys and secret codes to encrypt (encode) the content of a message using an encryption algorithm, to make it unreadable and therefore unusable by malicious entities.

To make an encrypted message readable, recipient entities have a key (code) and appropriate decryption algorithms to decrypt the message and make its contents readable and usable.

There are two types of cryptography: symmetric and asymmetric.

Certificates:
One of the results of cryptographic algorithms are certificates, which increase the level of security in VANETs.

Each vehicle has a single long-term certificate, which contains the identity and characteristics of the vehicle.

It is mainly responsible for renewing the short-term certificates. Thus, the vehicle has several short-term certificates, which contain a virtual identifier and communication aliases.

The certificates must allow the preservation of the privacy and anonymity of the vehicle.

Hash:
Consists in determining an information of fixed and reduced size called "the fingerprint" from a string of data provided in input of various longer sizes. The one-way hash functions are the most used.

The particularity of this function is that it is very easy to compute and extract a fingerprint from any given string, but very difficult, if not impossible, to retrieve the initial string from the fingerprint. It is an irreversible function.

The digital signature:
This is a digital code associated with an electronic message so that recipients can authenticate its origins and verify its integrity. Its implementation uses the hash and private key functions of the signatory.

MAC technique:
It is a code accompanying data that provides the same functionality of the digital signature, but its implementation is based on the use of the secret key and on functions similar to those of hashing.

The TPD (Tamper-Proof Device):
Is a device composed of hardware and software that contains several high-performance sensors that automatically destroy the stored information after each manipulation of the hardware.

Its mechanism allows storing and keeping secret the data related to the confidentiality of the vehicle, such as certificates and private pseudonyms. Thus, it takes care of the signature of all the messages sent by the vehicle.

6. THE IMPACT OF SECURITY THREATS ON AUTONOMOUS CARS

These different "attacks" highlight the presence of important vulnerabilities at different levels of automotive architectures: sensors, external communications, and internal communications.(Chowdhury et al., 2020)

Denial of service:
Consists of temporarily paralyzing services and resources in the network such as malfunctioning Cameras, Lidars and Sensors, which can lead to fatal accidents or loss of life.(Apvrille and Li, 2016)

Can overload the system with error messages and prevent the CAN system from functioning.

The braking system may refuses maintenance and the vehicle may stop suddenly or be unable to stop where it is needed.

Sniffing:
Allows listening to conversations exchanged in the network and can intercepting and recovering data, including user IDs and passwords.

Spoofing:
Attackers can perform several types of spoofing attacks such as GPS and Lidar spoofing attacks on autonomous cars.

A spoofing attack against a Lidar sensor, effectively tricking the system into perceiving an obstacle in its path that was not there. The attacker sent signals fired at the victim's Lidar at the nanosecond level, and the vehicle's Lidar believed that there was an object in front of the vehicle.

Thus, it may causes the vehicle's GPS to misread its location by about 10 meters, causing the vehicle to change lanes, move left or right, go off the road, and come to an abrupt stop.

Injection of erroneous messages:
Malicious entities broadcast erroneous messages and information in order to influence the behavior of vehicle drivers or to modify their trajectories, which can even endanger human life.

This attack can cause the network to malfunction and lead to road accidents.

The transmission of false data to a wireless conduit can cause a malicious car to increase or decrease the speed of other vehicles incorrectly.

The attackers could turn on and off the lights: immobilizing the entire burglar alarm system, and putting the car at risk for further attacks.

Privacy Threats:
The malicious entity collects information related to a vehicle's privacy, such as its identity and location to track its path.

7. CONCLUSION AND FUTURE WORK

Despite the few obstacles to its arrival on the world market, the autonomous car is a project that is rapidly being perfected, whose security is a major challenge as well as the difficulty of controlling the attackers that result in impacts that can even endanger human life.
It is difficult to control attackers, but in future work we hope to focus on improving the security of AI in AVs and mitigating potential threats and risks. This approach is motivated by the importance of relying on the pillars that have been at the heart of cybersecurity methodologies developed over the years for traditional software, while taking into account the particularities of AI systems.

REFERENCE

Amar Bensaber, B., Pereira Diaz, C.G., Lahrouni, Y., 2020. Design and modeling an Adaptive Neuro-Fuzzy Inference System (ANFIS) for the prediction of a security index in VANET. Journal of Computational Science 47, 101234.

Apvrille, L., Li, L.W., 2016. Sécurite des véhicules connectés et/ou autonomes. MISC Multi-System & Internet Cookbook 56–65.

Biglia, A., 2015. Analyse prospective sur l'implémentation de la voiture autonome : impact sur l'industrie automobile et le citoyen.

Billois, G., 2016. Voiture autonome : la cybersécurité d'abord. Les Echos Executives. URL https://business.lesechos.fr/directions-numeriques/technologie/cybersecurite/0211425976053-voiture-autonome-la-cybersecurite-d-abord-301650.php#Xtor=AD-6000 (accessed 7.10.21).

Chaib, N., 2011. La sécurité des communications dans les réseaux VANET. scholar.google.com. URL (accessed 7.14.21).

Chowdhury, A., Karmakar, G., Kamruzzaman, J., Jolfaei, A., Das, R., 2020. Attacks on Self-Driving Cars and Their Countermeasures: A Survey. IEEE Access 8, 207308–207342. https://doi.org/10.1109/ACCESS.2020.3037705

Dede, G., Hamon, R., Malatras, A., Naydenov, R., Sanchez, I., Junklewitz, H., 2021. Cybersecurity Challenges in the Uptake of Artificial Intelligence in Autonomous Driving. URL https://www.enisa.europa.eu/publications/enisa-jrc-cybersecurity-challenges-in-the-uptake-of-artificial-intelligence-in-autonomous-driving (accessed 7.14.21).

Forrest, A., Konca, M., 2017. Autonomous Cars and Society 54.

Gouty, F., 2020. Comment les hackers peuvent tromper les véhicules autonomes ? Journal du Geek. URL https://www.journaldugeek.com/2020/04/02/entretien-hackers-vehicules-autonomes/

Kornwitz, J., 2017. The cybersecurity risk of self-driving cars . URL https://news.northeastern.edu/2017/02/15/the-cybersecurity-risk-of-self-driving-cars/ (accessed 7.14.21).

Marzak, B., 2017. Clustering et Dissémination des Données dans les Réseaux Véhiculaires. URL https://slideplayer.fr/slide/ (accessed 7.10.21).

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

Ouiza, D., Ouiza, G., 2017. Le routage dans les réseaux véhiculaires VANETs (Thesis). Université Mouloud Mammeri.
Studnia, I., 2016. Détection d'intrusion pour des réseaux embarqués automobiles : une approche orientée langage. URL (accessed 7.14.21).