VANET security surveys

Richard Gilles Engoulou, Martine Bellaïche*, Samuel Pierre, Alejandro Quintero

Département de Génie Informatique et Logiciel, École Polytechnique de Montréal 2900, Boulevard Edouard-Montpetit, Montréal QC H3T 1J4, Canada

A R T I C L E   I N F O

Article history:
Received 11 July 2013
Received in revised form 23 February 2014
Accepted 27 February 2014
Available online 11 March 2014

Keywords:
Security
Vehicular ad hoc networks
Malicious nodes
VANETs

A B S T R A C T

Vehicular ad hoc networks (VANETs), a subset of Mobile Ad hoc NETworks (MANETs), refer to a set of smart vehicles used on the road. These vehicles provide communication services among one another or with Road Side Infrastructure (RSU) based on wireless Local Area Network (LAN) technologies. The main benefits of VANETs are that they enhance road safety and vehicle security while protecting drivers’ privacy from attacks perpetrated by adversaries. Security is one of the most critical issues related to VANETs since the information transmitted is distributed in an open access environment. VANETs face many challenges. This paper presents a survey of the security issues and the challenges they generate. The various categories of applications in VANETs are introduced, as well as some security requirements, threats and certain architectures are proposed to solve the security problem. Finally, global security architecture for VANETs is proposed.

© 2014 Elsevier B.V. All rights reserved.

1. Introduction

A vehicular ad hoc network is a specific type of Mobile Ad hoc NETwork (MANET) that provides communication between nearby vehicles and roadside equipment [1–3]. In this type of network, vehicles are considered as communication nodes that are able to belong to a self-organizing network without prior screening or knowledge of each other’s presence [4]. There are two categories of nodes: On-Board Units (OBUs) and Road Side Units (RSUs). OBUs are radio devices installed in vehicles that move, while RSUs are placed along the road and constitute the network infrastructure. RSUs work as a router between the vehicles. Using Dedicated Short Range Communication (DSRC) radios, OBUs can link to RSUs [5].

VANETs are becoming the most relevant wireless mobile technology. It is one of the promising approaches to implement Intelligent Transportation Systems (ITS). VANETs differ from MANETs in many ways: high node mobility, large scale of networks, a geographically constrained topology that is highly dynamic, strict real time deadline, unreliable channel conditions, unavoidably slow deployment, sporadic connectivity between nodes, driver behavior and frequent network fragmentation [1,2,6]. The goal of VANETs is to allow communication between vehicles. Thus, these nodes need to incorporate radio interfaces for communication and a specific range spectrum must be dedicated for VANET data exchange.

In order to be an integral component of a VANET and to communicate efficiently, nodes need certain features that will help them to gather information, to inform their neighbors and to make decisions by considering all of the collected information. Such features are sensors, cameras, on-board computers, Global Positioning System (GPS) receivers, Event Data Recorders (EDR) and omnidirectional antennas [7].

VANET technology presents certain advantages, such as a reduction in the number of road accidents, a more enjoyable driving and traveling experience with the simplification of certain payment processes for tolls, parking, fuel, etc. Road users employ various applications for safety and efficiency, traffic management, infotainment, warning, comfort, maintenance, music sharing and network gaming [8]. These applications involve the exchange of messages such as emergency message distribution, traffic incidents and road condition warnings that enhance traffic safety and driving efficiency. These applications require data communication between nodes. The content of the message can have an impact on drivers’ behavior. This may change the network topology and security may be threatened if a malicious user alters the message [9]. Some possible attacks could cause traffic jams, spread bogus information, cheat the positioning information, disclose IDs, replay, masquerade or forge data, violate privacy or cause wormholes, Denial-of-Service (DoS) attacks, in-transit traffic tampering, impersonation as well as hardware tampering [2].
Another challenge concerns users’ privacy: drivers will not accept to be tracked by a central system such as a big brother program, yet some security solutions may threaten users’ privacy.

In this paper, we shall classify the attacks according to their characteristics, the requirements involved, and the defences that could be used. A description of the type of attackers will also be introduced. Presenting security threats while keeping in mind all of the other aspects involved in such attacks consists of a new approach. A global security architecture in VANETs will also be proposed. Moreover, we plan to classify VANETs’ threats while considering the security layer level in the system.

This paper is structured as follows: Section 2 presents VANET’s architectures and their characteristics, Section 3 inventories the relevant challenges and Section 4 discusses VANETs’ applications. In Section 5, security requirements are examined, while security threats are presented in Section 6. Section 7 paints a portrait of the attackers’ profiles. Section 8 lists the attack characteristics while Section 9 presents users’ privacy issues and Section 10 offers some security solutions. Finally, Section 11 proposes a global security architecture.

2. VANET architecture and characteristics

VANET architecture can be divided into three categories: the cellular/WLAN, ad hoc and hybrid architectures [2].

If the infrastructure consists of a cellular gateway or a WLAN or a WiMAX access point, the network will be considered a pure cellular/WLAN.

When no infrastructure is available, the nodes must communicate with one another without relying on an infrastructure. This denotes a pure ad hoc architecture.

Sometimes, various access points, such as cellular gateways, will be available for communication. In this case, nodes can communicate with these infrastructures or they may also communicate directly with one another. This is called a hybrid architecture.

VANETs have many unique characteristics and some of them are presented in this section. First of all, the channel characteristics will be introduced. Secondly, we will present some equipments that helps vehicles to be smart and that enable them to communicate. Finally, the relationship between the vehicles and their infrastructures will be addressed.

2.1. Channel characteristics

In 1999, the United States Federal Communications Commission (FCC) allocated a block of spectrum in the 5.850–5.925 GHz for Vehicular Communications (VC). In Japan, the 700 MHz band is used and similar bands have been attributed in Europe. For the same purpose, a bandwidth of 75 MHz has also been allocated by the FCC for this kind of communication which is referred to as DSRC (Dedicated Short Range Communication) [4]. DSRC is based on IEEE 802.11 technology which is about to become the standard under the name 802.11p [6]. This standard, which is specified for VANETs, uses a 10 MHz channel. The data rate ranges between 3 and 27 Mbps for each channel [10].

Vehicles send periodic information to their neighbors by beacon packets with a required frequency of 10 messages per second and within a maximum range of 150 m.

2.2. On-board equipment

On-board equipment installed in vehicles makes them smart and provides them with the means to communicate [11,12]. They consist of different equipments in vehicle.

An Event Data Recorder (EDR) records transmissions and receives messages and all of the events that occurred in the vehicle environment during the trip. A Global Positioning System (GPS) receiver communicates the geographic location, the speed, the direction of the movement and the node acceleration at specified time intervals.

A computing device is used to take appropriate actions in response to messages received from other nodes. Radars and sensors are used to detect obstacles in the vehicle environment. An omnidirectional antenna is used to access wireless channels. An Electronic License Plate (ELP) is installed on every new vehicle in the factory. It provides an ID number used by the police or any official order [3].

2.3. Relationship between Vehicles and their Infrastructures

In a VANET system, some entities such as Regional Transportation Authorities (RTAs), NetworkAuthorities (NAs), Law Enforcement Authorities (LEAs) and roadside infrastructure consist of border RSUs for pseudonym management, simple and regular RSUs for Internet access and users’ vehicles [4,13]. In this system, the RSUs provide infrastructure access and network services. They are operated by third-party service providers. Service providers have business contracts with the RTA to build access infrastructure in the RTA’s region. Therefore, RSUs are not owned by the RTA although border RSUs are owned and operated by the RTA and they act as the agents delegated with the RTA’s authority.

There are three types of communication to consider in VANETs (see Fig. 1): Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I) and Infrastructure-to-Vehicle (I2V).

In V2V communication, vehicles can communicate with each other directly in wireless range or indirectly in a multi-hop mode. For example, when a car using V2V communication encounters a dangerous situation, it communicates with other cars and provides useful information, by suggesting that they avoid the area. Furthermore, V2V communication can be classified into two distinct categories depending on the positions of the sender and the receiver: single-hop and multi-hop. The vehicle’s local broadcasts send

![Fig. 1. System architecture in VANETs.](image-url)
safety warnings through single-hop V2V communication while non-safety related messages are exchanged through multi-hop V2V communication [14].

V2I safety message communication refers to the wireless exchange of critical safety and operational data between vehicles and roadside infrastructure elements. V2I communication applies to all types of vehicles and roads and it transforms infrastructure equipment into "smart infrastructure" through the incorporation of algorithms that use data exchanged between vehicles and infrastructure elements to perform calculations that recognize high-risk situations in advance, resulting in the production of alerts and warnings for drivers through specific countermeasures. One particularly important advance is the ability of traffic signal systems to communicate the Signal Phase and Timing (SPAT) information to vehicles in order to deliver active safety notices and warnings to drivers. An early implementation of the SPAT application can enable near-term benefits from V2I communication in the form of a reduced number of car crashes which, in turn, show that it may be beneficial to accelerate the deployment [15].

In I2V communication, the infrastructure can broadcast diverse messages to moving vehicles regarding road conditions as well as various, traffic information. Wireless Access points (Road-Side-Units, RSU) are used as the network infrastructure. Different protocols can be used: to maximize the throughput for the drivers and the passengers, a Medium Access Control (MAC) protocol [16], or WiMAX (802.16) provides a reliable end-to-end link [17], or the Cooperative Strategies for Low-Power Wireless Transmissions Between Infrastructure and Vehicle [18].

3. Challenges

Despite all of VANET’s advantages, many challenges remain to be addressed by the research community and the industry. Some of these challenges are presented as follows: time constraints, network scale, node mobility and volatility [19].

3.1. Time constraints

An important requirement of VANETs pertains to the node’s ability to transmit messages within an acceptable time limit. Some applications, such as those that pertain to safety, require strict deadlines [20]. However, it may be difficult to verify the authenticity of messages, which would consequently increase the delivery time and respect the delivery deadline of the message.

It is very important to respect critical deadlines in specific cases with certain applications [21]. For example, all of the applications used by the emergency services involve time constraints for message delivery. The driver who receives a warning message must have sufficient time to react. If the arrival deadline is not met, it will be too late and the consequences may be catastrophic.

3.2. The scale of the network

VANET is about to become the largest ad hoc network in the world. The number of nodes of this network exceeds 750 million and it is still growing [22]. However, many questions remain about the implementation and the deployment of this network. A global authority that would govern such a network has yet to be set up. It is well known that security and users' privacy issues differ in various areas of the world. Consequently, it will be complicated to standardize the rules regarding the deployment and the use of this network. Another question is: "which authority will be in charge of managing identifications and distributing public and private keys?" Such coordination regarding the key installations is needed by manufacturers all over the world [23].

3.3. The high mobility of nodes

The high mobility of nodes in VANETs causes considerable challenges in VANET research. It is impossible to apply classical authentication techniques for nodes and messages due to the high mobility of nodes. For example, one cannot propose a protocol that uses a handshake in a VANET environment given that some nodes will communicate only once and a lack of time impedes checking the authenticity of the messages received from these nodes. Therefore, securing mobility challenges represent a major problem and although many researchers have discussed these challenges, numerous issues remain to be resolved [24].

However, a security protocol ensures mobility constraints. Messages can be sent without considering the mobility of the secure cars. The messages will be transmitted through broadcast or unicast. Such an approach neither imposes special routes nor specific speeds for drivers to follow [25].

Since vehicles frequently change their point of network attachment when they access Internet services, they need mobility management schemes that provide seamless communication. This mobility management meets requirements such as seamless mobility, support IPv6, scalable overheads and low handoff latency.

In VANETs, all nodes are mobile. Vehicles make connections with one another which last only a few seconds. Hence, secure protocol requires significant interplay between the sender and receiver [26]. Two vehicles which have never crossed one another may never meet again [22,27].

3.4. Volatility

The connectivity time span between two nodes can vary and such an event may occur a single time. Each vehicle has a high level of mobility, so the connections between the vehicles would be lost and might remain so within a few wireless hops, for a limited period of time. Furthermore, the connected cars could even travel in opposite directions [23,26]. Due to the lack of long lived context in VANETs, it would be difficult or impossible to achieve long life passwords required to ensure the security of personal contacts in the channels of users’ devices.

The personal contacts in the secure channels of users’ devices require long life passwords and this is not a practical safety element in vehicular communication, due to the short lifespan of the context [22].

3.5. Incentives

Why would people accept to participate in VANETs? That is one of the main questions to ask before implementing this technology. It would be essential to provide them with the right incentives for them to agree to take part in this adventure. These incentives could be the advantages inherent to this technology, such as the ability of being informed about what is happening on the road ahead so that drivers can avoid certain unpleasant situations. Furthermore, such a technology may very well reduce the number of accidents and increase the safety of our roads. Indeed, research has shown that 60% of all accidents could be avoided if drivers were warned half a second before the impact of a collision [28]. Many accidents that happen on the road occur at intersections and dealing with intersections is one of the most important challenges for drivers. VANETs allow for new intersection applications to help drivers handle these issues [29]. Safety applications in VANETs will
provide users with information regarding the best routes to choose in order to reach their destination when they have to deal with such intersections. Drivers and all other road users will be able to enjoy an Internet connection and peer-to-peer applications to share music and videos. They will even be able to use the network to play games [30].

It will also be important to convince users to agree to cooperate with law enforcement authorities when the information and technologies shared in the network will be accessible.

4. Applications

The development of smart vehicles engenders a variety of new possible applications of VANETs. These applications can be categorized in two major groups: Intelligent Transport Applications (ITA) and Comfort Applications (CA) [2]. The ITA can be subdivided into two sub-groups which are: Transport Safety Applications (TSA) and Transport Efficiency Applications (TEA). The main purpose of ITA is to avoid and prevent road accidents [10]. We can present TSAs as those related to emergency situations while TEAs deal more with prevention. As for Comfort Applications, whose role is to make the road experience more enjoyable for both drivers and passengers, they will be used primarily for information and entertainment purposes [6]. The remainder of this section will deal with potential applications that will be presented according to their usefulness based on the abovementioned categories.

TSA includes applications designed to avoid collisions in specific situations. For example, if an accident occurs far ahead on the road, nodes will advise one another about the situation and they will be able to suggest to drivers to decelerate or select an alternative route. This kind of application would help to reduce long line ups of vehicles trapped in traffic after an accident [4]. Some intersections are devoid of traffic lights and an intersection light application can inform nodes of such cases. That will contribute to reducing collisions. Another safety application could advise nodes about the traffic situation and the state of the road ahead. However, this type of application fits better with the TEA presented below.

The Vehicle Safety Communication (VSC) Consortium formed by the government and industry highlighted eight applications [31]:

(1) Traffic Signal Violation Warning: the goal of this application is to warn drivers that they are about to violate a traffic signal that requires a complete stop (a red light, a flashing red light, a stop sign, a railroad crossing, etc.), and (2) Curve Speed Warnings: in this application, RSUs broadcast messages to vehicles approaching curves. The delivered information can include curve location, curve speed limits, level of curvature, information pertaining to the road banks as well as road surface conditions. Hence, drivers can be warned ahead of time of potential dangers [32].

(3) Emergency Electronic Brake Lights: the EEBL application is integrated within a Collaborative Adaptive Cruise Control (CACC) which uses network—provided information to automatically brake the car if the driver does not react to the warning [33].

(4) Pre-Crash Warning: if a crash is unavoidable, the vehicle involved will broadcast a pre-crash warning signal to neighboring vehicles, so that nearby drivers have more time to react, which may plausibly avoid a fatal pileup accident [34].

(5) Cooperative Forward Collision Warning: designed to aid the driver to avoid or mitigate rear-end collisions with vehicles ahead by warning the driver of the impending collision. (6) Left Turn Assistant: provides drivers with information about oncoming traffic to help them make a left turn at a signalized intersection devoid of a left turn arrow. (7) Lane Change Warning: this application warns the driver if an intended lane change could cause a collision with a nearby vehicle. (8) Stop Sign Movement Assistance: this application provides a warning to a vehicle that is about to cross through an intersection after having stopped at a stop sign.

The TEA is more interesting due to its role of preventing accidents. The main application in this subsection concerns traffic management. The specific case of this application could be the following: traffic monitoring applications in which nodes are informed about the traffic situation ahead. They are then able to suggest a detour route computation based on the information received [35]. Moreover, the traffic condition analysis on the fly application will help avoid and reduce congestion. When a node is informed of a line up ahead or a specific situation that may cause congestion, it will change the itinerary, if possible. Many other applications could be imagined in smart vehicles and VANETs, such as on-board navigation, location-based services inside the vehicle and traffic violation applications as well as cooperative driving for VANETs. All of these applications may optimize traffic [1,4].

The purpose of comfort applications, which can also be considered infotainment applications, is to enhance the users’ road experience. Many applications are exploitable. The goal consists of having a connection that will make all of the Internet applications available: music, video sharing downloading email access, Internet games and advertisements. However, other comfort applications can be accessed without an Internet connection. These applications pertain to weather information, interactive communications, game networks, information related to facilities such as hotels, gas stations, restaurants, payment services and other location-based services. Maintenance applications are useful for drivers who encounter mechanical emergencies: they would be able to access distance help from a mechanic service via a wireless diagnosis, an intervention [2,7].

5. Security requirements

Before addressing security issues of VANETs, it is paramount to address the requirements the system must respect for the appropriate operation of the network. Failure to respect a requirement may lead to a possible security threat. The main requirements defined in [4,7] are: authentication, integrity, confidentiality, non-repudiation, availability, access control, real time constraint and privacy protection. Most of these requirements are related to general security issues and others are specific to VANETs. The following section delves into the details pertaining to these requirements.

5.1. Authentication

This is one of the main requirements for any system. In VANETs, it is very important to have certain information concerning the transmitting node, such as its identification, and that of the message sender as well as its property and location. It is important to authenticate all users and messages which transit through the network. Authentication controls the authorization levels of vehicles. In VANETs, authentication prevents Sybil attacks by assigning a specific identity to each vehicle. For instance, congestion avoidance may prevent a single car from claiming to be a set of one hundred vehicles in order to give the illusion of a congested road. Powerful authentications provide legal evidence using external mechanisms, such as traditional law enforcement authorities to detect attacks [26].

There are several types of authentication approaches [36]:

ID authentication allows a node to identify the transmitter of a message in a unique manner. This authentication also allows a node to belong to the network. When the ID authentication is set, it is easy to avoid certain attacks such as impersonation or fake nodes.

Property authentication helps to determine what kind of entity is communicating: a car, an RSU or another type of equipment. Location authentication helps to authenticate the node position when a location application is involved.
5.2. Integrity

Integrity ensures that a message was not altered between the moment it was sent and received as the received message must match the message sent. The receiver will then be able to corroborate the sender’s identity during the transaction [37]. Integrity protects against the unauthorized creation, destruction or alteration of data. If a corrupted message is accepted, the integrity property is violated and the protocol would be deemed flawed.

To achieve integrity, the system must prevent attackers from altering messages since the contents of messages must be trusted [38]. Outsiders will refrain from interjecting messages through authentication [19,23].

A security protocol ensures that data are not compromised when they are forwarded from one secure car to another, its final destination, due to the message appended signature from secured traffic lights. The message can also be verified with similar ones that are generated in its immediate geographical neighborhood within a short moment of time [7].

5.3. Confidentiality

During communication between entities (vehicle or infrastructure), outsiders are not able to understand confidential information that pertains to each entity. This can be achieved due to message encryption that can protect the confidential information of each driver [38,39] such as usage profiles and users’ identity [19].

Message confidentiality in VANETs depends on the specific application scenario. For example, safety-related messages do not contain sensitive information. Their encryption is thus unnecessary. However, some messages from applications such as those used for toll payments, where vehicles need Internet service from RSUs, must be kept confidential by way of encryption schemes.

Confidentiality is achieved by using public or symmetric key encryptions to ensure secure communications [4].

In V2I communication, the RSU and the vehicle share a session key that is generated after mutual authentication. All of the messages are subsequently encrypted for confidentiality with the session key and they are also attached to the MAC (Message Authentication Code) for message authentication [40].

Non-repudiation: is defined as the impossibility for one of the entities involved in a communication to deny having participated in all or part of a communication event. This protects against false denials involved in the communication. Non-repudiation provides the receiver with proof that the sender is accountable for the messages it generated [41].

The main goal of non-repudiation consists of collecting, maintaining, making available and validating undeniable evidence about a claimed event or an action in order to resolve disputes about the occurrence or non-occurrence of that event or action. Non-repudiation depends on authentication, but it generates solid proof as the system can identify the attackers who cannot deny their crimes [26]. Violators or misbehaving users cannot deny their actions.

Any car information (speed, time, trip route and violation) will be stored in a Tamper Proof Device (TPD) and any authorized official will be able to retrieve such data [38,39].

5.4. Availability

The network and applications should remain operational even in the presence of faults or malicious conditions. This requires not only secure but also fault-tolerant design, resilience to deputation attacks, as well as survivable protocols, which resume their normal operations after faulty participants are removed [42].

An adequate routing protocol is needed to reach all of the required recipients that may be unknown to the sender. Also, certain messages (e.g. an icy road warning) must be kept in a specific location for a given period of time [43].

This property deals with the availability of certain resources manipulated by the protocol. For example, for a key-exchange protocol, we must be sure that a session will really be established. Therefore, if user x1 requests the server to set up a session key with the server, the system must subsequently reach a state in which x1 and the server both have knowledge of the new session key [44].

Many applications need faster responses from sensors or ad hoc networks since delays make certain message meaningless or they may have devastating consequences. Especially in cases where the application layer is not reliable, it can store partial messages that are completed in future transmissions to make the information forever available. Therefore, a real-time or a near real-time approach will be required for many applications used in VANETs [23].

5.5. Access control

This requirement has the role of determining rights and privileges in the network. Some sensitive communications such as those from police cars or other law enforcement authorities must not be heard by the other nodes in the network.

Access to specific services provided by the infrastructure nodes and the other nodes is determined through local policies. As part of access control, authorizations establishes the rights of each network node [42].

In [45], Moustafa et al. present a Kerberos model where every service requires some credentials for the client in the form of a ticket. There are two types of tickets: Ticket Granting Tickets (TGT) and Ticket Granting Services (TGS). The TGT allows the client to obtain TGSs while TGSs grant service access to the clients. Hence, clients must first obtain a TGT before they request a TGS for each service they wish to use.

Therefore, the access control provides another warranty which prevents unauthorized people from accessing the services for which they do not have access rights.

6. Security threats

Same as classical networks, VANETs are vulnerable to many attacks. The fact that these networks have yet to be implemented makes the situation even more complicated. Some attacks are thus imagined and solutions are proposed by considering the possible attacks to the system once it is implemented. In this section, VANETs’ security threats are presented while considering all of the other parameters involved, such as the scope of the attack, the impact, the requirements, the applicable security solution to protect the system from this attack and the profile of the attackers who may be able to perpetrate such attacks [1,2,4,6,7,23].

Denial of Service: This attack, one of the most popular in classic networks, can also be perpetrated in VANETs. The goal behind this kind of attack is to bring the network down, consequently rendering the VANET unavailable [7,23]. Attackers can perpetrate this attack by jamming the network or by inserting unnecessary information in the network [46]. A prankster can put down the VANET simply to prove that he has the capacity to do so. The scope of this kind of attack is particularly extended, since the attack will affect a large set of nodes before it can spread over an extended area through many nodes in a multi-hop way. Moreover, the impact of this attack is significant as it may be difficult to correct it in spite of the fact that it has been detected [47,48]. The requirements concerned by this attack consist of the data integrity as some messages could be altered due to the non-respect of all of the communication requirements. Obviously, in such a case, the data availability would be compromised as well. When the network is down, data are not
available. Finally, the real time constraint cannot be respected when the network undergoes a communication problem. A solution that could be implemented to face such threats is presented in [49], where an On-Board Unit (OBU) is used to make the decision to deter Denial-of-Service (DoS) attacks. In the event of a DoS attack, the processing unit will suggest that the OBU switches channel, technology or that it uses a frequency hopping technique. Any attacker, regardless of his profile, be it malicious or rational, is able to perpetrate this kind of attack. For the attacks to be more effective, the attacker must be an active insider of the VANET.

Eavesdropping: This attack occurs when an attacker is located in a vehicle, be it stopped or moving, or in a false RSU [50]. The goal is to illegally obtain access to confidential data. Confidentiality is the requirement relevant for this type of attack and it can be prevented through message encryption [51].

Impersonation: This attack happens when someone usurps someone else’s identity by adopting the identity of another node [42,50] before perpetrating malicious actions. When the time comes for the authorities to track a culprit, as in the case of an accident, for example, they might arrest an innocent person if the network contains erroneous information. In addition, the node whose identity has been hacked will be rated negatively by the other nodes in the network, and in this case, it could be excluded from the network. This is a single-hop attack because it is directed at a single node and the scope of the damage is limited to this node [52]. This type of attack is difficult to detect and even more difficult to correct, especially when the victim node is isolated. The requirement involved in this attack is non-repudiation. If the identity is not corrected, it is almost impossible to identify the real culprit. Confidentiality and access control requirements are also involved to the extent that the malicious node can receive information for the real owner of the hacked identity and it can also leave access to certain systems reserved for the owner of the identity. Finally, the privacy requirement of the victim’s node will be significantly affected. Digital signatures and certificates prevent impersonation, modification and unauthorized injection of packets without the proper credentials. Thus, an external attacker, an illegitimate member of the network, can only replay control or data packets [53]. The signature of the message could also be used to prevent such attacks since malicious nodes could receive unreadable messages. Furthermore, this kind of attack is perpetrated by insider nodes, those which already belong to the network [54]. Because the attack is aimed at a specific node, the attacker would be considered as rational. Attackers who belong to the network are considered active attackers.

Message falsification/alteration occurs when erroneous information is provided or when information that passes through a node is modified [55,56]. A malicious node could lie by indicating that there is an accident ahead when this is not the case. The target of this attack can be in a single-hop position or it can be far away so that a multi-hop communication is required. The message must be transmitted to many nodes. If the malicious node is the only node that retransmits the message to others, the attack will then affect many other nodes [19]. However, in the real world, the attack will simply concern the nodes that receive the information from malicious nodes. In this case, the scope of the attack would be limited to the nodes that received the corrupted messages. This attack could be detected and corrected if other nodes, which have not been hacked, have access to the same information. The requirement involved in this case is the integrity of the messages since they have been falsified or altered and the information transmitted obviously differs from the original message. One of the defences that could be applied in this situation is message data verification, a method that helps to check the data inside the message to ensure that the message is legitimate [57]. A node that would perpetrate such an attack must belong to the network, meaning an insider node. It could be rational or malicious and it is considered active.

Message delay and suppression refers to a situation in which a node will hold onto a message before sending it [58,59]. This creates a delay, or a message could simply be suppressed. Creating delays in message delivery can lead to unfortunate consequences when the application is time-constrained [26]. For instance, if an accident warning message is suppressed, vehicles will not be alerted as to the situation ahead and the scope of the accident may be enlarged. Furthermore, a malicious node can replay an obsolete accident message in order to slow down traffic [53]. These attacks are similar to the previous ones as they pertain to messages that are intercepted by malicious nodes. However, in this case, the integrity of the message is not affected, but only the message itself: it will not be received or it will be sent with a delay. This is not acceptable due to the real time constraint requirement in VANETs [22]. These attacks use single-hop communication and they are limited to the next node involved in the communication. This type of attack would be difficult to detect and correct. The requirements involved in this attack are real time constraint and availability. In the first case, the message will be received with a delay, whereas in the second, the message will not even be received [60].

Hardware tampering can occur at the manufacturing level or by way of mechanical means to manipulate the node physically [23,61]. It can also be perpetrated by other nodes in equipment such as radar or GPS receivers. The main requirement involved in this case is availability. If materials are physically damaged, communication is disturbed and it becomes unavailable [62]. Unavailability can also affect the real time constraint of non-compliance. The defence that could be applied in this case is the Trusted Platform Module (TPM) [63]. Moreover, the driver must perform a physical verification. For this kind of attack, the node can be an outsider or an insider, but it must be active and rational to target a specific node. Hardware tampering also includes sensor tampering which refers to the alteration of the position, the speed and the direction of other nodes by an attacker. In case of an accident, liability will fall on the attacking node rather than on the attacker. It is possible that other types of attacks will occur when VANETs are actually implemented in the real world. Hence, the attacks presented above do not constitute an exhaustive list.

7. Attacker profiles

When addressing security issues of VANETs, it is interesting to specify the network attackers’ profiles as well as the kinds of attacks that they can perpetrate. Raya et al. [64] categorize attackers according to three bipolar criteria which are presented in this section.

Outsider vs. Insider: Outsiders are nodes that do not belong to VANETs when they are not authenticated in the network. It is quite difficult for an outsider to perpetrate an attack. However, they can eavesdrop in the network in order to collect information about road users without their awareness and use them for a future attack [65]. They can also perpetrate a DoS attack. An attacker can flood or jam the network with bogus messages. Even if he does not belong to the network, some vehicles in the network may receive these messages and the network will be brought down subsequently. An outsider can devise a black hole attack or introduce false messages into the network [8].

Moreover, VANETs can be perpetrated by insiders. There are two types of insiders: the first is an authenticated node which is a full member of the network, and the holder of an authenticated public key. It has access to all the details pertaining to the available knowledge in the network. An insider has the possibility to
perpetrate all sorts of attacks in the network. Attacks in VANETs are presented in Section 6.

The other types of insiders are industrial insiders which can be mechanical units or entities in the assembly chain of the automobile industry endowed with the capacity to update the firmware of the vehicle [66]. This could give them the opportunity to inject a malicious program into the system. A manufacturer who is responsible to set up the VANET system can then manipulate some data into this system so that it will be difficult to detect the harm. The main attack that could be privileged by such attackers is the hardware tampering proof [67]. It is easy for an insider to conduct such an attack. Furthermore, attacks perpetrated by insiders can create much greater damages than those performed by outsiders.

Malicious vs. rational: malicious attackers are motivated simply by the pleasure to do so. They have no specific target and they do not seek a specific result. Their only interest consists of bringing down or harming the network [68]. An example of this kind of attacker is a prankster whose goal could be to create car accidents by giving false information to vehicles in a specific geographic area [69,70]. Such an attacker could perpetrate attacks such as network jamming, DoS, hardware tampering, message falsification attacks and so on.

Rational attackers have a specific target. Although they can be more dangerous [71], they are more predictable. They can attack with impersonations or eavesdropping schemes or they may even delay or suppress messages.

Active vs. passive: an active node is the one that can send messages to harm other nodes or a part of the network. Generally, this attacker has the authorization to operate within the network. Moreover, active nodes that have insider status could perpetrate almost any kind of attack on the VANET.

Furthermore, passive nodes simply eavesdrop communications between the other nodes in the network. This type of attacker does not have any authorization. It will monitor the network and try to find some information on the network. Although it cannot cause any direct damage to the network, the gathered information could be used for future attacks. In general, passive nodes are also outsiders.

8. Attack characteristics

In order to build robust security architecture for VANETs, it is important to study the characteristics of the attacks that could occur [23,47,64]. One can consider a malicious data attack as a situation in which a malicious node tries to convince other nodes to accept corrupted data. The attack is successful when a node accepts corrupted data from a malicious node. Golle et al. [39] characterized attacks in VANETs according to their nature, target, scope and impact.

The nature of the attack determines what type of attack is being perpetrated. For example, the DoS attack, the jamming or the Sibyl attack. Some malicious nodes will try to convince other nodes to change direction [58]. Yet, others will give false information regarding their identity, their position or their speed. Therefore, the nature of an attack will determine the way a malicious node can harm the network or its nodes.

The target of the attack depends on the distance that separates the malicious nodes from the victim nodes. If the victim nodes are close to the malicious ones, it will be easy to convince them to accept or process false data. However, malicious nodes will need some allies to help them convince other nodes that their information is legitimate, given that nodes in VANETs do not use information from a single vehicle to make a decision on an action [72]. If the distance is long, the malicious node will also need other malicious nodes to convince remote victims about the veracity of their information.

The scope of an attack refers to the extent of the damages [73]. If the number of victims is low or if the attack was successful only in a small area, one could say that the scope of the attack was limited. However, one can talk about an extended attack when the area of attack is broad or when a limited attack is propagated from a small area to a large one. Preventing such propagation is challenging.

The impact of the attack measures the amount of damage of an attack and the capacity to overcome those damages. There are three possibilities: (1) the malicious nodes are able to corrupt target nodes with false data and the victims realize the uncertainty of the data they received and correct this false information. In this case, the attack is detected and corrected. (2) If victims are able to detect the attack while others are unable to do so, one can say that the attack is detected but not corrected. (3) The worst situation occurs when all of the victims are unable to detect the attack: the attacks are undetected and uncorrected [74–76]. Certain contexts are more vulnerable to this situation. For example, if the victim nodes have no contact with honest nodes to help them realize that the data they are receiving are corrupted, they will be unable to overcome the situation.

All of these characteristics must be considered in order to build solid and robust architectures and algorithms and to ensure security in VANET systems.

9. Privacy

Privacy is one of the greatest challenges in the implementation of VANETs. However, most of the drivers want to keep their information protected and private and they do not wish to share their confidential information [24,27]. The information like identity of the driver, driving behavior, the past and present location of the vehicle, will be private.

The main question is this: “how can we build a system that will respect users’ privacy while protecting them from malicious nodes simultaneously?” The system must guarantee users’ privacy in order to prevent a situation in which their every movement would be tracked. The threat of a big brother scenario is always present. It is thus necessary to ensure users’ anonymity in the communication exchanged while respecting the trusted base system of VANETs [77].

Moreover, since information is sent via broadcasts in wireless communication, it can be received by any network node. These are privacy sensitive data (vehicle location, real identity, speed, time) and internal car sensor data [43]. The goal is to keep the drivers’ information out of reach of unauthorized observers.

Therefore, a driver’s location and movement must not be traceable. Nowadays, users’ privacy is a significant factor for the successful deployment of VANET technology.

9.1. Threats

Moreover, it will be easier to follow malicious persons such as criminals and terrorists by tracking their electronic identity [78]. Likewise, in the near future, cars will gather users’ information. At the same time, these cars are becoming more and more intelligent as various features are added to enhance the driving experience of road users. These features facilitate communication between cars so that the information gathered in a car could be shared, on a voluntary basis or not [79]. All these technologies and intelligent advances will lead to a greater number of threats and attempts to violate privacy. Communication between cars, the information shared between vehicles, will concern their
identification, their position and so on. Other privacy threats may be perpetrated by people with some authority. Dotzer et al. [80] present some privacy threats where the police would exploit drivers’ information from beacon frames. Business managers could exploit the data from their employees’ cars while they are parking their vehicles in the company parking lot. Insurance companies could track their clients’ data in order to assess their behavior, etc.

Privacy violation occurs when users’ identities are held by a third party or another node which is not authorized to have them [42,81]. Marketing firms could exploit users’ identities in order to custom make their advertisements to target clients’ habits.

9.2. The trade-off between privacy and security

On the one hand, the role of authorities is to ensure that users’ private data and identities will remain safe during communication between nodes. On the other hand, car manufacturers and system operators need to know users’ identity in order to intervene in their system when an issue arises. Most of the security protocols and architectures need to know the node’s identification in order to be able to ensure their security. This means that there must be a trade-off between users’ privacy and their security [82,83]. It is also difficult to ensure real time constraints when applying security and users’ privacy protocols.

9.3. Users’ reluctance

One of the greatest obstacles when implementing VANET technology concerns the users’ negative perception since they feel that they are being monitored under the authority of a third party [84–86]. However, users would be much less reluctant if they are convinced of the safety and transport optimization provided by VANETs. Users accept Internet and cellular technologies, so they will be open to accepting VANET technologies if the advantages are well explained to them. The main issues that will remain pertinent to the technical implementation of the technology.

9.4. Solutions proposed to ensure privacy

Many research solution projects and standardization studies have been conducted regarding privacy of VANETs.

According to Papadimitratos et al. [83], pseudonyms can be used to improve the level of privacy in VANETs to make communication anonymous. By region, a large number of certification authorities (CAs) are responsible for the identity’s vehicles management. Each node (vehicle or RSU) has a unique identity and a pair of private and public cryptographic keys.

Each private node has a set of distinct certified public keys as pseudonyms and appends the pseudonym to a message. The pseudonyms have a specific lifetime span.

Kargl et al. [32] propose an identity privacy solution which specifies how secret the identity of the sender should be kept and a location privacy which has different levels for the range location.

Raya et al. [23] propose the use of a set of anonymous keys that change frequently according to the driving speed. A key can only be used once. The key can then be preloaded in the vehicle’s Tamper Proof Device (TPD) and will be changed during the yearly checkup. CA certifies each key which has a short lifetime. The real identity of the Vehicle will be obtained from a judge.

Dotzer [80] proposed a three phase approach: (1) the initialization phase, which consists of matching the identity of the node with a set of pseudonyms under the authority of an independent body. These pseudonyms will then be used to apply for services from different car manufacturer that will map each pseudonym with a set of credentials. (2) The operational phase occurs when the node chooses one of its pseudonyms related to a credential to sign its messages and to participate in communication with other cars. (3) This credential will be verified by other cars to ensure the legitimacy of the node. If the data sent by a legitimate node are corrupted, a credential revocation phase is applied.

Lu et al. [87] introduce a privacy preservation (ECPP) protocol in VANETs for anonymous authentication. The protocol uses short-time anonymous keys between On-Board Units (OBUs) and Roadside Units (RSUs). The anonymous key needs a minimum of storage to avoid losing the security level. The network architecture is composed of the trusted authority (TA), the immobile RSUs on the road side, and the mobile OBUs equipped on the moving vehicles. The protocol consists of four parts:

1. System initialization: TA invokes an algorithm to obtain the private key for an ID of RSU or OBU.
2. OBU short-time anonymous key generation: to tackle the revocation when the OBU requests a short-time anonymous key certificate, the RSU will check whether the OBU is on the newly updated revocation list (retrieved from the TA). If it is the most updated, the RSU will not take any action to update the certificate revocation list.
3. OBU safety message generation and sending: the request-response protocol between the OBU and the RSU can use an anonymous key generation for short-time.
4. OBU fast tracking algorithm: after requesting a short-time anonymous key pair, the OBU can send the safety message within the short-period it is valid.

The format of the safety messages in ECPP protocol is also defined. OBU cannot reveal their real identity with this protocol.

Calandriello et al. [88] propose vehicle On-Board Units with a set of pseudonyms (public keys certified by CA) and the corresponding private keys, without affecting the system security. The CA provides a certificate on the vehicle public key. The private and the public key of the vehicle as well as the certificate are attached to each message. Each pseudonym of a vehicle is used for a certain period.

Upon receiving a message, a vehicle with the public key of the CA validates the certificate with the Certificate Revocation List (CRL). Each vehicle is equipped with a secret group signing key which allows any vehicle to sign a message on behalf of the group without the vehicle’s identity. This mechanism reduces the security overhead for safety beaconing, and retains robustness for transportation safety, even in adverse network settings.

Zheng et al. [89] introduce a decentralized group-authentication protocol that the group is maintained by each roadside unit (RSU) rather than by a centralized authority. The vehicles in the group can anonymously broadcast Vehicle-to-Vehicle (V2V) messages, which can be instantly verified by the vehicles in the same group. The vehicles request a secret member key and verify messages from vehicles that have moved into the range of the same RSU. There is no overhead on the certificate management, due to the small number of active vehicles within a range of a single RSU. The privacy is assumed because an eavesdropper cannot verify that two different messages come from the same vehicle. V2V communication implies security requirements such as message authentication, privacy protection and anonymity revocability. The protocol assumes that RSUs are densely distributed in the road side.

Zhang et al. [90] propose a vehicular authentication protocol referred to as APPA to trust the vehicular communications and privacy of vehicles. This protocol is identity-based cryptography, aggregate signature and one time signature. If a vehicle obtained a secret key from a trusted authority (secret key is associated with the vehicle’s identity), it can sign messages. The signature on a message uses the vehicle’s identity (one-time pseudonym). One aggregated signature (n signatures on n messages by n signers) can be verified as if it had been generated by a single signer.
Liqun et al. [91] propose a solution for reliability, privacy and auditability features simultaneously in V2V communications. When it is manufactured, the vehicle is equipped with a black box that has a public key and can perform cryptographic operations secure. A k-time anonymous signature scheme can reveal a signer’s identity to if the signer signs the same message more than k time. Different protocols permit to signs a message anonymously, verify an anonymous signature, check if a message has been signed by a certain number of independent users, show whether two anonymous signatures on the same message are from the same signer.

Solutions proposed to ensure privacy, use pseudonyms on Vehicle and the certification authorities are responsible of the management of vehicle’s certificate: generation, distribution and revocation [92]. Also, many pseudonyms or public keys have to be pre-loaded in vehicles, creating overhead for practical applications.

Although privacy has been recognized as a serious problem by the Car-to-Car Communication Consortium [93] or the IEEE P1609.2 standard [94], the appropriate technologies and architectures still have to be developed in order to address users’ privacy problems.

10. Security solutions

Many solutions have been proposed in the literature to address the security problem of VANETs. This section presents some of these solutions and architectures for confidentiality, integrity, authentication, and availability (privacy in section IX). Some mechanisms propose a solution for one or more security requirements.

Raya et al. [64] provide a detailed threat analysis and security architecture. They present a set of security and privacy protection protocols and they analyze their robustness.

Having presented some security requirements and attacker profiles, the authors propose certain solutions.

Firstly, digital signatures are presented as a building block. In this section, the fact that safe messages must be authenticated in VANETs is emphasized and the preferred way of securing messages involves a digital signature.

Secondly, a way to secure messages is presented. Before a vehicle sends a safety message, it signs it with its private key and includes the Certification Authorities (CA). After presenting this way of securing messages, a tamper-proof device is proposed to physically secure confidential information such as private keys. This device could also sign outgoing messages.

Thirdly, a way to manage keys is proposed. In other words, the issues of cryptographic key distribution, certification and revocation are addressed. For this purpose, they identified two components related to cryptography: the electronic identity and the anonymous key pairs used for privacy issues. This key will be bootstrapped and rekeyed by the governmental transportation authority or the car manufacturer. The key must be authenticated by the certification authorities. It would be possible to revoke the key if compromising activities are observed. In order to ensure users’ privacy, the use of anonymous public keys is proposed by the authors. In order to establish an authenticated session, the use of symmetric cryptographic primitives is suggested and switching between different channels or even communication technologies is suggested to prevent DoS attacks. To prevent bogus information attacks, the authors propose that the data received from a given source be verified by correlating it with those received from other sources. Anonymity is ensured by a key changing algorithm that adapts to the vehicle speed and takes into account key correlation by the attacker.

In [36], Frank Karl et al. suggest Security-Requirements Engineering using Cluster Analysis (SECA), an approach that allows the analysis of a large set of applications by selecting typical representatives that cover the requirements of a whole cluster of applications and developing a security solution for that subset (Fig. 2). Hence, during the first step of their work, an application list that comprises as many use cases as possible is collected. During the second step, a preliminary analysis of application characteristics and security requirements for all the applications is performed. After the analysis, similar applications are grouped by using cluster analysis. Fourthly, they apply some attack use cases in a selected small subset of representative applications from each cluster before analyzing them in more detail. After this step, they are able to derive a set of required security mechanisms that could prevent this attack. Finally, they analyze the possibility of the found solution in other applications within each cluster.

In [43], Klaus et al. propose a security architecture for VANETs (SAV), which is presented in Fig. 3. The communication model of the architecture is based on the fact that there are two types of communication: passive messages such as beacon messages, which are sent periodically and active messages, which are sent when an event occurs and a warning must be sent to forewarn other vehicles.

The SAV consists of three layers.

1. The bottom layer which includes basic security elements. In this layer, the authors suggest the use of a centralized Public Key Infrastructure (PKI) with a Trusted Third Party (TPP) to ensure user privacy.

2. The Single hop-Security is the layer where one can see how the beacons are secured. The receiver of beacons has the ability to verify the integrity of the beacons as well as the capacity to identify the sender as a valid participant of the VANET. This is possible because each node must sign its messages digitally. The verification is effected by the use of a certification, CertS. If two vehicles would like to communicate, they verify the authenticity of the CertS to ensure that they are reliable before communication can begin.

3. The multi-hop layer includes all of the other applications and services used in VANETs. This layer is applicable for alarm signals, warning applications such as cooperative forward collision warnings, vehicle-based road condition warnings, etc., and value added services. Due to the importance of verifying the information sent by nodes that would like to communicate, the receiving node can use a spatial cloak to verify the position of the vehicle. Even if in this case there is no way to exchange certificates or keys for cryptography issues, the digital signature available in the second layer could be used to provide authentication, non-repudiation and integrity.

In [77], Dhurandher et al. present Vehicular Security by way of a Reputation and Plausibility Check Algorithm (VSRP). To deploy security in VANETs, their algorithm takes into consideration three types of events: traffic jams, accidents and brake application. The algorithm uses a reputation based system along with sensors, not
only to detect, but also to isolate the malicious nodes present in the network. It also handles the problems of data aggregation and data dropping.

This algorithm follows an event-oriented approach that includes three types of events: (1) single-hops, (2) multi-hops and, (3) malicious-intent. The protocol distinguishes among three types of message packets: (1) data packets, (2) the neighbor req packets for the neighbor’s requests, and (3) the neighbor_rep packet, for the neighbor’s responses. To keep such information, each node maintains five tables: the neighbor table, the trust table, the reqseen table, which is used to maintain information about the node which has sent a neighbor req packet, the data table used to maintain information about data packets and the temp table used temporarily to store information about the data packets collected by a node. The proposed algorithm used in the case of traffic jams and road accidents is divided into four phases: (1) neighbor discovery, (2) data dispatching, (3) decision making and, (4) trust updates and neighbor monitoring.

In [39], Golle et al. propose a general approach to assessing the validity of VANET data. In this approach, a node searches for possible explanations regarding the data it has collected, based on the fact that malicious nodes may be present. Explanations that are consistent with the VANET’s node model are assigned a score and the node accepts the data associated with the highest score. The techniques to grant and score explanations rely on two assumptions: (1) nodes have the ability to exchange information with one another, (2) a parsimony argument accurately reflects adversarial behavior in the VANET. To achieve their goal, they propose a general sensor-driven technique that allows nodes to detect incorrect information and identify the node(s) at the source of this erroneous information with high probabilities. The success of this approach is based on the fact that each node maintains the model of the VANET containing all the knowledge that the node has of the VANET. In the presence of inconsistent data, the node will try to discover the reason. This task is performed by using the adversarial parsimony which is a heuristic built by the authors to deal with inconsistent data. One of the attacks perpetrated in VANETs could be Sybil attacks where a node could use virtual identities to pretend that there are several physical nodes. The authors use the distinguishability capacity to allow honest nodes to detect the physical presence of a node. They consider the local distinguishability where the node could use its own means such as a camera, a radio signal or a physical sensor to confirm the physical presence of the node. For extended distinguishability, they assume the network density and authenticated communication. Therefore, nodes can rely on other nodes that are farther away if they can convince their neighbors through their physical presence. In this model, users’ privacy refers to the capacity held by all nodes to change their identity periodically and also by the fact that the data validation is decentralized.

Qianhong et al. [95] propose a security framework in V2V communications for trustworthiness, safety and privacy. The message-linkable group signature (MLGS) can detect Sybil attacks, by vehicle that can trust only a number of anonymous vehicle. This number can change according to the traffic. Public keys or license plates authenticate the message. A trusted authority has a revocability mechanism to detect an attacker.

11. Global security architecture

In the global security architecture (Fig. 4), a five-level system is proposed: material, authentication, trust, message and the cryptographic level, for all security aspects.

In authentication, message/data level and cryptographic levels, involve cryptographic functionalities.

At the material level, the security involves resources such as the On-Board Unit (OBU), the Global Positioning System (GPS) receivers, radars, Event Data Recorder (EDR), antennas, etc. The security of these devices could be built around the Trusted Platform Module (TPM) [96] specifications, which can be integrated into any device. A TPM is a piece of hardware that requires a software infrastructure that is able to protect and store data in shielded locations [63].

The authentication level takes into account all kinds of authentications. First of all, users’ authentication in the system is considered in order to avoid access to the system by unauthorized users who would then be able to communicate in spite of the fact that they do not belong to the network. Second, messages must be authenticated so that the receivers can verify if the message received was sent by the appropriate entities and ensure that it has not been modified while in transit [97]. The property authentication is also verified at this level. The property refers to the kind of transmission equipment used in the network [98]. This will help avoid fake nodes such as those created by someone standing on a bridge with a laptop sending messages which it pretends to come from a car. Finally, the location authentication must help to verify the sender’s position. Practically all of these authentications are not conducted simultaneously, but progressively during the transmission while the treated information is received. This means that
the packets could be rejected at any level of the communication process. At that point, the access control requirement of the system could be warranted.

The trust level is where a trust system [62], a plausibility check system [77] or a reputation system [99] must be implemented. The reputation system uses information such as speed, position, acceleration, etc. collected locally, as well as information from other users to build an opinion concerning a node with which it intends to communicate. Then, if the rate is positive, the communication will be possible. However, if the rate is negative, communication will not be accepted and the node will be ejected from the network. The plausibility check simply verifies the information considering the event and the trust system uses mechanisms such as the TPM to ensure that nodes are trustworthy. Moreover, this level must guarantee the non-repudiation requirement. A sufficient quantity of information related to the sender’s node must be collected in order to ascertain that some traces will remain and that the node will not be able to deny its identity as the author of a message.

The message/data level. At this level, the message itself must be secured. The method proposed in the literature is digital signature, with the existence of the vehicular PKI: each vehicle would possess a set of public/private key pairs used to sign safety broadcasted messages [100]. If a malicious node remained undetected at the authentication and the trust levels, the message being transmitted would be verified to ensure the safety of the information. This is the level where the integrity of the message should be guaranteed. The priority consists of ensuring that there is no anomaly in the message received.

The cryptographic level. This level concerns users’ privacy in the network. At this level, privacy solutions such as a private/public key or anonymous identity protocol should be applied to ensure that the users’ privacy is respected [101]. Therefore, information is scripted before being sent. The confidentiality of the information should be ensured at this step. Many solutions are proposed in the literature to ensure confidentiality [64,102].

This architecture could be divided into three sections: (1) the prevention section, which concerns the security material and the authentication level, (2) the detection and correction section which concerns the trust level and the message/data level and finally (3), the privacy section which concerns the cryptographic level. This global architecture is not intended to be a standard but a generic scheme that could be implemented considering the system or the application.

12. Conclusion

This paper is comprised of a comprehensive state-of-the-art review of VANET security, after presenting channel characteristics, challenges and addressing the attackers’ profiles. Then, threats, privacy and security solutions were introduced. In addition, the VANETs characteristics and related applications were presented. Some security issues such as security requirements, adversaries’ profiles and attacks in VANETs have been pointed out. Certain solutions and architectures suggested in the literature were highlighted.

References

[34] K.V.N. Kavitha, A. Bagubali, L. Shalini, V2V wireless communication protocol for rear-end collision avoidance on highways with stringent propagation


