Vehicular Communications 7 (2017) 7–20

Contents lists available at ScienceDirect

Vehicular Communications

www.elsevier.com/locate/vehcom

VANet security challenges and solutions: A survey

Hamssa Hasrouny [a,b,*], Abed Ellatif Samhat [b], Carole Bassil [c], Anis Laouiti [a]

[a] SAMOVAR, Telecom SudParis, CNRS, University Paris-Saclay, 9 rue Charles Fourier, 91011 Evry Cedex, France
[b] Lebanese University, Faculty of Engineering-CRSI, University Campus, Hadath, Lebanon
[c] Lebanese University, Faculty of Sciences II, University Campus, Fanar, Lebanon

ARTICLE INFO

Article history:
Received 16 September 2016
Received in revised form 28 November 2016
Accepted 20 January 2017
Available online 27 January 2017

Keywords:
VANET
Security challenges
Attacks classification
V2V communication
Security solutions

ABSTRACT

VANET is an emergent technology with promising future as well as great challenges especially in its security. In this paper, we focus on VANET security frameworks presented in three parts. The first presents an extensive overview of VANET security characteristics and challenges as well as requirements. These requirements should be taken into consideration to enable the implementation of secure VANET infrastructure with efficient communication between parties. We give the details of the recent security architectures and the well-known security standards protocols. The second focuses on a novel classification of the different attacks known in the VANET literature and their related solutions. The third is a comparison between some of these solutions based on well-known security criteria in VANET. Then we draw attention to different open issues and technical challenges related to VANET security, which can help researchers for future use.

1. Introduction

VANET aims to insure safe drive by improving the traffic flow and therefore significantly reducing the car accidents. The latter is solved by providing appropriate information to the driver or to the vehicle. Still, any alteration of this real-time information may lead to system failure impacting people safety on the road. To insure its smooth functioning, securing this information becomes a must and hence it is on the top outlook of security researchers.

VANET is a special class of mobile ad-hoc network with predefined routes (roads). It relies on specific authorities for registration and management, Roadside units (RSUs) and On-Board units (OBUs). RSUs are widespread on the road edges to fulfill specific services and OBUs are installed in the vehicles navigating in VANET. All vehicles are moving freely on road network and communicating with each other or with RSUs and specific authorities.

Using DSRC (Dedicated Short Range Communication) in a single or multi-hop, the communication mode is either V2V (Vehicle-to-Vehicle), V2I (Vehicle-to-Infrastructure) or hybrid.

In the coming years, most of the vehicles in VANET will be equipped with on-*board* wireless device (OBU), GPS (Global Positioning System), EDR (Event Data Recorder) and sensors (radar and ladar) as shown in Fig. 1. These equipments are used to sense traffic congestions and status. Then automatically take appropriate actions in vehicle and relay this information through V2V or V2I within the vehicular network.

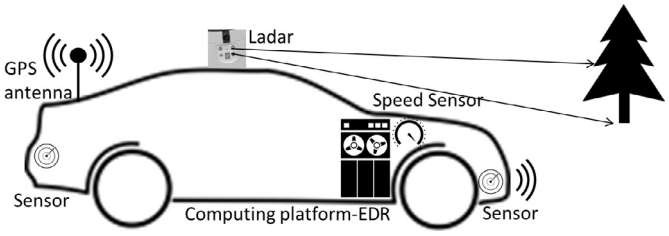

Fig. 1. Future vehicle design in VANET.

VANET users profit from many applications that are classified into active road safety, infotainment, traffic efficiency and management [1]; the latter stands for speed management and cooperative navigation.

The security is the state of being free from danger or threat. Security means safety, as well as the measures taken to be safe or protected. For example, in order to provide adequate security for the parade, town officials often hire extra guards.

In VANET, it is critical to guard against misuse activities and to well define the security architecture because it is a wireless communication which is harder to secure. The security and its guaranteed level of implementation affect people safety. Few years ago, many researchers have explored the security attacks and tried to find their related solutions. Others tried to define security in-

* Corresponding author.
E-mail addresses: hamssa.hasrouny@telecom-sudparis.eu (H. Hasrouny), samhat@ul.edu.lb (A.E. Samhat), cbassil@ul.edu.lb (C. Bassil), anis.laouiti@telecom-sudparis.eu (A. Laouiti).

http://dx.doi.org/10.1016/j.vehcom.2017.01.002
2214-2096/

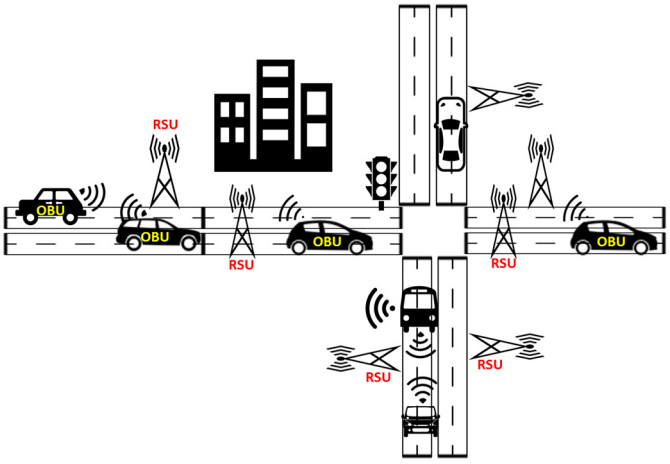

Fig. 2. VANET Network.

frastructures, or formalize standards and protocols. But still, the trend of trustworthiness of a node and misbehaving detection is large to explore.

This paper presents VANET security characteristics and investigates most of the VANET security challenges as well as the existing solutions in a comprehensive manner. After detailing the recent security architectures and the well-known security standards protocols, we present and discuss the recent frameworks that address the related issues. We focus on a novel classification of the different attacks known in the literature of VANET security and their solutions. Finally, despite all the promising opportunities that accompany VANET and after discussing the presented works, we have specified certain research challenges and open questions which may be future research directions. Thus enabling VANET to efficiently implement a system for trusting vehicles and protect it from malicious nodes.

The remainder of this paper is organized as follows: Section 2 expands VANET model and its security requirements. Section 3 details the attacker model. Section 4 presents the standardization efforts. Section 5 presents the solutions classified in a coherent manner. Section 6 expands the gap analysis. Section 7 highlights the emerging and open issues and we conclude in Section 8.

2. Vanet characteristics, security challenges and constraints

2.1. VANET characteristics

VANETs are ad hoc networks, highly dynamic, with little access to the network infrastructure and offering multiple services. The communication modes in VANET shown in Fig. 2 can be categorized into Vehicle to Vehicle (V2V), Vehicle to Infrastructure (V2I) and Hybrid. In V2V, the used communication media is characterized by short latency and high transmission rate. This architecture is used in different scenarios of broadcasting alerts (emergency braking, collision, deceleration, etc.) or in a cooperative driving. In V2I, vehicular network takes into account the applications that use the infrastructure points RSUs which multiply the services through internet portals in common. Hybrid mode is a combination of the two previous techniques. VANET characteristics explored in [1–6] can be grouped related to: i) Network topology and communication mode or ii) Vehicles and drivers.

i. *VANET Characteristics related to Network Topology and Communication Mode:*
   - *Unbounded and scalable network*: VANET can be implemented for one or several cities even for countries. Thus requires cooperation and management for security requirements.
   - *Wireless communication:* the nodes connection and their data exchange are done via wireless channels. Thus requires securer communication.
   - *High mobility and rapidly changing network topology:* nodes are moving at high/random speed which make harder to predict their position and the network topology. Thus enhancing node's privacy and causing *frequent disconnection, volatility and impossibility of handshake*. It lacks the relatively long life context (e.g., password) which is impractical for securing vehicular communication. Under these constraints, the alert dissemination delay should be respected. A good delay performance is needed either by using fast cryptographic algorithm or by entity authentication and message delivery on time. For this, a *prioritization of data packets* and *congestion control* is of higher significance; data related to traffic safety and efficiency should be faster than the others.
   - In addition to *reliability* and *cross layer* between transport and network layers are suggested to support real-time and multimedia applications.

ii. *VANET Characteristics related to Vehicles and Drivers:*
   - *High processing power and sufficient energy:* VANET nodes have no issue of energy and computation resources. They have their own power in the form of batteries and high computing powers to run complex cryptographic calculations.
   - *Better physical protection*: VANET nodes are physically better protected. It is more difficult to be compromised physically. Thus reduce the effect of infrastructure attacks.
   - *Known time and position*: most vehicles are equipped with GPS because many applications rely on position and geographical addressing or area. A tamper proof GPS is used for secure localization to protect nodes location against attackers.
   - *The majority of participants are honest:* the majority of drivers are assumed to be good and helpful to find the adversary.
   - *Existing law enforcement infrastructure:* Via the law enforcement officers, they can catch the adversary that attacked the system.
   - *Central registration with periodic maintenance and inspection*: vehicles are registered with central authority and have unique id (license plate). Vehicles periodic maintenance is for firmware and software updates. In PKC (Public key Cryptography), maintenance is for updating certificates, keys and obtaining fresh CRL (Certificate Revocation List).

Briefly, the vehicular network is an interaction between the behavior and cooperation of the drivers, the network, and the infrastructure. Probing a security solution must find a compromise to involve all parties within it. After presenting VANET characteristics, we will detail in the next section VANET security challenges and constraints.

2.2. VANET security challenges and constraints

In VANET, security must guarantee that the exchanged messages are not inserted or modified by attackers. As well, the liability of the drivers is essential to inform the traffic environment correctly within time constraint. Exclusive security challenges rise because of the distinctive characteristics of VANET. Mistreating these security challenges will lead to many constraints. We list below some of these security challenges:

- The *Network size*, the *geographical relevancy, the high mobility* and *dynamic topology*, the *short connection duration* and the *frequent disconnections* [1,2]: Network size can be geographically unbounded and very scalable, growing fast with no global authority to govern the standards for it.

– The *Trust* and *information verification:* trust is required as VANET ad hoc nature motivates the nodes to gather information from other vehicles and RSUs [7]. Hence this information exchange is frequent, it must be trusted and integrity verified. Trustworthiness of the data is more useful than trustworthiness of the nodes transmitting it [2].
– *Key distribution*: security mechanisms depend on keys, which make their distribution critical.
– The *Forwarding algorithms*: which is challenging concerning the number of transferred packets after finding the best route; is it unicast, broadcast, V2V, V2I or hybrid communication.

While for VANET constraints or requirements [1], we can list:

– *Congestion* and *collision control:* it is a must due to the unbounded network size.
– *Low Tolerance for Error* occurrence: some protocols are based on probability and any error can affect people life.
– *Environmental impact:* on magnetic waves due to obstacles [1] which prevent their propagation.
– *Risk analysis and management:* we can find sometimes solution for the attacks. But finding models for the attackers' behaviors are still missing.
– *Anonymity, privacy and liability:* nodes receiving data need to trust the sender. Privacy is ensured by anonymous vehicle identities. Sometimes even authenticated nodes can do malicious issues. Thus, a trade-off solution is needed between the anonymity, privacy and liability.

These security challenges and constraints can be minimized if we better handle the security services presented in the next section.

2.3. Security requirements (services)

The security services increase the security of processing and data exchange in VANET. The security requirements include:

- *Authentication*: ensures that the message is generated by a legitimate user using certificate. Or the receiver identifies the sender of a message via a pseudonym [8].
- *Availability:* by resisting to DoS (Denial of Service), we assure normal functioning. Because a delay in seconds makes the message meaningless [4].
- *Confidentiality:* involves a set of rules or a promise that limits access restrictions on certain resources. It is done using encryption or exchanging special message between OBUs and RSUs as some form of data verification [9].
- *Non-repudiation*: sender can't deny sending a message as he is already known from a good authority. They can retrieve attacker even after harm via Tamper Proof Device (TPD) [4].
- *Integrity:* no alteration for data. Digital signature is used for message and data integrity [3,10].
- *Privacy and anonymity*: hide the identity of the user against unauthorized nodes using temporary and anonymous keys. Thus affording the *Location privacy*, no one can track the trajectory of any node.
- *Data verification*: to eliminate false messaging. The verification of data consistency with similar messages is used for detecting data correctness, especially between neighboring vehicles.
- *Access control*: all nodes work according to rules and roles privileges [11].
- *Traceability and revocability*: Although a vehicle real identity should be hidden from others, still there should be a component with the ability to obtain vehicles' real identities to revoke them for future use.

Table 1
Classification of security requirements.

VANET communication mode	Security requirements
V2V, V2I	Availability Confidentiality Error detection Liability identification Authentication Non-repudiation Privacy and anonymity Flexibility and efficiency Location privacy Integrity Traceability Data verification
V2I	Revocability Access control
V2V	Data verification

- *Error detection*: for detecting malicious and erroneous transmission.
- *Liability identification*: accountability or user identification during communication. Messages can be used to identify users.
- *Flexibility and efficiency:* the flexibility in the security architecture and the system design is significant. Though it is essentially designed for traffic safety application that requires less time and bandwidth. This makes the channel efficiency crucial in its consequent low delay.

After defining and analyzing the security requirements, we classify them in Table 1 based on their needs in VANET communication mode, either for V2V, V2I or both. For each VANET communication mode, we define its prerequisites of security services.

3. Attacker model

The deployment of a security system for VANET is challenging. In fact, the highly dynamic nature with frequent disconnection, instantaneous arrivals and departures of vehicles, the usage of wireless channels to exchange emergency and safety messages, expose VANETs to various threats and attacks. In this section, we will classify the attacks, the attackers and analyze which VANET communication mode they affect.

3.1. Attacks

Many researchers in [2,3,5,7,9,10,23] investigated the attacks in VANETs. The classification of these attacks is useful because the nature of VANET brings vulnerabilities and constraints that require solutions. By dividing, we can better control.

Attacks can be categorized into four main groups: (1) those that pose a risk to wireless interface, (2) those that pose a threat to hardware and software, (3) those that pose a hazard to sensors input in vehicle and (4) those that pose a danger behind wireless access, which means in the infrastructure (CAs or vehicle manufacturer). The following sub-sections present the threats posed to each of the areas mentioned above.

1) *Threats to Wireless Interface*
   - *Identity and geographical position revealing* (*Location Tracking*): an attacker tries to get info of the driver and trace him. This exposes a certain node at risk. For example, a car rental company that wants to follow in an illegitimate manner its own vehicles. Users will be tracked and no privacy preserving.

- *DoS*: an attacker tries to make the resources and the services unavailable to the users in the network. It is either by jamming the physical channel or by "Sleep Deprivation".
  - *DDoS* (Distributed Denial of Service): it is a DoS from different locations.
- *Sybil Attack*: an attacker creates multiple vehicles on the road with same identity. It provides illusion to other vehicles by sending some wrong messages for the benefits of this attacker.
- *Malware:* an attacker sends spam messages in the network to consume the network bandwidth and increase the transmission latency. It is difficult to control this kind of attack, due to lack of necessary infrastructure and centralized administration. Attacker disseminates spam messages to a group of users. Those messages are of no concern to the users just like advertisement messages.
- *Spam*: an insider node transmits spam messages to increase transmission, latency and bandwidth consumption.
- *Man in the Middle Attack* (*MiM*): a malicious node listens to the communication established between two other vehicles. It pretends to be each one of them to reply to the other. It injects false information between them.
- *Brute force Attack:* is a trial-and-error method an attacker uses to obtain information such as a user password or personal identification number or to crack encrypted data, or to test network security.
- *Black Hole Attack*: a malicious node declares having the shortest path to get the data and then routes and redirects them. The malicious node is able to intercept the data packet or retain it. When the forged route is successfully established, it depends on the malicious node whether to drop or forward the packet to wherever he wants.

2) *Threats to Hardware and Software*
In addition to *DoS, Sybil attack, Malware and Spam, MiM, Brute force* mentioned above in sub-section (1), we can list:
- *Injection of erroneous messages* (*bogus info*): an attacker injects intentionally falsified info within the network. It directly affects the users' behavior on the road. It causes accidents or traffic redirection on the used route.
- *Message Suppression or alteration*: attacker drops packet from the network or changes message content. In addition to *Fabrication Attack* where new message is generated. Or *Replay Attack* by replaying old messages or *Spoofing and Forgery attacks* that consist of injection of high volume of false emergency warning messages for vehicles. Or *Broadcast tampering*: in which attacker injects false safety messages into the network to cause serious problems.
- *Usurpation of the identity of a node* (*Spoofing or Impersonation or Masquerade*): an attacker tries to impersonate another node. To receive his messages or to get privileges not granted to him. Doing malicious issues then declaring that the good one is the doer.
- *Tampering Hardware*: during yearly maintenance, in the vehicle manufacturer, some malicious employees try to tamper the hardware. Either to get or put special data.
- *Routing Attack*: an attacker exploits the vulnerability of the network layer, either by dropping the packet or disturbing the routing. It includes in addition to the *Black Hole Attack*:
  - *Wormhole attack*: Overhearing data; an attacker receives packets at a point targeted via a tunnel to another point. He replays it from there.
  - *Greyhole attack:* a malicious node misleads the network by agreeing to forward the packets. But sometimes, he drops them for a while and then switches to his normal behavior.
- *Cheating with position info* (*GPS spoofing*) *and tunneling attack*: hidden vehicles generate false positions that cause accidents. GPS doesn't work.
- *Timing attack*: Malicious vehicles add some timeslots to the received message, to create delay before forwarding it. Thus, neighboring vehicles receive it after they actually require, or after the moment when they should receive it.
- *Replay attack*: malicious or unauthorized users try to impersonate a legitimate user/RSU by using previously generated frames in new connections.

3) *Threats to Sensors input in vehicle*
In addition to *GPS spoofing* mentioned in sub-section (2), we present:
- *Illusion attack*: the adversary deceives purposefully the sensors on his car to produce wrong sensor readings. Therefore, incorrect traffic warning messages are broadcasted to neighbors.
- *Jamming attack*: the attacker interferes with the radio frequencies used by VANET nodes.

4) *Threats to Infrastructure*
In addition to *Spoofing*, *Impersonation* and *Tampering message and hardware* mentioned in sub-section (1) and (2), we identify:
- *Unauthorized access*: malicious entities try to access the network services without having the rights or privileges. This causes accidents, damage or spy confidential data.
- *Session Hijacking*: authentication is done at the beginning. After that, the hackers take control of the session between nodes.
- *Repudiation* (Loss of event traceability): denial of a node in a communication.

Table 2 shows the classification of the attacks and the VANET communication modes they hit (V2V, V2I or both). This classification helps to identify the predefined attacks on these entities (hardware or software, members or authorities) and on the VANET communication mode they affect. Thus preventing these attacks or trying to minimize their effects becomes easier as they are nominated and VANET becomes more secure.

3.2. Attackers

VANET attackers are one of the basic interest of the researchers in [2,3,9,24]. They got many canonical names listed below based on their actions and targets:

- *Selfish driver*: he can redirect the traffic.
- *Malicious attacker*: he has specific targets. He causes damages and harms via applications in VANET.
- *Pranksters*: attacker does things for his own fun; such as DoS or message alteration (hazard warning) to cause road traffic for example.
- *Greedy drivers*: they try to attack for their own benefit. For example: sending accident message may cause congestion on road. Or sending false messages for freeing up the road.
- *Snoops/eavesdropper*: attacker tries to collect information about other resources.
- *Industrial insiders*: while firmware update or key distribution, malicious employees do hardware tampering.

The attackers are classified into:

- *Insider vs. outsider*: insider represents authenticated user on the network vs. outsider one with limited capacity to attack.
- *Malicious vs. rational*: malicious presents any personal benefit vs. rational which has personal and predictable profit.

Table 2
Classification of Attacks based on four categories and VANET communication mode.

Attacks on	Attack name	Attack on VANET communication mode
Wireless interface	– Location Tracking – DoS, DDoS – Sybil – Malware and spam. – Tunnelling, Blackhole, Greyhole. – MiM – Brute force	V2V
Hardware and software	– DoS – Spoofing and forgery. – Cheating with position info (GPS spoofing). – Message suppression/ alteration/fabrication. – Replay – Masquerade – Malware and spam – MiM – Brute force	V2V, V2I
	– Sybil – Injection of erroneous messages (bogus info). – Tampering hardware – Routing, Blackhole, wormhole and Greyhole. – Timing.	V2V
Sensors input in vehicle	– Cheating with position info(GPS spoofing) – Illusion attack – Jamming attack	V2V
Infrastructure	– Session hijacking – DoS, DDoS – Unauthorized access – Tampering hardware – Repudiation – Spoofing, impersonation or masquerade	V2I and V2V

- *Active vs. passive*: active attacker generates signals or packets vs. passive one who only senses the network.
- *Local vs. extended*: local attacker works with limited scope even on several vehicles or base stations vs. extended attacker which broadens his scope by controlling several entities scattered across the network.

After detailing the classified attacks and attackers, we will detail in the next section the standardization and the recent projects efforts.

4. Standardization efforts

An *infrastructure* is an underlying foundation for a system. Security *architecture* is a security design. It addresses the necessities and potential risks involved in a certain environment and specifies when and where to apply security controls. *Standard* provides detailed requirements on how a policy must be implemented. In VANET, many groups [12–16] have investigated the security architectures and infrastructures. They generated either security standard protocols [17,21] or define security architecture [18]. Other projects Scoop@F [19], C-Roads [20] are currently investigating the security in the ITS(intelligent transport system).

In the following, we detail the most popular security infrastructure namely PKI (Public Key Infrastructure), the recent VANET security architectures and the well-known security standards protocols.

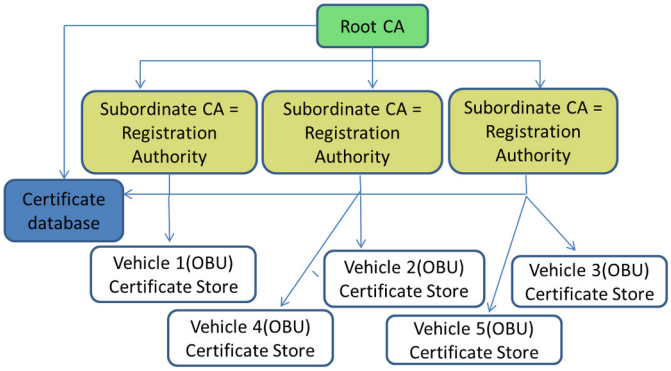

Fig. 3. PKI schema.

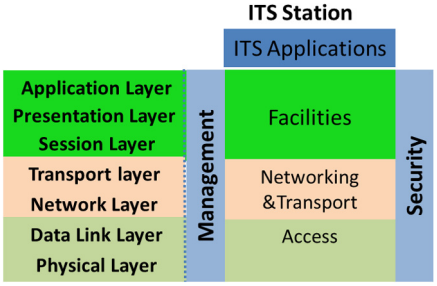

Fig. 4. Mapping OSI to ETSI architectural layers.

4.1. Security infrastructure: PKI

Exploring the VANET security infrastructures, PKI is the most used one. It is shown in Fig. 3. PKI supports the distribution and identification of public encryption keys. This enables users to securely exchange data over the network and verify the identity of the other party. PKI consists of hardware, software, policies and standards. All together manage the creation, administration, distribution and revocation of keys and digital certificates. PKI includes the following key elements:

- A trusted party, called a Root certificate authority (CA). It acts as the root of trust and provides services to authenticate the identity of entities.
- A registration authority, called a subordinate CA, certified by a root CA. It issues certificates for specific uses permitted by the root. It is used to protect the root CA. The users communication to the Root CA pass through the subordinate CA thus any attack can be detected before reaching the root CA.
- A certificate database, which stores certificate requests and issues/revokes certificates. It is accessible by the root and subordinate CAs.
- A certificate store, which resides on each vehicle to store issued certificates and private keys.

Briefly, the processes of distribution of encryption keys and certificates verification are done by the Root and Subordinate CAs. They identify the vehicles specific access within the vehicular network using specific hardware/software and wired/wireless communication.

4.2. Security architectures

Many groups in Europe and USA build their own security architectures based on PKI. In Europe (EU), ETSI in [18] define its security architecture for ITS (Intelligent Transport System). In USA, within the Vehicle Safety Communication Consortium (VSC),

Table 3
Security services in ETSI and NHTSA architectures.

Security service	Architectures
Authentication	NHTSA authenticates via digital signature and encryption. ETSI via signed messages.
Confidentiality	NHTSA and ETSI via symmetric and asymmetric encryption.
Integrity	NHTSA assures the integrity via Message Authentication Code. ETSI check the value of signed message.
Liability identification	NHTSA via Misbehavior Authority. ETSI via accountability and remote management.
Message security	NHTSA and ETSI use PKI. NHTSA use ECDSA.
Non-repudiation	ETSI and NHTSA have EDR for tracing.
Privacy	NHTSA uses an anonymizer proxy and privacy-preserving revocation via MA.

VSC-A (Vehicle Safety Communications-Applications), we consider the NHTSA (National Highway Traffic Safety Administration) [12] with its security architecture for VANET.

ETSI in [18] specifies security architecture for ITS communications. Based on the security services defined in [22], it identifies the functional entities and their relationships: EA (Enrollment Authority), AA (Authorization Authority) and ITS-S (Intelligent Transport System-Station). ITS-S security lifecycle begins in the manufacturer then enrolment, authorization and maintenance. ITS-S architecture is based upon four processing layers: Access Layer, Networking & Transport Layer, Facilities Layer and Applications Layer bounded by two vertical layers: Management and Security as shown in Fig. 4. EA validates (authenticates and grants) that an ITS-S is trusted to function in ITS communication. AA provides ITS-S proof to use specific services by issuing authorization ticket. CI (Canonical Identifier) is globally unique for an ITS-S facing the Enrolment credentials.

NHTSA proposed a security architecture [12] based on PKI. They detailed functional entities based on long term enrolment certificates for OBU (Bootstrap functions) and short term digital certificates (Pseudonym functions). Their basic issue is trust. The entities of the NHTSA architecture are shown in Fig. 5. Within their proposal, V2V communication consists of two types of messages: *BSM* (Basic Safety Message) and *security* information message. For *BSM*, the digital signature and certificate are used for verification purpose. For the communications between *vehicles* and *SCMS* (*Security certificate management System*), the asymmetric encryption ECIES (Elliptic Curve Integrated Encryption Scheme) is used for confidentiality and the digital signature ECDSA (Elliptic Curve Digital Signature Algorithm) is used to validate the device. For the *Communications inside the SCMS* (entity to entity), the symmetric encryption AES-CCM (Advanced Encryption Standard-Counter with CBC-MAC) is used for confidentiality with MAC (Message Authentication Code) for integrity and together they provide authenticity. This security architecture assures Privacy against insiders and outsiders; a single SCMS component cannot link any two certificates to the same device (no tracking) and no stored information within SCMS can link certificates to a particular vehicle or owner. MA (Misbehavior Authority) assures the continuation of the trusted nodes only, by producing/publishing CRL and misbehavior reports in VANET. LOP (Location Obscurer Proxy) acts as anonymizer proxy and shuffles misbehavior report sent by OBUs to MA. Efficient privacy-preserving revocation exists.

Table 3 presents the security services afforded within ETSI and NHTSA architecture. After presenting the security architectures, in the next section we will present the well-known security standards in VANET.

4.3. Security standards

For standardization, we consider the IEEE 1609.2 security standard and ETSI standards.

The IEEE 1609.2 security standard [16,19] presents methods to secure message formats, application messages, and messages processing used by WAVE (Wireless Access in Vehicular Environments) devices. All these security issues are based on PKI using keys and certificates management. The symmetric encryption AES-CCM, the asymmetric signature ECDSA, and the asymmetric encryption ECIES are used for the keys distribution and for the safety messages formats. The security requirements in this standard such as confidentiality, authenticity, non-repudiation and integrity are ensured but anonymity is limited and no mechanism is defined for multi-hop communication in V2V.

ETSI in [13,18,22] defined ITS security services and architecture and ITS-communications security management. We had discussed the security architecture of ETSI standard in section 4.2. Table 4 below summarizes the mapping between security services of ETSI and IEEE 1609.2 based on [22].

We conclude from Table 4, that some services in ETSI are still missing or under development in IEEE 1609.2. The accountability, remote management and report misbehaving are completely absent in IEEE 1609.2. While for plausibility check, IEEE 1069.2 doesn't check dynamic parameters. For replay protection, IEEE 1609.2 uses the timestamp but they do not use the sequence number. And finally for the security association management (session), IEEE 1609.2 check the security in any session on the fly, it checks the certificate and signature but does not establish and manage a security association between two ITS-S communicating together.

After describing the standardization efforts, we will move in the next section, to expand many proposed solutions for different attacks in VANET literature.

5. Proposed solutions from the literature to the previously described attacks

Many researchers worked on proposing solutions for the previously described attacks. We grouped these proposals based on the categorized attacks mentioned in section 3.1.

5.1. Attacks on wireless interface:

For Tracking, Eavesdropping and Traffic analysis attacks:

The privacy is one of the basic cures for these attacks. Many researchers investigated many techniques to maintain participants' privacy within VANET [53]: It can be ensured by a set of anonymous keys changing according to the driving speed or via pseudonyms that cannot be linked to the true identity of the user or the vehicle [25] or either via group signatures [12,27,26].

ETSI standard in [28] specifies the privacy management for a node based on anonymity, unobservability, pseudonyms, and unlinkability. The communication between nodes is done using the SA (Security Association) and key management. The authors in [3] propose to preload anonymous keys in TPD which are certified by CA and traced back to Electronic License Plate (ELP). [29] propose to keep node identity and location private. Thus using a decentralized group authentication with set of anonymous keys, pseudonyms, group signatures and ECPP (Efficient Conditional Privacy Preserving) protocol for anonymous authentication. In [30], the vehicles use many temporary certificates (pseudonyms) from their tamper proof device that cannot be linked with each other. [24] propose to use variables MAC (Media Access Control) and IP addresses to separate the addresses from the identities of vehicles and drivers [23]. [31] suggest VIPER (Vehicle-To-Infrastructure

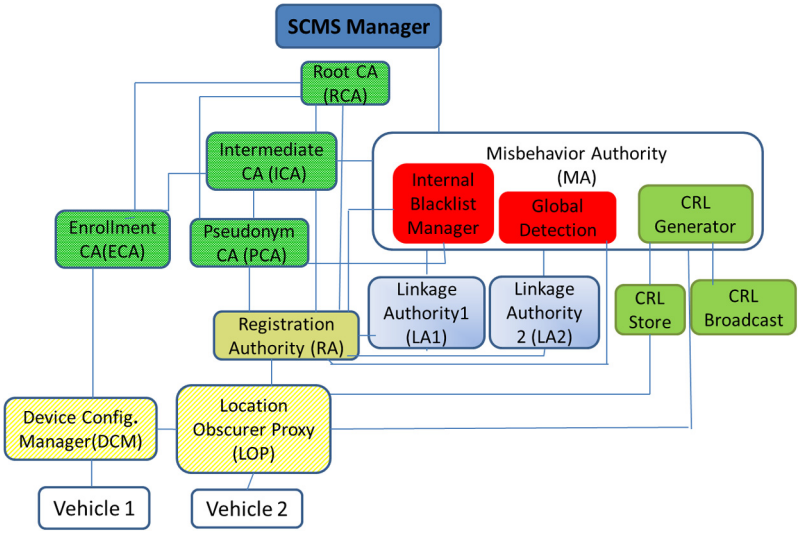

Fig. 5. NHTSA security system design.

Table 4
Mapping ETSI security services with IEEE 1609.2.

Security service group	ETSI security service at Rx/Tx	Mapping definition IEEE 1609.2
Enrolment	Obtain/Remove/Update Enrolment Credentials	Certificate Signing Request
Authorization	Obtain/Update Authorization Ticket Publish/Update authorization Status Add/Validate authorization credential to single message	Certificate Signing Request Certificate Revocation List(CRL) request/update Signed Messages and processing signed messages
Security association management (session)	Establish/Remove/Update Security Association	Not supported: support on the fly security associations by identifying the trust hierarchy and security service applied to the message in the body and content of the public key certificate.
Authentication	Authenticate ITS user/network	Signed messages.
Confidentiality	Encrypt/Decrypt message Send/Receive secured message using Security Association	Encrypted messages Not supported
Integrity	Insert/Validate check value	Signed messages.
Replay protection	Timestamp message Insert/Validate sequence number	Supported Not supported
Accountability Plausibility validation	Record incoming/outgoing message Validate data plausibility and dynamic Parameters	Not supported Basic support: rejected if geographic location far or expiry time too far in the past.
Remote management	Activate/Deactivate ITS transmission	Not supported
Report misbehaving	Report Misbehavior Report of ITS-S	Not supported

Communication Privacy Enforcement Protocol) for V2I communications.

For the group signature, it is used to sign message on behalf of the group, no revealing to the identity of the signer which prevents tracking and assure privacy [26]. Only the group manager can unlock the identity of the user and trace him via a secret trapdoor. In [12], V2V inside groups uses secret-key for their basics authentication. Groups or ring signatures enhance the privacy by saving communication in the most efficient way. In [27], a non-interactive authentication scheme is presented providing privacy among drivers assembled in groups for V2V communication networks; drivers may change their own set of public keys frequently without control from the third trusted party (TTP).

Also we can mitigate these attacks by encrypting the data. The authors in [2] propose an asymmetric cryptography via NMD (Non-Disclosure Method) routing protocol, [12] suggest the symmetric encryption for beacons to avoid being tracked. The security architecture for V2V and V2I communication adopted in [14,15,23] and [32] succeeded to protect privacy of the participants and were very efficient in terms of computing capabilities and communication bandwidth using the asymmetric and symmetric cryptography and tamper resistant hardware.

For Information Disclosure:

The authors in [2] propose SMT (Secure Message Transmission) and NMD routing protocol to solve this issue via MAC and asymmetric cryptography.

For DOS attack:

It can be lessened using the digital signature [24], specific authentication methods [33], routing protocols [1] or trustworthiness of a node [34]. Digital signature is used for secure and reliable message communication and authentication [35]. Digitally signing data acts as Proactive security for it [1], also customized hardware with non-public protocols let attackers take time to penetrate to the system. [36] suggest the usage of short life time private and public keys with a hash function. For the authentication, Tesla++ [33] is an authentication method used as effective alternative to

signatures. It uses symmetric crypto with delayed key disclosure. Secure and prevents memory based DoS attack. It reduces the memory requirement at the receiver end for authentication mechanism. For the routing protocol, [2] apply the SEAD (Secure and Efficient Ad-hoc Distance Vector) or ARIADNE routing protocol that use one way hash function and symmetric cryptography. Concerning the trustworthiness of a vehicle, [34] propose a trust model that calculates the trust metric values of nodes participating in VANET. One of its critical factors consists of limiting the number of accepted received messages from neighbors. Once exceeding a certain threshold (which is the case in DOS attack), using a fuzzy-based approach, a direct report is sent to MA to deactivate the attacker.

For Sybil attack:

Deploy a central Validation Authority (VA), which validates entities in real time directly or indirectly using temporary certificates [37]. Use PKI for key distribution and revocation [38]. Apply the registration, the ECDSA for signature and use timestamp per vehicle [8]. Ref. [39] proposes to use approved certification. In case of authentic and secure links with trusted nodes, [40] proposes validating unknown nodes with the method of secure location verification. Ref. [9] suggests the position verification by analyzing the signal strength and radio resource testing. Ref. [41] advocates strengthening the authentication mechanism by the use of distance bounding protocols based on cryptographic techniques. In [9] RobSAD (Robust Sybil Attack Detection) for abnormal/normal trajectory, with higher detection rate and lower system requirements. It can detect attacks independently by comparing digital signatures for the same motion trajectories. Ref. [42] proposes many privacy-preserving schemas with VANET architecture generating certificates/pseudonyms and monitoring vehicles then reporting to CA. Ref. [43] proposes to use on-board radar (virtual eye). Vehicle can see surrounding vehicles and receive reports of their GPS coordinates. By comparing, they can detect the real position and the malicious vehicles. In [3], Location is used to prevent Sybil attacks by checking its logical place. A vehicle receives message, examines certificate, its lifetime and location. If it is correct and in logical location, it accepts the message else it reports to the nearest CA. They also use TCRL (Timely geographical CRL) that contains fresh revoked CRLs of a specific area. Finally, [44] compared different Sybil attacks solutions.

For Malware and Spamming:

Digital signature of software and sensors is a must. Using trusted hardware make impossible to change existing protocols and values, except by authorized nodes [41].

For Man in the middle attack:

Use strong authentication methods such as digital certificates and confidential communication with key or powerful cryptography [9]. Include several authentication schemes mentioned in [45] where anonymity, pseudonyms, trust and privacy are ensured via short-lived keys changing frequently and RSU used for authentication and key distribution. In [36], a decentralized lightweight authentication scheme for V2V is given to protect valid users in VANETs from malicious attacks based on the concept of transitive trust relationships. Ref. [46] proposes an authentication via MM (Membership Manager) which can detect misbehaving nodes via RSUs that trace vehicles. In [47], an efficient cooperative message authentication permits vehicle users to cooperatively authenticate a bunch of message-signature pairs without trusted agent using Public Key Cryptography (PKC) and Secret key Cryptography (SKC).

For Brute force attack:

Use strong encryption and key generation algorithms unbreakable within a reasonable running time [49]. Then unauthorized access is prohibited.

5.2. Attacks on hardware and software

For Message tampering:

Use similarity algorithm [50], data correlation [26] and challenge response authentication method [33] to prove the reliability of the messages. Ref. [50] proposes a trust and reputation management framework based on similarity algorithm and trust of messages content between vehicles to help driver to believe or not a received message. By calculating the trust value if it surpasses a threshold they take appropriate action and rebroadcast the message. Otherwise they drop it.

In [26], a novel group signature based on a security framework assures authenticity, integrity, anonymity, accountability, access control approach and probabilistic signature verification scheme is used to detect the tampered messages for unauthorized node. Based on tamper resistance device, it correlates data from vehicles and cross-validates it via a set of rules. The security layer of this framework is composed of: capability check, signature generation, firewall, signature verification, authorization check, anomaly check.

In [33] a challenge-Response authentication method is proposed; a combination of digital signature and challenge response authentication. It is used to minimize the false message. A receiver getting any message sends a challenge to the sender. By replying, it transmits its location and timestamp to prove its authenticity. Location can tell us if the vehicle was at vicinity of an accident, which increases the reliability of the safety message.

For Spoofing and Forgery attacks:

Use vehicular PKI (VPKI) for authentication between vehicles [51], or sign warning messages [52], or establish group communications [54], or include a non-cryptographic checksum per message sent and apply plausibility checks on incoming one [25]. Or even use cryptographic certificate via routing protocol ARAN (Authenticated Routing for Ad-hoc network) [1] or use on-board radar (virtual eye) [43], then vehicle can detect the real position and the malicious vehicles.

For VPKI, it is a set of trusted third parties, one CA in each country, with delegated CA in regions, CAs mutually recognize vehicles in different areas. Each vehicle has their own private and public keys and short lifetime of certificates with anonymous keys changing according to the driver speed [51]. Only legal authorities can correlate between Electronic License Plate of a vehicle and its pseudonyms. So a disseminated signed message with certificate attached is authenticated via CA. Thus the communication between authenticated users is only established in a secure manner.

Use ECDSA for digital signature [47], it provides secure and fast dissemination of info; after validating the public key then authenticating the private key of a user signing a message.

For the group communication [54], keys can be managed by a group key management system. An intruder could not be able to communicate with the group. Drivers are organized into groups with shared public key between members [55], in case of a malicious behavior, the identity of the signer can be revealed only by the TTP. In [35], they use SECA (Security Engineering Cluster Analysis) for securing the group. For beacons security, they use certificate and digital signature while for multi-hop security, the geographical position is used.

For Message Saturation:

Ref. [25] proposes to limit the message traffic to V2I/I2V, implement station registration so only registered vehicles accept and process messages received from ITS infrastructure in its radio range, reduce the frequency of beaconing and add source identification (equivalent to IP address) in V2V messages. While the authors in [23,56] try to limit the flooding of the signed messages, built on location based grouping and aggregation signature.

Table 5
Attacks, compromised services and solutions.

Attacks	Compromised services	Solutions
Tracking	Privacy	[2,3,12,24–32]
Traffic analysis Eavesdropping	Confidentiality	[2,12,14,15,23,32]
Information disclosure	Authentication Privacy	[2]
DOS	Authentication Availability	[1,2,24,33–36]
Sybil attack	Authentication Availability	[3,8,9,37–44]
Malware	Availability	[41,41]
Spamming	Confidentiality	
Man in the middle attack	Authentication Confidentiality Integrity Non-repudiation	[9,36,45–47]
Brute force	Authentication Confidentiality	[49,48,49]
Tampering Hardware	Confidentiality Privacy	Control of manufacturer users' job.
Message tampering/ suppression/ fabrication/alteration	Authentication Availability Integrity Non-repudiation	[26,33,50]
Message saturation (Spoofing and forgery attacks)	Authentication Availability Integrity	[1,25,35,43,47,51,52,55,54,23]
Broadcast tampering	Availability Integrity	Cryptographic primitives are enabled with non-repudiation mechanism.
Node impersonation	Authentication Integrity Non-repudiation	[2,37,39,41]
Masquerading	Authentication Non-repudiation Integrity	[25,47]
Routing: Blackhole, Greyhole, Wormhole, Tunnelling	Authentication Availability Confidentiality Integrity	[2,9,48]
GPS spoofing/Position faking	Authentication Privacy	[25,35,58]
Timing attack	Availability	[9,24,36]
Replay	Authentication Integrity Non-repudiation	[2,25,43]
Illusion attack	Authentication Integrity	[25,35,58]
Jamming	Availability	[35,57]
Key and/or certificate replication (unauthorized access)	Authentication Confidentiality	[3,24,30,33,38,39]
Loss of event traceability (Repudiation)	Non-repudiation	[9,41,33]

For Replay attack:

Use time stamping technique for sensitive packets [43] or timestamp all messages by broadcasting time (UTC or GNSS), or digitally sign and include sequence number in each message [25]. Beside cryptographic certificate or symmetric cryptography and MAC via ARAN and ARIADNE routing protocol [2].

For Node Impersonation:

Use variables MAC and IP addresses for V2V and V2I communications [39]. Or Authenticate via digital certificates [37]. Ref. [41] proposes to strengthen the authentication mechanism using the distance bounding protocols based on cryptographic techniques. Or use cryptographic certificate via ARAN routing protocol as mentioned in [2].

For surpassing *Masquerading*:

[25] propose to include an authoritative identity in each message and authenticate it, or as suggested in [47], use the digital signature and sequence number.

For resisting against *Routing* attacks (*Blackhole, Greyhole, Wormhole and Tunnelling*):

Digital signature of software and sensors are used. In ARAN, ARIADNE and SEAD routing protocol [2] cryptographic certificate, symmetric cryptography, MAC (Message Authentication Code) and one way hash function are used respectively to solve these issues. In [9], HEAP an efficient technique is proposed to defend against Wormhole attack in the network. It is based on AODV protocol. It use geographical leash to limit the travelled distance from source to destination, if the threshold is surpassed then the packet is dropped. They propose also the TIK (TESLA with instant key disclosure) authentication protocol. [48] presents various mechanisms to improve different ad-hoc routing protocols for secure routing process by enhancing the trust among different nodes in VANETs.

For Timing attack:

Time stamping mechanism is used for packets of delay-sensitive applications in a trusted platform with strong cryptographic modules [9,24,36].

5.3. Attacks on Sensors input in vehicle

For Jamming attack:

The authors in [57] propose to switch the transmission channel or use the frequency hopping technique. While [35] suggest to switch either between different wireless technologies.

For GPS Spoofing or Faking Position or Illusion attack:

Use signature with positioning system to accept only authentic location data [58]. Or implement differential monitoring to identify unusual changes in position [25]. Or calculate a reputation score for safety application [35] by analyzing and filtering received queries to detect malicious and incorrect position. Hence potential adversaries are detected and ejected from VANET.

5.4. Attacks on Infrastructure

For *Key and/or certificate replication* that cause *Unauthorized Access*:

Use certified and disposable keys, or check the validity of the digital certificates in real time via CRL [24], or use the revocation protocols instead of CRL [3]. Use the cross certification between different CAs involved in VANETs security scheme [39]. Or adopt a hierarchical distributed CAs with trust going through a long chain [30].

A "Freshness" concept in [38] provides a constant verification time independent of the number of revoked certificates, thus no need for PKI to distribute the CRL and OBUs to maintain them. This reduces the storage requirement at OBUs.

Ref. [33] proposes to revoke the certificate either when cryptographic keys are compromised or when a fraudulent user issues signed certificates to transmit fake info. The certificate consists of a public key, certificate lifetime, signature of CA and CRL appended.

Some of the suitable revocation protocols are mentioned in [3]: RTPD (Revocation Tamper Proof Device), if activated in any vehicle prohibit it of sending messages, and DRP (Distributed Revocation Protocol) which allows vehicles to communicate and accuse others that misbehave and when possible report to CA. Then their TPD will no longer able to sign messages.

For Loss of event traceability (Repudiation):

The authors in [41] recommend using trusted hardware for which it is impossible to change the existing protocols and values except by authorized ones. As per [33], reading and updating

from sensors must be authenticated and verified e.g. by a challenge/response mechanism. While [9] propose the PVN (Plausibly Validation Network) to collect raw data from sensors and antenna to check if plausible or not.

Finally, ETSI in [13] proposes for attacks countermeasures to use the audit log, the remote activation and deactivation of nodes.

In Table 5, we present the previously described attacks, their related compromised services and their proposed solutions.

6. GAP analysis between different solutions

When performing a gap analysis in VANET, the aim is to identify gaps of missing/necessary needs in relation to what outcomes are desired. One must compare what has been done in the area, and compare this to the ambitions of what to aim for. There will probably be a gap in-between, which in that case must be identified. When this identifying process is completed the analysis hopefully proposes a solution of how to fill the gap.

Researchers in VANET tried to bypass the scalability problems and save the communication in the most efficient manner. They attain to reduce the delay in propagation. They worked on authentication, data delivery and try to propose how to trust messages between vehicles. They tried to find balance between the need to preserve user privacy and the traceability requirement for law enforcement authorities. They used cryptographic approaches based on PKI to distribute symmetric or asymmetric keys for message encryption, and certificates for authentication. They trust group formation based on symmetric and asymmetric cryptographic schemes in order to speed the processing and strengthen the security and the privacy. They encrypt data to prevent tracking. They use digital signature and trust model at the receiver end, to prevent DoS. They validate data in real time, by analyzing signal strength or buying virtual eye to detect Sybil attack. They use the digital signature or transitive relationship for malware and spamming detection. They suggest strong encryption and key generation algorithms unbreakable within a reasonable running time to resist to brute force attack. They propose similarity algorithm to check and detect tampering by calculating trust value surpassing a certain threshold. They adopt the group communication to limit the unauthorized access. They reduce the frequency of sending to limit the message saturation. They use special routing protocol and digital signature to prevent replay attack. They suggest switching between different wireless technologies to prevent jamming the channel. They use certified and disposable keys, and check the validity of the digital certificates in real time via CRL, or use instead the revocation protocols. For unauthorized access, they revoke the certificate when cryptographic keys are compromised. They use the reporting to specific authority and the remote activation and deactivation of nodes. They propose for attacks countermeasures to use the audit log.

Briefly, most of them agreed on using PKI, digital signature and certificates with cryptographic techniques and group formation to maintain the basic security issues in VANET. But each of the proposed solution is a wide field to explore and future work is required to test and prove the best that can fit.

Table 6 below shows a comparison between the solutions based on predefined criteria that tackle deeply the VANET security such as Centralized or decentralized, Privacy is preserved or not, Certification Authority/RSU is used or not, Support of routing protocol, Support of Cryptographic algorithm, Support of Group Formation, Reporting to specific authority, Remote activation or deactivation, Data verification, Detection Rate. This comparison is between some selected solutions and their attacks. Those attacks and their solutions are expanded in section 5. One can benefit from this table to find a compromised solution among these different services. After presenting and analyzing the different solutions in VANET security, many emerging and open issues are raised. We will expand them within the next section.

7. Emerging and open issues

Based on the security approaches presented in section 5, the researchers in VANET tried to bypass many constraints or vulnerabilities attacking the vehicular network. Although, many issues still open. We highlight below some of them which may become new research areas in the future:

1) *The trustworthiness evaluation of nodes participating in VANET and their misbehavior detection*:
   i. Evaluating the trustworthiness of a vehicle in VANET is an open problem. We mentioned above that any defection in the communication and/or messages endangered people's lives. So what are the criteria that would define if a node is trusty or not? Is it reliable to count on it for disseminating critical messages?
   ii. Based on these criteria we can detect the misbehavior either in vehicle or in the backend. Once the misbehavior detected, what are the appropriate actions to take? Punishment factors are not clearly defined also encouragement ones. Both factors can be incentives as they can limit the danger of malicious nodes.
2) *The revocation process and the certificate revocation list management and distribution*: once the misbehavior is detected how would be the revocation process? CRL-based solutions still under development. Using the short lifetime certificates in CRL and certificates change strategies are not defined yet and still vulnerability under no infrastructure for CRL. Certificate verification and revocation is longer in case of chain certificate authorities so what are the alternatives?
3) *The ability of the network to self-organize via a high mobile network environment:* the Group formation is a trend but how to deliver across partitions in VANET still not well-defined yet. In the group formation, the group leader is the center server for all nodes joining this group. The key management and basic communication pass through him. What happens if this GL decides to leave the group? Should be a backup group leader? What about the Key management when the GL leaves the group? It is not well clear. What happens if the GL leaves the group or a radio link cuts? Is the solution by trying to integrate different wireless technologies within VANET and switch between them in case of any problem occurrence?
4) *Data context trust and verification:* VANET aims to insure safe and cooperative drive. This happens by providing the appropriate information to the driver or vehicle. So it is very important to check and verify the exchanged information in VANET. For Data-centric trust and verification, the tamper-resistance hardware used in a vehicle to detect unnecessary accident warnings, needs to be further researched. For the context verification, a vehicle must be capable to act as an intrusion detection system by comparing received information about status and environment with its own available information. In addition, the reactive security concept needs to be enhanced.
5) *Cryptographic approaches for security, privacy and non-traceability assurance:* starting with the key distribution, it is exclusive to whom, the vehicle manufacturer or the government? For the key size, there are not a proposed key size, authentication delays and specific protocols. How to deal with keys of short duration? How to remove keys? It may cause overhead. Method of switching certificates periodically for privacy assurance is not defined yet. Also for non-traceability and privacy, more efficient method for partial pseudonym distribution and butterfly keys and linkage values are not employed yet. In ad-

Table 6
Brief summary of some solutions for different attacks.

Solution	Attack	Centralized/ decentralized	Privacy preserved of a node or not	Certification authority/RSU used or not	Support of routing protocol	Support of cryptographic algorithm	Support of group formation	Reporting to specific authority	Remote activation/ deactivation	Data verification	Detection rate
[28]	Tracking	centralized	yes	yes	no	yes	no	yes	yes	no	good
[29]	Tracking	decentralized	Yes, keep node identity and location private.	yes	no	Yes, using various anonymous keys using ECCP	yes	no	no	no	-
[31]	Tracking	decentralized	Yes, using VIPER protocol	yes	no	yes	yes	Yes, to RSU	no	no	Good, with limitation as number of vehicles increase
[27]	Tracking	decentralized	yes	yes	no	yes	yes	no	no	no	
[2]	DoS	decentralized	yes	yes	Yes, apply SEAD or ARIADNE protocol	yes	no	no	no	no	good, but availability remains major issue to solve
[34]	DoS	decentralized	yes	yes	no	yes	Yes	Yes to Misbehavior authority	yes	no	good
[3]	Sybil	decentralized	no	yes	no	yes	no	Yes to CA	Use geographic TCRL	–	good
[42]	Sybil	decentralized	yes	yes	no	yes	yes	Yes to CA	Using CRL	–	good
[50]	Message Temparing	decentralized	yes	yes	Yes, OLSR	yes	yes	Yes to neighboring	–	Yes, using similarity algorithm	good
[26]	Message Temparing	decentralized	yes	yes	no	yes	yes	no	–	Yes, based on probabilistic signature, it detects the tampered messages	Good, limited to the optimal key distribution method
[45]	Man in the middle	decentralized	Yes using short-lived keys changing frequently	Yes, RSU for authentica-tion and key distribution	no	yes	yes	yes	–	–	good
[47]	Man in the middle	decentralized	yes	yes	no	Yes using PKC	no	no	–	–	effective

(*continued on next page*)

Table 6 (*continued*)

Solution	Attack	Centralized/ decentralized	Privacy preserved of a node or not	Certification authority/RSU used or not	Support of routing protocol	Support of cryptographic algorithm	Support of group formation	Reporting to specific authority	Remote activation/ deactivation	Data verification	Detection rate
[54]	Spoofing	decentralized	yes	yes	no	Yes, using group key management system	yes	Yes, TTP	Yes, append to the CRL.	no	–
[51]	Spoofing	centralized	Yes, using anonymous keys changing according to driver speed	Yes, CAs in region and each country	no	yes	no	To CA	Using CRL	no	good
[25]	Replay	centralized	yes	yes	no	yes	no	yes	yes	Yes using sequence number	good
[2]	Replay	decentralized	yes	yes	Yes, apply ARAN or ARIADNE protocol	yes	no	no	no	no	good
[2]	Routing	decentralized	yes	yes	Yes, apply ARAN, SEAD or ARIADNE protocol	yes	no	no	no	–	good
[9]	Routing	decentralized	yes	yes	Based on AODV protocol	no	no	no	no	Limit travelled distance, if threshold surpassed, packet is dropped	–
[33]	Unauthorized access	centralized	Yes, location privacy	yes	no	yes	no	no	Broadcast CRL	yes	–
[3]	Unauthorized access	decentralized	yes	yes	no	yes	no	Yes, CA	Broadcast CRL	–	Into limits

Table 7
Open issues in VANET, communication modes and corresponding categories.

Open issue	Communication mode	Corresponding categories
Trustworthiness evaluation of nodes and misbehavior detection	V2V, V2I	Wi-H&S-Si-I
Revocation process and certificate revocation list management and distribution	V2V, V2I	Wi-H&S-I
Ability of the network to self-organize via a high mobile network environment:	V2V	H&S-I
Data context trust and verification	V2V, V2I	Wi-H&S-Si
Cryptographic approaches for security, privacy and non-traceability assurance	V2I	H&S-I
Anti-malware and Intrusion Detection System	V2I	Wi-H&S-I

dition to, using mobile IP or changing IP or MAC address by vehicles for preventing traceability is still under study.

6) *Anti-malware and Intrusion Detection System*: Embedded anti-malware frameworks are still problematic issues in VANETs. It is a must to develop an intrusion detection mechanism to enhance network security.

In Table 7, we categorize the open issues mentioned above based on which communication mode they hit (V2V, V2I or both) and which of the following categories they concern: (1) Wireless interface (Wi), (2) Hardware and Software (H&S), (3) Sensors input in vehicle (Si), (4) Infrastructure (I) (*CA or vehicle manufacturer*).

All these issues push to find a Trade-off between security and efficiency from one side, and anonymity/trust/privacy from the other side. Especially anonymity and adaptive privacy, where users are allowed to select their privacy level based on their own trust calculation over the others.

8. Conclusion

Users want safety and security much more on the road as many people life end there, due to misbehaving and maliciously of others. Overcoming these problems requires more efforts in the future to reach a secure VANET environment. This paper presented an extensive overview of the most of VANET security challenges and their causes as well as the existing solutions in a comprehensive manner. We give the details of the recent security architectures and the well-known security standards and protocols. We focused on the classification of the different attacks known in the literature and their solutions. Finally, we have specified certain research challenges and open questions which may be future research directions. Thus enable VANET to efficiently implement a system for trusting vehicles and protect it from any malicious node.

References

[1] G. Karagiannis, O. Altintas, E. Ekici, G. Heijenk, B. Jarupan, K. Lin, T. Weil, Vehicular networking: a survey and tutorial on requirements, architectures, challenges, standards and solutions, IEEE Commun. Surv. Tutor. 13 (4) (July 2011) 584–616.

[2] R.S. Raw, M. Kumar, N. Singh, Security challenges, issues and their solutions for VANET, Int. J. Netw. Secur. Appl. 5 (5) (September 2013).

[3] Gh. Samara, W.A.H. Al-Salihy, R. Sures, Security analysis of vehicular ad hoc networks (VANET), in: Second International Conference on Network Applications Protocols and Services (NETAPPS), IEEE, 2010, pp. 55–60.

[4] M.N. Mejri, J. Ben-Othman, M. Hamdi, Survey on VANET security challenges and possible cryptographic solutions, Veh. Commun. 1 (2014) 53–66, contents available at ScienceDirect, www.elsevier.com/locate/vehcom.

[5] N.K. Chauley, Security analysis of vehicular ad hoc networks (VANETs): a comprehensive study, Int. J. Netw. Secur. Appl. 10 (5) (2016) 261–274.

[6] B. Mokhtar, M. Azab, Survey on security issues in vehicular ad hoc networks, Alex. Eng. J. 54 (2015) 115–1126, available at www.elsevier.com/locate/aej.

[7] K. Lim, D. Manivannan, An efficient protocol for authenticated and secure message delivery in vehicular ad hoc networks, Veh. Commun. 4 (2016) 30–37.

[8] R. van der Heijden, Security architectures in V2V and V2I communication, in: 13th Twenty Student Conference on IT June 21st, Enschede, The Netherlands, 2010.

[9] V. La Hoa, A. Cavalli, Security attacks and solutions in vehicular ad hoc networks: a survey, Int. J. Netw. Syst. 4 (2) (April 2014).

[10] A.Y. Dak, S. Yahya, M. Kassim, A literature survey on security challenges in VANETs, Int. J. Comput. Theory Eng. 4 (6) (December 2012).

[11] R.K. Sakib, Security issues in vanet, in: Department of Electronics and Communication Engineering, BRAC University, Dhaka, Bangladesh, 2010.

[12] W. Whyte, A. Weimerskirch, V. Kumar, T. Hehn, A security credential management system for V2V communications, in: IEEE Vehicular Networking Conference, 2013.

[13] ETSI TS 102 731 V1.1.1-ITS-Security services and architectures.

[14] K. Plößl, H. Federrath, A privacy aware and efficient security infrastructure for vehicular ad hoc networks, Comput. Stand. Interfaces 30 (6) (2008) 390–397.

[15] M. Abuelela, S. Olariu, Kh. Ibrahim, A secure and privacy aware data dissemination for the notification of traffic incidents, in: Proceedings of the IEEE Vehicular Technology Conference, Spring, Barcelona, April 2009.

[16] H. Hasrouny, C. Bassil, A.E. Samhat, A. Laouiti, Group-based authentication in V2V communications, in: DICTAP, Fifth International Conference, IEEE, 2015, pp. 173–177.

[17] IEEE Trial-Use Standard for Wireless Access in Vehicular Environments: IEEE Std 1609.2™-2012.

[18] ETSI TS 102 940 V1.1.1-ITS – Communications security architecture and security management.

[19] https://ec.europa.eu/inea/en/connecting-europe-facility/cef-transport/projects-by-country/multi-country/2014-eu-ta-0669-s.

[20] https://www.sbdautomotive.com/en/intelligence-news.

[21] IEEE Trial-Use Standard for Wireless Access in Vehicular Environments: IEEE Std 1609.2™-2006.

[22] ETSI TS 102 867 V1.1.1- Security-Mapping for IEEE 1609.2.

[23] M. Raya, A. Aziz, J.P. Hubaux, Efficient secure aggregation in VANETs, in: Proceedings of the 3rd International Workshop on Vehicular Ad Hoc Networks, VANET '06, 2006, pp. 67–75.

[24] M. Raya, J.P. Hubaux, The security of vehicular ad hoc networks, in: Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks, SASN'05, November 7, Alexandria, Virginia, USA, 2005, pp. 11–21.

[25] ETSI TR 102 893 V1.1.1- ITS- Security- Threat, Vulnerability and Risk Analysis.

[26] J. Guo, J.P. Baugh, Sh. Wang, A group signature based secure and privacy-preserving vehicular communication framework, in: CD-ROM Proceedings of the Mobile Networking for Vehicular Environments (MOVE) Workshop in Conjunction with IEEE INFOCOM, Alaska, May 2007.

[27] F.M. Salem, M.H. Ibrahim, I. Ibrahim, Non-interactive authentication scheme providing privacy among drivers in vehicle-to-vehicle networks, in: Sixth International Conference on Networking and Services, 2010.

[28] ETSI TS 102 941 V1.1.1- ITS, Security- Trust and Privacy Management.

[29] R.G. Engoulou, M. Bellaïche, S. Pierre, A. Quintero, VANET security surveys, Comput. Commun. 44 (2014) 1–13, journal homepage: www.elsevier.com/locate/comcom.

[30] B. Aslam, C.C. Zou, Distributed certificate architecture for VANETs, in: Military Communications Conference, IEEE, 2009, pp. 1–7.

[31] A. Rawat, S. Sharma, R. Sushil, VANET: security attacks and its possible solutions, J. Inf. Oper. Manag. 3 (1) (2012) 301–304.

[32] G. Calandriello, P. Papadimitratos, J.P. Hubaux, A. Lioy, Efficient and robust pseudonymous authentication in VANET, in: Proceedings of the Fourth ACM International Workshop on Vehicular Ad Hoc Networks, VANET '07, 2007, pp. 19–28.

[33] A. Dahiya, V. Sharma, A Survey on Securing User Authentication in Vehicular Ad Hoc Networks, 2009.

[34] H. Hasrouny, C. Bassil, A. Samhat, A. Laouiti, Security risk analysis of a trust model for secure group leader-based communication in VANET, in: Second International Workshop on Vehicular Adhoc Networks for Smart Cities, IWVSC', 2016.

[35] R. Engoulou, Securisation des vanets par reputation des nœuds, Thesis Report, Ecole Polytechnique de Montreal, 2013.

[36] M.Ch. Chuang, J.F. Lee, TEAM: trust-extended authentication mechanism for vehicular ad hoc networks, IEEE Syst. J. 8 (3) (2013).

[37] M.S. Al-kahtani, Survey on security attacks in vehicular ad hoc networks (VANETs), in: 6th International Conference on Signal Processing and Communication Systems (ICSPCS), IEEE, 2012, pp. 1–9.

[38] A. Rao, A. Sangwan, A.A. Kherani, A. Varghese, B. Bellur, R. Shorey, Secure V2V communication with certificate revocations, in: IEEE Mobile Networking for Vehicular Environments, 2007.
[39] M. Raya, P. Papadimitratos, J.P. Hubaux, Securing vehicular communications, IEEE Wirel. Commun. 13 (5) (2006) 8–15.
[40] B. Xiao, B. Yu, C. Gao, Detection and localization of sybil nodes in VANETs, in: Proceedings of the 2006 Workshop on Dependability Issues in Wireless Ad Hoc Networks and Sensor Networks, ACM, 2006, pp. 1–8.
[41] D. Singelee, B. Preneel, Location verification using secure distance bounding protocols, in: IEEE International Conference on Mobile Adhoc and Sensor Systems, 2005, p. 7.
[42] T. Zhou, R.R. Choudhury, P. Ning, K. Chakrabarty, P2DAP – sybil attacks detection in vehicular ad hoc networks, IEEE J. Sel. Areas Commun. 29 (3) (March 2011).
[43] G. Yan, S. Olaruis, M. Weigle, Use of infrastructure in VANETs, Comput. Commun. 12 (2008) 2883–2897.
[44] D. Kushwaha, P.K. Shukla, R. Baraskar, A survey on sybil attack in vehicular ad-hoc network, Int. J. Comput. Appl. 98 (15) (July 2014).
[45] L. Song, Q. Han, J. Liu, Investigate key management and authentication models in VANETs, in: IEEE International Conference on Electronics, Communications and Control (ICECC), 2011.
[46] Ch.D. Jung, Ch. Sur, Y. Park, K.H. Rhee, A robust conditional privacy-preserving authentication protocol in VANET, in: First International ICST Conference, MobiSec, Italy, June 2009, pp. 35–45.
[47] R. Raiya, Sh. Gandhi, Survey of various security techniques in VANET, Int. J. Adv. Res. Comput. Sci. Softw. Eng. 4 (6) (June 2014).
[48] N. Patel, R.H. Jhaveri, Trust Based Approaches for Secure Routing in VANET: A Survey, Elsevier, 2015, available online at www.sciencedirect.com, ICACTA.
[49] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, A. Hassan, Vehicular ad hoc networks (VANETs): status, results, and challenges, Telecommun. Syst. 50 (4) (2012) 217–241.
[50] P. Caballero-Gil, Security issues in VANET, available http://cdn.intechopen.com/pdfs-wm/12879.pdf, 2011.
[51] R. Rajadurai, N. Jayalakshmi, Vehicular network: properties, structure, challenges, attacks, solution for improving scalability and security, Int. J. Adv. Res. 1 (3) (March 2013), IJOAR.org.
[52] J. Blum, A. Eskandarian, The threat of intelligent collisions, IT Prof. 6 (1) (2004) 24–29.
[53] S.S. Kaushik, Review of different approaches for privacy scheme in VANETs, Int. J. Adv. Eng. Technol. (ISSN 2231-1963) 5 (2) (2012).
[54] V. Vèque, C. Johnen, Hiérarchisation dans les réseaux ad hoc de véhicules, in: UBIMOB, Bayonne, France. CEPADUES, 2012, pp. 45–52.
[55] P. Fan, J.G. Haran, J. Dillenburg, P.C. Nelson, Cluster-based framework in vehicular ad-hoc networks, in: 4th International Conference, ADHOC-NOW, Proceedings, 2005, pp. 32–42.
[56] A.M. Malla, R.K. Sahu, A review on vehicle to vehicle communication protocols in VANETs, Int. J. Adv. Res. Comput. Sci. Softw. Eng. 3 (2) (February 2013).
[57] A.M. Malla, R.K. Sahu, Security attacks with an effective solution for Dos attacks in VANET, Int. J. Comput. Appl. (ISSN 0975-8887) 66 (22) (2013).
[58] L. He, W.T. Zhu Mitigating, Dos attacks against signature-based authentication in VANETs, IEEE Int. Conf. Comput. Sci. Automat. Eng. (CSAE) 3 (2012) 261–265.