Journal of Information Security and Applications 55 (2020) 102618

Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa

Pseudonym change-based privacy-preserving schemes in vehicular ad-hoc networks: A survey

Messaoud Babaghayou [a,*], Nabila Labraoui [a], Ado Adamou Abba Ari [b,c], Nasreddine Lagraa [d], Mohamed Amine Ferrag [e]

[a] STIC Lab, Abou Bekr Belkaid University, P.O.Box 230, chetouane, Tlemcen 13000, Algeria
[b] LI-PaRAD Lab, Saint-Quentin-en-Yvelines University, 45 Avenue États-Unis 78035 Versailles cedex, France
[c] LaRI Lab, Maroua University, P.O. Box 814 Maroua, Cameroon
[d] LIM Lab, Amar Telidji University, P.O. Box G37, Route de Ghardaia (M'kam), Laghouat 03000, Algeria
[e] Department of Computer Science, Guelma University, B.P. 401, 24000, Algeria

ARTICLE INFO

Keywords:
VANET privacy
Location tracking
Anonymity
Identification problem
Pseudonym change techniques

ABSTRACT

Vehicular Ad-hoc Networks (VANETs), which are a subclass of Mobile Ad-hoc Networks (MANETs), received a widespread attention during the last decades. With these promising set of safety applications, which are the main reason why they were developed, VANETs are considered as a tremendous support for the Intelligent Transportation Systems (ITS). However, several key issues remain to be solved before VANET becomes fully applicable; one of them being privacy preservation. To fulfill safety-requirements in VANETs, the vehicle needs to broadcast its status wirelessly. Consequently, any adversary can hear the broadcast messages at the aim of analyzing them, identifying, tracking and generating profile of his target. In other words, privacy of individuals may be seriously breached in VANETs if no safety measures were been taken. Using pseudonyms instead of the real identities of individuals, and changing them periodically during the communication is a promising solution for such crucial problems. There is a significant body of research work addressing this issue and a lot of researchers proposed various privacy protections basing on pseudonym change strategies. In this survey paper, we present an introduction to the privacy problem and give a recent and detailed state of the art of the different suggested pseudonym change strategies and approaches. We also propose a novel taxonomy to classify these strategies to diverse concepts. Finally, we discuss, give future directions and open issues and mention some of the observations that lead to better identify this problem for better future strategies.

1. Introduction

1.1. Background

Over the past few decades, the world witnessed a huge evolution in different fields (e.g., the wireless communication technologies and automobile industry), which let all of the: government, industry and the research community think about benefiting from this evolution to overcome the current challenges that the world is facing. The augmentation of the vehicles number and its implications (road safety, traffic efficiency, congestion problems, etc.) are a good example for such challenges. In addition to these problems (namely safety-related problems), there are also comfort-related problems, aimed at providing entertainment for both the driver and his passengers (connection to the internet, sharing files, instant conversation between drivers and passengers, etc.).

Vehicular Ad-hoc Networks (VANETs), that are essential for cooperative driving among vehicles on a given road, provide the communication among vehicles on the road and the Road Side Units (RSU) in an ad-hoc manner by using wireless technologies such as IEEE 802.11p. Taking their unique features (that include self-organization and self-management) in mind, these networks become key components for Intelligent Transportation Systems (ITS) [1,2]. Thus, the deployment of VANETs took part in this area. The main objective of VANETs is to give vehicles the ability to communicate either by Vehicle to Vehicle (V2V), Vehicle to Infrastructure (V2I) or even by Vehicle to everything (V2X) in

* Corresponding author.
E-mail addresses: messaoud.babaghayou@univ-tlemcen.dz (M. Babaghayou), nabila.labraoui@mail.univ-tlemcen.dz (N. Labraoui), adoadamou.abbaari@gmail.com (A.A. Abba Ari), n.lagraa@lagh-univ.dz (N. Lagraa), ferrag.mohamedamine@univ-guelma.dz (M.A. Ferrag).

https://doi.org/10.1016/j.jisa.2020.102618

Available online 10 October 2020

order to achieve (1) safety, (2) entertainment and (3) traffic efficiency. Therefore, each vehicle will be equipped with an On-Board Unit device (OBU) that allows vehicles to transmit over the wireless medium. Actually, VANETs are using wireless sensors allowing it to be aware of its environment. Consequently, this kind of networks is considered as a class of Mobile Ad-hoc Networks (MANETs) or a special kind of Internet of Things (IoT), more precisely, Internet of Vehicles (IoV) [3].

Each vehicle needs to broadcast beacon messages (also called heartbeat messages) that contain the vehicle's current position, speed, identifier and other useful information that are combined with a time stamp and signature which help to well-describe the vehicle's status. By doing so, the vehicle will have a pretty good knowledge about its environment. This knowledge is used by safety and traffic efficiency services to enormously enhance the traffic movement and to boost the line-of-sight of drivers, and by entertainment services to provide comfort to the driver and his passengers [4].

Despite the big and interesting benefit that accompanies the use of this technology, it introduces many problems that are mainly related to security aspects [5] (they will be further described in the next sections). Due to the unique characteristics of VANETs, the encryption of beacon messages is strongly not recommended because it introduces an additional latency. Thus, the position of the vehicle that is set in beacon messages will be readable for every eavesdropper; which endangers the privacy of drivers allowing the attacker to: track, identify and generate profiles of his targets.

The reason for what the attacker wants to track vehicles may vary depending on his purpose. For example, a boss who wants to get knowledge about his employers' exact location during the work time, a thief who wants to make sure the owner is really outside his home, or, in the worst cases, a criminal that follows his target in order to inflect a serious physical damage to him. That is what puts the driver's privacy on the top of VANET issues.

To solve the problem of knowing the driver's real identity by eavesdropping beacon messages, which endangers his privacy, a basic solution was proposed suggesting that each vehicle will have, instead of its real identity, a pseudonym that is used and changed over time in the vehicles' communications. This will prevent the adversary from knowing the exact identity of his target. However, the achieved privacy must not be absolute, because, in case of accountability which is indispensable, we must always be able to match the driver's pseudonym(s) with his real identity. Thus, this ability must be an option and restricted to privileged authorities.

Unfortunately, using pseudonyms will not solve all privacy problems because the adversary can still track vehicles that are broadcasting their locations even if they change pseudonym. Such attack is called: *linking attack*. It allows him to analyze the driver's trajectory which can be used next to know the exact identity of the driver. As a solution, a collection of non-conventional pseudonym change strategies was proposed in different researches [6–36]. The key in these strategies is to change the pseudonym at a proper location/moment to break the continuous tracking of vehicles.

1.2. Authors' contributions

This paper gives a set of contributions represented in:

- We provide an extended and detailed state of the art of the most interesting pseudonym change strategies that emerged since the suggestion of deploying VANETs to the recent moment that precedes the fulfillment of this study.
- We debate a set of prominent privacy-preserving strategies in a kind of comparison table with a rich set of metrics.
- We present a novel taxonomy that bases on the trigger-based (the opportunity; how, when and where the pseudonym change takes place) vs. the trigger-free (the randomness) pseudonym change; that we hope it will well-clarify the nature and mechanism of the various strategies to the new researchers.
- Finally, we give some influential concepts that must be taken during the design of any privacy-preservation strategy for better privacy level.

It is also important to mention that this research is not the first work done in this area, but, it is a complement to some other surveys such as [37,38] which gave a good guideline to privacy in VANETs. However, the different strategies, in our opinion, were not well-categorized according to all different perspectives leading to an ambiguity in the comprehension of the exact characteristics of each strategy, as an example, in [37], authors focus more on the abstract pseudonymous schemes than the proposed pseudonym change strategies, which was complemented by [38] where they categorized the strategies according to mix-zone vs. mix-context. However, there are other classifications that were not done yet and they are more meaningful compared to conventional classifications and that is the purpose of this survey paper in addition to its recency.

1.3. Organization of the paper

The remainder of this paper is organized as follows: In Section 2 we give a brief overview of the most relevant concepts in VANETs in order to put the non-experts in the picture (namely *VANETs: an Overview* section). Next, we outline the different security challenges in VANETs in Section 3. After that we have Section 4, in where we dive deeply in the privacy problem in order to well-understand the different solutions and their characteristics. In Section 5 (namely the *Extended Related Work* section), we present a detailed state of the art by a chronological order and in an exhausted way, that review the most relevant strategies proposed to solve the privacy problem in the two recent decades. After that, we show the comparative table of the different pseudonym change strategies, our novel taxonomy that is based on different perspectives and overviews compared to other classifications done in this scope, and, accompanied by a set of important and crucial remarks that must be taken into account during the design of any privacy scheme. These are shown in Section 6. Lastly but not least, we discuss and interpret the most prominent observations and characteristics resulting from Section 6 and that will be in Section 7. Finally, we conclude our work by giving an outline of the open research issues, tendencies and general remarks on the topic in Section 8.

2. VANETs: An overview

The yearly damages caused by vehicular accidents (1.3 million deaths with $518 billion of costs in the globe [39]) let the emerging of VANETs to benefit from the advances in the field of wireless communications, where its main creation purpose is to reduce the country's costs in terms of lives and economy [40]. The unique nature of ad-hoc networks that allows the quick spread of information let VANETs, that are extended from MANETs [41], be the most appropriate wireless network to be used for solving the previous problems [33]. Fig. 1 shows the position of VANET in relation to some other networks like MANET which is in its role a subclass of Wireless Ad hoc Network (WANET) [42].

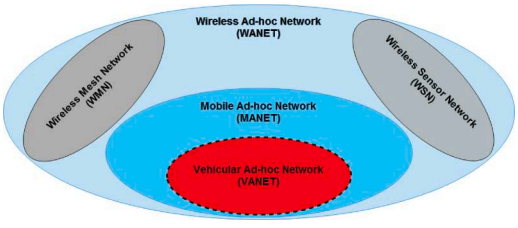

Fig. 1. VANET and its relation with other networks.

By this in mind, VANETs inherit most of WANETs' characteristics where the shared wireless medium has a lot of issues and vulnerabilities as will be shown in the next sections.

2.1. VANET architecture

Communications inside VANET need a predefined architecture. The vehicle, which is the essential element in this network, must be equipped with an OBU that allows it to transmit over the wireless medium, namely the wireless access in vehicular environment (WAVE) [18]. OBUs are used to exchange data between VANET components. Another device which may be used in coordination with the OBU is the Application Unit (AU), this device's main role is to communicate and connect to other services in the network [43]. In the components other than vehicles we may find:

B) Cell phones (sometimes referred to pedestrians)
C) Unmanned Air Vehicle (UAV) [44], a drone/Flying Ad-Hoc Network (FANET) system that may assiste the VANET system
D) Roadside Units (RSUs), which are devices fixed right in the roadside
F) Cell towers (3/4/5G [45] technologies provided to VANETs)
G) Different kinds of servers (location, authentication, application servers) [46]

Fig. 2 illustrates the previous VANET components and the different modes of exchanges between them.

2.2. VANETs' features

VANET is a subclass of MANET, resulting in an inheritance of most of MANET characteristics. However, due to the unique nature of VANETs [47,48], there exists the following special features:

1. No energy constraints: the big amount of battery energy with the on-the-driving recharge ability remove the energy constraint that does exist in most of the other wireless networks.
2. Fast topology change: since the speeds of vehicles are remarkably high, the topology changes frequently and quickly resulting in influencing some fundamental functionalities like routing algorithms and congestion applications.
3. High Computational ability: strong and modern CPUs are used which result in efficient and non time-consuming calculations.
4. A non-static network density: because the topology changes so fast as stated before, this results in the variation of network density spatially and/or temporally.
5. A known mobility pattern: since the movement is restricted by roads and highways, it is likely to be easily predictable.
6. Safer and comfortable driving: due to the communication ability between vehicles, ensuring an environment awareness between them for the sake of safety becomes possible.
7. A non-secure communication medium: because of the wireless medium's nature, the security of the wirelessly exchanged information is going to be a challenging issue.

2.3. VANET applications

The different sensor types and the GPS device give the vehicle the ability to know its environment through collecting and processing the gathered information. Then, spreading it to the other vehicles that are in the vicinity [49]. Thus, many potential VANET applications are suggested by researchers under various VANET projects and they are up to be implemented. We can distinguish two main application categories:

- *Safety related applications*: their main objective is to make decisions, warn the driver about the situation [50], improve road safety and to avoid as much accidents as possible. There are lots of safety related applications including: traffic signal violation warning, emergency electronic brake light, pre-crash sensing, lane-change warning, etc. [49]
- *Entertainment/infotainment (or non-safety) related applications*: In some works, they are splitted into (1) *Entertainment* and (2) *Traffic Efficiency Applications*. This category of applications mainly aim at achieving a good level of traffic management and infotainment for both the driver and his passengers [16]. A set of non-safety applications can be: speed management, co-operative navigation, global internet service, etc. [51]

2.4. VANETs communication model and standards

As mentioned in the VANETs architecture section, the protocol suite used by vehicles to communicate is WAVE. The protocol layers of WAVE are well-defined in the conducted work done in [51] by Karagiannis et al. In VANETs, we find many kinds of communications, V2V and V2I are the most used. Therefore, the Dedicated Short Range Communication protocol (DSRC) emerged and went through several standardization phases to well-fit the nature of VANETs; coming with promising features (3 to 27 Mbps as a transfer rates, a low latency to operate in a range up to 1 Km, etc.). The DSRC was also accompanied by the 1609 (described in Table 1) standards family to solve some issues like establishing communications in different channels. There is a variety of vehicular communications other than V2V and V2I, the general term to describe such communications is Vehicle to everything (V2X), where it creates a wide research area (V2P for Vehicle to Pedestrian, V2N for Vehicle to Network, etc.) Fig. 3 shows the format of a V2V packet according to Qu et al. [41].

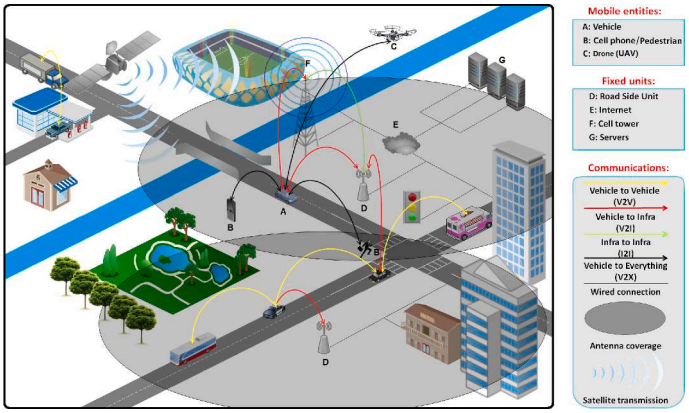

Fig. 2. VANET architecture and its main components.

Table 1
a set of VANET standards that support the ITS applications.

Standard	Description
IEEE 1609.1	Provide OBUs with the ability to use external resources to enhance their calculation potentials
IEEE 1609.2	Secure message formats in WAVE
IEEE 1609.3	The WAVE network layer (routing and addressing tasks)
IEEE 1609.4	Appends the multi-channel operation to the IEEE 802.11p
IEEE 802.2	The Logical Link Control (LLC) in the link layer
IEEE 802.11p	Physical and MAC layers management and an improvement of the IEEE 802.11 standard to permit the WAVE protocol

Fig. 3. V2V packet format.

3. Security in VANETs, a general overview

The main objective of VANET is to ensure safety and entertainment with its various safety related and non-safety related applications respectively. However, if the communications inside VANET is not secured, the results will be disastrous in terms of human lives and economically. This is due to the different kinds of attacks that can be launched against such networks, and that is why the study of security attacks, requirements and countermeasures must not be neglected [40, 52].

3.1. Security requirements and aspects

In VANETs, a set of security requirements must be guaranteed [42, 53,54]. The most important requirements are presented in Fig. 4 and defined as follows:

Authentication: when a node (vehicle) receives a message, it must be able to know whether the generated message is from a legitimate sender or not. This is mostly done using the verification of the sender's signature which may add a certain amount of latency. Hence, this process has to be done in as short period as possible by using fast authentication schemes. *Availability*: Despite the high mobility and the existence of some security attacks (e.g., Denial of Service attacks that will be shown next), the network must always be available for receiving/sending messages especially for the safety-related messages. *Integrity*: it means that the delivered message must not be altered by a malicious node. Integrity is relevant to authentication, where the verification of the received message tells if it is correct or corrupted (either altered or not respectively). *Non-Repudiation*: where the real sender of a message must not be able to deny the fact that he really was the origin of that sent message. The proof is assured via cryptographic techniques (base on the private key used for signature). *Confidentiality*: during the communication, only the concerned members involved in this communication must be able to decrypt the messages; a good example is the group members' broadcasts, no other than this group can read the messages. However, in safety-related messages, the encryption is not recommended due to the additional latency. So, confidentiality is not considered as an important characteristic for safety-related applications. *Privacy and Anonymity*: the driver's personal information must be kept private and protected against unauthorized access. Due to the nature of the wireless medium, it is hard to achieve a total privacy because the security related messages are sent in clear due to the latency problem when encrypted, that is why there is a big trade-off between privacy and security. Privacy has a strong relation with anonymity, where the anonymity refers to the ability to prevent the unauthorized entities from physically identifying the originator of the message, and by consequence, matching the identifier used in the message with the persons real identity. This may cause some serious problems when the attacker tracks his target according to his cars broadcasts (the periodic location is sent in clear due to the safety-applications' requirements). That is why privacy is considered as one of the essential security requirements. *Traceability*: it must be always possible to know the origin of the safety message and to trace it. However, this ability must be kept to authorized entities such as the Law Enforcement Authority (LEA). The safety messages are supposed to be stored in the Event Data Recorder (EDR) [53]. *Revocability*: it means the elimination of a misbehaving node from the network. This depends on the responsible authoritys decision. According to the research work performed in [55] Wasef et al., there are two revocation mechanisms: centralized and decentralized revocation (either by a specific authority or by the node's neighbors respectively).

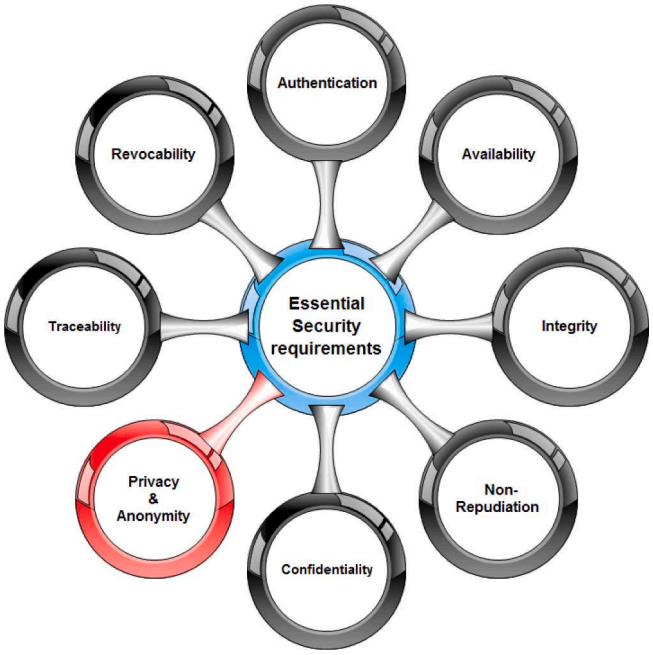

Fig. 4. The essential security requirements in VANETs.

3.2. Security architecture

From a security perspective, we can see VANET (as illustrated in Fig. 5) as a set of three main components [41]:

A) Trusted Third Parties (TTPs): are considered as the holders of the vehicles' credentials, identities and certificates. They are also reinforced with sufficient storage devices and high performances servers to manage the aforementioned tasks. **B) Roadside Units (RSUs):** they are

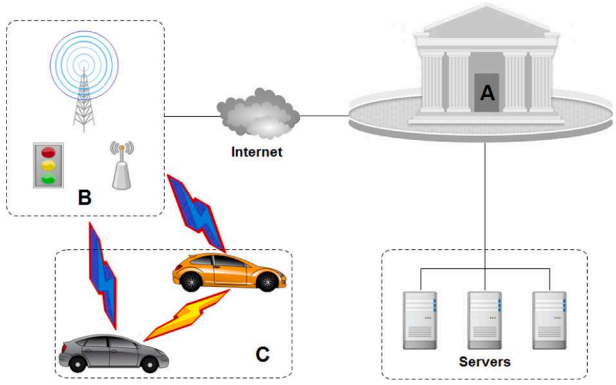

Fig. 5. Security architecture in VANETs.

fixed devices on the roadsides controlled by the TTPs. The TTP can revoke a RSU if it finds that the RSU is a malicious entity under the control of an attacker. **C) Vehicles:** the main entity in VANET. Vehicles can communicate with other vehicles, RSUs or with TTPs (via RSUs). Just like the case of RSUs, vehicles can also be considered as malicious entities.

3.3. Adversary types, potential attacks and countermeasures

Before we proceed to the real problem, it is important to know the features and characteristics of the environment that the driver is dealing with. The adversary type and what kind of attacks he can execute are very crucial factors to make better decisions and countermeasures.

3.3.1. Adversary types

In VANETs, there are a lot of adversary/attacker types [37,42,56]. They can be classified, according to the research papers and our observation, based on the following perspectives:

1- **"Actively" (Active or Passive):** An active attacker can alter, remove or generate new messages in order to affect the performance of the network. On the contrary, a passive attacker does not do more than eavesdropping the exchanged communications. Thus, he cannot directly harm the network.
2- **"Behaviourally" (Malicious or Rational):** The primary objective of a malicious attacker is to execute a destructive attack that damages the network with various methods. The rational attacker aims to achieve a personal benefit from his attack. This means his actions are more predictable than those of a malicious attacker.
3- **"Locationally" (Insider or Outsider):** The insider attacker is an authenticated member in VANET. He is by then able to perform a lot of serious attacks on the network. Whereas the outsider attacker does not have the ability to directly participate in the network. Hence, the insider attacker is more dangerous than the outsider one.
4- **"Proprietarily" (Global or Local):** A global adversary controls a large area in terms of radio stations deployed across the network. Thus, he can easily detect the mobile entities inside the covered area (also called region of interest). The local adversary controls less network entities than the global one; hence, he is limited in terms of the covered area. The utilization of the collected data may vary, we see some dangerous attacks resulting from the unauthorized data collection in the next chapters.
5- **"Movably" (Static or Dynamic):** The adversarys eavesdropping stations are either put fixed in some specific spots or moving across the observed map. The strength of each of these kinds depends on the used mechanisms and algorithms. The moving ones need a delicate processing (e.g., moving to follow a specific node) which is hard to be ensured. But, it is useful in the case where the adversary has few stations. On the other hand, the fixed stations do not need a lot of management except the synchronization and the sharing resources management. This one provides the adversary with a good monitoring ability if he has enough stations to cover an area. If not so, then he cannot monitor whatever he wants.
6- **"Occasionally" (Permanent or Temporal):** The adversary could be seen as a permanent or a temporal observer of the covered area. A permanent observer is more dangerous due to the fact that he gathers data and eavesdrops the different communications that occurs all the time. Contrary, a temporal observer would just eavesdrop at some period of times depending on his interests, intentions and benefits.

3.3.2. Potential attacks

In VANETs, and as discussed before, the nature of the shared wireless network grants the attacker the ability to execute and launch diverse attacks. Each attack has its specific characteristics and benefits. Many researches done in this scope had highlighted the potential attacks that exist in VANETs [41,42,54,55,57,58]. Because our paper is dealing more with location privacy, we recall the attacks that mainly affect the privacy of individuals as follows:

1. *Denial of Service*: in the Denial of Service (DoS), the attacker focuses on paralyzing the targeted service, in this scope, it may be the service responsible of delivering the set of pseudonyms used by vehicles to ensure their privacy.
2. *Eavesdropping attack*: in where the attacker eavesdrops (i.e., listens to) the transmitted packets over the shared wireless medium. This attack can be seen as a preamble to other critical attacks that are based on the collected data.
3. *Identity disclosure*: in identity (or ID) disclosure attacks, the malicious node reveals the location of its neighbor node. In most cases, it does this after being infected by a virus [42] sent by the attacker at the aim of getting the current location of a specific node. By this, he targets the node's neighbor (or neighbors) where it periodically discloses its neighbor's location. It is clear that this attack strongly breaches the privacy of VANET nodes.
4. *Location tracking*: because of the periodic broadcasts imposed by safety applications, the attacker can read the location of his target vehicle after eavesdropping its safety broadcasts (beacons). He can later benefit from a lot of private data like the real identity of the driver, the frequent visited places and other sensitive information. We will talk about location tracking and other privacy related issues (the pseudonym linking attacks) in the next section.
5. *Malware attack*: as viruses and malwares infect computers, VANETs are also susceptible to be infected by malwares. Thus, an anti-malware framework should be further developed in order to be deployed on VANET entities (i.e., OBUs, RSUs, etc.). The malware can expose the individual's most critical and secret data such as his location, heading and so on.
6. *Man in the middle attack*: in such attacks, the attacker interferes in the communication between two other nodes; he firstly eavesdrops the communication, then, he acts as the other part involved in the communication so that he can intercept and reply to each side with his own created packets (the original two parts do not know that they are dealing with an attacker). The attacker can also extract private data that is related to the individuals' privacy.
7. *Masquerade attack*: in order to exploit the network, the attacker impersonates a legitimate node (faking his authentication by taking a legitimate identity of another authenticated node) then he executes a lot of attacks, like extracting privacy related data, that could not be done without being authenticated.

3.3.3. Countermeasures

To provide the right solution against a specific attack, it is recommended and important to know the characteristics of that attack in its exact context.

In [58], Laurendeau and Barbeau. classified the different attacks according to the appropriate security requirement. They categorized them into attacks related to availability (DoS, malware, etc.), authenticity (masquerading, GPS spoofing, etc.) and confidentiality (eavesdropping, location tracking).

Mokhtar and Azab classified in [54] the attacks according to the targeted network layer (Application, transport, network, link and physical layer). They mentioned the most serious attacks with the corresponding solutions basing on the operating layer.

Another interesting research is that of [42], where La and Cavalli made a detailed survey on the attacks, their characteristics and their convenient countermeasures. We mention some of them: as in the bogus information attack, they recalled that the Elliptic Curve Digital Signature Algorithm (ECDSA), which is a message authentication scheme, is the suitable solution for this kind of attacks. Or, in the DoS attack, the solution is to base on a particular processing unit which is a support for the OBU. This piece indicates to the OBU that it is under a DoS attack resulting in a necessity to switch the current communication channel for

example. Also, for black hole attack, they pointed out that allowing more than one route for the packet delivery is an acceptable solution.

Finally, despite the diverse and large number of attacks threatening security in VANETs, there are a lot of efforts that were undertaken to intercept these attacks. The most satisfying and used solution is that of the Public Key Infrastructure (PKI) schemes [41] where it uses cryptographic techniques based on public and private keys in order to secure the communications. However, PKI itself cannot solve all security related issues. For example, it cannot protect from the location tracking (discussed in more details in the next section) because the location of vehicles must remain revealed for safety-related requirements. It is also important to mention that cryptographic techniques add a remarkable latency which is not so suitable for VANET needs.

4. Privacy: A crucial security aspect in VANET

Because the employing of VANETs comes to provide safety, entertainment and traffic management efficiency, vehicles need to broadcast their status in terms of identifier, position, velocity and other useful information. However, from the position information gotten after an eavesdropping, an adversary can easily track the vehicle and identify its driver [59]. Thus, the privacy of the driver must be delicately maintained. The basic solution to provide a certain level of privacy is to use æpseudonymsɡ. A pseudonym is a replacement of the real identifier that is set in the periodic beacon messages. It solves the problem of the identification of the driver in the case of a basic adversary but an advanced adversary can identify the driver even after using the pseudonym by analyzing the trajectory of the vehicle and the history of all its trips; hence, he can link the pseudonym with the real identity of that driver. To break the linkage of the vehicle's sequence of locations, the use of pseudonym change technique must be performed as an acceptable solution for such threats [60,61]. To better understand the problem of privacy, we recall the most important characteristics that must be maintained. The location privacy and all what concerns the pseudonym change techniques is described in the following subsections.

4.1. Privacy indispensable requirements

As explained before, privacy is considered as one of the most critical security requirements due to what it can lead to if it is not well-ensured. Moreover, privacy itself has to be maintained by the following requirements according to Schaub et al. [62]:

Minimum disclosure: during the communication, a vehicle sends data where it reveals a certain amount of information. This amount of information must be kept as minimum as possible. i.e., must be kept to the bare minimum for a basic functionality of VANETs. **Anonymity:** when a message is sent, the origin of that message (the sender) must be kept anonymous within a set of other potential senders. The identity resolution must always be supported through the different authorities by solving the linkage between the anonymous credential and the real identity of the individual in order to achieve the accountability requirement. Moreover, the larger the set of potential senders is, the better the anonymity of the sender is fulfilled. **Unlinkability:** in VANETs, there are what we call æitems of interestɡ such as persons, vehicles, credentials, messages, etc. The aim of the unlinkability is to guarantee that the relation between these items of interest (two or more) could not be linked. Also, the main target of an adversary is to link an item of interest to an individual person. They can do it either (1) directly by linking the person with his vehicle or (2) indirectly by linking the vehicle with its sent messages then, linking the vehicle with the person so that they would know the person who sent the message. Moreover, the unlinkability tends to implicitly achieve other privacy concerns like the anonymity. Among the ways to cope with this requirement, there is the deployment of a "distributed resolution authority" which is defined as the ability to identify an individual within VANET must be partitioned between more than one authority so that only the cooperation between the different authorities would be the mean that leads to fully identifying that individual. The use of more than one authority has a lot of benefits like (1) achieving a higher level of privacy compared to one single authority or party and (2) to stand against the situation where an authority gets hijacked or corrupted; the loss here will be minimal.

Perfect forward privacy: a VANET user has a lot of credentials that are used during his usual communications. However, there are some cases in where the resolution process of one of the credentials to an identity must be realized by an appropriate authority. In such a scenario, this resolution should not reveal any information that may affect negatively the unlinkability of the other credentials of that user.

4.2. Identity and location privacy

The identity privacy in VANETs is the act of preventing unauthorized entities from knowing the real identity of the driver. We mean by unauthorized entities the different VANET entities other than the trusted authorities. keeping the identity hidden must be conditional due to the fact that revealing the real identity is mandatory in case of a revocation or resolution process launched by a law authority after observing a suspicious behavior of one of the vehicles. The other concept is Location privacy which is defined as the ability to prevent other entities from knowing the current and/or past location of an individual [63]. Besides, location services play a vital role nowadays in different areas (e.g., informing the user about the nearest hotel, a less-congested road suggestion, etc.) they also cause privacy issues by revealing the user's location in an appropriate circumstance.

Individuals do not want their location to be exposed especially in sensitive areas [64], thus, giving them the option to be invisible is likely to let them feel safer [65]. The fact of the possibility to know the exact location of an individual at a specific time will bother him. Moreover, knowing all his exact location during a wide duration that occurred in the past few days may expand his worries and annoyance enormously. Thus, location privacy must be maintained carefully by only letting the allowed parties to have the ability to get the location of the individual and preventing (or limiting) as maximum as possible the unwanted parties from getting such sensible location information. There are other privacy models like interest privacy, backward privacy, content oriented privacy and other models [66]. We only described the two models; namely identity and location privacy. Due to their indispensable importance in VANETs, the majority of drivers want to get a good level of such privacy models. Among the most interesting solutions to ameliorate both identity and location privacy we find pseudonym schemes deployment. It is worth mentioning the efforts of the pseudonym management standardization like that of the "ETSI TR 103415" standard [67].

4.3. Pseudonymity

Instead of using one static identifier all the time; which fosters the tracking and the identification of that vehicle, the use of different identifiers, the so called pseudonyms, must be employed. Basically, a set of pseudonyms is stored in the OBU. This set plays the role of useable identifiers that enhances enormously the driver's privacy. There are a lot of proposed schemes to achieve high privacy levels basing on the use of pseudonyms.

4.3.1. Pseudonym schemes

To achieve a robust communication system with a high level of privacy, the need to implement effective pseudonym schemes arises. The desired schemes should base on cryptographic techniques that fulfill the privacy requirements. Due to the importance of such schemes, many works and suggestions were done in this scope. Petit et al. [37] had mentioned four pseudonym schemes, namely asymmetric cryptography, symmetric cryptography, group signature and Identity-based cryptography schemes. These schemes are described as follows:

Asymmetric cryptography schemes Asymmetric cryptography or often called public key cryptography is based on pair of keys mechanism. One key is public; used to encrypt data or to verify the digital signature set in the packet. The second key is private; used to decrypt the encrypted data or to make digital signatures. Moreover, among the main characteristics of asymmetric cryptography we find the mathematics bind between these two keys [41]. Even though asymmetric cryptography provides high efficiency, it also introduces an additional overhead and requires big computational processes which do not fit the real-time applications and constraints of VANETs.

Symmetric cryptography schemes Symmetric cryptography schemes are characterized by their high efficiency in the authentication phase and do not consume a lot of computational time as asymmetric cryptography does. The symmetric cryptography uses a Hashed Message Authentication Code (HMAC) to authenticate messages. This is done by hashing the message and a secret key. For that, the other nodes, who aim to verify the validity of the received message, must also have the private key in order to use it for verification and to send their own messages as well. There is an interesting benefit from this technique which is the extension of its anonymity set because every node that knows the private key can generate valid authenticated messages letting it be indistinguishable. However, this breaches the accountability requirement because this scheme implies the impossibility of achieving the non-repudiation of the sender [37].

Group signature schemes Because using a set of pseudonyms has a bad impact in terms of generating, delivering, storing and verifying these pseudonym certificates, the group signature schemes mainly base on the self-creation of signatures used to sign the message by a group member. This message can be verified by a common group public key. It enormously reduces the overhead since the need of other authorities and entities like the Certificate Authority (CA) or the Pseudonym Provider (PP) becomes mostly unnecessary. However, the group manager should determine the real identity of the sender inside that group because he is responsible for providing the group member secret key used in the communication [62].

Identity-based cryptography schemes Identity-based cryptography (IBC) resembles the asymmetric cryptography in where they both use a key to encrypt the sent data except that the key in IBC is the identifier itself of the node. In what concerns the private key, it can be generated (by authorized entities) from the same identifier of that node. By this notion, the verification of any message only requires the knowledge of the sender's public identifier [37]. In this scheme, the need for a centralized trusted authority to manage private keys is necessary to prevent the unappropriated nodes from deriving and generating private keys from a specific identifier, thing which breaches the authenticity requirement. By this way, the node's authenticity is well-guaranteed due to the fact that the centralized trusted authority gives the node its private key that will work with its public identifier.

For a detailed description of the aforementioned schemes, we redirect the reader to the survey of Petit et al. [37] since authors had focused on the those pseudonymous schemes in their research work.

4.3.2. Pseudonym lifecycle and phases

Despite the large proposed schemes that could be used to achieve pseudonymity, there are always phases that accompany the use of pseudonyms. To provide vehicles with pseudonyms, and to ensure an acceptable functionality of the VANET system, the lifecycle (called abstract pseudonym lifecycle in [37]) shown in Fig. 6 must be respected. The different phases are explained as follows:

1. *Pseudonym issuance*: In order to let the vehicle be able to communicate inside the VANET system, it needs to be authenticated. This is done by authenticating its OBU using the Vehicle Identifier (VID); a long-term signed certificate and pre-installed in the vehicles OBU [37]. Using its VID, a vehicle gets the ability to obtain pseudonyms, if necessary, from the pseudonym issuance authority after contacting it. Thus, the authentication step is a must before obtaining valid pseudonyms.
2. *Pseudonym use*: After acquiring a set of pseudonyms, a vehicle can use one of those pseudonyms in its ordinary broadcasts and communications. Pseudonyms are used to (a) sign the outgoing packets; i.e., for authenticating its messages. And to (b) verify the incoming packets to ensure that the received packet is valid. This signature and verification are ensured by the cryptographic mechanisms that respect the general security requirements.
3. *Pseudonym change:* Because the use of one pseudonym all the time leads to critical security issues such as location tracking that was described before, the need for changing pseudonyms is an absolute necessity. However, this change must respect a set of rules and must be maintained carefully because a pseudonym change performed in an inappropriate location/moment will just consume the pseudonyms set and add additional overhead while requesting new pseudonyms which decreases the performances of the VANET system. We will see pseudonym change in more details in the next sections.
4. *Pseudonym resolution:* when the law authority wants to know the identity of a sent message's holder, it requests a pseudonym resolution process from the pseudonym issuing authority. The reasons may vary, so it depends on the case, but it will not change the result of this request which is the acquisition of the vehicle's identity (VID). Therefore, it reduces the individual's privacy considerably.
5. *Pseudonym revocation:* Sometimes, a vehicle may not use its authentication properly; we talk about the case of a malicious node. If the monitoring authority, like the law authority, detects an illegal behavior from one or more vehicles inside the system, it may proceed to the pseudonym resolution process [68] in order to know the exact identity of the sender. Afterwards, it revokes its pseudonym. The scenario where the vehicle uses its other stored pseudonyms to continue participating in the VANET system must also be maintained. Thus, a mechanism to find out all of the vehicle's pseudonyms and revoking them must be ensured.

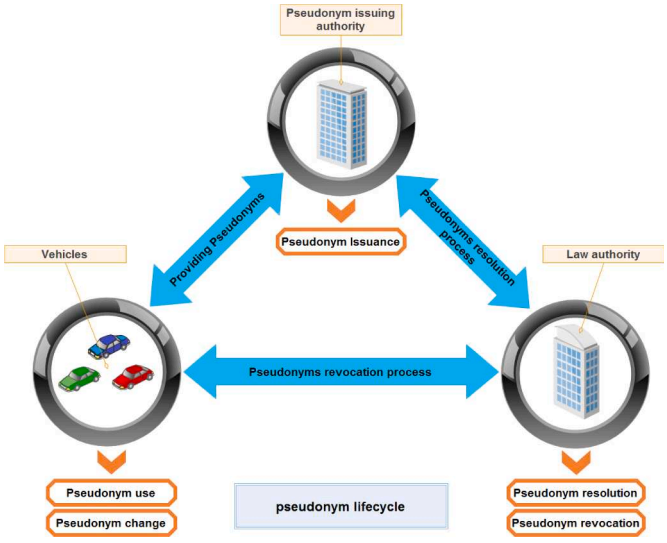

Fig. 6. Pseudonym life cycle and its different phases.

4.3.3. Pseudonym requirements

Before employing pseudonyms in VANET, we need to ensure a set of properties to fulfill the different VANET requirements and to avoid unwanted abnormalities that may occur and lead to put the VANET functionality down [37]:

1. **Distinct identity:** Each vehicle must have a unique pseudonym at a given time. To ensure this property, the use of a strong and coherent

cryptographic mechanism to generate (i.e., not to overlap with other vehicles' pseudonyms) and maintain pseudonyms is needed.

2. **Ensuring availability of pseudonyms:** At a specific time, if a vehicle needs a new pseudonym that pseudonym must be available. A common way to achieve this would be by storing a large set of pseudonyms in the OBU.
3. **Ensuring limited duration of pseudonyms:** The use of a pseudonym must not be infinite because, if it is so, the location tracking attack will be easily performed by an adversary. To force the discontinuity of using a pseudonym, adding a duration time to the signed certificate that accompanies the used pseudonym would solve the problem.
4. **Identity full change:** If a vehicle decides to change its pseudonym, it must change all its other identifiers used recently in its communication layers stack; because changing one identifier and letting the others would be useless and renders the breaking of its anonymity an easy job. In this way, the adversary links the new pseudonym with the old one according to his analysis and matching of the other communication layers' identifiers.
5. **Pseudonym change block ability:** The frequent changes and the overuse of pseudonyms cause several problems like the *Sybil attack* and the *high overhead* respectively. Thus, stopping pseudonym change must be assessed by the corresponding authorities or by a strong reputation system that can detect and remove any malicious vehicle from the VANET system if it breaches this feature.

4.3.4. Privacy implications on safety

Despite being the privacy mechanisms, especially those basing on the pseudonym change, beneficial to the user's privacy to some extent, they also open safety issues since being in silent periods, which will be discussed in details later, lets the vehicle be invisible not only to the tracker but also to the nearby legitimate vehicles which leads to both fooling the tracker and those nearby vehicles. Also, exchanging the used pseudonyms between vehicles has the same effect which endangers the users' safety as stated and detailed in "ETSI TR 103415" standard [67] that also discusses the current existing project working on the aspect of pseudonym change (we redirect the reader to the "ETSI TR 103415" standard for a more details); that is the "trade-off" between privacy and safety.

4.3.5. Location tracking techniques

Due to the severity of knowing the one's location, and what it implies from threatening his life in some cases, preventing the adversary from getting the exact location and the trajectory of that individual becomes imperative. The Adversary's methodology and tracking techniques may diverse. However, they generally base on the following two categories: *radio-based* and *license plate recognition* techniques.

A. *Radio-based techniques*

They do benefit from the feature of beaconing used by vehicles [38]. Because the vehicle broadcasts safety messages with a high frequency, an eavesdropper can easily exploit the broadcasted safety messages and knows a lot of information that facilitates the process of gathering and storing the vehicles' success locations and the corresponding pseudonyms used during its trip. We give two examples of such techniques as follows:

A.1) *Syntactic linking attack:* By continuously hearing the wireless shared medium, the adversary tends towards monitoring all the vehicles by eavesdropping their safety messages. More precisely, by focusing on (1) the pseudonym and (2) the time it was used in. If a pseudonym change happens, the adversary looks after the recently disappeared pseudonym and matches it with the newly one resulting in identifying the same vehicle that had changed its pseudonym. This attack becomes stronger when the vehicles do not perform the pseudonym change synchronously. In the other case, a synchronized pseudonym change will render this attack useless. Fig. 7 shows how the adversary can link pseudonyms changed (from 178 to 203) by just one vehicle where Psd means pseudonym, [A,T] means [Pseudonym value, corresponding time] and Δt means the time difference between the two time instants.

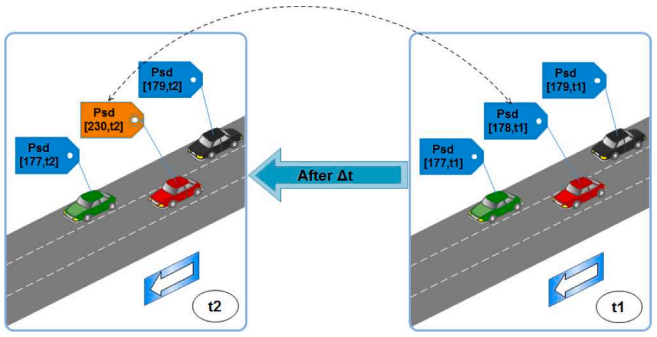

Fig. 7. Linking the new changed pseudonym (used at t2) with the old one (used at t1).

A.2) *Semantic linking attack:* It also exploits the information inside the safety messages. Even if the pseudonym change is done synchronously, the adversary can still identify and matches each new pseudonym with its corresponding old one. This is due to the fact that a safety message contains the vehicle's location and velocity which gives the adversary the ability to predict the vehicle's next position. Moreover, the higher the frequency of beacon messages is, the better is the achieved precision by the adversary. An illustration of this attack in Fig. 8 shows that even changing pseudonyms simultaneously at an instant t2 the adversary can still be able to resolve the matching (using prediction techniques). Thus, this kind of adversaries is more dangerous than that of the linking attack.

The exploited fields in the beacon messages to predict the next position are generally: the x & y geographic coordinates, the timestamp and the velocity of the vehicle. Fig. 9 shows that the adversary predicted the next position of the three vehicles V1,V2 and V3. According to that, he could match each vehicle's old and new pseudonyms.

B. *License plate recognition techniques*

These techniques use the license plate recognition systems that base on the image processing algorithms and the set of image capturing devices such as cameras. This technique's efficiency is much stronger than that in the radio-based technique if it is well-exploited. However, unlike the radio-based technique where the radio devices are cheap relatively, it is hard to create such systems because of the expensiveness of this devices and the large scale of the monitored area. The principal aim of this technique is to acquire the distinct license plates of observed vehicles and to build a general scheme which stores and processes their movements and locations.

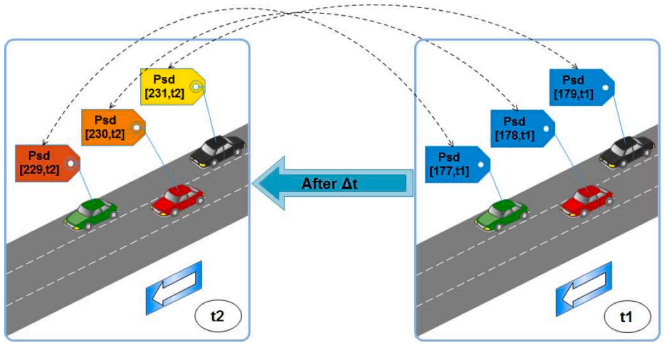

Fig. 8. Linking all pseudonyms that are changed simultaneously using prediction techniques.

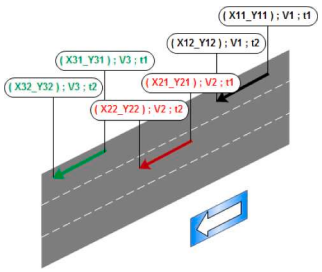

Fig. 9. Exploiting the information existing in beacon messages by the three vehicles in the semantic linking attack.

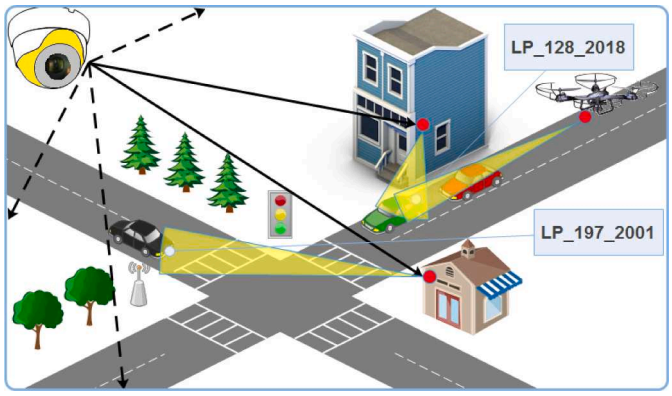

Fig. 10. License plate recognition system.

Fig. 10 shows a license plate recognition system employed in an urban environment near an intersection where there are two cameras set in two spots and a drone equipped with a dedicated camera in order to get any license plate of any vehicles passing by the controlled area and even pursuing the target for long distances if needed.

4.4. Privacy metrics

When we come to the question of how to quantify the achieved location privacy in the VANET scope, a set of various proposed metrics arises. Among the most relevant metrics we find the following ones as in the research of Wagner and Eckhoff. [69]:

1. *Set of Anonymity Size (SAS) :* It refers to the indistinguishability of a target vehicle in comparing to other vehicles in the same context. This metric is characterized by its simplicity in terms of calculation and imposition of the privacy problem. Also, it highly depends on the total number of the existing vehicles. It is important to mention that this metric does not describe the anonymity level in all scenarios because the adversary may find out that the tracked vehicle is not fully undistinguishable by observing the heading direction, velocity, power of the used signal and other features to determine and identify it successfully.
2. *Entropy (Ent):* This metric emerged just after finding that the SAS is not a well-describing metric. Thus, researchers trended towards the entropy metric which refers to the uncertainty in a random variable [69]. By combining this concept with the SAS, we find that the entropy is just the measure of a vehicle's anonymity inside the set; i.e., not all vehicles are alike in terms of being the target inside that set [70]. The Entropy's formula is given in Eq. (1).

$$H_p = -\sum_{i=1}^{|AS|} p_i \log_2 p_i \tag{1}$$

Where $|AS|$ refers to the SAS and p_i refers to the probability of vehicle i being the target. The more the vehicles are equally in the probability of being the target, the more the entropy metric gives its highest value $H_{\max}$ which is described in Eq. (2).

$$\forall i : p_i = \frac{1}{|AS|}, H_{pmax} = -\sum_{i=1}^{|AS|} p_i \log_2 p_i = \log_2 |AS| \tag{2}$$

3. *The degree of anonymity (d):* It treats the scenario where the adversary, at the beginning, has no knowledge about the vehicle's anonymity set. Here, the expected value of the measure would not be equal to that of the other scenario where he already has a certain amount of knowledge. Hence, the degree of anonymity (d) was proposed in [29] which aims to normalize the evaluated anonymity. (d) is described in Eq. (3).

$$d = 1 - \frac{H_{max} - H}{H_{max}} = \frac{H}{H_{max}} \tag{3}$$

4. *Adversary's Success Rate (ASR):* As the adversary's exact purpose may change depending on his interests, knowing exactly what he is looking for would be more significant. Thus, the adversary's success rate concerns the privacy property targeted by the adversary against a specific vehicle. Despite the meaningful results that are revealed after applying this measurement, it also introduces some challenges. As an example, a significant question emerges: ædoes the adversary really target the supposed privacy property?ɡ. In sum, this metric only works in the case of applying it according to what exactly the adversary is searching for.
5. *Maximum Tracking Time (MTT):* In most cases, the main goal of an adversary is to achieve the longest vehicles tracking time as possible. Thus, this measurement concerns the ability of that adversary to accumulatively tracking the vehicles. Additionally, it supposes that performing a pseudonym change at a certain time will make the adversary become confused. Unfortunately, this metric does not consider the case where the adversary uses additional techniques like probabilistic conclusions and benefits from an historic paths log of his target that is recorded/obtained earlier.
6. *Statistics on Pseudonym Change (SPC):* From its name, statistics on pseudonym change metric aims to measure anything that has a relation with pseudonym changes like the total number of successful pseudonym changes; i.e., the unlinkabikity [38]. This metric had only investigated the unlinkability property in most researches that used it [69].

It is extremely important to point out that not every metric is applicable to all pseudonym change strategies. The nature and the characteristics of the pseudonym change strategy are the only key that determines the correctness and applicability of such metrics. Therefore, it does not make sense to compare between a set of strategies that are not studied using the same metrics, and telling which strategy is the best in this scenario would not be significant.

5. Extended related work

The problems of re-identification and location tracking come generally from the supplementary information provided either by the car's transmitted messages under the corresponding protocol (e.g., the BSMs under WAVE) or by querying the Location Based Service (LBS) [71]. Stopping the generation of such sensitive information (the fine-grained locations of the vehicle) is not a suitable solution due to the fact that such information would enormously serve the individual and the whole system [63], and that what made a lot of researches and

projects arise. Using and keeping one identifier by a vehicle for its diverse communications inside the system is not acceptable for sure according to the standardization and as discussed previously. Using pseudonyms instead and making them temporary changed is fair enough to achieve a better privacy level. However, a simple change of these pseudonyms is not sufficient because of some techniques used by the adversary to link pseudonyms and even reveal the real identity of the driver. We present in the following, an exhaustive and chronological state of the art of a large body of privacy-preserving and pseudonymous schemes emerged during the last two decades:

In [6], Sampigethaya et al. propose CARAVAN, a scheme that employs the group forming technique and the use of silent periods between pseudonym changes. Indeed, because forming groups not only reduces the amount of redundant transmissions but, also gives the vehicles other than the leader the ability to stay silent, which for sure, enormously enhances the privacy of vehicles. However, this technique may only be employed in a probe vehicle scenario where the vehicles may stay silent for quite long periods without beaconing safety-messages. Additionally, the general case and standardization enforce the safety-message broadcasts in a high frequency so as to meet the requirements of safety-applications. Also, the leader's privacy is not fulfilled since it communicates all the time instead of its members.

Huang et al. [7] explore the silent period concept that can be used either temporally (at a variable time) or spatially (at a fixed location). After taking the MTT metric in their study, they showed that using silent periods brings a good enhancement to the privacy of wireless nodes.

Because the user-centric approach, which mainly bases on the vehicle's independent desire, lacks synchronization, Li et al. [8] present the Swing protocol that aims to increase the number of vehicles changing their pseudonyms at an appropriate opportunity. They also present an amelioration of the Swing protocol; the use of the Swap protocol that enables the exchange of pseudonyms instead of a simple change. However, as they mentioned it, the exchange process is not suitable in VANETs due to the accountability requirements (revocation, resolution of pseudonyms) and the management of identities. Hence, swap will highly depend on the infrastructure at any pseudonym exchange action (if we suppose that the exchange feature would be allowed).

Sampigethaya et al. [9] define the AMOEBA scheme that uses the group navigation as an advantage by letting vehicles belong to a group and only the group leader is able to communicate, on behalf of other members, with the LBS. Therefore, vehicles not only benefit from an extended silent period but also dispense with the redundant data that may be broadcasted by vehicles in the same vicinity. Authors also introduced the potential breaches of privacy that may occur while using the AMOEBA scheme which highly relies on the group concept; that has a set of vulnerabilities caused by the disclosure of one group member, like giving the group key used in communication to the adversary. This last one is the worst scenario that introduces a lot of privacy and security issues.

CMIX [10] is an another pseudonym change strategy that was proposed by Freudiger et al. that uses the idea of mix-zones, in addition to the encryption feature where vehicles inside the mix-zone encrypt their safety messages in order to prevent the adversary from accessing and reading the location information set in the packet. It is mainly formed by three phases: establishing the symmetric key by an RSU, ensuring the forward of this key to coming vehicles before they reach the mix-zone and finally the key update management where the RSU generates a new key (mostly when the traffic density reduces) and ensures the deliverance of that key to the CA (in case of a potential resolution or revocation process). Despite the effectiveness of this strategy against the unauthorized collection of location traces done by the adversary, the strategy introduces a set of challenges like the overhead minimization and synchronizing the key management between RSUs to let only one symmetric key in the system.

Gerlach and Guttler employ the Mix-context strategy [11] that uses an algorithm which aims at letting vehicles change their pseudonym synchronously when they meet some specific triggers. By adding a flag (or bit, æcalled ready to change flagg) in the normal beacon messages, the vehicle can show its desire and need for a pseudonym change operation and all other vehicles having the same desire will collaborate to make a synchronous pseudonym change.

In an earlier time (2003), Beresford et al. adopt the mix-zone concept [63] in pervasive computing, which is defined as a spatial region where the node would not provide any location information to other entities (even to location applications). The key in this technique is to perform the pseudonym change inside that zone so that the adversary would be confused because of the existing vehicles at the same time inside the zone. Once the vehicle leaves the zone, the adversary would not be able to distinguish it from the other vehicles that entered the zone. However, a high scale zone is not recommended because the adversary would estimate the time needed for a vehicle to leave that zone. Also, a low density zone helps the adversary to identify vehicles even after performing the pseudonym change. Basing on the same concept, Buttyán et al. [12] evaluate the effectiveness of the mix-zone in VANETs against an adversary that has already some knowledge about the used technique to face location tracking. They found after various simulations that the achieved level of privacy highly depends on the strength of the adversary where the stronger the adversary is, the less privacy level is achieved. The optimal deployment of the mix-zones is an open issue and has a high impact on the provided location privacy and it was investigated by other researchers like Freudiger et al. in [72].

Chaurasia and Verma investigate in [13] the real anonymity of a vehicle inside a set of vehicles (z zone in their work) and found that before joining the anonymity zone, the old communications used by a vehicle have a negative impact on the indistinguishability of that vehicle from its neighborhood vehicles due to the non-uniform probability distribution. Thus, not all vehicles inside the zone are really contributing to the effective privacy level. According to that, they proposed a heuristic pseudonym change that aims to find the right time and place when there are a certain number of neighbors in order to maximize the anonymity with only few (optimal) pseudonym changes.

Buttyán et al. provide a pseudonym change strategy called SLOW [14] (Silent at LOW speed). In SLOW, vehicles stop broadcasting safety messages when their speed drops below a certain threshold. It is true that this strategy not only prevents the adversary from tracking his target while it is silent, but also gets rid of the verified beacons amount by each vehicle (especially in high traffic jam where the condition of the low speed is fulfilled). However, forcing vehicles to stop beaconing safety messages is not always acceptable even if the accident probability is low in low speeds (a sudden brake in a low speed is a good example of the utility of safety messages). A better solution may be reducing beaconing frequency instead of stopping it definitely.

In order to maximize the number of vehicles that simultaneously change their pseudonyms, Liao and Li suggest a pseudonym change strategy which uses an algorithm that is called synchronous pseudonym change [15]. This algorithm uses triggers (like the vehicle's status) to guarantee a high synchronization between vehicles that have a similar status. After simulating and comparing their strategy (using traffic density and penetration rate as parameters) with other basic pseudonym change strategies (like random and fixed pseudonym change), they found that the level of privacy achieved by their synchronous pseudonym change algorithm is better than the other ones. However, the same trigger may differ depending on the chosen accuracy. In one hand, the more specific the precision of the trigger is, the more the pseudonym change (if performed) is successful and the less chance to meet it at the same time. In the other hand, the higher the trigger is global, the less pseudonym change is useless and the more chance to meet that trigger.

In another context, Lu et al. employ SPRING [73], a protocol dedicated for delay tolerant networks (DTNs) where they have shown that SPRING is both good for packet delivery in such sparse networks after holding the packet until a coming opportunity, and, for packet tracing

prevention because the packet is stored for a while before it is sent. Using RSUs in this protocol is also possible and serves as a mix-zone. They tested the effectiveness of the protocol against black-hole (grey--hole implicitly) attacks using a customized Java simulator, and it was shown up that it can resist against such attacks.

Song et al. present a density-based location privacy scheme (DLP) [16]. In DLP each vehicle knows about its vicinity (neighboring vehicle count or density as they called it). The density of vehicles is the main parameter that is used as a threshold for pseudonym changes. With the use of density zones of one intersection of four road sections per zone, they simulated their scheme and showed that the probability of a success tracking by an adversary relies on both the vehicles' variation of speeds and the arrival rates to the density zones. The more these two parameters are high the less chance there is for an adversary to perform a successful tracking attack.

In [17], Wasef and Shen apply the random encryption periods (REP) scheme. The main idea of REP is to ensure an effective and hidden (from the adversary) pseudonym change by letting all legitimate vehicles have a set of symmetric keys that helps them to provide one shared secret key. When a vehicle wants to change its pseudonym, it uses the shared secret key to create an encryption zone with the help of its neighbors. Thus, REP could be seen as a dynamic CMIX-zone since it is created on demand instead of at fix places like intersections. The strategy seems to be interesting and promising compared to CMIX since it dispenses with RSUs, however, when there is a high density, the encryption process may slow down the VANET performances and introduce an additional overhead.

In the same scope, a new metric called time-to-confusion (explained in the metrics section) and an algorithm called the uncertainty-aware path cloaking algorithm are given by Hoh et al. in [74] for two main privacy issues; target tracking and home identification. To test their algorithm, a real world GPS data set was used. Because GPS location traces (especially in low density areas) lead the adversary to identify, with a high certainty, his target, the proposed algorithm removes these location traces. Moreover, the algorithm deals with the case of vehicles that are driving in an opposite direction from the other ones. Hence, their location traces are removed as well.

The location privacy could be breached by ways other than safety messages. The investigation done in [75] by Ishtiaq et al. reveals the effect of the wireless tire pressure monitoring system on the driver's location privacy. Each vehicle in their model is wirelessly equipped with four tire pressure sensors (due to the nature of tires, there is no wire connections). These sensors have IDs to communicate with and to send the tires' status. However, because the design of this interesting technique does not take privacy risks into consideration (no cryptography means used), an adversary can easily track the vehicle target by eavesdropping its tire pressure sensors' messages in a distance of about 40 m. Indeed, the work tells that privacy of vehicles must be treated delicately in order not to let any potential privacy risks that may be used by adversaries to perform a successful tracking.

In [18], Eckhoff et al. propose Slotswap, a location privacy enhancement approach. Slotswap uses a set of pseudonyms (time-slotted pseudonym pool). In each time slot, the vehicle changes its pseudonym, more precisely it will use the current time slot pseudonym. The benefits of this technique would be the independence of many authorities like the CA and it prevents them from resolving the vehicle's real identity. Yet, the privacy, as it is described, must be conditional. The identity resolution must be always available for the appropriate (law) authorities. The authors mentioned the possibility of performing pseudonym exchange between vehicles that desire (have the trigger) to change their pseudonyms. This last proposition will increase the effectiveness of the synchronous pseudonym changes. However, pseudonym exchange is not suitable in VANET systems due to the accountability requirement.

Pan et al. [59] study analytically the effectiveness of random changing pseudonyms (RPC) scheme. They simulate and compare this scheme using two distributions: the uniform discrete distribution (taking into consideration the minimum and maximum use time) and the age-based distribution (refers to the pseudonym use time). They found that the RPC under the uniform discrete distribution gives better results than the age-based distribution in terms of location privacy.

Synchronized pseudonym changing protocol (SPCP) [19] is another privacy-preserving scheme that is proposed by Weerasinghe et al., in where SPCP mainly bases on the use of groups. Indeed, groups provide high synchronization which implies high location privacy. The protocol uses six phases that, some of them do, perform an initial phase (registering and providing vehicles with some parameters), forming and joining the group to the final phase of changing pseudonyms. They run a set of simulations and they showed after comparing their protocol with other strategies like the silent period, AMOEBA and REP that the proposed SPCP is the best among the other ones while it gives a higher privacy level.

Another idea in privacy-preserving is that of Lu et al. which is pseudonym change at social spot (PCS) [20] strategy. The strategy aims to maximize the number of simultaneous pseudonym changes and for that, the authors defined the right moment as the gathering of many vehicles at the same time and place (e.g., road intersections with a recent turning to red traffic light or parking lots near shopping malls). To show the effectiveness of their strategy, they developed two analytic models of anonymity set. They described a mandatory model (called KPSD) used by PCS to securely generate and provide vehicles with a set of on-demand short-life keys. Indeed, changing pseudonyms in such a condition ensures a high synchronization. However, there are other road conditions that let the vehicle stay for a long time without finding the mentioned opportunities.

Pan and Li provide a cooperative pseudonym change scheme [21] that is based on the vehicle's neighbors number (CPN). The scheme mainly benefits from the different triggers and helps the vehicle to choose the right moment for changing the pseudonym. Indeed, using triggers like the number of neighbors ensures a synchronized pseudonym change which leads to an effective location privacy enhancement compared to the individual behavior (the non-CPN). The proposed CPN is interesting because it achieves better location privacy results. However, it highly depends on the number of neighbors which is, unfortunately, not suitable in many other road scenarios. We mean here the dispersed distribution of vehicles (like in DTNs) in where the performances of CPN will surely decrease.

In the Endpoint Protection Zone (EPZ) [22] scheme, which have addressed the problem of colluding LBS and RSU operators, lets vehicles use the same login credentials while in the same zone (devided by the protocol) in order to extend their anonymity while requesting the LBS frequently. However, in order not to expose their locations included in the BSMs, vehicles are required to stay silent while in such zones; which, as Corser et al. claim, reduces some system functionalities.

Freudiger et al. study the effect of selfish nodes on the achieved location privacy (i.e., evaluating the achieved location privacy in a selfish environment). Because changing pseudonyms may be costly in terms of network performances and overhead, nodes prefer not to participate in the pseudonym change process. The authors use a game-theoretic model (called pseudonym change game) that has helped them in modeling and evaluating the location privacy. Using the gathered results, a pseudonym change protocol (namely PseudoGame [23]) was proposed. The proposed PseudoGame protocol mainly aims to balance the privacy and the involved cost of pseudonym changes. If the selfish nodes find out that the pseudonym change cost is high and costly but their privacy level is low, they will try to cooperate in order to maximize their location privacy to a certain level.

Dynamic Mix-zone for Location Privacy strategy (DMLP) [24] is introduced by Ying et al. for the location privacy problematic. DMLP forms mix-zones dynamically according to some properties like the vehicle's predicted location and privacy requirements and/or road traffic statistics and history. DMLP is also characterized by the encryption of its messages when the vehicle is inside the Dynamic mix-zone which makes

it impossible for an adversary to find out what messages are exchanged without the use of encryption keys. Authors tested the DMLP strategy in various scenarios and they found that it provides a high location privacy level. However, if the dynamic mix-zone is dense to some extent, the encryption of messages will cause a huge overhead and it will affect negatively the VANET performances.

Boualouache and Moussaoui give the Silent & Swap at Signalized Intersection (S2SI) [25] scheme. The S2SI scheme uses two protocols: one is responsible for creating safe silent mix-zones and the other one for exchanging pseudonyms. Just like the swap protocol used in [8], performing an exchange in VANETs is not welcomed due to the implicated accountability issues which is the main obstacle that prevents the use of such a technique by standardization.

Basing on the same DMLP strategy discussed earlier, Ying et al. employ the Motivation for Protecting Selfish Vehicles' Location privacy (MPSVLP) [26] which is a strategy that deals with the selfish environment. Indeed, due to the overhead and bandwidth consuming, vehicles prefer not to participate in the pseudonym change. The role of MSPVLP is to motivate vehicles to cooperate by adding a reputation system. Each time a vehicle needs to update its pseudonym it creates a dynamic mix-zone and can by then earn reputation credits after performing a pseudonym change.

Inspired by the dynamic mix-zone concept, Ying and Makrakis propose the Pseudonym Change based on Candidate-location-list (PCC) [27] scheme. PCC forms mix-zones dynamically by taking the candidate location list (CLL) into consideration. CLL, which contains the vehicle's status information such as the ID, position, timestamp, etc., is maintained by each vehicle and it is broadcasted periodically so that the values inside the CLL will determine when and where should the vehicle perform a pseudonym change; without requesting the creation of a mix-zone, the CLL is enough to help it doing the task. The effectiveness of PCC was shown in the different simulations and it was compared to other strategies like the CPN and DMLP.

Basing on the PCS scheme [20] that exploits the social spots feature of individuals and basing on their own remark that is "the wasted opportunities between frequently meeting vehicles in other than social spots; the individual spots", Yu et al. present MixGroup [28], a scheme that benefits from both the social spots and the individual spots to enlarge the vehicles' pseudonym mixture. By letting vehicles join the available groups after entering their area, vehicles use the same group identifier gotten from the group leader to stay anonymous with the option of exchanging their own pseudonyms between themselves and validating the operation once they meet an RSU at the end of the zone. In spite of its promising simulation results, the scheme introduce high communication overhead and group leader privacy loss.

In [29], Boualouache et al. suggest the Vehicular Location Privacy Zone (VLPZ) principle for location privacy. VLPZ is similar to infrastructures like the RSU (e.g., gas stations or toll booths). They assume that the map is divided into grid cells, and that each grid cell contains at least one VLPZ responsible for the pseudonym management and change. VLPZ is formed by an entry point (they called it the router) and an exit point (the aggregator) and a limited lanes number starting from two lanes. Authors evaluated their strategy both analytically and numerically. They found that the number of vehicles and the capacity of VLPZs have an important role in enhancement of the location privacy level.

Boualouache and Moussaoui propose a pseudonym changing strategy for urban environments, the Urban Pseudonym Changing Strategy (UPCS) [30]. By exploiting the already existing signalized intersections, UPCS benefits from such places to construct one Silent Mix-zone (SM) or more. UPCS is able to either use pseudonym change or pseudonym exchange (that has accountability problems) techniques. Authors also proposed another strategy: the Traffic-Aware Pseudonym Changing Strategy (TAPCS) [31] that uses silent periods. In TAPCS, the pseudonym change is performed according to the road conditions, more precisely, the strategy implements the following parts: detecting the traffic congestion, electing an initiator (like the leader of the group that will extend the silent period), creating silent mix-zones, extending the silent mix-zone (it is performed while the road congestion is still on) and finally the detection of the traffic congestion's end. TAPCS was simulated and authors showed the effectiveness of their strategy after studying the analytic evaluation of its location privacy level. The strategy was then compared to prior strategies like CARAVAN, PCS and DMLP.

The location privacy does not always rely on the vehicles' safety messages and broadcasts but also on the use of the different available services (mainly LBSs like map services). Arain et al. suggest the use of a new strategy called the Multiple Mix-zones with Location Privacy Protection (MMLPP) [32]. Unlike traditional mix-zone strategies that do not take the map services' impact into consideration, MMLPP prevents the leakage of the vehicle's sensitive location information that may be exposed after requesting a route query; that contains the start and the end of the trip. It does so by replacing the end point of the trip by another point that is called Point Of Interest (POI), more precisely: by another nearest POI to that vehicle. Graph theory was used in MMLPP to build their multiple mix-zone model and the strategy was analyzed using real route queries provided by map services.

In [33], Eckhoff and Sommer propose and study the effect of a privacy-preserving scheme, similar to that of [18], which is safety-preserving solution with the use of non-Overlapping Time-Slotted Pseudonym Pools (referred as nO-TS-PP in the reminder of our paper). Authors perfectly described the problem of safety-privacy trade-off with a special way; that is, the claim that defeating safety by rising privacy level is not an acceptable solution, hence, the pseudonym change strategies that may confuse the adversary may also confuse safety-critical applications. Against a local passive adversary, authors investigate their nO-TS-PP performances in various scenarios. The strategy bases on a circular synchronized time-slotted system that uses pseudonyms in predefined time-ranges (time-slots) defined by the length of the pseudonym pool in addition to the validity duration of each pseudonym. Since all vehicles do change their pseudonyms synchronously; because of the GPS, the confusion of the local adversary achieves its high levels (expressed by the tracking fail rate metric in their paper).

Zidani et al. present ENeP-AB [34], an adaptive beaconing approach for privacy-preservation. Enep-AB allows vehicles to change their pseudonyms when there is a high probability to confuse the adversary. For this, vehicles set a flag-bit named Readyflag in their paper to declare the willingness to pseudonym change in the next slot time. By this, vehicles will be able to synchronize their pseudonym changes. Another feature is used by Enep-AB is the Adaptive Beaconing rate approach (E-ABRP) which let vehicles change the time, that was constant, between two successive beacons; resulting in a defending against the temporal correlation attack. However, the strategy lacks effectiveness in sparse densities especially with the high and precise location beaconing.

In the context of Vehicular Social Networks (VSNs), Babaghayou et al. [76], and motivated by the fact that the VSN user's start point (e.g., home) reveals his identity, suggested to cease beaconing while leaving the user's district and only resumes broadcasting when exiting his district (called gateway in their work). The study is also accompanied by simulations in where just a percentage of VSN users apply the scheme. The results show that the more VSN user apply the scheme, the more the adversary is confused about the one's leaving probability.

One of the factors that allows an adversary to easily track his targets is the eavesdropping coverage. Babaghayou and Labraoui, by then, deployed a Transmission Range Adjustment (TRA) [77] mechanism into two of the well-known privacy schemes; CAPS and SLOW. TRA aims at reducing the transmission range on-the-fly when vehicles are driving with low speeds (they mentioned 4 speed levels). With this technique, the adversary loses much eavesdropping capabilities as the probability of eavesdropping packets will be diminished compared to when vehicles are broadcasting with the standardized 300m safety-messages range. The authors used metrics such as the traceability and found that the traceability was dropped indeed after integrating TRA on both CAPS and

SLOW giving the option to apply such mechanisms in the upcoming privacy-preserving schemes.

Most privacy-preserving schemes rely on the pseudonymous identities and certificates but the majority of such works do neglect the pseudonym issuance and refilling phases. By this motivation, Benarous et al. [35] have developed an on-demand pseudonyms and/or certificates refiling scheme. Their scheme bases on (1) anonymous tickets and (2) challenge-based authentication. The scheme's performances against the most prominent security requirements are investigated using a set of methods and tools such as the BAN logic, SPAN and AVISPA tools that have proved the feasibility and robustness of the scheme.

Coupling Privacy with Safety (CPS) [36] is another scheme that is given by Wahid et al. to mitigate the location privacy exposing. CPS uses the principle of "talk only when necessary" meaning that vehicles, and unlike other silent period schemes as authors claim, will keep the radio on in order to fast-react when emergent events occur. The scheme mainly bases on RSU, once vehicles enter to its range, a call to a function that uses the vehicle's speed and the RSU's range to calculate "trip-time" which is an extendable estimated time for the vehicle to last in the RSU's range. Vehicles do not send BSMs while inside the range and while the timer does not expire. In spite of the less resulting overhead, the scheme is still using the principle of silent period which is not highly recommended according to the standardization.

6. Pseudonym change taxonomy

In this section, and unlike in the other surveys, we give a novel taxonomy that is based on the opportunity perspective instead of other considerations like mix-zone vs mix-context or distributed vs centralized, etc. The reason we make such a classification is due to the fact that the adversary observes and focuses on the time and/or place (i.e. opportunity) when/where the pseudonym change takes place. This, in our opinion, is more meaningful compared to other classifications. Thus, knowing how, when and where pseudonyms may change is the key towards a better pseudonym change strategy conception that deals with the adversary's thinking. We firstly start with a comparative table in order to characterize each strategy. Then, we proceed to our proposed pseudonym change taxonomy. Finally, we mention some very important concepts that absolutely affect the effectiveness of pseudonym change schemes.

6.1. Comparison of existing strategies

Each proposed pseudonym change strategy has its own features. To better understand them, a set of metrics has to be used. According to the research done in [38] and the studies of some other strategies and our own observations, we present a comparative table (Table 2) of the different strategies that emerged from 2005 until 2019 with different metrics like (a) the synchronization method (namely: Protocol, Infrastructure or GPS), whether it (2) uses the silent period or not, (3) uses the encryption or not, (4) the brought amount of overhead, (5) the conducted study's evaluation method (by simulation "S" means, analytically "A" or both "B"), (6) if the accountability mapping is still applicable by the appropriate law authority or not and (7) if it is LBS resistant or not (whether it deals with and takes the problem of compromised LBSs into account or not).

6.2. Our proposed taxonomy for pseudonym change strategies

The proposed taxonomy (as presented in Fig. 11) uses the opportunity that may be exploited by the strategy when it decides to perform a pseudonym change. Hence, we distinguish two main distinct categories: the Trigger-based and the Trigger-Free. In the Trigger-based category, the pseudonym change action is performed when a specific event occurs. The event can be:

(1) Entering a fixed zone which is predefined.
(2) When reaching an exact time (or time elapsed since the last pseudonym change).
(3) When one of the following conditions is satisfied:
   (*) When the number of neighbors reaches or exceeds a certain threshold number.
   (*) When a vehicle finds other vehicles in the vicinity that have its same status (e.g. same velocity, lane and/or group) / wanting to perform the pseudonym change, here, the vehicle will cooperatively participate with them in this action / when there is a specific distance between the two vehicles, one of the reasons it is important because the adversary will be more confused when the two vehicles change their pseudonyms at the same time while they are close (i.e., cannot easily make the prediction according to the past coordinates) / when there are other vehicles conducting the same action (e.g., changing pseudonyms synchronously while entering an intersection with another vehicle that is entering or leaving the same intersection, turning to the same direction, quitting the same parking lot, etc.).
   (*) When the vehicle's speed reaches or exceeds a specific threshold (hard trajectory and future coordinates prediction) / when the speed drops below a specific threshold (generally,

Table 2
Comparison of existing strategies according to a set of metrics.

	Year	Synchronization by	Staying Silent	Using Encryption	Overhead Cost	The Evaluation Method	Authority Mapping	LBS Resistant
CARAVAN [6]	2005	Protocol	✓	×	Low	B	✓	✓
Swing & Swap [8]	2006	Protocol	✓	✓	High	B	×	×
CMIX [10]	2007	Infrastructure	×	✓	High	S	✓	×
Mix-Context [11]	2007	Protocol	×	×	Low	S	✓	×
Slow [14]	2009	Protocol	✓	×	Low	S	✓	×
DLP [16]	2010	Protocol	×	×	Low	A	✓	×
REP [17]	2010	Protocol	×	✓	High	S	✓	×
SlotSwap [18]	2011	GPS	×	×	High	S	×	×
SPCP [19]	2011	Protocol	×	×	High	S	✓	×
SocialSpots [20]	2012	Infrastructure	×	×	Low	B	✓	×
CPN [21]	2013	Protocol	×	×	Low	B	✓	×
DMLP [24]	2013	Protocol	×	✓	High	S	✓	×
EPZ [22]	2013	Protocol	✓	×	Low	S	×	✓
MixGroup [28]	2016	Protocol	×	×	High	S	✓	×
MMLPP [32]	2018	Protocol	×	×	High	S	✓	✓
nO-TS-PP [33]	2018	GPS	×	×	Low	S	✓	×
ENeP-AB [34]	2018	Protocol	×	×	Low	S	✓	×
CPS [36]	2019	Infrastructure	✓	×	Low	B	✓	×

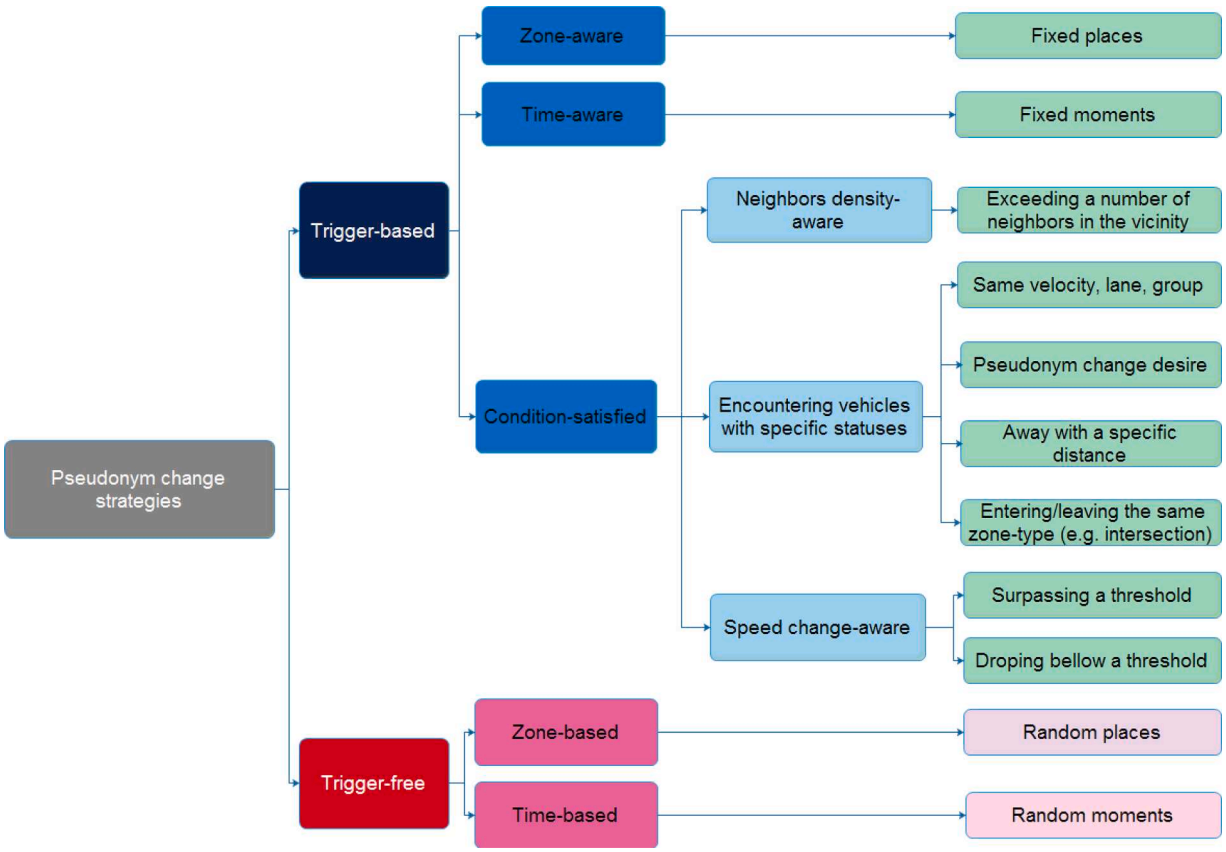

Fig. 11. The novel taxonomy of pseudonym change strategies.

in low speed environments, the number of vehicles is sufficient, hence, more cooperating vehicles).

On the other hand, in the Trigger-Free category, the notion of trigger or opportunity does not exist. As an example, the pseudonym change action, in this class, is performed according to random moments (after random times) or places (entering random road segments or zones without specification). This class is characterized by the randomization and it is better than keeping the same pseudonym along the whole trip. However, it is not based on logic and best opportunities. Hence, the adversary can, in majority of cases, predict the pseudonym change action and succeeds in linking the old and new pseudonyms.

6.3. *The changing technique considerations*

For a tough and robust privacy mechanism, each pseudonym change strategy must -delicately- take the following elements into account:

- *Silent period*: because the pseudonym change may be observable by the adversary in some, if not most, situations (e.g., non-dense scenarios, low speeds with high beaconing frequency, etc.), a silent period of time that happens between safety broadcasts is needed. This aims at confusing the adversary while he is trying to link the old and the new pseudonym basing on the time/location of the old disappeared pseudonym. The negative effect caused by the silent period mainly appears in the safety-related applications due to the exigence of the high safety beaconing frequency; the less frequency there is, the less achieved safety will be.
- *Pseudonym exchange*: in the presence of neighbors, the pseudonym change strategy gives better results because the adversary will be more confused when the vehicles change their pseudonyms cooperatively. However, the adversary can still observe and know that the pseudonym change is done. To avoid this scenario, the exchange of pseudonyms, instead of using new ones, is preferred. By this, the adversary will not be sure whether the pseudonym change was performed in the first place or not. This technique works perfectly against the *syntactic linking attack* but it is useless against the *semantic linking attack* because he still can find it by calculating the velocity of vehicles (for example) and makes a prediction of the next coordinates, hence, linking the exchanged pseudonyms. The negative effect of this technique is represented in the accountability feature (accountability mapping) loss if no mechanism is deployed, which is an important requirement for a basic VANET functioning since exchanging pseudonyms implies giving the secrete key used in signing messages to the exchanging vehicle; giving the latter the option to read the sent messages that are encrypted (or even impersonating other vehicles).
- *Pseudonym encryption*: in fact, the main reason for why the pseudonym concept is created is to send the vehicle's status in clear (a sender with its visible status). This is needed because of the VANET unique requirements in where the negative effect comes from. Because, a heavy computational process of encryption/decryption implies a low VANET functioning. Thus, if it comes into a high necessity to encrypt the vehicle's status, using light encryption algorithms would have a good impact on preventing the outsider adversaries from performing the data collection properly and ensures a basic functioning. The encryption by this, introduces a trade-off between safety and privacy.
- *Transmission strength-aware*: in the case of advanced adversaries, the transmission strength of vehicles, while performing their normal communications, plays a significant role in determining the vehicle's whereabouts, i.e., its location; that is, the triangulation technique. Even if it is not evidently apparent, the transmission strength must be taken into account while designing a pseudonym change mechanism.

Varying the strength (even if it is a hardware-related more than being software-related solution) must always be an available option.

- *All layers Identifier change (cross-layer)*: when the strategy decides to perform the pseudonym change, the vehicle's other identifiers (e.g., the mac and the IP address identifiers) must also be changed; because changing one identifier and letting the other one is absolutely useless. The negative effect in this technique is the heavy overhead caused by the repeated changing of these identifiers. In other words, affecting the VANET performances like routing by retransmitting the packets when the old identifier is no longer available. Schoch et al. [78] have studied the impacts of the frequent pseudonym changes on geographic routing protocols and have found that it affects negatively the performances of the system.
- *Manufacturer's unique fingerprint identification avoidance*: if there are no unified transmission devices, the distinguishability of each vehicle will be possible by the adversary. Thus, benefiting from this to enhance his tracking algorithms and mechanisms. As an example, if two vehicles A and B that are not created (or at least their communication devices) by the same manufacturer, the possibility of analyzing the fingerprint resulting by the transmission signals of vehicles will be feasible; leading to identifying these vehicles. Just like in the case of protocols (softwares) in any research field, the effort towards applying unified hardwares that will be used in VANETs is still challenging.
- *Tamper-Proof Device (TPD) robustness*: to ensure that any credentials (like pseudonyms) are securely stored in the OBU, i.e., it is not possible for an adversary to read, write or move these credentials, the use of TPDs is needed. However, using such techniques and embedding them in the OBU does cost compared to the creation of ordinary OBU devices. Fortunately, and in spite of the cost, most recent OBUs do integrate TPDs in their design.
- *Sensors manipulation resistance*: the defense against data manipulation and forgery is ensured by the different security mechanisms such as the use of cryptography and authentication means. However, the adversary can still jeopardize the system by physically affecting the sensors which will cause the acceptance of false data (semantically) inside the system. Performing GPS spoofing attack or affecting the thermometer sensor by external heat or freeze factors is a good example of such a problem. It is true that most drivers are not interested by these vulnerabilities, but this does not change the fact that we still may find spoilers who have different reasons beyond performing this kind of physical attacks.
- *Divided and distributed keys to different authorities*: the ability to execute delicate and crucial actions like pseudonym resolution, which leads to reveal the individual's identity, must not be entrusted to only one single organization. Hence, distributing/separating the resolution process and letting it be doable if and only if all organizations cooperate and agree on the necessity of this process must be ensured. It is a pretty good solution towards the single probable collusive (suspicious) organization.
- *Extra and exploitable information avoidance*: Some of the data, that is already standardized, included in frequently sent packets can, if well exploited, dramatically augment the unlikeability of other vehicles to be the target, resulting in determining the target with higher probability. As an example of such data we find the vehicle's size included in BSM messages [33], the reputation value of a vehicle in case the system includes reputation and the communication channel number on which the communication and the packets are sent in.

7. Discussion and future work

In the surveyed strategies, a lot of techniques (e.g. silent periods, the use of groups, mix-zones, etc.) were employed to enhance the effectiveness of pseudonym change strategies. However, the majority of these works (that used different techniques, algorithms, privacy metrics and under diverse environments) did not take the full road scenarios into consideration in both: simulation studies and analytically. Hence, they show no proof and cannot be blindly followed. Another important remark is that the adversary's strength and his available tools did not take a big attention in these studies which is very crucial in our opinion. The proposed taxonomy aims to better-characterize the pseudonym change strategies in a meaningful way. Fortunately, there is still no precise pseudonym change strategy that took the absolute attention and agreement for the location tracking problem.

This opens the door to farther possible investigations to ameliorate the future strategies. We can distinguish a bunch of challenges and future directions like: 1) the design of robust schemes for the location privacy problem basing on all road scenarios (general scheme), 2) giving more interest on the adversary's nature and abilities during the study and 3) taking the mentioned observations in the literature and our observations (hardware and software vulnerabilities) that are related to privacy and studying their effects on the achieved privacy level.

Furthermore, strategies must also be judged and evaluated according to their nature. For example, (a) when a strategy uses the silent period concept discussed earlier, its draw back must be investigated as in the case of high-speeds environments in where the risk of crashes is very high. (b) When it uses the encryption mechanism, considering the additional resulting delay and its influence is required. (c) If the used scheme gives rise to losing the accountability feature (authority mapping), it will likely not to be supported by most of the research parties. In the other part, (d) if the strategy does give a resilience against LBS adversaries collusion, it likely be welcomed and encouraged as it offers and additional security measurement. Finally, (e) the strategy has to have some tough defending mechanisms that fits the aforementioned observations and changing technique considerations given in this paper.

From here, the insights on how to develop, test and choose the privacy-preserving mechanism will be more clear; letting the future work and direction be guided upon these base remarks and observations.

8. Conclusion

Despite the large body of literature in the VANET privacy field, until now there is no exact and final solution for the location tracking problem. The proposed solutions to this problem mainly base on changing the vehicle's identifier (or the so called pseudonym). In this paper, we gave a general overview on the privacy in VANETs, its requirements and metrics, the different pseudonym change strategies and an exhaustive state of the art from the old to the recent strategies. We also presented a comparative table of a set of different pseudonym change strategies followed by our novel taxonomy that bases on the strategy's pseudonym change opportunity instead of the other considerations made in the other surveys and the literature. Then, we shed light on a bunch of significant concepts and considerations that must be taken into account during the design of any strategy. Finally, we gave some observations and future guidelines and trends for the location privacy problem in VANETs. We hope that our paper will be a fundamental axis and base for the next coming strategies and a dependable guide for the new researchers in this domain as well.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Supplementary material

Supplementary material associated with this article can be found, in the online version, at 10.1016/j.jisa.2020.102618.

References

[1] Mfenjou ML, Ari AAA, Abdou W, Spies F, Kolyang. Methodology and trends for an intelligent transport system in developing countries. Sustain Comput Inform Syst 2018;19:96–111.
[2] Fan N, Wu CQ. On trust models for communication security in vehicular ad-hoc networks. Ad Hoc Netw 2018.
[3] Sun Y, Wu L, Wu S, Li S, Zhang T, Zhang L, et al. Security and privacy in the internet of vehicles. 2015 International conference on identification, information, and knowledge in the internet of things (IIKI). IEEE; 2015. p. 116–21.
[4] Hussain R, Kim S, Oh H. Towards privacy aware pseudonymless strategy for avoiding profile generation in VANET. International workshop on information security applications. Springer; 2009. p. 268–80.
[5] Pan L, Zheng X, Chen H, Luan T, Bootwala H, Batten L. Cyber security attacks to modern vehicular systems. J Inf Secur Appl 2017;36:90–100.
[6] Sampigethaya K, Huang L, Li M, Poovendran R, Matsuura K, Sezaki K. CARAVAN: Providing location privacy for VANET. Tech. Rep. Washington Univ Seattle Dept of Electrical Engineering; 2005.
[7] Huang L, Matsuura K, Yamane H, Sezaki K. Enhancing wireless location privacy using silent period. 2005 IEEE Wireless communications and networking conference. vol. 2. IEEE; 2005. p. 1187–92.
[8] Li M, Sampigethaya K, Huang L, Poovendran R. Swing & Swap: user-centric approaches towards maximizing location privacy. Proceedings of the 5th ACM workshop on privacy in electronic society. ACM; 2006. p. 19–28.
[9] Sampigethaya K, Li M, Huang L, Poovendran R. AMOEBA: Robust location privacy scheme for VANET. IEEE J Sel Areas Commun 2007;25(8).
[10] Freudiger J, Raya M, Félegyházi M, Papadimitratos P, Hubaux J-P. Mix-zones for location privacy in vehicular networks. ACM Workshop on wireless networking for intelligent transportation systems (WiN-ITS), LCA-CONF-2007-016. 2007.
[11] Gerlach M, Guttler F. Privacy in VANETs using changing pseudonyms-ideal and real. 2007 IEEE 65th Vehicular technology conference, VTC2007-Spring. IEEE; 2007. p. 2521–5.
[12] Buttyán L, Holczer T, Vajda I. On the effectiveness of changing pseudonyms to provide location privacy in VANETs. European workshop on security in ad-hoc and sensor networks. Springer; 2007. p. 129–41.
[13] Chaurasia BK, Verma S. Optimizing pseudonym updation for anonymity in VANETs. 2008 IEEE Asia-pacific services computing conference, APSCC'08. IEEE; 2008. p. 1633–7.
[14] Buttyán L, Holczer T, Weimerskirch A, Whyte W. Slow: a practical pseudonym changing scheme for location privacy in VANETs. 2009 IEEE Vehicular networking conference (VNC). IEEE; 2009. p. 1–8.
[15] Liao J, Li J. Effectively changing pseudonyms for privacy protection in VANETs. 2009 10th International symposium on pervasive systems, algorithms, and networks (ISPAN). IEEE; 2009. p. 648–52.
[16] Song J-H, Wong VW, Leung VC. Wireless location privacy protection in vehicular ad-hoc networks. Mob Netw Appl 2010;15(1):160–71.
[17] Wasef A, Shen XS. REP: Location privacy for VANETs using random encryption periods. Mob Netw Appl 2010;15(1):172–85.
[18] Eckhoff D, German R, Sommer C, Dressler F, Gansen T. SlotSwap: strong and affordable location privacy in intelligent transportation systems. IEEE Commun Mag 2011;49(11):126–33.
[19] Weerasinghe H, Fu H, Leng S, Zhu Y. Enhancing unlinkability in vehicular ad hoc networks. 2011 IEEE International conference on intelligence and security informatics (ISI). IEEE; 2011. p. 161–6.
[20] Lu R, Lin X, Luan TH, Liang X, Shen X. Pseudonym changing at social spots: an effective strategy for location privacy in VANETs. IEEE Trans Veh Technol 2012;61(1):86.
[21] Pan Y, Li J. Cooperative pseudonym change scheme based on the number of neighbors in VANETs. J Netw Comput Appl 2013;36(6):1599–609.
[22] Corser G, Fu H, Shu T, D'Errico P, Ma W. Endpoint protection zone (EPZ): protecting LBS user location privacy against deanonymization and collusion in vehicular networks. 2013 International conference on connected vehicles and expo (ICCVE). IEEE; 2013. p. 369–74.
[23] Freudiger J, Manshaei MH, Hubaux J-P, Parkes DC. Non-cooperative location privacy. IEEE Trans Dependable Secure Comput 2013;10(2):84–98.
[24] Ying B, Makrakis D, Mouftah HT. Dynamic mix-zone for location privacy in vehicular networks. IEEE Commun Lett 2013;17(8):1524–7.
[25] Boualouache A, Moussaoui S. S2SI: A practical pseudonym changing strategy for location privacy in VANETs. 2014 International conference on advanced networking distributed systems and applications (INDS). IEEE; 2014. p. 70–5.
[26] Ying B, Makrakis D, Hou Z. Motivation for protecting selfish vehicles' location privacy in vehicular networks. IEEE Trans Veh Technol 2015;64(12):5631–41.
[27] Ying B, Makrakis D. Pseudonym changes scheme based on candidate-location-list in vehicular networks. 2015 IEEE International conference on communications (ICC). IEEE; 2015. p. 7292–7.
[28] Yu R, Kang J, Huang X, Xie S, Zhang Y, Gjessing S. MixGroup: accumulative pseudonym exchanging for location privacy enhancement in vehicular social networks. IEEE Trans Dependable Secure Comput 2016;13(1):93–105.
[29] Boualouache A, Senouci S-M, Moussaoui S. VLPZ: The vehicular location privacy zone. Procedia Comput Sci 2016;83:369–76.
[30] Boualouache A, Moussaoui S. Urban pseudonym changing strategy for location privacy in VANETs. Int J Ad Hoc Ubiquitous Comput 2017;24(1–2):49–64.
[31] Boualouache A, Moussaoui S. TAPCS: Traffic-aware pseudonym changing strategy for VANETs. Peer-to-Peer Netw Appl 2017;10(4):1008–20.
[32] Arain QA, Memon I, Deng Z, Memon MH, Mangi FA, Zubedi A. Location monitoring approach: multiple mix-zones with location privacy protection based on traffic flow over road networks. Multimed Tools Appl 2018;77(5):5563–607.
[33] Eckhoff D, Sommer C. Readjusting the privacy goals in vehicular ad-hoc networks: a safety-preserving solution using non-overlapping time-slotted pseudonym pools. Comput Commun 2018;122:118–28.
[34] Zidani F, Semchedine F, Ayaida M. Estimation of neighbors position privacy scheme with an adaptive beaconing approach for location privacy in VANETs. Comput Electr Eng 2018;71:359–71.
[35] Benarous L, Kadri B, Bitam S, Mellouk A. Privacy-preserving authentication scheme for on-road on-demand refilling of pseudonym in VANET. Int J Commun Syst 2019:e4087.
[36] Wahid A, Yasmeen H, Shah MA, Alam M, Shah SC. Holistic approach for coupling privacy with safety in VANETs. Comput Netw 2019;148:214–30.
[37] Petit J, Schaub F, Feiri M, Kargl F. Pseudonym schemes in vehicular networks: a survey. IEEE Commun Surv Tutor 2015;17(1):228–55.
[38] Boualouache A, Senouci S-M, Moussaoui S. A survey on pseudonym changing strategies for vehicular ad-hoc networks. IEEE Commun Surv Tutor 2018;20(1):770–90.
[39] Road crash statistics. Accessed: 2019-08-19, https://www.asirt.org/safe-travel/road-safety-facts/.
[40] Wasef A.. Managing and complementing public key infrastructure for securing vehicular ad hoc networks2011;.
[41] Qu F, Wu Z, Wang F-Y, Cho W. A security and privacy review of VANETs. IEEE Trans Intell Transp Syst 2015;16(6):2985–96.
[42] La Vinh H, Cavalli AR. Security attacks and solutions in vehicular ad hoc networks: a survey. Int J AdHoc Netw Syst(IJANS) 2014;4(2):1–20.
[43] Raw RS, Kumar M, Singh N. Security challenges, issues and their solutions for VANET. Int J Netw SecurAppl 2013;5(5):95.
[44] Kerrache CA, Lakas A, Lagraa N, Barka E. UAV-Assisted technique for the detection of malicious and selfish nodes in VANETs. Veh Commun 2018;11:1–11.
[45] Ari AAA, Gueroui A, Titouna C, Thiare O, Aliouat Z. Resource allocation scheme for 5G C-RAN: a swarm intelligence based approach. Comput Networks 2019;165:106957.
[46] Sun S-h, Hu J-l, Peng Y, Pan X-m, Zhao L, Fang J-y. Support for vehicle-to-everything services based on LTE. IEEE Wireless Commun 2016;23(3):4–8.
[47] Al-Sultan S, Al-Doori MM, Al-Bayatti AH, Zedan H. A comprehensive survey on vehicular ad hoc network. J Netw Comput Appl 2014;37:380–92.
[48] Lim SH, Chia YK, Wynter L. Accurate and cost-effective traffic information acquisition using adaptive sampling: centralized and V2V schemes. Transp Res Procedia 2017;23:61–80.
[49] Hartenstein H, Laberteaux L. A tutorial survey on vehicular ad hoc networks. IEEE Commun Mag 2008;46(6):164–71.
[50] Lefevre S, Petit J, Bajcsy R, Laugier C, Kargl F. Impact of V2X privacy strategies on intersection collision avoidance systems. 2013 IEEE Vehicular networking conference (VNC). IEEE; 2013. p. 71–8.
[51] Karagiannis G, Altintas O, Ekici E, Heijenk G, Jarupan B, Lin K, et al. Vehicular networking: a survey and tutorial on requirements, architectures, challenges, standards and solutions. IEEE Commun Surv Tutor 2011;13(4):584–616.
[52] Kerrache CA, Lagraa N, Calafate CT, Lakas A. TFDD: A trust-based framework for reliable data delivery and DoS defense in VANETs. Veh Commun 2017;9:254–67.
[53] Kim BH, Choi KY, Lee JH, Lee DH. Anonymous and traceable communication using tamper-proof device for vehicular ad hoc networks. 2007 International conference on convergence information technology. IEEE; 2007. p. 681–6.
[54] Mokhtar B, Azab M. Survey on security issues in vehicular ad hoc networks. Alex Eng J 2015;54(4):1115–26.
[55] Wasef A, Lu R, Lin X, Shen X. Complementing public key infrastructure to secure vehicular ad hoc networks [security and privacy in emerging wireless networks]. IEEE Wirel Commun 2010;17(5):22–8.
[56] Diaz C. Anonymity metrics revisited. Dagstuhl seminar proceedings. Schloss Dagstuhl-Leibniz-Zentrum für Informatik; 2006.
[57] Saini M, Singh H. VANET its characteristics attacks and routing techniques: a survey. Int J Sci Res 2016;5(5):1595–9.
[58] Laurendeau C, Barbeau M. Threats to security in DSRC/WAVE. International conference on ad-hoc networks and wireless. Springer; 2006. p. 266–79.
[59] Pan Y, Li J, Feng L, Xu B. An analytical model for random changing pseudonyms scheme in VANETs. 2011 International conference on network computing and information security. IEEE; 2011. p. 141–5.
[60] Eichler S. Strategies for pseudonym changes in vehicular ad hoc networks depending on node mobility. 2007 IEEE Intelligent vehicles symposium. IEEE; 2007. p. 541–6.
[61] Förster D, Kargl F, Löhr H. PUCA: A pseudonym scheme with strong privacy guarantees for vehicular ad-hoc networks. Ad Hoc Netw 2016;37:122–32.
[62] Schaub F, Ma Z, Kargl F. Privacy requirements in vehicular communication systems. 2009 International conference on computational science and engineering, CSE'09. vol. 3. IEEE; 2009. p. 139–45.
[63] Beresford AR, Stajano F. Location privacy in pervasive computing. IEEE Pervasive Comput 2003;(1):46–55.
[64] Gruteser M, Liu X. Protecting privacy, in continuous location-tracking applications. IEEE Secur Privacy 2004;2(2):28–34.
[65] Snekkenes E. Concepts for personal location privacy policies. Proceedings of the 3rd ACM conference on electronic commerce. 2001. p. 48–57.
[66] Ferrag MA, Maglaras L, Ahmim A. Privacy-preserving schemes for ad hoc social networks: a survey. IEEE Commun Surv Tutor 2017;19(4):3015–45.

[67] Ministry for Primary Industries. ETSI TR 103 415, Intelligent transport systems (ITS); security; pre-standardization study on pseudonym change management, eTSI standards; 2018.
[68] Hasrouny H, Samhat AE, Bassil C, Laouiti A. Misbehavior detection and efficient revocation within VANET. J Inf Secur Appl 2019;46:193–209.
[69] Wagner I, Eckhoff D. Privacy assessment in vehicular networks using simulation. Proceedings of the 2014 winter simulation conference. IEEE Press; 2014. p. 3155–66.
[70] Chaurasia BK, Verma S, Tomar G, Abraham A. Optimizing pseudonym updation in vehicular ad-hoc networks. Transactions on computational science iv. Springer; 2009. p. 136–48.
[71] Saxena AS, Bera D, Goyal V. Modeling location obfuscation for continuous query. J Inf Secur Appl 2019;44:130–43.
[72] Freudiger J, Shokri R, Hubaux J-P. On the optimal placement of mix zones. International symposium on privacy enhancing technologies symposium. Springer; 2009. p. 216–34.
[73] Lu R, Lin X, Shen X. SPRING: A social-based privacy-preserving packet forwarding protocol for vehicular delay tolerant networks. 2010 Proceedings IEEE INFOCOM. 2010. p. 1–9.
[74] Hoh B, Gruteser M, Xiong H, Alrabady A. Achieving guaranteed anonymity in GPS traces via uncertainty-aware path cloaking. IEEE Trans Mob Comput 2010;(8): 1089–107.
[75] Ishtiaq Roufa RM, Mustafaa H, Travis Taylora SO, Xua W, Gruteserb M, Trappeb W, et al. Security and privacy vulnerabilities of in-car wireless networks: a tire pressure monitoring system case study. 19th USENIX Security symposium, Washington DC. 2010. p. 11–3.
[76] Babaghayou M, Labraoui N, Ari AAA. Epp: extreme points privacy for trips and home identification in vehicular social networks.. JERI. 2019.
[77] Babaghayou M, Labraoui N. Transmission range adjustment influence on location privacy-preserving schemes in VANETs. 2019 International conference on networking and advanced systems (ICNAS). IEEE; 2019. p. 1–6.
[78] Schoch E, Kargl F, Leinmüller T, Schlott S, Papadimitratos P. Impact of pseudonym changes on geographic routing in VANETs. European workshop on security in ad-hoc and sensor networks. Springer; 2006. p. 43–57.

Messaoud Babaghayou is a member in the STIC Lab and a Ph. D. student at Abou Bakr Belkaid University of Tlemcen, Algeria. He received his Master of Science degree in "Networks, Applications and Distributed Systems" from the University of Laghouat, Algeria in 2016 and He is preparing his Ph.D. thesis in the domain of "Networks and Distributed Systems". Currently, his research includes "Security and Privacy in Vehicular Ad-hoc Networks".

Nabila Labraoui is an associate professor in computer engineering at the University of Tlemcen, Algeria. She received her Ph.D. in computer engineering and the HDR from the University of Tlemcen, Algeria. Her current research interests include VANETs, wireless ad hoc sensor networks, security and trust management for distributed and mobile systems, Cognitive Radio, Cloud Computing and Big data security.

Ado Adamou Abba Ari Ado Adamou Abba Ari is a Research Associate at the LI-PaRAD Lab of the University of Versailles Saint-Quentin-en-Yvelines, France and at the LaRI Lab of the University of Maroua, Cameroon. He received his Ph.D. degree in computer science in 2016 from UniversitĘ Paris-Saclay in France with the higher honors. He also received the master degree of business administration (MBA) in 2013, the Master of Science (M.Sc.) degree in computer engineering in 2012 and the Bachelor of Science (B.Sc.) degree in mathematics and computer science in 2010 from the University of NgaoundĘrĘ, Cameroon. He served/serving on several journals and conferences program and reviewing committees. Thus, he achieved the outstanding reviewer status with the Elsevier Computer Networks (IF: 3.030). Moreover he his recognized reviewer of a number of journals including IEEE Access (IF: 4.098), Journal of Network and Computer Applications (IF: 5.273), Computer Communications (IF: 2.766), Remote Sensing (IF: 4.118), Sensors (IF: 3.031), Electronics (IF: 1.764), Telecommunication Systems (IF: 1.707), Wireless Personal Communications (IF: 0.929), Sustainable Computing: Informatics and Systems (IF: 1.800), etc. His current research is focused on bio-inspired computing, Wireless Networks, IoT, 5G and the Cloud Radio Access Network.

Nasreddine Lagraa received his Ph.D. in automation from the Ecole Nationale Polytechnique, Algeria (2008). He is currently the director of the Laboratoire dInformatique et de Mathematiques, University of Laghouat, Algeria. He is teaching various courses on computer architecture, multimedia, mobile networks and network security. His research interests are: Vehicular networks, network security, decentralized control, and fuzzy and artificial neural networks. He is serving in the technical program committees of many international conferences, Wireless and Mobile Computing, Networking and Communications (WiMob), and Innovations in Information Technology (IIT).

Mohamed Amine Ferrag received the bachelor's, master's, and Ph.D. degrees from Badji Mokhtar - Annaba University, Algeria, in 2008, 2010, and 2014, respectively, all in computer science. Since 2014, he is a senior lecturer with the Department of Computer Science, Guelma University, Algeria. His research interests include wireless network security, network coding security, and applied cryptography. He serves on the Editorial Board of several International peer-reviewed journals such as the IET Networks (IET), the International Journal of Information Security and Privacy (IGI Global), the International Journal of Internet Technology and Secured Transactions (Inderscience Publishers), and the EAI Endorsed Transactions on Security and Safety (EAI). He has served as an Organizing Committee Member (the Track Chair, the Co-Chair, the Publicity Chair, the Proceedings Editor, and the Web Chair) in numerous international conferences.