Received: 14 May 2023 | *Revised:* 25 July 2023 | *Accepted:* 18 August 2023
DOI: 10.37917/ijeee.20.1.3 *Vol. 20 | Issue 1 | June 2024*

Iraqi Journal for Electrical and Electronic Engineering
Review Article

Open Access
IJEEE University of Basrah College of Engineering

Privacy Issues in Vehicular Ad-hoc Networks: A Review

Zahra K. Farhood*[1], Ali A. Abed [1], Sarah Al-Shareeda[2]
[1]Department of Computer Engineering, Collage of Engineering, University of Basrah, Basrah, Iraq
[2]Department of Electrical and Electronics Engineering, University of Bahrain, Isa Town, Bahrain

Correspondance
*Zahra K. Farhood
Department of Computer Engineering,
College of Engineering, University of Basrah, Basrah, Iraq
Email:pgz.zahra.farhood@uobasrah.edu.iq

Abstract
Vehicle Ad-hoc Network (VANET) is a type of wireless network that enables communication between vehicles and Road Side Units (RSUs) to improve road safety, traffic efficiency, and service delivery. However, the widespread use of vehicular networks raises serious concerns about users' privacy and security. Privacy in VANET refers to the protection of personal information and data exchanged between vehicles, RSUs, and other entities. Privacy issues in VANET include unauthorized access to location and speed information, driver and passenger identification, and vehicle tracking. To ensure privacy in VANET, various technologies such as pseudonymization, message authentication, and encryption are employed. When vehicles frequently change their identity to avoid tracking, message authentication ensures messages are received from trusted sources, and encryption is used to prevent unauthorized access to messages. Therefore, researchers have presented various schemes to improve and enhance the privacy efficiency of vehicle networks. This survey article provides an overview of privacy issues as well as an in-depth review of the current state-of-the-art pseudonym-changing tactics and methodologies proposed.

Keywords
Privacy, Safety, VANETS, Silent Periods, Mix Zones, Pseudonym Changing

I. Introduction

Vehicular Networks (VANET) is a special type of Mobile Ad-hoc Network (MANET) that has gained researchers' attention. In VANET, each vehicle (e.g., car, bus, bicycle) represents a node, and a group of vehicles represents a group of nodes that communicate with each other or with the Road-Side Units (RSUs) by sending beacons [1]. All vehicles in the network have a set of sensors or electronic devices, such as an On-Board Unit (OBU), micro-sensors, Global Positioning System (GPS), and embedded system [2], which make them smart and enable communication within the network. Therefore, in VANET's safety applications, messages called Beacon Messages (BMS) are transmitted continuously at a frequency of 1-10Hz and can be received by any person or vehicle within the network communication range of 300-1000 meters. These messages increase traffic efficiency and maintain public safety by providing warnings of collisions, changing the path, or information related to traffic jams or accidents. Additionally, these messages contain information about the speed and location of the vehicle [3]. As VANET is crucial for achieving safety, it faces many security challenges. There are various attacks that the network can be exposed to, such as alteration attacks, Denial-of-Service (DoS) attacks, Sybil attacks, replay attacks, obstacle attacks, and message attacks [4]. Attackers may attempt to track vehicles for specific purposes, such as stealing, causing harm to an organization, or sending fake, old, manipulated, or modified messages [5, 6]. Regarding private information, messages contain location, speed, and direction, threatening the driver's privacy. Attackers can collect and analyze these messages to identify the driver's location by linking information transmitted by the vehicle at different periods [5]. Furthermore, all vehicle messages must be authenticated before processing them to ensure that any privacy issues are addressed to the satisfaction of users in the network.

Authentication occurs at two levels: the node level, which is called node authentication, and the message level, which is referred to as message authentication. At the message level, the message contains a special signature by the sending party, which is verified by the receiving devices or the receiving party [6]. Thus, the privacy of vehicles is a complex and challenging issue that must be solved.

To address this problem, many researchers have proposed schemes in which vehicles use pseudonyms or fake names instead of their real names in communicating or sending messages to other vehicles within the specified communication range. These schemes also allow official authorities to distinguish the vehicle's real identity from the pseudonym, enabling them to track the vehicle and hold the driver accountable for any bad behavior [6]. Hence, this article presents a study on VANETs and privacy issues and reviews current state-of-the-art pseudonym-changing tactics and methodologies proposed to maintain the privacy of vehicles. The remaining sections of this article are structured as follows. Section II. describes the VANET network. Section III. lists the needed security and privacy measures in VANETs. Section IV. presents a state-of-the-art comprehensive survey of the privacy preservation schemes literature highlighting their strengths and weaknesses. Finally, Section V. concludes the article with future work directions.

II. VANETs: An Overview

The world's population continues to grow, and so does the number of vehicles, which is expected to surpass two billion by 2040; this increase in vehicles leads to traffic congestion, accidents, and, unfortunately, loss of life, as accidents are now the fifth leading cause of death [7]. This is where VANETs come into play, as it aims to reduce these issues. VANET is a specialized type of MANET designed for vehicles. However, it has several advantages over traditional MANET, including a high degree of vehicle movement, which can reach up to 100 meters, and the ability to adapt to changes in the network topology based on the current situation [8]. VANET inherits many properties from MANET but also has unique features, including [8]:

- No power restrictions due to large battery power and the possibility of recharging.
- High-speed vehicle movement leads to rapid topology changes, affecting routing algorithms, congestion control, and other functions.
- Powerful CPUs for fast calculations.
- Density is constantly changing due to rapidly changing topology.
- Movement is restricted by roads, making it more easily predictable.
- Vehicles communicating with each other enhance safety and driving experience.
- Exposed to security challenges due to wireless transmission.

A. VANET's Architecture

VANET has a communication architecture designed specifically for vehicles, where the vehicle serves as the main component equipped with a set of electronic devices and sensors. One of these devices is the OBU, which is responsible for wireless transmission and facilitating communication between vehicles using the Wireless Access in Vehicular Environment (WAVE) protocol. The OBU enables data exchange between elements of the VANET. Additionally, the vehicle is equipped with an Application Unit (AU) responsible for communication between vehicles and other services in the network [5]. In VANETs, various components are involved in communication, including cell phones (sometimes referred to as pedestrians), RSUs fixed on the roadside multiple times, and servers of different types (authentication, location, and application servers). Communication in VANET occurs through several types, as shown in Fig. 1 and listed below.

- Vehicle to Vehicle (V2V): performs direct communication between vehicles without using the RSUs. This type is mainly used for security, safety, and distributed applications.
- Vehicle to RSU (V2R): RSU is set up along the side of the road, and it is from this point that the signal is broadcast. Each vehicle will get the signal for communicating with other vehicles from a nearby RSU.
- Vehicle to Everything (V2X): Every vehicle can connect to the traffic system, which consists of other vehicles and RSU.
- Roadside to Roadside Units (R2R): RSU connects with other RSUs in the network in this communication.

B. VANETs' Communication Standards

The Dedicated Short Range Communication (DSRC) standard, which enables all V2R and V2V communications up to 1km and requires a data rate of up to 27 Mbps, was first suggested by the Federal Communication Commission (FCC) in 1999. To precisely satisfy the requirements of VANET, such as self-organization, self-configuration, excellent mobility, and active topology, DSRC was developed. DSRC uses a

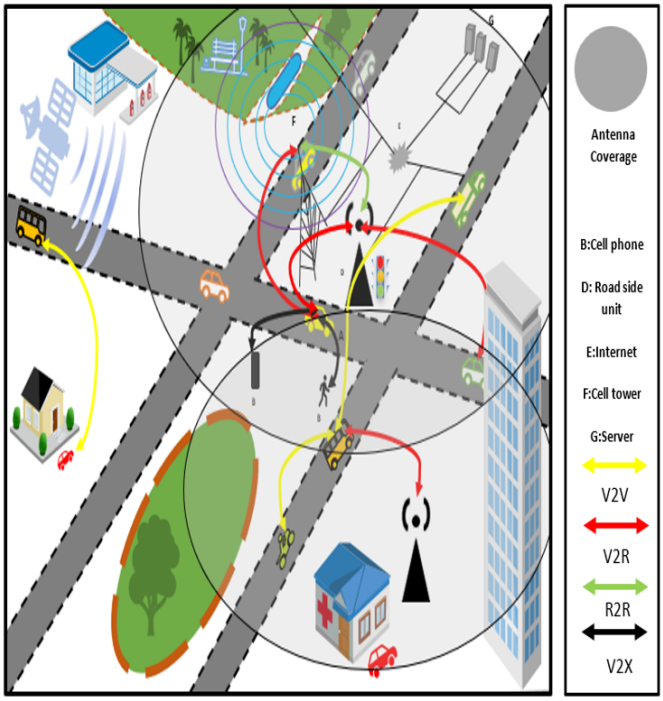

Fig. 1. VANETs architecture and main elements.

30MHz bandwidth in Japan and Europe and a 75MHz bandwidth in the United States in a 5.9 GHz (5.850 - 5.925 GHz) frequency range, respectively. Figure 2 shows the guard band, one 10MHz Control Channel (CCH), and six 10MHz Service Channels (SCHs). Only safety-related communications are sent through the CCH, which carries the most crucial beacons and alerts. The two channels closest to the spectrum's edge are retained for potential use and use in certain applications, such as advanced collision avoidance and public safety. On the other hand, SCHs are employed for normal communication and residual applications in safety and non-safety applications. Using the DSRC, two SCHs may be combined to create 20MHz channels to sustain 54Mbps high data speeds. DSRC is often referred to as WAVE. The DSRC protocol, which employs the IEEE 802.11p standard for communication via wireless networks, is necessary for nodes in this scenario to connect. The DSRC architecture shown in Fig.3 employs many protocols, one for each tier. The PHY and MAC levels are covered by the IEEE 802.11p protocol, whereas the top layers interacting with specific facilities directly are covered by the IEEE 1609.2, 1609.3, and 1609.4 protocols. In particular, they are shown in Table I [9, 10].

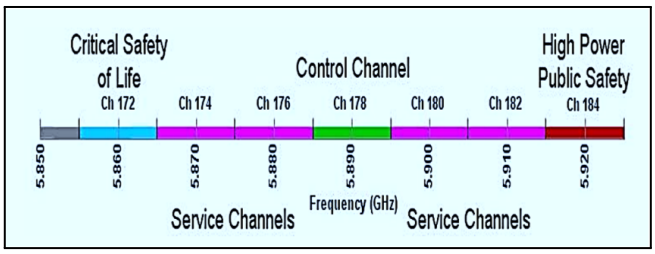

Fig. 2. DSRC spectrum band and channels in the US [10].

TABLE I.
VANETs DSRC Protocols [10].

Standard	Explanation
IEEE1609.1	Provide OBUs access to outside resources to improve their capacity for computation.
IEEE1609.2	WAVE secure messaging formats.
IEEE1609.3	WAVE (routing and addressing tasks) is a network layer.
IEEE1609.4	Adds multi-channel functionality to IEEE 802.11p specification.
IEEE 802.2	The link layer's logical link control (LLC).
IEEE 802.11p	Management of the MAC and physical layers and an upgrade to an IEEE 802.11 standard that enables the WAVE protocol.

C. VANET's Applications

Many applications have been developed that enable drivers and users in the VANET environment to access information

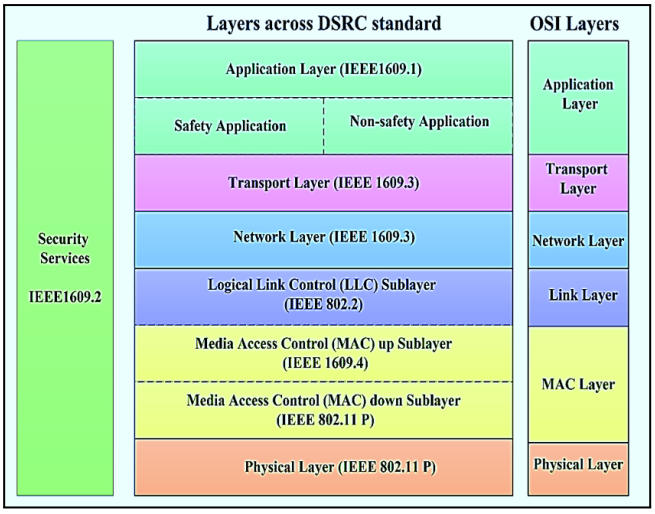

Fig. 3. Comparison between DSRC and the OSI model [9].

using technologies integrated into the OBU [11,12]. The most significant applications are outlined below:

1) Safety Applications

These applications play an important role in assisting drivers by providing road information. The vehicle safety communication association has identified several key safety-related applications, including speed measurement, lane change detection, pre-collision detection, traffic sign violation detection, activation of the electronic brake light, identification of stop sign movement, and left turn assistance. Utilizing these safety applications on highways is crucial to reducing road accidents and fatalities. They offer essential information about traffic and road conditions, enabling drivers to avoid collisions [13]. Several widely recognized safety applications are being explored, designed to mitigate the risk of traffic accidents caused by human error or obstacles.

- The Lane Change Assist [11]: This application measures vehicle distances and calculates gaps between neighboring vehicles. It alerts the driver regarding potential collisions during lane changes or when vehicles get too close. Its goal is to reduce accidents, especially in blind spots, while changing lanes.
- Head-on Collision Warning [12] is intended to provide drivers moving in the other direction with early notice.
- Intersection Collision Warning [5]: The system warns the driver when there is a high likelihood of colliding with another vehicle at a traffic intersection.
- Cooperative Collision Alerts: These applications ensure that when a vehicle slows down or stops due to curves or downhill slopes, it actively communicates this information to the following vehicles. This timely notification enables other drivers to react promptly, adjust their driving, and prevent potential collisions.

2) Infotainment Applications

They are divided into entertainment and traffic effectiveness applications. This group of apps primarily aims at serving drivers and their passengers with a high level of infotainment and traffic management, such as speed management, cooperative navigation, worldwide internet access, and other non-safety applications [5].

III. Security and Privacy in VANETs

A. VANETs' Security

Protecting VANET connections is crucial, as attacks can have catastrophic consequences for human lives and the economy. Therefore, several security requirements must be met [14]:

- Authentication: Nodes must be able to determine the reliability of message senders, preferably using rapid authentication methods to minimize delays.
- Availability: Networks must remain accessible for sending and receiving safety-related messages despite high mobility and potential security attacks.
- Integrity: Hostile nodes must not be able to alter sent messages, and verifying message accuracy is essential for authentication.
- Confidentiality: Only authorized members should be able to access and decode message contents, although encryption is not recommended for safety-related messages due to added delay.
- Privacy and Anonymity: The driver's private information must remain protected against unwanted access, and preventing unauthorized parties from connecting message identification to the sender's real identity is essential for privacy.
- Traceability: Safety messages must be traceable back to their source, with access to this capability limited to approved organizations such as the Law Enforcement Authority.
- Revocability: Bad nodes must be removed from the network, with the appropriate authorities making decisions using centralized or distributed revocation methods.
- Non-repudiation: This involves not contesting the integrity of a message's contents or the identity of the sender of the message. Thus, non-repudiation is a crucial need for the trustworthy usage of VANET.

From a security standpoint, vehicular networks include three primary architectural elements as shown in Fig. 4 [15]:

A) Trusted Third Parties (TTPs): These parties manage the vehicles' licenses, registrations, and identification documents. They also have adequate storage devices and powerful servers to carry out these tasks.

B) RSUs: fixed devices on the roadside that serve as TTPs. If the TTP identifies a hostile entity under the control of an attacker, it may revoke the RSU. Vehicles can be considered malicious entities, similar to RSUs, and exchange information with each other, RSUs, and TTPs (via RSUs).

C) Vehicles: are the core component of VANET and can exchange information with each other, RSUs, and TTPs (via RSUs). Vehicles can also be considered malicious entities like RSUs.

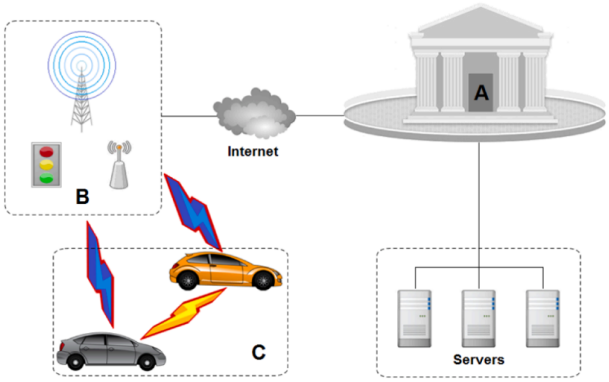

Fig. 4. VANETs' three primary architectural elements from a security perspective.

1) Attackers and Attack Types

Understanding the characteristics and components of the environment in which the vehicle is operating is crucial before addressing the actual issue. There are various types of adversaries or attackers in VANET [5]. These attackers can be classified into the following categories:

- "Actively" (Active or Passive): An active attacker alters, deletes, or creates new messages to actively disrupt the network's performance. In contrast, a passive attacker listens to the exchanged messages without directly causing harm to the network.
- "Behaviorally" (Malicious or Rational): The first type is a malicious attacker who employs various techniques to carry out damaging assaults that harm the network. In contrast, the rational attacker seeks personal gain from their attack, making their behavior more likely than that of malevolent attackers.
- "Locationally" (Outsider or Insider): Insiders, authorized associates of VANETs, pose a significant threat by launching attacks on the network's infrastructure. Outsiders, unable to directly interact with the network, pose a lesser threat than insiders.
- "Proprietarily" (Globally or Local): Global adversaries have extensive influence over network radio stations, swiftly identifying moving objects within a designated region of interest. Local adversaries have limited influence over network elements, restricting the region they can exploit.
- "Occasionally" (Perpetual and Temporal): Observers can be perpetual or temporal. Perpetual observers pose a greater threat as they accumulate information by constantly listening in on communications. Temporal observers only listen to specific moments based on their interests, goals, and rewards.
- "Fixed vs. Dynamic": The adversary's listening positions can be static or dynamic. Dynamic positions require careful processing, especially for tracking specific nodes, while static stations require minimal maintenance. The effectiveness of each type depends on the number of nodes available for monitoring the region.

The shared medium in VANET makes it easy for these attackers to launch various attacks. Some of the most popular attacks that concentrate on location privacy include:

- Denial of Service (DoS): The attacker renders the targeted service unusable, such as the service that supplies pseudonyms to protect vehicles' anonymity.
- Eavesdropping attack: The attacker listens in on wireless packets transmitted across the shared media, which can lead to more serious attacks based on the collected data.
- Identity revelation: The attacker exposes the position of nearby nodes, often after infecting them with a virus, to learn their exact location. This attack violates the security of VANET nodes.
- Location tracking: The attacker can read the position of a target vehicle from safety broadcasts and use the collected data for nefarious purposes.

- Malware attack: VANET is susceptible to malware infection, which can reveal sensitive and private information.
- Man-in-the-Middle attack: The attacker eavesdrops on a conversation between two nodes and pretends to be one of the parties, potentially obtaining personal information.
- Masquerade attack: The attacker poses as an authenticated node to extract privacy-related data that would be otherwise impossible to obtain without authentication.

Making informed decisions and implementing effective countermeasures relies heavily on identifying the type of adversary and the attacks they may carry out [2].

B. VANETs' Privacy

Privacy is considered a critical security criterion in VANET due to the potential consequences if it is not maintained. Several privacy models include content-oriented privacy, interest privacy, backward privacy, and location and identification privacy. In VANET, location and identity privacy is crucial to prevent unauthorized parties from learning the driver's real identity. Only authorized authorities should have access to this information, except in cases where law enforcement agencies require it. On the other hand, location privacy is the ability to keep a person's current and historical position hidden from unauthorized entities. Since location services may compromise privacy, it is important to provide vehicles with the option of being invisible to ensure their safety [16]. According to Schaub et al. [17], the following conditions must be met to ensure location and identity privacy:

- Minimal disclosure: During communication, only the necessary information should be disclosed, and requirements should be kept to a minimum to ensure VANET functions at their basic level.
- Anonymity: The sender's identity must remain anonymous, and accountability must be maintained through anonymous credentials and connections to the sender's real identity.
- Unlinkability: It is essential to ensure no connection exists between "items of interest" in VANET, such as people, cars, credentials, and messages. This is achieved through a distributed resolution authority that divides the power to identify a person between multiple authorities, preventing a single authority from being taken over or corrupted.
- Complete forward privacy: the resolution process of one credential to identity should not reveal information affecting the user's other credentials' capacity to remain unlinked.

In this sense, vehicles rely on such anonymity models in VANET, and one way to improve the models is through the deployment of pseudonym-based schemes and standardizing pseudonym management with the "ETSI TR 103415" standard [11].

1) Pseudonym-based Schemes

Vehicles must broadcast their identification, position, velocity, and other relevant information in VANETs. However, an adversary can use eavesdropping to identify the driver by tracking the vehicle's position. Using multiple pseudonyms instead of static identities improves privacy and makes tracking and identifying a vehicle harder. OBUs store collections of pseudonyms, which greatly enhance drivers' privacy [11]. Pseudonyms can be created using public cryptography, group signatures, and identity-based encryption. Asymmetric public cryptography-based pseudonyms are efficient but computationally expensive. Group signature systems eliminate the need for additional authorities but require a trusted group manager. Identity-based encryption uses a node's unique identification but requires a trusted centralized authority to handle private keys [16]. In general, the abstract pseudonym lifecycle, shown in Fig. 5, must be considered to provide vehicles with pseudonyms and ensure the proper functioning of the VANET system. These stages are as follows [11]:

- Pseudonym issuance: To communicate within VANETs, the vehicle's OBUs must be authenticated using the Vehicle Identifier (VID), a pre-installed, long-term signed certificate. Before obtaining legitimate pseudonyms, the vehicle must undergo an authentication stage. The vehicle can contact the authority responsible for issuing pseudonyms through its VID if necessary.
- Pseudonym Usage: Once a collection of pseudonyms is gathered, a vehicle can utilize one for regular broadcasts and communications, resulting in identifying the vehicle's VID through pseudonyms. However, this can greatly compromise the individual's privacy.
- Pseudonym Change: Changing pseudonyms is necessary because using the same one might always result in serious security problems like the location monitoring that has already been mentioned. However, to maintain the performance of the VANET system, this change must adhere to a set of rules. Changing a pseudonym at the wrong time or place will consume the existing pseudonyms and add more overhead when requesting new ones.

- Pseudonym Resolution: When a law enforcement agency needs to find out who sent a communication, it asks the agency that issued the pseudonym for a pseudonym resolution procedure. The causes may vary depending on the circumstances, but they have no bearing on the request's outcome, which is obtaining the VID. As a result, the individual's privacy is greatly compromised.
- Pseudonym Revocation: In the event of a rogue node, we discuss how occasionally a vehicle may not utilize its authentication appropriately. Suppose one or more cars inside the system exhibit illegal activity. In that case, the monitoring authority, as the law authority, may go on to the pseudonym-resolving procedure to determine the precise sender's identity. It then cancels its alias. It must also be possible for the vehicle to participate in the VANET network using one of its other stored pseudonyms. Therefore, it is necessary to implement a system for discovering all of the vehicle's pseudonyms and canceling them.

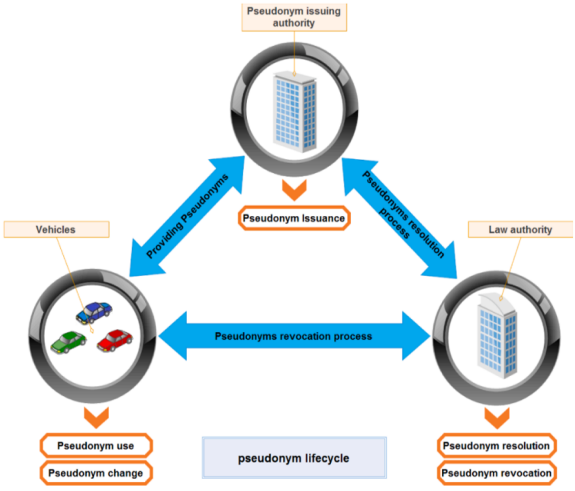

Fig. 5. Steps of the pseudonym life cycle.

To use pseudonyms in VANETs, certain conditions must be met:

- Each vehicle must always have a unique pseudonym.
- Fresh pseudonyms should be readily available.
- Pseudonyms should not be used indefinitely to prevent location-tracking attacks.
- If a vehicle changes its pseudonym, all other recently used identifiers in its communication layers stack must also change.
- Frequent changes and abuse of pseudonyms must be prevented to avoid safety issues like Sybil attacks and excessive overhead.
- While pseudonym change can help with user privacy, it also raises safety concerns. Silent periods can make vehicles invisible to trackers and nearby vehicles, leading to tricking. According to the "ETSI TR 103415" standard, trading using pseudonyms across vehicles jeopardizes user safety. It represents a trade-off between safety and privacy.

Even when these conditions are met, experienced attackers can connect the pseudonym to the real identity by analyzing the vehicle's trajectory and trip history using the following two recognition techniques [18]:

1. Radio-based Recognition Techniques: Eavesdroppers benefit from the vehicle beaconing function [19], which transmits safety messages frequently, allowing them to collect and store information about the vehicle's successful locations and corresponding pseudonyms used during travel. Here are two examples of such techniques:
   - Syntactic connecting attack: The adversary can monitor all cars through their safety signals via wireless shared media. If a vehicle changes its pseudonym, the opponent compares the previous and current pseudonyms to determine which vehicle has changed its identity. The attack is stronger when the pseudonym changes are not synchronized. If pseudonym changes are synchronized, the attack is futile; see Fig. 6 for an illustration of this attack. *PSD* represents pseudonym, $[A,T]$ represents [Pseudonym value, corresponding time], and t represents the interval between two instances. One vehicle changed its pseudonym from 178 to 230.

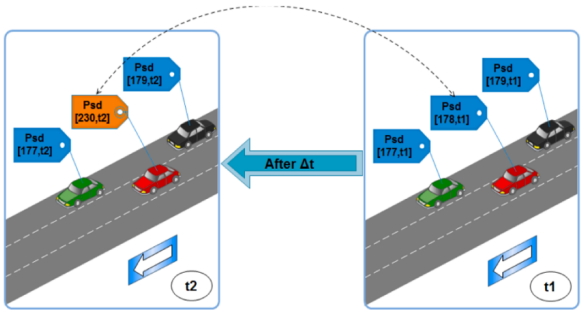

Fig. 6. Connecting modified pseudonyms from $t1$ to $t2$.

- Semantic link attack: This attack also uses safety message information. Even with simultaneous pseudonym changes, adversaries can match new pseudonyms with their corresponding old ones because the safety messages contain the vehicle's location and speed, which help the attacker predict the future location of the vehicle. Additionally, the more frequently the beacon messages are sent, the more accurate the attacker's estimation becomes. This attack is more dangerous than a connecting attack. Fig. 7 illustrates how the adversary can still match new and old pseudonyms even when the pseudonyms change simultaneously. The attacker predicts the next position of the vehicle using its x and y coordinates, timestamp, and velocity from the beacon signals. Fig. 8 demonstrates how the attacker anticipates the future positions of three vehicles $(V1, V2, and V3)$ and matches their new and old pseudonyms.

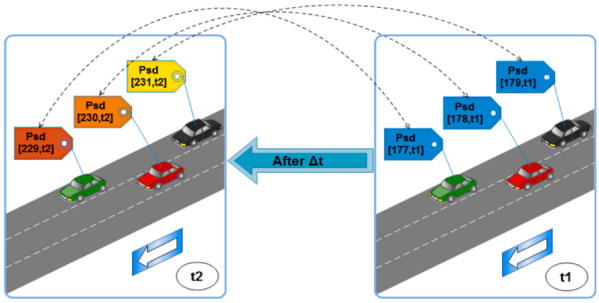

Fig. 7. Prediction algorithms linking updated pseudonyms simultaneously.

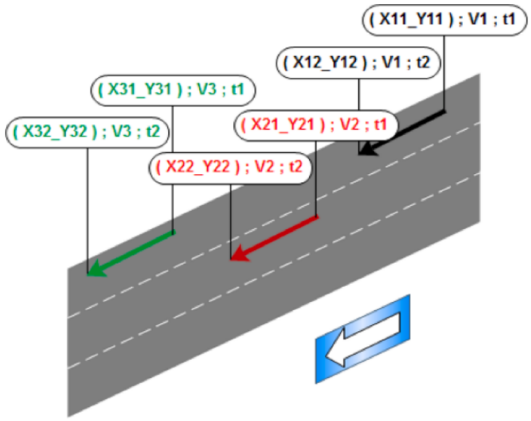

Fig. 8. Semantic linking attack utilizing information from a beacon broadcast by three vehicles.

2. Identifying License Plates Techniques: License plate recognition systems use image processing algorithms and cameras to read license plates, making them more efficient than radio-based methods. However, these systems are expensive to develop and implement, making it challenging to cover large areas. The aim is to collect unique license plate numbers and analyze vehicle movements. Fig. 9 shows a license plate recognition system near an intersection, utilizing two cameras and a drone for long-distance tracking if necessary.

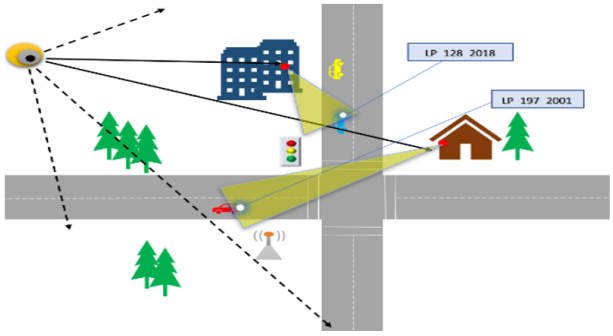

Fig. 9. System for recognizing license plates.

As we can see, a simple change of these pseudonyms is insufficient, and adversaries can still use various methods to correlate these pseudonyms and even identify the real identity of the driver. Therefore, advanced efforts have been exerted in the literature to address location privacy as discussed in Section IV. .

IV. Location Privacy Preservation: Literature

Over the past 20 years, many schemes have been presented to address privacy preservation in VANETs. Sampigethaya et al. [18] proposed the CARAVAN approach, which employs the grouping technique and uses silent intervals between pseudonym changes to increase vehicle privacy. However, this method is only applicable in the case of a probe vehicle, as other vehicles communicate constantly, and safety applications require high-frequency broadcasts of safety messages. Huang et al. [20] examined the silent period notion and demonstrated that adopting silent periods, which may be used geographically or temporally (at a variable duration or a fixed location), significantly improves the privacy of nodes. The Swing protocol, proposed by Li et al. [21], aimed to enhance the number of cars that change their pseudonyms at the same time, but the responsibility requirements (revocation, pseudonym resolution, and identity management) of VANETs make the exchange procedure inappropriate. Therefore, the

infrastructure at every pseudonym exchange activity will be crucial to the swap process, assuming the exchange feature is enabled. This is due to the need for synchronization in the user-centric strategy, mostly based on the vehicle's desire. Sampigethaya et al. [22] presented the AMOEBA system, which utilizes group navigation to allow cars to form a group and only the group leader interacts with base station on behalf of other members, avoiding duplicate information and enabling a long period of silence. However, the scheme heavily relies on the idea of a group, making it vulnerable to privacy violations if one group member is compromised.

Another approach, CMIX [23], used mix-zones and encryption to protect location data. This technique involves several challenges, including minimizing overhead and synchronizing key management amongst RSUs to allow only one symmetrical key inside the system. Gerlach and Guttler's Mix-context technique [24] used a flag in beacon messages to allow synchronous pseudonym changes when triggered. Beresford et al. proposed using mix-zones to change pseudonyms and confuse adversaries. Buttyan et al. [25] assessed the effectiveness of mix-zones for VANETs, and Freudiger et al. [26] investigated the influence of mix-zones on location privacy. Chaurasia and Verma [27] found that a vehicle's previous communications affect its anonymity within an anonymity zone and suggest a heuristic method to maximize anonymity with the fewest pseudonym changes.

The SLOW technique, which stands for Silent at LOW speed, is a pseudonym-changing technique introduced by Buttyan et al. [28]. This technique causes vehicles to stop sending safety alerts when their speed falls below a certain threshold. While this tactic eliminates the adversary's ability to monitor the target while quiet, it also stops the certified beacons that each vehicle has installed, which is not always appropriate. For instance, quick braking at low speeds is an excellent example of the value of safety signals. Therefore, it might be preferable to lower the beaconing frequency instead of halting it. Liao and Li [29] proposed a pseudonym change approach that uses the synchronous pseudonym change algorithm to increase the number of vehicles that change their pseudonyms concurrently. This approach takes advantage of triggers, such as the vehicle's state, to provide strong synchronization among cars with similar statuses. After modeling and contrasting their approach with other fundamental pseudonym change strategies, they discovered that their synchronous pseudonym change algorithm achieved higher privacy than the others. They did this by using parameters such as traffic density and penetration rate. However, the selected precision may cause the same trigger to behave differently.

Lu et al. [30] used SPRING, a protocol designed for delay-tolerant networks, to prevent packet tracking and deliver packets in sparse networks after hanging onto them for a time before sending them. It is also possible to use RSUs in this protocol as a mix-zone. Using a modified Java simulator, they examined the protocol's efficiency against black-hole (also known as grey-hole) assaults and discovered that it could withstand such attacks. Song et al. [31] presented a Density-based Location Privacy technique (DLP). In DLP, each car knows its immediate surroundings, the nearby vehicles' count or density. The key factor affecting vehicle density is a parameter that serves as a threshold for pseudonym changes. Using density zones consisting of one intersection of four road sections per zone, they demonstrated that the likelihood of an adversary carrying out a successful tracking assault decreases as these two parameters increase. Wasef and Shen [32] used the Randomized Encryption Periods (REP) technique to ensure that a pseudonym change is efficient and concealed from the adversary. This technique allows all legal vehicles to have a group of symmetric key encryption that enables them to supply a single shared secret key. When a vehicle wants to change its pseudonym, it collaborates with its neighbors to create an encryption zone using a shared secret key. Because the resulting REP is created on demand rather than at fixed locations like junctions, it can be seen as a dynamic CMIX zone. The lack of RSUs makes this technique more intriguing and promising than CMIX. However, at high densities, the encryption process can cause added overhead and affect VANET's performance.

Hoh et al. [33] proposed a novel metric called time-to-confusion and an uncertainty-aware route cloaking algorithm to address privacy concerns related to target detection and home identification. They evaluate their approach using GPS data collected from the real world. The proposed method eliminates GPS position traces that allow attackers to identify their targets, especially in low-population areas, accurately. The program also addresses situations where vehicles travel in opposite directions, eliminating their locational traces. Ishtiaq et al. [34] demonstrate how wireless tire inflation monitoring systems can compromise location privacy. They install four tire pressure sensors wirelessly on each car, and an attacker can track the vehicle's location by eavesdropping on the signals transmitted by these sensors from around 40 meters. This technique does not use cryptographic measures, thus making privacy vulnerable. The study emphasizes the importance of safeguarding vehicle privacy to prevent adversaries from exploiting privacy issues to conduct effective tracking. Eckhoff et al. [35] proposed Slotswap, a privacy enhancement method that uses a pool of time-slotted pseudonyms. The vehicle changes its pseudonym for each time slot, making it difficult for various authorities, including the Certificate Authority (CA), to determine the vehicle's identity. However, privacy must be subject to certain conditions, and law enforcement agencies must always have access to identity resolution. The

authors highlight the idea of pseudonym exchange between vehicles that wish to modify their pseudonyms.

Pan et al. [36] analyzed the efficiency of the Random Changing Pseudonyms (RPC) system. They simulate and compare this technique using the uniform discrete and age-based distribution (which refers to pseudonym use time). They find that the age-based distribution does not provide as good outcomes for location privacy as the RPC under the uniform discrete distribution. Pan and Li [37] proposed a Cooperative Pseudonym chaNge mechanism (CPN) that utilizes the number of neighbors as triggers for synchronized pseudonym changes, improving location privacy. However, CPN is unsuitable for scenarios with a scattered distribution of vehicles. Emara et al. [38] presented the Context-Aware Privacy scheme (CAPS), which minimizes pseudonym usage when monitoring is simple and determines the required stillness period for the confusion of trackers. In contrast, Al-ani et al. [3] introduced the Safety-Related Privacy Scheme (SRPS) to reduce the negative effects of a pseudonym-changing silence period on VANET's safety applications. Babaghayout et al. [39] equipped CAPS and SLOW with a Transmission Range Adjustment mechanism (TRA) to decrease the eavesdropping capabilities of adversaries and increase location privacy. Additionally, WHISPER utilizes a shift in transmission power to maintain or enhance location privacy [40]. Lastly, Babaghayout proposed the OVerseer Role vehicle (OVR) scheme, which uses regular cars as overseers to increase location privacy when public vehicles are insufficient [41].

These techniques, including silence periods, group activities, and mix-zones, were utilized in the examined strategies to enhance privacy. However, most of these methods do not consider all road scenarios in simulation studies or analysis and do not consider the adversary's strength and tools. Therefore, they can only be unquestioningly accepted with evidence. Although privacy in VANETs has been thoroughly researched, only a few VANET simulators have been used for evaluating privacy systems based on different assumptions and mobility models, making determining their effectiveness difficult. Emara et al. [42] introduced the PRivacy EXTension (PREXT) privacy extension for the Veins framework to simplify comparing and assessing these privacy strategies. PREXT accurately represents the network layers of IEEE 1609.4 DSRC/WAVE and 802.11p and vehicular mobility provided by the SUMO traffic simulator. PREXT enables seven privacy schemes to be tested in a realistic VANET setting instead of using simplistic scenarios. Supporting privacy policies within a VANET simulator would encourage authors to consider privacy restrictions when designing and evaluating network and application protocols. The proposed extension facilitates assessing privacy impacts on different applications or communication protocols, providing the flexibility to study, compare, and evaluate their security capabilities.

V. Conclusion and Future Work

Despite significant efforts in vehicular network privacy, the challenge of location tracking still needs to be solved. Our study comprehensively examines privacy concerns in vehicular networks, covering tactics and essential considerations for developing privacy-preserving methods. This study surveys all the available contemporary privacy schemes and identifies their strengths and weaknesses. Since no widely accepted method exists to address location tracking, further research is required to create a reliable architecture suitable for all highway scenarios. The scheme must address the capabilities of potential adversaries and software and hardware vulnerabilities.

Conflict of Interest

The authors have no conflict of relevant interest to this article.

References

[1] T. Greeshma and T. Roshini, "A review on privacy-preserving authentication in vanets," in *2018 International Conference on Control, Power, Communication and Computing Technologies (ICCPCCT)*, pp. 235–238, IEEE, 2018.

[2] F. Qu, Z. Wu, F.-Y. Wang, and W. Cho, "A security and privacy review of vanets," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 6, pp. 2985–2996, 2015.

[3] R. Al-Ani, T. Baker, B. Zhou, and Q. Shi, "Privacy and safety improvement of vanet data via a safety-related privacy scheme," *International Journal of Information Security*, pp. 1–21, 2023.

[4] H. V. Maddiboyina and V. S. Ponnapalli, "Fuzzy logic based vanets: A review on smart transportation system," in *2019 International Conference on Computer Communication and Informatics (ICCCI)*, pp. 1–4, IEEE, 2019.

[5] R. Al-Ani, B. Zhou, Q. Shi, T. Baker, and M. Abdlhamed, "Adjusted location privacy scheme for vanet safety applications," in *NOMS 2020-2020 IEEE/IFIP Network Operations and Management Symposium*, pp. 1–4, IEEE, 2020.

[6] D. Manivannan, S. S. Moni, and S. Zeadally, "Secure authentication and privacy-preserving techniques in vehicular ad-hoc networks (vanets)," *Vehicular Communications*, vol. 25, p. 100247, 2020.

[7] M. A. Al-Shareeda, M. Anbar, I. H. Hasbullah, and S. Manickam, "Survey of authentication and privacy schemes in vehicular ad hoc networks," *IEEE Sensors Journal*, vol. 21, no. 2, pp. 2422–2433, 2020.

[8] S. H. Lim, Y. K. Chia, and L. Wynter, "Accurate and cost-effective traffic information acquisition using adaptive sampling: Centralized and v2v schemes," *Transportation Research Part C: Emerging Technologies*, vol. 94, pp. 99–120, 2018.

[9] F. Arena, G. Pau, and A. Severino, "A review on ieee 802.11 p for intelligent transportation systems," *Journal of Sensor and Actuator Networks*, vol. 9, no. 2, p. 22, 2020.

[10] S. Y. A. Al-Shareeda, *Enhancing security, privacy, and efficiency of vehicular networks*. PhD thesis, The Ohio State University, 2017.

[11] M. Babaghayou, N. Labraoui, A. A. A. Ari, N. Lagraa, and M. A. Ferrag, "Pseudonym change-based privacy-preserving schemes in vehicular ad-hoc networks: A survey," *Journal of Information Security and Applications*, vol. 55, p. 102618, 2020.

[12] I. A. Aljabry and G. A. Al-Suhail, "A qos evaluation of aodv topology-based routing protocol in vanets," in *2022 International Conference on Engineering & MIS (ICEMIS)*, pp. 1–6, IEEE, 2022.

[13] S.-h. Sun, J.-l. Hu, Y. Peng, X.-m. Pan, L. Zhao, and J.-y. Fang, "Support for vehicle-to-everything services based on lte," *IEEE Wireless Communications*, vol. 23, no. 3, pp. 4–8, 2016.

[14] S. S. Manvi and S. Tangade, "A survey on authentication schemes in vanets for secured communication," *Vehicular Communications*, vol. 9, pp. 19–30, 2017.

[15] P. Mundhe, S. Verma, and S. Venkatesan, "A comprehensive survey on authentication and privacy-preserving schemes in vanets," *Computer Science Review*, vol. 41, p. 100411, 2021.

[16] S. Al-Shareeda and F. Özgüner, "Preserving location privacy using an anonymous authentication dynamic mixing crowd," in *2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC)*, pp. 545–550, 2016.

[17] F. Schaub, Z. Ma, and F. Kargl, "Privacy requirements in vehicular communication systems," in *2009 International Conference on Computational Science and Engineering*, vol. 3, pp. 139–145, IEEE, 2009.

[18] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki, "Caravan: Providing location privacy for vanet," *Proceedings of Embedded Security in Cars (ESCAR)*, vol. 8, 2005.

[19] A. Boualouache, S.-M. Senouci, and S. Moussaoui, "A survey on pseudonym changing strategies for vehicular ad-hoc networks," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 770–790, 2017.

[20] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki, "Enhancing wireless location privacy using silent period," in *IEEE Wireless Communications and Networking Conference, 2005*, vol. 2, pp. 1187–1192, IEEE, 2005.

[21] M. Li, K. Sampigethaya, L. Huang, and R. Poovendran, "Swing & swap: user-centric approaches towards maximizing location privacy," in *Proceedings of the 5th ACM workshop on Privacy in electronic society*, pp. 19–28, 2006.

[22] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, "Amoeba: Robust location privacy scheme for vanet," *IEEE Journal on Selected Areas in communications*, vol. 25, no. 8, pp. 1569–1589, 2007.

[23] T. Limbasiya and D. Das, "Secure message confirmation scheme based on batch verification in vehicular cloud computing," *Physical Communication*, vol. 34, pp. 310–320, 2019.

[24] M. Gerlach and F. Guttler, "Privacy in vanets using changing pseudonyms-ideal and real," in *2007 IEEE 65th Vehicular Technology Conference-VTC2007-Spring*, pp. 2521–2525, IEEE, 2007.

[25] L. Buttyán, T. Holczer, and I. Vajda, "On the effectiveness of changing pseudonyms to provide location privacy in vanets," in *Security and Privacy in Ad-hoc and Sensor Networks: 4th European Workshop, ESAS 2007, Cambridge, UK, July 2-3, 2007. Proceedings 4*, pp. 129–141, Springer, 2007.

[26] I. Goldberg and M. J. Atallah, *Privacy enhancing technologies*. Springer, 2009.

[27] B. K. Chaurasia and S. Verma, "Optimizing pseudonym updation for anonymity in vanets," in *2008 IEEE Asia-Pacific Services Computing Conference*, pp. 1633–1637, IEEE, 2008.

[28] L. Buttyán, T. Holczer, A. Weimerskirch, and W. Whyte, "Slow: A practical pseudonym changing scheme for location privacy in vanets," in *2009 IEEE vehicular networking conference (VNC)*, pp. 1–8, IEEE, 2009.

[29] J. Liao and J. Li, "Effectively changing pseudonyms for privacy protection in vanets," in *2009 10th International Symposium on Pervasive Systems, Algorithms, and Networks*, pp. 648–652, IEEE, 2009.

[30] Q. Li, S. Zhu, and G. Cao, "Routing in socially selfish delay tolerant networks," in *2010 Proceedings IEEE Infocom*, pp. 1–9, IEEE, 2010.

[31] J.-H. Song, V. W. Wong, and V. C. Leung, "Wireless location privacy protection in vehicular ad-hoc networks," *Mobile Networks and Applications*, vol. 15, pp. 160–171, 2010.

[32] A. Wasef and X. Shen, "Rep: Location privacy for vanets using random encryption periods," *Mobile Networks and Applications*, vol. 15, pp. 172–185, 2010.

[33] B. Hoh, M. Gruteser, H. Xiong, and A. Alrabady, "Achieving guaranteed anonymity in gps traces via uncertainty-aware path cloaking," *IEEE Transactions on Mobile Computing*, vol. 9, no. 8, pp. 1089–1107, 2010.

[34] I. Rouf, R. Miller, H. Mustafa, T. Taylor, S. Oh, W. Xu, M. Gruteser, W. Trappe, and I. Seskar, "Security and privacy vulnerabilities of {In-Car} wireless networks: A tire pressure monitoring system case study," in *19th USENIX Security Symposium (USENIX Security 10)*, 2010.

[35] D. Eckhoff, R. German, C. Sommer, F. Dressler, and T. Gansen, "Slotswap: Strong and affordable location privacy in intelligent transportation systems," *IEEE Communications Magazine*, vol. 49, no. 11, pp. 126–133, 2011.

[36] Y. Pan, J. Li, L. Feng, and B. Xu, "An analytical model for random changing pseudonyms scheme in vanets," in *2011 International Conference on Network Computing and Information Security*, vol. 2, pp. 141–145, IEEE, 2011.

[37] Y. Pan and J. Li, "Cooperative pseudonym change scheme based on the number of neighbors in vanets," *Journal of Network and Computer Applications*, vol. 36, no. 6, pp. 1599–1609, 2013.

[38] K. Emara, W. Woerndl, and J. Schlichter, "Caps: Context-aware privacy scheme for vanet safety applications," in *Proceedings of the 8th ACM conference on security & privacy in wireless and mobile networks*, pp. 1–12, 2015.

[39] M. Babaghayou, N. Labraoui, A. A. A. Ari, and A. M. Gueroui, "Transmission range changing effects on location privacy-preserving schemes in the internet of vehicles," *International Journal of Strategic Information Technology and Applications (IJSITA)*, vol. 10, no. 4, pp. 33–54, 2019.

[40] M. Babaghayou, N. Labraoui, A. A. Abba Ari, M. A. Ferrag, L. Maglaras, and H. Janicke, "Whisper: A location privacy-preserving scheme using transmission range changing for internet of vehicles," *Sensors*, vol. 21, no. 7, p. 2443, 2021.

[41] M. Babaghayou, N. Chaib, N. Lagraa, M. A. Ferrag, and L. Maglaras, "A safety-aware location privacy-preserving iov scheme with road congestion-estimation in mobile edge computing," *Sensors*, vol. 23, no. 1, p. 531, 2023.

[42] K. Emara, "Poster: Prext: Privacy extension for veins vanet simulator," in *2016 IEEE Vehicular Networking Conference (VNC)*, pp. 1–2, IEEE, 2016.