Privacy and Safety Improvement of VANET Data via a Safety-related Privacy Scheme

Ruqayah Al-ani, Thar Baker, Bo Zhou, and Qi Shi

Email: Ruqayah.alani@uoanbar.edu.iq; t.shamsa@brighton.ac.uk; b.zhou@ljmu.ac.uk; Q.Shi@ljmu.ac.uk

***Abstract*—Vehicular Ad-hoc NETwork (VANET) safety applications allow vehicles to exchange messages with surrounding vehicles periodically to improve the contextual awareness of the drivers about the driving environment which significantly enhances traffic safety. However, these messages usually contain sensitive information such as the Spatio-temporal information of each vehicle which might be exploited by malicious entities for various purposes (e.g., monitoring the vehicle for a long period and breaching the driver's privacy). Researchers have proposed different schemes to enhance the privacy level of drivers and their vehicles alike. However, most of the existing schemes have a negative impact on safety applications; they stop broadcasting messages for a period which increases the chance of accidents. In this paper, we propose a Safety-related Privacy Scheme (SRPS) that enhances both the privacy and safety of VANET safety applications by reducing silent periods without degrading the privacy level. Whilst the vehicle continues monitoring neighbour vehicles, if an accident is expected, it exits the silent period and starts sharing its location with its neighbour vehicles. The SRPS consists of two algorithms based on the status of the vehicle (i.e., *silent* vs. *active*). These algorithms use a multi-target tracking algorithm to search for an effective context to change pseudonyms and avoid potential accidents. Four simulators are used to implement SRPS. The latter has been compared with five pseudonym-changing schemes (PPC, RSP, CSP, SLOW, and CAPS). The simulation results indicate that SRPS achieves an efficient balance between security, privacy, and safety when compared to the other schemes.**

***Index Terms*— Privacy, Pseudonym, Safety, Silent period, Tracker, VANET.**

I. INTRODUCTION

Population growth has played a crucial role in increasing the number of vehicles, which is expected to reach two billion by 2040 [1]. Thus, the increase in traffic jams is directly related to the increase in the number of road traffic accidents. According to the World Health Organization (WHO), nearly 1.35 million people are killed yearly and more than 20 million suffer from non-fatal injuries due to road traffic accidents [2].

The development of wireless communications and sensing technologies has encouraged car manufacturers and telecommunication industries to equip vehicles with wireless devices, embedded sensors, and processing capabilities. Therefore, vehicles are enabled to collect data about themselves and their surrounding environment. Then, they exchange the collected data with neighbouring vehicles via a so-called Vehicular Ad-hoc NETwork (VANET), which is mainly developed to improve road safety [3].

Accordingly, VANET safety applications have attracted the attention of many researchers and manufacturers. These applications require the vehicle to broadcast messages periodically at 1-10 Hz in so-called Beacon Messages (BMs) that can be received by anyone within its communication range (such as 300 meters) to improve the level of awareness between vehicles such as blind-spot warning, cooperative collision warning, and lane change warning [4]. Moreover, with the era of the Internet of Things (IoT), vehicles are further connected to the internet and the conventional VANETs are changing to the Internet of Vehicles (IoV) [5], in which the broadcasted messages from vehicles can be sent, stored, and processed in the fog/edge computing [6-8]. Accordingly, efficient service to the driver and service provider could be enabled [9] such as in pay-as-you-drive, where vehicle insurance will be depending on its annual mileage [10].

However, a BM usually contains the current location of the vehicle, its speed, and its direction, which are all being broadcasted in plaintext format [4, 11, 12]. This could threaten the privacy of the driver as eavesdroppers can collect and analyze the broadcasted BMs to track the individual driver's whereabouts by linking subsequent BMs. Therefore, the location privacy of the driver must be protected well prior to the deployment of any VANET applications [13]. Kindly refer to point 6 in Section III where more details about the eavesdropper are given.

Anonymous vehicular communication is commonly accepted as a method to protect privacy [14]. However, fully anonymous communication is not acceptable because most safety applications are life-critical and thus accountability is highly important [6, 9, 15]. Therefore, a pseudonym has been used instead of a real identity to balance security and privacy. These pseudonyms must be issued by a trusted party who is able to resolve them later in case of dispute [16, 17], in which vehicles on the road can cooperatively report detected misbehaviours to

the authorities [15, 18]. Moreover, each BM should contain a time-stamp to avoid replaying a legitimate message [16].

Using a static pseudonym is not enough to protect privacy as vehicles could still be easily tracked by an external eavesdropper based on their spatio-temporal information in the broadcasted BMs. Thus, each vehicle is provided by a set of pseudonyms, in which each pseudonym is only used for a limited period, and, then it switches to another one. A simple pseudonym updating strategy would not be successful to provide unlinkability between BMs. An adversary can utilize multi-target tracking techniques to establish a link between BMs sent using different pseudonyms [19, 20].

Thus, pseudonyms should only be changed in unobserved situations. This is achieved by allowing vehicles to change their pseudonyms in mix-zone areas [21-23] or after being silent for a period [24, 25]. Mix-zone areas depend typically on infrastructure to be installed at road intersections or petrol stations to increase the number of vehicles that change their pseudonyms simultaneously. However, mix-zone areas are expensive to be deployed, which makes them impractical. Hence, most pseudonym-changing schemes tend to utilize silent periods [26, 27] to hide BMs. In a silent period, the vehicle stops sending a BM for a period before using a new pseudonym to avoid linkability.

These periods should be long enough to prevent an adversary from linking an old pseudonym with the new one using the spatio-temporal information in the BMs. However, in VANET safety applications, it is important that the vehicle continuously updates its surrounding vehicles with its current states (location, speed, and direction) and thus the silent period would impact the decision-making process (i.e. a potential accident cannot be prevented during this period). The optimal compromise between privacy and safety is still a challenge faced by most silent-based pseudonym-changing schemes [28].

A closer look at the literature on VANET privacy and safety schemes reveals that most of the existing silent-based pseudonym-changing schemes concentrate mainly on achieving privacy and/or reducing the security overheads but compromising safety such as in [24, 29-32]. Few schemes, such as [26, 33, 34], have considered the impact on safety applications; even though, they have not addressed the potential accidents during silent periods which motivated this work. In this paper, the Safety-related Privacy Scheme (SRPS), which reduces the impact of silent periods on safety applications, has been designed and implemented. SRPS assumes a vehicle in its silent period stops sharing its state but keeps receiving or expecting its neighbour states to avoid any potential accidents during this period.

The main contributions of this paper can be summarized as follows:

- Since the future mobility patterns of vehicles are predictable (i.e., they follow controlled patterns by roads, streets, traffic lights, and speed limits), we utilize a Multi-Target Tracker (MTT) algorithm [34] to predict the state of the vehicle itself and the states of its neighbours (i.e., silent and active neighbours).
- Propose a novel pseudonym-changing scheme (SRPS) that not only preserves privacy but also enhances the efficiency of VANET safety applications.
- Implement SRPS, which mainly consists of two algorithms (SRPS-Silent and SRPS-Active). The SRPS-Silent algorithm is activated when a vehicle stops sharing BMs. Contrarily, the SRPS-Active algorithm is activated when the vehicle starts sharing BMs.
- Compare the security overheads, privacy level, safety level, and efficiency of SRPS with five state-of-the-art pseudonym-changing schemes (PPC, RSP, CSP, SLOW, and CAPS).

In this paper, we use messages instead of BMs because safety applications could send out road conditions with BMs (e.g., an icy road or an accident).

The rest of this paper is organized as follows: in Section II, we review several safety applications, followed by the main requirements and challenges of these applications. Then, the highlighted research efforts to address these challenges are explained at the end of section II. In Section III, we explain the system model, pseudonym management, and vehicle tracker essential for SRPS. We also specify an adversary model used for the design and evaluation of SRPS. The proposed scheme is explained in Section IV. In Section V, we outline practical components as well as an implementation and evaluation process. The comparison of the implemented SRPS with five well-known pseudonym-changing schemes is given in Section VI before we conclude this paper in Section VII.

II. BACKGROUND

A. Sensors

In VANET, vehicles are equipped with different kinds of sensors and other smart devices and electronic systems [34] to collect information about themselves and their surrounding environment, including:

- A Global Positioning System (GPS) to detect the position of vehicles.
- A Tamper Proof Device (TPD) to store sensitive data.

- An Event Data Recorder (EDR) to store information related to accidents.
- Forward and rear sensors to alert the driver of obstacles.
- A speed sensor collects information on how fast the vehicle is travelling.
- An ice sensor for the warning of a slippery road could help other vehicles to change their routes.

The collected information could be used by the vehicle itself (e.g., to warn the driver of the current speed) and/or broadcasted to other VANET entities to make an informed decision (e.g., divert the traffic in case of a traffic jam ahead in the current route).

B. Application Scenario

A wide range of applications is being designed along with the development of VANET. These applications are generally divided into four main categories which are safety, commercial, convenience, and productivity applications. The main motivation for developing such networks is to enhance safety by enabling real-time communication between their entities, which is expected to significantly reduce the number of accidents. Thus, in this paper we mainly focus on safety applications with some examples illustrated briefly below [35, 36]:

- Post-Crash Notification: a warning message about the position of the accident is broadcasted by an involved vehicle to their neighbours that might be rebroadcasted to other vehicles if needed. This would prevent consecutive accidents, especially on the highway by giving another vehicle sufficient time to take an appropriate decision such as changing its direction or stopping.
- Lane Change Notification: the locations of nearby vehicles are monitored constantly and if an attempted lane change puts the driver in a hazard, then a warning is generated to change the behaviour.
- Forward Collision Notification: give a warning to the driver about an expected rear-end collision with a heading vehicle driving in the same lane and the same direction, due to, for example, stopping or slowing down before arriving at a sharp bend or hill.
- Head-on Collision Notification: provide an early warning to vehicles travelling in the opposite direction if there is a collision probability.
- Intersection Collision Notification: warn the driver when approaching a road intersection if there is a high collision probability with other vehicles.

C. Safety Application Requirements

The requirements of safety applications could be derived from the functionality need, the characteristics of VANET, or the need for obtaining public acceptance and facilitating the dissemination of these applications.

First, the essential requirements, which facilitate safety functionality to work properly, are illustrated:

- Safety messages contain the state of vehicles (position, speed, and heading) and traffic-related information (accidents, traffic jams, icy roads, etc.).
- Safety messages are broadcasted periodically with high frequency (1-10 Hz) in so-called beacons or they are generated when detecting safety events in so-called event-driven messages [37].
- The vehicle could broadcast messages directly to its neighbouring vehicles within its communication range, such as 300m using single-hop communication. However, sometimes, multi-hop communications are required when there is a need to broadcast messages to other vehicles beyond the communication range [38-40].
- Secure Communications of road-safety applications are highly important to be implemented well. Malicious messages sent out by attackers could cause severe damage or fatal consequences [41, 42].
- Short-term linkability is important for most safety applications, in which the receiver should be able to recognize messages over a short period issued by the same sender. Otherwise, it becomes harder and error-prone to infer an accident risk based on unlinkable messages [43]. For example, in a lane change warning alert application, the receiver builds a map of nearby vehicles upon receiving subsequent beacons and then decides if changing the lane is safe or not [44].

The special characteristics of VANET, which are high mobility, rapidly changing topology, and many vehicles, would introduce some special requirements, as illustrated below:

- Real-time Constraints: Vehicles can travel up to 112 km/h, which means connectivity between them is short. This emphasizes the need for real-time decision-making (i.e., most safety applications require latency of 100 ms -1000 ms) and

thus any communication and computation overheads should be minimized [38, 40, 45].

- Overheads: The number of vehicles can be increased to a large scale, especially in large cities which requires reducing both communication and computation overheads of any embedded schemes such as security schemes.

- Distributed and Non-Cooperative Scheme: Scalability would challenge any centralized scheme and the speed of vehicles would mean that the cooperation between them is not applicable, i.e. communication between vehicles would last for a short period.

Finally, two other requirements are highly important to meet the public acceptance and successful deployment of any VANET applications [46], which are illustrated below.

- Cost Constraints: the embedded devices in vehicles, communication media, storage media, and infrastructure dependency should be kept at a low cost to facilitate the deployment of such networks [35, 47].

- Privacy of the driver/vehicle: the amount of broadcasted location information could enable an adversary to track a vehicle and breach the privacy of the driver as there is a strong correlation between a vehicle and its driver i.e. most vehicles are driven by their owner only [42, 48].

Despite the above-mentioned requirements, security and privacy [49] of the exchanged messages are identified as the main concerns of wireless applications especially if the applications are related directly to people's life (i.e. any dispute could cause disasters, accidents, injuries, and loss of life). Thus, we will elaborate further on the main requirements of security and privacy in VANET safety applications and what are the main challenges and possible solutions.

D. Security and Privacy Challenges

VANET safety applications need to provide secure communications between their entities, in which vehicles only accept and react upon messages received from authenticated entities. Moreover, the receiver must ensure that messages have not been tampered with (i.e. ensure its integrity) during transmission or replayed later (i.e. ensure the freshness of the information) by another entity such as the received message from an ambulance could resend later by the greedy driver to empty his road. A sender of the messages should be accountable for his activities such as the driver will not be able to deny sending a false warning in a later stage when further investigation is needed [50].

Accordingly, current standardisation and research efforts mainly applied traditional Public Key Infrastructure (PKI) and digital signatures to secure communications in VANET [16]. In PKI, a pair of keys (public and private) is required, in which the public key must be certified by a trusted third party to ensure the authenticity of the driver/vehicle. Then, a vehicle digitally signs the sent message using the private key to prove its integrity and attaches the signature and the certificate of the public key to the broadcasted messages. Moreover, a timestamp is required to be attached to the message to avoid replaying messages later.

Yet, preserving the privacy of the driver is highly important to obtain public acceptance and enable the dissemination of VANET applications. Therefore, the public key must be stripped from any identification details and used as a pseudonym to protect the identity of the driver [30]. More details regarding pseudonyms are given in subsection III.A. A static pseudonym is not sufficient to protect privacy as the driver can still be identifiable via long-term linkability of the vehicle's locations (i.e. identify the driver using his/her points of interest such as home or work address). Thus, a set of pseudonyms is required to be assigned to each vehicle and each pseudonym should only be used over a short period before switching to another one.

However, privacy is still an issue even if pseudonyms change because vehicles could be still vulnerable to syntactic attack (i.e., it is the only vehicle B1 to chang its pseudonym during Δt from B1 to B2) or to semantic attack (i.e., its route is different from other neighbours' routes thus the adversary can easily link B1 to B2 using one of the tracking method such as in [20]), as illustrated in Fig. 1 [33, 51], in which the green cars represent the cars that have not changed their pseudonyms while the orange cars represents the cars that have changed their pseudonyms. Therefore, pseudonyms should only be changed in unobserved situations by allowing vehicles to change their pseudonyms in a mix-zone area [21] or after being silent for a period [24].

In mix-zone-based strategies, vehicles change their pseudonyms inside predefined road areas such as road intersections [21, 52-54], and social spots [51, 55, 56]. Infrastructure is required to be installed to inform vehicles of the boundary (enter and exit points) of the mix-zone area and thus all vehicles inside this area will stop sharing messages and change their pseudonyms. Then, when the vehicle exits this area, it will share messages again but using the new pseudonyms. In a silent-period-based strategy, there is no need for any infrastructures because the vehicle decides locally when to stop and start sharing messages either depending on time [24, 57] and/or on context (i.e., the state of the vehicle itself or its neighbours) [26, 32, 58-60].

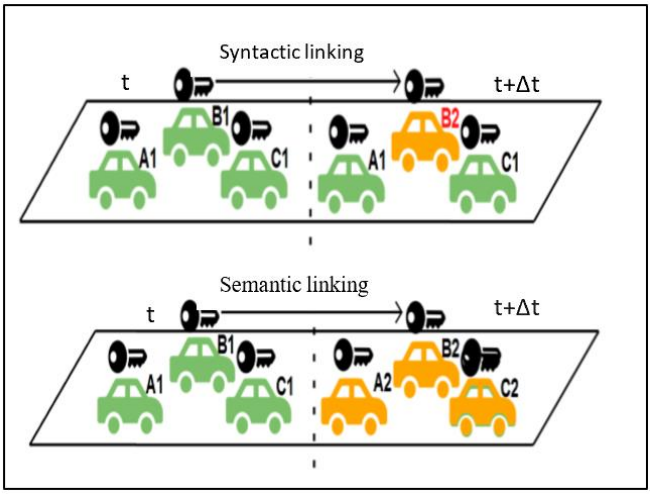

Fig. 1. Linking attacks

Most researchers and standardization efforts nominated the silent period over the mix-zone because there is no need for infrastructure and thus it is more likely to facilitate the deployment of VANET applications soon. In silent period-based strategies, the vehicle should synchronize this period with its neighbours and only start sharing its state if the attacker is probably to be confused (i.e., its state is probably to be mixed with its neighbour (s)) [26, 32, 58-60].

Changing pseudonyms more frequently and having longer silent periods should enhance privacy but these would have a negative impact on safety applications because:

- Increase security overheads and thus more messages could be lost via increasing communication (i.e. only a certificate is required to be attached if there is a new neighbour or if the pseudonym is new) and computation (i.e. verified the new pseudonym only; otherwise the already verified pseudonyms are stored in a table) overheads [16]. Kindly refer to [61, 62] for more details regarding security overheads.
- An accident could have happened during silent periods as a vehicle stops sharing its positions.

In the last decade, a wide range of pseudonym-changing schemes have emerged to achieve an adequate balance between security and privacy but only a few of them consider the impact on safety applications. Yet, it is still a scientific challenge to design a pseudonym scheme that effectively addresses the three key issues: privacy, security, and safety. The next sub-section will provide a review of such schemes available in the literature and highlight the need for the proposed SRPS.

E. Related Work

A number of pseudonym-changing schemes have been proposed to improve the privacy of the drive and/or reduce security overheads. In this section, related research works are reviewed and how the requirements of safety applications failed to be met.

A periodical pseudonym update scheme is used to only allow short-term linkability to protect the privacy of the driver from long-term linkability, which allows vehicles to update their pseudonyms at either fixed [63] or random periods [64]. In the fixed period scheme, all vehicles change their pseudonyms at the same time, which increases the number of vehicles changing their pseudonyms simultaneously to confuse an adversary. However, it is easy for the adversary to predict this period by monitoring several consecutive messages. To deal with this issue, randomly changing periods [64] are applied in [65] to allow the lifetime of a pseudonym to be chosen randomly between the minimum and maximum values. However, this could reduce the simultaneous change, which reduces the confusion and increases traceability. Therefore, a cooperative pseudonym-changing scheme was suggested in [59], in which vehicles only change their pseudonyms~~,~~ when a number of nearby vehicles want to change their pseudonyms as well. Yet, if vehicles have different predictable routes, they will still be easily tracked via their spatio-temporal information.

To avoid linkability due to continuous tracking, Beresford and Stajano [66, 67] suggested that vehicles only change their pseudonyms in mix-zone areas where infrastructure is required to be installed at intersections or petrol stations. A vehicle would become unobservable when entering these areas and, thus, it may change its pseudonym to confuse the attacker [11, 12, 17]. This scheme needs additional infrastructure to be deployed on the roads and its effectiveness depends on the number of vehicles in that area. Moreover, it is difficult to avoid timing and transition attacks [52], in which the attacker can link old and new pseudonyms together by monitoring enter and exit points of these areas and then calculating the time that a vehicle could spend inside them.

To overcome the mix-zone issues, another solution has emerged, in which a vehicle can decide locally to be in the unobserved situation by staying silent for a period before updating its pseudonym. Sampigethaya *et al.* apply a random silent period to VANET in [24]. However, if there is only one vehicle on the road, it would be still identifiable even if it changes its pseudonym and enters a silent period. Thus, Tomandle *et al.* [68] and Li *et al.* [31] suggest that vehicles enter silent periods cooperatively with their neighbours. Moreover, the work in [31] suggests changing pseudonyms and entering silent periods only when the speed and direction of vehicles are changed.

As VANET safety applications need continuous location information, silent periods could have a negative impact on their performance (i.e., an accident could be unavoidable). Thus, a

scientific challenge is how to balance privacy and safety as a short silent period would enhance safety but decrease the privacy level and vice versa. In the SLOW [33] safety protocol, it was suggested that the vehicle is only being silent when its speed is lower than a threshold value, meaning that the probability of an accident is decreased [69]. Emara *et al.* [34] proposed a Context-Aware Privacy Scheme (CAPS) [26] that enhances safety by reducing silent periods but without degrading the privacy level. In CAPS, vehicles cooperatively enter a silent period and then resume message sending if their contexts are likely to be mixed with other nearby silent vehicles or they are in unobserved positions. A Multi-Target Tracking (MTT) algorithm [70] is utilized by CAPS to predict the state of a silent vehicle in order to decide if there is a mix-context situation.

Despite the aforementioned research, the performance of safety applications still needs further enhancements before applying silent periods. Thus, we aim to design a new scheme that enhances safety without degrading privacy. We follow CAPS in terms of applying an MTT algorithm to not only predict the state of nearby vehicles (i.e. searching for a mix-context) but also to avoid an expected accident during silent periods. Moreover, we aim to enhance the performance of safety applications by reducing silent periods as well.

III. Model Settings

A. System Model

Depending on the requirements and characteristics of VANET safety applications, we assume the following:

- Each vehicle is equipped with an On-Board Unit (OBU) which can store, process, and communicate with other VANET entities [12].
- According to the requirements of safety applications [4, 11, 12], OBU would broadcast BMs, which contain the current position, speed, and heading of the vehicle, periodically (1-10 Hz) to nearby entities within the communication range of 300m via Dedicated Short-Range Communications (DSRC) [71].
- Physical devices called Roadside Units (RSUs) are located at fixed positions along the roadside or highway. An RSU is responsible for routing messages, extending the communication range, providing internet connectivity to the vehicles on the roads, serving as a proxy between vehicles and trusted authorities, etc.
- To secure communications in VANET, we will follow PKI in which each vehicle/RSU needs to register first with a designated authority [72] and obtain certified public keys to be able to securely exchange messages [73] and participate in any VANET applications.
- To preserve the privacy of a vehicle/driver, its certified public keys are stripped from any identification details and used as pseudonyms [30] which are stored in a TPD. Moreover, to protect the privacy of vehicles against authority in case it is compromised, role separation between authorities has been proposed and widely applied, for instance in [74-76] there are at least three authorities: one for issuing a Long-Term Pseudonym (LTP), the second for issuing a Short-Term Pseudonym (STP), and the last one for controlling a resolution centre and a key revocation process. The issuing authorities should keep a database which include a link between the real identity and LTP as well as the link between the LTP and STP for later accountability of misbehaved entities. A pseudonym management system will be illustrated in the next sub-section.
- We assume a global passive adversary model [77] which aims to breach the privacy of vehicles by eavesdropping and monitoring all the broadcasted messages. A global adversary can listen to all network communications. For instance, an untrusted service provider can eavesdrop on all the broadcasted messages to track a vehicle and breach the privacy of the driver.
- The communication among RSUs or between RSUs and authorities is usually via wired communication. On the other hand, OBUs (or vehicles) communicate with other OBUs and RSUs wirelessly through Vehicle-to-Vehicle (V2V) and Vehicle-to-Roadside (V2R) communications respectively as shown in Fig. 2, in which the gray straight lines represent the wire connections between RSUs while the circles represent the rang of the wireless connections of vehicles in V2V and V2R connections.
- Furthermore, each vehicle employs an MTT algorithm [70], which is illustrated in detail later in section D. MTT is responsible for maintaining the state of neighbours even if their messages are missed due to silent periods or communication faults. Moreover, the future state of a vehicle itself would be predicted using the first step of the tracker, which will be explained in section D (Kalman filter), to monitor the confusion level of an adversary or to predict an accident during its silent period, as we will illustrate later in Section IV.

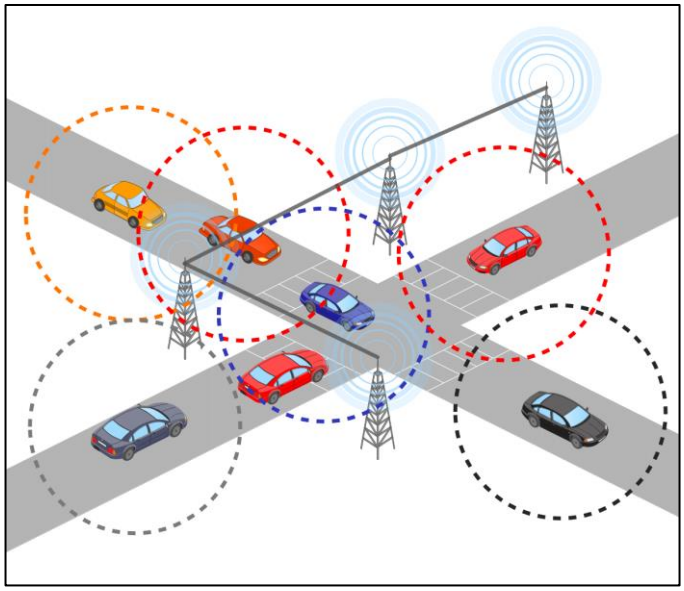

Fig. 2. VANET Communications

B. *Pseudonym Management Model*

Every vehicle in a VANET has a set of certified pseudonyms, which should be issued offline, to facilitate the privacy-preserving of the driver during VANET communications. The main steps of pseudonym management are illustrated below and shown in Fig. 3. These steps are summarized below based on the requirements stated in Section II.C and the survey paper on pseudonym management schemes [78]:

- We assume that there are two trusted authorities: a Long-Term Issuing Authority (LTIA) and a Short-Term Issuing Authority (STIA). Each authority has a pair of public and private keys. The public keys are known by each VANET entity and their private keys are used to sign issued key certificates.
- Each vehicle requests an LTP from LTIA by submitting its required documents directly. This pseudonym will be used as a static identity by the vehicle and changed only when the owner of the vehicle is changed. LTP is signed by LTIA's private key.
- Each LTP is coupled with a private key used to sign requests to obtain STPs from STIA either directly from STIA or with the help of RSUs. STIA uses LTIA's public key to verify the validity of the vehicle's LTP (or key certificate) and then checks the authenticity of the vehicle's request for an STP using the public key in the certificate in order to approve the STP (public key certificate) issuing.
- STPs are used to authenticate safety messages that are exchanged mainly between vehicles in real-time. First, a timestamp is added to a safety message and then signed using the private key associated with the current valid STP. The timestamp is used to avoid replaying legitimate messages later by an adversary such as replaying messages from emergency cars to make space for them.
- Each STP has a minimum lifetime to provide short-term linkability and a maximum lifetime to avoid long-term linkability. The vehicle can communicate with STIA later to request more STPs either annually or when they are needed, depending on a selected policy.
- A vehicle's LTP and STPs must be kept secret in the vehicle and no one can extract them, so they are stored in the vehicle's TPD.

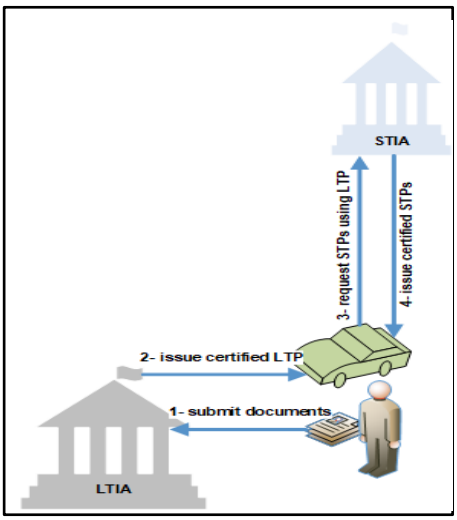

Fig. 3. Pseudonym Management Model

C. *Vehicle Tracker*

To investigate the context of any message (i.e. the state of vehicles), we assume that a multi-target vehicle tracker [20, 70] is installed in each vehicle. This tracker is responsible for maintaining the state of nearby vehicles even if they are in a silent period. This feature can enhance safety and help vehicles to choose an appropriate context to change their status. In [20, 70], Karim *et al.* designed and implemented Vehicle Tracking (VTr) which consists of four phases: state estimation, gating, data association, and track maintenance [15] as summarized below:

1) A Kalman filter [79] is used to estimate the state of the vehicle, which includes its position, speed, and direction. The inaccurate state measurements obtained from the vehicle's sensors in each time and an estimated

measurement obtained from a predefined kinematic model are used to find the best estimation of the vehicle state.

2) In the data association process, messages from the same vehicle with different pseudonyms are tried to be linked to their originating vehicle via computing an assignment probability matrix. The Nearest Neighbour Probabilistic Data Association (NNPDA) technique in [80] is used that allows real-time calculations even with a large number of vehicles. Otherwise, messages are only linkable by matching the same pseudonyms.

3) To enhance the efficiency of data association, a gating process is applied before the association in which unlikely associations are deleted.

4) The last phase is needed to delete any vehicles out of the communication range and only track neighbouring vehicles even if they are silent.

IV. Proposed Safety-Related Privacy Scheme (SRPS)

The main aim of the proposed Safety-related Privacy Scheme (SRPS) is to reduce the impact of the existing pseudonym-changing schemes, which applied silent periods, on VANET safety applications. This could be achieved by determining the appropriate context for a vehicle to update its pseudonyms or enter/exit a silent period [26] and by avoiding any predicted accidents through this period. Fig. 4 shows an example of three vehicles' traces and four states which represent the noteworthy positions. In these four states, two vehicles are expected to be at the same time in the same positions that may confuse the attacker or cause an accident.

Accordingly, the main contribution of SRPS is to find the above noteworthy positions in Fig. 4, which could achieve the following:

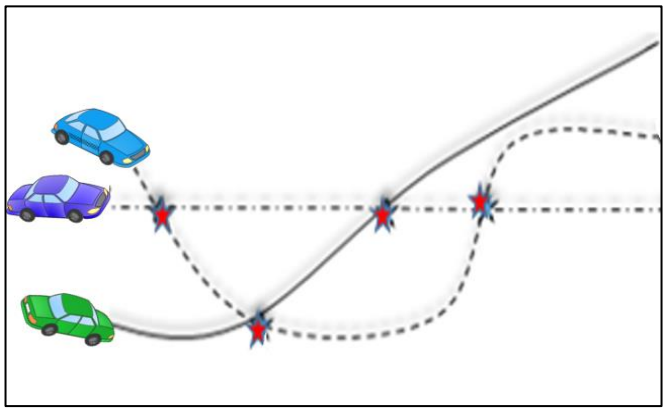

Fig. 4. Vehicles'–Traces

1) Reducing accidents during silent periods as each vehicle (silent/active) in each time step calculates in advance its predicted next positions and its predicted neighbours' (silent/active) positions using the Kalman filter. Then, if a silent vehicle predicted any accident in the next time step, it exits the silent period and starts sharing its state.

2) Reducing the need for pseudonyms, that need to be issued, stored, verified, and sent, because of reducing the change of pseudonyms in an observed situation i.e. wasting pseudonyms in an observed situation.

3) Enhancing the functionality of safety applications via reducing silent periods, in which a vehicle can successfully change its pseudonym without entering a silent period. That is because the vehicle calculates the next predicted position of itself and neighbours' (silent/active) positions using Kalman filter and then if its position is probably to be mixed with others, it will broadcast its new state using a new pseudonym.

4) Increasing the chance of mixing context because vehicles cooperatively enter a silent period and directly start looking for the mix-context with their silent neighbours before being far away from each other. Unlike other cooperative schemes as they force a minimum silent period to ensure protecting the privacy, for example, in CAPS [28], vehicles cooperatively enter a silent period and after 3s start looking for the mix-context but as the vehicle can travel [135] up to 60m within the 3s, it would have less chance to find mix context i.e. they will be far away from each other.

We have designed and implemented two main algorithms: SRPS-Active to guide each vehicle in its *active* status as illustrated in Algorithm1; and SRPS-Silent to guide the vehicle in its *silent* period as shown in Algorithm 2. The notations used in these algorithms are illustrated in Table 1. In SRPS-Active, a vehicle tries to synchronize silent periods or finds a mix-context to change its pseudonym while in SRPS-Silent the vehicle keeps tracking its neighbours to avoid any potential accidents and looking to exit the silent state when the attacker is probably confused by its state as illustrated below. Note that in both algorithms we refer back to the vehicle tracker in section III.C.

Table 1: Table of Notations

Symbol	Stand for	Notations
vL	vehicle Lifetime	The vehicle enters and exits the road at different times. Thus, the lifetime for each vehicle is the difference between the departure and arrival times.
BR	Beacons Rate	The number of sent BMs per second.

Symbol	Stand for	Notations
VS	Vehicle State	The current vehicle state (position, speed, and heading) sensed by GPS
EVS	Estimated Vehicle State	Estimated at the next step using the Kalman filter.
p'_v	next Position of the vehicle itself	The expected position of the vehicle itself using the Kalman filter.
SBM	Sent BMs	It is either 1 when the vehicle shares its state or 0 when the vehicle is silent.
RBMs	Received Beacon Messages	Received current states of nearby vehicles within a specific communication range.
ERBMs	Estimated Received Beacon Messages	Estimate the new state of neighbours (RBMs) for the next step using the vehicle tracker.
p'_n	next neighbour Position	The expected position of neighbour vehicles, which is estimated using the vehicle tracker.
nV	number of Vehicles	The total number of vehicles on the roads.
nN	number of Neighbors	The number of neighbours within a specific communication range.
vL	vehicle Lifetime	The vehicle enters and exits the road at different times. Thus, the lifetime for each vehicle is the difference between the exits and the entry time.
MinPL	Minimum Pseudonym Lifetime	It is recommended to be 60s to ensure the stability of communications [81].
MaxPL	Maximum Pseudonym Lifetime	A longer lifetime would decrease privacy but enhance safety.
MinSP	Minimum Silent Period	Used to enhance privacy.
MaxSP	Maximum Silent Period	Used to decrease the effect on safety.
CT	Current Time	The current real-time
PL	Pseudonym Lifetime	It is initiated when a pseudonym is changed.
PD	Pseudonym Distance	It is initiated when the pseudonym is changed.
ST	Silent Time	It is the start time for ceasing (i.e. stop sharing) safety messages and initiated when the vehicle enters a silent period.
MTs	Missed Tracks	Check if any vehicle within 50m enters a silent period. If yes, store its state in MTs.
EMTs	Expected Missed Tracks	The expected missed track of silent neighbor vehicles using the Kalman filter.
SBMs/s	Sent Beacon Messages per Second	The average number of sent messages per second.
T_i	Tracking Vehicle	The maximum tracking period of the vehicle
nPseud	number of Pseudonyms	The total number of used pseudonyms in the whole scenario.
chPseud	Change Pseudonym	The average number of pseudonyms changes during the scenario.
nV_{ch}	number of Vehicles that changed their pseudonyms	The total number of vehicles that changed their pseudonyms.
m	Meters	Measurement of the distance
ms	MilliSeconds	Measurement of the driven-time
m/s	Meters per Second	Measurement of the speed of a vehicle

A. Algorithm1: SRPS-Active

- Algorithm1 takes as input the status of the vehicle, the Received Beacon Messages from its neighbour (RBMs), its current Vehicle's State (VS), the Expected Vehicle State (EVS) of the current state from the previous step, the predefined MINimum and MAXimum Pseudonym Lifetime (MinPL, MaxPL), and the current Pseudonym Lifetime (PL).
- A vehicle will continue broadcasting messages with the current valid pseudonym until the PL passed MinPL, as demonstrated in steps 2 to 5.
- Then, when the MinPL is passed, the vehicle starts searching for an opportunity, as shown in Algorithm1 steps 6 to 34, to change its pseudonym or its status depending on the following conditions below:
  - Changing pseudonym: the EVS from the previous time step (i.e. expected current state) which was predicted by the installed vehicle tracker using Kalman-filter is compared with the actual current VS. The comparison is achieved by calculating the distance between EVS and VS. Accordingly, if the distance is sufficient to confuse the adversary, the vehicle will broadcast its state with a new pseudonym. That

is because the state of the vehicle is different from the state that could be predicted by the adversary, such as if the vehicle is intending to go ahead but under specific circumstances (i.e. accidents or traffic jam warning), it might change its direction (i.e. turn right, stop).

- Changing pseudonym: if the above condition has not been met, the EVS and the expected neighbour states ERBMs are predicted for the next time step using the vehicle tracker. The EBRMs are calculated for all vehicles (i.e. silent and active neighbours) within the communication range. Then, the distance between EVS and ERBMs is calculated and if the distance between the EVS and any of the ERBMs is small enough (i.e. the state of the vehicle could be mixed with another neighbour in the next time step), then, the vehicle broadcasts its current state and changes its pseudonym for broadcasting the next state, as shown in steps 13 to 23. However, if the nearby vehicle does not change its pseudonym (such as its pseudonym lifetime has not passed), the vehicle should search again to find another opportunity in order to confuse the attacker as it is still linkable by its spatio-temporal information, which is out-of-the-scope of our scheme.

- Change status: if the above two conditions have not been met, the vehicle would check if any of its neighbour vehicle are being silent to cooperatively enter a silent period, as shown in steps 25 to 30. A silent vehicle can be recognized by the vehicle tracker when two consecutive messages from a neighbour are missed (i.e. if just one beacon message is missed, it could be due to the overheads) [26]. Moreover, even if the neighbour vehicle enters its silent period, its next states can still be expected by the vehicle tracker for a period of time using the state maintenance phase (i.e. the period of time meant that the vehicle keeps predicting its silent neighbours vehicles up to the Maximum Silent Period (MaxSP)).

- Otherwise, if the above three conditions have not been met, the vehicle will keep broadcasting safety messages using the same pseudonym until the PL has passed its MaxPL, as shown in steps 32 to 34. Then, when PL has passed MaxPL, the vehicle will be forced to stop sharing messages to avoid long-term linkability.

- The outputs from this algorithm are the vehicle's status, EVS, RBM, SP, and PL.

Algorithm1: SRPS-Active

Input (Status, RBMs, VS, EVS, MinPL, MaxPL, PL)

```
1.  If (Status = = Active)
2.    If (PL <= MinPL)
3.      Broadcast (VS)
4.      PL := PL + BR
5.      GoTo step 1
6.    Else If (PL >= MinPL) and (PL <= MaxPL)
7.      If (VS<>EVS)
8.        Change Pseudonym ( )
9.        PL := BR
10.       Broadcast (VS)
11.       GoTo step 1
12.     Else
13.       Kalman_update (ERBMs, RBMs)
14.       Kalman_predict (ERBRs)
15.       nN := size of (ERBMs)
16.       Kalman-update (EVS, VS)
17.       Kalman-Predict (EVS)
18.       for i := 0 to nN
19.         if (ERBMs[i]) ≈ EVS)
20.           Broadcast (VS)
21.           Change Pseudonym ( )
22.           PL := 0
23.           GoTo step 1
24.     Else
25.       MTs := MissedTracks (ERBMs)
26.       mN := size of (MTs)
27.       If (mN > 0)
28.         Status := Silent
29.         SP := 0
30.         Call (SRPS-Silent)
31.     Else
32.       Broadcast (VS)
33.       PL := PL + BR
34.       GoTo step 1
35.   Else If (PL >= MaxPL)
36.     Status := Silent
37.     SP := 0
38.     Call (SRPS-Silent)
```

Output (Status, RBMs, EVS, SP, PL)

B. Algorithm2: SRPS-Silent

- Algorithm2 is run when the vehicle starts its silent period and it takes as input the status of the vehicle, the Received Beacon Messages from its neighbour (RBMs), its current Vehicle State (VS), and its expected current state from the previous time step (EVS), the predefined MAXimum Silent Period (MaxSP), and the total Silent Period (SP).

- A silent vehicle will directly start searching for an opportunity to resume sending messages according to the following conditions.

- Unexpected state: if the state of the vehicle from the previous time step (EVS) is not equal to the current actual state (VS), i.e. the position of the vehicle becomes unexpected, it will change its status and resume sending messages, as illustrated in steps 3 to 7.
- Mixed-context/ Predicted-accident: in every time step, the vehicle predicts its next state EVS and its next silent/active neighbour states ERBMs using the Kalman filter. Then, calculating the distance between EVS and ERBMs and if the state of the vehicle could be mixed with another neighbour in the next time step (i.e. if the distance between EVS and any ERBM is small, the adversary is probably to be confused between them), then the vehicle will change its pseudonym and share its state, as shown in steps 13 to 23. Moreover, when the context of two vehicles is probably to be mixed, it means they probably will be in the same position or near to each other, which could cause an accident if the vehicle continues ceasing its state.

- Otherwise, if the above conditions have not been met, the vehicle will keep ceasing safety messages until the SP has passed its MaxSP. Then, the vehicle will be enforced to share its states to avoid affecting the efficiency of safety applications.

- The outputs from this algorithm are the status of the vehicle itself, EVS, SP, PL, RBM, and the total number of Potential Avoided Accidents (PAA).

Algorithm2: SRPS-Silent

Input (Status, RBMs, VS, EVS, MaxSP, SP)

```
1.   If (Status = = Silent)
2.     If (SP <= MaxSP)
3.       If (EVS<>VS)
4.         Status := Active
5.         Change Pseudonym ( )
6.         PL := 0
7.         Call (SRPS-Active)
8.       Else
9.         Kalman_update (ERBMs, RBMs)
10.        Kalman_predict (ERBRs)
11.        nN := size of (ERBMs)
12.        Kalman-update (EVS, VS)
13.        Kalman-Predict (EVS)
14.        for i := 0 to nN
15.          if (ERBMs[i] ≈ EVS)
16.            PAA := PAA + 1
17.            Change Pseudonym ( )
18.            PL := 0
19.            Call (SRPS-Active)
20.      Else If (PL >= MaxSP)
21.        Status := Active
22.        Change Pseudonym ( )
23.        PL := 0
24.        Call (SRPS-Active)
25.      Else
26.        Ceasing (VS)
27.        SP := SP + BR;
28.        GoTo step 1
Output (Status, EVS, RBMs, SP, PL, PAA)
```

V. Simulations and Implementation

A. Simulation Setup

To implement the SRPS-Active and SRPS-Silent algorithms, we employ the following components:

1) Network Simulator: OMNeT++ [82] version 5.0 (Object-oriented Modular NETwork) is a discrete event simulator used to build wireless communication networks between vehicles.

2) Mobility Simulator: SUMO [83] version 0.25.0 (Simulation of Urban MObility) is a time-driven discrete simulator used to generate large road traffic networks.

3) Communication Protocol: (Traffic Control Interface) TraCI is a standard protocol used to provide a bidirectional connection between OMNeT++ and SUMO.

4) Vehicular Simulator: the framework Veins [82] version 4.4 (vehicle in network simulation) is used to simulate the vehicular network which is a combination of OMNeT++ and SUMO.

5) Privacy Simulator: PREXT [84] (PRivacy EXTension for Veins), which supports several privacy metrics and schemes, is used to evaluate the proposed privacy scheme.

We downloaded the road map area of (3.8 km*2.8 km) of Liverpool/UK (such as, Scotland Road, St Bartholomew Road, Alderney Road, Herm Road, etc.) using the Open Street Map (OSM) database [85], which is a free editable map of the entire world. The OSM is converted into the SUMO network using two command-line applications [83]: "netconvert"[1] and "polyconvert"[2]. The downloaded map is shown in Fig. 5. The selected map was chosen according to two specific criteria. The first criterion is achieved by having two or more vehicles with

[1] https://sumo.dlr.de/docs/netconvert.html

[2] https://sumo.dlr.de/docs/polyconvert.html

the same probability to be in the same position as shown in Fig. 6.a. The other criterion is met by having vehicles with two or more directions having the same probability as shown in Fig. 6.b. These criteria would increase the confusion level of the attacker and thus we can see the effect of the schemes in a shorter time (i.e. the mixed context would be difficult to be found in straight highway roads that do not include the above criteria.

Subsequently, vehicles are generated with randomly chosen trips for the given network, in which the source and destination of each vehicle are derived through Python scripts (randomTrips.py)[3]. The arrival rate of vehicles is one per second (v/s) by default but we also increased that rate (one vehicle per 0.5s and 0.3s) to investigate the performance of our scheme in different traffic scenarios (i.e., when the density of vehicles increases). It is worth noting that some trips are discarded because the downloaded network is not fully connected; an example is given in Fig. 7 in which there is no connection between edge -217900398 and edge 3129843#4.

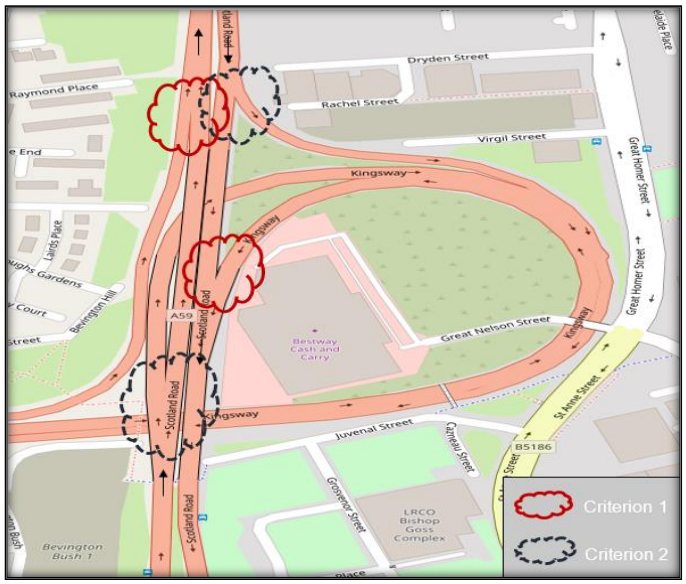

Fig. 5. OSM road network

B. *Implementation*

In the PREXT simulator [84], a number of well-known pseudonyms-changing schemes are implemented and thus we only need to implement our scheme. As OMNeT++ modules are implemented using C++, we use the same language to implement SRPS algorithms. The rest of the paper uses the notations illustrated in Table 1. We compare the SRPS scheme against the following five state-of-the-art schemes which apply different techniques as briefly explain below:

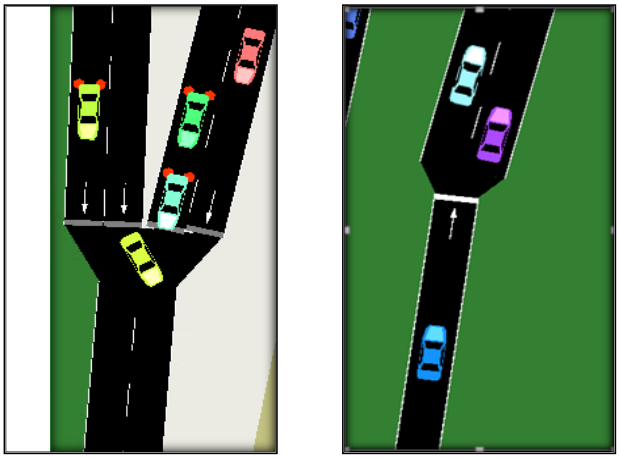

Fig. 6. Sections of the road

```
Error: No connection between edge '-217900398' and edge '31290438#4' found.
Error: Mandatory edge '31290438#4' not reachable by vehicle '0'.
Error: The vehicle '0' has no valid route.
Error: No connection between edge '5036087' and edge '-60198091#2' found.
Error: Mandatory edge '-60198091# 2' not reachable by vehicle '10'.
Error: The vehicle '10' has no valid route.
```

Fig.7. An Example of Discarded Trips

- Periodical Pseudonym Changing (PPC) scheme [64], in which each vehicle changes its pseudonym at random times selected between MinPL and MaxPL.
- Random Silent Period (RSP) scheme [24] which allows a vehicle to use its pseudonyms for a fixed time PL and then enters a random silent period selected between MinSP and MaxSP.
- Coordinate Silent Period (CSP) [68] scheme which coordinates all vehicles in the network to use their pseudonym for a fixed time PL and then enter a fixed silent period SP before changing their pseudonyms.
- Speed LOWer (SLOW) [33] scheme which allows a vehicle to only enter a silent period when the speed is lower than 30 km/h and then changes pseudonyms if the silent period exceeds a specific value SP.

[3] https://sumo.dlr.de/docs/Tools/Trip.html

- Context-Aware Privacy Scheme (CAPS) [26], in which a vehicle keeps looking for an appropriate context to change its status (silent/ active).

Then, the performance of SRPS against the above schemes is evaluated using quantitative measurements. The statistics obtained from OMNeT++ and PREXT[4] are discussed below, along with the newly designed metrics, for comparison purposes:

1) Security Overheads

The average number of changed pseudonyms (ChPseud) per second is used to compare the security overheads of each scheme, as calculated in Equation (1). The total number of changed pseudonyms is divided by the number of vehicles that changed their pseudonyms at least one time during the simulation time. Then, to obtain the average number of changed pseudonyms per second, the result is divided by the average vehicle lifetime The security overheads should be kept as low as possible to enhance the efficiency of the applications.

$$ChPseud/s = \frac{nPseud}{nV_{ch} * \overline{vL}} \quad (1)$$

where:

$$\overline{vL} = \frac{\sum_{i=1}^{nV} vL_i}{nV}$$

2) Privacy Level Evaluation:

The ability of a tracker to reconstruct each vehicle's traces is employed to design a quantitative privacy metric [21, 57, 86-88]. In [88], a maximum continuous tracking period percentage is used as a privacy metric. The author calculated the ability of the adversary to track each vehicle continuously for over 90% of its original traces. For each vehicle, a tracker tries to link messages using VTr and then calculates the maximum continuous tracking period (T). The average traceability percentage (Trac%) for the whole scenario is given in Equation (2) neglecting vehicles that have never changed their pseudonyms.

$$Trac\% = \frac{1}{nV_{ch}} \sum_{i=1}^{nV} \lambda_i \times 100, \quad (2)$$

where

$$\lambda_i = \begin{cases} 1, & \frac{T_i}{vL_i} \geq 90\% \\ 0, & Otherwise \end{cases}$$

3) Safety Functionality Evaluation:

We calculated the performance of safety based on two values: the average number of Sent BMs per second (SBM/s) and the number of Potentially Avoided Accidents (PAA).

The SBM/s is calculated by calculating the total number of SBMs from each vehicle and then dividing by the vL. Then, the average of SBMs/s for all vehicles is calculated, as shown in Equation (3). The value of SBM/s indicates the impact of the privacy scheme on safety, in which the higher value would improve the functionality of safety applications.

The second value is PAA in which SRPS calculates the total number of expected accidents (i.e. if vehicles stay silent) during the simulation time as shown in Equation (4).

$$SBMs/s = \frac{1}{nV} \sum_{i=1}^{nV} \frac{1}{vL_i} \left(\sum_{j=1}^{vL_i} \sum_{k=1}^{br} S \right), \quad (3)$$

$$PAA = \sum_{i=1}^{nV} \left(\sum_{j=1}^{vL_i} \sum_{k=1}^{br} \sum_{l=1}^{nN} Z \right), \quad (4)$$

where:

$$Z = \begin{cases} 1 & if\ P_s'(X_i, Y_i) = P_n'(X_k, Y_k) \\ 0 & otherwise \end{cases}$$

$$S = \begin{cases} 1 & if\ Status = Active \\ 0 & if\ Status = Silent \end{cases}$$

4) Efficiency Overheads Evaluation

Efficiency overheads can be understood by achieving the best balance between the three key issues: security overheads, privacy level, and safety, as illustrated below:

Privacy levels can be enhanced in three ways which are by stopping broadcasting a vehicle's locations, using pseudonyms for short period, and/or changing pseudonyms only when the adversary is probably to be confused (i.e., the two consecutive messages cannot be linked probably).

Safety levels would be negatively affected if a vehicle stops broadcasting its states in which it is difficult to avoid accidents.

[4] https://github.com/karim-emara/PREXT

Thus, SBMs/s should be kept as high as possible. Moreover, when the number of vehicles synchronizing the silent period increases, traceability will be decreased. However, safety would be affected as it is also difficult to get a knowledge of other neighbours' positions which increased the possibility of accidents.

Changing pseudonyms more frequently will increase security overheads. Thus, the number of lost messages increases and safety functionality would be worsening. The best way to balance the three key issues is to increase the confusion level during pseudonym changes and try to reduce pseudonyms change and silent periods.

Accordingly, we calculate the average confusion level percentage (conf%) for each scheme using Equation (5) and calculate the number of traceable vehicles (nVtrac) despite their pseudonyms being changed using Equation (9).

$$Conf\ \% = \frac{1}{nV}\sum_{i}^{nV}\sum_{j}^{vL}\sum_{k}^{br}\beta_{i,j,k} \times 100\%, \qquad (5)$$

where

$$\beta_{i,j,k} = \begin{cases} 1, & SBM_{i,j,k}\ cannot\ link\ to\ SBM_{i,j-1/br,k-1} \\ 0, & Otherwise \end{cases}$$

C. Setting up parameters

To compare the schemes, their parameters are assigned equally whenever it is possible, such as pseudonym lifetime and silent periods. However, each scheme has its own aims, e.g., SRPS aims to avoid any accidents and thus does not have a minimum silent period, whereas SLOW and CSP do not have a silent period range instead of having only one value so we assign 5s to the silent period. In general, longer silent periods increase privacy but decrease safety because of the decreased number of exchanged safety messages [34]. Moreover, a shorter pseudonym lifetime will improve privacy as fewer messages can be linked continuously to the same pseudonym but decrease the efficiency as more pseudonyms are needed and impact the position-based routing protocols [81, 89]. In SRPS and CAPS, vehicles keep track of their neighbours within a specific radius which is initiated by 50 m in this experiment. The 50 m was chosen depending on the speed of roads' sectors that we have selected, in which the max speed is 64 km/h (i.e. nearly 50 m/3s) as these roads are inside city. However, if we try to increase the radius value in order to increase the probability of finding more silent vehicles or/and vehicles with the mix-context, the overheads will also be increased (i.e. extra memory and time are required to keep tracking more vehicles). In the future, we aim to adjust this value depending on the traffic status (i.e., the number of neighbours). For example, if we choose highway roads, the number of neighbours will be decreased and thus we need to increase the radius. The parameters of each scheme and their values are given in Table 2.

To allow vehicles enough time to change their pseudonyms, each test was run for 360s which is 6 times the value of the minimum pseudonyms' lifetime. Since a random trip generation function is used, our evaluation depends on the average values of three different trip databases with different vehicle densities shown in Table 3 and the density of vehicles over time is illustrated in Fig. 8. Finally, we selected the highest beaconing rate for exchanging safety messages, which was 10 Hz to show the worst possible tracking ratio.

Table 2: Schemes Parameters

Scheme	parameters
SRPS	MinPL=60 s
	MaxPL=120 s
	MinSP=0 s
	MaxSP=13 s
	Neighbour Radius=50 m
CAPS	MinPL=60 s
	MaxPL=120 s
	MinSP=3 s
	MaxSP=13 s
	Neighbour Radius=50 m
SLOW	SP=5 s
	Speed Threshold=8 m/s
RSP	PL=60 s
	MinSP=3 s
	MaxSP=13 s
CSP	PL=60 s
	SP=5 s
PPC	MinPL=60 s
	MaxPL=120 s

Table 3: Number of Vehicles

Arrival Rates	Test1	Test2	Test3	Average	vL>=60s	vL>=120
v/1s	162	146	173	160	133	87
v/0.5s	281	308	262	283	230	148
v/0.3s	474	504	468	482	397	272

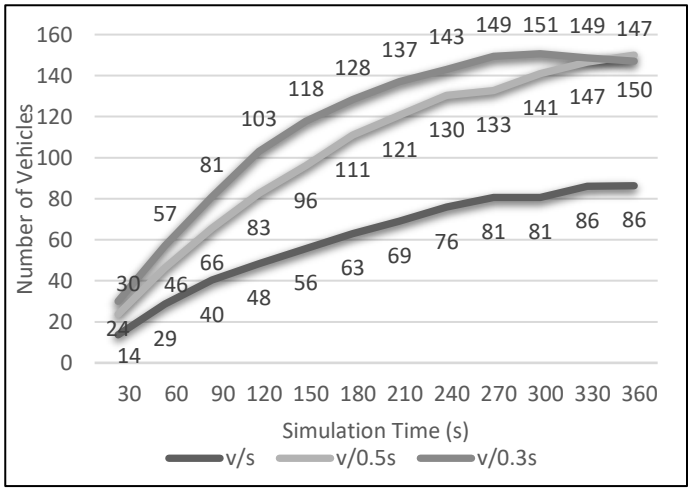

Fig. 8. Density of vehicles during simulation in three arrival rates

VI. SCHEMES COMPARISON

In this section, we provide an experimental comparison of SRPS against the above-mentioned privacy schemes. It is worth mentioning that SRPS, CAPS, and CSP change a vehicle's status cooperatively with its neighbours. However, CSP changes at a periodic interval, while SRPS and CAPS depend on the context of vehicles to reduce wasting pseudonyms in observed situations. Moreover, RSP depends on random periods to change vehicle states while PPC does not have a silent period and the vehicle only changes its pseudonym. Finally, to avoid accidents due to silent periods, SLOW only enters silent when a vehicle's speed is low.

A. Security Overheads

The average number of changed pseudonyms per second for each scheme in different traffic densities is presented in Fig. 9.

Overall, changing pseudonyms in schemes, which allows for a vehicle to decide locally, depending on its state or its neighbours' states, to enter a silent period and/or changing pseudonyms, is increased when the number of vehicles increases, as illustrated below:

- In SRPS and CAPS, each vehicle monitors its neighbours, which increases in dense traffic, to cooperatively start its silent period and/or change pseudonyms. The correlation between traffic density and pseudonym change in SRPS is consistent (i.e., 0.62/s, 0.66/s, and 0.73/s). However, in CAPS, it is inconsistent (i.e., 0.61/s, 0.61/s, and 0.65/s) which may be because a vehicle randomly exits silent and changes its pseudonym when finding a cooperative neighbour.

- In SLOW, the speed of vehicles is usually low in dense traffic. Thus, vehicles enter longer silent periods more frequently (i.e., pseudonyms change only if the silent period is above a predefined threshold) which increases the average pseudonym change (i.e., 0.59/s, 0.66/s, and 0.69/s).

However, traffic density does not affect the centralized schemes that depend only on time to enter silent periods and/or change pseudonyms, as illustrated in Fig. 9, for the three schemes RSP, PPC, and CSP, as illustrated below:

- In RSP and CSP, it suggested enabling vehicles to enter a silent period before changing pseudonyms but in different strategies (in RSP, each vehicle decides locally to enter a random silent period after holding a pseudonym for 60 s while in CSP all vehicles in the network enter a fixed silent period every 60 s depending on system time such as GPS). The average number of pseudonyms change per second of both schemes in all arrival rates is between 0.59/s and 0.63/s.

- In PPC, the traffic density does not have an effect on changing pseudonyms; that is because it enables a vehicle to change its pseudonym periodically after a random period chosen within a predefined range (60 s – 120 s) without considering other factors (such as its speed or its neighbours' state/number).

Overall, PPC has the highest number of pseudonyms up to 0.74 which is probably because the vehicle does not enter a silent period (i.e., after changing pseudonyms, it will directly calculate the pseudonym lifetime to change it again while other schemes start calculating after the silent period has passed).

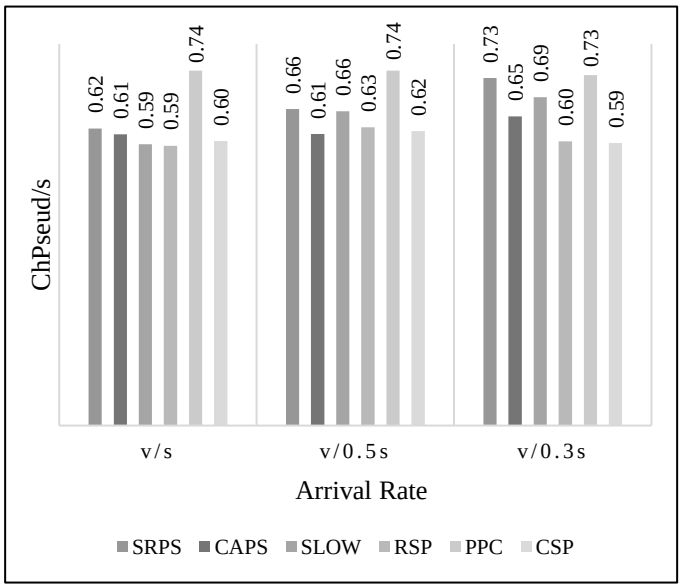

Fig. 9. Number of pseudonym changes per vehicle

B. Privacy-preserving level

Fig. 10 shows the comparisons of the average traceability percentage that are calculated for each scheme using Equation (5), in three different traffic densities. The general trend is that the traceability percentages decrease when the number of vehicles increases except in CSP where it has fluctuated around 5. Moreover, in Fig. 10, the cooperative pseudonym changes and applying silent periods have shown their effectiveness to reduce traceability, as illustrated below:

- In CSP, all vehicles on the road have cooperatively synchronized silent periods and therefore the lowest traceability percentages are achieved when applying CSP. It might be because the chosen road network always has a high number of vehicles as shown in Fig. 8. Moreover, the properties of the chosen road network shown in Fig. 6 would increase the difficulties for the adversary to link messages after the silent period.

- In SRPS and CAPS, a vehicle cooperatively enters a silent period if it recognizes any other nearby silent vehicles. Then, the vehicle starts looking for a mix-context with its neighbour or be in an unexpected position to start broadcasting SBM with its new pseudonym. However, SRPS reduces the traceability percentage nearly by 30% because it starts looking for the mix-context directly when starting its silent period while in CAPS, silent vehicles only monitor each other to find the mix-context while in SRPS, all vehicles monitor each other which increases the probability of finding the mix-context. In CAPS, the hypothesis is that the silent vehicle has to stop sending messages for at least 3s to ensure its privacy but in SRPS, the hypothesis is that the silent vehicle has to start looking for the mix-context with another silent vehicle before being far away from each other (i.e., increase the probability of finding the mix-context). Thus, we amended the parameters in CAPS by omitting the minimum silent period and therefore the traceability is decreased up to 12% as shown in Fig. 11, where ACAPS refers to amended CAPS.

- In SLOW, a vehicle is being silent when its speed is low and the vehicle's speed decreases with the increasing number of vehicles so that more vehicles will cooperatively enter a silent period. Thus, it achieves low traceability percentages specifically when the number of vehicles increases (the traceability percentage reduces to 14%). However, this reduction is not only from the cooperative silent period but also from the length of this period as will be illustrated later at the end of this section in the efficiency.

- In RSP, a vehicle individually enters the silent period and thus it is easier to be tracked (up to 83%) using its spatio-temporal information especially but the adversary could be confused if by chance there are other nearby vehicles being silent as well. However, privacy is worse in PPC because vehicles continuously send messages and are being tracked most of the time even if their pseudonyms change via using spatio-temporal information. Thus, PPC has recorded the highest traceability percentage (it is up to 94%).

C. Safety level

Fig. 12 shows the average number of SBMs per second which is initialized by 10 Hz but it is decreased depending on the silent period. As there is no silent period in PPC, the SBMs are 10 per second which is compatible with the requirement of safety applications. However, SLOW has the lowest updating states (i.e. SBMs/s) that are always less than 6.50 (i.e., it means on average 3.5 messages missed every second). RSP has scored the second lowest value, in which it is less than 7.65 messages every second. Accordingly, SLOW and RSP have the highest negative impact on safety.

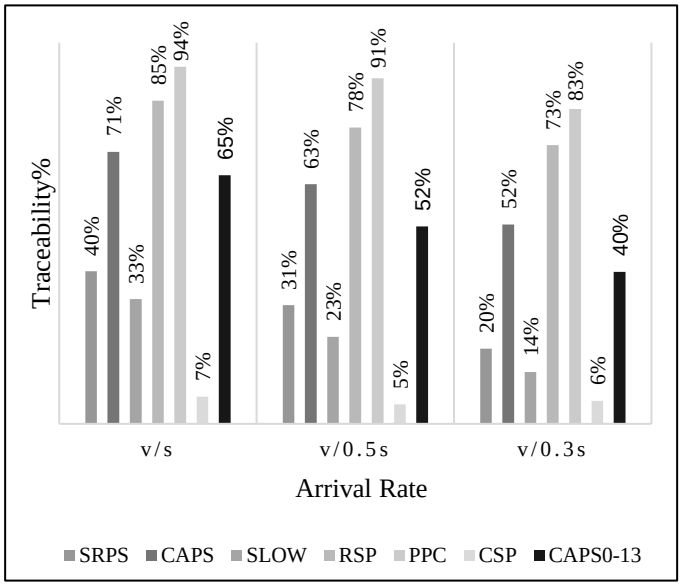

Fig. 10. Average traceability percentage

The cooperative silent period schemes can improve safety by reducing the length of silent periods such as in CSP and CAPS, the value of SBMs is always higher than 9 per second (i.e., if SBMs/s is 9.82, it means vehicles with a journey of 100s will broadcast 982 messages and cease only 18 messages). In CSP all vehicles synchronize their fixed-silent periods while in CAPS, a vehicle synchronizes its silent period with another silent neighbour (s) and exits this period as soon as the adversary could be confused. Similar to CAPS, in SRPS, the vehicle also synchronizes its silent period but is different from CAPS because of the following:

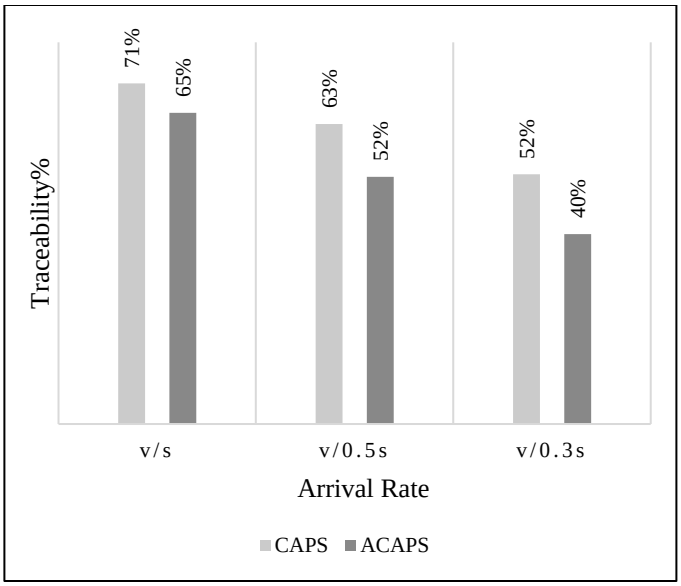

Fig. 11. Traceability in the Adjusted minimum silent period in CAPS

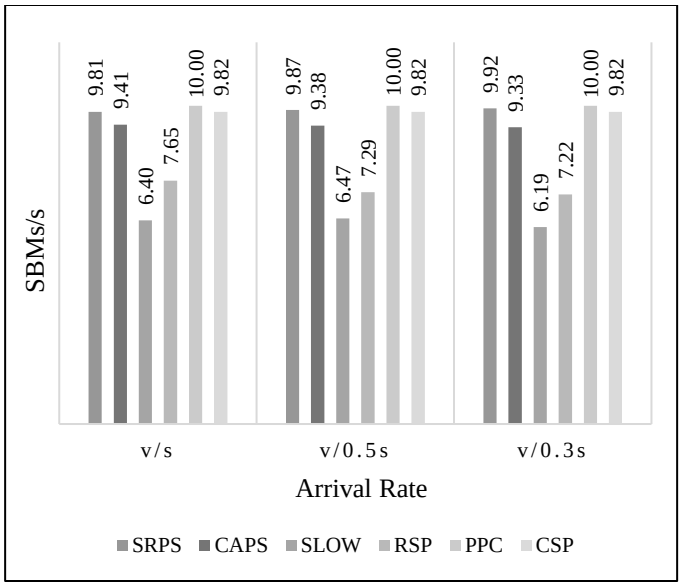

Fig. 12. Average number of sending beacon messages per second

- It is allowed for the silent vehicle to broadcast its state once there is a forward potential accident. In the previous point (privacy level), we discuss the improvement in the privacy level in case of omitting the minimum silent period which was applied to CAPS (ACAPS). This would also improve the safety level as it increases the chance of finding the mix-context as soon as possible which decreases the silent period, as shown in Fig. 13, the number of exchanged messages increased nearly by 0.20,0.30, and 0.60 along with the arrival rate.

- SRPS has increased SBMs/s over CAPS also because not only the silent vehicle is looking for a mix-context with its neighbours but also active vehicles. Thus, an active vehicle can change its pseudonym without being silent if its state is probably to be mixed with other nearby vehicles (silent/active), which increased the SBMs/s. Moreover, when the number of vehicles increased, the possibility of accidents increased, and the silent period minimized (i.e., SBMs/s increased by 0.40 in sparse traffic then 0.49 and up to 0.60 in dense traffic).

- Finally, the number of predicted accidents that could be prevented in SRPS is illustrated in Fig. 14, in which it is increased with the increase in the number of vehicles.

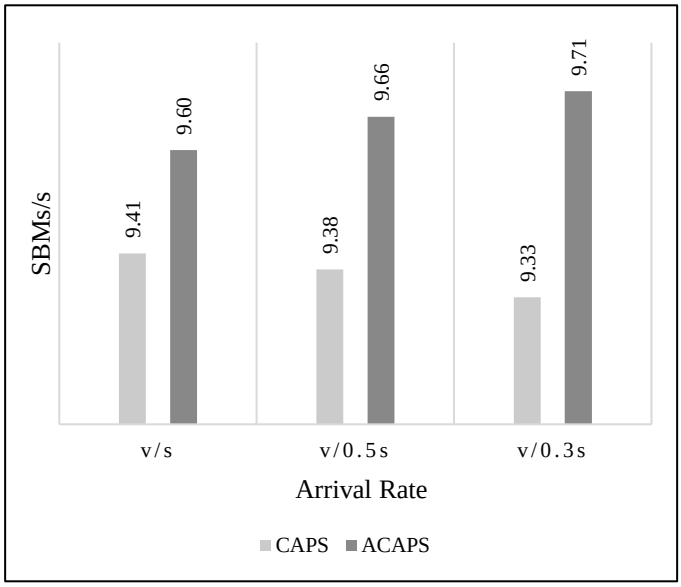

Fig. 13. SBMs in the Adjusted minimum silent period in CAPS (ACAPS)

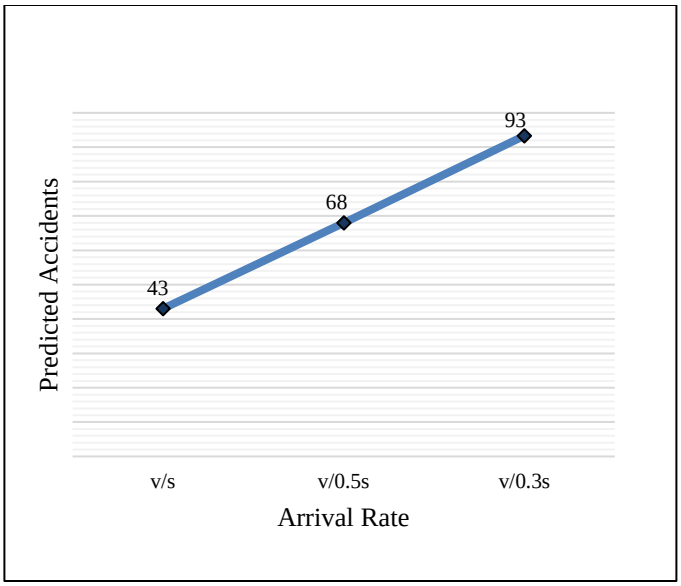

Fig. 14. Number of predicted accidents in SRPS

D. *Efficiency*

Fig. 15 demonstrates the average confusion level and Fig. 16 demonstrates the number of vehicles that are unable to protect their privacy instead of changing pseudonyms. The results of these two figures are summarized next.

- It is obvious from these two figures that the higher confusion level would reduce the number of traceable vehicles and vice versa.
- The confusion level is increased when the density of vehicles increases (i.e., the arrival rates increase).
- The silent period is highly important to prevent long-term linkability and maintain privacy, otherwise, vehicles would be traceable most of the time via their spatio-temporal information. Accordingly, PPC has the lowest confusion level, in which the highest is only 10%, and thus changing pseudonyms has usually failed (i.e., scored the highest nV_{trac} which is up to 250 vehicles wasted pseudonyms).
- The random silent period is insufficient as well because if the vehicle changes its pseudonym alone, it will remain traceable as shown in Fig. 15. Thus, RSP is similar to PPC, it is inefficient in which the highest conf% is only 22% and nV_{trac} is up to 141.
- CSP has achieved the best confusion level of 100% and the lowest wasting pseudonyms (less than 19 vehicles). Despite CSP can achieve the best confusion level, it compromises safety during its silent periods as all vehicles will stop broadcasting their states.
- SLOW is able to confuse the adversary due to its long silent period, as demonstrated in Fig. 12 nearly 4 messages are missed every second which has a negative impact on safety.
- Finally, CAPS and SRPS have employed the in-vehicle tracker to reduce the silent period by monitoring the confusion level and as soon as it is expected that the adversary could be confused, the vehicle will exit the silence. We enhance the confusion level significantly by more than 39% and reduce wasting pseudonyms specifically when the number of vehicles increased. That is because, in our scheme, the silent vehicle starts looking for the confusing content with all nearby vehicles (silent/active) as soon as being silent. In contrast with CAPS, the silent vehicle will wait for 3s before start looking to be confused with another silent vehicle.

The comparisons between the six pseudonym-changing schemes are concluded in Table 4. by calculating the average values of the three arrival rates from Fig. 8 to Fig. 13 and then assigning the score 6 to the worst rate and 1 to the best rate.

- SLOW has the lowest vehicle status updates as shown in Fig. 10, which negatively impacts safety functionality. Moreover, the value is decreased with a higher density of vehicles while more accidents could occur. Thus, even if it achieves a good privacy level due to ceasing messages for a longer period, it is not recommended as safety is the first aim of VANET applications.

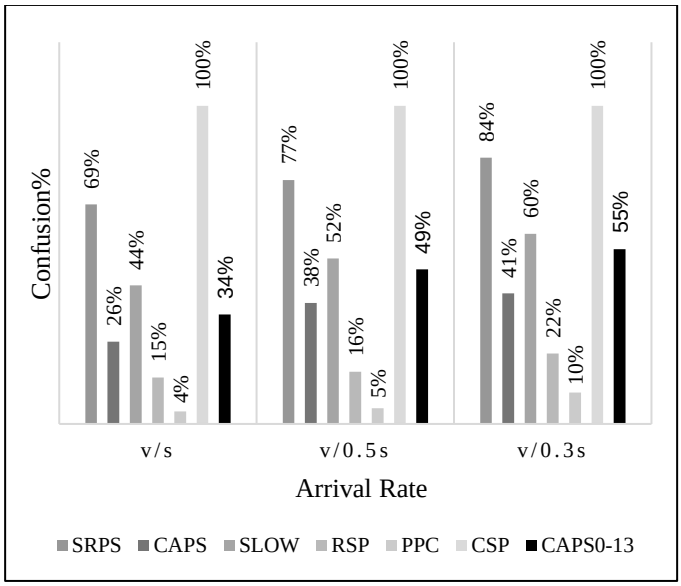

Fig. 15. The average confusion level percentage

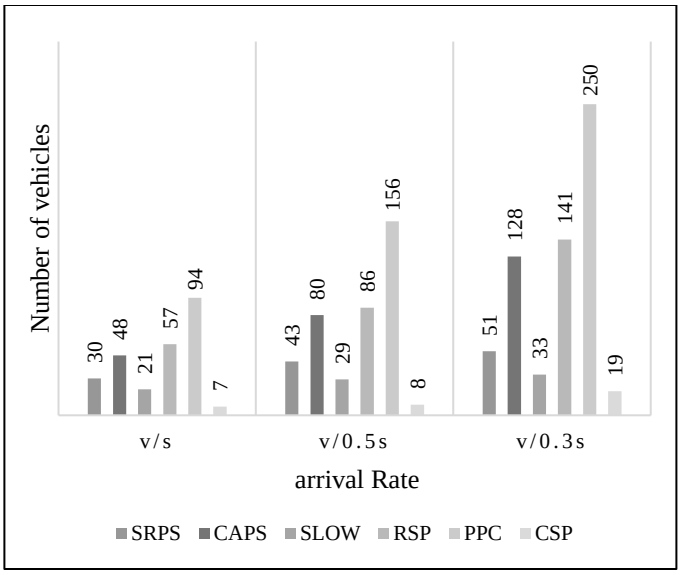

Fig. 16 Number of vehicles wasted pseudonyms

Table 4: Schemes Comparison

Scheme	Privacy	Safety	Overheads
SRPS	3	2	2
CAPS	4	3	1
SLOW	2	6	4
RSP	5	5	5
CSP	1	4	6
PPC	6	1	3

- CSP has the highest overhead as shown in figures 12 and 13 in which more than 85% of vehicles were changing their pseudonym every minute. Moreover, instead of achieving the highest privacy level, the negative impact of such a high overhead on the functionality of VANET applications would be high. Besides, VANET would be disabled when all vehicles enter the silent period at the same time.

- PPC leads to long-term linkability and thus wasting pseudonyms, as it is continuously sending messages that are easily linkable through spatio-temporal information. This is confirmed in figures 8 and 10 with PPC having the highest linkability ratio.

- CAPS has achieved the lowest overhead which is the main aim of this scheme as shown in figures 12 and 13.

- SRPS has achieved the best balance between the three key issues of privacy, safety, and efficiency according to the result listed in Table 4. The main aim of SRPS is compatible with the main aim of VANET, which is to improve road safety. It is the only scheme that allows a vehicle in its silent period to check for the possibility of an accident as shown in Fig. 11 and exits the silent status in case an accident could happen (i.e., assuming the vehicle in its silent period will stop sending its state but keep receiving its neighbours' states). Moreover, it is obvious from Fig. 10, the SRPS is the only privacy scheme that does not reduce sending messages when the number of vehicles increases in which more accidents are expected.

VII. Conclusions and Future Work

In this paper, we have presented a new scheme, called the safety-related privacy scheme (SRPS), which improves the privacy level of vehicles and enhances the efficiency of safety applications. The improvements include: 1) avoiding accidents during silent periods by allowing silent vehicles to track all nearby vehicles, 2) reducing silent periods by changing pseudonyms without entering silent periods, in which active vehicles keep tracking nearby silent vehicles and then changing their pseudonyms if there is a probability of confusion with silent vehicles, 3) further reduction in the silent period by allowing a silent vehicle to track all vehicles in its area and resuming broadcasting safety messages when finding a probability of mix-contexts. Finally, we have compared the efficiency of our scheme with the other five well-known pseudonym-changing schemes based on the statistical data collected from the OMNET++ and PREXT simulators. The results have shown that our scheme produces an efficient balance between safety and privacy. In future work, we aim to adjust the distance of the nearby vehicles depending on the traffic density in which the overheads could be reduced during the high density and the probability of finding the mixed context could be increased in sparse traffic especially if we apply our scheme in different roads (highway and urban roads).

Ethical approval: This article does not contain any studies with human participants performed by any of the authors.

Research Data Policy and Data Availability Statements. Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

References

[1] M. N. Smith, "The number of cars worldwide is set to double by 2040," in "World Economic Forum, Geneva," 2016, Available: https://www.weforum.org/agenda/2016/04/the-number-of-cars-worldwide-is-set-to-double-by-2040, Accessed on: 22/11/2019.

[2] W. H. O. (WHO), "Road traffic injuries," United Nation,21/06/2021, Available: https://www.who.int/news-room/fact-sheets/detail/road-traffic-injuries, Accessed on: 11/03/2022.

[3] A. Vaibhav, D. Shukla, S. Das, S. Sahana, and P. Johri, "Security challenges, authentication, application and trust models for vehicular ad hoc network-a survey," *International Journal of Wireless and Microwave Technologies (IJWMT)*, vol. 7, no. 3, pp. 36-48, 2017.

[4] D. SAE, "J2735 dedicated short range communications (dsrc) message set dictionary," *Society of Automotive Engineers, DSRC Committee*, 2009.

[5] F. Yang, S. Wang, J. Li, Z. Liu, and Q. Sun, "An overview of internet of vehicles," *China communications*, vol. 11, no. 10, pp. 1-15, 2014.

[6] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: Architecture, enabling technologies, security and

privacy, and applications," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125-1142, 2017.
[7] S. A. Soleymani, S. Goudarzi, M. H. Anisi, M. Zareei, A. H. Abdullah, and N. J. V. C. Kama, "A security and privacy scheme based on node and message authentication and trust in fog-enabled VANET," vol. 29, p. 100335, 2021.
[8] S. Goudarzi *et al.*, "A privacy-preserving authentication scheme based on Elliptic Curve Cryptography and using Quotient Filter in fog-enabled VANET," p. 102782, 2022.
[9] J. A. Stankovic, "Research directions for the internet of things," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 3-9, 2014.
[10] T. A. Litman, "Pay-as-you-drive vehicle insurance: implementation, benefits, and costs," 2006.
[11] T. ETSI, "Intelligent transport systems (ITS); vehicular communications; basic set of applications; definitions," ETSI TR 102 6382009.
[12] F. Ahmed-Zaid *et al.*, "Vehicle Safety Communications–Applications (VSC-A) Final Report: Appendix Volume 3 Security," 2011.
[13] P. Mundhe, S. Verma, and S. J. C. S. R. Venkatesan, "A comprehensive survey on authentication and privacy-preserving schemes in VANETs," *Computer Science Review*, vol. 41, p. 100411, 2021.
[14] T. Benz, "PRECIOSA: V2X Privacy Issue Analysis," IST-224201, 2009, Available: https://cordis.europa.eu/docs/projects/cnect/1/224201/080/deliverables/001-PRECIOSAD1V2XPrivacyIssuesAnalysisv41.pdf, Accessed on: 12/2/2009.
[15] Y. Jiang, S. Ge, and X. J. I. A. Shen, "AAAS: an anonymous authentication scheme based on group signature in VANETs," *IEEE Access*, vol. 8, pp. 98986-98998, 2020.
[16] F. Kargl and J. Petit, "Security and privacy in vehicular networks," in *Vehicular Communications and Networks*: Elsevier, 2015, pp. 171-190.
[17] L. Benarous, B. Kadri, S. Bitam, and A. J. I. J. o. C. S. Mellouk, "Privacy-preserving authentication scheme for on-road on-demand refilling of pseudonym in VANET," *International Journal of Communication Systems*, vol. 33, no. 10, p. e4087, 2020.
[18] K. Zhang, X. Liang, R. Lu, and X. Shen, "Sybil attacks and their defenses in the internet of things," *IEEE Internet of Things Journal*, vol. 1, no. 5, pp. 372-383, 2014.
[19] B. Wiedersheim, Z. Ma, F. Kargl, and P. Papadimitratos, "Privacy in inter-vehicular networks: Why simple pseudonym change is not enough," in *Wireless On-demand Network Systems and Services (WONS), 2010 Seventh International Conference on*, 2010, pp. 176-183: IEEE.
[20] K. Emara, W. Woerndl, and J. Schlichter, "Vehicle tracking using vehicular network beacons," in *2013 IEEE 14th International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM)*, 2013, pp. 1-6: IEEE.
[21] J. Freudiger, M. Raya, M. Félegyházi, P. Papadimitratos, and J.-P. Hubaux, "Mix-zones for location privacy in vehicular networks," in *ACM Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS)*, 2007, no. LCA-CONF-2007-016.
[22] I. S. Shaleesh, A. A. Almohammedi, N. I. Mohammad, and A. A. J. T. J. o. E. S. Ahmad, "Cooperation and radio silence strategy in Mix Zone to Protect Location Privacy of Vehicle in VANET," *Tikrit Journal of Engineering Sciences*, vol. 28, no. 1, pp. 31-39, 2021.
[23] Y. Li, Y. Yin, X. Chen, J. Wan, G. Jia, and K. J. I. T. o. I. T. S. Sha, "A Secure Dynamic Mix Zone Pseudonym Changing Scheme Based on Traffic Context Prediction," *IEEE Transactions on Intelligent Transportation Systems*, 2021.
[24] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki, "CARAVAN: Providing location privacy for VANET," Washington Univ Seattle Dept Of Electrical Engineering,2005.
[25] A. Didouh, Y. El Hillali, A. Rivenq, and H. J. E. Labiod, "Novel Centralized Pseudonym Changing Scheme for Location Privacy in V2X Communication," *Energies*, vol. 15, no. 3, p. 692, 2022.
[26] 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*, 2015, p. 21: ACM.
[27] K. Emara, W. Woerndl, and J. Schlichter, "Context-based pseudonym changing scheme for vehicular adhoc networks," *arXiv preprint arXiv:1607.07656*, 2016.
[28] W. Xin, H. M. Moonam, J. Petit, and W. Whyte, "Towards a Balance between Privacy and Safety: Microsimulation Framework for Assessing Silence-Based Pseudonym-Change Schemes," *Transportation Research Record*, p. 0361198119825833, 2019.
[29] H. Dok, H. Fu, R. Echevarria, and H. Weerasinghe, "Privacy issues of vehicular ad-hoc networks," *International Journal of Future Generation Communication and Networking*, vol. 3, no. 1, pp. 17-32, 2010.
[30] M. Gerlach, "Assessing and improving privacy in VANETs," *ESCAR, Embedded Security in Cars*, 2006.
[31] 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*, 2006, pp. 19-28: ACM.
[32] J. Liao and J. Li, "Effectively changing pseudonyms for privacy protection in vanets," in *Pervasive Systems, Algorithms, and Networks (ISPAN), 2009 10th International Symposium on*, 2009, pp. 648-652: IEEE.
[33] L. Buttyán, T. Holczer, A. Weimerskirch, and W. Whyte, "Slow: A practical pseudonym changing scheme for location privacy in vanets," in *Vehicular Networking Conference (VNC), 2009 IEEE*, 2009, pp. 1-8: IEEE.
[34] K. A. A. E.-S. Emara, "Safety-aware location privacy in vehicular ad-hoc networks," Technische Universität München, 2016.
[35] J. Guo and N. Balon, "Vehicular ad hoc networks and dedicated short-range communication," *University of Michigan*, 2006.
[36] A. M. Vegni, M. Biagi, and R. Cusani, "Smart vehicles, technologies and main applications in vehicular ad hoc networks," in *Vehicular technologies-deployment and applications*: IntechOpen, 2013.
[37] E. Schoch and F. Kargl, "On the efficiency of secure beaconing in vanets," in *Proceedings of the third ACM conference on Wireless network security*, 2010, pp. 111-116: ACM.
[38] F. Bai, T. Elbatt, G. Hollan, H. Krishnan, and V. Sadekar, "Towards characterizing and classifying communication-based automotive applications from a wireless networking perspective," in *Proceedings of IEEE Workshop on Automotive Networking and Applications (AutoNet)*, 2006, pp. 1-25: San Francisco, CA, USA.
[39] S. Djahel and Y. Ghamri-Doudane, "A robust congestion control scheme for fast and reliable dissemination of safety messages in VANETs," in *2012 IEEE Wireless Communications and Networking Conference (WCNC)*, 2012, pp. 2264-2269: IEEE.
[40] V. J. U. D. o. T. CAMP, Washington, DC, Tech. Rep. DOT HS 809 859, "Vehicle safety communications project task 3 final report-identify intelligent vehicle safety applications enabled by dsrc," 2005.
[41] A. Studer, M. Luk, and A. Perrig, "Efficient mechanisms to provide convoy member and vehicle sequence authentication in VANETs," in *2007 Third International Conference on Security and Privacy in Communications Networks and the Workshops-SecureComm 2007*, 2007, pp. 422-432: IEEE.
[42] L. Wei, J. Cui, Y. Xu, J. Cheng, H. J. I. T. o. I. F. Zhong, and Security, "Secure and lightweight conditional privacy-preserving authentication for securing traffic emergency messages in VANETs," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 1681-1695, 2020.
[43] M. Khodaei and P. Papadimitratos, "Evaluating on-demand pseudonym acquisition policies in vehicular communication systems," in *Proceedings of the First International Workshop on Internet of Vehicles and Vehicles of Internet*, 2016, pp. 7-12: ACM.
[44] A. Studer, E. Shi, F. Bai, and A. Perrig, "TACKing together efficient authentication, revocation, and privacy in VANETs," in *Sensor, Mesh and Ad Hoc Communications and Networks, 2009. SECON'09. 6th Annual IEEE Communications Society Conference on*, 2009, pp. 1-9: IEEE.
[45] M. N. Tahir, M. Katz, and U. Rashid, "Analysis of VANET wireless networking technologies in realistic environments," in *2021 IEEE Radio and Wireless Symposium (RWS)*, 2021, pp. 123-125: IEEE.
[46] W. Yang, "Security in vehicular ad hoc networks (vanets)," in *Wireless network security*: Springer, 2013, pp. 95-128.
[47] T. Leinmüller *et al.*, "Sevecom-secure vehicle communication," in *IST Mobile and Wireless Communication Summit*, 2006, no. POST_TALK.

[48] M. Gruteser and B. Hoh, "On the anonymity of periodic location samples," in *International Conference on Security in Pervasive Computing*, 2005, pp. 179-192: Springer.

[49] (2016, 02/02/2020). *What are your main concerns about IoT adoption?* . Available: https://www.statista.com/statistics/690190/iot-adoption-hurdles-and-obstacles/

[50] M. Raya and J.-P. Hubaux, "The security of vehicular ad hoc networks," presented at the Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks, Alexandria, VA, USA, 2005.

[51] A. Boualouache, S.-M. Senouci, and S. Moussaoui, "Vlpz: The vehicular location privacy zone," *Procedia Computer Science*, vol. 83, pp. 369-376, 2016.

[52] B. Palanisamy and L. Liu, "Mobimix: Protecting location privacy with mix-zones over road networks," in *Data Engineering (ICDE), 2011 IEEE 27th International Conference on*, 2011, pp. 494-505: IEEE.

[53] X. Liu and X. Li, "Privacy preservation using multiple mix zones," in *Location Privacy Protection in Mobile Networks*: Springer, 2013, pp. 5-30.

[54] X. Liu, H. Zhao, M. Pan, H. Yue, X. Li, and Y. Fang, "Traffic-aware multiple mix zone placement for protecting location privacy," in *2012 Proceedings IEEE INFOCOM*, 2012, pp. 972-980: IEEE.

[55] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen, "Pseudonym changing at social spots: An effective strategy for location privacy in vanets," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 1, pp. 86-96, 2012.

[56] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen, "Anonymity analysis on social spot based pseudonym changing for location privacy in VANETs," in *2011 IEEE International Conference on Communications (ICC)*, 2011, pp. 1-5: IEEE.

[57] 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, 2007.

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

[59] 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.

[60] Y. Pan, Y. Shi, and J. Li, "A novel and practical pseudonym change scheme in VANETs," in *International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, 2017, pp. 413-422: Springer.

[61] H. Rifa-Pous and J. Herrera-Joancomartí, "Computational and energy costs of cryptographic algorithms on handheld devices," *Future internet*, vol. 3, no. 1, pp. 31-48, 2011.

[62] M. Brown, D. Hankerson, J. López, and A. Menezes, "Software implementation of the NIST elliptic curves over prime fields," in *Cryptographers' Track at the RSA Conference*, 2001, pp. 250-265: Springer.

[63] 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.

[64] Y. Pan, J. Li, L. Feng, and B. Xu, "An analytical model for random changing pseudonyms scheme in VANETs," in *Network Computing and Information Security (NCIS), 2011 International Conference on*, 2011, vol. 2, pp. 141-145: IEEE.

[65] Y. Pan, J. Li, L. Feng, and B. Xu, "An analytical model for random pseudonym change scheme in VANETs," *Cluster Computing*, vol. 17, no. 2, pp. 413-421, 2014.

[66] A. R. Beresford and F. Stajano, "Location privacy in pervasive computing," *IEEE Pervasive computing*, no. 1, pp. 46-55, 2003.

[67] A. R. Beresford and F. Stajano, "Mix zones: User privacy in location-aware services," in *Pervasive Computing and Communications Workshops, 2004. Proceedings of the Second IEEE Annual Conference on*, 2004, pp. 127-131: IEEE.

[68] A. Tomandl, F. Scheuer, and H. Federrath, "Simulation-based evaluation of techniques for privacy protection in VANETs," in *2012 IEEE 8th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, 2012, pp. 165-172: IEEE.

[69] W. A. Leaf and D. F. Preusser, *Literature review on vehicle travel speeds and pedestrian injuries*. US Department of Transportation, National Highway Traffic Safety Administration, 1999.

[70] K. Emara, W. Woerndl, and J. Schlichter, "Beacon-based vehicle tracking in vehicular ad-hoc networks," 2013.

[71] D. Jiang, V. Taliwal, A. Meier, W. Holfelder, and R. Herrtwich, "Design of 5.9 GHz DSRC-based vehicular safety communication," *IEEE Wireless Communications*, vol. 13, no. 5, 2006.

[72] L. Guo *et al.*, "A secure mechanism for big data collection in large scale internet of vehicle," *IEEE Internet of Things Journal*, vol. 4, no. 2, pp. 601-610, 2017.

[73] I. Committee, "Ieee standard for wireless access in vehicular environments-security services for applications and management messages," *IEEE Vehicular Technology Society*, vol. 1609, 2013.

[74] L. Fischer, A. Aijaz, C. Eckert, and D. Vogt, "Secure revocable anonymous authenticated inter-vehicle communication (SRAAC)," in *4th Conference on Embedded Security in Cars (ESCAR 2006), Berlin, Germany*, 2006: Citeseer.

[75] F. Schaub, F. Kargl, Z. Ma, and M. Weber, "V-tokens for Conditional Pseudonymity in VANETs," in *Wireless Communications and Networking Conference (WCNC), 2010 IEEE*, 2010, pp. 1-6: IEEE.

[76] N. Bißmeyer, J. Petit, and K. M. Bayarou, "CoPRA: Conditional pseudonym resolution algorithm in VANETs," in *2013 10th annual conference on wireless on-demand network systems and services (WONS)*, 2013, pp. 9-16: IEEE.

[77] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of computer security*, vol. 15, no. 1, pp. 39-68, 2007.

[78] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym schemes in vehicular networks: A survey," *IEEE communications surveys & tutorials*, vol. 17, no. 1, pp. 228-255, 2015.

[79] R. E. Kalman, "A new approach to linear filtering and prediction problems," *Journal of basic Engineering*, vol. 82, no. 1, pp. 35-45, 1960.

[80] R. J. Fitzgerald, "Development of practical PDA logic for multitarget tracking by microprocessor," in *1986 American Control Conference*, 1986, pp. 889-898: IEEE.

[81] C. Lochert, H. Hartenstein, J. Tian, H. Fussler, D. Hermann, and M. Mauve, "A routing strategy for vehicular ad hoc networks in city environments," in *IEEE IV2003 Intelligent Vehicles Symposium. Proceedings (Cat. No. 03TH8683)*, 2003, pp. 156-161: IEEE.

[82] C. Sommer, R. German, and F. Dressler, "Bidirectionally Coupled Network and Road Traffic Simulation for Improved IVC Analysis," *IEEE Transactions on Mobile Computing*, vol. 10, no. 1, pp. 3-15, 2011.

[83] P. A. Lopez *et al.*, "Microscopic Traffic Simulation using SUMO," in *2018 21st International Conference on Intelligent Transportation Systems (ITSC)*, 2018, pp. 2575-2582: IEEE.

[84] K. Emara, "PREXT: Privacy Extension for Veins VANET Simulator," presented at the in Vehicular Networking Conference (VNC), 2016.

[85] M. Haklay and P. Weber, "Openstreetmap: User-generated street maps," *Ieee Pervas Comput*, vol. 7, no. 4, pp. 12-18, 2008.

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

[87] L. Buttyán, T. Holczer, and I. Vajda, "On the effectiveness of changing pseudonyms to provide location privacy in VANETs," in *European Workshop on Security in Ad-hoc and Sensor Networks*, 2007, pp. 129-141: Springer.

[88] K. Emara, W. Woerndl, and J. Schlichter, "On evaluation of location privacy preserving schemes for VANET safety applications," *Computer Communications*, vol. 63, pp. 11-23, 2015.

[89] I. Stojmenovic, "Position-based routing in ad hoc networks," *IEEE communications magazine*, vol. 40, no. 7, pp. 128-134, 2002.