Article

WHISPER: A Location Privacy-Preserving Scheme Using Transmission Range Changing for Internet of Vehicles.

Messaoud Babaghayou [1]*, Nabila Labraoui [1], Ado Adamou Abba Ari [2,3], Mohamed Amine Ferrag [4], Leandros Maglaras [5]*, Helge Janicke [6]

[1] University of Abou Bekr Belkaid, Chetouane Tlemcen 13000, Algeria
[2] University of Paris Saclay, Avenue États-Unis 78035 Versailles, France
[3] University of Maroua, P.O. Box 814 Maroua, Cameroon
[4] Department of Computer Science, Guelma University, Guelma 24000, Algeria
[5] School of Computer Science and Informatics, De Montfort University, Leicester LE1 9BH, UK
[6] Cyber Security Cooperative Research Centre (CSCRC), Perth, WA 6027, Australia
* Correspondence: messaoud.babaghayou@univ-tlemcen.dz

Version March 27, 2021 submitted to Sensors

Abstract: Internet of Vehicles (IoV) has the potential to enhance road-safety with environment sensing features provided by embedded devices and sensors. This benignant feature also raises privacy issues: as vehicles announce their ne-grained whereabouts mainly for safety requirements, adversaries can leverage this to track and identify users. Various privacy-preserving schemes have been designed and evaluated, for example, mix-zone, encryption, group forming, and silent-period-based techniques. However, they all suffer inherent limitations. In this paper, we review these limitations and propose WHISPER, a safety-aware location privacy-preserving scheme that adjusts the transmission range of vehicles in order to prevent continuous location monitoring. We detail the set of protocols used by WHISPER, then we compare it against other privacy-preserving schemes. The results show that WHISPER outperformed the other schemes by providing better location privacy levels while still ful lling the road-safety requirements.

Keywords: location privacy, pseudonym change strategy, transmission range adjustment, IoV privacy, IoV safety, VANET

1. Introduction

Vehicular Ad-hoc Network (VANET) with its variety of protocols (e.g., IEEE 802.11P, IEEE 1609) [1] and communication types like Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) [2] have served as a basis for the promising Internet of Vehicles (IoV) paradigm [3–5]. IoV bene ts from VANET to extend the usability range by allowing non-conventional communications and applications, e.g., Vehicle to Everything (V2X) communications, to emerge. IoV is an important sub-domain of IoT as well as a clear example of System of Systems domain [6]. Fig. 2 shows the V2X external communications and internal equipments. A vehicle using V2X can enhance road-safety by broadcasting Basic Safety Message (BSM) [7] beacon message with a 300m range and a frequency of 1 to 10 BSMs per second from its OBU [8]. The data included in BSMs are illustrated in Fig. 1. This allows receiving vehicles to be aware of the potential dangers posed by nearby vehicles in addition to managing the road-congestion, that is considered as one of the high-level challenges [9], through the network of Road-Side-Units (RSUs).

Figure 1. BSM beacon format

Figure 2. V2X technology illustration

Since BSMs contain ne-grained location data, even though they are useful for road safety, they do open privacy-related issues: any entity with eavesdropping capability can monitor the whereabouts of IoV users. mart cars' safety and infotainment applications may also reveal user private information. Using these data, a system that is ultimately designed to offer safety and comfort applications to drivers can be abused by third parties, such as employers, insurance companies or criminal organizations to track individuals [12]. The introduction of mechanisms that can preserve location privacy has become a new research trend that has attracted widespread attention among researchers. Most existing location privacy schemes, e.g., mix-zone, synchronized schemes, etc., are ineffective in achieving a high privacy level because of the very precise locations included in BSMs and because of their resource and overhead-consuming characteristics. The better candidate mechanism used is that of the silent period schemes by ceasing BSMs broadcasting until emerging from another location with a new pseudo-identi er. However, the major drawback of such a technique is the sacri ce of safety for the sake of privacy [13].

As safety is way substantial requirement underpinning the introduction of V2X communication, silent period schemes have been received with reservations by the research community. Our motivation is to nd a solution to allow the nearby vehicles to be aware (providing safety) and reduce an adversary opportunity to employ eavesdropping attacks. The purpose of protecting user location privacy in the IoV context is related to the risk of user private information being disclosed. Location privacy is directly connected to other types of privacy. Location privacy leaks can reveal the home and work address of the driver, some visits to sensitive places, his travel habits, times of absence from home, etc. Correlation of this spatio-temporal information with other data allows an adversary to come to conclusions about health habits, social contacts, religion beliefs, etc. Protecting user location privacy has many bene ts both to the users and the system. First of all privacy preservation improves the performance of the IoV system and reduces users' concerns about security and privacy. Thus IoVs can attract more users to use their functions and applications, especially those that are related to safety, promoting further innovation and development in the automobile industry. In this paper, we propose a mechanism that is reducing the transmission range occasionally to just inform the nearby vehicles and prevent the adversary from tracking users through BSMs. The design of a pseudonym change scheme that exploits such a transmission range adjustment feature is inspired by our previous work [9] where we studied the effect of changing the transmission range using existing strategies. The novel method that is proposed in the current article, entitled "WHISPER", maintains road-safety since vehicles are only hidden from the tracker (occasionally) and not from their close vehicles (always) which makes the use of WHISPER an advantageous feature that comes in favor of safety and privacy.

The main contributions of this paper are as follows:

- We propose a novel location privacy-preserving scheme, entitled WHISPER, that maintains privacy without sacri cing safety.

- We detail the techniques and protocols used by WHISPER for adjusting the transmission range and performing pseudonym change.
- We compare WHISPER to well-known location privacy-preserving schemes as CPN [14], RSP [15] and SLOW [16] in a manhattan-grid model with various densities using location privacy and QoS as metrics in addition to a comparative table.

The remainder of this paper is organized as follows: In section 2, we review and discuss existing techniques to address the location privacy problem in V2X. Then, we give our supposed system model in section 3. Next, the proposed WHISPER scheme with its techniques and protocols are presented in section 4. After that, WHISPER performances are analyzed in section 5. Later in section 6, we discuss the schemes in the obtained results perspective. Finally, section 7 concludes the paper and gives future work.

2. Related Work

The location privacy problem is being considered as one of the crucial parameters for the adoption of a successful IoV system. There are a number of efficient privacy preservation techniques for LBS (e.g.), however, they are using location obfuscating (e.g., [30]), hiding, anonymizing, and making dummies. These techniques are explained in [22], however, they are not recommended in the context of achieving safety via BSMs broadcasting and this is because of the safety-related requirements that do not recommend risking drivers' safety for the sake of privacy: using such techniques implies tricking the adversary alongside the nearby vehicles.

Beresford and Stajano (2003) [31] introduce the mix-group concept; that is defined as a group region where vehicles are mixed within that region. However, broadcast beacons that contain high precision locations still represent a problem for drivers' privacy. Based on the mix-group concept, Freudiger et al. (2007) proposed CMIX [17], a location privacy scheme that uses symmetric key-based cryptography to ensure that beacons are not readable by the adversary. This approach uses a key shared by RSUs to encrypt BSMs. Their approach did not consider the internal attacker scenario in addition to the heavy infrastructure reliance.

The silent period, a concept that was firstly introduced in the field of wireless LANs by Huang et al. (2005) [15], ceases any BSM broadcasts for a specific period of time in order to achieve a good level of privacy. The strategy works well against correlation attacks [32]. However the silent periods introduce a reduction in safety relevant data being shared within the IoV - reducing the safety properties of the system and potentially invalidating safety requirements of ("ETSI TR 103 415" [33] and "ETSI TS 103 601" [34] Standards). This safety-privacy trade-off is addressed in our work on WHISPER.

Buttyán et al. (2009) proposed the SLOW strategy [16]. SLOW aims at letting vehicles choose the best moment to update their pseudonyms. This decision is based on a threshold of the vehicles speed, assuming that for low speeds the risk of crashes will be low and the vehicle is allowed to stay silent for a period of time. SLOW, does not necessarily respect the beaconing frequency of once per second at minimum [9] and this occurs in congested areas. Eckhoff et al. (2011) proposed Slotswap [18], a strategy that uses a time-slotted pool to manage pseudonyms by each vehicle. Each slot is used for a period of time with the possibility to re-use pseudonyms after reaching the last time-slot. The exchange of pseudonyms between time-slots of different vehicles is also an option of their approach.

Lu et al. (2012) leveraged the feature of social spots [19] for privacy enhancement. Social spots are places in where vehicles meet more frequently and are characterized with the high densities such as intersections and parking lots. An adversary will be more confused in such dense areas because the probability to successfully match the old changed pseudonym with the new one inside a set of vehicles n will be tied inversely with the size of n. In the same social context, Babaghayou et al. (2019) proposed the Extreme Points Privacy (EPP) [22] scheme. EPP exploits the feature that IoV users are generally situated in district (where they live) and since turning the vehicle's engine results in beaconing, this gives an indication to the adversary that the user is about to leave his home, thus, the authors propose to cease beaconing until leaving the district. The probability of leaving a district under different scenarios are evaluated.

Tomandl et al. (2012) [35] investigated the effects of both mix-zones and silent periods. The work was also implemented by Emmara et al. (2016) in their privacy extension PREXT [36] under the name of Coordinated Silent Period (CSP). Emmara et al. (2015) also proposed their own privacy scheme: Context-Aware Privacy

Table 1. Comparison of Related works

Year	Scheme	Network model	Technique used	Pros (+)	Cons (-)
2007	Freudiger et al. [17]	Vehicular networks	Symmetric key-based cryptography	+ Provides location privacy	- The proposed scheme did not consider the internal attacker scenario
2009	Buttyán et al. [16]	Vehicular networks	Pseudonym changing scheme	+ Ensures both silent periods and synchronized pseudonym change in time and space	- Intrusion detection is not considered
2011	Eckhoff et al. (2011) [18]	Intelligent transportation systems	A time-slotted pool to manage pseudonyms by each vehicle	+ Affordable location privacy	- Resistance against Sybil attacks is not considered
2012	Lu et al. [19]	Vehicular networks	The feature of social spots, which are places in where vehicles meet more frequently	+ Provides the location privacy	- Limited analysis against threat models
2013	Pan and Li [14]	Vehicular networks	Cooperative pseudonym change scheme based on the number of neighbors	+ Provides the anonymity	- Intrusion detection is not considered
2017	Ferrag and Ahmim [20]	vehicular peer-to-peer social network	Searchable encryption with vehicle proxy re-encryption	+ Provide privacy for resources, authentication and data integrity of the demand's source	- Limited analysis with threat models against botnet attacks
2018	Zidani et al. [21]	Vehicular Ad-Hoc Network	Estimation of neighbors position privacy scheme with an adaptive beaconing approach	+ Provides the location privacy	- Limited analysis against threat models
2019	Babaghayou et al. [22]	Vehicular networks	Location-privacy evaluation within the extreme points privacy	+ Provides the location privacy	- Limited analysis against threat models
2020	Aman et al. [23]	Internet of vehicles	Physical unclonable functions	+ Reduces the overhead of authentication and improves the throughput of application layer packets	- Resistance against DDoS attacks
2020	Song et al. [24]	Internet of vehicles	Fog-based identity authentication scheme	+ Reduces the burden on the traffic control center	- Resistance against Botnet attacks
2020	Sutrala et al. [25]	Internet of vehicles	Elliptic Curve Cryptography (ECC) technique	+ Secures against a passive/active adversary through various security analysis	- Communication and computation overhead
2020	Dwivedi et al. [26]	Internet of vehicles	Blockchain technology	+ Supports data immutability property	- The limited analysis against the threat models
2020	Zhang and Li [27]	Internet of vehicles	- Task allocation and data aggregation mechanism - Robin Steiner bargaining game model	+ Encourages selfish nodes to perform data transmission and reduce time delay	- Limited analysis against threat models
2020	Vasudev et al. [28]	V2V Communication in the Internet of Vehicles	Lightweight mutual authentication protocol	+ Secure communication, while minimizing computational cost	- Limited analysis against threat models
2021	Kamal et al. [28]	V2V Communication in the Internet of Vehicles	Blockchain technology and channel characteristics of wireless networks in V2V communication	+ Provides real time adversary detection within the network	- Energy and computation overhead
2021	Bagga et al. [29]	Internet of Vehicles-enabled intelligent transportation system	Mutual authentication and key agreement protocol	+ Secures against a passive/active adversary through various security analysis	- Communication and computational overhead

Scheme (CAPS) [37]. CAPS lets vehicles choose the best opportunity to enter a silence period and to change their pseudonyms.

Pan and Li (2013) proposed the Cooperative pseudonym change (CPN) [14] scheme that exploits the best opportunity to achieve a synchronous pseudonym change with the help of neighbors. This way, the adversary loses his tracking since vehicles are considered as the target and are indistinguishable. Yet, vehicles are not fully indistinguishable due to the fact that they broadcast fine-grained location. This means that an attacker is still able to identify the vehicles basing on their precise location.

Emmara et al. (2016) also apply the silent period mechanism [15] to propose the Random Silent Period (RSP) scheme [36]. RSP is based on entering silence for a random range of time, then, it performs the pseudonym change. The scheme's nature is considered as a spatial mix-zone because when vehicles enter silence period and leave it after some time this implies diapering from a point and emerging from another point which is the same idea with spatial mix-zones.

Another scheme was proposed by Zidani et al. (2018) [21] which is the Estimation of Neighbors Position privacy scheme with an Adaptive Beaconing approach (ENeP-AB) strategy that uses the number of neighbors and the predicted positions d as a pseudonym change trigger. Zidani et al. had also compared ENeP-AB to some other strategies like CAPs and the mix-context enhanced.

The effect of pseudonym change is mostly beneficial to privacy, however, Schoch et al. (2006) [38] shed light on some adverse consequences of intense pseudonym changes on the overall network performances and geo-routing protocols. Their results show that high pseudonym change frequencies affect negatively the system performances. Following a different direction, Zhang et al. (2019) [7] had touched upon the problem of collisions that occur while sending BSMs with high frequency, more precisely the problems occurring on the medium access control (MAC) layer. They demonstrated the issue and proposed a hybrid MAC Protocol and showed its effectiveness via analysis and simulation means.

Goudarzi and Asgari (2018) proposed a congestion control mechanisms algorithm called (NOPC) [39] that bases on the beacon transmission power control. The scheme performs well in the bandwidth usage and fairness, nevertheless, its influence was not evaluated versus the achieved location privacy. In the same area, SAB Mussa et al. (2014) [40] shed light on the challenging issues that have to be addressed in the beaconing and transmission range control in the vehicular domain but without mentioning the privacy requirement [24]. A summary of recent location privacy-preserving schemes for the Internet of Vehicles is presented in Table 1. In the same table the major advantages and drawbacks of all these methods are also presented.

Based on the methods that were analyzed in the previous paragraphs and the ones presented in Table 1, it is obvious that the reviewed schemes have serious limitations. The silent period schemes are the most promising solutions but at the cost of road-safety which makes them not so welcomed by the research community. Moreover, pseudonym schemes on the other hand cannot reassure privacy preservation since an adversary can still track vehicles that are broadcasting their locations even if they change pseudonym by performing the so called linking attack. The proposed idea in this research paper (WHISPER) comes to fill these limitations, by ensuring privacy along with a high road-safety level, by acting as a silent period scheme on some occasions.

3. System Model

In this section, we define and describe the Overall System Model comprised of network model, the threat/attacker model, a set of assumptions that are taken while making such a research study in addition to technical details and a mathematical model that reflects the fundamentals of using certificates under an IoV system.

3.1. Network Model

The network model used in this paper is illustrated in Fig. 3, and contains the following entities:

- Vehicles: They are the basic units of the VANET paradigm which provides a platform to the V2X applications. The communication is done via the 802.11p [3] standard and can perform Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) communications. The set of vehicles is defined as $V = \{v_1, v_2, ...v_n\}$.

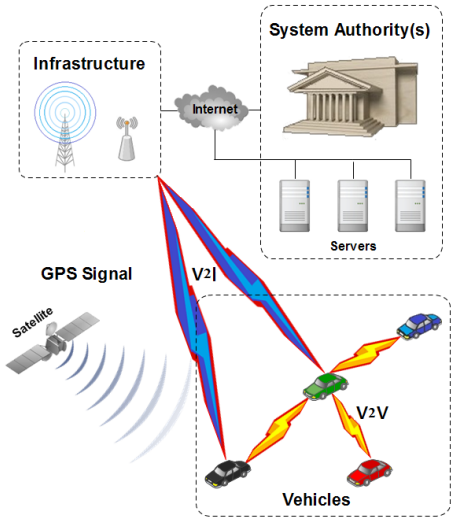

Figure 3. The different entities of the vehicular network

- System Authorities: They are the the entities related to the law-side (e.g., governmental bodies) that have different resources, tasks and roles like: distributing, issuing, revoking pseudonyms, etc. [41]. It is also important that the system authorities almost always be able to fulfill the accountability requirement in order to track down and determine the misbehaving users [42].
- Infrastructure: Composed by different components and stations, its role is to relay and facilitate the connectivity between the vehicles and any potential attached network entity. The most interesting feature is the Vehicle to Infrastructure (V2I) communications. Additionally, V2X communications may exploit the Infrastructure.

3.2. Threat Model

The threat model is shown in Fig. 4 and is composed from the following elements:

- Tracker: The malicious element in the system, even though it is not active, it still can execute many influencing attacks such as eavesdropping, tracking, profile-generation, etc. In most researches, the Global Passive Adversary (GPA) [10] is considered as the adversary type used while evaluating their own schemes. The GPA is a strong adversary that covers almost the whole map (or at least, the region of interest) and can obtain every sent message passively, i.e., no data forgery, modification or creation is executed by him.
- Eavesdropping stations: They are stations capable of collecting the transmitted BSMs where all of the coverage mode, the emplacement and the transmission range of vehicles do affect the amount of the collected packets.
- Tracker resources: They are the various materials and software used in conjunction with the eavesdropping stations. They can be high performance servers, tracking algorithms and methods, etc.

3.3. Assumptions

We put a set of assumptions for what is included in this research:

- Vehicles are able to adjust their transmission range by changing the used transmission power.
- The adversary is setting eavesdropping stations in accordance to the standardization (300m of transmission range for vehicles).
- The distributed eavesdropping stations do overlap in 30m and have a moderate coverage mode to collect much BSMs by effectively exploiting his resources. This is illustrated in Fig. 5.
- At a given time, the adversary can exclude the remaining of the map and only focuses on a region of interest. This is done at the aim of targeting only specific vehicles for better calculations and to well-exploit his resources (it is shown in Fig. 5).

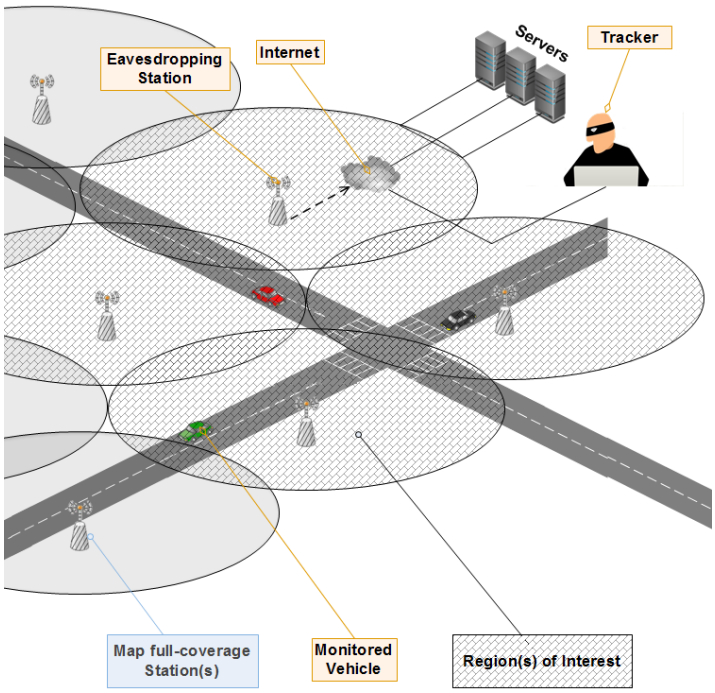

Figure 4. Threat model and its resources, capabilities and coverage

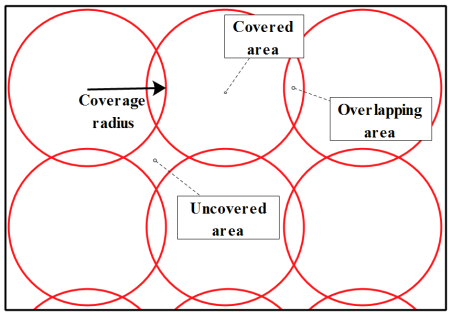

Figure 5. The used coverage mode (moderate mode) details

- Vehicles use the Public Key Infrastructure (PKI) certificates mechanism to communicate, thus, changing the used pseudonym implies using a new certificate. This later, is assumed to be issued from a trusted authority by doing the certificates refill request.

3.4. Certificates Management

Since the use of pseudonyms implies the use of certificates, a better management is envisioned in order not to affect the functioning of the whole system. With this said, having a large set of certificates with less consumption frequency would be preferred and hence minimizing their refill requests. In order to quantify the used certificates for each vehicle per unit of time, an estimation is highly needed. For that aim, we provide the following equations related to the used certificates:

- The estimated number of Certificates per day $NbrCerts_{day}$ without changing the certificate by a mean other that expiration is calculated as in Equation 1.

$$NbrCerts\_day = NbrCerts\_m * DrivTime\_day \quad (1)$$

Where $NbrCerts\_m$ is the number of used certificate per minute and $DrivTime\_day$ is the estimated amount of time (in minutes) that the user is going to drive per day.

- The number of necessary certificates per year, assuming that a normal refill is made each year, is like in Equation 2.

$$NbrCerts\_year = NbrCerts\_day * 365 \tag{2}$$

- From here, the estimated remaining certificates after d days since the last yearly refill ($NbrRemainCerts(d)$) is calculated as written in Equation 3.

$$NbrRemainCerts(d) = NbrCerts\_year - d * NbrCerts\_day \tag{3}$$

- However, certificates may also get invalid due to a certificate change (triggered by a pseudonym change for example) and thus, the exact remaining certificates after d days since the last yearly refill ($RealNbrRemainCerts(d)$) can be calculated as in Equation 4.

$$RealNbrRemainCerts(d) = NbrCerts\_year - d * NbrCerts\_day - NbrCerts\_chngd \tag{4}$$

Where $NbrCerts\_chngd$ is the number of times the certificate got changed due to a reason other than a normal expiration.

4. The Proposed WHISPER Strategy

WHISPER uses the change of transmission power to preserve or at least augment the level of location privacy in addition to ensuring road-safety while driving. Vehicles monitor the neighborhood and their proper speeds on-the-fly in order to adjust their beacons transmission range. This is because the adversary, in our assumptions, distributes his eavesdropping stations intelligently and economically according to the standardization (that vehicles transmit with $300m$ of range). Thus, when driving in low speeds the vehicle (i.e., v_i) may reduce, according to the value of its speed (and the surrounding vehicles' speeds), its own range to ensure that:

- the safety of its neighbor vehicle(s) (e.g., v_j) is preserved unlike the case of the silent period schemes that do not make much safety-considerations when going to enter silent. This is fulfilled by continuously checking its own speed. Thus, when in high speeds, the risk of a sudden crash will be high that is why v_i ought to be earlier visible to the surrounding vehicles (v_j).
- its own safety. This is fulfilled by the neighbor vehicle(s) v_j that are using the same behavior as v_i while driving in different speeds. They aim, as a consequence, to inform v_i earlier when they are driving in high speeds. Once receiving a BSM with a powerful transmission range, v_i takes that as a parameter and adjusts, in its role, its own transmission range basing on that parameter and on its own speed. By doing so, v_i will be visible to the other neighbors v_j as well.
- the two aforementioned points lead to a collective awareness that will ensure the safety of both v_i and its neighbor v_j.
- to benefit and exploit the already deployed eavesdropping mode, as these eavesdropping stations will not be able to collect BSMs all the time even if the vehicles are inside the area of the eavesdropping station. This is because each eavesdropping station was placed at the aim of intercepting every sent BSM in the range of $300m$.

4.1. System Initialization

Each vehicle v_i is equipped with M certificates and each one of them is defined as ($Cert_{i,j}$) where j represents the i^{th} certificate of v_i. Thus, each vehicle v_i has a set of certificates C_i defined as follows: $C_i = \{Cert_{i,1}, Cert_{i,2}, ...Cert_{i,m}\}$. When referring to a pseudonym change, this implies the use of another certificate.

Before we dive into the detailed modus-operandi of WHISPER, we define the set of concepts (find them in Table 2) that are key-parameters used to determine the exact behavior of WHISPER.

Generally speaking, in WHISPER, every vehicle v_i can be in one of the following main states:

- *Vehicle ON*: is the state when a vehicle is turned on (to be ready for driving).

Table 2. WHISPER keywords, concepts and detailed definitions

The concept	Its definition
The different speed levels (km/h)	Low(≥ 0 & < 18), Medium(≥ 18 & < 36), beyond-Medium(≥ 36 & < 54), High(≥ 54)
My_Pos and His_Pos (x,y,z)	The position of v_i which does the calculation and v_j which sent the BSM
My_Speed and His_Speed (km/h)	The speed of v_i which does the calculation and v_j which sent the BSM
$Speed$ (km/h)	The highest speed that was encountered while v_i was waiting
$Dist$ (m)	The distance between the sending vehicle v_j and the receiving vehicle v_i
$Calc\_Dist(A,B)$ (m)	Calculates the distance between point A and B.
$BSM.X()$ $(depends)$	$X()$ is the method applied on *BSM* to retrieve different fields like position, speed, etc.
$GeneralNR$ (m)	A virtual range with the same value for each receiving vehicle v_i. This range determines whether a sending vehicle v_j is considered as a "General Neighbor" to v_i or not. If v_j is inside that range when sending its BSM, then it is considered to be v_i's General Neighbor.
$RoadNR$ (m)	A virtual range with the same value for each receiving vehicle v_i. This range determines whether a sending vehicle v_j is considered as a "Road Neighbor" to v_i or not. v_j is only considered as a Road Neighbor to v_i if it is inside the *RoadNR* range and if it and v_i share the same road segment.
$CloseNR$ (m)	A virtual range with the same value for each receiving vehicle v_i. This range determines whether a sending vehicle v_j is considered as a "Close Neighbor" to v_i or not. v_j is only considered as a Close Neighbor if it is inside the *CloseNR* range. Noting that *CloseNR* range ought to be very small in order to let both v_i and v_j be as much indistinguishable as possible to confuse the attacker when doing the pseudonym change action
$Close$ $(boolean)$	A local variable that each vehicle v_i has. Being *True* means that v_i is currently at the proximity of another vehicle v_j. In the other case, when v_i is alone (with regard to the *CloseNR* range), its value becomes *False* (to achieve road-safety, entertainment, congestion-aware actions, etc.)
$Proccess\_Beacon(BSM)$ $(procedure)$	This procedure uses the received BSM packet for the IoV objectives and requirements (to achieve road-safety, entertainment, congestion-aware actions, etc.)
OBU_Is_On $(boolean)$	A true or false value which means a sending vehicle v_i is on or off respectively
$Beacon\_Interval\_Time$ (s)	An amount of time in where v_i is waiting before sending the next BSM
$Prepare\_Beacon(BSM)$ $(Beacon)$	Generates a BSM packet that will be ready for broadcasting
$nic.mac80211p.txPower$ $(milliwatt)$	The transmission power given to the network interface used to control the transmission range of v_i
$Counter$ $(number)$	A counter variable used later on to decide the pseudonym change action
Def_Val $(number)$	The default value of $counter$. It is used to both reinitialize $counter$ and to do a test to find out the eligibility of v_i for changing its pseudonym
$Send\_Beacon(BSM)$ $(Beacon)$	Gives the BSM packet to the lower layers which will broadcast it to the neighbors
$Checking\_Pseudonym\_Change\_Trigger()$ $(procedure)$	Checking whether the trigger of v_i for changing its pseudonym is met or not
$Pseudonym\_Change()$ $(procedure)$	Once the conditions are met and once it is executed correctly, v_i acquires a new pseudonym (and certificate respectively)

- *Listening*: once On, v_i keeps monitoring the transmission medium to detect any transmitted BSM. both its neighbor(s) status (found in their transmitted BSMs) and its own speed.
- *Receiving BSMs*: When receiving a BSM from v_j, v_i proceeds into diverse calculations at the aim of knowing the status of v_j.
- *Adjusting the transmission power*: in this status, v_i takes as parameters its own speed and the neighbors' speed and may, accordingly, adjust its transmission range in order to ensure road-safety and preserve location-privacy of the present vehicles.

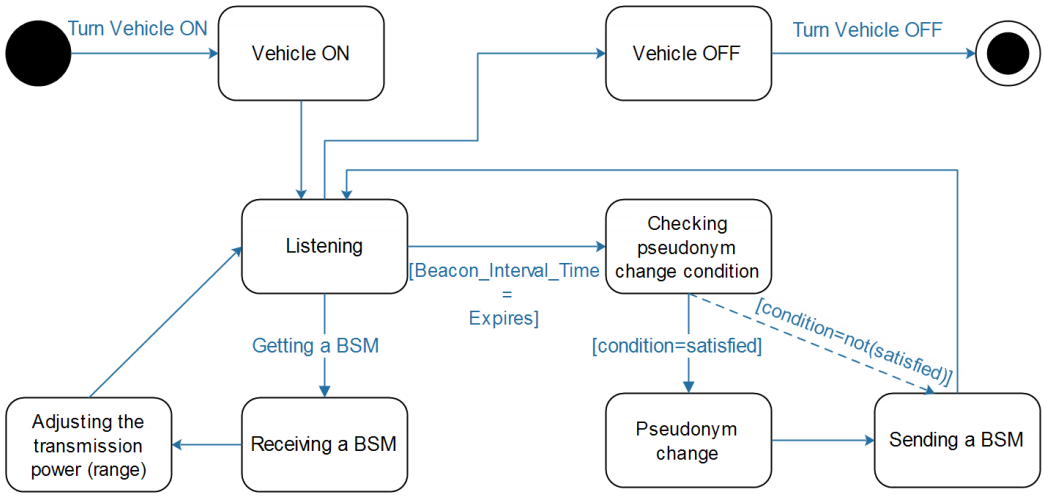

Figure 6. The state diagram of WHISPER

- *Checking pseudonym change condition*: this status comes after the *Beacon_Interval_Time* expires. v_i will check its eligibility for a pseudonym (and certificate) change. When favorable, v_i moves into the next status.
- *Pseudonym change* in this status, a pseudonym change takes place and the BSM will be sent right after.
- *Sending a BSM* this status happen after the *Pseudonym change* action. Sometimes, the pseudonym change trigger will not be satisfied, thus, v_i just sends the BSM. In both scenarios, v_i returns to the next status(*Listening*) afterwards.
- *Vehicle OFF* the status where a vehicle is turned off and thus the ending status.

A state diagram is presented in Fig. 6 which gives a better illustration and understanding on the aforementioned states and the existing transitions.

4.2. Receiving Beacon Messages Protocol

Vehicles are always ready to receive BSMs. When receiving a BSM, the receiving vehicle v_i considers the sender's position and calculates the distance between itself and the sender. By doing this simple calculation, v_i will be able to get a set of useful information that will determine its behavior. The pseudo-code of receiving a beacon message in WHISPER is illustrated in Algorithm. 1. The main conclusions that v_i is going to have after parsing the BSM sent by v_j, are the followings:

- Knowing the distance between itself and v_j.
- Whether to consider v_j's BSM for transmission power adjustment or just ignore it.
- It considers v_j's BSM for transmission power adjustment if *Dist* is less than or equal to *GeneralNR* (shown in the scenario that is illustrated in 7).
- It considers v_j's BSM for transmission power adjustment if *Dist* is less than or equal to *RoadNR* but also share the same road segment with each other (shown in the scenario that is illustrated in 8).
- It considers itself eligible for the pseudonym change if *Dist* is less than or equal to *CloseNR*. It does change *Close* to *True* as a consequence.

This protocol is called whenever v_i receives a BSM generated by v_j and with each call, less than 10 instructions are executed; thus a linear complexity per each call $\mathcal{O}(10)$. With this said, by receiving (R) BSM, the complexity of the whole protocol will be as in Equation 5:

$$\mathcal{O}(R \times 10) = \mathcal{O}(n) \tag{5}$$

This indicates that the *ReceivingBeaconMessages* Protocol is neither time nor resources consumer.

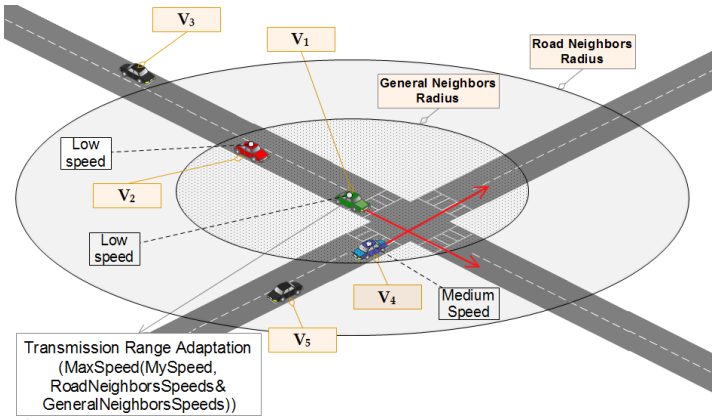

Figure 7. WHISPER behavior in the presence and influence of general neighbors on the transmission range adjustment

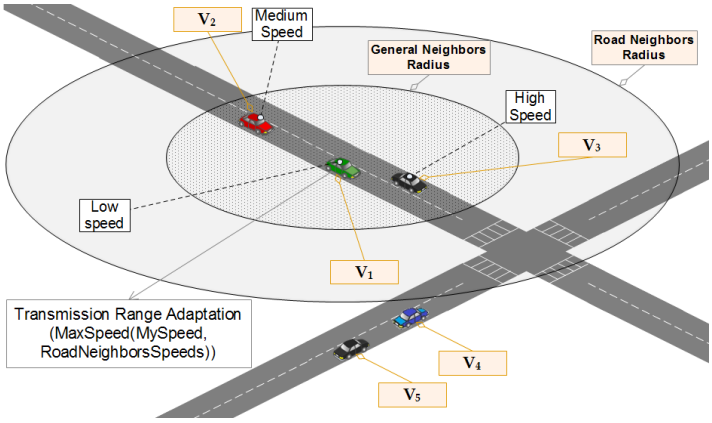

Figure 8. WHISPER behavior in the presence and influence of road neighbors on the transmission range adjustment

4.3. Transmission Range Adjustment Protocol

Each vehicle v_i, and after the *Beacon_Interval_Time* expires, will send a BSM to inform the nearby vehicles about its location. Particularly, WHISPER adjusts the transmission range prior to the final BSM broadcast. The adjustment is done each time a BSM is received by v_i as explained before. When going to broadcast, v_i uses the value of *Speed* to decide the appropriate transmission range (between all of the four levels: Low, Medium, beyond-Medium and High). Algorithm. 2 shows the pseudo-code of sending a BSM after making the transmission range adjustment step. Additionally, *Speed* is reinitialized to 0 after that and $Checking\_Pseudonym\_Change\_Trigger()$ is called during this protocol and that is to see the eligibility of changing v_i's pseudonym (and certificate respectively). Moreover, *Counter* is decreased depending on the value of *Speed* and this is to trigger the pseudonym change (will be seen in the next point). However, if *Speed* is at max level, there will be no meaning for changing the pseudonym and that is because the attacker is able to collect every sent beacon (the maximum transmission range is used) and that is why *Counter* is reinitialized to its default value Def_Val.

This protocol is called whenever v_i *Beacon_Interval_Time* expires and thuse, one time per call. However, it calls, in its role, the $Checking\_Pseudonym\_Change\_Trigger()$ protocol. In total, there are (7) instructions without counting the called protocol ($\mathcal{O}(7)$). With this said, the complexity o the *TransmissionRangeAdjustment* Protocol is defined as in Equation 6:

$$\mathcal{O}(1 \times (7 + \mathcal{O}(Checking\_Pseudonym\_Change\_Trigger()))) = \mathcal{O}(Checking\_Pseudonym\_Change\_Trigger()) \quad (6)$$

Algorithm 1 Receiving Beacon

```
1:  procedure RECEIVING_BEACON(BEACON* BSM)
2:      His_Pos ← BSM.SenderPos();
3:      Dist ← Calc_Dist(My_Pos,His_pos);
4:      if ((Dist <= GeneralNR) OR ((Dist <= RoadNR) AND (MyRoadID = HisRoadID)) then
5:          His_Speed ← BSM.SenderSpeed();
6:          Speed ← Max(My_Speed,His_Speed);
7:          if (Dist <= CloseNR) then
8:              Close ← TRUE;
9:          end if
10:     end if
11:     Process_Beacon(BSM);
12: end procedure
```

This indicates that the *TransmissionRangeAdjustment* protocol does depend on the *PseudonymChangeTrigger* Protocol.

Algorithm 2 Sending Beacon

```
1:  procedure SENDING_BEACON
2:      while (OBU_Is_On) do
3:          Wait(Beacon_Interval_Time);
4:          Prepare_Beacon(BSM);
5:          Speed ← Max(My_Speed,Speed);
6:          if (Speed < 18) then
7:              nic.mac80211p.txPower ← 0.2;
8:              Counter ← Counter − 5;
9:          else if (Speed < 36) then
10:             nic.mac80211p.txPower ← 0.8;
11:             Counter ← Counter − 10;
12:         else if (Speed < 54) then
13:             nic.mac80211p.txPower ← 3.1;
14:         else
15:             nic.mac80211p.txPower ← 7;
16:             Counter ← Def_Val;
17:         end if
18:         Speed ← 0;
19:         Checking_Pseudonym_Change_Trigger();
20:         Send_Beacon(BSM);
21:     end while
22: end procedure
```

4.4. Pseudonym Change Trigger Protocol

In order to avoid wasting pseudonyms (certificates) in an inappropriate opportunity, finding an almost good opportunity requires that the pseudonym change trigger must be implemented delicately. Algorithm. 3 shows, in a pseudo-code, the way vehicles perform a check to see the eligibility for changing their pseudonyms. When the trigger *Counter* reaches or drops below (0) (which is an indicator that v_i was sending BSMs with a short range for some important period of time) v_i changes its pseudonym then initializes the trigger *Counter*. This whole process provides high confusion chances since the pseudonym change is performed not in the favor of the tracker (see the scenario illustrated in Fig. 9). The *PseudonymChangeTrigger* protocol is used each time the *TransmissionRangeAdjustment* is executed. Its complexity depends on a small and fixed number of instructions (5), thus, can be defined as in Equation 7:

$$\mathcal{O}(5) = \mathcal{O}(1) \tag{7}$$

The *PseudonymChangeTrigger* protocol has $\mathcal{O}(1)$ as a complexity.

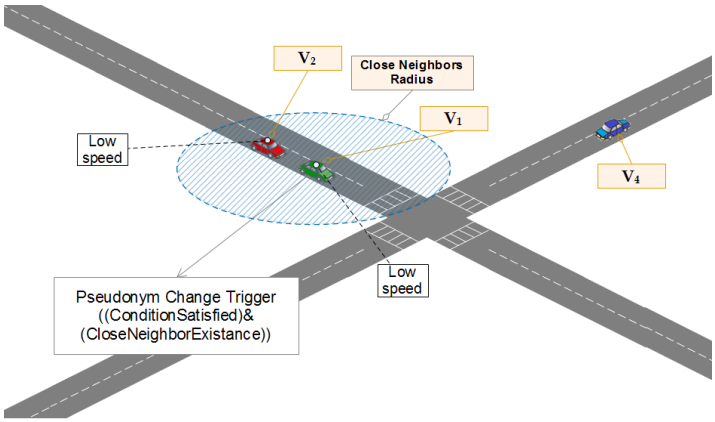

Figure 9. WHISPER, pseudonym change process triggered by a close neighbor's status

Algorithm 3 Checking Pseudonym Change Trigger

```
1:  procedure CHECKING_PSEUDONYM_CHANGE_TRIGGER
2:      if ((Counter <= (Def_Val/2)) AND (Close)) then
3:          Counter ← Def_Val;
4:          Pseudonym_Change();
5:      else if (Counter <= 0) then
6:          Counter ← Def_Val;
7:          Pseudonym_Change();
8:      end if
9:      Close ← FALSE;
10: end procedure
```

5. Performance Evaluation

To validate the performances of WHISPER, we use simulation runs in a manhattan grid model created using NETEDIT script included in SUMO; the mobility simulator [43]. SUMO is considered as one of the most credible and realistic mobility simulators. The mobility and environment information used for the simulation are presented in Table. 3. The manhattan grid model consists of 9 intersected roads with attached segments where each segment has a length of $200m$.

In what concerns the network simulator, we use OMNeT++ [44]; the component c++ based and discrete events simulator. OMNet++ allows the integration of diverse frameworks depending on the simulation nature like Veins [45]; the vehicular network simulator. Veins acts as a bridge between the mobility simulator SUMO and the network simulator OMNet++. We also employ the PREXT extension [36] that is developed by Emmara et al.; a Veins extension that integrates a set of (1) location privacy schemes, (2) some privacy metrics such as the traceability and the normalized traceability (described in [46]) and (3) a Quality of Service (QoS) metric (the consumption of pseudonyms/certificates). A block diagram is elaborated in order to facilitate the comprehension of the interaction between the different simulation tools (shown in Fig. 10). Basing on PREXT, WHISPER is evaluated and compared against some other schemes under the same environmental condition using the aforementioned metrics. The schemes' parameters and the evaluation metrics are also presented in Table. 3.

5.1. The Adversary's Achieved Traceability

Traceability, that is the location privacy metric used in this study, is defined as the correctness of an adversary to build the target vehicle's traces using its eavesdropped beacons [46]. The results, provided in Fig. 11 show that WHISPER is outperforming SLOW, RSP and CPN in the traceability metric with a clear difference (that is ranging in the interval of 10% to 20%). An important remark is that at dense situations (e.g., with the density of 200 vehicle), the traceability gets augmented a bit. The reason behind the decrease in the privacy level is due to the higher density of vehicles, that can help the attacked collect BSMs from the legitimate cars.

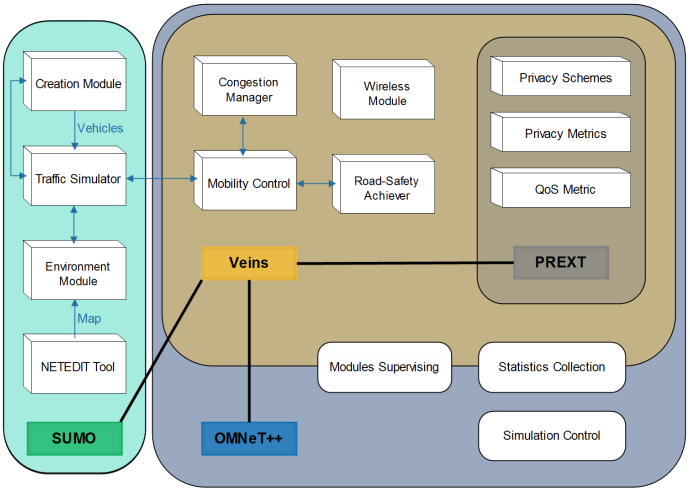

Figure 10. The block diagram of the different used simulation tools

Table 3. Simulation parameters and values

	Parameters	Value
Mobility	Vehicles Number	Simultaneously=50,100,150,200 Total=100,200,300,400
	Insertion method	Quasi-Instant (first second insertion)
	Mobility Model	RandomTrips with minimum distance=1500(m)
Environment	Used Map	Manhattan grid model 9 roads, 200(m) per segment
	Map size	2000*2000($m*m$) 4(km^2)
	Simulation Time	300(s)
Evaluation	Privacy metrics	Traceability N_Traceability
	Pseudonym usage/ consumption	Number of changed-pseudonyms
Strategy	SLOW	Speed threshold=8(m/s) Silence threshold=5(s)
	RSP	Pseudonym duration=60(s) Silence period= from 3 to 9(s) randomly
	CPN	Neighbors radius=100(m) Neighbors threshold=2
	WHISPER	Road neighbors radius=100(m) General neighbors radius=30(m) Close neighbors radius=30(m) Counter default value=50

In general, as presented in Fig. 11, WHISPER performs better in terms the level of privacy that it offered since it achieves a traceability ranging in the interval of 10% to 20%. We interpret this as being WHISPER reducing the vehicle's transmission range according to its and/or the neighbor vehicles' speeds (according to the

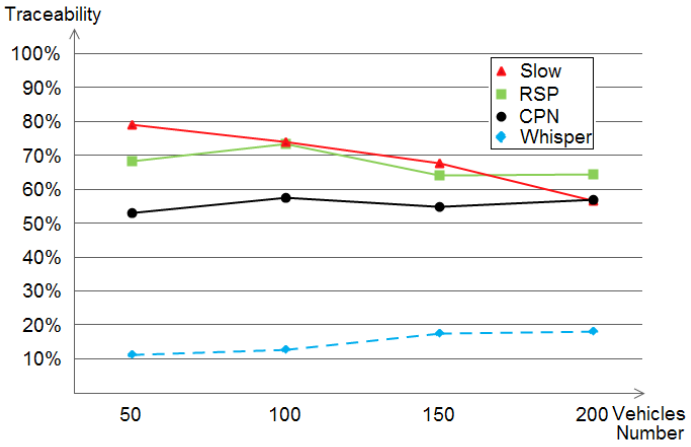

Figure 11. The achieved traceability by SLOW, RSP, CPN and WHISPER within different densities

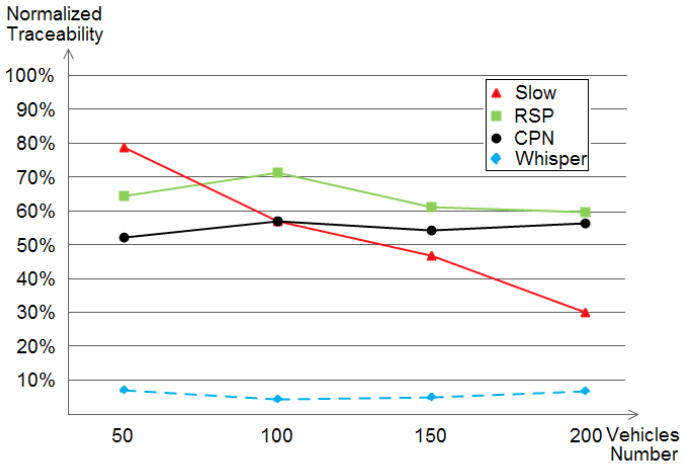

Figure 12. The achieved normalized traceability by SLOW, RSP, CPN and WHISPER within different densities

safety situation) followed by CPN, RSP then SLOW, in addition we observe that the traceability decreases when augmenting the number of vehicles in SLOW. The reason is that, in high densities, vehicles would drive with lower speeds, thus, SLOW performs better.

5.2. The Adversary's Achieved Normalized Traceability

As some vehicles may not perform the pseudonym change, building their traces becomes easy, thus, excluding them gives more fairness to the real level of privacy [46]; that is the normalized traceability. With this definition, our conducted simulation under the normalized traceability is aiming to give a more credible and better privacy-reflecting metric to quantify the achieved privacy level of WHISPER, SLOW, RSP, and CPN (shown in Fig. 12).

As stated above, by taking the case of just the vehicles which did change their pseudonyms, we get the achieved normalized traceability as shown in Fig. 12. The results always give WHISPER the leading position since it outperforms the other schemes but this time by achieving an even higher privacy level represented in a lower than 10% of normalized traceability. The same order of performance remains; CPN, RSP then SLOW. However, SLOW has achieved better-normalized traceability of about 30% due to removing vehicles that did not change their pseudonyms at all from the calculation.

Table 4. A brief comparison of SLOW, RSP, CPN and WHISPER strategies according to a set of metrics

	Staying Silent	Monitoring Neighbors	Pseudonyms Consumption	Safety Ensuring	More Efficiency When
SLOW [16]	✓	✗	Low	✗	Driving in low speeds, hence, keeping silence
RSP [15]	✓	✗	Low	✗	Entering silence and changing pseudonyms synchronously
CPN [14]	✗	✓	Very high	✓	The set of vehicles happens to be large
WHISPER	✗	✓	Medium	✓	Low transmission power condition is satisfied

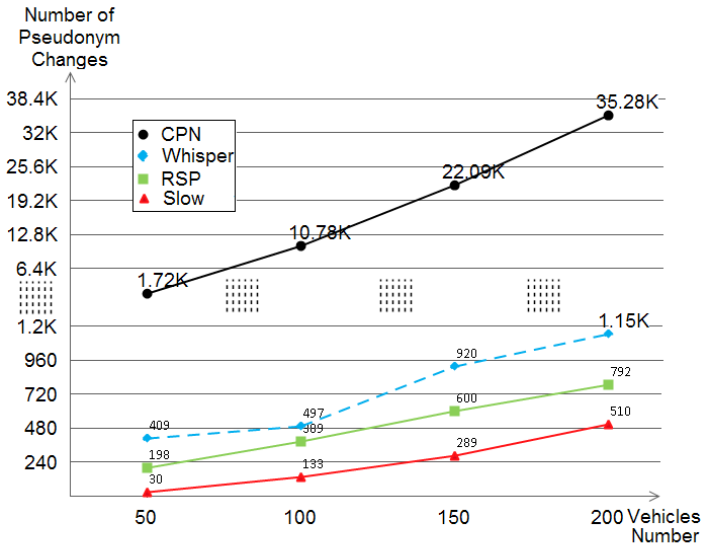

Figure 13. The pseudonyms changes (consumption) evaluation of CPN, WHISPER, RSP and SLOW within different densities

5.3. Pseudonym Consumption

Also considered as the QoS metric. The pseudonym consumption has multiple effects and impacts like the use of different pseudonyms (thus, certificates), extra-communications with the corresponding authorities to refill pseudonyms, affecting the routing algorithms [38], etc. For this reason, the pseudonym consumption metric is crucial. With a clear view, Fig. 13 shows that SLOW is the less pseudonyms consuming scheme followed by RSP and WHISPER respectively, while CPN had a considerable high pseudonyms consumption level. We argue this by the scheme's nature, when the trigger of k neighbors is satisfied, a pseudonym change is performed and as k was taken as 2 by the default parameters, a lot of pseudonym changes occurred.

6. Discussion

For an overall investigation, the performances of CPN, RSP, SLOW, and WHISPER were evaluated in terms of (1) location privacy that gives WHISPER the leading in both (a) the traceability and (b) the normalized traceability and (2) QoS that comes in the favor of SLOW. CPN, under the default parameters (i.e., $k = 2$), has resulted in a very high pseudonyms consumption, thus, considered as a non-wise choice for a deployed pseudonym scheme. The results, clearly show that WHISPER has a very good level of privacy since it achieves traceability ranging in the interval of 10% to 20%. In terms of normalized traceability, WHISPER outperformed the other schemes achieving an even higher privacy level.

Despite being WHISPER more pseudonym consuming (with a remarkably low amount in general) than SLOW and RSP, having it a very high location privacy level represented in the traceability and the normalized

traceability gives it the leading position. Thus, we can say that WHISPER, as also compared and summarized in Table. 4, has outperformed the other schemes especially in both the safety and the location privacy that are known to be on the top of the security requirements.

Except for the evaluation comparison, WHISPER is an important solution that offers privacy preservation while maintaining at the same time road-safety. This is achieved since vehicles are only hidden from the tracker (occasionally) and not from52their close vehicles (always) which makes the use of WHISPER an advantageous method that comes in favor of safety and privacy.

7. Conclusion and Future Work

In this paper, WHISPER, a novel location privacy-preserving scheme that is based on reducing the transmission range while sending the safety beacons was proposed. We presented WHISPER protocols, techniques, and algorithms and compared them against other methods, namely CPN, RSP, and SLOW in terms of location privacy level (traceability), normalized traceability) and QoS (pseudonyms consumption) metrics. WHISPER has clearly outperformed the other schemes in the location privacy evaluation, which is an important security requirement, but consumed -lightly- more pseudonyms than SLOW and RSP as the QoS evaluation demonstrated. Furthermore, WHISPER showed its robustness during the evaluation and also provided (1) road-safety that is missed by all other silent period schemes in conjunction with (2) location-privacy.

The reason why WHISPER was a road-safety mechanism is that the vehicle is only hidden from the tracker (occasionally) and not from the close vehicles (always) which made the use of WHISPER (or at least, the change of transmission range protocol) an advantageous feature that came in the favor of safety and privacy alike.

As this new technique was not exploited before in the privacy field, we intend on evaluating the achieved location privacy level versus an internal attacker; i.e., when vehicles act as malicious eavesdropping stations in order to bypass the reduction of transmission range and increase the coverage of the attacker. Also, some of the values (e.g., existing in Algorithm. 2) are set heuristically, evaluating the performance by optimally adjusting those values dynamically would certainly enhance the obtained privacy level of WHISPER. Moreover technologies like blockchain[47], cryptography [48], IDSs[49] and Edge Computing[50] that are widely recognized as key enablers for the IoV could be integrated or used in parallel with our solution. Finally, using other metrics like the number of sent BSMs, the number of verified signatures, and evaluating WHISPER's performance under different scenarios like the free-way model are some of our future plans.

Author Contributions: Conceptualization, M.B., N.L., and L.M.; Methodology, M.B., A.A., and L.M.; Software, M.B., H.J, M.A.F., and N.L.; Validation, M.A.F., N.L., and L.M.; formal analysis, A.A. M.A.F. and N.L.; investigation, M.B., N.L., A.A, and M.A.F.; resources, M.A.F, N.L., and M.B.; data curation, M.B., H.J., N.L., and L.M.; writing—original draft preparation, M.B., N.L., and M.A.F; writing—review and editing, A.A., H.J., and L.M.; visualization, M.A.F., M.B., N.L., and L.M.; supervision, N.L., A.A., M.A.F.

Funding: This research received no external funding.

Conflicts of Interest: All authors declare no conflict of interest.

References

1. Karagiannis, G.; Altintas, O.; Ekici, E.; Heijenk, G.; Jarupan, B.; Lin, K.; Weil, T. Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions. *IEEE communications surveys & tutorials* **2011**, *13*, 584–616.
2. Al-Sultan, S.; Al-Doori, M.M.; Al-Bayatti, A.H.; Zedan, H. A comprehensive survey on vehicular ad hoc network. *Journal of network and computer applications* **2014**, *37*, 380–392.
3. Wang, J.; Shao, Y.; Ge, Y.; Yu, R. A survey of vehicle to everything (v2x) testing. *Sensors* **2019**, *19*, 334.
4. Yang, F.; Wang, S.; Li, J.; Liu, Z.; Sun, Q. An overview of internet of vehicles. *China communications* **2014**, *11*, 1–15.
5. Lin, K.; Li, C.; Li, Y.; Savaglio, C.; Fortino, G. Distributed learning for vehicle routing decision in software defined Internet of vehicles. *IEEE Transactions on Intelligent Transportation Systems* **2020**.

6. Fortino, G.; Savaglio, C.; Spezzano, G.; Zhou, M. Internet of Things as System of Systems: A Review of Methodologies, Frameworks, Platforms, and Tools. *IEEE Transactions on Systems, Man, and Cybernetics: Systems* **2020**.
7. Zhang, M.; Ali, G.M.N.; Chong, P.H.J.; Seet, B.C.; Kumar, A. A novel hybrid mac protocol for basic safety message broadcasting in vehicular networks. *IEEE Transactions on Intelligent Transportation Systems* **2019**, *21*, 4269–4282.
8. Lu, R.; Lin, X.; Zhu, H.; Ho, P.H.; Shen, X. ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications. IEEE INFOCOM 2008-The 27th Conference on Computer Communications. IEEE, 2008, pp. 1229–1237.
9. Babaghayou, M.; Labraoui, N.; Ari, A.A.A.; Gueroui, A.M. Transmission Range Changing Effects on Location Privacy-Preserving Schemes in the Internet of Vehicles. *International Journal of Strategic Information Technology and Applications (IJSITA)* **2019**, *10*, 33–54.
10. Ferrag, M.A.; Maglaras, L.; Ahmim, A. Privacy-preserving schemes for ad hoc social networks: A survey. *IEEE Communications Surveys & Tutorials* **2017**, *19*, 3015–3045.
11. Babaghayou, M.; Labraoui, N.; Ari, A.A.A.; Lagraa, N.; Ferrag, M.A. Pseudonym change-based privacy-preserving schemes in vehicular ad-hoc networks: A survey. *Journal of Information Security and Applications* **2020**, *55*, 102618.
12. Maglaras, L.A.; Al-Bayatti, A.H.; He, Y.; Wagner, I.; Janicke, H. Social internet of vehicles for smart cities. *Journal of Sensor and Actuator Networks* **2016**, *5*, 3.
13. Eckhoff, D.; Sommer, C. Readjusting the privacy goals in Vehicular Ad-Hoc Networks: A safety-preserving solution using non-overlapping time-slotted pseudonym pools. *Computer Communications* **2018**, *122*, 118–128.
14. Pan, Y.; Li, J. Cooperative pseudonym change scheme based on the number of neighbors in VANETs. *Journal of Network and Computer Applications* **2013**, *36*, 1599–1609.
15. Huang, L.; Matsuura, K.; Yamane, H.; Sezaki, K. Enhancing wireless location privacy using silent period. Wireless Communications and Networking Conference, 2005 IEEE. IEEE, 2005, Vol. 2, pp. 1187–1192.
16. Buttyán, L.; Holczer, T.; Weimerskirch, A.; Whyte, W. Slow: A practical pseudonym changing scheme for location privacy in vanets. Vehicular Networking Conference (VNC), 2009 IEEE. IEEE, 2009, pp. 1–8.
17. Freudiger, J.; Raya, M.; Félegyházi, M.; Papadimitratos, P.; Hubaux, J.P. Mix-zones for location privacy in vehicular networks. ACM Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS), 2007, number LCA-CONF-2007-016.
18. Eckhoff, D.; German, R.; Sommer, C.; Dressler, F.; Gansen, T. Slotswap: Strong and affordable location privacy in intelligent transportation systems. *IEEE Communications Magazine* **2011**, *49*, 126–133.
19. Lu, R.; Lin, X.; Luan, T.H.; Liang, X.; Shen, X. Pseudonym changing at social spots: An effective strategy for location privacy in vanets. *IEEE transactions on vehicular technology* **2012**, *61*, 86–96.
20. Ferrag, M.A.; Ahmim, A. ESSPR: an efficient secure routing scheme based on searchable encryption with vehicle proxy re-encryption for vehicular peer-to-peer social network. *Telecommunication Systems* **2017**, *66*, 481–503.
21. Zidani, F.; Semchedine, F.; Ayaida, M. Estimation of Neighbors Position privacy scheme with an Adaptive Beaconing approach for location privacy in VANETs. *Computers & Electrical Engineering* **2018**, *71*, 359–371.
22. Babaghayou, M.; Labraoui, N.; Ari, A.A.A. Location-Privacy Evaluation Within the Extreme Points Privacy (EPP) Scheme for VANET Users. *International Journal of Strategic Information Technology and Applications (IJSITA)* **2019**, *10*, 44–58.
23. Aman, M.N.; Javaid, U.; Sikdar, B. A privacy-preserving and scalable authentication protocol for the internet of vehicles. *IEEE Internet of Things Journal* **2020**, *8*, 1123–1139.
24. Song, L.; Sun, G.; Yu, H.; Du, X.; Guizani, M. Fbia: A fog-based identity authentication scheme for privacy preservation in internet of vehicles. *IEEE Transactions on Vehicular Technology* **2020**, *69*, 5403–5415.
25. Sutrala, A.K.; Bagga, P.; Das, A.K.; Kumar, N.; Rodrigues, J.J.; Lorenz, P. On the design of conditional privacy preserving batch verification-based authentication scheme for Internet of vehicles deployment. *IEEE Transactions on Vehicular Technology* **2020**, *69*, 5535–5548.
26. Dwivedi, S.K.; Amin, R.; Vollala, S.; Chaudhry, R. Blockchain-based secured event-information sharing protocol in internet of vehicles for smart cities. *Computers & Electrical Engineering* **2020**, *86*, 106719.
27. Zhang, W.; Li, G. An Efficient and Secure Data Transmission Mechanism for Internet of Vehicles Considering Privacy Protection in Fog Computing Environment. *IEEE Access* **2020**, *8*, 64461–64474.
28. Vasudev, H.; Deshpande, V.; Das, D.; Das, S.K. A Lightweight Mutual Authentication Protocol for V2V Communication in Internet of Vehicles. *IEEE Transactions on Vehicular Technology* **2020**, *69*, 6709–6717.

29. Bagga, P.; Das, A.K.; Wazid, M.; Rodrigues, J.; Choo, K.K.R.; Park, Y. On the Design of Mutual Authentication and Key Agreement Protocol in Internet of Vehicles-Enabled Intelligent Transportation System. *IEEE Transactions on Vehicular Technology* **2021**.
30. Huang, R.; Ying, B.; Nayak, A. Protecting location privacy in opportunistic mobile social networks. NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium. IEEE, 2018, pp. 1–8.
31. Beresford, A.R.; Stajano, F. Location privacy in pervasive computing. *IEEE Pervasive computing* **2003**, pp. 46–55.
32. Petit, J.; Schaub, F.; Feiri, M.; Kargl, F. Pseudonym schemes in vehicular networks: A survey. *IEEE communications surveys & tutorials* **2015**, *17*, 228–255.
33. ETSI, TR. Intelligent Transport Systems (ITS); Security; Pre-standardization study on pseudonym change management, 2018.
34. ETSI, TS. Intelligent Transport Systems (ITS); Security; Security management messages communication requirements and distribution protocols, 2020.
35. Tomandl, A.; Scheuer, F.; Federrath, H. Simulation-based evaluation of techniques for privacy protection in VANETs. 2012 IEEE 8th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob). IEEE, 2012, pp. 165–172.
36. Emara, K. Poster: PREXT: privacy extension for veins VANET simulator. 2016 IEEE Vehicular Networking Conference (VNC). IEEE, 2016, pp. 1–2.
37. Emara, K.; Woerndl, W.; Schlichter, J. CAPS: Context-aware privacy scheme for VANET safety applications. Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks. ACM, 2015, p. 21.
38. Schoch, E.; Kargl, F.; Leinmüller, T.; Schlott, S.; Papadimitratos, P. Impact of pseudonym changes on geographic routing in vanets. European Workshop on Security in Ad-hoc and Sensor Networks. Springer, 2006, pp. 43–57.
39. Goudarzi, F.; Asgari, H. Non-Cooperative Beacon Power Control for VANETs. *IEEE Transactions on Intelligent Transportation Systems* **2018**, pp. 1–6.
40. Mussa, S.A.B.; Manaf, M.; Ghafoor, K.Z. Beaconing and transmission range adaptation approaches in vehicular ad hoc networks: Trends & research challenges. 2014 International Conference on Computational Science and Technology (ICCST). IEEE, 2014, pp. 1–6.
41. Nowatkowski, M.E.; Wolfgang, J.E.; McManus, C.; Owen, H.L. The effects of limited lifetime pseudonyms on certificate revocation list size in VANETS. Proceedings of the IEEE SoutheastCon 2010 (SoutheastCon). IEEE, 2010, pp. 380–383.
42. Bouchelaghem, S.; Omar, M. Secure and efficient pseudonymization for privacy-preserving vehicular communications in smart cities. *Computers & Electrical Engineering* **2020**, *82*, 106557.
43. Krajzewicz, D.; Erdmann, J.; Behrisch, M.; Bieker, L. Recent Development and Applications of SUMO - Simulation of Urban MObility. *International Journal On Advances in Systems and Measurements* **2012**, *5*, 128–138.
44. Varga, A.; Hornig, R. An overview of the OMNeT++ simulation environment. Proceedings of the 1st international conference on Simulation tools and techniques for communications, networks and systems & workshops. ICST, 2008, p. 60.
45. Sommer, C.; German, R.; Dressler, F. Bidirectionally coupled network and road traffic simulation for improved IVC analysis. *IEEE Transactions on mobile computing* **2011**, *10*, 3–15.
46. Emara, K.; Woerndl, W.; Schlichter, J. Context-based pseudonym changing scheme for vehicular adhoc networks. *arXiv preprint arXiv:1607.07656* **2016**.
47. Merzougui, S.E.; Ferrag, M.A.; Friha, O.; Maglaras, L. EASBF: An Efficient Authentication Scheme over Blockchain for Fog Computing-enabled Internet of Vehicles. *Journal of Information Security and Applications* **2021**.
48. Tselikis, C.; Douligeris, C.; Maglaras, L.; Mitropoulos, S. On the conference key distribution system with user anonymity. *Journal of Information Security and Applications* **2020**, *54*, 102556.
49. Kosmanos, D.; Argyriou, A.; Maglaras, L. Estimating the relative speed of RF jammers in VANETs. *Security and Communication Networks* **2019**, *2019*.
50. Xu, X.; Xue, Y.; Qi, L.; Yuan, Y.; Zhang, X.; Umer, T.; Wan, S. An edge computing-enabled computation offloading method with privacy preservation for internet of connected vehicles. *Future Generation Computer Systems* **2019**, *96*, 89–100.