sustainability

MDPI

Article

A Distributed Mix-Context-Based Method for Location Privacy in Road Networks

Ikram Ullah [1], Munam Ali Shah [1], Abid Khan [2], Carsten Maple [3], Abdul Waheed [1] and Gwnaggil Jeon [4,*]

[1] Department of Computer Science, COMSATS University Islamabad, Islamabad 45550, Pakistan; ikram.comsats.cs@gmail.com (I.U.); mshah@comsats.edu.pk (M.A.S.); gallian92@gmail.com (A.W.)
[2] Department of Computer Science, School of Computing, Engineering and Digital Technologies, Teesside University, Middlesbrough TS1 3BX, UK; abk15@aber.ac.uk or its.abidkhan@gmail.com
[3] Secure Cyber Systems Research Group, WMG, University of Warwick, Coventry CV4 7AL, UK; cm@warwick.ac.uk
[4] Department of Embedded Systems Engineering, Incheon National University, 119 Academy-ro, Yeonsugu, Incheon 22012, Korea
* Correspondence: gjeon@inu.ac.kr

Abstract: Preserving location privacy is increasingly an essential concern in Vehicular Adhoc Networks (VANETs). Vehicles broadcast beacon messages in an open form that contains information including vehicle identity, speed, location, and other headings. An adversary may track the various locations visited by a vehicle using sensitive information transmitted in beacons such as vehicle identity and location. By matching the vehicle identity used in beacon messages at various locations, an adversary learns the location history of a vehicle. This compromises the privacy of the vehicle driver. In existing research work, pseudonyms are used in place of the actual vehicle identity in the beacons. Pseudonyms should be changed regularly to safeguard the location privacy of vehicles. However, applying simple change in pseudonyms does not always provide location privacy. Existing schemes based on mix zones operate efficiently in higher traffic environments but fail to provide privacy in lower vehicle traffic densities. In this paper, we take the problem of location privacy in diverse vehicle traffic densities. We propose a new Crowd-based Mix Context (CMC) privacy scheme that provides location privacy as well as identity protection in various vehicle traffic densities. The pseudonym changing process utilizes context information of road such as speed, direction and the number of neighbors in transmission range for the anonymisation of vehicles, adaptively updating pseudonyms based on the number of a vehicle neighbors in the vicinity. We conduct formal modeling and specification of the proposed scheme using High-Level Petri Nets (HPLN). Simulation results validate the effectiveness of CMC in terms of location anonymisation, the probability of vehicle traceability, computation time (cost) and effect on vehicular applications.

Keywords: anonymity; formal modeling; location privacy; mix context; pseudonyms; traceability; VANETs

Citation: Ullah, I.; Shah M.A.; Khan, A.; Maples, C.; Waheed, A.; Jeon, G. A Distributed Mix-Context-Based Method for Location Privacy in Road Networks. *Sustainability* **2021**, *13*, 12513. https://doi.org/10.3390/su132212513

Academic Editor: Tan Yigitcanlar

Received: 1 October 2021
Accepted: 5 November 2021
Published: 12 November 2021

1. Introduction

With the growth of wireless technology and intelligent transportation systems, vehicular ad hoc networks (VANETs) are attracting significant attention. Current goals are to make the ad-hoc network more efficient, secure and provide comfort to passenger on the road [1]. The main concern is to provide information regarding traffic congestion, collision notification, emergency, location services, weather conditions, and so on. VANETs can improve road safety and relief of vehicle drivers on the road. Traffic related information is analyzed and shared by vehicles in the network. VANETs is a subclass of mobile ad-hoc networks, which provide communication facilities to nearby vehicles in the road environment, which makes it different from others due to characteristics such as dynamic road topology, communication, sensing capabilities and transmission power for vehicles' function [2].

The basic architecture of vehicular networks consists of Road Side Units (RSU), On-Board Units (OBU), Event Data Recorders (EDR), various sensors, and navigation systems (such as GPS) [3]. RSUs are a road infrastructure that increase the communication connectivity to vehicles. The OBU is fixed in the vehicle with a temper proof device that protects the cryptographic credentials of vehicles. This is used for wireless communication among vehicles and with infrastructure [4]. An EDR archives various events of vehicles communication during a trip on the road. GPS can be used to provide geographical location, vehicle speed, movement direction, and acceleration for a specific time interval [5]. Obstacles on the road are detected with the aid of radar and sensors. In-vehicle, an omnidirectional antenna is fixed for wireless channel access in the network.

The deployment of onboard units permits communication among nearby vehicles and fixed road infrastructure, which make possible three communication models, i.e., Vehicle to Vehicle (V2V), Vehicle to Infrastructure (V2I), and hybrid communication model [3,6]. In the V2V model, there is no support of infrastructure and vehicles are communicated directly. For data and information gathering, vehicles communicate with road side infrastructure through the V2I model. In the hybrid model, vehicles do not communicate with infrastructure directly but communicate in a single or multihop manner, depending on the transmission range of vehicles. This enables long-distance communication between vehicles in the network. Various wireless technologies are suggested for communication in vehicular networks, such Dedicated Short Range Communication (DSRC), Cellular network, WiMax, WiFi, and VeMAC protocol [6,7]. Among the existing technologies, DSRC has the potential for use in wide range variety of applications, including collision avoidance which can save thousands of lives and billions of dollars annually [8].

The mobile node (vehicle) in a network can broadcast Basic Safety Messages (BSMs), Cooperative Aware Messages (CAM) or beacons to disseminate road environment information. The beacon message's contents consist of vehicle identity, velocity, position, and other information [9]. The vehicle broadcasts beacon messages in plaintext format, and so other entities in the network are able to learn the actual identity and location of vehicles by analyzing these beacon messages. Similarly, an adversary can obtain the personal information of a vehicle driver by collecting beacon messages and tracking the various locations visited, thus coming to know the behavior and activities of the vehicle driver. This has the potential to pose several types of threat to the vehicle driver, such as damage to social reputation, physical harassment, blackmailing, and property loss [10]. To protect the privacy of the vehicle, pseudonyms can be used in place of the real identity in the message, and this is a commonly accepted solution. The pseudonym is an alias or randomized identity of a vehicle inserted in the beacon message. However, the use of fixed pseudo-identity is not suitable for protecting the privacy of a vehicle, and it must be changed over time to guard against the linking the pseudonym of a vehicle over time.

For the protection of vehicle location privacy, various pseudonym-changing strategies have been proposed in the literature. Some techniques use the concept of a mix zone [11–15] to hide the vehicle identities in a zone created by the vehicle to change pseudonyms cooperatively. However, the performance of the mix zone is degraded in conditions of lower traffic density [16]. Techniques based on group signatures are introduced [17–20] to protect location privacy of vehicles in which the broadcast beacons are signed with a key assigned to a group to protect the identity of a vehicle in a group. However, the management of signatures in the group administratively burdensome [16]; large groups have difficulty with managing signatures while small group size impacts privacy protection. Schemes based on a silent period [21–23] can hide the identity of vehicles. However, these schemes have a detrimental effect for road safety applications. To overcome the onward limitations of existing schemes, we propose a novel scheme, the Crowd-based Mix Context (CMC) method that efficiently provides location privacy protection under diverse vehicle traffic conditions.

The existing pseudonym changing scheme, Ref. [24] addresses the problem of location privacy in mix zones under lower traffic density. It uses a concept of creating fake

pseudonyms to anonymize the vehicle in the concerned region. However, generating fake pseudonyms in large quantities impact VANET applications and create computational overheads for the vehicle OBU. If a single-vehicle creates fake pseudonyms for anonymity purposes, the attacker may be able to find similarities in beacon messages, to ascertain that only one vehicle is on the road. Furthermore, fake pseudonyms create a liability issue in the network. The work undertaken in [25] is based on both mix zones and silent periods, where a large number of vehicles gather and anonymize identities in silent mode. However, while this works well in an urban scenario that consists of a higher number of vehicles, it is not consistent in the case of lower congested areas such as highways in which vehicles may rarely change pseudonyms [26].

Therefore, to preserve the location privacy of a vehicle, there is a need for an efficient approach that works under various traffic density conditions and also provides privacy outside mix zone areas. In this paper, we propose a distributed scheme CMC that offers privacy protection to vehicles in VANETs. In this paper, the terms network, road network, vehicular network, vehicular communication network and VANETs denote interchangeably and they all refer to vehicular ad-hoc networks. Our contributions in this paper are given below.

1. We introduce a virtual pseudonym exchange suitable method for a low number of vehicles in transmission range. This will mix vehicle identities to provide anonymisation to a target vehicle in that region.
2. Efficiently utilize the diverse traffic density according to the road context information to hide location privacy of a vehicle.
3. We utilize the road network context for the protection of location privacy, which reduces its impacts on road network applications.

The rest of the paper is organized as follows: Section 2 contains details of the existing literature on location privacy schemes. System models and goals are discussed in Section 3. The proposed solution is explained in Section 4. Formal modeling and specification of the proposed model are given in Section 5. Section 6 provides details of the experimental setup and evaluation criteria for location privacy. In Sections 7 and 8, we discuss the performance analysis and comparison of the proposed scheme, respectively. Finally, the paper is concluded in Section 10.

2. Related Work

As mentioned, a pseudonym can be used in beacon messages, rather than the real identity of a vehicle, as a means to provide privacy. However, some limited knowledge of the whereabouts of a vehicle means that the pseudonym of a vehicle can be identified, and all journeys of that vehicle can be recovered. For this reason, pseudonyms are changed periodically. However, simple pseudonym-exchange schemes may suffer from pseudonym linkability. That is, an adversary can discover the relationship between pseudonyms and hence recover vehicle journeys. Several schemes of pseudonym changing are proposed and tested in the literature; here, we review some of these. A taxonomy of location privacy schemes is shown in Figure 1. Table 1 contains details of a comparative analysis of existing schemes in a vehicular network.

A group navigation, in combination with a random silence period, is proposed in [21]. The vehicle remains silent, not broadcasting beacons in the network for a random period to avoid linkability. The vehicles are restricted to forming groups on the road, and the group leader will broadcast messages while other members of the group remain silent. Similarly, an advanced version is presented in [27] again using the combination of silent periods with the group formation concept. The vehicles remain silent if a certain low-speed threshold is met (below 30 km/h) and should change pseudonyms during this period as given in [28]. This means that a vehicle will not broadcast heartbeat messages at slow speeds, with the justification that the possibility of an accident during lower speeds is low. In [29], a safe-distance metric is used to find an obfuscation radius in which the value of velocity, position, and direction is perturbed to enhance the privacy of vehicles.

In addition, if a vehicle did not find any other vehicle within a safe distance, it remains silent to preclude tracking. An autonomous pseudonym update mechanism is presented in [23], which takes the speed and direction as parameters. If a certain traffic weight threshold is met, the vehicle will update its pseudonym in a silent mode, otherwise the vehicle waits for one more silent period. In the context-based scheme, the vehicle adaptively enters and exits from a silent period, changing the pseudonym based on the number of silent neighboring vehicles [30]. A similar scheme is introduced in [31] in which vehicle changes its pseudonym based on the context of silent neighbors. It also assesses the presence of misbehaving vehicles in the network and checks the success of the pseudonym changing process. Another scheme is based on a silent period that uses the concept of permutation to exchange pseudonyms between vehicles to create confusion for an adversary attempting location identification [32]. Silent period-based schemes have certain limitations, i.e., it impacts road network applications, the management of silent period duration for a vehicle trip is difficult to utilize for location protection: the use of a short silent period can provide one way to measure the effectiveness of a pseudonym linkability attack, while, for a long silence period, the knowledge of spatial and temporal relationship makes it possible for an adversary to track the vehicle [33].

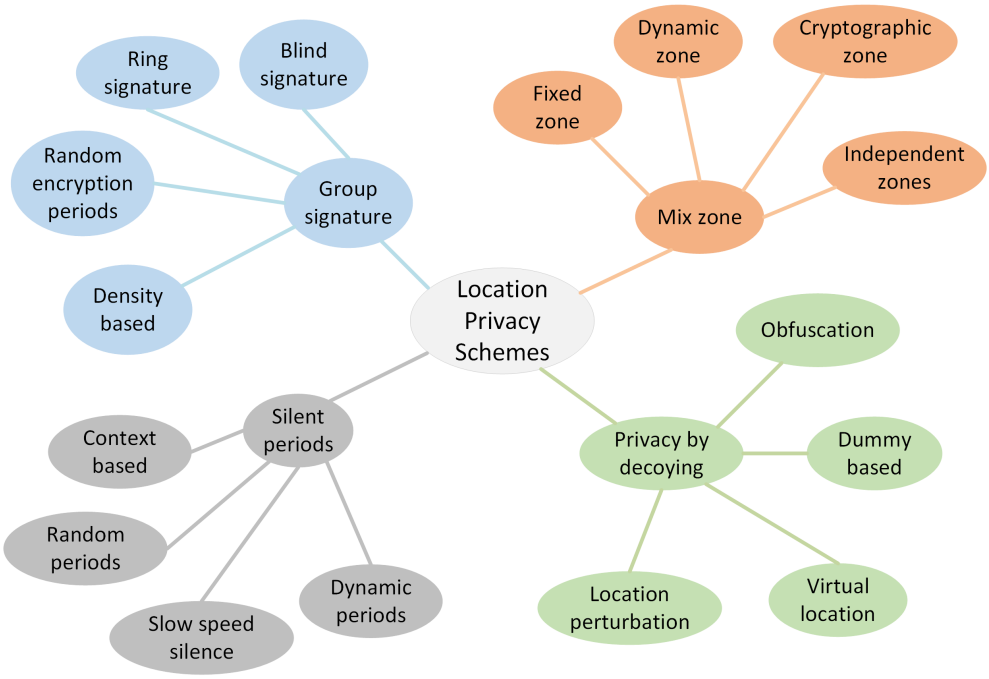

Figure 1. Categories of location privacy schemes.

A group communication method with a random encryption period is introduced in [20,34] for location privacy in VANETs. The scheme increases the confusion of the external attacker by creating an encryption zone around a vehicle's OBU. Another synchronized pseudonym changing protocol is proposed in [35] to provide unlinkability of the vehicle location tracks. The main aim is to break the spatial and temporal relationship of the vehicle pseudonyms. A data forwarding protocol is used in [36] for location privacy based on the social behavior of a vehicle driver. The social behavior of vehicles is collected from visiting social spots, i.e., shopping malls, intersections, and museums. If a vehicle visits a social spot, it can retrieve messages from RSU anonymously. The protocol achieves two things in parallel, i.e., preserves the location privacy and provides reliable transmission in the network. In [18], the concept of a cryptographic mix zone is used to hide the location information of vehicles that are based on one-time identity-based authentication. It has no dependency on trusted party, and the keys are updated within the zone. Any vehicle in the group may be a group key distributor in the cryptographic zone. A revocable group

signature scheme is proposed in [37] for location privacy based on the Chinese remainder theorem and digital signature algorithm. It protects the anonymity of the vehicle as well as providing traceability to TA in case of a dispute of signature. However, the group signature method has certain issues regarding the management of signatures in the group. The signature of a large group is difficult to manage, while smaller groups affect the privacy protection level [33]. In [38], a dynamic grouping and virtual pseudonym exchange scheme is proposed in which diverse traffic conditions are utilized to update pseudonyms of vehicles for location protection.

Some techniques employ dummy data or inaccurate data to generate confusion for an adversary to identify the real location of a vehicle. In such a case, a perturbation algorithm is proposed in [39] that utilizes the reported position of two users at proximity and slightly modifies their position to create confusion for an adversary. The inaccurate beacon message is sent in between the periodic actual beacon messages to break the link between various locations of vehicles [40]. Dummy locations are generated in [41] for privacy protection of vehicles. In [42], the location of the neighboring vehicle is taken as a virtual shadow and sends two requests to LBS with two different locations. It will hide the actual location of a target vehicle from the location attacker. Similarly, virtual position points are generated in [43] that bridge between user and LBS. The sensitivity-based pseudonym changing scheme is introduced in [44] that takes regularities in vehicle movements to achieve personalised vehicle location protection. A new concept of multilevel obfuscation scheme is introduced in [45] to protect the location privacy of vehicles while communicating with LBS. The vehicle generates duplicate messages in connection with the surrounding vehicle to increase vehicle identity anonymisation in the vicinity. The concept of differential privacy and pseudonym permutation is used in [46] to hide the location trajectory of the vehicle. The trajectory of the user is divided into coarse-grained and fine-grained under the personalized user privacy requirements. Similarly, a new technique is introduced in [47] that protects the user's semantic location trajectory. It uses the concept of reinforcement learning based on differential privacy that randomizes the locations of the vehicle's trajectory. The optimized obfuscation policy is used in terms of privacy improvement and the loss of quality of the services. The obfuscation and hiding in the crowd concept are combined in [48] to increase confusion for an adversary trying to link vehicles' pseudonyms. The dummy-based location privacy scheme improves the level of privacy to some extent. However, there are certain problems related to these schemes, including management of dummy data being an issue, their impact on the quality of services, and generating overhead in the network.

Table 1. Comparative analysis of location privacy schemes in VANETs.

Ref.	Method	Adversary Model	Mode of Execution	Accountability	Preserve VANETs Applications	Privacy Metrics	Cost (Time, Computation, Communication)
[49]	Cooperative	General adversary	Infrastructure less	No	No	Protection rate	Not given
[13]	Mix zone	GPA	Infrastructure based	No	No	ASS, Location privacy gain	Reduced
[14]	Random selection	Passive adversary	Infrastructure based	No	No	ASS	Increased
[50]	Silent mode	Global passive adversary	Infrastructure less	No	No	ASS, entropy, tracking probability	Reduced
[32]	Scheme permutation	Global passive adversary	Infrastructure less	Yes	Yes	ASS, traceability, confusion, entropy	Not computed
[24]	Dummy data	External global attacker	Infrastructure less	No	No	Anonymity	Reduced
[12]	Cheating detection	Global passive adversary	Infrastructure based	No	No	ASS, entropy, attacker probability	Not mentioned
[30]	Silent mode	Global passive adversary	Infrastructure less	No	Yes	Anonymity, Traceability	Not mentioned
[31]	Silent mode	Global passive adversary	Infrastructure less	No	Yes	ASS, entropy, traceability	Not computed
[9]	Triggered based	External passive adversary	Infrastructure less	Yes	Yes	Anonymity, entropy, Tracking percentage,	Not computed
[51]	Dummy data	Global passive adversary	Infrastructure less	No	Yes	ASS, entropy, tracking probability	Not computed
[42]	Route confusion	General attacker	Infrastructure based	No	No	ASS, entropy, traceability	Not mentioned

A mix zone scheme is proposed in [52] which considers context information to change pseudonyms. The context information may be the number of neighbors, direction, and speed. The vehicles will find suitable opportunities to blend and be an anonymisation set with vehicles having similar properties. Julien et al. proposed to create mix zones at suitable areas to protect the location information of vehicles [53]. The privacy of vehicles in the mix zone is improved in [54] with the help of using a cryptographic concept. Here, the vehicle shares the status information only with neighboring vehicles. In [13], the pseudonym changing strategy is applied at a social spot which may be a road intersection or shopping malls, where several vehicles gather. The social spot becomes a mix zone to hide vehicle identities. The vehicles form a mix zone dynamically in [55] to guard against the linking of an old pseudonym to the new one. The messages of vehicles are encrypted in the zone. A similar scheme, introduced in [56], creates a mix zone dynamically and changes pseudonym based on the vehicle candidate location list. Abdelwahab et al. [57] introduced the concept of a silent mix zone, in which vehicles remain silent at the roadside intersection. An improvement is made in [15] to build an urban pseudonym changing strategy in silent zones; the vehicles exchange their pseudonyms in the silent zone.

Reputation-based schemes are proposed in [58,59] and these encourage the "selfish" vehicle behavior for pseudonym changing in the mix zone to protect location privacy. Pseudonym management and changing techniques are introduced in [60], where vehicles create a privacy zone at roadside infrastructure. The level of privacy protection is subject to a number of vehicles in the zone. In [61], a secure mix zone is created based on spatial and temporal factors. It has been shown that a temporal factor shift improves the privacy of vehicles. The virtual mix zone is created dynamically based on the expiry of pseudonyms [62]. A reputation model is also presented to encourage selfish vehicles to join the zone. The dynamic pseudonym changing technique proposed in [16] constructs multiple mix zones in the network. The privacy of the mobile object is protected with the help of the cryptographic methods in the communication. In [11], mix zones are planted at specific regions where vehicles change pseudonyms to hide their identities for the protection of vehicle privacy. A de-correlation privacy scheme is proposed in [63] that creates multiple mix zones in parking lots and traffic places. It achieves a high level of privacy protection of vehicle trajectory. Despite the useful features of the mix zone-based location privacy techniques, there are certain limitations. Firstly, in the mix zone, the level of privacy is degraded when operating in lower traffic density environments [17]. Secondly, privacy is provided to vehicles within the zone, and there is no privacy protection outside it. Thirdly, if the zones are deployed at fixed regions, only these areas provide the privacy protection and deployment costs increase the need to build a large number of zones with infrastructure support in the road network area.

Based on problems and limitations in the existing schemes for location privacy in a vehicular network, we propose a novel scheme using a crowd-based mix context that utilizes the diverse nature of vehicle traffic densities. The pseudonyms changing process depends on the number of neighbors in the transmission range and road context information. This improves the anonymisation of a target vehicle (a vehicle that an adversary wants to locate) in a crowd of similar-status vehicles in a concerned region.

3. Models and Goals

In this section, we discuss the system model and the adversary model. After that, the goals of this research work are explained. The first subsection provides a details of the entities used in the system model. The second subsection discusses assumptions about the strength of an adversary, and in the last subsection, we discuss the goals of the research work.

3.1. System Model

The system model is comprised of three things, namely the Trusted Authority (TA), RSU, and Vehicles. The depiction of the system model is shown in Figure 2. The Trusted

Authority (or certification authority or Government Authority) is assumed to be honest and will not take part in compromising vehicle location [62,63]. The vehicle must be registered with the TA before joining the ad hoc network. The TA provides a pseudonym pool to vehicles to be used for a number of days. The pseudonym is used for anonymous broadcast of beacon messages. On the expiry of its pseudonym pool, the vehicle can request another pseudonym pool from the TA. We assume that the vehicle has been registered with TA and is assigned a pseudonym pool. An RSU is a roadside infrastructure fixed on the road to increase the communication range of vehicles. It is a semi-honest entity in the system model, and it may or may not compromise the privacy of a vehicle. RSUs also play a role in the dissemination of data to other entities of the system model. We also assume that the authentication process is performed by each vehicle. The vehicle contains an OBU that is used for communication with other OBUs and infrastructure in the network. OBU records communication events of vehicles. The vehicle has a tamper-proof device that stores the key materials securely, such as anonymous identities and records of all communication events [64]. The vehicle is also equipped with GPS for precise location updates.

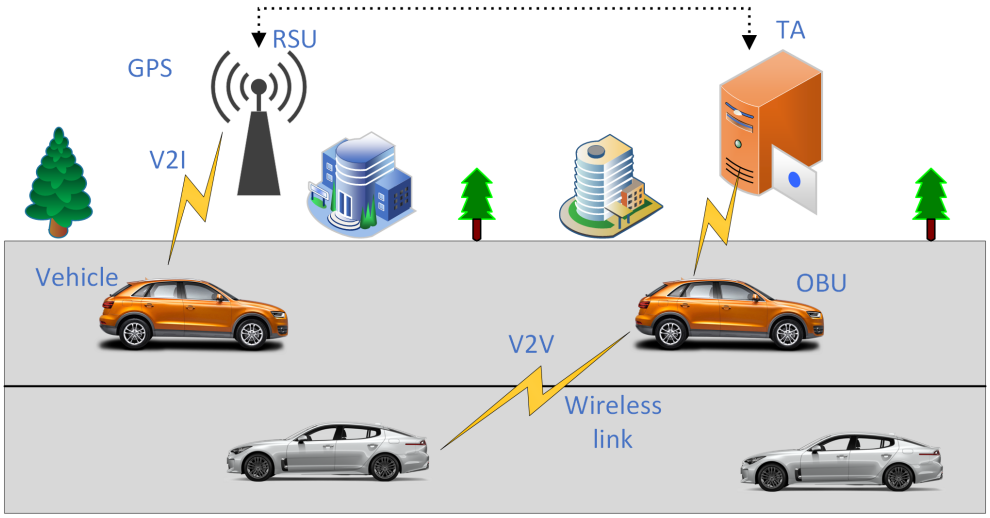

Figure 2. Basic system model.

3.2. Adversary Model

We assume a Global Passive Adversary (GPA) in this work. The detail of the adversary model is shown in Figure 3. The aim of the GPA is to track various locations to identify the journeys of a target vehicle in the network. In this model, we make various assumptions about the GPA. The GPA can deploy a low-cost radio transceiver to intercept broadcast beacon messages in the region of interest. The contents of the beacon message are pseudo-identity, speed, location, direction, and other headings. The adversary can capture a large portion of the network to catch the messages exchanged between vehicles. It can track the various locations of a vehicle with the help of eavesdropping vehicle communication [22]. It also has the ability to capture the pseudonyms of vehicles and can link the various pseudonyms of a vehicle used during a trip. The adversary captures beacon messages to try to correlate the old pseudonym with the newly changed pseudonym. By matching the different pseudonyms of a vehicle at different locations, the adversary gets knowledge of the target vehicle's behavior and could predict a vehicle's future locations.

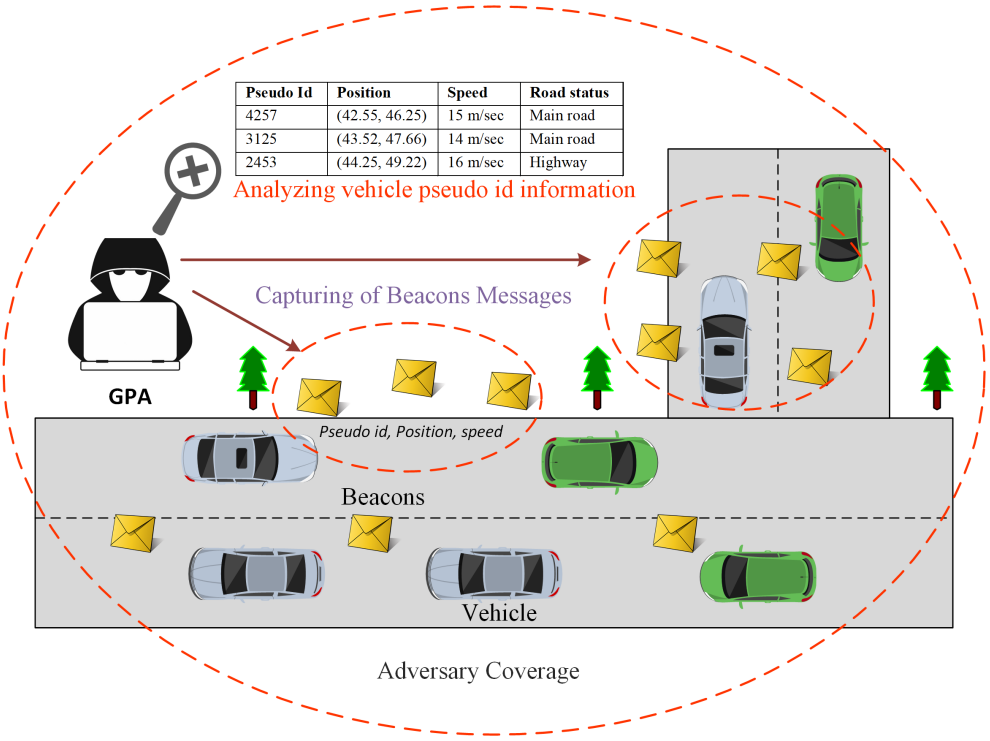

Figure 3. Adversary model.

3.3. Goals

Our primary concern in this research work is to achieve a high level of location privacy in a vehicular network. For this purpose, various factors and parameters are required. The factors include vehicle speed, traffic density, moving direction, and other road context information. The following goals are set to be achieved in this research work:

1. Location anonymisation at diverse vehicle traffic conditions.
2. Virtual pseudonym exchange process to protect location under low traffic conditions.
3. Dynamic mix context zone creation based on different road parameters such as vehicle speed, direction, and traffic density.
4. The pseudonym change and exchange process are based on the road context information.
5. Preventing an adversary from linking various pseudonyms of a vehicle at different location spots.
6. Reducing the impact of privacy protection on the efficacy of road network applications.

4. Proposed Solution

We propose a crowd-based mix context scheme which offers location privacy to vehicles in a vehicular network. The scheme comprises two cases based on the vehicle speed, direction, and traffic density. The first case in our proposed scheme is the road intersection or the situation in which vehicles have low speed and traffic congestion on the road. In the second case, vehicles have low speed and fewer neighbors within transmission range. We use a mix context method to hide the actual identity of the vehicle in a crowd. A crowd of vehicles of similar status neighboring vehicles is established where they mix their context and identities to blur the sensitive information of vehicles. Here, context means a vehicles' direction of movement, speed range, and the number of transmission range neighboring vehicles. The proposed scheme block diagram is shown in Figure 4. The vehicle senses the environment to find the number of neighboring vehicles in its range. Based on the road context information, vehicles change pseudonyms to mix it in the crowd of vehicles. Otherwise, the virtual crowd method is used to mix the identities of vehicles. In the first case, there is a higher number of neighboring vehicles in the vicinity, and the simple pseudonym changing process is used, while in the second case, there is a lower

number of neighboring vehicles in the transmission range, so the target vehicle selects neighboring vehicles randomly to exchange pseudonyms with. In both of these cases, there is a need for the protection of location privacy of vehicles. The whole process of the crowd-based mix context procedure is explained with the help of Algorithm 1. *DenThreshold* is the vehicle traffic threshold and *NeigThreshold* is the number of transmission range vehicles in the vicinity of a target vehicle. The high-level flowchart of the mix context scheme is shown in Figure 5.

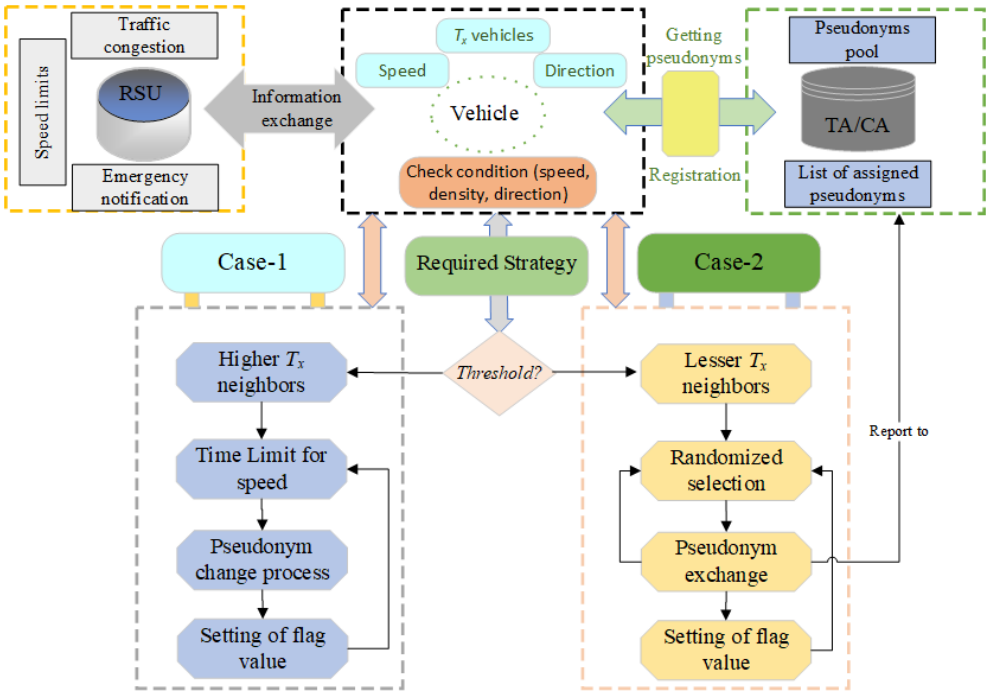

Figure 4. The block diagram of vehicles context mixing.

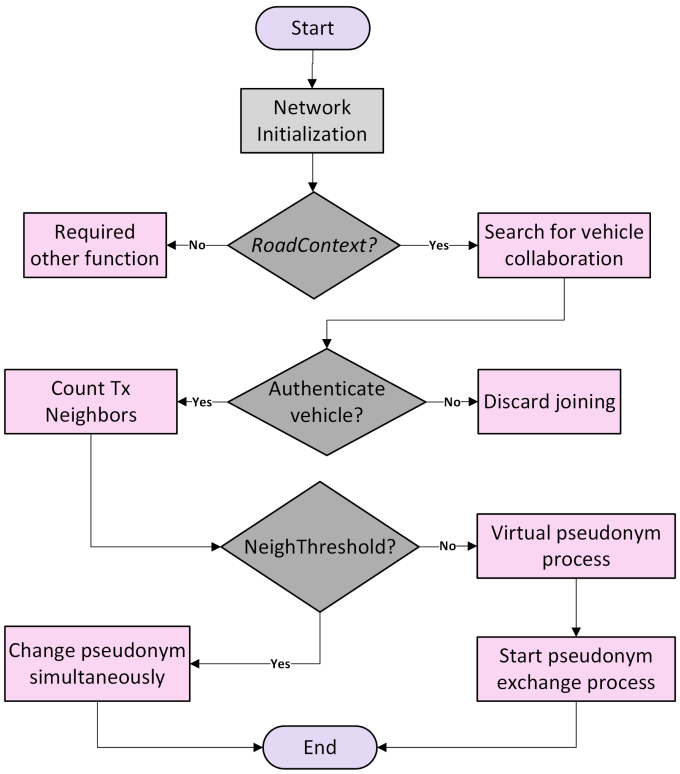

Figure 5. The high-level flow of the mix context method.

Algorithm 1 Crowd-based Mix Context.

Initialization: V_i: Any vehicle i, T_x: Transmission range, $DenThreshold$: Density threshold, $NeigThreshold$: Neighbor threshold, VD: Vehicle density, SP_R: Speed range, $LatencyBroad$: Beacon broadcast latency, D: Direction of vehicle
Input: SP_R, D, $DenThreshold$, T_x
Output: Successful pseudonym update process

for $V_i = 1 \rightarrow n$ **do**
  $NeighborFunction(SP_R, D, T_x)$
  if $VD \geq DenThreshold$ **then**
    Wait (TimeLimit)
    if Speed (lower) **then**
      Increase $LatencyBroad$(BSMs)
    else
      Normal broadcast
    end if
  end if
  if $Neigbhors(V_i) \geq NeigThreshold$ **then**
    Change pseudonym cooperatively
    Set $PUpdate(V_i)$ to 0
  else
    Randomize selection of T_x neighboring vehicle
    Select V_j as virtualizer of V_i
    Exchange $Msgs(V_i, V_j)$
    Report Pseudonyms exchanged to TA
  end if
  Set timer for pseudonym change $Pseudo(t)$
    Expiry of $Pseudo(t)$
    Set $PUpdate(V_i)$ to 1
    Start beacon transmission and wait for at least k context neighbors
end for

The neighbor function is used to search and count the number of neighboring vehicles in the transmission range. The procedure of neighbor function is given in Algorithm 2. The speed range, transmission range, and distance are given to the algorithm as input.

Algorithm 2 Neighbor Function.

Initialization: V_i: any vehicle i, T_x: Transmission range, SP_R: Speed Range, D: Direction of a vehicle, $CountV_{ID}$: Counting of number of vehicles
Input: SP_R, T_x, D
Output: Number of transmission range vehicles ($CountV_{ID}$)

for $V_i = 1 \rightarrow n$ **do**
  $MessageReceived(M_i)$
  Check(V_{ID}, Distance, SP_R)
  Calculate Distance (V_i, V_j)
  if $(V_{ID} \neq V_{ID}(i) \quad and \quad Distance \leq 300$ m) **then**
  $CountV_{ID}++$
  else
    Check again(Limit)
  end if
end for
Return $(CountV_{ID})$

4.1. Vehicle High Traffic Density at Low Speed

The vehicles sense the road environment and search for transmission range neighboring vehicles. In this case, the vehicle neighbor threshold is checked and verified, and based on the neighbor threshold, the pseudonyms of all vehicles are changed in the crowd. It mixes the context and pseudonyms of vehicles and confuses an adversary attempting to identify the vehicle in such a fluxed environment. This concept is shown in Figure 6. A crowd of vehicles is established when the vehicle's speed is reduced due to a roadside intersection or due to some traffic congestion situation occurring on the road. Every vehicle will broadcast a beacon message to ensure its presence in the congested vehicles' area and inform each neighboring vehicle about the pseudonym change. Each vehicle's neighborhood is verified based on the beacon message's information, i.e., transmission range, same direction, and same speed range. The vehicle will wait and continuously search for neighbors until a certain vehicle threshold is reached, when all vehicles start to change pseudonyms instantaneously. This means that each vehicle changes pseudonyms in the crowd of vehicles to anonymize itself. The contents of a beacon message include $BM(P_{ID}, T_x, V, NeighCount, D, DThresh, PUpdate)$, where P_{ID} is the pseudonym assigned to the vehicle, T_x is transmission range, V is the speed of the vehicle, $NeighCount$ counts the number of vehicles in the transmission range, D is the direction of the vehicle, $PUpdate$ is the updated pseudonym, and $DThresh$ is the vehicle density threshold.

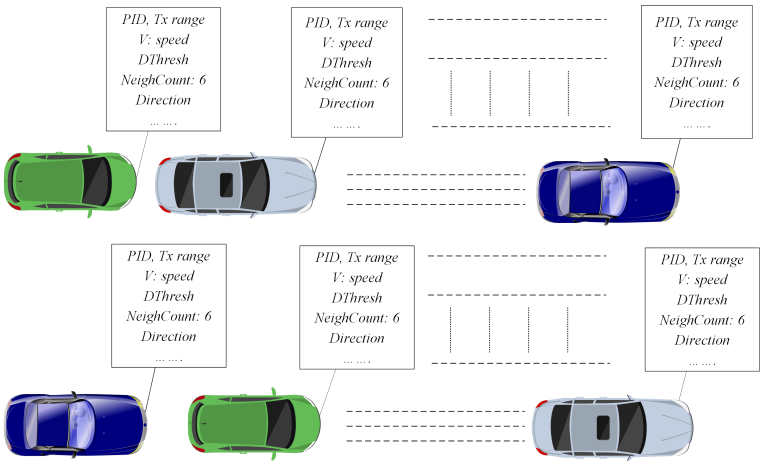

Figure 6. Mixing of context information in the crowd of vehicles.

The main procedure of case 1 is shown in Algorithm 3. The vehicle will monitor its speed and check neighboring vehicles in its transmission range. If the speed is less than a certain threshold, the vehicles will set the $Pupdate$ value to 1, which means that vehicles are ready to change pseudonyms. The vehicles will wait a certain amount of time if their speed remains low; the broadcast delay of beacon messages is increased. The delay in the broadcast of beacon messages reduces neighboring vehicles' burden for counting the number of vehicles in the vicinity. For pseudonym changing, all vehicles in the transmission range will change simultaneously and set $Pupdate$ to 0, which means that the pseudonym has been changed successfully. The pseudonym has a specific expiry time, and after this time, the flag is set to 1 and waits for another pseudonym change in the best context situation.

Algorithm 3 Mix context at higher density.

Initialization: V_i: Any vehicle i, T_x: Transmission range, $NeighThreshold$: Neighbor threshold, SP_R: Speed range, $TimeLimit$: waiting time limit, D: vehicle direction
Input: SP_R, direction, $NeighThreshold$, T_x
Output: Successful pseudonym change process

for $V_i = 1 \rightarrow n$ **do**
  $NeighborFunction(SP_R, D, T_x)$
  Set $PUpdate(V_i) = 1$
    Wait $(TimeLimit)$
  if SpeedCheck (lower) **then**
    Increase delay in Beacon broadcast
  else
    Otherwise normal broadcast
  end if
  if $Neighbors(V_i) \geq NeighThreshold$ **then**
    Change pseudonyms simultaneously
      $PUpdate(V_i)$ set to 0
      Set timer for pseudonym change $Pseudo(t)$
        After expiry of $Pseudo(t)$
        $PUpdate(V_i)$ set to 1
  else
    Case 2 function
  end if
end for

4.2. Vehicle Low Traffic Density at Low Speed

The second case of the proposed scheme involves low vehicle speed under low-traffic conditions. In this case, the virtual mix crowd method is used. The virtual crowd method scans the road environment for neighborhood vehicles in the surroundings, and based on the context of the vehicle neighbor's, the virtual pseudonym exchange process is executed. The target vehicle randomly selects one of the neighboring vehicles to exchange real and virtual pseudonyms with, as shown in Algorithm 4. Recall the beacon message include $BM(P_{ID}, T_x, V, NeighCount, D, DTresh, PUpdate)$ and is used to sense the vehicle traffic environment. In the virtual pseudonym exchange scheme, the vehicle randomly selects one of the transmission range neighbors to exchange pseudonyms and update its $PUpdate$ attribute. We discuss the virtual pseudonym exchange process with the help of an example. If vehicle V_1 wants to change the pseudonym and has V_2, V_3, V_4, and V_5 in its neighbor list. V_1 will randomly select one of the vehicles and start an exchange of pseudonyms with V_4. After completing the exchange process, both vehicles update their status of $PUpdate$ and publish it to the vehicle's crowd. Each vehicle that exchanges pseudonyms must report to the CA the pseudonyms exchanged. This process will reduce the liability issue in the network. The vehicle generates an image of its real pseudonym and exchanges it with its neighboring vehicle. The receiving vehicle verifies both of these pseudonyms, accepts the real one, and rejects the fake pseudonym. The vehicle generates such an image of a pseudonym that it is difficult for an adversary to identify it. Similarly, other vehicles such as V_2, V_3, and V_5 also apply the virtual pseudonym exchange process in the vicinity. As many vehicles take part in the virtual pseudonym exchange process, this produces a virtual crowd of vehicles in the network, which mixes each vehicle identity and location in the crowd. The pseudonyms exchange process is shown in Figure 7.

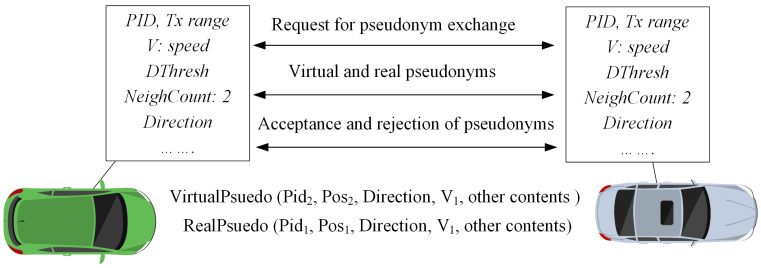

Figure 7. Virtual pseudonym exchange process between two vehicles.

Algorithm 4 Virtual Mix Context.

Initialization: V_i: Any vehicle i, T_x: Transmission range, $NeighThreshold$: Neighborhood threshold, SP_R: Speed range, D: Direction of vehicle, $LatencyBroad$: Beacon broadcast latency, $PUpdate$: Pseudonym update value
Input: SP_R, D, $NeighThreshold$, T_x
Output: Pseudonym Exchange process

for $V_i = 1 \rightarrow n$ **do**
  $NeighborFunction(SP_R, D, T_x)$
  if $Neighbor(V_i) \geq NeighThreshold$ **then**
    $CallAlgo2()$
  else
    Set $PUpdate(V_i) = 1$
    Increase $LatencyBroad$(BSMs)
  end if
  Randomize selection of a T_x neighboring vehicle
  select V_j as virtualizer of V_i
  Exchange $Msgs(V_i, V_j)$
    $Msg_1(P_{ID1}, POS_1, othercontents)$
    $Msg_2(P_{ID2}, POS_2, othercontents)$
  Set $PUpdate(V_i) = 0$
  Report Pseudonyms exchanged to TA
  Set timer for pseudonym change $Pseudo(t)$
    After expiry of $Pseudo(t)$
    Set $PUpdate(V_i)$ to 1
end for

5. Formal Modeling and Specification

High-Level Petri Nets (HLPN) is used for two reasons [65]: to simulate the proposed model and provide mathematical representation for analyzing the proposed model's behavior and structure properties. Formal modeling benefits are the interconnection of system components and processes, information flow among the processes, and information processing. We used HLPN for formal modeling and specification of the proposed scheme. HLPN is a set of seven tuples $(P, T, F, \varphi, R, L, M_0)$ as defined in [66].

In this section, we formally model and specify the proposed scheme CMC. We present the CMC scheme in HLPN in terms of mathematical properties (rules). For the representation of the system in HLPN, we define places and their associated data types; then, we specify a set of rules used in HLPN. Tables 2 and 3 contain details of the symbols and places used in the Petri nets. We design HLPN for Algorithms in the proposed model. Figure 8 shows the HLPN for the mix context scheme. The vertical bar shows transitions, and the circle shows places used in HLPN. The arrowheads in the diagram show the data flow in HLPN.

Table 2. Symbol description used in the mix-context method.

Symbol	Description
Reg-Request	Request for vehicle registration to TA
VRD	Vehicle registration data
AssignPool	Assign pseudonym pool to vehicles
PL	Pseudonym list
SM	Speed monitor
DC	Distance calculation
NS	Neighbor selection
NC	Neighbor count
NT	Neighbor threshold
SameID	Same vehicle (only one vehicle)
RC	Vehicle ready to change pseudonym
CPC	The cooperative pseudonym change process
ExpiryT	Pseudonym expiry time
PEP	Pseudonym exchange process
TxN	Transmission range neighbors
RSN	Random selection of neighbors
PE	Pseudonym exchange
BC	Broadcast beacon messages
LPN	Vehicle license plate number
V_{ID}	Vehicle identity
P_{ID}	Pseudo IDs of a vehicle
WT	Waiting time

Table 3. Places used in HLPN for mix-context method.

Types	Description
φ (Reg-Request)	$P(V_{ID} \times LPN)$
φ (VRD)	$P(V_{ID} \times PK_v \times P)$
φ (Pseudo-Request)	$P(V_{ID} \times LPN)$
φ (PL)	$P(P_{ID} \times PK_v \times P)$
φ (Road-Condition)	$P(SP_R \times D \times T_x)$
φ (SM)	$P(P_{ID} \times SP \times SP_R \times D)$
φ (DC)	$P(P_{ID} \times POSV_i \times POSV_j \times Dist)$
φ (NS)	$P(P_{ID} \times T_x \times Neigh)$
φ (NC)	$P(P_{ID} \times Dist \times NeighC)$
φ (NT)	$P(P_{ID} \times NeighC \times Dist \times Flag)$
φ (SameID)	$P(P_{ID} \times Dist)$
φ (RC)	$P(P_{ID} \times N_{ID} \times Thresh \times Indicator)$
φ (CPC)	$P(P_{ID} \times N_{ID} \times IndicatorS)$
φ (PUpdate)	$P(P_{ID} \times WT \times Flag)$
φ (ExpiryT)	$P(P_{ID} \times ThreshT \times WT \times Flag)$
φ (PEP)	$P(P_{ID} \times N_{ID} \times Thresh \times Indicator)$
φ (T_xN)	$P(P_{ID} \times N_{ID} \times IndicatorS \times RSN)$
φ (PE)	$P(P_{ID} \times N_{ID} \times Msg_i \times Msg_j)$
φ (BC)	$P(P_{ID} \times MsgP_i \times MsgP_j)$

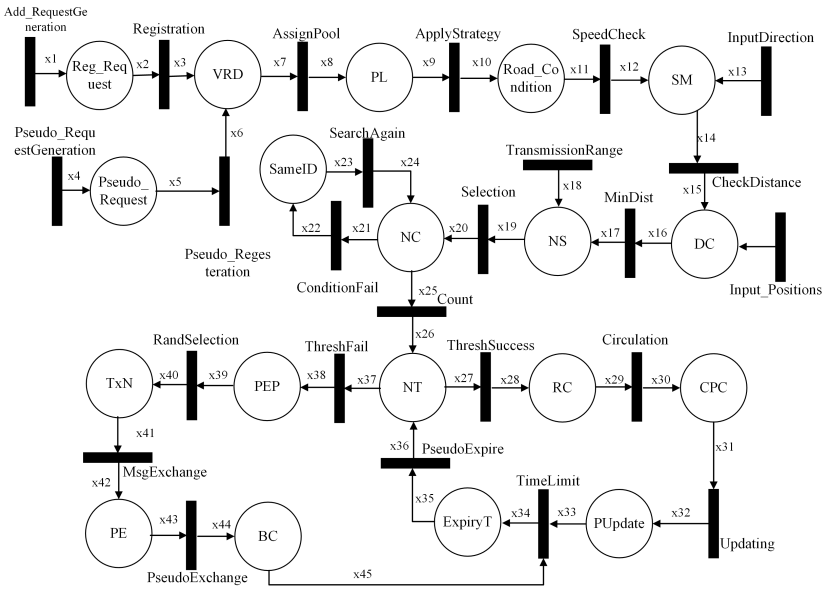

Figure 8. HLPN for mix context method.

The vehicle must register with TA before joining the network. For this purpose, the vehicle requests TA for registration. The TA processes the demand and provides Public Key (PK_v) and pseudonyms (P) in Equation (1). In Equation (2), a vehicle requests a pseudonym pool if it has expired. To assign the pseudonym pool to a vehicle, the vehicle's identity is verified, and the pseudonym pool is assigned to a vehicle as given in Equation (3). The identity of the vehicle is matched with V_{ID} and LPN in the vehicle registration list. The data in VRD is updated with a pseudonym pool assignment:

$$\begin{aligned} \boldsymbol{R(Registration)} = \forall\, i2 \in x2 \wedge i3 \in x3 \mid i2[1] \neq i3[1] \\ \wedge\, x3' := x3 \cup \{i2[1], i3[2], i3[3]\}. \end{aligned} \tag{1}$$

$$\begin{aligned} \boldsymbol{R(Pseudo-Registeration)} = \forall\, i5 \in x5 \wedge i6 \in x6 \mid \\ Add-request(x6' := x6 \cup \{i5[1], i6[1]\}). \end{aligned} \tag{2}$$

$$\begin{aligned} \boldsymbol{R(AssignPool)} = \exists\, i7 \in x7 \wedge i8 \in x8 \mid compare \\ (i7[1], i8[1]) = True \rightarrow x8' := x8 \wedge i8[1]. \end{aligned} \tag{3}$$

After the vehicle registration process, the concerned strategy of mix context is started as given in Equation (4), where vehicles sense the road conditions. First, vehicles will monitor the speed using speed check-in Equation (5). If the vehicle speed is in a particular range, then the distance (Equation (6)) is calculated with its neighboring vehicles. The distance calculation process takes position coordinates of transmission range vehicles. The vehicle will select another neighboring vehicle with a minimum distance for mixing road context information. The minimum distance is checked in (Equation (7)):

$$\begin{aligned} \boldsymbol{R(ApplyStrategy)} = \forall\, i9 \in x9 \wedge i10 \in x10 \\ \mid RoadCondition(i10[1], i10[2], i10[3]) \wedge \\ x10' := x10 \cup \{i9[1], i10[1]\} \end{aligned} \tag{4}$$

$$\begin{aligned} \boldsymbol{R(SpeedCheck)} = \forall\, i11 \in x11 \wedge i12 \in x12 \mid \\ i11[1] \in i12[3] \wedge x12' := x12 \cup \{i12[1], i12[2]\}. \end{aligned} \tag{5}$$

$$\begin{aligned} \boldsymbol{R(CheckDistance)} = \forall\, i14 \in x14 \wedge i15 \in x15 \mid \\ i14[1] \in i15[1] \wedge Distance(i15[2], i15[3]) \rightarrow i15[4]. \end{aligned} \tag{6}$$

$$\boldsymbol{R(MinDist)} = \forall\, i16 \in x16 \wedge i17 \in x17 \mid (i16[4] \leq i17[2]) = True \rightarrow x17 := x17 \cup \{i17[3]\}. \tag{7}$$

After measuring the minimum distance between neighboring vehicles, the neighbor with minimum distance is selected as given in Equation (8). Next, the number of neighbors within the transmission range is counted in Equation (10). Certain conditions are required and, if the condition fails, as given in Equation (9), then finding of neighbors in transmission range starts again:

$$\boldsymbol{R(Selection)} = \forall\, i19 \in x19 \wedge i20 \in x20 \mid (i19[1] \neq i20[1] \wedge i20[2] \leq 300) = True \rightarrow x20' := x20 \cup \{i20[3]\}. \tag{8}$$

$$\boldsymbol{R(ConditionF)} = \forall\, i21 \in x21 \wedge i22 \in x22 \mid (i21[1] = i22[1]) \wedge \exists\, (i22[1] = x22[1]). \tag{9}$$

$$\boldsymbol{R(Count)} = \forall\, i25 \in x26 \wedge i26 \in x26 \mid i25[1] \neq i26[1] \wedge (i25[3] \leq 300) = True \rightarrow x26' := x26 \cup \{i26[2] + +\}. \tag{10}$$

When the counting of neighbors is complete, the neighbor threshold is checked to determine the concerned case of mix context. In Equation (11), the neighbor threshold is met, and the process of cooperative pseudonym changing is circulated in the neighborhood as given in Equation (12):

$$\boldsymbol{R(ThreshSuccess)} = \forall\, i27 \in x27 \wedge i28 \in x28 \mid (i27[2] \geq i28[3]) = True \rightarrow x28' := x28 \cup \{i28[2], i28[4]\}. \tag{11}$$

$$\boldsymbol{R(Circulation)} = \forall\, i29 \in x29 \wedge i30 \in x30 \mid (i30[3] = i29[4]) \wedge x30' := x30 \cup \{i30[3]\}. \tag{12}$$

Next, Equation (13) shows the start of cooperative pseudonym updating process, and the vehicles in the transmission range change their pseudonyms; set a flag to 0 means that all neighboring vehicles change pseudonyms successfully. A time limit (Equation (20)) is set for the newly changed pseudonym, and after the pseudonym time expiry, vehicles set a flag to 1 (Equation (15)), which means that vehicles are ready for another pseudonym changing process:

$$\boldsymbol{R(Updating)} = \forall\, i31 \in x31 \wedge i32 \in x32 \mid i31[1] = i32[1] \rightarrow x32' := x32 \cup \{i32[3] == 0 \wedge i32[2]\}. \tag{13}$$

$$\boldsymbol{R(TimeLimit)} = \forall\, i33 \in x33 \wedge i34 \in x34 \mid (i33[2] \geq i34[2]) = True \rightarrow x34' := x34 \cup \{i34[3]\}. \tag{14}$$

$$\boldsymbol{R(PseudoExpire)} = \forall\, i35 \in x35 \wedge i36 \in x36 \mid (i35[1] = i36[1] \wedge i35[3] \geq i35[2] = True \rightarrow x36' = x36 \cup \{i36[4] == 1\}. \tag{15}$$

If the neighbor threshold is not met (Equation (16)), then the second case of mix context is chosen, in which a target vehicle in a vicinity randomly selects a neighboring vehicle (as given in Equation (17)) for a virtual pseudonym exchange process. The messages are exchanged between selected neighboring vehicles (Equation (18)) for a pseudonym update process. Next, vehicles exchange pseudonyms as given in Equation (19). In Equation (20), again a time limit is set for the expiry of the newly changed pseudonym:

$$\boldsymbol{R(ThreshF)} = \forall\, i37 \in x37 \wedge i38 \in x38 \mid (i37[2] < i38[3]) = True \rightarrow x38' := x38 \cup \{i38[2], i38[4]\}. \tag{16}$$

$$\boldsymbol{R(RandSelection)} = \forall\, i39 \in x39 \wedge i40 \in x40 \mid i39[4] = i40[3] \wedge x40' := x40 \cup \{i40[4]\}. \tag{17}$$

$$\boldsymbol{R(MsgExchange)} = \forall\, i41 \in x41 \wedge i42 \in x42 \mid if(i42[2] \in i41[4]) = True \rightarrow x42' := x42 \cup \{Exchange(i42[3], i42[4]\}. \tag{18}$$

$$\boldsymbol{R(PseudoExchange)} = \forall\, i43 \in x43 \wedge i44 \in x44 \mid Exchange(i43[3], i43[4]) = True \rightarrow x44' := x44 \cup \{Exchange(i44[2], i44[3])\}. \tag{19}$$

$$\boldsymbol{R(TimeLimit)} = \forall\, i45 \in x45 \wedge i34 \in x34 \mid (Exchange(i44[2], i44[3])) = True \rightarrow x34' := x34 \cup \{i34[3]\}. \tag{20}$$

6. Experimental Setup

We conducted various simulations of our proposed scheme to analyze its performance in vehicular networks. This section contains two parts: in the first part, we explain the simulation environment setup and parameters used in the simulation. In the second part, we discuss the evaluation metrics used for location privacy.

6.1. Simulation Setup

For the simulation of the proposed CMC scheme, we used Network Simulator 2 (NS2). The simulation parameters are described in Table 4. We run the simulations for 400 s in an urban environment. We deploy 200 vehicles on the real world map created with SUMO. The simulation area is approximately 5249 × 5053 square meters. The speed range is up to 10 m per second in the road network. We use SUMO for realistic mobility generation of vehicular networks. The OpenStreet map is used to provide a real world road scenario, as shown in Figure 9. The map is converted into SUMO to generate vehicle traffic on a real-world map. The vehicle mobility model file is generated with the help of SUMO. The simulation is run with diverse vehicle traffic densities.

Table 4. Simulation parameters for CMC.

Parameters	Value
Simulator	NS2, SUMO
MAP	OpenStreetMap
Routing protocol	AODV
Bit rate	6 MBPS
Simulation time	400 s
Number of Vehicles	200
Road area	5249 × 5053 m
Speed range	0–10 m/s
MAC protocol	IEEE 802.11p
Transmission range	500 m
Beacon interval	300 ms

Figure 9. Real-world road network scenario using SUMO and OpenStreetMaps.

6.2. Evaluation Criteria

The evaluation criteria used in the majority of the literature are anonymity set size, entropy, and location traceability. These parameters are used to calculate the privacy protection level in VANETs. The privacy metrics are given below.

6.2.1. Anonymity Set Size

Anonymity is one of the significant metrics for evaluation of location privacy. It is the process of the grouping of users of similar status in a vicinity that hides the identity of a user in the group. Anonymity Set Size (ASS) is defined is the set of users/vehicles, including target users that are indistinguishable among the group of users. ASS achieves the anonymisation of the vehicle in a group of vehicles of similar status. In the road network, ASS is preferred, which hides the actual identities of a target vehicle during communication. Its value affects the location privacy of vehicles. The higher the ASS, the higher will be the level of vehicle privacy. We consider the arrival of vehicles at a particular point at the road is the Poisson process with rate λ and X is a random variable that denotes the number of vehicles gathered at the congested area for an interval of time T; then, the probability is calculated as follows [12]:

$$P(X = x) = \frac{(\lambda T)^x}{x!} e^{-(\lambda T)}, \tag{21}$$

where λT is the expected number of vehicles that change pseudonyms cooperatively. This can improve the anonymity of vehicles in the vicinity by updating pseudonyms at the same time. Hence, the expected number of vehicles during the time T is denoted as:

$$E(X = x) = \sum_{x=1}^{\infty} x \frac{(\lambda T)^x}{x!} e^{-(\lambda T)} = \lambda T. \tag{22}$$

After the computation of probability and the expected number of vehicles at a certain time, the anonymity set size is calculated as follows:

$$|ASS| = \sum_{i,j=1}^{n} V_i PC_j = \sum_{i=1}^{n} E(X_i = x) = \sum_{j=1}^{n} \lambda_j T. \tag{23}$$

where $V_i PC_j$ is the number of vehicle update pseudonyms that anonymize the target vehicle in the region.

6.2.2. Entropy

The entropy is used to evaluate the level of privacy of vehicles in the network. It calculates the degree of uncertainty in information from an adversary's perspective by

linking various pseudonyms of a vehicle during communication and the pseudonym changing process. This measures the level of privacy achieved or anonymisation of vehicles. Let V_x be a set of vehicles that may be taking part in the pseudonym changing procedure, and V_y is a set of vehicles that successfully changed pseudonyms. Let $P(_{V_x} \rightarrow_{V_y})$ be the probability of mapping the number of vehicles to the number of pseudonyms changed. The uniform probability of distribution evaluates the higher level of entropy and higher confusion for an adversary to identify the target vehicle. Consider the number of vehicles that have changed pseudonyms at time t; the entropy can be calculated as follows [12]:

$$H_t = \sum_{V_x, V_y \in V} P_{V_x} \rightarrow_{V_y} log_2 P_{V_x} \rightarrow_{V_y}. \tag{24}$$

where H_t is the entropy of vehicles anonymisation in the concerned area, and V is the total number of vehicles taking part in the pseudonym changing process. The average entropy can be calculated as follows:

$$H_{avg} = \frac{1}{V} \sum_{x,y \in V} H_t(x, y). \tag{25}$$

6.2.3. Vehicle Traceability

Traceability is another privacy metric that measures the tracking percentage of vehicles during a trip. It is inverse to the level of location privacy. It is the probability of an adversary determining the location spots of the vehicles. Let T_v be the tracing probability of an attacker itself, a measure of anonymity set. Traceability can be defined as given below [42]:

$$T_v = [1 - Pr(|ASS|)]. \tag{26}$$

Pr is the probability of vehicle anonymisation during the pseudonym change process. The value of T_v equal to 1 means that the adversary successfully tracked the target vehicle by linking its various pseudonym during various location spots. With increasing anonymisation, the traceability strength of an adversary reduces over time.

7. Performance Analysis

In this section, we analyze the proposed scheme's performance with the help of various experimental results. First, we discuss the performance of CMC under various traffic densities with the pseudonym update process. The proposed scheme CMC consists of both pseudonym change and exchange processes under diverse traffic conditions. We analyzed the anonymisation with the pseudonym change and exchange process as shown in Figure 10. During the pseudonym changing process, vehicles with high traffic density, i.e., have a higher number of neighbors in transmission range, the anonymisation of vehicles is improved. The pseudonym exchange process has lower anonymity due to fewer neighbors in transmission range. Depending on the process of pseudonyms update under various vehicle traffic conditions, the vehicle identity anonymisation is certainly different. A higher number of vehicles in a region that can change pseudonyms cooperatively will improve identity protection. Figure 11 shows the number of pseudonyms updated for various vehicle densities. We take two traffic densities. The lower traffic density case contains fewer vehicles in a road region, while higher density means a higher number of transmission range vehicles, as given in [52]. A higher number of vehicles taking part in the pseudonym update process increases identity protection. The figure clearly shows that a higher number of pseudonyms are updated during higher traffic conditions, which improves the anonymity of a vehicle in the crowd.

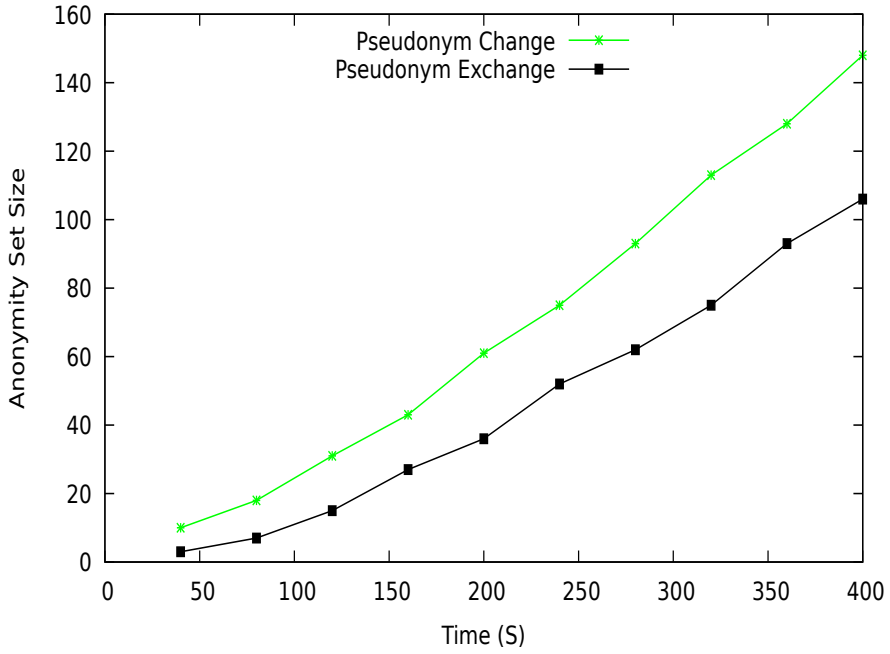

Figure 10. Anonymity of pseudonym change and exchange process.

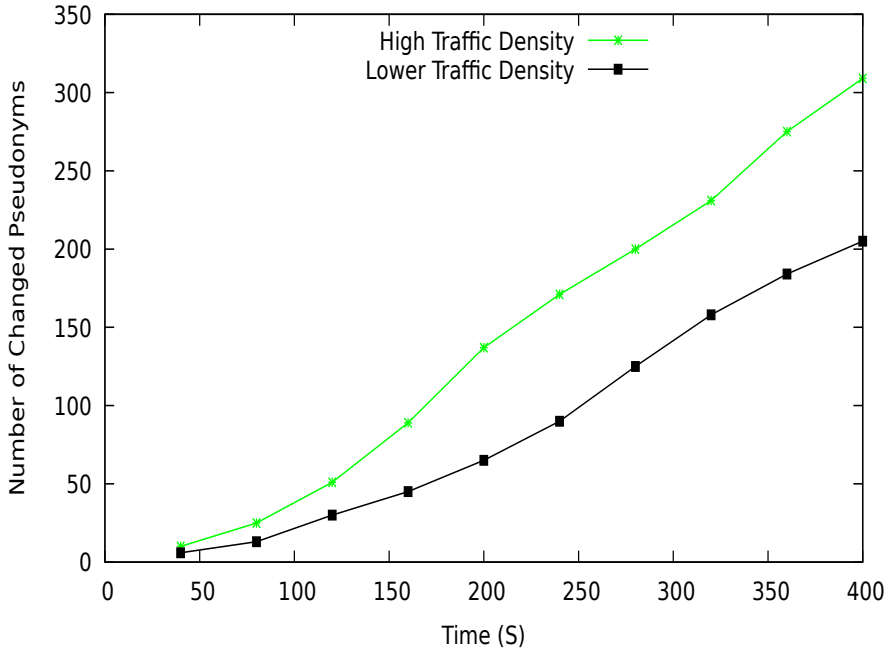

Figure 11. The number of pseudonyms updates at various vehicle densities.

8. Performance Comparison of CMC with Existing Schemes

The results of the proposed scheme CMC with existing schemes IndMZ [24] and TAPCS [25] in terms of ASS, entropy, and location traceability. The reason for choosing these two techniques is the similarity with our proposed scheme working with vehicle traffic conditions and used for privacy protection of vehicles in a road network environment. The values collected during simulations for anonymity set and entropy are given in Table 5. If a higher number of pseudonyms are changed by vehicles in a region, the target vehicle anonymisation is increased which ultimately increases entropy and confusion for an adversary to exploit the actual identity and location of a target vehicle. The location privacy scheme intends to create uncertainty in location information to generate confusion for an

adversary. Here, confusion means adding uncertainty in the vehicle location information for an adversary that makes it difficult to identify a vehicle by linking old pseudonyms with newly changed pseudonyms. The uncertainty can be produced by the proper pseudonyms changing process. The proposed scheme CMC improves entropy and increases confusion for an adversary when compared with existing schemes IndMZ [24] and TAPCS [25] as shown in the table. The average ASS is evaluated based on vehicle density and simulation time. Figures 12 and 13 show the proposed scheme's results in comparison to existing schemes for vehicle anonymisation. CMC improves vehicle anonymity over IndMZ and TAPCS. The reason behind this is the efficient management of vehicles that took part in the pseudonym update process. Initially, the anonymity is low due to a smaller number of transmission range vehicles. After some time, the anonymity of vehicles increases due to the successful change of pseudonyms. In Figure 13, the proposed scheme's behavior is slightly undulating due to the lack of vehicle interest in cooperation with neighbors in the region. However, the overall process moves towards improvement in the anonymisation of vehicles.

Table 5. Values collected during simulations.

Number of Vehicles	Number of Pseudonyms Changed	Entropy of ASS	Adversary Confusion
	CMC		
100	71	8	40%
200	169	14.7	70%
	TAPCS [25]		
100	51	6.5	32%
200	135	12.6	56%
	IndMZ [24]		
100	36	4.8	14%
200	111	11.2	37%

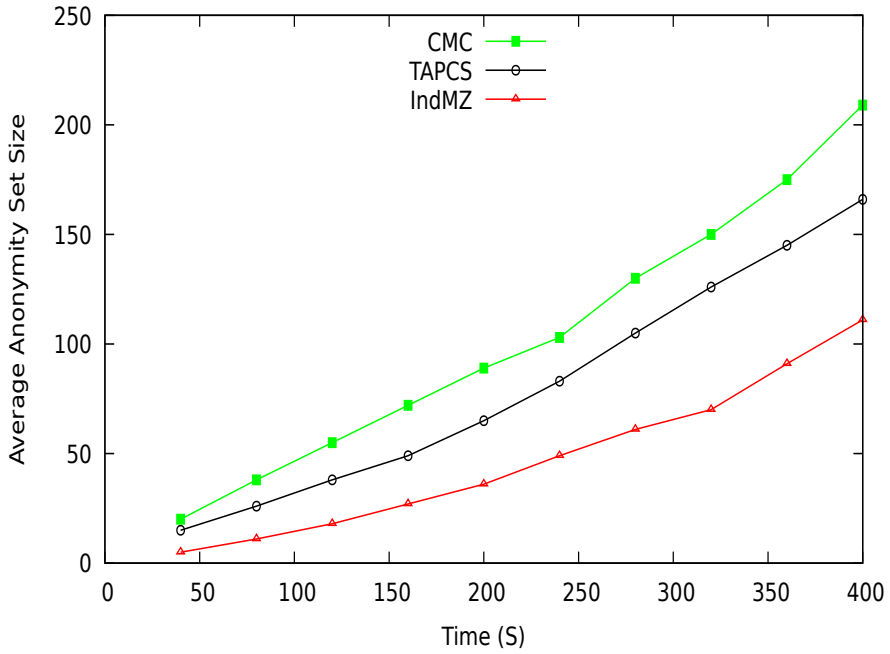

Figure 12. Average anonymity versus time.

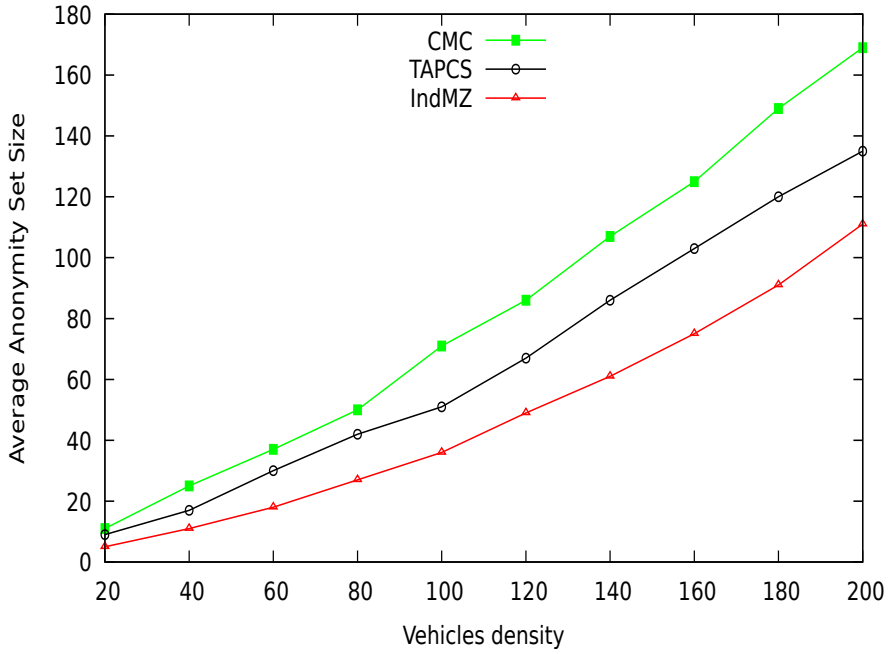

Figure 13. Anonymisation of vehicle identity at different vehicles' density.

Figure 14 shows the entropy of average anonymity set size at a certain time. The proposed scheme CMC beats the existing schemes TAPCS and IndMZ in terms of entropy. This shows the confusion generated concerning the target vehicle in the pseudonym updating process. CMC produces greater confusion than existing schemes for an adversary to find a target vehicle's actual identity in the communicating region. Ultimately, it improves the privacy protection level of vehicles. Similarly, in Figure 15, entropy is evaluated based on the number of vehicles took part in the pseudonym changing process. The entropy shows irregular behavior at different traffic densities; this is due to the lack of cooperation of vehicles in that region for the anonymisation process. CMC achieves higher confusion than TAPCS and IndMZ in various vehicle traffic. The achievement of the proposed CMC scheme regarding entropy is because of the efficient utilization of road context and pseudonym updating process. The IndMZ [24] generates fake pseudonyms in an individual manner and so the target vehicle can be easily identified by an adversary, which reduces the confusion level. The reduced performance of TAPCS compared with CMC regarding entropy is due to inefficient management of the pseudonym changing process in the silent period.

The vehicle tracking percentage during simulation time is shown in Figure 16. Initially, the proposed scheme CMC and TAPCS have similar tracking ratios at a certain amount of time. Over time, CMC reduces vehicle traceability for an adversary. The proposed scheme gets better results regarding reducing vehicle tracking probability compared with existing methods TAPCS [25] and IndMZ [24]. Similarly, tracking probability concerning the number of vehicles is shown in Figure 17. While there is a low number of vehicles at the start of the network, the tracking probability is also high. Whenever the number of vehicles is increasing, tracking probability is reduced to a certain level. CMC has a lower tracking percentage compared to existing schemes. The proposed scheme efficiently manages the road environment and makes use of any neighbor's cooperation in the pseudonym changing process, increasing the confusion for an adversary to track the pseudo-identities of vehicles.

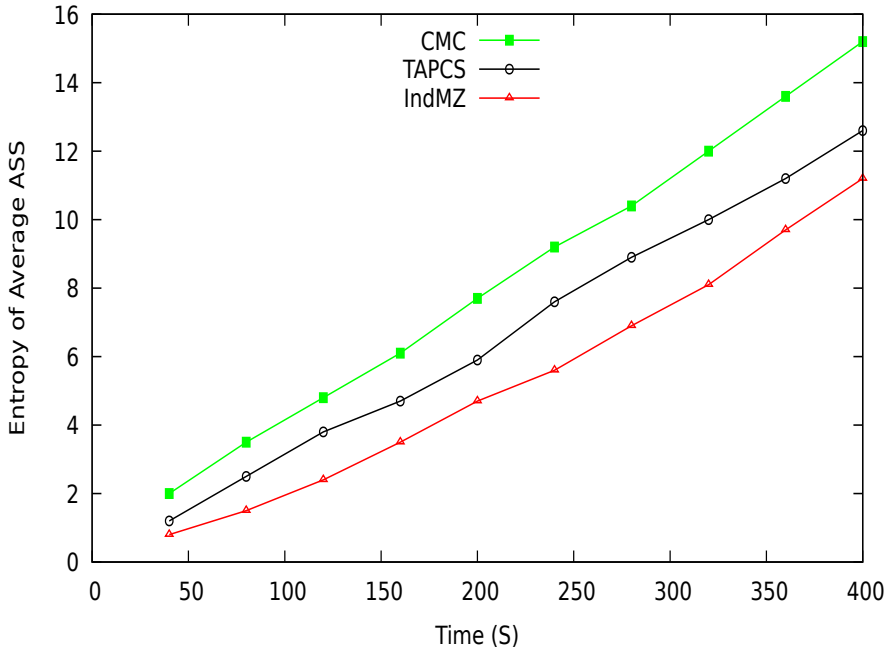

Figure 14. Entropy with different periods.

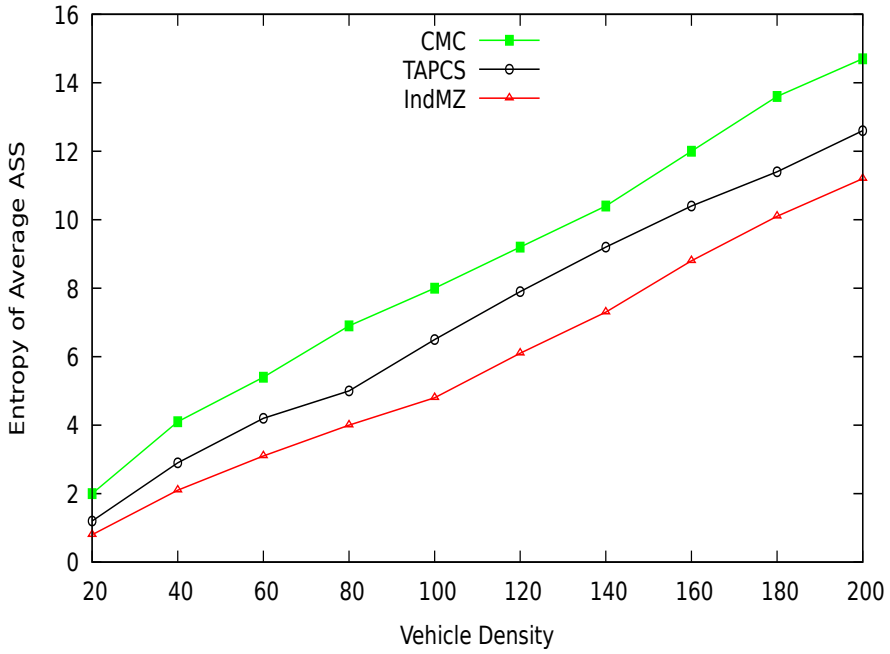

Figure 15. Entropy with different vehicle traffic density.

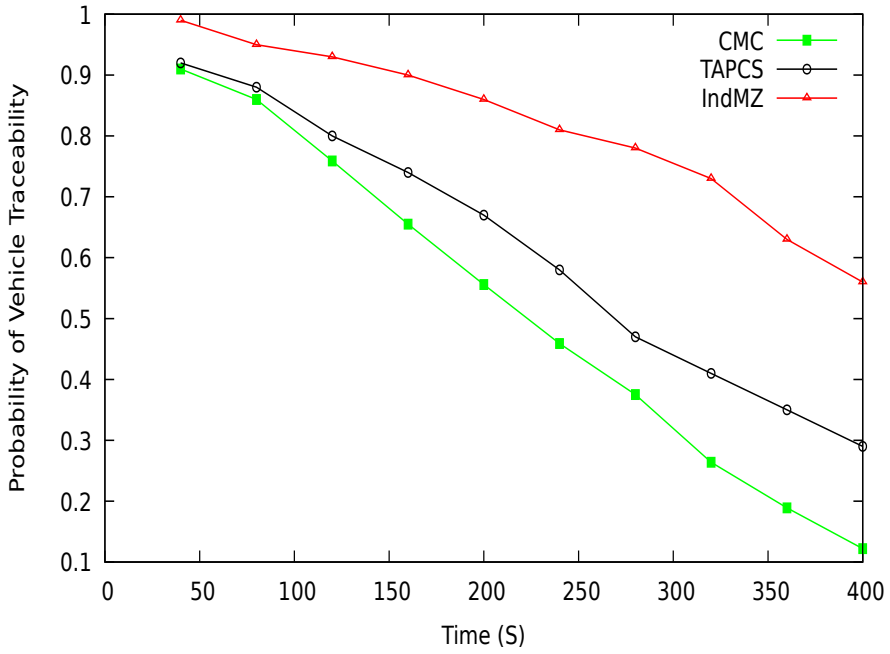

Figure 16. Vehicle tracing probability.

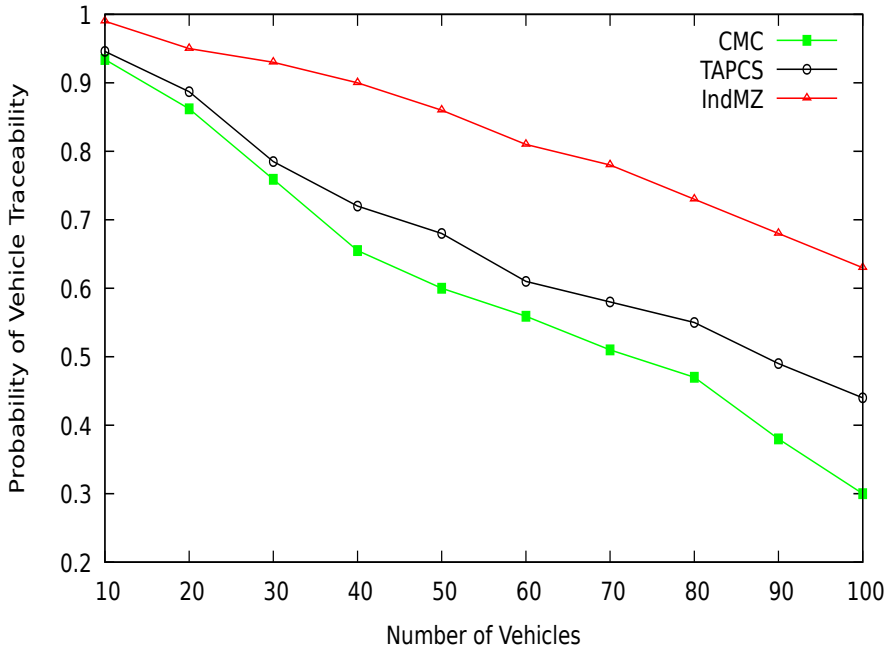

Figure 17. Tracking probability of the number of vehicles.

9. Analysis and Discussion

This section discusses the CMC's general security against GPA, the proposed scheme's impact, and its computation overhead. The details are given below.

9.1. Protection against GPA

The GPA can cover a large part of the network to capture beacon messages broadcast by vehicles. GPA analyzes the beacon messages for pseudo-identities of vehicles and matches them with old pseudonyms. If the adversary successfully matches these pseudonyms, then it can identify vehicles at various visited locations. Here, we examine the strength of GPA to extract the identity of a target vehicle. We investigate the strength of GPA with and without additional knowledge about a target vehicle. The additional information about the

target vehicle may be collected at some road intersections or frequently visited locations. The information may be vehicle frequently visited roads, old pseudonyms, and location of interest. Based on this information, the adversary tries to match the pseudonyms of a target vehicle at the earlier locations with pseudonyms changed at the new visited locations. This knowledge improves an adversary's strength to identify a target, which may be used for matching vehicle pseudonyms. Figure 18 shows the average confusion per trace of GPA with and without additional knowledge. The GPA with additional knowledge has lower confusion in identifying a vehicle, and without additional knowledge, confusion is increasing at a higher rate. Our proposed scheme CMC increases an adversary's confusion with additional information because it efficiently mixes the vehicle context under diverse traffic conditions. Similarly, Figure 19 shows the confusion for both GPA with and without additional knowledge under different vehicle traffic densities. The increasing number of vehicles improves the average confusion rate for the GPA. Eventually, it increases the protection level of the location privacy of a target vehicle.

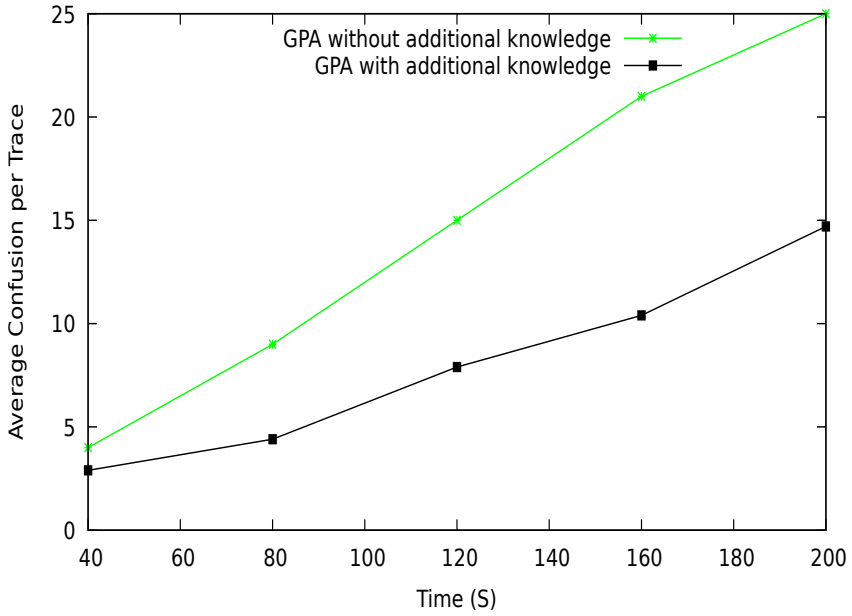

Figure 18. Adversary confusion for vehicle traces.

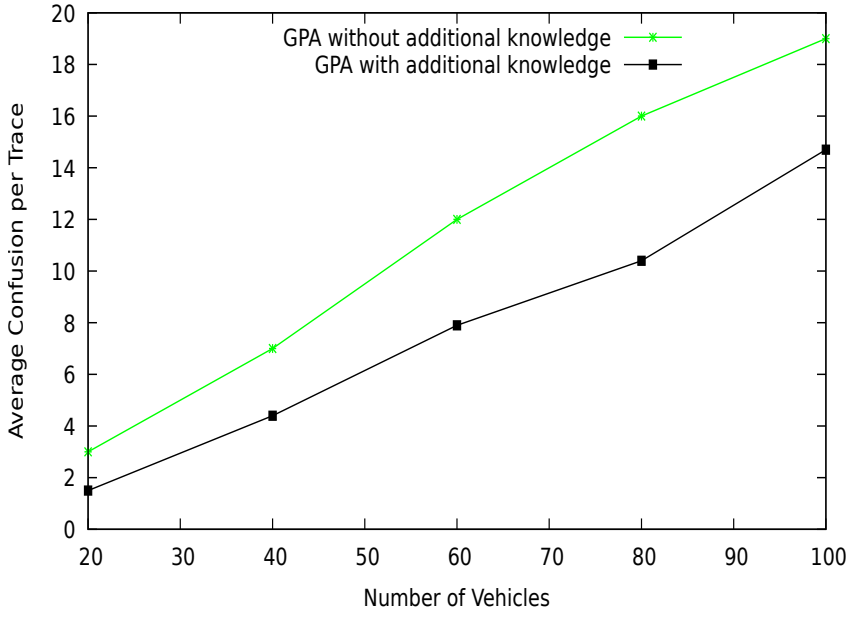

Figure 19. Adversary confusion with a different number of vehicles.

9.2. Impact on VANETs Applications

We analyze the impact of location privacy scheme on the vehicular network applications that may be safety-related and comfort applications. Achieving a higher level of privacy certainly will need to reduce its impact on road network applications. However, dummy data or wrong information is disseminated in the network for anonymizing a vehicle, which significantly reduces the application services of the vehicular network. Supposing inaccurate information is circulated, how would the vehicles efficiently utilize the applications of VANETs? The existing scheme IndMZ [24] takes the help of fake pseudonyms to anonymize the vehicles. This scheme falls into two problems. The first one is the computation burden on the vehicles. Secondly, it affects safety applications. The generation of fake pseudonyms for anonymisation reduces the application service quality. A large number of fake pseudonyms may also suffer communication among vehicles. The TAPCS [25] scheme is based on the radio silence period to preserve vehicles' location privacy. The use of silence periods during communication networks such as in VANETs is dangerous for vehicles' safety. During silent modes, mobile nodes do not broadcast road network information such as emergency, accident, the danger of lane changing, etc., and how the other vehicles will know about the road status information at a certain period. Safety application is critical, and delays in information dissemination compromise driver safety on the road. Thus, the TAPCS has a higher impact on road safety applications than the proposed scheme CMC. There is no concept of a silent period and generation of fake pseudonyms in our scheme CMC that impact road safety and comfort application. CMC disseminates road status information on a timely basis and utilizes road context information for vehicle anonymisation. CMC reduces privacy impact on safety applications compared with IndMZ and TAPCS.

9.3. Computation Overhead

The vehicle computation time for the pseudonyms changing process is analyzed in this section. Figure 20 shows the average computation time of the proposed scheme CMC using number of neighbors in the transmission range. A higher number of transmission range neighbors will take more time to compute the pseudonyms changing process as compared to lower transmission range neighbors. At the start of the simulation, there is a lower number of transmission range neighbors and a lower computation burden on the vehicles for the pseudonym changing process. The proposed scheme's average computation cost is compared with TAPCS [25] and IndMZ [24], as in Figure 21. The CMC creates a lower computation overhead than existing schemes. This is because of the utilization of road context information and pseudonym changing process for vehicle anonymisation. IndMZ scheme produces a much higher computation cost due to the generation of fake pseudonyms in larger quantities. The TAPCS generates a lower cost of computation than IndMZ by utilizing the vehicle traffic conditions in the road environment, although the proposed scheme CMC has a lower computation overhead as compared with the existing scheme. However, this overhead can be reduced further to optimize the computation and communication time of vehicles by applying a privacy scheme.

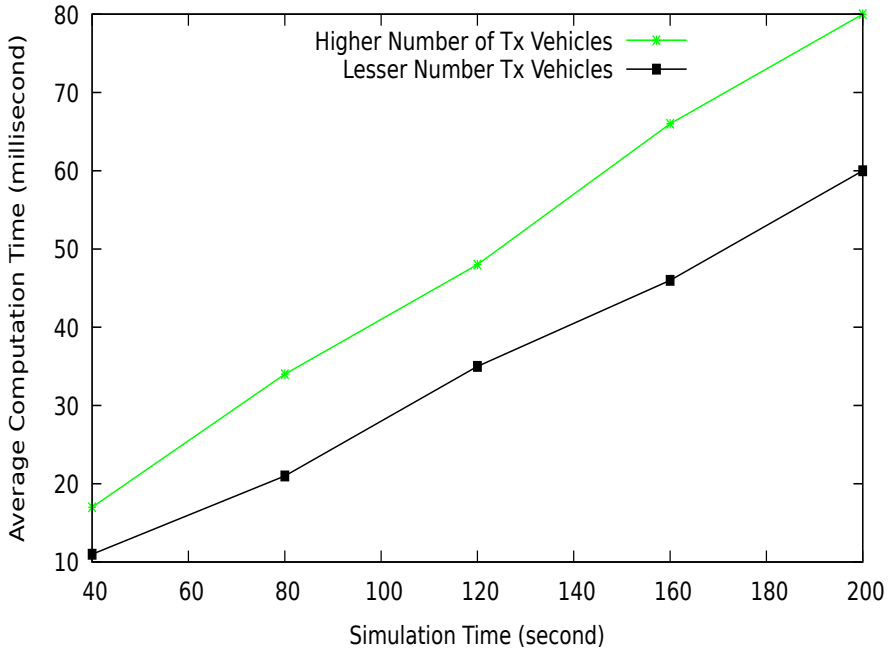

Figure 20. CMC computation overhead for the pseudonyms' changing process.

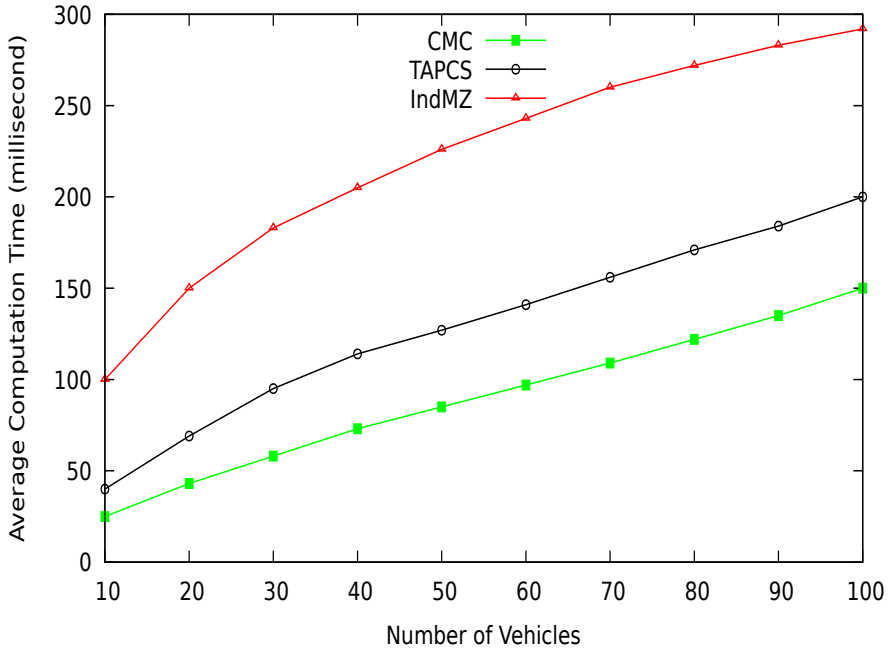

Figure 21. Average computation cost with a various number of vehicles.

9.4. Privacy and Traffic Optimization

The majority of the research conducted for location privacy protection in VANETs is based on the pseudonyms' changing process. The design of the privacy scheme may have an impact on the performance of other fields of the VANETs. One consideration is the impact on communication protocols, high frequency of changing pseudonym improves privacy but creates complications for the routing protocols. It degrades the performance of communication protocols that may impact the packet delivery ratio. The impact of the pseudonym changing process discussed in [67] on the packet delivery ratio is as follows: if vehicles (nodes) change their pseudonyms after every five seconds, the packet delivery ratio is about 60% to the destination. If pseudonyms are changed after every

10 s, the successful packet delivery ratio is about above 75%, while increasing duration to 30 s successful delivery ratio becomes above 85%. However, the increasing duration for pseudonym changes will reduce the level of privacy. Thus, there should be a reasonable balance between privacy protection and traffic optimization.

10. Conclusions

This paper takes on the problem of location privacy in a vehicular network. We have proposed a new Crowd-based Mix Context (CMC) scheme for location privacy preservation in the vehicular network. CMC employs vehicle speed, direction, and traffic density for the pseudonym changing process. Based on these parameters, the vehicles update pseudonyms simultaneously, which creates confusion for an adversary to break the pseudonyms of vehicles at different location spots. We formally model and analyze the proposed scheme using HLPN. The evaluation results show that CMC improves the anonymisation of vehicles compared with existing schemes IndMZ and TAPCS at various traffic densities. This prevents the adversary from linking pseudonyms of vehicles and identifies a target vehicle in the road region. The proposed scheme reduced the computation burden on vehicles for generating fake pseudonyms in the existing methods. The CMC also minimizes the impact of anonymisation on safety applications by managing road context information. In the future, we are eager to do more experiments on the vehicle high speed and low traffic density and will determine a robust privacy preservation method in such a dynamic road network condition.

Author Contributions: Conceptualization, I.U. and M.A.S.; methodology, A.K.; software, I.U.; validation, A.W., M.A.S., G.J. and A.K.; formal analysis, I.U., G.J. and A.W.; investigation, C.M.; resources, C.M.; data curation, A.K.; writing—original draft preparation, I.U.; writing—review and editing, M.A.S., G.J. and A.W.; visualization, G.J., I.U. and A.W.; supervision, M.A.S.; project administration, A.K. and C.M.; funding acquisition, C.M. All authors have read and agreed to the published version of the manuscript.

Funding: Ikram Ullah wants to thank the Higher Education Commission Pakistan for supporting PhD studies. Maple would like to acknowledge the support of UKRI through the grants EP/R007195/1 (Academic Centre of Excellence in Cyber Security Research—University of Warwick), EP/N510129/1 (The Alan Turing Institute), EP/R029563/1 (Autotrust), and EP/S035362/1 (PETRAS, the National Centre of Excellence for IoT Systems Cybersecurity).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: Thanks to Higher Education Commission, Pakistan for supporting academic studies.

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

References

1. Cunha, F.; Villas, L.; Boukerche, A.; Maia, G.; Viana, A.; Mini, R.A.; Loureiro, A.A. Data communication in VANETs: Protocols, applications and challenges. *Ad Hoc Netw.* **2016**, *44*, 90–103. [CrossRef]
2. Liang, W.; Li, Z.; Zhang, H.; Wang, S.; Bie, R. Vehicular ad hoc networks: Architectures, research issues, methodologies, challenges, and trends. *Int. J. Distrib. Sens. Netw.* **2015**, *11*, 745303. [CrossRef]
3. Cunha, F.D.D.; Boukerche, Z.; Villas, L.; Viana, A.C.; Loureiro, A.A.F. *Data Communication in VANETs: A Survey, Challenges and Applications*; [Research Report] RR-8498; INRIA Saclay: Palaiseau, France, 2014; pp. 1–26.
4. Qu, F.; Wu, Z.; Wang, F.Y.; Cho, W. A security and privacy review of VANETs. *IEEE Trans. Intell. Transp. Syst.* **2015**, *16*, 2985–2996. [CrossRef]
5. Engoulou, R.G.; Bellaïche, M.; Pierre, S.; Quintero, A. VANET security surveys. *Comput. Commun.* **2014**, *44*, 1–13. [CrossRef]
6. Omar, H.A.; Lu, N.; Zhuang, W. Wireless access technologies for vehicular network safety applications. *IEEE Netw.* **2016**, *30*, 22–26. [CrossRef]
7. Al-Sultan, S.; Al-Doori, M.M.; Al-Bayatti, A.H.; Zedan, H. A comprehensive survey on vehicular Ad Hoc network. *J. Netw. Comput. Appl.* **2014**, *37*, 380–392. [CrossRef]

8. Kenney, J.B. Dedicated short-range communications (DSRC) standards in the United States. *Proc. IEEE* **2011**, *99*, 1162–1182. [CrossRef]
9. Wang, S.; Yao, N.; Gong, N.; Gao, Z. A trigger-based pseudonym exchange scheme for location privacy preserving in VANETs. *Peer-to-Peer Netw. Appl.* **2018**, *11*, 548–560. [CrossRef]
10. Ullah, I.; Wahid, A.; Shah, M.A.; Waheed, A. VBPC: Velocity based pseudonym changing strategy to protect location privacy of vehicles in VANET. In Proceedings of the 2017 International Conference on Communication Technologies (Comtech), Rawalpindi, Pakistan, 19–21 April 2017; pp. 132–137.
11. Amro, B. Protecting Privacy in VANETs Using Mix Zones with Virtual Pseudonym Change. *Int. J. Netw. Secur. Its Appl.* **2018**, *10*, 11–21. [CrossRef]
12. Memon, I.; Chen, L.; Arain, Q.A.; Memon, H.; Chen, G. Pseudonym changing strategy with multiple mix zones for trajectory privacy protection in road networks. *Int. J. Commun. Syst.* **2018**, *31*, 1–44. [CrossRef]
13. 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 Trans. Veh. Technol.* **2011**, *61*, 86–96. [CrossRef]
14. Boualouache, A.; Senouci, S.M.; Moussaoui, S. Vlpz: The vehicular location privacy zone. *Procedia Comput. Sci.* **2016**, *83*, 369–376. [CrossRef]
15. Boualouache, A.; Moussaoui, S. Urban pseudonym changing strategy for location privacy in VANETs. *Int. J. Ad Hoc Ubiquitous Comput.* 2017, 24, 49–64. [CrossRef]
16. Ali, Q.; Zhongliang, A.; Imran, D. Location Privacy with Dynamic Pseudonym-Based Multiple Mix-Zones Generation over Road Networks. *Wirel. Pers. Commun.* **2017**, *97*, 3645–3671.
17. Yu, R.; Kang, J.; Huang, X.; Xie, S.; Zhang, Y.; Gjessing, S. MixGroup: Accumulative pseudonym exchanging for location privacy enhancement in vehicular social networks. *IEEE Trans. Dependable Secur. Comput.* **2015**, *13*, 93–105. [CrossRef]
18. Zhang, L. OTIBAAGKA: A new security tool for cryptographic mix-zone establishment in vehicular ad hoc networks. *IEEE Trans. Inf. Forensics Secur.* **2017**, *12*, 2998–3010 [CrossRef]
19. Mei, Y.; Jiang, G.; Zhang, W.; Cui, Y. A collaboratively hidden location privacy scheme for VANETs. *Int. J. Distrib. Sens. Netw.* **2014**, *10*, 473151. [CrossRef]
20. Wasef, A.; Shen, X.S. REP: Location privacy for VANETs using random encryption periods. *Mob. Netw. Appl.* **2010**, *15*, 172–185. [CrossRef]
21. Sampigethaya, K.; Huang, L.; Li, M.; Poovendran, R.; Matsuura, K.; Sezaki, K. *CARAVAN: Providing Location Privacy for VANET*; Department of Electrical Engineering, University of Washington: Seattle, WA, USA, 2005.
22. Khacheba, I.; Yagoubi, M.B.; Lagraa, N.; Lakas, A. Location privacy scheme for VANETs. In Proceedings of the 2017 International Conference on Selected Topics in Mobile and Wireless Networking (MoWNeT), Avignon, France, 17–19 May 2017; pp. 1–6.
23. Amro, B.; Saygin, Y.; Levi, A. Enhancing privacy in collaborative traffic-monitoring systems using autonomous location update. *IET Intell. Transp. Syst.* **2013**, *7*, 388–395. [CrossRef]
24. Guo, N.; Ma, L.; Gao, T. Independent Mix Zone for Location Privacy in Vehicular Networks. *IEEE Access* **2018**, *6*, 16842–16850. [CrossRef]
25. Boualouache, A.; Moussaoui, S. TAPCS: Traffic-aware pseudonym changing strategy for VANETs. *Peer-to-Peer Netw. Appl.* **2017**, *10*, 1008–1020. [CrossRef]
26. Zidani, F.; Semchedine, F.; Ayaida, M. Estimation of Neighbors Position privacy scheme with an Adaptive Beaconing approach for location privacy in VANETs. *Comput. Electr. Eng.* **2018**, *71*, 359–371. [CrossRef]
27. Sampigethaya, K.; Li, M.; Huang, L.; Poovendran, R. AMOEBA: Robust location privacy scheme for VANET. *IEEE J. Sel. Areas Commun.* **2007**, *25*, 1569–1589. [CrossRef]
28. Buttyán, L.; Holczer, T.; Weimerskirch, A.; Whyte, W. Slow: A practical pseudonym changing scheme for location privacy in vanets. In Proceedings of the 2009 IEEE Vehicular Networking Conference (VNC), Tokyo, Japan, 28–30 October 2009; pp. 1–8.
29. Wei, Y.-C.; Chen, Y.-M. Safe Distance Based Location Privacy in Vehicular Networks. In Proceedings of the 2010 IEEE 71st Vehicular Technology Conference, Taipei, Taiwan, 16–19 May 2010; pp. 1–5.
30. Emara, K.; Woerndl, W.; Schlichter, J. CAPS: Context-aware Privacy Scheme for VANET Safety Applications. In Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks, New York, NY, USA, 22–26 June 2015; pp. 21:1–21:12.
31. Khacheba, I.; Yagoubi, M.B.; Lagraa, N.; Lakas, A. CLPS: Context-based location privacy scheme for VANETs. *Int. J. Ad Hoc Ubiquitous Comput.* **2018**, *29*, 141–159. [CrossRef]
32. Singh, P.K.; Gowtham, S.N.; Tamilselvan, S.; Nandi, S. CPESP: Cooperative pseudonym exchange and scheme permutation to preserve location privacy in VANETs. *Veh. Commun.* **2019**, *20*, 100183. [CrossRef]
33. Arain, Q.A.; Memon, I.; Deng, Z.; Memon, M.H.; Mangi, F.A.; Zubedi, A. Location monitoring approach: Multiple mix-zones with location privacy protection based on traffic flow over road networks. *Multimed. Tools Appl.* **2018**, *77*, 5563–5607. [CrossRef]
34. Deng, X.; Xin, X.; Gao, T. A location privacy protection scheme based on random encryption period for VSNs. *J. Ambient. Intell. Humaniz. Comput.* **2020**, *11*, 1351–1359. [CrossRef]
35. Weerasinghe, H.; Fu, H.; Leng, S.; Zhu, Y. Enhancing unlinkability in vehicular ad hoc networks. In Proceedings of the 2011 IEEE International Conference on Intelligence and Security Informatics, Beijing, China, 10–12 July 2011.

36. Ni, J.; Lin, X.; Shen, X. Privacy-preserving data forwarding in VANETs: A personal-social behavior based approach. In Proceedings of the GLOBECOM 2017—2017 IEEE Global Communications Conference, Singapore, 4–8 December 2017; pp. 1–6.
37. Huanguo, Z.; Yi, M. *A Privacy Protection Scheme in VANETs Based on Group Signature*; Springer: Singapore, 2019; Volume 10.
38. Ullah, I.; Shah, M.A.; Khan, A.; Maple, C.; Waheed, A. Virtual Pseudonym-Changing and Dynamic Grouping Policy for Privacy Preservation in VANETs. *Sensors* **2021**, *21*, 3077. [CrossRef] [PubMed]
39. Hoh, B.; Gruteser, M. Protecting location privacy through path confusion. In Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05), Athens, Greece, 5–9 September 2005; pp. 194–205.
40. Karim, E. Location privacy in vehicular networks. In Proceedings of the 2013 IEEE 14th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM), Madrid, Spain, 4–7 June 2013.
41. Chaudhary, B.; Singh, K. A Dummy Location Generation Model for Location Privacy in Vehicular Ad hoc Networks. In Proceedings of the International Conference on Innovative Computing and Communications, New Delhi, India, 20–21 February 2021; Springer, Singapore, 2021; pp. 1–10.
42. Cui, J.; Wen, J.; Han, S.; Zhong, H. Efficient Privacy-preserving Scheme for Real-time Location Data in Vehicular Ad-hoc Network. *IEEE Internet Things J.* **2018**, *4662*, 1–8. [CrossRef]
43. Yu, H.; Li, G.; Wu, J.; Ren, X.; Cao, J. A location-based path privacy protection scheme in internet of vehicles. In Proceedings of the IEEE INFOCOM 2020—IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Toronto, ON, Canada, 6–9 July 2020; pp. 665–670.
44. Zhong, H.; Ni, J.; Cui, J.; Zhang, J.; Liu, L. Personalized Location Privacy Protection Based on Vehicle Movement Regularity in Vehicular Networks. *IEEE Syst. J.* **2021**. [CrossRef]
45. Ullah, I.; Shah, M.A.; Khan, A.; Jeon, G. Privacy-preserving multilevel obfuscation scheme for vehicular network. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4204. [CrossRef]
46. Chen, Z.; Bao, X.; Ying, Z.; Liu, X.; Zhong, H. Differentially private location protection with continuous time stamps for VANETs. In Proceedings of the International Conference on Algorithms and Architectures for Parallel Processing, Guangzhou, China, 15–17 November 2018; Springer: Cham, Switzerland, 2018.
47. Wang, W.; Min, M.; Xiao, L.; Chen, Y.; Dai, H. Protecting Semantic Trajectory Privacy for VANET with Reinforcement Learning. In Proceedings of the ICC 2019–2019 IEEE International Conference on Communications (ICC), Shanghai, China, 20–24 May 2019; pp. 1–5.
48. Benarous, L.; Kadri, B.; Boudjit, S. Alloyed Pseudonym Change Strategy for Location Privacy in VANETs. In Proceedings of the 2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 10–13 January 2020; pp. 1–6.
49. Chen, Y.; Lo, T.; Lee, C.; Pang, A. Efficient Pseudonym Changing Schemes for Location Privacy Protection in VANETs. In Proceedings of the 2013 International Conference on Connected Vehicles and Expo (ICCVE), Las Vegas, NV, USA, 2–6 December 2013; pp. 937–938.
50. Corser, G.; Fu, H.; Shu, T. Endpoint Protection Zone (EPZ): Protecting LBS User Location Privacy Against Deanonymisation and Collusion in Vehicular Networks. In Proceedings of the 2013 International Conference on Connected Vehicles and Expo (ICCVE), Las Vegas, NV, USA, 2–6 December 2013; pp. 369–374.
51. Corser, G.; Fu, H.; Shu, T.; D'Errico, P.; Ma, W.; Leng, S.; Zhu, Y. Privacy-by-decoy: Protecting location privacy against collusion and deanonymisation in vehicular location based services. In Proceedings of the 2014 IEEE Intelligent Vehicles Symposium Proceedings, Dearborn, MI, USA, 8–11 June 2014; pp. 1030–1036.
52. Gerlach, M.; Felix, G. Privacy in VANETs using Changing Pseudonyms—Ideal and Real. In Proceedings of the IEEE 65th Vehicular Technology Conference-VTC2007-Spring, Dublin, Ireland, 22–25 April 2007; pp. 2521–2525.
53. Freudiger, J.; Raya, M.; Félegyházi, M.; Papadimitratos, P.; Hubaux, J.-P. Mix-Zones for Location Privacy in Vehicular Networks. In Proceedings of the Association for Computing Machinery (ACM) Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS), Vancouver, BC, Canada, 14–17 August 2007; Volume 51, pp. 1–7.
54. Carianha, A.M.; Barreto, L.P.; Lima, G. Improving Location Privacy in Mix-Zones for VANETs. In Proceedings of the 30th IEEE International Performance Computing and Communications Conference, Orlando, FL, USA, 17–19 November 2011; pp. 1–6.
55. Ying, B.; Makrakis, D.; Mouftah, H.T. Dynamic mix-zone for location privacy in vehicular networks. *IEEE Commun. Lett.* **2013**, *17*, 1524–1527. [CrossRef]
56. Ying, B. Pseudonym Changes Scheme based on Candidate- Location-List in Vehicular Networks. In Proceedings of the 2015 IEEE International Conference on Communications (ICC), London, UK, 8–12 June 2015; pp. 7292–7297.
57. Boualouache, A.; Moussaoui, S. S2si: A practical pseudonym changing strategy for location privacy in vanets. In Proceedings of the 2014 International Conference on Advanced Networking Distributed Systems and Applications, Bejaia, Algeria, 17–19 June 2014; pp. 70–75.
58. Ying, B.; Makrakis, D.; Hou, Z. Motivation for protecting selfish vehicles' location privacy in vehicular networks. *IEEE Trans. Veh. Technol.* **2015**, *64*, 5631–5641. [CrossRef]
59. Bidi, Y.; Makrakis, D. Reputation-based Pseudonym Change for Location Privacy in Vehicular Networks. In Proceedings of the 2015 IEEE International Conference on Communications (ICC), London, UK, 8–12 June 2015; pp. 7041–7046.

60. Boualouache, A.; Senouci, S.; Moussaoui, S. Towards an Effi cient Pseudonym Management and Changing Scheme for Vehicular Ad-Hoc Networks. In Proceedings of the 2016 IEEE Global Communications Conference (GLOBECOM), Washington, DC, USA, 4–8 December 2016; pp. 1–7.
61. Zuberi, R.S.; Ahmad, S.N. Secure Mix-Zones for Privacy Protection of Road Network Location Based Services Users. *J. Comput. Netw. Commun.* **2016**, *2016*. [CrossRef]
62. Guo, N.; Ma, L.; Gao, T. A Location Privacy-Preserving Scheme for VANETs Based on Virtual Mix Zone. 2017; Volume 3, pp. 1–8.
63. Memon, I.; Mirza, H.T.; Arain, Q.A.; Memon, H. Multiple mix zones de-correlation trajectory privacy model for road network. *Telecommun. Syst.* **2019**, *70*, 557–582. [CrossRef]
64. Kalaiarasy, C.; Sreenath, N.; Amuthan, A. An effective variant ring signature-based pseudonym changing mechanism for privacy preservation in mixed zones of vehicular networks. *J. Ambient Intell. Humaniz. Comput.* **2020**, *11*, 1669–1681. [CrossRef]
65. Wahid, A.; Yasmeen, H.; Shah, M.A.; Alam, M. Holistic approach for coupling privacy with safety in VANETs. *Comput. Netw.* **2019**, *148*, 214–230. [CrossRef]
66. Sajjad, H.; Kanwal, T.; Anjum, A.; Malik, R. An efficient privacy preserving protocol for. *Comput. Secur.* **2019**, *86*, 358–371. [CrossRef]
67. Schoch, E.; Kargl, F.; Leinmüller, T.; Schlott, S.; Papadimitratos, P. Impact of pseudonym changes on geographic routing in vanets. In *European Workshop on Security in Ad-Hoc and Sensor Networks*; Springer: Berlin/Heidelberg, Germany, 2006; pp. 43–57.