A Comprehensive Review of Pseudonym Changing Strategies in Vehicular Networks

Ikjot Saini, Sherif Saad, and Arunita Jaekel
(Corresponding author: Sherif Saad)

Department of Computer Science, University of Windsor
401 Sunset Ave, Windsor, ON N9B 3P4, Canada
(Email: saini11s, shsaad, arunita@uwindsor.ca)
(Received Apr. 28, 2018; Revised and Accepted Aug. 18, 2018; First Online June 5, 2019)

Abstract

The area of location privacy in VANET is getting more attention after the emergence of V2X technologies. As the security and privacy are important for the customer's safety, the vehicles equipped with V2X technology must have strong techniques to preserve the security and privacy. Pseudonymous authentication proves to satisfy these requirements. The pseudonyms used in this process are subjected to change frequently as the using same pseudonym can be used for tracking the vehicle. Therefore, the pseudonym changing strategies are required for the unlinkability of a pseudonym, untraceability of the vehicle and higher location privacy. In this survey, we examine and discuss the general pseudonym authentication, the requirements, security threats, attack models, privacy metrics and provide a detailed analytical review of pseudonym changing strategies. It gives extensive classification of the strategies with a comparison based on various parameters which will help in understanding the current state of research and will also serve researchers to address the weaknesses of these schemes. This survey reviews the current state of the research for pseudonym changing strategies for improving location privacy and identifies the research gaps and states the open research problems for the future work.

Keyword: Anonymity; Location Privacy; Pseudonym Authentication; Pseudonym Changing Scheme; Untraceability; Unlinkability; V2X Communication; VANET

1 Introduction

Vehicular Ad Hoc Networks (VANET) has received a lot of attention in recent years from automotive industry and research community. The primary focus of VANET is on the road safety and the traffic management. The communication among vehicles and infrastructure enables various applications for safety, infotainment, and traffic management. The communication can be carried out as Vehicle to Infrastructure (V2I) and Vehicle to Vehicle (V2V). The communication of the vehicle with the infrastructure is used for non safety commercial applications such as toll collection, location based services and announcements. The cooperative communication among vehicles involves the Basic Safety Message (BSM), which broadcasts beacons over the control channel of DSRC every 10 milliseconds for safety applications. This message contains the information of the current state of the vehicle including the location, location accuracy, speed, direction, steering wheel angle, vehicle size, brake system status and other identifiers. This set of information gives the detailed mobility pattern of the driver. The eavesdropping attacker can potentially analyze the frequently visited locations, driving behavior, and can track the driver in real time which could be fatal in criminal cases. Therefore, the safety message broadcast directly impacts the privacy of the driver.

Anonymous communication can protect the sensitive information of the driver. It does not use the real identity of the sender for the authentication and verification of the safety message. However, the authorities must be able to recover the real identity of the misbehaving vehicle from its temporary identity which is important for the accountability. Hence, the privacy can be maintained conditionally, where the anonymous communication is limited to the vehicles and the authorities are still able to track the vehicles. Again, there can be an attack on the authorities or the authorities may be involved in eavesdropping attack. In such condition, there is a requirement of the conditional privacy with the anonymous authentication of the safety message and distribution of the trust among the authorities rather than completely trusting one centralized authority.

2 General Pseudonym Lifecycle

The general life cycle of the pseudonym in the context of the vehicular environment involves pseudonym issuance, pseudonym usage, pseudonym change, pseudonym resolution and pseudonym revocation. These five phases are

interdependent and affect the functioning of each other. The description of each phase is as follows:

Pseudonym Issuance: The real identity of the vehicle is the vehicle ID (VID) and it is provided by the department of motor vehicles when the vehicle is registered. VID is securely stored in the On Board Unit of the vehicle. VID is the signed certificate which provides unique identification of the vehicle. This identity is associated with information of the driver and the vehicle.Therefore, the driver does not want to reveal VID and pseudonyms are used to preserve privacy. VID is used to authenticate the valid vehicle and after successful authentication, the vehicle can participate in the vehicular network. For the pseudonym issuance process, a Trusted Authority (TA) is responsible. This Trusted Authority can be a Certificate Authority (CA) or Pseudonym Provider (PP).

Pseudonym Usage: The vehicle authenticates the message by using the pseudonym signed by Certificate Authority and the receiver verifies the message and checks that if the sender is a legitimate vehicle. The pseudonym should not be revoked or expired. The verification of the pseudonym is done locally and most of the schemes allow the certificate attachment with the message. This certificate ensures that the vehicle is legitimate and the pseudonym used by the sender is authentic. The verification process imposes a problem for the vehicles. The number of verification exponentially increases than the number of authentication, as the received messages will be more than the number of messages sent. Hence, the efficiency of the real time applications may be compromised.

Pseudonym Change: The vehicle must not possess a single pseudonym because it leverages tracking in long term and opens the attack surface for information gathering and various security attacks. Also, a single vehicle can not change its pseudonym because it does not prevent the tracking [32]. An adversary can easily notice that only one pseudonym is different and this change becomes obvious which allows linkability. The old and new pseudonyms associated with a vehicle are linkable based on the location, movement, actions and other parameters in the communication stack. The frequency, place, time and situation for changing the pseudonym are the open research issues [7].

Pseudonym Resolution: During the security attack and accidents, the authorities need the real identity of the vehicle as pseudonym is used for anonymity. Thus, the trusted authority like Certificate Authority holds the resolution information and can provide it to law enforcement representatives when requested. This process works as the database lookup which should also be strictly secured.

Pseudonym Revocation: The misbehaving vehicle should be revoked and prohibited to participate in the vehicular communications [25]. Here, the revocation refers to the invalidation of the pseudonym associated with the faulty vehicle. Most of the existing schemes revoke only one pseudonym of the vehicle which is known to LEA at that time, therefore, other pseudonyms associated with the vehicle can still allow the vehicle to participate [19, 25]. In order to revoke all the pseudonyms of the vehicle, VID of the vehicle should be revoked with further denial of refills. This scheme also allows participation of the vehicle until the vehicle has the pseudonyms. Thus, the effective pseudonym revocation is an open issue.

3 Classification of Pseudonym Changing Strategies

3.1 Mix Zone

The mix zone is an unobserved zone where the vehicles can not be eavesdropped due to radio silence and mix in such a way that after leaving the mix zone they are indistinguishable. In 2003, Beresford [2] introduced this concept in the context of pervasive computing. In order to understand mix zone, assume that the attacker has installed the radio receivers at specific points on the road. Now, the attacker can listen to the network communication, especially, the broadcasting beacons which contains sufficient information to know the movement of the vehicle and the driving behavior. This knowledge can help an attacker in prediction when the identifiers are changed and the vehicles are having different pseudonyms.

3.1.1 General Mix Zone Schemes

In 2007, Buttyan [7] introduced the first idea of using mix zone in context of the vehicular networks. The mix zone is the area which is not controlled by the adversary and the pseudonyms can be changed without eavesdropping of the attacker. This provides unlinkability of the pseudonyms enabling location privacy. Buttyan evaluated the effectiveness of this kind of mix zone by using the success probability with Bayesian decision algorithm. The success probability is the successfully mapped vehicles from the number of vehicles in mix zone. The author emphasizes on the minimum error probability which is provided by Bayesian decision algorithm. The simulations on MOVE and SUMO results show that higher success probability can be obtained with a stronger adversary. In addition, there is a saturation of success probability at 60 percent due to changing mobility patterns at junctions with half of controlled junctions. In other words, if 50 percent of the intersections are compromised, then there is 60 percent of success probability of the linking pseudonyms.

Freudiger [12] proposed the first implementation of the mix zone in vehicular ad hoc networks in 2007. According to Freudiger, the intersections are the mix zones which have infrastructure like RSU that assist in the pseudonym change. Additionally, the vehicles within mix zones encrypt the safety messages with the symmetric key provided by the RSU. Therefore, this mix zone is also known as Cryptographic Mix Zone(CMIX). The CMIX protocol has three phases in its lifecycle, namely, key establishment, key forwarding, and key update. Also, it has mix zone and extended mix zone. The entropy and success ratio of the vehicles are used as the privacy metrics. By simulation on MATLAB, the Manhattan network is assessed with the highly dense vehicular network. As entropy is used for evaluation, the tracking depends on the traffic density and its delay characteristics. The success ratio is inverse to the entropy which indicates that with increasing entropy, an attacker would not be able to successfully link pseudonyms. The anonymity of the vehicle increases linearly while the success ratio of adversary becomes negligible. This approach does not prevent internal adversary and it is not scalable and adaptable.

Carianha [9] addresses the vulnerability in the CMIX protocol and proposed an effective approach that mitigates the risk. CMIX has encryption with the mix zone and the shared key is available to the participating vehicles. This increases the risk associated with the internal adversary who is authenticated for the vehicular network and therefore can have the shared key. The proposed scheme consists of a status forwarding scheme limited to the neighbors and two of the overhead compensation strategies. The evaluation of the given scheme is carried out on OMNET, SUMO, and Veins based on the success rate. The results show that the success rate directly proportional to the number of vehicles in the mix zone. As this scheme extends CMIX, it has a limitation of fixed mix zone because vehicles may or may not pass through such mix zone.

OTIBAAGKA is the strategy to eliminate the use of fully trusted authorities in the vehicular networks proposed by Zhang [35]. OTIBAAGKA stands for One Time Identity Based Authenticated Asymmetric Group Key Agreement. It is used to create CMIX while dealing with the potential security attacks. He also suggested the benefit of using group key rather than using shared key in CMIX. It makes the network more dynamic and diverse. Even the internal adversary can have access to a few vehicles in that group. Unlike other group schemes, it does not force the group to change the group key when a vehicle leaves. The results based on the simulation on NS2 shows the effectiveness of this scheme.

In 2011, Scheuer [28] proposed the idea of ProMix Zone(PMZ) that is the communication proxy in the mix zone. The intersections of highways and crossroads are the mix zones which have the infrastructure units dedicated for pseudonym change. These infrastructure units are proxies which are interconnected and have a pair of asymmetric keys with CA certificate. This proposal does

Table 1: General Mix Zone schemes

Author [ref]	Year	Key concept	Changing Strategy	Privacy metric	Problems	Evaluation method
Buttyan [7]	2007	First idea of Mix Zone in VANET	Intersection as Mix Zone	Success probability	Frequency of pseudonym change	Analysis, Simulation
Freudiger [12]	2007	First implementation of Mix Zone	Cryptographic Mix Zone (CMIX)	Entropy	prone to the internal adversary,Not scalable,Not adaptable	Simulation
Carianha [9]	2011	Eliminate risk of internal adversary in CMIX	Extended secure CMIX	Success rate	Vehicles must pass at least one mix zone	Simulation
Scheuer [28]	2011	Communication proxy in mix zone with asymmetric key encryption	ProMix Zone(PMZ)	Number of vehicles (Anonymity Set Size)	Bandwidth overhead caused by increased beacon size	Simulation
Boualouache [3]	2014	Silence and Swap	Signalized Intersection as Mix Zone	Entropy of Anonymity Set Size	Silence cause problem in safety applications and vehicle may not pass a mix zone	Analysis, Simulation
Zhang [35]	2017	Does not rely on fully trusted authorities, group key instead of shared key in CMIX	One Time Identity Based Authentication Asymmetric Group Key Agreement	Group Size (Anonymity Set Size)	Group key change and management	Simulation

Table 2: Dynamic user centric Mix Zone schemes

Author [ref]	Year	Key concept	Changing strategy	Privacy metric	Problems	Evaluation method
Lu [18]	2011	For city environment, scalable and adaptable	Social Spot as Mix Zone	Anonymity Set Size	Only applicable in dense scenarios	Analysis
Boualouache [5, 6]	2016	VLPZ, Prevent both linking attacks	Dedicated roadside infrastructure as Mix Zone	Anonymity Set Size	Every vehicle may not be able to visit such zone	Analysis, Simulation
Ying [34]	2013	DMLP, practical and simple to implement	Dynamic Mix Zone on demand of vehicle	Entropy of anonymity set size	Traffic density may not be enough to create mix zone	Analysis
Ying [33]	2015	Dynamic Mix Zone	Candidate Location List, defined timeslot for change	Anonymity Set Size and Success Rate	Sparse network	Analysis, Simulation
Arain [1]	2017	DPMM, use reported servers with RSU	Dynamic Pseudonym based on Multiple Mix zone (DPMM)	Delay and packet delivery ratio	No privacy evaluation for anonymization	Simulation

not involve the pseudonym distribution strategy. The simulation of PMZ on JAVA shows the results and dependencies. With the growing number of vehicles in PMZ, the performance increases. The problem may arise with the size of the beacon which then causes bandwidth overhead. But the author suggested that it can be resolved by using ECC. PMZ is scalable while its deployment is still fixed.

Boualouache [3] presented the idea of Silence and Swap at Signalized Intersection(S2SI) which would be the mix zone. The silence and swap are the two protocols which together form a mix zone. The silence protocol creates secure silent mix zone and swap protocol ensures the exchange of the pseudonyms within vehicles of that mix zone under a controlled RSU. The author argued that the radio silence in the mix zone has no effect on the safety. Unlike other mix zones, it exchanges the pseudonyms among vehicles rather than changing them for an individual vehicle. This might increase the confusion for the adversary as tracking become difficult but the communication stack parameters are not changed which can still enable the tracking. In addition to that, there is another problem which may result in no change of pseudonym. There is the moderate probability of a vehicle to not pass through such a signalized intersection that prevent the vehicle to change its pseudonym. The author evaluated the privacy based on the entropy of the anonymity set size and the success rate of the attacker. More privacy is offered with lesser success rate and higher entropy of anonymity set size. The entropy of anonymity set depends on the arrival rate. With small arrival rate, the number of vehicles at signalized intersection increases which increases entropy. The simulation on OMNET, SUMO and VEINS gives the comparative analysis of the CMIX and S2SI. According to the author, this scheme can avoid more than 60 percent of the signature verification as compared to CMIX strategy.

3.1.2 Dynamic User Centric Mix Zone

Lu [18] suggested a pseudonym changing scheme using mix zone where the social spot acts as mix zone. The social spots are the temporary aggregation places where many vehicles stop by for certain time period. The places can be the road intersection at a red light and parking lot in public places. The anonymity set size is the parameter for the evaluation of the privacy. In the small social spot, the anonymity would increase with the increase of anonymity set size. In other words, more of the vehicles at intersection changing pseudonyms simultaneously, more the anonymity provided. On the other hand, the large social spots provide more anonymity when the inter arrival time of the vehicles is less and the duration of the vehicle to stay in the mix zone is more. The author provided the analysis for the privacy provided by both the small and large social spots. Additionally, the numerical results are given for further validation. This scheme is effective in a city environment and it is scalable and adaptable. However, it does not support the sparse vehicular networks.

Boualouache [5, 6] introduced another mix zone concept with the existing roadside infrastructure which is dedicated to change the pseudonyms. The toll booth and gas stations are the examples of such mix zone as these places provide high traffic density which helps in increasing anonymity set size. The scheme is named as Vehicular Location Privacy Zone (VLPZ). By interrupting the continuous tracking for some time, the pseudonyms can be changed securely without eavesdropping. The author has given the analytical model for the proposed scheme and further supported with the numerical analysis. In [59], the simulation results are given based on a reputation mechanism. SUMO, OMNET++, and VEINS are used for the

simulation. The problem in this scheme can be caused by the silence provided within VLPZ which jeopardizes the safety communication to some extent. There is a need of balance of safety and privacy.

Ying [34] proposed a scheme which is user centric and simple to implement. Dynamic Mix-Zone for Location Privacy (DMLP) that enable the vehicle to create mix zone on demand based on the traffic statistics, privacy level required and predicted location of the vehicle. It is more adaptable, scalable and performs well in sparse networks. The messages in mix zone are encrypted. The analysis shows the entropy of the anonymity set size of the mix zone varies with changing network size. As the scheme is compared with DLP, the size of mix zone in DLP does not change but in case of DMLP, it changes and increases the location privacy.

Recently, Arain [1] proposed a pseudonym changing strategy which outperforms RPCLP, EPCS, and MODP, this technique is known as Dynamic Pseudonym based multiple mix zone (DPMM). It uses roadside infrastructure as RSU and a network of reported servers. The technique uses encryption and vehicle cooperation based on reputation techniques. On SUMO simulator, the delay characteristics and packet delivery ratio are measured and compared with the existing techniques. The outcome demonstrates the effectiveness of DMPP over RPCLP, MODP and EPCS.

3.1.3 Road Network Based Mix Zone

MobiMix is the idea presented by Palanisamy [20] in 2011 in context of the anonymization effectiveness and attack resilience. The author argues that the placement of rectangular mix zones in the road network are vulnerable and careful measures should be taken before its placement. Palanisamy also proposed a method for road network mix zone placement which provide location privacy. This method is evaluated on GTMobiSim with geographical maps on different scales. In addition, MobiMix offers high level of resilience to timing and transition attack. Later in 2012, the author recognizes two major vulnerabilities and evaluated the efficiency of the prevention measures [22]. The vulnerabilities are found in the user mobility which, in some manner, is restricted as well as the road network characteristics and temporal and spatial information. In 2013, Palanisamy [23] demonstrated the risks associated with the location privacy of the vehicles in the mix zones and how the location exposure can be restricted in order to prevent timing and transition attacks.

Liu [17] suggested the concept of using multiple mix zones to prevent the attacks based on the side information provided by the user. Majorly, the author gives a method to place the mix zone in such a manner that it reduces the privacy risks. The idea of multiple mix zones is effective in breaking the continuity of the tracking more frequently. Liu indicated three placement constraints of the mix zone and two of the heuristic algorithms for the placement. The constraints are related to cost and service, graph, and traffic. The scheme is analyzed based on the information entropy. The simulation analysis on CPLEX reveals that the traffic density increases the location privacy as there are more vehicles for finding the best match.

3.2 Mix Context

In order to mitigate the predictability of the node movement, there are a few approaches; Increasing the size of mix zone, increasing silent periods, and increasing the frequency of updates. But these may not be either feasible or safety effective when implemented in real world. In case of longer silent periods, the chances of accidents increase exponentially and the larger mix zones would still not promise that all vehicles would pass through the certain area and will be able to change the pseudonym. All these conditions are critically important to consider for the development of the pseudonym changing strategy.

3.2.1 General Mix Context

Li [15] proposed the idea of mix context for the first time in 2006. It is a user centric approach which does not rely on a particular location as in case of mix zone. The vehicles can independently determine when to change the pseudonyms. Unlike mix zone, mix context allows vehicles to decide when and where to change pseudonyms. Now every vehicle on the road has a high probability of changing its pseudonym as it does not need to pass through a mix zone for the change and depending on user requirements for location privacy. The technique proposed by Li has two phases, namely, *swing* and *swap*. *Swing* enables vehicles to synchronize updates loosely during the change in their velocity and *swap* is the extension of the *swing*, it facilitates the exchanging of the pseudonyms among vehicles to increase the location privacy. The author evaluated the scheme with the entropy of anonymity set size as the privacy metric under the random and restricted pedestrian mobility. This scheme uses random silent technique as the base and focuses on the prevention of the tracking mitigation. The drawbacks of this scheme are that it makes use of silent periods and the exchange of pseudonyms needs accountability. Also, it is not reliable in a non-cooperative environment.

The first implementation of the mix context was done in 2007 by Gerlach [13]. The context mix models arguably prevent vehicle tracking better than mix zone. As the vehicles are changing the pseudonyms independent of the location which removes the certainty of change at a particular location. Now freely moving vehicles change pseudonym while they are moving on the road and decide among themselves for synchronized change. The location privacy significantly increases as the number of vehicles increases. The observation from the simulation on JAVA using JIST/SWANS and STRAW shows that the tracking time is affected due to traffic density. The entropy of the anonymity set size is measured for the comparisons.

Table 3: Road network based Mix Zone schemes

Author [ref]	Year	Key concept	Changing strategy	Privacy metric	Problems	Evaluation method
Palanisamy [20–23]	2011-2015	Attack resilient, placement strategies	MobiMix	Information entropy	Difficult to compare with other schemes due to different evaluation metric	Analysis, Simulation
Liu [17]	2012	Three Placement constraints and two heuristic placement algorithms	Multiple mix zones preventing information attacks	Information entropy	Primarily focussed on placement, not the changing scheme	Analysis, Simulation

Table 4: General Mix context schemes

Author [ref]	Year	Key concept	Changing strategy	Privacy metric	Problems	Evaluation method
Li [15]	2006	First idea of Mix Context	User centric, swing and swap	Entropy of Anonymity Set Size	Silent periods and exchange needs accountability	Simulation
Gerlach [13]	2007	First implementation of Mix Context	Vehicles cooperate, No infrastructure needed, No fixed places	Entropy of Anonymity Set Size	Non-cooperative behavior of vehicles	Simulation
Liao [16]	2009	Synchronous pseudonym change algorithm	Prevent semantic and syntactic attacks	Success Rate	In case other vehicles do not have similar status	Simulation

Liao [16] attempted to propose a scheme called as synchronous pseudonym change algorithm. In this approach, the status information of the vehicle and the simultaneity of the pseudonym change are considered. The author described the algorithm and supported it by giving simulation results. The simultaneous change ensures the prevention of the syntactic attacks in which the adversary is not able to identify the vehicle if there a number of vehicles changing their pseudonyms altogether. There is no risk to safety in this scheme as it does not use radio silence. The simulation is carried out on C++ and STRAW by using evaluation metric as success rate.

3.2.2 Trigger Based Mix Context

Eckhoff [11] presented the usage of pseudonym pools which enables the vehicles to change their identities autonomously. The scheme can be enhanced with the slotted time for static sized pseudonym pool. It also has an exchange of pseudonyms which increases location privacy exponentially. The mapping and tracking of the vehicles become harder. The entropy of the anonymity set size is the privacy metric used for evaluation of the scheme. The simulation setup uses SUMO, OMNET, and INET. The drawback of the scheme is the accountability of the exchanged pseudonyms. The authorities must have a new mapping in order to revocate the malicious user.

Song [29] proposed the concept of location privacy based on vehicular density. The pseudonyms of all the vehicles in vicinity change as the threshold reaches. There is a vehicular threshold which is the triggering factor and it is defined as k-1 that is if there are k-1 neighbors in the vicinity of the vehicle and they all can listen to each other, then they all change the pseudonyms altogether. This simultaneous change increases the confusion for the attacker. This scheme is evaluated based on the success rate of the adversary. In this strategy, the frequency of pseudonym change does not affect. The author has provided the comparison with AMOEBA and CMIX schemes and the simulation results support the comparison. It outperforms both schemes with respect to success rate. The simulation using NS2, SUMO, and TRaNS shows the performance of the dense network. This scheme may not perform well in sparse networks as it requires a certain number of the vehicular density around the vehicle for pseudonym change. On the other hand, it is applicable to the vehicle to vehicle communication.

Buttyan [8] proposed a scheme which uses silent periods based on the velocity of the vehicles. The pseudonym change would occur as the velocity of the vehicles drop below 30 km/h and the vehicles stop sending the beacons for the duration when the vehicle is moving slowly. It makes this scheme independent of the explicit synchronization and pseudonym change in a fixed place. This idea of an implicit trigger is applicable in the traffic jams and at the red light where the vehicle moves slowly, therefore, it is named as SLOW. The author also argues that this scheme

has no problem with safety applications as slow moving traffic has fewer chances of accidents. The analysis of the scheme shows that the success rate is directly related to the velocity and the density of the vehicles. The author has also shown the effects on safety and computational complexity. The drawback of this scheme is that the vehicles in the light traffic are more traceable as the change becomes obvious when there are no or a few vehicles in the vicinity.

Eckoff [10] presented *SlotSwap* which is the extension of the work in [11]. This scheme promises strong and affordable location privacy with consideration of the network and computational overhead. The time slotted pseudonym pools are used which regulate the change of the pseudonym based on the time slot and to make the synchronized change, GPS signal is used. In this type of pseudonym pools, the pseudonyms are reusable as they are bound to the particular time slot. The author has also proposed an idea of swapping the pseudonyms among the vehicles. But as the scheme is suitable for V2V communication and not depending on the infrastructure, this swapping may not be reported to the concerned authority for the accountability purpose. The simulations on SUMO, OMNET, and INET provides the analysis in two different scenarios of urban and freeway. The results show that the sufficient level of privacy is achievable with this scheme in dense and sparse scenarios on basis of entropy and the traffic overhead caused is insignificantly low.

Pan [24] proposed another trigger based mechanism for pseudonym change which depends on the number of the neighboring vehicles. As the cooperation of the vehicles introduces higher anonymity, the author presented the idea of using the neighboring density as a trigger. Due to the reason that the synchronized change improves location privacy, the proposed scheme allows implicit synchronization on the V2V communication. It is easy to implement but it does not perform well in sparse networks. The author provided a comparison of the not cooperating vehicular network to the cooperative network in one and multi lane and the results of the MATLAB simulations show that with the anonymity set increment, the unlinkability increases which increases the location privacy. On the other hand, the scheme is deprived of the mechanism which regulates the number of required updates of pseudonym which may cause overhead at times.

Ying [33] introduced a flexible approach which eliminates the problem of fixed mix zones. It is called as Pseudonym Changes based on Candidate-location-list (PCC). This strategy uses the dynamic mix zones along with the candidate location list for changing the pseudonyms. The list has various identifiers and one of them tells about the slot when the pseudonym is to be changed. As the vehicles maintain this location list, it changes pseudonym at the same time due to this identifier. It works well in dense networks but it may be not effective in light traffic as the adversary may identify the vehicle after its updating due to fewer vehicles around and position prediction. The author provided the beacon format for candidate location list, algorithm, and analysis of the scheme. The size of anonymity set and success rate are used for the simulation comparison of the stratey CPN [24], DMLP [34], and PCC [33].

Boualouache [4] has provided the concept of traffic awareness which is used along with radio silence. The scheme ensures the safety and balances the privacy and safety. The scheme proposed is closely related to SLOW as it monitors the traffic and chooses a suitable place to change pseudonym. The author suggests the congestion is the best opportunity for the updating but in real time it may cause a problem for the vehicles which do not pass through a congested area and would not get an opportunity for changing the pseudonym.

3.2.3 Group Based Mix Context

CARAVAN/AMOEBA is the approach for the location privacy proposed by Sampigethaya [26] in 2005. The group of vehicles is formed on the basis of broadcast listening. If vehicles can listen to each other's broadcast, they will form a group with a group manager. The group manager is a proxy for anonymous access. It represents the entire group and communicates on behalf of its group as the vehicles in the group are relative with respect to velocity of the nearby vehicles. The analytical and simulation results show that average anonymity in free way model increases with increase in anonymity set size [27]. The tracking time is reduced significantly with increase in a number of vehicles as more number of vehicles increase the entropy. This paper has detailed mathematical analysis of the scheme and step by step explanations of the simulation which would be very helpful in order to understand the scheme and its implementation. The only possible drawback with this scheme can be seen in the group formation and silence of the group members. The group management in the vehicular environment is challenging and the silence risks safety even though it is for short duration.

Wasef [30] has introduced the Random Encryption Periods for enhancing the location privacy. The strategy uses Public Key Infrastructure along with probabilistic symmetric key distribution. The symmetric key is the group based secret key which is shared among the neighboring vehicles. The scheme promises reliability, efficiency, and scalability. The author has provided a detailed analysis of the REP and supported with the simulation on MATLAB by using evaluation metric as anonymity set size. The problem with this scheme arises with the group communication which is difficult to manage in vehicular environments.

Weerasinghe [31] introduced the concept of a group based synchronized pseudonym changing protocol for the first time in 2011. The advantage of the scheme is that it takes larger anonymity set and higher entropy during the pseudonym change. It is not only safety compliant but also prevents continuous tracking. The group manager decides the time to change the pseudonym and other group

Table 5: Trigger based Mix context schemes

Author [ref]	Year	Key concept	Changing strategy	Privacy metric	Problems	Evaluation method
Eckhoff [11]	2010	Time slot synchronization	Use of static size pseudonym pools	Entropy of Anonymity Set Size	Accountability of exchanged pseudonyms	Simulation
Song [29]	2009	Trigger based on vehicular density	No effect of frequency of pseudonym change	Success rate	Inefficient in sparse network and no semantic protection	Simulation
Buttyan [8]	2009	SLOW, implicit trigger	Change occurs as velocity drop down 30 km/h	Success rate	Traceable in light traffic	Analysis
Eckhoff [10]	2011	SlotSwap	extension of [26], strong and affordable	Entropy	Reusable pseudonym and swapping is not accountable	Simulation
Pan [24]	2013	Trigger based on number of neighboring vehicles	Cooperative pseudonym scheme	Anonymity set	Inefficient in sparse network and number of updates regulation	Analysis, Simulation
Ying [33]	2015	Dynamic Mix Zone	Candidate Location List which implicitly has defined timeslot for change	Anonymity Set Size and Success Rate	Sparse network	Analysis, Simulation
Boualouache [4]	2017	TAPACS	Traffic awareness with radio silence	Entropy of Anonymity Set	Need congested area for change	Analysis, Simulation

Table 6: Group based Mix context schemes

Author [ref]	Year	Key concept	Changing strategy	Privacy metric	Problems	Evaluation method
Sampigethaya [26, 27]	2005	CARAVAN/ AMOEBA	Group based, group manager is proxy for anonymous access	Anonymity Set Size	Group management is difficult in VANET	Analysis, Simulation
Wasef [30]	2010	Random Encryption Periods (REP)	PKI used with probabilistic symmetric key distribution	Anonymity Set Size	Group communication in VANET is difficult	Analysis, Simulation
Weerasinghe [31]	2011	Group based synchronization	Signal strength changes which change temporal and spatial properties	Anonymity Set Size, Entropy of Anonymity Set Size, and Tracking Probability	Group communication in VANET is difficult	Simulation

members are informed and after changing the pseudonym, the group is dissolved. Also, the signal strength is changed as the pseudonym is changed. Weerasinghe added an interesting idea of using a group identifier for certain time between two of the pseudonyms. It changes temporal and spatial properties as it adds the confusion and complicate the process for the tracking. The metrics used to evaluate the scheme were anonymity set, the entropy of anonymity set, and tracking probability. The simulation is performed on NS2 with Manhattan and urban model.

4 Comparison

There are a number of schemes proposed for changing the pseudonym but each scheme has certain advantages and disadvantages. Some of them are applicable only in urban areas and some work well on freeways. Various mechanisms are used in the proposed schemes which affect not only the performance and overhead but also the safety of the vehicles. In this section, we discuss the different entities in the pseudonym change and their benefits and effects with respect to location privacy.

Radio silence is majorly suggested as it disrupts the continuous frequent broadcasts which result in untraceability of the vehicles if this silence period is used for the pseudonym change and status change. The radio silence is effective because the attacker can not use the information for linking two or more pseudonyms of the vehicles, thus gives high location privacy. The concept of radio silence was first introduced in 2006 by Li [20] and has been used in number of other schemes in different manner [6, 8, 11, 14, 20, 34, 35]. This privacy preserving technique of silence may have benefits but it cannot avoid the risk posed by silence to the safety related applications. The vehicular network aims to provide safety to the driver and passengers which must not be compromised. Therefore, there is a need of balance in between the privacy and safety.

Another significant factor which also disrupts the continuous eavesdropping and tracking is the encryption. This encryption is not proposed for entire communication of the vehicular network. It is limited to the certain zones or areas where all the vehicles are high in number and feasible to change the pseudonyms. The encryption in such areas provides a security layer over the vehicular communication which cannot be listened by the attacker for some time. This idea of encryption is scalable, feasible to V2V communication and can eliminate the use of infrastructure as well if required. The only threat posed by encryption is the internal adversary. When the internal adversary helps global adversary, the tracking can be possible with high success rate. The schemes use encryption along with radio silence or in mix zone [1, 3, 15, 28].

There are schemes which propose the exchange of the pseudonyms among the vehicles which helps in increasing the confusion for the adversary. While these schemes do not give a suitable mechanism to report these exchanges to the authorities, which need to have the pseudonym to VID mapping for the revocation purpose, in cases of security attack. Thus, using the swapping technique significantly impact overall working of the pseudonym authentication. Accountability is mandatory and there is need to have the swapping techniques with accountability. This may introduce a higher level of location privacy.

In the vehicular environment, group management is critical due to the highly dynamic network. The events of entering and exiting are fast and large in number, which complicate the group management processes. Therefore, it may not be a good idea to introduce grouping for the pseudonym change schemes as it then has to deal with different other problems regarding the group in the network performance. As many of the schemes are concerned with the anonymity set size which is the number of neighboring vehicles, the schemes are applicable to the dense scenarios like urban and busy highways. There are no schemes yet which can protect the vehicles in light traffic areas, mainly, because the adversary can predict the next possible location of the vehicle and can relate the pseudonyms. Thus, there is lack of location privacy in sparse networks.

The trigger based techniques are excellent because it enables implicit trigger for a change of pseudonym. These are more effective as the adversary is not aware when vehicles are changing pseudonyms and it can only see the change and it is not easy to correlate after an implicit trigger. Another advantage is that even if the adversary is monitoring the information, it does not know when exactly and where the change is going to happen. Therefore, the prediction of such events is very difficult with no significant related information. These allow more flexibility and scalability to the pseudonym changing schemes. The possible drawback associated with this technique is that if there are not a sufficient number of vehicles, then adversary may trace the vehicle. Therefore, trigger technique is bound to the anonymity set size or the number of neighboring vehicles.

The mix context schemes are based on the cooperative behavior of the vehicles which is essential for the V2V communication. Therefore, in such cases, if some of the vehicles refuse to cooperate then other would suffer as they cannot change their pseudonyms. It is possible when there is a limit to the pseudonym change as the frequency of the change must be bounded otherwise, the vehicle either run out of the pseudonyms or may not be able to contact certificate authorities to obtain more of the pseudonyms. Thus, non cooperative behavior has a negative effect on the mix context schemes.

While comparing the schemes, it can be difficult to understand the effectiveness as different schemes use different privacy metrics and when the evaluation is carried out on basis of separate factors, it is challenging task to analyze. There is not a set of standardized evaluation privacy metrics which resolve this problem so that different schemes can be analyzed under a consistent set of metrics. Similarly, the schemes are analyzed in diverse simulation platforms with different mobility and adver-

Table 7: Comparison among pseudonym changing strategies

Scheme	Category	Radio silence	Infra-structure	Encryp-tion	Safety effect	overhead	Syntactic preven-tion	Semantic preven-tion	exchange
CMIX	Mix Zone	No	Yes	Yes	No	Yes	+	+	No
Social-Spots	Mix Zone	No	Yes	No	No	No	+ + +	No	No
S2SI	Mix Zone	Yes	Yes	No	Yes	No	+ + +	+ +	Yes
VLPZ	Mix Zone	Yes	Yes	No	No	No	+ + +	+ +	No
DMLP	Mix Zone	No	Yes	Yes	No	Yes	+	+	No
PMZ	Mix Zone	No	Yes	Yes	No	No	+ +	No	No
Extended CMIX	Mix Zone	No	Yes	Yes	No	No	+ +	+	No
Swing-Swap	Mix Context	No	No	No	No	No	+ +	+ +	Yes
Mix Context	Mix Context	No	No	No	No	No	+ +	+ +	No
CARVAN/ AMOEBA	Mix Context	Yes	No	No	Yes	No	+ +	+ +	No
Liao	Mix Context	No	No	No	No	Possible	+ + +	+ +	No
DLP	Mix Context	No	No	No	No	No	+ +	No	No
SLOW	Mix Context	Yes	No	No	Yes	No	+ +	+ +	No
REP	Mix Context	No	No	Yes	No	Yes	+	+	No
Weerasin-ghe	Mix Context	No	No	No	No	Possible	+ +	+ +	No
CPN	Mix Context	No	No	No	No	No	+ +	No	No
SlotSwap	Mix Context	No	No	No	No	Yes	+ + + +	No	Yes
PCC	Mix Context	No	No	No	No	Yes	+ +	No	No
SPCP	Mix Context	No	No	No	No	Yes	+ +	No	No
TAPCS	Mix Context	Yes	No	No	No	No	+ +	+ +	No

sary models which cause the problem of understanding, evaluating, comparing and analyzing the underlying idea and algorithm.

5 Recommendations for Further Research

The existing work points out and resolves the problem of changing pseudonym but there are many open problems related to safety, scalability, flexibility, and applicability. Here, we will identify the research gaps and discuss the potential subjects where work is required in future.

First of all, the schemes refer how to change pseudonym but the frequency of this change is not discussed. The mechanism is required which properly deals with the number of updates required for optimal performance and privacy. Secondly, the re-usability of the pseudonym should be addressed carefully with respect to the location privacy because if same pseudonym is used by a vehicle, it may still have some chances of being traced when the strong adversary is placed. Also, the schemes referring to the fixed area are subjected to the problem of passing through such an area as it may not be possible for all the vehicles on the road. Such fixed areas for changing pseudonym may not lie in the route of the vehicle which increases the traceability only because it was not going through such area. All the vehicles must be able to change pseudonym irrespective of trip or location.

The safety and privacy are required to have a balance such that using a scheme for pseudonym change does not pose any risk to human lives as safety is the primary objective of the VANET. The radio silence is proposed in a number of schemes but stopping communication at highly dense area increase the safety risk. Therefore, the future research can be directed to find an alternative to radio silence for communication interruption or to find a trade-off between safety and privacy.

Another major problem is the accountability which requires attention in the future work. The exchange of the pseudonym increases location privacy and adds confusion to adversary tracking. There are no schemes which can provide a reliable exchange of the pseudonyms that is reported back to the authorities for further processing in case of revocation. The swapping should not hinder overall performance and should result in effective privacy. Keeping the beacon size in limit may improve the network performance. The upcoming work also needs attention on the applicability of the proposed scheme in the dense as well as sparse scenarios because every vehicle in every situation is subjected to change of pseudonym. The flexibility and adaptability are important as the vehicular environment are highly dynamic. The triggers are the excellent ideas which can be implicit or explicit, however, these triggers should be working in dense and sparse networks. When there is an internal adversary then many of the schemes fails to preserve privacy, for example, the group

based schemes and encryption schemes. Thus, the forthcoming work may introduce the prevention schemes for internal adversary explicitly or may propose the scheme which is not affected by the internal adversary.

6 Conclusion

The discussion and comparison provided in this paper enable the deeper understanding of the various perspectives of different approaches and their requirements and challenges. The comparison not only highlights the significant details of each approach but also shows the relation and impact of the scheme on safety, security, privacy, and performance. We identified a number of challenges for future research such as safety and privacy trade-off, accountable exchanges of pseudonyms and usage of a consistent set of privacy metrics. To the best of our knowledge, this survey provides the most detailed and comprehensive overview of the existing pseudonym changing schemes for VANET till date. We expect that this survey is considered helpful in the development of pseudonym changing strategies for Vehicular Ad Hoc Networks eventually leading to privacy preserving V2X systems.

References

[1] Q. A. Arain, Z. Deng, I. Memon, A. Zubedi, J. Jiao, A. Ashraf, and M. S. Khan, "Privacy protection with dynamic pseudonym-based multiple mix-zones over road networks," *China Communications*, vol. 14, no. 4, pp. 89–100, 2017.

[2] A. R. Beresford and F. Stajano, "Location privacy in pervasive computing," *IEEE Pervasive Computing*, vol. 2, no. 1, pp. 46–55, 2003.

[3] A. Boualouache and S. Moussaoui, "S2si: A practical pseudonym changing strategy for location privacy in vanets," in *International Conference on Advanced Networking Distributed Systems and Applications (INDS'14)*, pp. 70–75, 2014.

[4] A. Boualouache and S. Moussaoui, "Tapcs: Traffic-aware pseudonym changing strategy for vanets," *Peer-to-Peer Networking and Applications*, vol. 10, no. 4, pp. 1008–1020, 2017.

[5] A. Boualouache, S. M. Senouci, and S. Moussaoui, "Towards an efficient pseudonym management and changing scheme for vehicular ad-hoc networks," in *IEEE Global Communications Conference (GLOBECOM'16)*, pp. 1–7, 2016.

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

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

[8] L. Buttyán, T. Holczer, A. Weimerskirch, and W. Whyte, "Slow: A practical pseudonym changing scheme for location privacy in vanets," in *IEEE Vehicular Networking Conference*, pp. 1–8, 2009.

[9] A. M. Carianha, L. P. Barreto, and G. Lima, "Improving location privacy in mix-zones for vanets," in *IEEE 30th International Performance Computing and Communications Conference (IPCCC'11)*, pp. 1–6, 2011.

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

[11] D. Eckhoff, C. Sommer, T. Gansen, R. German, and F. Dressler, "Strong and affordable location privacy in vanets: Identity diffusion using time-slots and swapping," in *IEEE Vehicular Networking Conference (VNC'10)*, pp. 174–181, 2010.

[12] J. Freudiger, M. Raya, M. Félegyházi, P. Papadimitratos, and J. P. Hubaux, "Mix-zones for location privacy in vehicular networks," in *ACM Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS'07)*, no. LCA-CONF-2007-016, 2007.

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

[14] C. Lai, H. Chang, and C. C. Lu, "A secure anonymous key mechanism for privacy protection in vanet," in *9th International Conference on Intelligent Transport Systems Telecommunications (ITST'09)*, pp. 635–640, 2009.

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

[16] J. Liao and J. Li, "Effectively changing pseudonyms for privacy protection in vanets," in *10th International Symposium on Pervasive Systems, Algorithms, and Networks (ISPAN'09)*, pp. 648–652, 2009.

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

[18] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen, "Anonymity analysis on social spot based pseudonym changing for location privacy in vanets," in *IEEE International Conference on Communications (ICC'11)*, pp. 1–5, 2011.

[19] M. E. Nowatkowski, "Certificate revocation list distribution in vehicular ad hoc networks," *Georgia Institute of Technology*, 2010. (`https://smartech.gatech.edu/bitstream/handle/1853/33971/nowatkowski_michael_e_201005_phd.pdf`)

[20] B. Palanisamy and L. Liu, "Mobimix: Protecting location privacy with mix-zones over road networks,"

in *IEEE 27th International Conference on Data Engineering (ICDE'11)*, pp. 494–505, 2011.

[21] B. Palanisamy and L. Liu, "Attack-resilient mix-zones over road networks: Architecture and algorithms," *IEEE Transactions on Mobile Computing*, vol. 14, no. 3, pp. 495–508, 2015.

[22] B. Palanisamy, L. Liu, K. Lee, A. Singh, and Y. Tang, "Location privacy with road network mix-zones," in *Eighth International Conference on Mobile Ad-hoc and Sensor Networks*, pp. 124–131, 2012.

[23] B. Palanisamy, S. Ravichandran, L. Liu, B. Han, K. Lee, and C. Pu, "Road network mix-zones for anonymous location based services," in *IEEE 29th International Conference on Data Engineering (ICDE'13)*, pp. 1300–1303, 2013.

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

[25] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J. P. Hubaux, "Eviction of misbehaving and faulty nodes in vehicular networks," *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 8, 2007.

[26] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki, *Caravan: Providing Location Privacy for Vanet*, 2005. (`https://pdfs.semanticscholar.org/fb10/495488bfc72edaf63bd17bc7963b34b6cefe.pdf`)

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

[28] F. Scheuer, K. P. Fuchs, and H. Federrath, "A safety-preserving mix zone for vanets," in *International Conference on Trust, Privacy and Security in Digital Business*, pp. 37–48, 2011.

[29] J. H. Song, V. W. S. Wong, and V. C. M. Leung, "Wireless location privacy protection in vehicular ad-hoc networks," *Mobile Networks and Applications*, vol. 15, no. 1, pp. 160–171, 2010.

[30] A. Wasef and X. S. Shen, "Rep: Location privacy for vanets using random encryption periods," *Mobile Networks and Applications*, vol. 15, no. 1, pp. 172–185, 2010.

[31] H. Weerasinghe, H. Fu, S. Leng, and Y. Zhu, "Enhancing unlinkability in vehicular ad hoc networks," in *IEEE International Conference on Intelligence and Security Informatics (ISI'11)*, pp. 161–166, 2011.

[32] B. Wiedersheim, Z. Ma, F. Kargl, and P. Papadimitratos, "Privacy in inter-vehicular networks: Why simple pseudonym change is not enough," in *Seventh International Conference on Wireless On-demand Network Systems and Services (WONS'10)*, pp. 176–183, 2010.

[33] B. Ying and D. Makrakis, "Pseudonym changes scheme based on candidate-location-list in vehicular networks," in *IEEE International Conference on Communications (ICC'15)*, pp. 7292–7297, 2015.

[34] B. Ying, D. Makrakis, and H. T. Mouftah, "Dynamic mix-zone for location privacy in vehicular networks," *IEEE Communications Letters*, vol. 17, no. 8, pp. 1524–1527, 2013.

[35] L. Zhang, "Otibaagka: A new security tool for cryptographic mix-zone establishment in vehicular ad hoc networks," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 12, pp. 2998–3010, 2017.

Biography

Ikjot Saini is currently a PhD Candidate in the Department of Computer Science at the University of Windsor. Her research interests include computer security and privacy, vehicle ad hoc networks, and network communications. Ikjot Saini has B.Tech. and M.Tech. degrees in Computer Science and Engineering from India. Her recent research interests focus on Vehicular Ad hoc Networks, security and privacy issues, pseudonymous authentication and threat modeling in the vehicular environment.

Sherif Saad has more than ten years of industry experience in cybersecurity. During these years. He designed and built security systems for the RCMP, DRDC, DIUx and many other customers. Dr. Saad received his Ph.D. in Computer Engineering from the University of Victoria, BC Canada in 2015. In 2017 Dr.Saad joined the School of Computer Science, University of Windsor, Canada as an assistant professor. Dr. Saad has published many research papers and journal articles in security incident analysis, network forensics, biometrics, botnet, and malware analysis, digital cash, electronic voting, spam review and authorship verification. His current academic research focuses on access control, blockchain, applied machine learning in cybersecurity and security and privacy in IoT.

Dr. Arunita Jaekel received her B. Engg. in Electronics and Telecommunications Engineering from Jadavpur University, India, and her M.A. Sc and Ph.D. in Electrical Engineering from University of Windsor, Canada. Since 1995, she has been working as a faculty member in the School of Computer Science at the University of Windsor, where she is currently a tenured professor. Her research is supported by grants from the Natural Sciences and Engineering Research Council (NSERC), Canada. She has served as an external reviewer for NSERC strategic grant proposals and as a member of the NSERC PGS Scholarships and Fellowships Committee for Math and Computer Science. She has been a member of the organizing committee for a number of international conferences such as Boradnets, ICCCN and TridentCom. She has also served as TPC co-chair of the Optical Networking Symposium in Globecom 09. Her current research interests include vehicle-to-vehicle (V2V) communication, design of reliable wireless sensor networks and optical networks.