Exploring Pseudonymous based Schemes for Safegaurding Location Privacy in Vehicular Adhoc Network (VANET)

Arslan Akhtar Joyo[†] **,Fizza Abbas Alvi**[†], Rafia Naz Memon[††], Irfana Memon[†], and Sajida Parveen [††]

[†]Department of Computer Systems Engineering Quaid e Awam University (QUEST), Pakistan
[††]Department of Software Engineering Quaid e Awam University (QUEST), Pakistan

Summary
Vehicular Ad Hoc Network (VANET) is considered to be a subclass of Mobile Ad Hoc Networks (MANET). It has some challenges and issues of privacy which require to be solved before practical implementation of the system i.e., location preservation privacy. Many schemes have been proposed. The most prominent is pseudonym change based location preservation scheme. Safety message can be compromised when it sends via a wireless medium, consequently, an adversary can eavesdrop the communication to analyze and track targeted vehicle. The issue can be counter by use of pseudo identity instead of real and their change while communication proves to be a sufficient solution for such problems. In this context, a large amount of literature on pseudonym change strategies has been proposed to solve such problems in VANET. In this paper, we have given details on strategies proposed last two decades on pseudonym change based location preservation along with issues that they focus to resolve and try to give full understanding to readers.

Keywords:
VANET, Privacy, Location, Pseudonymity.

1. Introduction

For a few decades, the world has been witnessing changes in technology. In context, innovation is also observed in Wireless Ad-hoc Network fields like "Vehicular Ad-hoc Networks" - VANET, to control challenges connected with surges of vehicles. As bring challenges i.e. road safety, traffic efficiency, Traffic Jamming. Moreover, problems like comfort, a connection of driver and passengers with entertainment and infotainment. Fig. 1 shows VANET Inter-relation with other networks it is a subclass of Wireless Ad hoc Network (WANET). VANETs prove to be helpful in case of providing communication between the vehicles. It enables communication features with the aid of Road Side Unit (RSU) and On Board Unit (OBU), based on IEEE 802.11p [1]. It provides the ability for vehicles to judge their surroundings with the help of V2V (Vehicle-to-Vehicle) and V2X (Vehicle-to-Infrastructure) or it can be V2X (Vehicle-to-Everything). In VANETs boundary each vehicle requires to broadcast an information-based message known as a beacon in the network, which mainly contains the vehicle's current position, speed, identifier (vehicle number plate), and other related information that are combined with signature and timestamp to describe vehicle status[2]. This type of knowledge is pursued by traffic efficiency and safety services to enhance the driving experience in traffic movement and boost the line of sight of the drivers to establish ease and comfort for drivers and passengers [3].

Despite all the praises of VANET, there are unavoidable flaws i.e. Beacon message encryption creates extra latency and overhead. Due to broadcast of a safety with position of the vehicle can easily be compromised and eavesdropper can access location which creates a potential threat to drivers' privacy. Tracking a driver's position may vary depending upon the situation, for instance, a boss wants to locate the exact location of his colleague or a thief wants to know the house owner's location to break in while the owner is away. This type of situation creates severe consequences for the vehicle's owner therefore fake identity (pseudonym) instead of a real identity to protect itself from eavesdroppers, so for this reason pseudonymous schemes have been proposed to counter privacy and security problems in VANET. However, besides implementing a pseudonymous scheme in a Vehicular environment still adversary can easily track the vehicle's location. In this context, a large amount of research has been done to investigate the issues related to pseudonymity in vehicular networks. This paper highlights these schemes in detail along with their limitations. Moreover, this paper also provides research challenges in VANET.

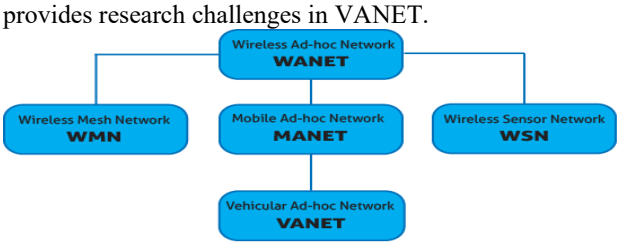

Fig. 1 VANET inter-relation with other networks.

Manuscript received February 5, 2023
Manuscript revised February 20, 2023
https://doi.org/10.22937/IJCSNS.2023.23.2.11

The rest of the paper is organized as follows. Section 2 presents the background. In Section 3 Existing works on pseudonym change schemes, In Section 4, we present the research challenges. Section 5 concludes the paper.

2. Background

In this section, we provided detailed information on VANET security requirements, security-related challenges standards and type of adversary.

2.1 Security Requirements

Privacy: The privacy factor to be deployed in the VANET network zone, ensure that the driver's real identity should be safe from unauthorized access except for law agencies [4] and the location of the vehicle should be protected.

Unforgeability: Unforgeability means that an adversary remains unable to link the signature on the transmitted beacon to know the real identity of the vehicle. An adversary can reuse the exact transmitted message to create a replica of the signature [5].

Unlinkability: It ensures that the adversary would not link the signature or message with the actual identity of the vehicle and ensure that secret information of VANET remains hidden from the adversary even though the signature or message is captured and analyzed [6].

Access control: To differentiate the access level of various entities [7]. There should be a type of mechanism, that agencies i.e., law enforcement, can use to revoke the malicious vehicle from the network.

Physical Security: It refers to the protection of cryptography-based credentials from unauthorized users or access can be achieved by selecting non-tempered hardware within the OBU of the vehicle [5].

Traceability and Revocation: Traceability and Revocation ensure that Trusted Authority (TA) found the vehicle involved in any illegal activity i.e., malicious activities, disclose the vehicle's true identity, and revoke it from the VANET network zone [5].

Forward Secrecy: The new vehicles that join the group unable to read sent messages, which is being sent by new group members [5].

Backward Secrecy: The vehicles leave the group unable to read sent messages, which are being sent by new group members [5].

Transparency: The transparency of the Administrator and Trusted Authority (TA), ensures that the operation of the TA is reliable and trustable. In VANET transparency also ensure the trust of the respective members involved in the Trusted Authority operation in the network [6].

Key Liberty: Key Liberty is achieved via a combination of forward and backward secrecy [5].

Fig. 2 VANET Security Requirements

2.1 VANET Security-Related Challenges

In [8] literature different security-related challenges of VANET are highlighted and also shown in Fig 3.

1. **Mobility:** Due to high mobility in VANET traditional cryptographic techniques are unsuitable to apply [9]. Therefore, networks should have cryptographic-based techniques, which have low overhead and computational cost.
2. **Scalability:** Due to the high scalability of the network, it is quite challenging to know the actual level of security requirement at the very initial stage of networks. As vehicle count increases then network size and security requirements also increase.
3. **Data:** Huge increasing count of vehicles can produce a large volume of data on daily basis and a variety of data from restrictions for Central Authority (CA) in management. Therefore, decentralized approach consider to be better; however, it has issues like it impedes revocation and non-repudiation [8]
4. **Communication Range of RSU:** Road Side Unit (RSU) range of communication has a huge impact on the VANET Network. The range of RSU in radius is about 500m. The 1km distance between RSUs makes it impractical for congested traffic. In [10] various communication pattern of VANET is discussed.
5. **Trust Management Hurdles:** Despite VANET's high scalability, it possesses some chances of two vehicles

having trust in each other. In the VANET scenario thousands of vehicles communicating with each other daily, produce a huge amount of data load on the vehicle's OBU. which make it difficult for OBU to manage data. In [11] trust reference and modeling are shown.

6. **Infrastructure Dependency:** Authentication is an essential part of vehicular communication and a vehicle must authenticate with the trusted authority (TA) and be mandatory to achieve non-repudiation and revocation. Secure communication depends highly on RSU or infrastructure as transmitted became weak and needs amplification, which is done by infrastructure [12]. so for reliable transmission, vehicles depend on roadside infrastructure.

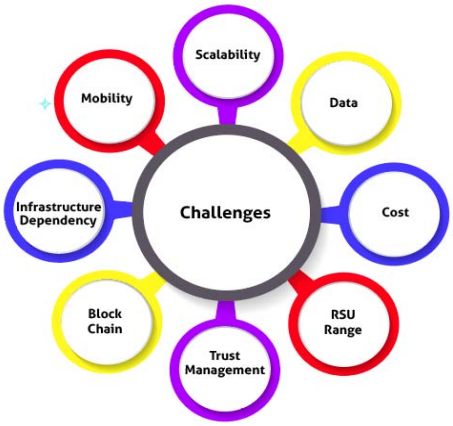

Fig. 3 VANET Security Related Challenges

2.2 Type of Adversary

It an essential to consider exact problems by understanding the characteristics and features of the driver's environment, and adversary types that can be executed by an adversary as crucial factors to understand the scenario to make decisions and countermeasures. In Vehicular Ad Hoc Networks (VANET),some adversaries and attack types are mentioned in the literature [13]. So based on the aforementioned research papers' review we have concluded our observation depends on the following context:

1. **Passive or Active – "Actively":** Passive attacker is restricted to perform eavesdropping on the transmitted information; therefore, it cannot directly influence or alter the communication on the other hand an active attacker can alter or add self-typed messages in transmitted information to affect the network performance.
2. **Rational or Malicious –"Behaviorally":** Rational attackers perform an attack based on the aim to achieve personal benefit from the executed attack on a network, which is considered more predictive as compared to malicious attack because malicious attackers deliberately perform the highly destructive attack on a network via different methods to damage the network.
3. **Static or Dynamic– "Movably":** The Eavesdropping stations are being fixed or moveable at a particular spot or across the map. The strength of these each kind depends mainly on the algorithm and mechanism. The moving station requires delicate processing i.e. (moving to follow a particular node) difficult to ensure. However useful in the case where the adversary does not have a lot of stations. A fixed station does not require management except sharing resources and synchronization management, it provides the adversary with good vision with good monitoring abilities only if an adversary has stations in greater numbers to cover the area, if does not have sufficient stations then cannot be able to monitor whatever adversary want.
4. **Outsider or Insider- "Locationally":** The outsider attacker is not officially a member of the VANET network, which means he/she cannot participate in the network directly without restriction, in contrary to this Insider is an official and authorized member of the VANET network, in which the attacker can participate directly without any restriction, hence it is obvious that an insider is comparably more dangerous for the network than an outsider attacker.
5. **Temporal or Permanent- "Occasionally":** The adversary can be temporary or permanent, an observer of the targeted covered area. Temporal performs eavesdrop at some or specific period based on his/her interest, benefits, and intention. Contrary to this, a permanent observer performs eavesdrops on distinct communication that occurs at all times and gathers the data.
6. **Local or Global- "Proprietarily:** The local adversary is restricted to control less network entities as compared to a global adversary; local adversary is limited to a covered area. On contrary, a global adversary can detect moving (mobile) entities inside of a covered area easily because it can control huge areas deployed across the network in terms of a radio station.

3. Existing Work

This section highlights existing work-related pseudonyms and pseudonym-based location preservation schemes. The word "Pseudonym" is used as an alternative name instead of a real name, individual in each organization are known through their pseudonym identity instead of their original names to preserve real identity and privacy in an anonymous way. These pseudonym identities are generated in such a way that they cannot link to real identity thus

adversary is unable to reveal the real information of any entity later by using his/her credential and this way it provides unlinkability[14]. Using one identifier all the time can create serious complications like tracking and identification of the vehicle therefore it is essential in VANET to use various identifiers known by the name of pseudonyms.

3.1 Pseudonym Based Location Preservation Schemes

To preserve the location privacy, the large amount of literature has been proposed. In this we have covered pseudonym-based location preservation schemes proposed from 2005 to 2022. We have provided reviewed literature in which elaborated each scheme to present core difference between them and then concepts, attributes, adversary of types are being considered in the table 1 and table 2 shows comparison of recent techniques. These schemes are developed in past two decades. We have notice that all the schemes proposed on location preservation by using pseudonym change based schemes are more or like based on similar metrics and concepts e.g., Mix Zone and Silence etc. which create hurdle for implementing schemes in real world scenario, this paper is provided with brief in detailed and in tabular form to select best scheme.

Sampigethaya k et al.[15] proposed a scheme named CARAVAN, In which formed a group-based technique to establish a group and also use silent periods between pseudonym changes, they added that forming a group makes one of the vehicles to be leader and others to be members and group reduces the amount of redundant transmission and allow other than group leader to stay silent which surely enhances vehicles' privacy. However, this technique is only suitable to apply in probe vehicle scenario, where vehicle remain silent for a long time without broadcasting beacon related to safety and this is not feasible in case of high-frequency safety- message broadcasting. Huang et al. [16] Investigated a silent period-based scheme used spatially (fixed location) or temporally (random time), and showed that utilizing a silent period establishes enhances the privacy of wireless-based nodes, as it is based on a user-centric based approach, which majorly depends on vehicle's desire. Li et al. [17] form Swing protocol to increment vehicle numbers aim to change their pseudonym at a suitable opportunity, it presents an improvement of the Swing protocol; the utilization of the protocol i.e., Swap, that use for the exchange of pseudonyms than as compare to ordinary change. However, feature lack in proper accountability requirement and identities' management (resolution and revocation of a pseudonym) which impacts the performance of VANET. Swap protocol depends fully on infrastructure for the exchange process of a pseudonym. Sampigethaya k et al. In [18], authors define the concept of a scheme named AMOEBA, in which vehicles are grouped for short period by evaluating a silent period. During the short period group leader broadcast the information while other member vehicles remain silent. They added that it will create an extended silent period against the adversary and would not be able to track the targeted vehicle. However, it will create instability in the safety of VANET, as the vehicle remains silent during the silent period thus it would not inform about any incident. Freudiger et al.[19] proposed CMIX (Cryptography Mix) Zone is a pseudonyms change strategy based on a mixing zone as a hidden area, in this scheme they used the concept of encrypting the vehicle inside the mix zone, where the vehicle inside the mix zone encrypt the safety messages to prevent it from adversary to accessing the location and other useful information. It introduced three stages, establishing the symmetric key by RSU (Road Side Unit). Ensure forward of the key to vehicles before entering into mix zone, and the third stage is key management where RSU generates a new key (during reduction of traffic density) and ensure deliverance of key to the CA, besides effectiveness, it creates problems like overhead and key management synchronizing in between RSUs to allow only one symmetric key in the system. Chaurasia et al. [20] investigated the real anonymity of vehicles among neighboring vehicles about when to change pseudonyms identity and optimized the pseudonyms updating for anonymity. In which they proposed heuristic pseudonym change schemes aimed to change pseudo identity of vehicle depending upon the right time and place when there are certain numbers of vehicles in the vicinity to maximize the effect of anonymity with only few pseudonym changes.

However, he limitation that is embedded with the system i.e. Vehicle change pseudonym if any vehicle comes nearby, it otherwise will not change. It can be considered in drawback because it depends upon the neighboring vehicle. Buttyan et al. [21] proposed a SLOW (Silent at Low Speed) pseudonym change strategy, in which the vehicle remain silent by stopping forwarding safety message below the threshold of 30 km/h, and during this silent period vehicle should change pseudonym identity, although it prevents an adversary from accessing the location of the target, however, it also stops providing beacon message related to traffic jam situation because it fulfilled silent period criteria in jam and also utilization of safety message regarding low-speed accident (sudden braking at low speed) cannot forward. Wasef and Shen et al. [22] proposed and apply the REP(Random Encryption Period) scheme, in which the main concept of REP is to create a hidden and effective pseudonym change by allowing all legitimate vehicles to have a set of symmetric keys. It helps them to provide one shared secret key. When any vehicle wants to change a pseudonym, will use the secret key to create an encrypted zone with aid of neighbors.

This seems to be promising, however, the high-density encryption process may degrade the VANETs' performance, and create additional overhead also this scheme depends upon neighboring for pseudonyms change. Eckhoff et al. [23] proposed Slot swaps a pseudonyms changing strategy, Slot swaps strategy uses time slotted pseudonym pool, in which a vehicle changes its pseudonyms in each slot and the duration of the timeslot is 10 minutes. The main advantage of this scheme is that vehicle has valid pseudonyms even the pseudonyms provider is not available. However, chance of tracking real identity remains same due to the fixed allotted time slot. Lu et al. [24] proposed a pseudonym change at social spot (PCS) strategy. Which base on the concept of pseudonym change at social spot i.e., traffic signal, and parking area, and this strategy aim to maximize the number of simultaneous pseudonym changes. For this authors have selected right spot (parking lot, traffic signal) where the possibility of the number of vehicles' gathering increase. In this work two suggestion are given (1) Vehicles stopped at a red traffic signal and changes its pseudonyms as signal turn to green (2) Vehicles stopped at car parking (e.g., Shopping Mall Parking) changes its pseudonyms before leaving the parking area. To show the efficiency of the strategy, they developed two analytics models of anonymity set. an essential model named KPSD used PCS (Pseudonym change at the social spot) to securely provide and generate on-demand short-life keys, In such conditions, it ensures high synchronization.

However, despite its effectiveness, it has some limitations e.g. road conditions that let the vehicle stay for a long time without finding the mentioned opportunities where the vehicle has to depend on its current pseudonyms identity such a scenario can be counted as a drawback of strategy because an adversary can easily find an opportunity to track the vehicle. Pan and Li.[25] proposed pseudonyms change scheme, named the cooperative pseudonym change scheme (CPN), is based on the concept of neighbors' vehicle numbers. The scheme is embedded with different triggers, which help the vehicle to select the right moment for pseudonym change, in this scheme triggers like the number of neighbors ensure synchronized pseudonyms change which proves to be an effective location privacy enhancement as compared to other individual behavior based schemes, it achieves better results However it depends on the number of neighbors, which is unsuitable for other road conditions. Ying et al. [26] introduced a novel location privacy scheme known as Dynamic Mix-Zone for Location Privacy Strategy (DMLP), they introduced it for location privacy problems. This strategy dynamically forms mix-zones according to the properties i.e. predicted vehicle location and road traffic statistics, history, and privacy requirements. Vehicle inside the Dynamic Mix-Zone encrypts the message which makes the adversary unable to find out what messages are exchanged without the use of encryption keys. It was tested in various scenarios and proved to be an efficient location privacy scheme. However, if the dynamic mix-zone is dense to some level then encryption of messages may cause a huge overhead and will affect VANET performance negatively. Boualouache and Moussaoui et al. [27] give the concept of a scheme known as Silent & Swap at Intersection of Signalized (S2SI), which utilize two protocols, one for establishing a silent mix zone and other one for pseudonyms exchange, However, pseudonym exchange is considered an obstacle because it creates accountability issue, which not suitable for VANET system according to it standardization. Ying et al. [28] proposed a motivation for Protecting Selfish Vehicles' Location Privacy (MPSVLP) based on the previous Dynamic Mix-Zone Location Privacy Strategy (DMLP) discussed in [26], MPSVLP scheme encourages selfish vehicles which may not involve pseudonym change because restricted to resources (such as bandwidth and pseudonym), so that vehicle can participate in pseudonym change by dynamically forming Mix Zone when pseudonym about to expire and also earn repudiation credit by executing pseudonym change. It forms a Dynamic mix zone each time when vehicles want to change their pseudonym and earn repudiation system credit on each pseudonym change.

Yu et al. [29] proposed Mix Group a pseudonyms change scheme, which is based on the concept of both social spots and individual spots which helps in enlarging of vehicle's pseudonym area. It allows the vehicles to join the available groups after entering the area, after getting into group vehicles use the identifier of that particular group acquired from the group leader to stay anonymous with an option of exchanging their pseudonyms among themselves and validating the operation once it meets with Road Side Unit (RSU) at the end of the road, however despite its promising simulation results, scheme introduces high communication overhead and privacy loss of group leader. Boualouache and Moussaoui. [30] Proposed Urban Pseudonym Changing Strategy (UPCS), In which authors have utilized existing signalized intersections, the scheme benefits from such places to construct one or more Silent Mix Zone (SM). Urban Pseudonym Changing Strategy (UPSC) uses pseudonym change or pseudonym exchange technique (that has accountability problem). Boualouache and Moussaoui. [31] Proposed another scheme is known as Traffic Aware Pseudonym Changing Strategy (TAPCS) based on the Silent period concept, In which road condition plays a crucial role in pseudonym change, The strategy relies on the following discussed parts, traffic congestion detection, electing an initiator (i.e. Silent period extension via group leader), creating and extending
the silent mix zone.

Table.1 Location Preserving Pseudonym Change Schemes (LPCS)

LPCS	Year	Concept	Attributes	Adversary	
				Type	Attacks
[15]	2005	Group based random silence.	Group dependent	GPA	ST, CLT
[16]	2005	Fix & variable silence period	Movement dependent	Passive	CLT
[17]	2006	Random silence period	-	GPA LAA	CLT
[18]	2007	Extend silence period based on mix –group	Crowd dependent	LPA GPA	-
[19]	-	mix zones	Road & infrastructure dependent	GPA	-
[20]	2008	Anonymity based on zone	Infrastructure & crowd dependent	Passive	
[21]	2009	Silence, synchronize change (velocity, traffic light)	Crowd Dependent	GPA	Syntactic & Semantic
[22]	2010	Random Encryption Period	Infrastructure Dependent	GPA	-
[23]	2011	Synchronous change	Neighbor dependent	GPA	CLT
[24]	2012	Social spot based on mix zone	Crowd dependent	GPA	CLT
[25]	2013	Cooperative change simultaneously	Trigger & crowd dependent	GPA	CLT
[26]	2013	Dynamic mix zone	Infrastructure dependent	GPA	CLT
[27]	2014	Silence mix zone	Infrastructure & crowd dependent	GPA	Syntactic & Semantic
[28]	2015	Repudiation based dynamic mix zone	Infrastructure & crowd dependent	Global, Passive, External	-
[29]	2016	Mix-group based on groups & social spot	Crowd dependent	GPA, RPA IBA, ITA	-
[30]	2017	Synchronous change based on silence Mix	Infrastructure dependent	EGPA ILPA	Syntactic & semantic
[31]	2017	Simultaneous change based on distributed traffic aware.	Traffic congestion & crowd dependent	GPA	Syntactic & Semantic
[32]	2018	Neighbor position estimation based adaptive beaconing rate	Neighbor dependent	GPA	Spatial correlation
[33]	2019	Cooperative change and silence	Crowd dependent	GPA	Semantic correlation
[34]	2020	Simultaneous change	Infrastructure, Crowd & Map Dependent	GPA	Syntactic & semantic
[35]	2021	Silence based simultaneous cooperative change	Infrastructure & crowd dependent	GPA	Syntactic & semantic, O-Map L-Map
[36]	2022	Silence simultaneous cooperative change based on obfuscation	Infrastructure, crowd & map dependent	GPA	Syntactic & semantic, O-Map L-Map
[37]	2022	Cooperative change based on groups	Infrastructure & group dependent	GPA	CLT

Table 2. Recent literature Comparison

Reference	Year	Key Concept	Changing Strategy	Privacy Metric	Evaluation Metric
[36]	2019	Exchange & permutation	Cooperative Pseudonym Exchange and Permutation (CPESP)	Entropy, Anonymous set size	Simulation, Analyzation
[37]	2020	Location obfuscation	Alloyed Pseudonym Scheme	Anonymity set	Simulation
[38]	2021	Silence Concept	Concerted Silence Scheme (CSLPPS)	Anonymity set	Simulation
[39]	2022	Cooperative Silence, obfuscation	Cloud Enabled Scheme (CE-IoV)	Entropy, Anonymity set	Simulation, Analyzation
[40]	2022	Personalized pseudonym Scheme	Sensitivity-based pseudonym scheme	Entropy, Tracking	Simulation, Analyzation

EGPA: - External Global Passive Adversary
ILPA: - Internal Local Passive Adversary
GPA: - Global Passive Adversary
IBA: - Internal Bilateral Adversary
RPA: - Rational Passive Adversary
ITA: - Internal Tracking Adversary
LAA: Local Active Adversary
O-Map: - Observation Mapping
L-Map: - Linkage Mapping
CLT: - Correlation Tracking

The strategy was simulated for evaluation for location privacy to show the effectiveness of strategy after understanding analytics and comparison with previous strategies i.e. CARVAN and DMLP. Zidani et al. [32] Proposed ENeP-AB, an adaptive beaconing approach for privacy preservation, it allows a vehicle to change pseudonyms identity when there is a high probability to confuse an adversary, vehicles set a flag-bit named Ready flag to willingly change pseudonym next time slot, by this aid vehicle will have the ability to synchronize their pseudonym changes. Another feature used by the scheme is the Adaptive Beaconing rate approach (E-ABRP) which allows a vehicle to change the time, which was constant between two successive beacons outcome defending against a temporal correlation attack. However, the scheme lacks in fulfilling the criteria of efficiency in scattered densities, especially with high and precise location beaconing. Singh et al. [33] proposed pseudonym based scheme known as " Cooperative Pseudonym Exchange Cooper And Scheme Permutation (CPESP)", to change the pseudonym via the cooperation of the vehicles and novel scheme (like pseudonym) to create confusion for adversary by vehicle permutation of the scheme and restrict service provider from location privacy and creates no additional overhead in the communication process. Benarous et al. [34] proposed Alloyed pseudonym change strategy, which focus on the location preservation with help of robust scheme based on pseudonym change which ensures unlinkability by confusing the attacker while pseudonym update phase and counter the linking attack. This scheme prevents from semantic and syntactic attacks. Benarous et al. [35] proposed "Concerated Silence Based Location Privacy Preservation Scheme (CSLPPS)", for ensuring unlinkability and anonymity of Internet of Vehicles (IoV) with aid of silence based simultaneous cooperative change. The scheme provides production against global passive adversary. Benarous et al. [36] introduced location preservation scheme based on Silence, obfuscation and Cooperativeness for Cloud -Enabled Internet of Vehicles for (CE-IoV) users to overcome linking and tracking attacks i.e. syntactic, semantic, mapping linking and observation. Zhong et al [37] developed sensitivity-based pseudonym change scheme, which rely on vehicles' movement for ensuring personalize location privacy preservation. Moreover, introduced metric to measure the protection level of personalized location privacy.

4. Conclusion

This paper provides literature produced by different authors to counter the privacy-related challenges in VANET. Moreover, brief of VANET security-related challenges and analyzed and assessed the pseudonym change based location preservation scheme developed in last 22 years. The paper focuses on location preservation strategies only to give new researcher full overview on existing solution for location tracking based on pseudo-identity change schemes. This paper organized in such way that can be helpful to understand and select best possible scheme for implementation and for further research purposes.

References

[1] V. Hoa La and A. Cavalli, "Security Attacks and Solutions in Vehicular Ad Hoc Networks: A Survey," *International Journal on AdHoc Networking Systems*, vol. 4, no. 2, pp. 1–20, Apr. 2014, doi: 10.5121/ijans.2014.4201.

[2] M. Babaghayou, N. Labraoui, A. A. Abba Ari, N. Lagraa, and M. A. Ferrag, "Pseudonym change-based privacy-preserving schemes in vehicular ad-hoc networks: A survey," *Journal of Information Security and Applications*, vol. 55, Dec. 2020, doi: 10.1016/j.jisa.2020.102618.

[3] R. Hussain, S. Kim, and H. Oh, "Towards Privacy Aware Pseudonymless Strategy for Avoiding Profile Generation in VANET."

[4] S. Khan, I. Sharma, M. Aslam, M. Z. Khan, and S. Khan, "Security Challenges of Location Privacy in VANETs and State-of-the-Art Solutions: A Survey," *Future Internet*, vol. 13, no. 4, p. 96, Apr. 2021, doi: 10.3390/fi13040096.

[5] A. K. Malhi, S. Batra, and H. S. Pannu, "Security of vehicular ad-hoc networks: A comprehensive survey," *Computers and Security*, vol. 89. Elsevier Ltd, Feb. 01, 2020. doi: 10.1016/j.cose.2019.101664.

[6] O. S. Al-Heety, Z. Zakaria, M. Ismail, M. M. Shakir, S. Alani, and H. Alsariera, "A Comprehensive Survey: Benefits, Services, Recent Works, Challenges, Security, and Use Cases for SDN-VANET," *IEEE Access*, vol. 8, pp. 91028–91047, 2020, doi: 10.1109/ACCESS.2020.2992580.

[7] T. Wang, L. Kang, and J. Duan, "Dynamic fine-grained access control scheme for vehicular ad hoc networks," *Computer Networks*, vol. 188, p. 107872, Apr. 2021, doi: 10.1016/j.comnet.2021.107872.

[8] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "VANet security challenges and solutions: A survey," *Vehicular Communications*, vol. 7, pp. 7–20, Jan. 2017, doi: 10.1016/j.vehcom.2017.01.002.

[9] S. Harrabi, I. ben Jaafar, I. ben Jaafar, and K. Ghedira, "Performance Analysis of Vanets Routing Protocols," 2021, doi: 10.21203/rs.3.rs-487685/v1.

[10] E. Schoch, F. Kargl, and M. Weber, "Communication patterns in VANETs," *IEEE Communications Magazine*, vol. 46, no. 11, pp. 119–125, Nov. 2008, doi: 10.1109/MCOM.2008.4689254.

[11] Y. Ruan and A. Durresi, "A survey of trust management systems for online social communities – Trust modeling, trust inference and attacks," *Knowl Based Syst*, vol. 106, pp. 150–163, Aug. 2016, doi: 10.1016/j.knosys.2016.05.042.

[12] M. Jerbi, S.-M. Senouci, T. Rasheed, and Y. Ghamri-Doudane, "An Infrastructure-Free Traffic Information System for Vehicular Networks," in *2007 IEEE 66th Vehicular Technology Conference*, Sep. 2007, pp. 2086–2090. doi: 10.1109/VETECF.2007.438.

[13] C. Díaz, "Anonymity Metrics Revisited," 2005. [Online]. Available: http://drops.dagstuhl.de/opus/volltexte/2006/483

[14] S. A. Jan, N. U. Amin, M. Othman, M. Ali, A. I. Umar, and A. Basir, "A Survey on Privacy-Preserving Authentication Schemes in VANETs: Attacks, Challenges and Open Issues," *IEEE Access*, vol. 9, pp. 153701–153726, 2021, doi: 10.1109/ACCESS.2021.3125521.

[15] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki, "CARAVAN: Providing Location Privacy for VANET."

[16] Leping Huang, K. Matsuura, H. Yamane, and K. Sezaki, "Enhancing wireless location privacy using silent period," in *IEEE Wireless Communications and Networking Conference, 2005.*, pp. 1187–1192. doi: 10.1109/WCNC.2005.1424677.

[17] M. Li, K. Sampigethaya, L. Huang, and R. Poovendran, "Swing & swap," in *Proceedings of the 5th ACM workshop on Privacy in electronic society*, Oct. 2006, pp. 19–28. doi: 10.1145/1179601.1179605.

[18] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, "AMOEBA: Robust location privacy scheme for VANET," *IEEE Journal on Selected Areas in*

Communications, vol. 25, no. 8, pp. 1569–1589, 2007, doi: 10.1109/JSAC.2007.071007.

[19] J. Freudiger, M. Raya, M. Félegyházi, P. Papadimitratos, and J.-P. Hubaux EPFL, "Mix-Zones for Location Privacy in Vehicular Networks."

[20] B. K. Chaurasia and S. Verma, "Optimizing pseudonym updation for anonymity in VANETS," in *Proceedings of the 3rd IEEE Asia-Pacific Services Computing Conference, APSCC 2008*, 2008, pp. 1633–1637. doi: 10.1109/APSCC.2008.110.

[21] L. Buttyan', T. Holczer, A. Weimerskirch, and W. Whyte'', "SLOW: A Practical Pseudonym Changing Scheme for Location Privacy in VANETs," 2009.

[22] A. Wasef and X. Shen, "REP: Location privacy for VANETs using random encryption periods," *Mobile Networks and Applications*, vol. 15, no. 1, pp. 172–185, Feb. 2010, doi: 10.1007/s11036-009-0175-4.

[23] D. Eckhoff, R. German, C. Sommer, F. Dressler, and T. Gansen, "SlotSwap: strong and affordable location privacy in intelligent transportation systems," *IEEE Communications Magazine*, vol. 49, no. 11, pp. 126–133, Nov. 2011, doi: 10.1109/MCOM.2011.6069719.

[24] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen, "Pseudonym changing at social spots: An effective strategy for location privacy in VANETs," *IEEE Trans Veh Technol*, vol. 61, no. 1, pp. 86–96, Jan. 2012, doi: 10.1109/TVT.2011.2162864.

[25] 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, Nov. 2013, doi: 10.1016/j.jnca.2013.02.003.

[26] 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, doi: 10.1109/LCOMM.2013.070113.122816.

[27] A. Boualouache and S. Moussaoui, "S2SI: A practical pseudonym changing strategy for location privacy in VANETs," in *Proceedings - 2014 International Conference on Advanced Networking Distributed Systems and Applications, INDS 2014*, Nov. 2014, pp. 70–75. doi: 10.1109/INDS.2014.20.

[28] B. Ying, D. Makrakis, and Z. Hou, "Motivation for protecting selfish vehicles' location privacy in vehicular networks," *IEEE Trans Veh Technol*, vol. 64, no. 12, pp. 5631–5641, Dec. 2015, doi: 10.1109/TVT.2015.2487262.

[29] R. Yu, J. Kang, X. Huang, S. Xie, Y. Zhang, and S. Gjessing, "MixGroup: Accumulative Pseudonym Exchanging for Location Privacy Enhancement in Vehicular Social Networks," *IEEE Trans Dependable Secure Comput*, vol. 13, no. 1, pp. 93–105, Jan. 2016, doi: 10.1109/TDSC.2015.2399291.

[30] A. Boualouache and S. Moussaoui, "Urban pseudonym changing strategy for location privacy in VANETs," 2017.

[31] A. Boualouache and S. Moussaoui, "TAPCS: Traffic-aware pseudonym changing strategy for VANETs," *Peer PeerNetw Appl*, vol. 10, no. 4, pp. 1008–1020, Jul. 2017, doi: 10.1007/s12083-016-0461-4.

[32] F. Zidani, F. Semchedine, and M. Ayaida, "Estimation of Neighbors Position privacy scheme with an Adaptive Beaconing approach for location privacy in VANETs," *Computers and Electrical Engineering*, vol. 71, pp. 359–371, Oct. 2018, doi: 10.1016/j.compeleceng.2018.07.040.

[33] P. K. Singh, S. N. Gowtham, T. S, and S. Nandi, "CPESP: Cooperative Pseudonym Exchange and Scheme Permutation to preserve location privacy in VANETs," *Vehicular Communications*, vol. 20, Dec. 2019, doi: 10.1016/j.vehcom.2019.100183.

[34] L. Benarous, B. Kadri, and S. Boudjit, "Alloyed Pseudonym Change Strategy for Location Privacy in VANETs," in *2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC)*, Jan. 2020, pp. 1–6. doi: 10.1109/CCNC46108.2020.9045740.

[35] L. Benarous, S. Bitam, and A. Mellouk, "CSLPPS: Concerted Silence-Based Location Privacy Preserving Scheme for Internet of Vehicles," *IEEE Trans Veh Technol*, vol. 70, no. 7, pp. 7153–7160, Jul. 2021, doi: 10.1109/TVT.2021.3088762.

[36] L. Benarous and B. Kadri, "Obfuscation-based location privacy-preserving scheme in cloud-enabled internet of vehicles," *Peer PeerNetw Appl*, vol. 15, no. 1, pp. 461–472, Jan. 2022, doi: 10.1007/s12083-021-01233-z.

[37] H. Zhong, J. Ni, J. Cui, J. Zhang, and L. Liu, "Personalized Location Privacy Protection Based on Vehicle Movement Regularity in Vehicular

Arslan Akhtar Joyo received the bachelor's in Telecommunication Engineering from Quaid e Awam University of Engineering, Science & Technology (QUEST), Pakistan in 2020. He is currently pursuing master's degree in computer communication and networking from Quaid e Awam University of Engineering, Science & Technology (QUEST), Pakistan.

Fizza Abbas received her Bachelor's Degree in Computer System Engineering from Quaid-e-Awam University of Engineering, Science and Technology, Pakistan in 2007. She received her Master's in Communication System and Networks from Mehran University, Pakistan in 2011. She received her Ph.D. in Computer Engineering from Hanyang University, South Korea in 2017. Her research interests are security and privacy in social network services, mobile social networks, cloud computing, mobile cloud computing and vehicle ad hoc networks (VANETs). She has more than 15 years of teaching experience and working as Associate Prof. in Quest Pakistan.

Rafia Naz Memon received her Bachelor's Degree and Master's Degree from Mehran University, Pakistan. She received her Ph.D degree from Malaysia. She has more than 16 years of teaching experience and working as Associate Prof. in Quest Pakistan.

Irfana Memon received her Bachelor's Degree in Computer System Engineering from Quaid-e-Awam University of Engineering, Science and Technology, Pakistan. She received her Master's and PhD from France, in 2013. She has more than 16 years of teaching experience and working as Associate Prof. in Quest Pakistan.

Sajida Parveen received her Bachelor's Degree in Computer System Engineering from Quaid-e-Awam University of Engineering, Science and Technology, Pakistan. She received her Master's degree from Mehran University, Pakistan. She received her Ph.D degree from Malaysia in 2016. She has more than 15 years of teaching experience and working as Associate Prof. in Quest Pakistan.