The Heroes and Villains of the Mix Zone: The Preservation and Leaking of User's Privacy in Future Vehicles

Shreyas Madhav A V[1], Ilavarasi AK[2][0000-0003-1483-4092], Amit Kumar Tyagi[1][0000-0003-2657-8700]

[1]School of Computer Science and Engineering, Vellore Institute of Technology, Chennai

[2]Centre for Healthcare Advancement, Innovation and Research/ SCOPE, Vellore Institute of Technology, Chennai

shreyas.madhav@gmail.com, ilavarasi.shakthi@gmail.com
amitkrtyagi025@gmail.com

Abstract. The privacy of computer users has become more important over the last decade considering the rapid advances that have occurred in the technological industry. Cloud computing, distributed computing, the future internet network, sensor networks, and ad hoc networks, to name a few, are now under assault from a variety of sources, putting the data of millions of users (car users) at jeopardy. Vehicular Adhoc Network (VANET) is a type of Mobile Adhoc Network, having low security infrastructure, faces many serious concerns like security, privacy and trust, etc., over the road network (during travelling). In the last decade, several researchers/scientists have come up with various solutions to these essential concerns. In spite of this, many studies concentrate exclusively on data privacy or identity privacy, and not on location privacy. In 2003, the Mix Zone idea was established to address the issue of privacy for drivers and passengers on highways. When it comes to mixing zones, there are a variety of options, but they all fail due to various benefits and downsides. The main objective of this article is to act as a comprehensive information repository of mix-zones in order to protect the privacy of vehicle occupants from a variety of angles. This paper also discusses a number of interesting concepts, such as prospective improvements or research gaps in the mix zone.

Keywords: Mix-Zone, Privacy Preservation, Vehicular Ad-hoc Network, Leaking Information, Route Confusion, Security Issues.

1 Introduction

Moving automobiles serve as nodes in a mobile network called the Vehicular Ad-Hoc Network (VANET). In order to broadcast data to the network, each car serves as a transmitter, receiver, and router. Once this data is collected, it is put to good use in order to maintain a smooth flow of traffic. For connection with other cars and roadside units, automobiles include a radio interface termed On Board Unit. The Global Positioning

System and other similar technologies are standard equipment in modern vehicles (GPS). In the near future, VANETs will alter the way people drive, but whether or not they do so for the better or worse is totally dependent on the security measures that are put in place. VANETs may aid with traffic flow and roadside safety by reducing congestion. A VANET, on the other hand, has its own set of problems, especially in terms of security and privacy. A VANET is particularly vulnerable to the security risks that come with mobile ad hoc networks, making it a prime target for attacks and service abuse. It's possible that an attacker might manipulate traffic apps and convince people to take another route, thereby freeing up the original route for the attacker's advantage. Using a phoney identity to sign culpability statements would be a more serious example of an attacker trying to avoid being tied to an automobile accident scene. Other less obvious, but no less criminal, uses of network apps include following individuals in their cars. So, there is a clear need for security methods, particularly those that preserve the user's privacy. One of the security aspects of VANET is against its malicious software. In order to execute harmful assaults, the attacker employs malicious viruses to access the vehicle's network through wireless connection. As a result, the Internet of Vehicles' security will be gravely jeopardised since these harmful viruses will disrupt routine vehicle connection while also deceiving or altering data. Figure 1 depicts the architecture of VANETs involved in this process.

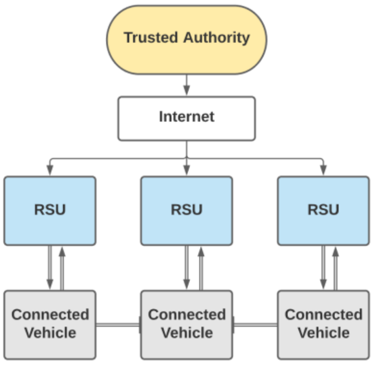

Fig. 1. VANET Architecture

Radio communications interfaces are planned to be added to automobiles in the near future as they become more sophisticated systems. As a result, mobile ad hoc networks may be used to create vehicular networks, often known as VANETs (Vehicular Ad hoc NETworks). Conventional security techniques are not always successful in VANETs because of their mobility, short connection periods, and other unique aspects. The inherent properties of vehicle communication have thus prompted a broad range of research contributions to be lately made available. Data transmission through VANETs relies heavily on its authentication method for both security and privacy. In other cases, such as cloud computing, the abundance of storage and processing resources boosts efficiency. OBUs that store sensitive data must typically validate between 1000 and

5000 messages per second with a network of 100 to 500 cars. Due to the increased computational load and improved traffic flow, cloud-assisted VANET has been a huge asset for OBUs. The metadata stored by cloud providers is often stored in relational databases, which leaves the data privacy of users open to attack.

Using pseudonyms to communicate with each other and the roadside units, VANETs authenticate their vehicles and hide their real identities by using these pseudonyms, which are frequently changed so that the pseudonyms cannot be easily linked together and thus reveal the real identities of the vehicles. A pseudonym change will be of little benefit if past and present pseudonyms are connected in any way. Because of this, a variety of approaches have been suggested to obscure the pseudonym reforms to make it impossible to connect pseudonyms together. When changing your pseudonym in a low-traffic setting, many of these solutions don't completely protect your anonymity.

2 Motivation

VANETs demand a unique grade of requirements to maintain responsibility and accountability of drivers engaged in accidents, traffic infractions, emission standards and anomalies in order to conduct punitive steps if a driver commits any crime. Besides that, location and context-aware services must pin-point user location and preferences to deliver the most detailed, accurate and complete list of customised information. Despite such, sharing of such information presents serious privacy considerations that cannot be overlooked. Also, privacy considerations in vehicular communications are important to give security for the user data from profiling and monitoring. Several aspects effect on the success of mix-zone method, such as user population, mix-zones shape, location sensing rate and spatial resolution, as well as geographical and temporal limits on user movement patterns. None of the current mix-zone techniques address all these aspects properly. Most of the previous mix-zone ideas fail to offer effective mix-zone creation algorithms that are effective for mobile users moving on road networks and yet impervious to timing and transition assaults [26]. The objective of this article is to present a detailed explanation of mix-zones in order to safeguard the privacy of vehicle passengers from a range of aspects. This study also explores a variety of fascinating issues, such as possible enhancements or research gaps in the mix zone [27-30].

3 Privacy Preservation in Autonomous Vehicles

A system for protecting the privacy of one's whereabouts Obfuscation, anonymization, and the addition of fake events are all examples of primitives. Users' paths are obscured and events are mapped with various timings while concealing events. Additional events, such as those of a typical user, are included while creating mock events. It's possible to obfuscate locations by adding noise. Cloaking in space and time are two examples of this. Unlinkability between a place and a user's identity ensures anonymity in anonymization. For example, pseudonymous or pseudonymous identification may be performed via the use of pseudonyms, mix zones, group signatures, and silent periods. In order to keep track of upcoming events, users must register their interest in the application zone. This helps the consumer stay up to speed on the latest product information. A user's location may be readily tracked when they connect directly with an application. Communication between car and application is done through middleware, which prevents a direct link between a vehicle and the network. When a vehicle is in the mix zone, it comes into contact with a vehicle that does not have an application callback. Store and forward networks, such as Mix networks, are used to allow anonymous communication. Prior to transmission, the messages are rearranged based on several variables. As a result, there is no way to connect the two messages that were sent and received. Users' location privacy is protected via a variety of mix zone strategies. Geometry, population, spatial and time resolution, and spatial restrictions in road networks all have a role in how effective a mix zone is. Due to the lack of a location-based service connection and an application call back, it is not possible to link a place to a vehicle's identity in the mix zone. An individual's identity is readily discernible when they communicate with the app in this manner. Middleware acts as a go-between between the car and the application, keeping the user's identity private. The use of middleware protects the confidentiality of the data and the anonymity of the user. The previous and new pseudonyms of a user in a regular traffic environment are simply connected. When a person switches pseudonyms in the mix zone, their identity can no longer be tied to their current location, allowing for unlinkability.

4 Necessity of Mix-Zone

We have identified three main avenues for an attacker to connect pseudonyms:

- The use of non-volatile data (such as unencrypted upper layer identifiers or the radio fingerprint of a unit) to infer a relationship between two messages is an example of an attack based on non-volatile data.
- Use of protocol knowledge (e.g., a vehicle consistently transmits in one time slot, regardless of its pseudonym) to connect messages is an example of a protocol-based attack.
- This kind of attack relies on physical factors and limitations to determine a node's present location, which may then be used to establish a connection between two messages as being from the same node. The perpetrators of this assault have characterised it as a straightforward tracking operation.

As a starting point, we have identified three main avenues for an attacker to connect pseudonyms:

- The use of non-volatile data (such as unencrypted upper layer identifiers or the radio fingerprint of a unit) to infer a relationship between two messages is an example of an attack based on non-volatile data.
- To connect communications, attackers utilise attacks based on protocol information (for example, a car consistently communicates within a certain time slot, regardless of its pseudonym).
- This kind of attack relies on physical factors and limitations to determine a node's present location, which may then be used to establish a connection between two messages as being from the same node. Simple tracking has been used to characterise this attack.

In order to connect a pseudonym, there are three main ways an attacker may go about it. Extra data, such as unencrypted upper layer IDs, or the radio fingerprint of a unit (such as the radio fingerprint of a unit), are utilised to infer a link between two messages.Protocol-based attacks, in which knowledge of the proto-col (e.g., a vehicle consistently transmits at a given time-slot, regardless of its pseudonym) is used to connect messages, notwithstanding the pseudonym's anonymity [6]. The physical parameters and restrictions are used to infer the current location and connect two messages as belonging to the same node, for example, by using the estimated distance travelled and the previous position. The term "simpletracking" has been used to characterise this attack. An attacker might take one of three routes, which we've identified. Pseudonyms for links are as follows: Based on non-volatile data, where extra information is required for an attack. Such as an unencrypted upper layer) does not alter the radio fingerprint of a device, which is used as an identifier [7,8].

A method known as mix-zone was devised to ensure that past and new pseudonyms could not be linked. This kind of zone allows unlinkability by having a large number of users enter in a random sequence, adjust their pseudonyms, and then leave the zone in a different order. The mix-zone concept makes the following assumptions to preserve privacy: k participants must arrive in a mix zone area before any participant may exit the territory. Each participant in the zone spends an unspecified amount of time in the territory, beginning and ending at various points. Transition probabilities follow a uniform distribution. Methods for constructing mixed zones: Based on the mix-zone paradigm [9-14], three building methods have been devised for the development of functional mix-zones. The time window limited method defines a rectangle at the centre of the intersection in a predetermined size. On the basis of this assumption, an anonymity set is created depending on how many people enter the mix-zone at a given moment. There should be a relatively short time frame in which to conduct the experiment. The size of the window is determined by criteria such as the size of the zone, the anonymity level of the user, and the speed of the user. TWB shifted Rectangular Mix-zones include two additional features: First, the rectangle is defined in a shifted manner. A non-rectangular size is described in the TWB NonRectangular mix-zones as well. Using a non-rectangular method eliminates the risk of timing attacks.

To maintain their anonymity, each user talks with the network infrastructure using a pseudonym or their actual name and device number. In order to access location-based services, users first get their location through a positioning system, and then submit this information to the LBS application server. Although pseudonyms may protect a user's true identity, the LBS application server may deduce a user's position or movement path from this information, resulting in a breach of location privacy.

5 Variants of Mix-Zone

The position of a car in a vehicular network is a critical piece of information. It is possible to safeguard vehicle privacy by using a technique known as "pseudonym change," in which a large number of cars collectively adopt different pseudonyms in order to create a "mix zone." But the number of collaborators in the spatiotemporal environment is a factor. Figure 2 showcases the mixzones and their visualization.

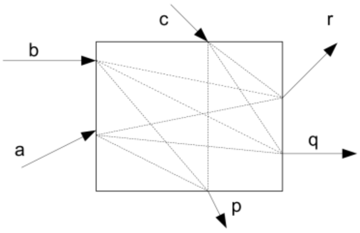

Fig. 2. Mixzone Visualization

MobiMix is a mix-zone architecture for road networks focused on the protection of mobile users' location privacy. MobiMix's solution to location privacy protection is to employ mix-zones, where no programmes may track user movement, in place of spatial cloaking. Certification issuance and pseudonym issuance methods are included in indMZ's pseudonym scheme for vehicular networks. When a vehicle joins a roadside unit, its pseudonym will be L. When a pseudonym is about to expire, the car may create a mix zone by broadcasting beacon signals to the area. The independent mix zone implies that each of the collaborating vehicles will generate some randomised pseudonyms and contribute to the required k-anonymous mix zone. It is possible for the vehicle to create a k-anonymous pseudonym change region even if there is no input from anybody else.

In [30], time-window-based options for protecting location privacy in mix zones are discussed. Based on the mix-zone paradigm, three building methods have been devised for the development of functional mix-zones. The time window limited method defines a rectangle at the centre of the intersection in a predetermined size. On the basis of this assumption, an anonymity set is created depending on how many people enter the mix-zone at a given moment. There should be a relatively short time frame in which to conduct the experiment. The size of the window is determined by criteria such as the size of the zone, the anonymity level of the user, and the speed of the user. TWB shifted Rectangular Mix-zones include two additional features: First, the rectangle is defined in a shifted manner. A non-rectangular size is described in the TWB NonRectangular mix-zones as well.

6 Background Work

Using pseudonyms to hide one's identity in a dedicated infrastructure (DI) system has been suggested by Raya et al. Pseudonyms are fictitious names that are only valid for a short period of time. VANET pseudonyms may be used in a variety of ways [23–24]. For the time being, it has been proved that pseudonyms may be tracked and their genuine identities revealed using various probabilistic models as stated in [5]. Mix zones were a popular way to connect pseudonyms. To describe mix zones, a group of people may alter their pseudonyms together at a secret location, without being connected to each other. Pseudonyms will be harder to connect if the pseudonym shift is concealed in this manner. Dedicated Infrastructures could benefit from the usage of pseudonyms and mix zones (VANETs). There are no significant deployments of the DI technique at this time [1,4,13,25]. Online privacy preservation is an important method for safeguarding the private of moving things. There are a variety of ways to keep location data private. Cloaking, either in time or space, is a common method [3,10,12]. Generalization, in this case, is the process of expanding in both time and space in order to meet the k-anonymity level [16]. k-anonymity refers to the condition of being anonymous among other k things. On the basis of the quality of the data, cloaking can ensure k-anonymity. If you want to hide your position, you'll have to utilise one of two methods: a trusted third party or a group of people updating their locations simultaneously [11, 12]. The latter depends on open and honest communication among the group's members, which calls for mutual trust. Virtual trip lines (VTLs) were introduced by Hoh and Gruteser [3]. Vehicles must update their position when they pass a VTL border, which is sent to the client programme. Because cars do not update their whereabouts outside of VTL areas, the system is unable to collect traffic conditions. Pseudonyms may easily be linked to hacked VTLs if any of the lines are compromised. As a result of the considerable time and effort put into selecting VTLs and making them available to users, the system is not suitable for usage by a large number of people [15]. Location cloaking is used in [11] by the writers to obscure the location of users. As a result, the precise position of the data is obscured by a jumble of temporal and geographical parameters. It ensures k-anonymity in terms of both the temporal and spatial aspects. However, it still depends on a trustworthy third party and reduces the data quality. Using [8], the authors propose a two-way cloaking technique, in which a user submits her cloaked position to an anonymization server, which in turn produces an anonymous cloaking rectangle with k users inside of it[16]. By generalising location to the safe zone, cloaking depends on an untrusted third party to determine the safe region. It is comparable to the technique used by [12] in which users collaborate to construct a secure zone without the assistance of a trusted third party [17-23]. In this approach, users are presumed to be honest and trust each other to determine the safe region.

7 The Mix Zone Network Model

There are two basic kinds of designs for the anonymization methods used in Location Based Servcies (LBS) to improve privacy. [23] Peer to peer and a Trustworthy Third-Party (TTP) server are two different ways of doing this. Mix-Zones [18] may be used to create a real-time anonymity system based on the previous design. Third-party trustworthy servers are the trusted servers of the telecom operator linked with the Location Based Services server and the end user. The anonymization method will be performed only by the TTP, which is expected to maintain complete security over the data it processes [24]. In order for this technique to be effective, the MO's routes must cross. Generally, these intersections are traffic signal junctions on the road networks [25]. Because of this, the intersections of traffic lights are known as Mix-Zones. According to the trusted third-party server that links the MOs with the Location Based Service providers, a Mix-Zone is a particular region. LBS application servers connecting to this trusted server must know the identities of the appropriate MOs. Pseudonyms, rather than real names, should be used for this purpose. Anonymizing all users inside the Mix-Zone further enhances the MO's real-time privacy. A period of time will be set aside for this anonymization to take effect, which corresponds to the length of time it takes for the TTP server to activate the Mix-Zone. In addition, the existing MOs will be re-seudonymized in order to confuse the user's privacy thief. The TTP server informs MOs in advance of their entering the network about the Mix-location Zone's and duration. Figure 3 depicts composition of a gate in a mixzone.

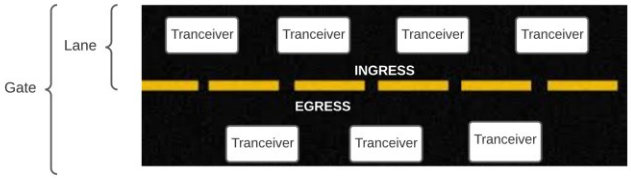

Fig. 3. Gate Composition in a Mix Zone

7.1 Confidentiality Threats

The security of communications in a vehicle network is especially jeopardised by methods like as eavesdropping and broadcast messaging, which may be used to gain position data and read private messages. An insider or an outsider may eavesdrop on other drivers' conversations without their consent, and then utilise that information for their own purposes without the drivers' knowledge. For drivers, privacy and anonymity are critical considerations. Protecting users' privacy by hiding their precise spatial and temporal position is a kind of location privacy. Anonymity may be obtained by making a user's request indistinguishable from those of other users.

7.2 Pseudonym Switching

Location privacy, the capacity to keep others from knowing one's present or previous location, is crucial in VANETs. Whenever vehicles exchange data across communication channels, such data may be uniquely identified by the other cars in the system as originating from that specific car. To be clear: If this identification were to stay constant, other external users might de-anonymize individuals via broadcast messages that correlate to this constant ID, which could be used by other users to identify them. When it comes to location privacy, an adversary would be able to follow the vehicle's position and movement over a period of time if they detected that the same identification was being broadcast along a route. The method VANETs interact must be changed to avoid this breach of privacy.

7.3 Pseudonym Scheme Change Effectiveness

Pseudonyms are being studied for their usefulness in altering schemes, which is a major focus of the study. An adversary's ability to link changes in pseudonyms to the appropriate user is often used to assess this. The pseudonym changing technique is insecure if an attacker is able to determine the connection. Although this thesis does not concentrate on the details of a pseudonym-changing strategy, numerous previous publications have analysed various strategies and their usefulness. The degree of privacy acquired is one of the key issues that will be examined in this thesis. Entering and departing a mix zone affects how much location privacy an individual user has. Pseudonym-changing schemes are necessary for assessing the severity of any other attack threat models that might compromise the system's location privacy [36, 37].

7.4 VANET Cryptographic Mix Zones

To make it more difficult for the enemy to determine who performed a certain action, Chaum [5] proposes anonymous systems. Anonymizing areas in virtual networks (VNs) may be created using a cryptographic approach known as mix-zones [2]. Adversaries can't read communications containing sensitive information, such as vehicle signatures, if they use a pseudonym that can be easily linked to it. This means they can't link two different pseudonyms that are used by the same vehicle at the same time. In order to provide location privacy, anonymizing zones need to be densely populated with cars and unpredictable in their movements. We suggest that preset areas be designated as "mix zones," in which pseudonym modifications must be enforced. Because road crossings are where traffic's speed and direction fluctuate the greatest, the most cars are mixed together.

7.5 CMIX Protocol

The opponent may readily identify mix-zones due to their fixed locations. As a result, communications emanating from the mix-zone region might be intercepted. While in a cryptographic MIX zone (CMIX), all valid cars are given a symmetric key by a roadside unit (RSU) of the mix-zone, and they use this key to encrypt all communications sent and received while in the zone. Once the symmetric key has been established, it may be used. It is possible for nodes entering the mix-zone via a key forwarding technique to acquire the mix-zone key, and then the RSU may switch to a new key using a key update mechanism.

7.6 Private Pseudonym Change Chaff Mechanisms

Cooperative awareness messages are vital for safety and efficiency applications in vehicle communication systems. Passenger privacy may be compromised if these conversations are not properly designed. For this reason, the use of ephemeral credentials such as pseudonyms was recommended, in order to divide up an excursion into unlinkable sections. Encrypted mix-zones allow vehicles to covertly change their pseudonyms during segment transitions. In spite of previous attempts to address the location, design, and procedures of mix zones, attacks on cars entering and existing these zones remain a problem. Earlier techniques primarily looked at homogeneous traffic, ignoring variations in vehicle density caused by changes in the population of drivers, the shape of the route, and even the time of the day. It is dangerous to draw conclusions about the practicality of a new technology based just on anecdotal information. As a result, a unique method that works regardless of vehicle movement patterns has been developed. If there are a sufficient number of fictive chaff vehicles present, the system will create them and broadcast their traces, but otherwise it will remain undetectable. This greatly enhances privacy protection in low-traffic areas, such as suburban areas, and during low traffic times. Since chaff vehicles (and messages) must not interfere with the proper operation of safety applications, the new method ensures that an external attacker cannot tell the difference between real and chaff vehicles.

8 Problem, Issues, and Challenges Today in Mix Zone Network Model

Despite the present tendency, future VANETs and their applications will include new developing technologies that bring new capabilities. Future VANETs face a number of difficult difficulties, some of which are listed below: Control and management of vehicle-to-infrastructure communication networks is a major problem. Vehicular networks should not have intermittent connections owing to high vehicle mobility or significant packet loss. Future VANETs will need vehicles that are both mobile and cognizant of their surroundings in order to function properly. In the event of an emergency, each car in the network should be aware of the location of the other vehicles. Management of heterogeneous smart cars will be necessary in the future, since there will be many of these types of vehicles on the road. Another problem of future VANETs is the management of diverse vehicles and their erratic connectivity. The content and location of a user's data are constantly at danger [31-36]. When automobiles talk to one other, users should be able to choose what information they want to give and what information they don't. Instead of transmitting sensitive data to the cloud for analysis, local examination may ensure privacy. Future VANETs have the task of supporting network intelligence, which is one of the most pressing issues. The edge cloud receives and preprocesses the data acquired by cars in future VANETs before sharing it with other portions of the network, such as standard cloud servers.

9 Possible Enhancement in Near Future towards Mix Zone

The edge cloud receives and preprocesses the data acquired by cars in future VANETs before sharing it with other portions of the network, such as standard cloud servers. In the same way that we're all accustomed with and rely on mobile phones in our daily lives, VANETs have a bright future ahead of them. It's now a component of the government's overall plan. A new form of laser speed camera is being considered by NSW and Victoria police in Australia. This camera can detect mobile phone use and speeding cars from half a mile away [13]. As part of a zero-tolerance campaign against driving crimes, Dorset police in the United Kingdom are using cameras developed by Tele-Traffic UK branded as Concept II. Numerous VANET traffic safety and reliability initiatives are now underway in nations throughout the world. Because of the potential of associating prior and current pseudonyms, privacy-preserving approaches that use shifting pseudonyms might result in privacy leakage and disclose true identities [37, 38, 39, and 40]. Users may change their pseudonyms in secret by using mix zones, however it has been shown that statistical algorithms can trace this pseudonym change under certain conditions.

10 Conclusion

VANETs are a new kind of ad hoc network that establishes communications between smart vehicles, devices and associated infrastructure. Drivers and passengers alike benefit from VANET's enhanced safety and entertainment features. There are a wide variety of threats and assaults that may be launched against automobiles using wireless communication technology. As a result, protecting VANETs is more difficult than securing any other kind of network. In order to maintain one's privacy, this research examines alternative pseudonym tactics and mix zone formation methods. A review of recent studies dealing with VANET privacy, authentication, and secure message distribution was provided in this presentation. We categorised the publications based on the tools and strategies employed in them. We compared and contrasted the procedures in each area and evaluated the benefits and limitations of each. After that, we spoke about some of the difficulties that still need to be resolved. With any luck, the results of this poll will be useful to others doing similar work and will help to clarify some of the remaining questions.

References

1. F. Dotzer, "Privacy issues in vehicular ad hoc networks," In proceedings of the Workshop on Privacy Enhancing Technologies, (2006).
2. B. Amro, Y. Saygin, and A. Levi, "PA-CTM: Privacy Aware Collaborative Traffic Monitoring System Using Autonomous Location Update Mechanism," in 4th ACM SIGSPATIAL International Workshop on Security and Privacy in GIS and LBS SPRINGL 11, Chicago, USA, 2011.
3. B. Hoh, M. Gruteser, R. Herring, J. Ban, D. Work, J. C. Herrera, A. M. Bayen, M. Annavaram, and Q. Jacobson, "Virtual Trip Lines for Distributed Privacy-Preserving Traffic Monitoring," in Proceedings of the Sixth International Conference on Mobile Systems, Applications, and Services, Mobisys'08. 2008, pp. 15-28.
4. G. Calandriello, P. Papadimitratos, J. P. Hubaux, and A. Lioy, "Efficient and Robust Pseudonymous Authentication in VANET," in Proceedings of the Fourth ACM International Workshop on Vehicular Ad Hoc Networks Vanet'07, New York, NY, USA, 2007, pp. 19-27.
5. L. Buttyan, T. Holczer, and I. Vajda, "On the effectiveness of changing pseudonyms to provide location privacy in VANETs," in Security and Privacy in Ad-hoc and Sensor Networks. LNCS, 4572, Springer- Berlin, 2007, pp. 129-141.
6. E. Fonseca, A. Festag, R. Baldessari, and R. Aguiar, "Support of anonymity in VANETs - Putting pseudonymity into practice," in 2007 IEEE Wireless Communications & Networking Conference, WCNC Hong Kong: IEEE, 2007, pp. 3402-3407. International Journal of Network Security & Its Applications (IJNSA) Vol. 10, No.1, January 2018 20
7. A. R. Beresford and F. Stajano, "Mix zones: User privacy in location-aware services," in Second IEEE Annual Conference on Pervasive Computing and Communications Workshop, 2004, pp. 127- 131.
8. H. B. Hu, J. L. Xu, and D. L. Lee, "PAM: An Efficient and Privacy-Aware Monitoring Framework for Continuously Moving Objects," IEEE Transactions on Knowledge and Data Engineering, vol. 22, pp. 404-419, Mar 2010.
9. B. Hoh and M. Gruteser, "Protecting location privacy through path confusion," in First International Conference on Security and Privacy for Emerging Areas in Communications Networks, Proceedings, 2005, pp. 194-205.
10. C. Y. Zhang and Y. Huang, "Cloaking locations for anonymous location-based services: a hybrid approach," Geoinformatica, vol. 13, pp. 159-182, Jun 2009.
11. B. Gedik and L. Liu, "Protecting location privacy with personalized k-anonymity: Architecture and algorithms," IEEE Transactions on Mobile Computing, vol. 7, pp. 1-18, Jan 2008.
12. C. Y. Chow, Chi-Yin, M. Mokbel, and X. Liu, "A peer-to-peer spatial cloaking algorithm for anonymous location-based service," in Proceedings of the 14th annual ACM international symposium on Advances in geographic information systems Arlington, Virginia, USA: ACM, 2006.
13. M. Gerlach and F. Guttler, "Privacy in VANETs using changing pseudonyms - Ideal and real," in IEEE 65th Vehicular Technology Conference, 2007, pp. 2521-2525. [14] J. Freudiger, M. Raya, and M. Felegyhazi, "Mix-Zones for Location Privacy in Vehicular Networks," in ACM Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS), Vancouver: Canada, 2007.
14. M. Raya, P. Papadimitratos, and J. P. Hubaux, "Securing vehicular communications," IEEE Wireless Communications, vol. 13, pp. 8-15, Oct 2006.
15. P. Samarati, "Protecting respondents' identities in microdata release," IEEE Transactions on Knowledge and Data Engineering, vol. 13, pp. 1010-1027, Nov-Dec 2001.

16. A. R. Beresford and F. Stajano, "Location privacy in pervasive computing," IEEE Pervasive Computing, vol. 2, pp. 46-55, Jan-Mar 2003.
17. Amit Kumar Tyagi, S U Aswathy, Autonomous Intelligent Vehicles (AIV): Research statements, open issues, challenges and road for future, International Journal of Intelligent Networks, Volume 2, 2021, Pages 83-102, ISSN 2666-6030. https://doi.org/10.1016/j.ijin.2021.07.002.
18. Sampigethaya, K., Huang, L., Li, M., Poovendran, R., Matsuura, K., Sezaki, K.: Caravan: Providing location privacy for VANET. In: ESCAR 2005. Proc. of 3rd workshop on Embedded Security in Cars, Cologne, Germany (2005)
19. A. R. Beresford and F. Stajano, "Mix zones: user privacy in location-aware services," Pervasive Computing and Communications Workshops, 2004. Proceedings of the Second IEEE Annual Conference on, 2004, pp. 127-131
20. Qiang Xu, Rong Zheng, Walid Saad, Zhu Han:Device Fingerprinting in Wireless Networks: Challenges and Opportunities. IEEE Communications Surveys and Tutorials 18(1): 94-104 (2016) International Journal of Network Security & Its Applications (IJNSA) Vol. 10, No.1, January 2018.
21. Julien Freudiger, Reza Shokri, and Jean-Pierre Hubaux. 2009. On the Optimal Placement of Mix Zones. In Proceedings of the 9th International Symposium on Privacy Enhancing Technologies (PETS '09), Ian Goldberg and Mikhail J. Atallah (Eds.). Springer-Verlag, Berlin, Heidelberg, 216-234.
22. Xiaoling Zhu, Yang Lu, Benhong Zhang, and Zhengfeng Hou, “A Distributed Pseudonym Management Scheme in VANETs,” International Journal of Distributed Sensor Networks, vol. 2013, Article ID 615906, 9 pages, 2013. doi:10.1155/2013/615906
23. Hari Vasudevan, Abhijit R. Joshi, Narendra M. Shekokar, Nirav J. Patel, Rutvij H. Jhaveri, International Conference on Advanced Computing Technologies and Applications (ICACTA)Trust Based Approaches for Secure Routing in VANET: A Survey, Procedia Computer Science, Volume 45, 2015, Pages 592-601, ISSN 1877-0509, http://dx.doi.org/10.1016/j.procs.2015.03.112
24. Jibi Abraham, Vishal Bhatnagar, Navjot Kaur, Sandeep Kad, 1st International Conference on Information Security & Privacy 2015A Review on Security Related Aspects in Vehicular Adhoc Networks, Procedia Computer Science, Volume 78, 2016, Pages 387-394, ISSN 1877-0509, http://dx.doi.org/10.1016/j.procs.2016.02.079.
25. Amit Kumar Tyagi and N. Sreenath, A Comparative Study on Privacy Preserving Techniques for Location Based Services, British Journal of Mathematics & Computer Science, Vol.: 10, Issue.: 4, 2015
26. Freudiger J, Raya M, Félegyházi M, et al. Mix-zones for location privacy in vehicular networks. ACM Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS), 2007:1-7.
27. Carianha A M, Barreto L P, Lima G. Improving location privacy in mixzones for VANETs. Performance Computing and Communications Conference (IPCCC), IEEE 30th International, 2011:1-6.
28. Palanisamy B, Ravichandran S, Liu L, et al. Road network mix-zones for anonymous location based services. Data Engineering (ICDE), IEEE 29th International Conference on, 2013: 1300-1303.
29. Ying B, Makrakis D, Mouftah H T. Dynamic mix-zone for location privacy in vehicular networks. IEEE Communications Letters, 2013, 17(8): 1524-1527.
30. Li, X., Liu, P., Zhang, S., & Xie, Y. (2022). An improved secure and efficient group key agreement scheme in VANETs. International Journal of Communication Systems, 35(3), e5025.

31. Didouh, Ahmed, Yassin El Hillali, Atika Rivenq, and Houda Labiod. "Novel Centralized Pseudonym Changing Scheme for Location Privacy in V2X Communication." Energies 15, no. 3 (2022): 692.
32. Memon, Imran, Hina Memon, and Qasim Ali Arain. "Pseudonym changing strategy with mix zones based authentication protocol for location privacy in road networks." Wireless Personal Communications 116, no. 4 (2021): 3309-3329.
33. Al-Marshoud, Mishri Saleh, Ali H. Al-Bayatti, and Mehmet Sabir Kiraz. "Improved Chaff-Based CMIX for Solving Location Privacy Issues in VANETs." Electronics 10, no. 11 (2021): 1302.
34. Jan, Sagheer Ahmed, Noor Ul Amin, Mohamed Othman, Mazhar Ali, Arif Iqbal Umar, and Abdul Basir. "A Survey on Privacy-Preserving Authentication Schemes in VANETs: Attacks, Challenges and Open Issues." IEEE Access 9 (2021): 153701-153726.
35. Abi Sen, Adnan Ahmed, Ayman Alnsour, Sara Abdulaziz Aljwair, Sara Saad Aljwair, Hissah Ibrahim Alnafisah, and Beshayr Ali Altamimi. "Fog Mix-Zone Approach for Preserving Privacy in IoT." In 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom), pp. 405-408. IEEE, 2021.
36. Nair, Meghna Manoj; Tyagi, Amit Kumar "Privacy: History, Statistics, Policy, Laws, Preservation and Threat Analysis", Journal of Information Assurance & Security. 2021, Vol. 16 Issue 1, p24-34. 11p.
37. Tyagi, Amit Kumar; Nair, Meghna Manoj; Niladhuri, Sreenath; Abraham, Ajith, "Security, Privacy Research issues in Various Computing Platforms: A Survey and the Road Ahead", Journal of Information Assurance & Security. 2020, Vol. 15 Issue 1, p1-16. 16p.
38. Tyagi A.K., Kumari S., Fernandez T.F., Aravindan C. (2020) P3 Block: Privacy Preserved, Trusted Smart Parking Allotment for Future Vehicles of Tomorrow. In: Gervasi O. et al. (eds) Computational Science and Its Applications – ICCSA 2020. ICCSA 2020. Lecture Notes in Computer Science, vol 12254. Springer, Cham. https://doi.org/10.1007/978-3-030-58817-5_56
39. A.Mohan Krishna, Amit Kumar Tyagi, S.V.A.V.Prasad "Preserving Privacy in Future Vehicles of Tomorrow", JCR. 2020; 7(19): 6675-6684. doi: 10.31838/jcr.07.19.768
40. Nair, M.M., Tyagi, A.K. (2022). Preserving Privacy Using Blockchain Technology in Autonomous Vehicles. In: Giri, D., Mandal, J.K., Sakurai, K., De, D. (eds) Proceedings of International Conference on Network Security and Blockchain Technology. ICNSBT 2021. Lecture Notes in Networks and Systems, vol 481. Springer, Singapore. https://doi.org/10.1007/978-981-19-3182-6_19