# PRESERVING PRIVACY IN FUTURE VEHICLES OF TOMORROW

**A.Mohan Krishna[1], Amit Kumar Tyagi[2], S.V.A.V.Prasad[3]**

[1]Department of Computer Science and Engineering, Lingaya's Vidyapeeth, Faridabad, Haryana, India.
[2]School of Computing Science and Engineering, Vellore Institute of Technology, Chennai, Tamilnadu, India.
[3]School of Engineering and Technology, Lingaya's Vidyapeeth, Faridabad, Haryana, India.

Email: [1]amkrishna@hotmail.com, [2]amitkrtyagi025@gmail.com, [3]prasad.svav@gmail.com

Received: 14 April 2020 Revised and Accepted: 8 August 2020

**ABSTRACT:** With the rapid development in autonomous industries, very soon connected and autonomous vehicles will be giving a new face to our transportation system and re-shape our cities. Future vehicles equipped with their smart technology are likely to prevent accidents, optimize parking space, lower the traffic congestions and pollution. Such services will be provided by using different types of sensors and wireless interfaces that are connected to other vehicles through internet. Connected future devices like internet of things/ internet connected things are vulnerable to serious unwanted attacks which might cause adverse effects on passengers and therefore concerns of security as well as privacy needs to be resolved in the future vehicles. Privacy is a concern because functionality of the vehicle is controlled by Electronic Control Units (ECUs) that are fully programmable to track location. As vehicles become more programmable, complex and interconnected, they are likely to become more vulnerable to physical and cyber-attacks. This paper attempts to explore the methods for preserving personal information of vehicle user in autonomous vehicles, and making vehicles tamper-proof against such attacks. We will be reaching this aim by developing preserving techniques to secure each component and sharing pseudonyms in mix zones for providing anonymity of the vehicle's electronic architecture. We preserve privacy of user's in future autonomous vehicles by using pseudonym mechanism in mix-zone over the road network. Simulation results shows that our approach yield efficient and reliable results.

**KEYWORDS:** Preserving Privacy, Security, Future Vehicles, Mix-zone, Autonomous Systems, and Cyber-Attacks.

## I. INTRODUCTION

Vehicular Ad-hoc Network consists of three main entities, i.e., On Board Units (OBUs), Road Side Units (RSUs) and Trusted Authority (TA) [1]. Modern wireless enabled high-technology devices like anti lock-brake system (ABS), Electronic brake system(EBS), Global positioning system(GPS) have made the vehicles to behave in intelligent manner and thus making self-reliant Vehicular Ad-hoc Network (VANET). Each vehicle in VANET have two modes of data transmission: Vehicle to Vehicle(V2V) and Vehicle to Infrastructure(V2I) [23, 15], which is also referred as inter vehicle communication and vehicle to infrastructural communication. Fig. 1 depicts the communication of V2V and V2I including RSUs, TAs. If Vehicular Communication Systems (VCS) dysfunction even a minute due to unauthenticated modification of data or system error, then it will be disastrous for both drivers and passengers. VANET bargains a distinct set of requirements in order to have consistent reliability, pin-point user location and preferences. It is expected to provide protection for the user data, which might be used by adversaries to create profile or tracking since privacy is a major concern for any vehicle user. Criticality of time factor in VANET applications is grossly diversified because safety related messages needs to delivered quickly whereas security enforcing algorithms are highly time consuming. Therefore security concerns and also quick transmission concerns are very vital to be observed in VANETs while architects design sophisticated systems.

Undoubtedly security is an important major concern [4] in the design and development of such sophisticated systems but other factors that demand equal attention are authentication, integrity, accountability, non-repudiation, restricted credentials usage, credential revocation, and data consistency. Concerns that require special consideration in security are anonymity, conditional privacy, confidentiality, unlinkability, minimum disclosure, distributed resolution and perfect forward secrecy. In addition, some of the system's mandatory facts to be thought about while designing VANET are scalability, storage requirements, availability, real-time requirements and robustness [26, 5, and 8]. Issues of privacy and accessibility can be handled by any one of the security approaches (i) anonymity as a service i.e group signature (ii) pseudonym authentication. The former technique enables every individual identity in the group to produce a signature, keeping its anonymity promised.

This signature scheme has two components: a group's manager who is accountable for key distribution and a group member responsible for without other members being able to identify the exact identity of sender. In pseudonymous authentication method, initially system stores various pseudonym certificates, followed by choosing randomly one out of the available certificates at a time. In this method, instantaneous identification varies with time by using Trusted Authority (TA) and therefore, an attacker will find it very hard to locate a vehicle. Because of change in the certificate, a hacker may not be able to connect the former and later certificates, which is nothing but loosing the trace of the vehicle. Cryptograph methods are utilized to maintain data uniqueness and integrity includes Message Authentication Code (MAC). Pseudonym is one of the common approach to achieve such type of anonymity [11].

Adversaries are a group of people or an individual, who threaten the security and privacy of a given system [23, 11]. Various types of adversaries present in VANET are (i) External and internal identity adversaries, (ii) Passive and active adversaries depending on influence on user's behavior, (iii) Local, extended and global adversaries depending on limit of territorial effect and independent and colluding adversaries. In VANET applications, security attacks may occur on application layer, transport layer, network layer and physical layer. Security attacks on transport layers include movement tracking, impersonation attack, sybil attack, information block and malicious vehicle [8].

**Security and privacy:**

In any electronic framework, security is one of the concerns and therefore, it has to be ensured in all situations for building confidence. On another side, privacy is required to be maintained for any data which is communicated or collected in the form of motion and/or rest in VANET applications. Privacy and Security have different meaning depending on the context but they are inseparably related [2]. Security can both be an ally and also an enemy to privacy. Though privacy and security seem to complement each other, privacy has a socialistic perspective while security has a technical perspective. The relationship between them is that the security technologies might provide mechanisms by which privacy can be ensured. Privacy and Security are two important integrated issues in the deployment of every technology dealing with data and their inherent meanings are associated with the context. If two nodes want to communicate each other, the level of trust worthiness of two nodes must be high enough to continue the communication process [7]. For understanding purpose, consider an instance of data stored in any device. It is not possible to alter the data which is stored in read only device whereas if it is in transit, some of such data can be replaced in the midway by breaching the network security protocols before it reaches the destination. Hence security and confidentiality needs to be ensured during transmission over a network. Security is the degree of confrontation or protective nature from destruction, valuable goods, humans, nation, institution, etc. On the contrary, privacy refers to "masking oneself from others", i.e., securing ones personal details, location, etc., from illegal access or rather, privacy refers to certain information which everyone would like to keep in incognito mode of theirs. In vehicular ad-hoc network, user's privacy is utmost important while commuting with other users and particularly women passengers as they worry about their personal data and exact location of the vehicle [2, 4].

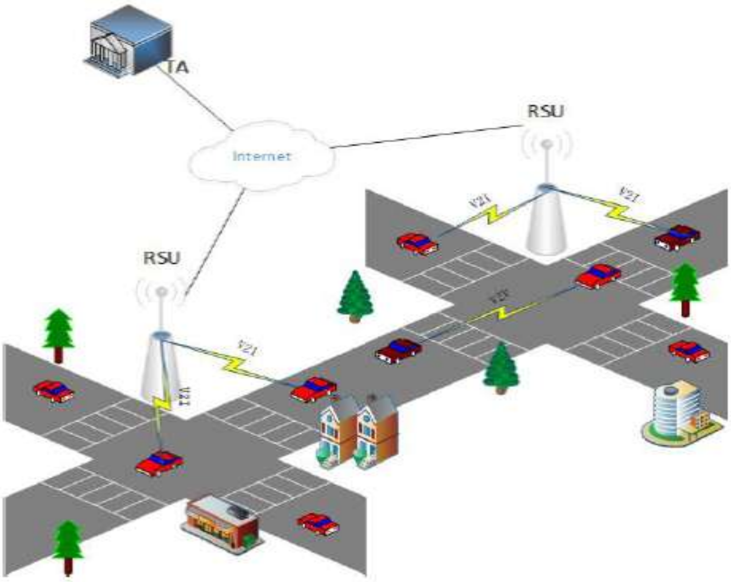

**Fig. 1: Vehicular Ad hoc Network Models**

Privacy is that information which one may not like to share with unknown people or outside world [1, 2, 26 and 4]. It depends on trust and confidence that one possesses on the opposite party and further interrelated with several other factors like authentication or control. Security and privacy are different components that need to be protected throughout a vehicle user's journey. Sometimes, user's journey details should not be revealed even after the completion of journey to any other users. Privacy is four fold in general [1, 2]:

- Identity privacy
- Location privacy
- Data/ information privacy
- Genomic privacy

In this work, we are focusing to preserve location privacy of user's vehicle during the travel and also while accessing any location based services. Location privacy preserving in future vehicles [8] like autonomous cars, hybrid intelligent vehicles, autonomous intelligent vehicles, intelligent transportation systems, etc., is too complex procedure and particularly privacy of a user in that vehicle is a serious issue which has to be protected by efficient and robust solutions.

**Mix Zone:**

Mix zone is a virtual intersection in the middle of two parallel roads to confuse an attacker or a tracker who is tracking without consent, and the vehicle's real route is only processed by a proxy server [10]. Mix-zone may also be constructed dynamically according to the vehicle's request which is generally referred in the literature as dynamic mix-zone. Fig. 2 shows a simple structure of a mix zone and procedure of moving and sharing pseudonyms inside the mix zone.

A.K. Tyagi et al in [4] have elaborated the differences between security and privacy. Our work mainly focused on preserving privacy for the vehicles.

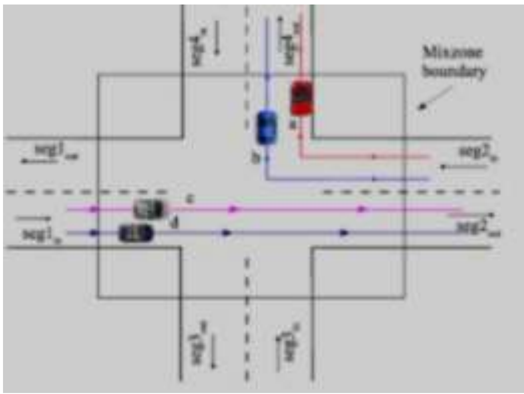

**Fig. 2: Pictorial Representation of a Mix – Zone [11] using Vehicles**

Remaining sections of this paper are organized as follows. In Section 2, we have identified several challenges and opportunities in current and future vehicles. Section 3 discusses our motivation behind this research by highlighting the privacy concerns of the passenger during their travel. Section 4 discusses several practical issues of smart era with a specific concerns to transportation sector. In section 5, we have reviewed the work of previous researchers and in Section 6, we have defined the research problem. In section 7, we have described the proposed solution as how the planned research objectives can be achieved. Section 8 focuses on the simulation exercises that we have carried out and analysis of the simulation results. Section 9 concludes this paper with some important identified research gaps for future research.

**Challenges And Opportunities In Current And Vehicles Of Tomorrow**

In near future, major changes are anticipated in transportation sector for addressing the growing demands of human population due to increase in their earning potential and technological advancements. Exponential increase in the number of vehicles hitting the roads daily is likely to pose several types of difficulties, issues and challenges. Further, very soon such issues are bound to multiply and situation might become worse, if suitable solutions are not implemented. A. K. Tyagi et al [8], have listed out few important concerns, issues, challenges and opportunities with regards to future vehicle and we are augmenting that list.

Negative impact of automobiles on modern life: Apparently the comforts provided by automobiles made us to feel that everything is fine but listed below are some of the negative impacts of automobiles:

- Expenses for fuel, maintenance, insurance, registration, taxes etc.
- Deaths and Injuries

- Urban sprawl.
- Traffic congestion leading to wastage of fruitful time
- Pollution impacting health of human beings.

The future of automobiles: Future vehicle may belong to any of the following categories:

- Hyperloop: It is the reinvention of the transport system to eliminate unwanted wastage of time and distance which will be a reality very soon. Travel speed on the road may go up which can be approximately equivalent to Flight travel. Thousands of passengers can travel at a time.
- Flying cars: It has a high frequency and its top speed increases to 180 km/hour, and its range drops to 500 km (310 miles). Some times only single passenger can travel.
- Electric Planes: Going back and forth in air made taxis for making regional flights more affordable and environmentally friendly.
- Automatic cars: Features of automated mode of transmission will soon be a reality where the computational facilities installed within the vehicle can change the gears based on the requirement. Technology is improving to make the vehicles as fuel efficient.
- Electric cars: These are immediate requirement as electric cars are expected to replace petrol or diesel cars which is a solution for the major concern of high carbon emissions. Banning petrol and diesel vehicles might reduce gigaton of Carbon dioxide emissions across the globe. The running cost of an electric car is expected to be much lesser compared to petrol and diesel cars.
- Smart hybrid vehicle: Most of the existing vehicles on the road fall under this category. Over a period, majority of the automobile manufacturers have improved their product line for energy consumption and output power. Changing a car from economy to sport or luxury or off-road is an example.
- Hybrid electric vehicles: These are mostly combined with other models and especially in race cars. They can support high accelerations for initial pickup with electric motor as well as supporting to reach top speeds with fuel run engines.

In near future, vehicles are likely to be correlated with many Internet of Things (IoTs) devices/ smart devices (called as Internet of Vehicles) and we will be observing several significance changes.

- Design
- Materials
- Mechanical Efficiency
- Fuels (CNG, Electric cars, Hydrogen, etc.)
- Communications
- Roads and highways (Driver Safety, Fuel Economy)
- Safety

Note that the Internet of Vehicles (IoV) is a distributed network that supports the use of data created by connected cars and Vehicular ad hoc networks (VANETs) [8, 9]. In Internet of Vehicles, communicated data is being stored in the cloud and retrieved from the same. Some examples of IoV are: Connected vehicles, Autonomous vehicles, Hybrid electric vehicles, Smart hybrid vehicles. In the coming smart era, transportation sector is likely to transform the behavior of human population as everyone wants to move from one place to another with and without any definite objectives.

**The Car of tomorrow (CoT)/ Vehicle of Tomorrow**

It would be quite a big leap we are going to have from today's automobiles to that of future's. Self-driving vehicle [8] will be at the pinnacle, thanks to their fuel efficiency, eco-friendliness, safety, precision and luxury. The transition of our today's automobiles may not be quick and it might take a decade or two to completely transform our automobile sector. Building new services for new vehicles might take even longer, since politics and other issues always exist to damp the process. However, economic policies of few governments have created large number of jobs and enhanced the purchasing power and hence the pace of our advancement is bound to increase, which makes our dream a reality.

**Now, here a big question arises "Can we trust our vehicles?"**

Before answering this question, one may refer to any daily news paper to assess the gravity of this topic and particularly judge the cruel methods adopted by human beings while committing crime. While discussing about automotive security, most people restrict the topic to protecting cars from thieves. But with the emergence of automated driving, fast expanding connectivity options and ever-increasing complexity, vehicles are vulnerable to various kinds of cyber-attacks also. In the new environment, vehicles need more protection than ever before. Future vehicles are inbuilt with Internet of Things (IoTs) [8, 6], which works based on sensors, actuators etc.

These sensing devices may record information or track footprints of vehicle users during travelling along the highway which can be misused. Research communities have been addressing such issues and automobile industry would not have progressed to this stage if these concerns would not have resolved.

### Environmental concerns

Society is looking for economically good solutions which make transport aesthetically pleasing rather than a distress. We are looking for better solutions for transport without further disturbing the nature. Such solutions should respect the nature, air, water, land, and other living beings as well while integrating technology.

### Innovating Tomorrow's Drive

Urban areas are expanding and traffic congestion in them is growing. Increased vehicle count has become another issue, making it challenging to secure driver and passenger safety. With every second passing, natural factors like air and sound are becoming more polluted and efforts are nevertheless being made to convert the lifestyle of automobile fashion to make our transport more efficient at the same time less costly, both environmentally and technologically. It is undeniable that challenges are evolving with us while exploiting nature.

### Motivation

Future vehicles are necessary for making human life comfortable, convenient and easier to live. Today autonomous vehicles are the primary objectives for many research communities and they are focusing in building autonomous vehicles which can move with a high speed to cover long distances in shortest span of time. However, sensing devices like internet of things or internet connected things may track user's movement and also record communication of passengers for their personal use. It is also possible that such information may be leaked to other malicious users by these smart devices or sensing devices, or an attacker may breach into some autonomous car systems and may steal some sensitive information of passengers. Even a service provider who provides service on road may also reveal the personal information of vehicle users to unknown persons for malicious purpose. In other words, service providers are likely to use such information without taking consent of the vehicle users for their personal benefits. Hence, leakage of personal passenger information in vehicular ad-hoc network's applications is a serious issue and require efficient algorithms from computer science research communities to stop such vulnerabilities. In the previous decade, many researchers have attempted but due to high mobility and system updating process at different intervals, they were not able to protect the information against few specific type of attacks like linking, timing, transition, Sybil, etc. Hence, this is still an open area for research and appropriate methods needs to be explored for preserving privacy and security of vehicle users from such critical attacks.

### Issues In Smart Era And Their Applications In Transportation Sector

As we are looking for major changes in automobile industry, attacks on privacy are also increasing in this sector on the similar rate. In the recent times, Internet of Thing (IoTs)/ smart things are being extensively used in VANET to provide reliable communication. IoT devices have many layers for communication and particularly for circulating packet form source to destination. Ray P.P in [22] described the architecture of Internet of Things and A. K. Tyagi et al[6] have observed that the attacks on Network layer includes location disclosure, trajectory disclosure, packet dropping, fabrication attack, and wormhole attack. Security attacks on physical layer includes eavesdropping, On-board/ Vehicle Information tampering or Illusion attack, in-transit traffic tampering attack, jamming attack, denial of service (DoS) attack, and RSU relocation. An attacker is defined as an entity that would breach into another system by breaking security protocols. Different attackers have different impacts on VANETs and broadly they may be categorized as malicious driver, snoopers or eavesdroppers, industrial attackers. Certain comforts built in few Vehicle Control Software(VCS) solutions tempt the passengers to adopt such comforts which is one of the weakest place from where attackers are gaining entry to steal and are successful in breaching privacy of the vehicle users.

### Vehicular network attacks:

Vehicles are released with factory installed On Board Unit (OBU) which will be in contact with various RSUs while travelling on the road [11]. Importantly, in order to have a traceability free trip, there has to be protection for privacy of every OBU. Supporting protection to the privacy of OBU is measurable because RSU, that frequently serves various sets of OBUs, has no need to support protection of privacy. An OBU having single unique identity is prone to be tracked when access is given and hence preserving its privacy is difficult. Thus, giving multiple identities for the same OBU at RSUs is one of the solution that we are proposing in this work. At the same time, the sets of identities kept for OBUs are to be unique from other sets of identities. Nevertheless, it is ensured that such set identifications are stored at the distribution centre are out of reach to RSUs. Multiple Target Tracking (MTT) codes may be triggered to analyze the path of the target using various other measurands. For example, a single OBU may be responsible for connection with the services across multiple RSUs, therefore data is sent to the single destination and such type of issues are solved by plugging in an anonymizer between the OBU and the services. Various types of data is also generated by MTT code to locate a vehicle. Transponders are used to count number of vehicles passing through them. An MTT code will then take the data and narrow down the possibilities to track a vehicle going in other routes. A technique like validating vehicle number with manual identification is very difficult and such physical level tracking can be taken up as a separate research. In summary, many internal or external attacks may harm vehicle users in a bad way, i.e., can control user' vehicles via internet or breaching in embedded devices in vehicles.

**Vehicles of tomorrow/ Future vehicles:**

Over a period, notion of sustainable development is drastically changed as what was sustainable few years ago is no more relevant today and at times it is considered as disastrous. Therefore, pushing limits is no more a good idea; rather we have to create sustainability in our already exploited resources instead of pushing limits. Rebuilding sustainability needs newer techniques, newer resolutions, newer materials and it requires propulsion of the idea of sustainability in all industries which pollute the nature no matter in small or large scale and not merely an automobile sector. The intelligent, connected, electric, automated vehicle [8] presents designers, vehicle developers, materials scientists and production specialists with new tasks, because it opens up new opportunities and allows for new concepts in areas such as the body, chassis, power train and interior. These may require the use of innovative components and combinations of materials, for yielding safe, high-quality and cost-effective results. In addition, the development of new business models particularly on the growth of the sharing society may have major influence on future mobility solutions that are to be designed keeping in view of safety, efficiency, sustainability from the perspective of the entire product life cycle. ATZ live conference titled "Vehicles of Tomorrow 2020" scheduled at Frankfurt, Germany during November, 2020 is a good platform for deliberating such issues comprehensively and the ideas presented in this paper are expected to catch an attention of vehicle manufacturers.

## Related Work

Various attempts made in previous decades for preserving vehicle location privacy have been examined in this section. Many have used Mix zone method and made improvements by considering number of scenarios, and some others have proposed silent periods, swing and swap, pseudonyms, cryptographic approaches for preserving user's privacy. Grutese et al [14] have added the deviation to the application's permissible range within the location based services. In their work, for confusing the tracker, a non-existing path is constructed between two paths which are parallel, and a proxy server processes the actual route of the car. Limitations of this method may not be appropriate in Vehicular Ad-hoc Network but a point of concern is the virtual interactions which makes it difficult to determine the route. Further, it also affects Vehicular Ad-hoc Network in terms of traffic and the discrepancy caused by it. A small interference won't cause too much effect but it might affect the Vehicular Ad-hoc Network privacy of the location. During certain randomly selected times, the vehicle begins transmitting traffic related messages and then updates the username which carrying on the next broadcast contact. In combination with occasional silent times and community interactions, a scheme for protection and privacy of other groups was discovered by Krishna Sampigethaya et al[16] where the vehicles are assigned to manager who broadcasts the routes and the location of the surrounding vehicles are either in the ghost mode or silent mode. These groups question the selfishness of the vehicles who decide to go on silent mode, hence this issue is difficult to resolve. An agent suggested by Florian Scheuer [24] known as a Pro-Mix zone scheme where cars behave as agents who have infrastructural communication that have RSU and develop CMIX by the communication which involves encryption. At intersections that have greater traffic density, they install roadside units (RSUs) that create mix-zones. When the vehicle enters the mix-zone, the roadside unit acquires a symmetric key. A mix of authors such as Palanisamy and Liu [11] addressed the earth portions and the characteristics of road on the mix zone performance of privacy and suggested a different shape mix zone using the TWB-Time window limitation which is better than the regular mix zone timing resistance. Also, Zeng et al [29] had suggested a pseudonym change before the movement of their social spot, which will be recognized as their social spot when they leave, except this pseudonym changes according to time and place. Yuanyuan Pan [28] suggested a strategy that changes the pseudonym by the vehicles surrounding it. George Corser [13] had suggested a location based scheme for preserving privacy but have several limitations. Researchers [1, 2, and 3] have made very exhaustive literature survey on preserving vehicle' user location privacy. Further, several essential and useful techniques for preserving user' privacy are available in [17, 18, 19, 20, 23, and 27].

## Problem Description

As discussed above, future vehicles like autonomous cars, hybrid electric vehicles, vehicles running in Internet of Things (IoTs) based cloud environment, Hyperloop are few names which are considered for improving the quality of human life during their road travel. Some of the factors behind the emergence of autonomous vehicles include:

the need for a driver and driving safety, growth in population, expanding infrastructure, increase in the number of vehicles, efficient time management, resource utilization and optimization. High earning potential of human population has increased the number of vehicles on the roads due to which transportation infrastructure became unmanageable ranging from roads and parking spaces to fuel stations (for fuel engines) and charging stations (for electric engines). In the past few decades, governments have taken serious measures for road safety by introducing both static and dynamic technologies such as closed-circuit television (CCTV) cameras, road sensors, and many more. Vehicular ad-hoc network enable communication among inter vehicles and also with roadside infrastructure and it helps in avoiding traffic congestion, reducing traffic accidents or total number of vehicles or any other similar issues like suggesting alternate routes.

However, to enable such communication among vehicles they may have to disclose some basic information about themselves to the service provider. Such disclosed details may be used in some other applications without taking the consent of the user by the service provider. Further, attacker may provide false information to vehicles and take them to a different route. Incidents like misleading a user, breaching privacy or leaking someone identity or location to other users might occur in future applications of VANET and therefore, protection of such shared information in efficient way required to be addressed. Under no circumstances, such information should not be revealed to any other users. Hence, in this section we have described our research objective as preserving the privacy of vehicle user by protecting the personal information that was disclosed for certain definite purpose.

## Proposed Solution

Reaching this aim by developing preserving methods to ensure security of every component of the system's electronic architecture: ensuring that each Electronic Control Unit (ECU) only executes code that is suitably authenticated; using model learning techniques to develop a framework for automated security testing of ECUs in a way that it scales; securing the vehicle's sensors such as Radar, Lidar and Optical Cameras [8] against signal spoofing, tampering and denial of service attacks which would cause them to output inaccurate readings; and improving the communication protocols between vehicles and between the vehicles and the infrastructure in order to provide authenticity, non-repudiation and privacy while adhering to inflexible real-time constraints.

A pseudonym is an anonymous certificate [11, 18, 23 and 29] that does not reveal any information about real identifier of the vehicle. Based on the architecture, Pseudonyms are either generated or pre-generated. If they are pre-generated, such pseudonyms will be stored in the vehicle's on-board unit. However, B. Palanisamy et al [11] have observed that the position of a vehicle can be tracked if pseudonyms are stored in the vehicle's on-board unit leading to pseudonym linking attack. Further, On Board Unit (OBU) is a semi-trusted computing unit with lower computing power and storage capacity load on the vehicle which is responsible for calculating and issuing traffic-related messages, receiving notification messages from the RSU. We will be utilizing the principles of Blockchain Technology described by Nakamoto, Satoshi[21] for preserving privacy. Communicated messages among users are stored in cloud by adding blocks to a Blockchain with proper encryption after verified by various miners. This Blockchain facility is immutable, transparent, auditable and accessible to all existing users in a public network. A. K. Tyagi et al[9] proposed several improvements to Blockchain technology but most of them are extremely difficult to implement in real life.

To solve the pseudonym change problem in the low density of vehicles, we are proposing mixing in mix zone scheme (mMZ) by specifying a pseudonym scheme for vehicular networks in this work. Each vehicle will have L pseudonyms when it enrolls to a RSU. Just before the expiry of pseudonym, the vehicle can establish an mixing in mix zone which means that the vehicle can still establish a q anonymous pseudonym change region even if the number of collaborative ones is less than q; in the worst case it will establish a mix zone all by itself. Beacon message is adopted to carry the related information of pseudonym change, which are inherently broadcasted in neighborhood periodically. We have evaluated mMZ and other mix zone schemes with respective to performance and location privacy strength in the low density of vehicular networks. It shows that to ensure a q anonymous pseudonym change region, the proposed mMZ scheme takes an average q=2 (not q=1, because one person may not require any protection of privacy) broadcast cost without rely on any other trusted third party. We have also considered the options of authentication after pseudonym change and revocation of pseudonym if the vehicle is compromised. We have used the CMIX protocol for creating cryptographic mix-zones at road intersections wherein vehicles are permitted to change their pseudonyms. The combination of mix-zones into vehicular mix-networks permits the accumulation of unlink ability over the Vehicular network. Vehicle mix-networks rely on the mobility of vehicles to provide location privacy without jeopardizing the efficiency of safety messages.

## Simulation Scenario And Analysis Of Results

For simulation, we have used SUMO and NS-3, Mobility generator as Network Generator, simulation time as 360 min, vehicle density as 20, 000, RSU as 300, map of freeway, road structure as 2-lane road with vehicle moving in bi-directions, road length as 2-50 Km, road width as 12m (3.50m/lane), traffic density as combinations of low, medium and high. We have used speed range 20-200kn/h, total number of parking location 2500 in radius of 400m, CAM generation 0.1s, interval 1 min, pseudonym period 20x, MAC protocol as 802.11, channel bandwidth 80 Mbps, transport protocol UDP, interval at traffic signals as 0.8-0.1ms, waiting time at parking lot 0.5-1.5ms.

**Table 1: Performance Analysis**

| S. No. | Broadcast cost of message (worst and best) | Algorithm | Cryptography Cost | Trusted Third part dependency | Applications in used |
|---|---|---|---|---|---|
| 1 | 0, 0 | MPSVLP | Encryption | Yes | Travelling over road only |
| 2 | P+q, 1+q | AVATAR | Signature Encryption | No | Travelling over road only |
| 3 | 1+q, 1 | indMZ | Encryption | No | Travelling over road only |
| 4 | 1+q, 1+p+q | mMZ | Encryption | Yes | Travelling + Parking |

In table 1, we have assumed the length of the broadcast message as fixed in all three schemes for total times of sending and receiving broadcast messages by future vehicle. We have observed that in MPSVLP scheme [12], control servers need to be deployed in vehicular networks to assist vehicles in mix zone establishment, with the help of expected location the vehicle sends the encrypted request and the control server broadcasts it. If other vehicles also want to cooperate, then they may have to respond to the control server and change their pseudonyms. Such dependency on control server mitigates broadcast cost among vehicles but still needs two times of broadcast by the control server; at the same time, it also increases communication cost between vehicles and the control server. In AVATAR scheme [25], the vehicle broadcasts the request message on its own and due to low density of vehicles it may affect in enlarging the broadcast region and also in resending the request messages. Let the times of resending be q which is uncertain until the vehicle collects q collaborators. Vehicles which want to collaborate have to generate several footprint signatures and dispatch to the request vehicle which then sends the footprint signatures to all collaborators as rewards for their cooperation. Therefore, the broadcasting of message is at least (1 - q) and at most p - q, as depicted in Table 1. In mMZ, the vehicle encapsulates the request in beacon message, which is inherently broadcasted periodically in the region. After pseudonym change, the vehicle encrypts new pseudonym and its randomized versions. Moreover, the vehicle broadcasts "Msgnotify" to notify pseudonym change to the neighbors. The total number of broadcast messages to deal with is at least one and at most (1 -q). Finally, we have observed that verification of broadcast message in creating blocks is less than other existing mechanisms and therefore, privacy has been preserved in future vehicles that are travelling and also in the parking. We have simulated a multiple mix zone de-correlation trajectory privacy models to protect dynamic attack priorities. Vehicles frequently stop either at traffic jam/signal or at their destination. Privacy concerns at such locations is not completely ruled out specially if the destination is public place. Our technique, safe guarded the concern of privacy in such locations. Implementation of multiple mix zones technique has also been studied to come up with facts upon de-correlation trajectory and model's privacy. Mix zone dimensions and attacker's probability measures are what we take into account and (with increase in the mix zones dimension higher goes the probability), the more coordinate privacy we can achieve and obviously, with lower attacker probability metrics. We have observed that our results are relatively better than some of the existing works.

## II. CONCLUSION

In near future, we are set to use smart vehicles which will make people life easier to travel (and live) or moving/ from one place to another. Future vehicles will be enough smart to make early detection and taking decision to avoid any kind of issue like traffic congestion, traffic accidents, etc., over the road networks. However, such efficient services will come after sharing a lot of information with public transportation and authorities. For example, for any accidents (in near future) ambulance number will be dialed automatically and necessary aid will be reach in minimum time. With future or smart/ developed technology, we would be able to save millions of lives. On another side, we will be on a boundary or doubt of losing our personal information (i.e., issue of privacy breach) to such smart/ automated/ future vehicles. For such serious concerns, this article has provided a novel mechanism to preserve the privacy of user's information via sharing pseudonyms inside mix-zones for providing anonymity among users. Our simulation results demonstrated that our proposed approach provides efficient and highly accurate results in compare to existing work related to privacy protection. In near future, this work can be enhanced to address other specific situations like peak hours or having high density of vehicles at traffic signals to provide anonymity and preserving privacy of users along the highway.

## III. REFERENCES

[ 1] Amit Kumar Tyagi and N. Sreenath, “Location privacy preserving techniques for location based services over road networks", Proc. Int. Conf. Communication and Signal Processing(ICCSP), **(2015)** April 02-04**,** pp: 1319-1326.

[ 2] Amit Kumar Tyagi and N.Sreenath, “Future challenging issues in location based services”, International Journal of Computer Applications, vol. 114, no. 5, **(2015)**, pp:51-56.

[ 3] Amit Kumar Tyagi and N. Sreenath, “A Comparative Study on Privacy Preserving Techniques for Location Based Services”, Journal of Advances in Mathematics and Computer Science, vol. 10, no. 4, **(2015)**, pp:1-25. https://doi.org/10.9734/BJMCS/2015/16995

[ 4] Amit Kumar Tyagi, Niladhuri, S., and Priya, R, “Never Trust Anyone: Trust-Privacy Trade-offs in Vehicular Ad-Hoc Networks”, Journal of Advances in Mathematics and Computer Science, vol. 19, no. 6, **(2016),** pp:1-23. https://doi.org/10.9734/BJMCS/2016/27737

[ 5] Amit Kumar Tyagi and Niladhuri, Sreenath, “ISPAS: An Intelligent, Smart Parking Allotment System for Travelling Vehicles in Urban Areas”, International Journal of Security and Its Applications, vol. 11, no. 12 (**2017**), pp:45-64.

[ 6] Amit Kumar Tyagi and Meghna Manoj Nair, "Internet of Everything (IoE) and Internet of Things (IoTs): Threat Analyses, Possible Opportunities for Future", Proc. World Congress on Information and Communication Technologies(WICT- **2019**), December 16-18, Special Issue.

[ 7] Amit Kumar Tyagi, A Mohan Krishna, Shaveta Malik, Meghana Manoj Nair and Sreenath Niladhuri, “Trust and Reputation Mechanisms in Vehicular Ad-hoc Networks: A Systematic Review”, Advances in Science, Technology and Engineering Systems Journal, vol. 5, no. 1, (**2020**), pp:387-402.

[ 8] Amit Kumar Tyagi, “Autonomous Intelligent Vehicles (AIV): Research Statements, Open Issues, Challenges and Road for Future”, Wireless Personal Communications, Springer, **2020** (Communicated).

[ 9] Amit Kumar Tyagi, “Decentralized Everything: A Practical Use of Blockchain Technology in Future Applications”, Mathematical Foundations of Computing, **2020** (Communicated).

[ 10] A.R. Beresford and F.Stajano, “Mix zones: User privacy in location-aware services”, Proc. IEEE Annual Conference on Pervasive Computing and Communications, Workshops, (**2004**), pp:127 - 131.

[ 11] B. Palanisamy and L. Liu, “MobiMix: Protecting location privacy with mix-zones over road networks”, Proc. IEEE Int. Conf. Data Engineering, Hannover, (**2011**), April 11-16, pp: 494-505.

[ 12] B. Ying, D. Makrakis and Z. Hou, "Motivation for Protecting Selfish Vehicles' Location Privacy in Vehicular Networks", IEEE Trans. on Vehicular Technology, vol. 64, no. 12, (**2015**), pp. 5631-5641.

[ 13] George Corser, Fu Huirong, Tao Shu, Patrick D'Errico, WarrenMa, Supeng Leng and Ye Zhu, “Privacy-by-Decoy: Protecting location privacy against collusion and deanonymization in vehicular location based services’, Proc. IEEE Intelligent Vehicles Symposium, Dearborn, Michigan, USA, (**2014**), pp:1030-1036.

[ 14] M. Gruteser and D. Grunwald, “Anonymous usage of location-based services through spatial and temporal cloaking”, Proc. of the International conference on Mobile Systems, Applications and Services, ACM, New York, USA, (**2003**), pp:31-42.

[ 15] Kakan Chandra Dey, Anjan Rayamajh, Mashrur Chowdhury, Parth Bhavsar and James Martin, “Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication in a heterogeneous wireless network – Performance evaluation”, Transportation Research Part C: Emerging Technologies, vol. 68, (**2016**), pp. 168-184.

[ 16] Krishna Sampigethaya, Leping Huangy, Mingyan Li, Radha Poovendran, Kanta Matsuura and Kaoru Sezaki, “Caravan: Providing Location Privacy for VANET”, Proc. of Embedded Security in Cars(Escar), Berlin, Germany, (**2005**), pp:01-15.

[ 17] L. Sweeney, “k-anonymity: a model for protecting privacy”, International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, vol. 10, no. 5, (**2002**), pp:557-570.

[ 18] Lu R., Lin X., Liang X., Member S., Shen X.S, “A Dynamic Privacy-Preserving Key Management Scheme for Location-Based Services in VANETs”, IEEE Transaction Intelligent Transportation Systems, vol. 13, no. 1, (**2012**), pp:127–139.

[ 19] Ashwin Machanavajjhala, Johannes Gehrke, Daniel Kifer, Venkitasubramaniam and Muthuramakrishnan, “l-Diversity: Privacy Beyond k-Anonymity”, ACM Transactions on Knowledge Discovery From Data - TKDD. Vol. 1, no.1 (**2007**), pp. 01-24.

[ 20] N. Li, T. Li and S. Venkatasubramanian, "t-Closeness: Privacy Beyond k-Anonymity and l-Diversity", IEEE International Conference on Data Engineering, Istanbul, (**2007**), pp. 106-115.

[ 21] Nakamoto, Satoshi, “Bitcoin: A Peer-to-Peer Electronic Cash System”, Cryptography Mailing list (**2009**), at https://metzdowd.com. Also available at https://bitcoin.org/bitcoin.pdf

[ 22] Ray, P.P. “A Survey on Internet of Things Architectures”, Journal of King Saud University – Computer and Information Sciences, vol 30, no. 3, (**2016**), pp: 291-319.

[ 23] Sun J., Zhang C., Zhang Y., Fang Y. “An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks”,. IEEE Trans. Parallel Distributed Systems, vol. 21, no.9, (**2010**), pp:1227–1239.

[ 24] Scheuer, Florian & Fuchs, Karl-Peter & Federrath, Hannes. “A Safety-Preserving Mix Zone for VANETs”, Trust Privacy and Security in Digital Business, Springer, (**2011**), pp: 37-48.

[ 25] Suguo Du, Haojin Zhu, Xiaolong Li, Kaoru Ota, and Mianxiong Dong “MixZone in motion: Achieving dynamically cooperative location privacy protection in delay-tolerant networks", IEEE Trans. Vehicular Technology, vol. 62, no. 9, (**2013**), pp: 4565-4575.

[ 26] Sherali Zeadally, Mohamad Badra edited “Privacy in a Digital, Networked World: Technologies, Implications and Solutions”, Book, Springer (**2017**).

[ 27] T. M. Truta and B. Vinay, "Privacy Protection: p-Sensitive k-Anonymity Property", International Conference on Data Engineering Workshops (ICDEW'06), Atlanta, USA, (**2006**), pp: 94-94.

[ 28] Yuanyuan Pan and Jianqing Li, “Cooperative pseudonym change scheme based on the number of neighbors in vanets”, Journal of Network and Computer Applications, vol. 36 no.6, (**2013**), pp: 1599–1609.

[ 29] Zeng Mengjia and Xu Huibin, “Mix-Context-Based Pseudonym Changing Privacy Preserving Authentication in VANETs”, Mobile Information Systems (**2019**), pp: 01-09 https://doi.org/10.1155/2019/3109238