Mix-Zones as an Effective Privacy Enhancing Technique in Mobile and Vehicular Ad-hoc Networks

NIRUPAMA RAVI, C. M. KRISHNA, and ISRAEL KOREN, University of Massachusetts Amherst, Amherst, USA

Intelligent Transportation Systems (ITS) promise significant increases in throughput and reductions in trip delay. ITS makes extensive use of Connected and Autonomous Vehicles (CAV) frequently broadcasting location, speed, and intention information. However, with such extensive communication comes the risk to privacy. Preserving privacy while still exchanging vehicle state information has been recognized as an important problem.

Mix zones have emerged as a potentially effective way of protecting user privacy in ITS. CAVs are assigned pseudonyms to mask their identity; a mix zone is an area where CAVs can change their pseudonyms to resist being tracked.

In order to be effective, mix zone placement must take account of traffic flows. Also, since a mix zone can degrade throughput, mix zones must be used sparingly. Determining the number and placement of mix zones is a difficult dynamic optimization problem. This paper outlines the various approaches recently taken by researchers to deal with this problem.

CCS Concepts: • **Security and privacy → Human and societal aspects of security and privacy**; • **Computing methodologies**;

Additional Key Words and Phrases: location privacy, mix-zones, Location based services, connected and autonomous vehicles, ITS, VANET

1 INTRODUCTION

Intelligent Transportation Systems (ITS), consisting of Connected and Autonomous Vehicles (CAVs), promise significant improvements in safety, trip duration and traffic throughput. By frequently exchanging information about speed, acceleration/braking, and heading, vehicles in congested traffic areas can travel in platoons by coordinating their movements and avoiding “traffic waves" which are detrimental to throughput. Real-time monitoring and dissemination of traffic conditions (including accidents and emergency vehicle activity) can allow traffic to be detoured around bottlenecks as they arise or are anticipated. However, since CAVs require extensive wireless communication, ITS is vulnerable to attackers who might intercept and modify messages, thereby causing chaos, or worse, throughout the system. Monitoring such communication also allows eavesdroppers to track vehicles from journey’s start to end, thereby being a significant privacy risk. To deal with this last problem, vehicles use pseudonyms as identifiers (ID) in their messages. Since the use of the same pseudonym throughout a vehicle’s journey would open the door to start-to-end tracking of a vehicle, *mix zones* are introduced.

A mix-zone is a designated area where vehicles exchange pseudonyms. The definition of a mix-zone includes its location, dimensions, the protocol to be followed while exchanging pseudonyms, and who defines the mix-zone. Either vehicles in the specific area can announce the mix-zone formation or an infrastructure engineer, in which case the Road Side Unit (RSU) will announce the existence of the mix-zone. In the case where vehicles determine mix-zones that are formed in an ad-hoc manner, they are known as ad-hoc mix-zones. The only other way to form mix-zones is infrastructure defined mix-zones, simply referred to as mix-zones.

While mix zones enhance privacy, their existence can degrade traffic performance. To be effective without significantly affecting throughput or trip delay, mix zones must be used sparingly; furthermore, they must take account of traffic patterns while being positioned. Determining the number and placement of mix zones in a road network is a difficult optimization problem that has attracted much attention in recent years; recent approaches developed to attack this problem are the focus of this survey.

In this survey, we cover:

- Taxonomy of mix-zone schemes based on privacy preserving technology.
- The effectiveness of mix-zone schemes in preserving privacy against well-resourced attackers and their impact on security and traffic efficiency.
- Taxonomy of mix-zone placement algorithms.
- Impact of the number of mix zones and their placement on traffic flow.

We organize the paper as follows. In Section II, we delve into related surveys concerning security and privacy issues while also highlighting the unique contributions of this paper. Section III presents a comprehensive overview of the ITS architecture, covering topics such as the pseudonym lifecycle, security requirements, potential attacks, privacy requirements, attacker types, and considerations related to safety applications and traffic efficiency. We critically assess the impact of our pseudonym change scheme on each of these requirements. Moving to Section IV, we compare our pseudonym change strategy with existing alternatives, offering insight into mix-zone schemes and a taxonomy of mix-zone protocols. Section V introduces synchronous multi-vehicle schemes and underscores mix-zones’ efficiency as a pseudonym change strategy, drawing comparisons with other strategies. We thoroughly analyze various mix-zone schemes in the context of different road conditions and their efficacy against varying attacker strengths. Additionally, we investigate the side effects of mix-zone

Authors’ Contact Information: Nirupama Ravi, nirupamaravi@engin.umass.edu; C. M. Krishna, krishna@ecs.umass.edu; Israel Koren, koren@ecs.umass.edu, Electrical and Computer Engineering, University of Massachusetts Amherst, Amherst, Massachusetts, USA.

ACM 0360-0300/2024/4-ART

https://doi.org/10.1145/3659576

schemes on security, safety applications, and traffic efficiency, recognizing the need for multiple mix-zones to ensure privacy in urban settings. In Section VI, we present mix-zone placement algorithms and discuss their strengths and limitations. Section VII delves into open research questions, laying the foundation for further exploration. Finally, in Section VIII, we offer a conclusion summarizing our findings and propose directions for future research.

2 RELATED SURVEYS

Mobile Ad-hoc NETworks (MANETs) and Vehicular Ad-hoc NETworks (VANETs) are both self-configuring networks of mobile devices and vehicles, enabling communication among the individual devices with VANETs or MANETs without relying on the infrastructure. Consequently, both MANETs and VANETs share similar security and privacy issues.

We begin by considering published surveys of security and privacy issues of ITS or Vehicular Ad-Hoc Networks [1–8]. Table 1 lists the coverage each of them provides along the following dimensions: privacy, safety, impact on security, traffic efficiency, and attack diversity. We outline here a sampling of them.

Petit et al. (2015) present a detailed discussion on the pseudonym life cycle and message authentication schemes [8]. However, analysis of privacy-preserving techniques, efficiency against security attacks, safety applications, and traffic efficiency are not within the scope of their paper.

Qu et al. (2015) provide an excellent summary of security and privacy issues in ITS from 2004 to 2015 [6]. They describe security threats, discuss authentication mechanisms, and summarize the tradeoff between security and privacy. However, this survey does not discuss the tradeoff between privacy and traffic efficiency.

Ferrag et al. (2017) survey privacy techniques from 2006 to 2016 for mobile and vehicular ad-hoc networks [9]. They evaluate each privacy measure against privacy and security attacks for each network. However, their coverage ends at 2016.

Boualouache et al. (2018) discuss mix-zone based pseudonym changing strategies [7]. They do not, however, examine the tradeoff between privacy and traffic efficiency.

Asuquo et al. (2018) cover privacy-enhancing techniques and cryptographic solutions in location-based services for vehicular and mobile networks [10]. The survey provides a comprehensive review of location privacy techniques for location-based services. However, analysis of effectiveness of each privacy enhancing technique, safety, resilience against security attacks, and traffic efficiency is not included.

Talat et al. (2019) [5] classify privacy-preserving schemes in vehicular ad-hoc networks into two groups based on the modification type of a basic safety message: a) a vehicle changes its ID, and b) a vehicle obfuscates its location information. The authors evaluate each privacy-preserving technique against diverse criteria such as the CPU load of the On-Board Unit (OBU) of a vehicle and the associated RSU, the performance of road networks, and the performance of location obfuscation techniques. This survey does not, though, analyze tradeoffs of the privacy techniques against traffic efficiency and safety.

Lu et al. (2019) cover the following: a) cryptographic solutions for message authentication and anonymity, b) threats and vulnerabilities of each cryptographic solution, c) survey of privacy attacks, tracking attack algorithms and protection mechanisms, d) trust management systems for RSUs and vehicles, and e) various simulator tools for ITS [11]. While this survey paper covers many security aspects in detail, it does not include a discussion of attacker strength vs. pseudonym change strategies and impact on traffic efficiency and safety.

Babaghayou et al. (2020) categorize pseudonym change schemes from 2005 to 2019 as trigger-based or trigger-free [4]. The trigger-based changes depend upon the location, time, or timing of specific trigger conditions to satisfy requirements such as the availability of enough vehicles wishing to change pseudonyms or having a minimum density of vehicles on the road. Trigger-free schemes are either fixed-location-based or fixed-time-based. However, the side effects of each pseudonym change scheme on safety, computational load, and traffic efficiency, are not considered.

Khan et al. (2021) review the location privacy schemes of vehicles and analyze them against operational and safety issues [3]. They analyze authentication schemes and their associated overheads. While this survey looks at privacy schemes under diverse road conditions and computational overhead, a detailed coverage of mix zone management is not provided.

Mundhe et al. (2021) review existing message authentication schemes including symmetric key cryptography, public key generation-based, ID-based certificate-less, group-signature-based, ring-signature-based and blockchain-based cryptographic schemes [2]. This survey also comprehensively describes, categorizes, and highlights the limitations of various message authentication schemes and discusses the resilience of the schemes against security attacks such as message replay. However, it does not discuss attacks on location privacy.

Suo et al. (2022) list various physical and cyber threats to CAVs including jamming sensors, injecting false signals to mislead LIDAR or ultrasonic sensors, blinding cameras, and so on [1]. The authors mention privacy issues such as false traffic message injection or simulating a ghost vehicle. While this survey is valuable for understanding the state of the art of mitigating physical and cyber threats to CAVs, privacy protection is not its focus.

The above surveys are valuable in highlighting diverse aspects of security and privacy issues in ITS and VANET. However, a comprehensive survey of a) pseudonym changing protocols and their efficiency in preserving privacy, b) their viability across a range of traffic conditions and operating environments, c) tradeoffs against security, safety, and d) limitations against powerful attackers is required. Such a survey is the aim of this paper.

Table 1. Relevance to existing surveys

Survey	Published year	Security risks	Privacy risks	Safety Tradeoff	Traffic Efficiency	Attacker Strength	Road conditions	Focus
[8]	2015	×	✓	×	×	×	✓	A comprehensive survey of pseudonym: its life-cycle, authentication schemes, and pseudonym change strategies.
[6]	2015	✓	✓	✓	×	×	×	Cryptographic solutions tradeoff analysis on security vs. privacy, and safety.
[9]	2017	✓	✓	×	×	×	×	Security and privacy vulnerabilities to privacy schemes for Mobile Ad-hoc networks and VANET.
[12]	2018	×	×	✓	×	×	×	Security and privacy requirements for safety applications.
[10]	2018	×	✓	×	×	×	×	Cryptographic and privacy enhancing techniques for LBS services for vehicular and mobile networks.
[7]	2018	×	✓	✓	×	×	×	Mix-zone based pseudonym changing strategies and their limitations
[13]	2018	✓	✓	✓	×	×	×	Security and privacy schemes, scalability, privacy, communication overhead, latency and computation cost.
[5]	2019	×	✓	×	×	×	✓	Location privacy using pseudonym changing and location obfuscation techniques
[11]	2019	✓	✓	×	×	×	×	Cryptographic solutions their vulnerabilities to security and privacy risks.
[14]	2019	✓	×	×	×	×	×	Cryptographic solutions, their vulnerabilities to security attacks.
[4]	2020	×	✓	×	×	×	×	Pseudonym schemes
[3]	2021	✓	✓	×	×	×	✓	Analysis of authentication schemes against security threats, computation and communication overhead.
[2]	2021	✓	✓	✓	×	×	×	Comprehensive analysis of security schemes and impact on privacy and safety.
[1]	2022	✓	×	×	×	×	×	Physical and cyber security threats and countermeasures
This paper	2023	✓	✓	✓	✓	✓	✓	Tradeoff with Safety Traffic Efficiency Security threats and Countermeasures for mix-zones as PET

3 BACKGROUND

The objective of ITS is to carry heavy loads of traffic safely and efficiently. As noted earlier, this is accomplished by extensive communications: both vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) [jointly referred to as V2X]. In this section, we outline the structure and key operational aspects of an ITS.

3.1 ITS Architecture

Key participants in managing an ITS are the Trusted Authority (TA), Road Side Unit (RSUs), and vehicle On-Board Units (OBUs).

3.1.1 Trusted Authority. The Trusted (or Trust) Authority (TA) is at the apex of the overall system [11, 15]. It controls the registration of vehicles as they join the network and is responsible for issuing security certificates. It manages a database of vehicle information and is aware of the mapping between a vehicle's pseudonym and its real identity. If a vehicle is behaving sufficiently suspiciously, the TA can revoke its security credentials. It monitors the health of RSUs. It is assumed to have significant computational and memory resources.

3.1.2 Road Side Unit (RSU). RSUs are stationary and enable communication between a vehicle and a TA. They report to the TA details of traffic incidents near intersections, road segments, and security violations. An RSU typically connects with the TA through wireline means. When a vehicle starts its journey, it registers with the local RSU for updates of traffic and road conditions. A vehicle initiates

authentication by first connecting to an RSU. It sends its authentication information to the TA through the secure channel established through RSU mediation. In addition, an RSU listens to safety beacons from vehicles and estimates traffic intensity on each road segment. When an RSU receives alerts about traffic congestion or accidents, it validates that information as best it can and then propagates that information to other nearby RSUs in order to suitably alert vehicles that may be approaching the affected region. Also, any notification from the TA concerning malicious vehicles is forwarded to relevant vehicles in the vicinity.

3.1.3 On Board Unit (OBU). Each vehicle has an OBU, which is a computer with access to security credentials stored in a tamper-resistant device. Upon engine start, the OBU registers with the local RSU to forward the vehicle's credentials to the TA which then authenticates the vehicle.

The OBU mediates cooperation between its vehicle and others nearby. When status messages are received from the RSU or neighboring vehicles, the OBU responds by issuing instructions to adjust the speed, throttle/brake setting, and heading to maintain the appropriate inter-vehicle headway. In its turn, it puts together status reports to share with other vehicles and the local RSU.

3.2 Pseudonyms for Communication

Each vehicle periodically transmits status information in the form of a Basic Safety Message (BSM). Figure 1 shows a typical BSM format defined by IEEE 1609.3. A BSM includes the vehicle's identifier, timestamp, and additional information, e.g., location, vehicle size and mass, heading, acceleration, steering angle, and the current throttle and brake status.

Protocol Version	Message Type	Message	Certificate	Signature
1 byte	1 byte	67 bytes	125 bytes	56 bytes

			Vehicle Status										
			Location				Motion						
Message Count	Pseudonym	Time stamp	Latitude	Longitude	Elevation	Position Accuracy	Speed	Heading	Steering Wheel Angle	Acceleration Set4Way	Braking Status	Vehicle Size	Optional Parts I, II
1 byte	4 bytes	1 byte	4 bytes	4 bytes	2 bytes	4 bytes	2 bytes	2 bytes	1 byte	7 bytes	2 bytes	3 bytes	30 bytes

Fig. 1. Basic Safety Message Format

Using an identifier such as the registration number or vehicle identification number (VIN) in the BSM is fatal to privacy. For this reason, vehicles use pseudonyms which can be changed dynamically. This reduces the chances of a vehicle being tracked end-to-end on a journey and also of its being linked to particular individuals.

Figure 2 presents the pseudonym cycle, which consists of generation, assignment, authentication, usage, and removal/revocation phases. Different nodes of the ITS are involved in different phases of the pseudonym cycle. The pseudonym has as its primary purpose the hiding of the vehicle's identity. An attacker can compromise a vehicle's privacy by mapping a pseudonym to a vehicle ID. Hence, only a TA should know the correct mapping. Thus, pseudonym generation, assignment, authentication, and revocation all involve the TA. Vehicles use their assigned pseudonyms and must change them frequently to protect their identity. V2X messages carry important location information or life-saving safety alerts. Each V2X message source requires authentication. Checking the integrity of received messages by vehicles or RSU is crucial and can be done by standard cryptographic techniques such as a) Symmetric key, b) Asymmetric key, c) Group-based, d) ID-based, and e) Blockchain-based [2].

Pseudonym Generation. Two approaches have been developed for using pseudonyms: certificate-based and certificate-less [2]. In certificate-based solutions, vehicles get pseudonyms and corresponding certificates from the TA. In certificate-less cryptographic solutions, the TA provisions vehicles with a Registration ID (RID) at the time of registration. Each vehicle establishes a one-time secure connection to TA through a nearby RSU. TA authenticates vehicle's RID. Vehicle acquires the secret key and public parameters from the TA. Vehicles use the secret key and public parameters to generate a pseudonym and public key; further messages can be encrypted using the secret key.

Pseudonym Assignment. Certificate-based schemes require a periodic update of pseudonyms and corresponding certificates from the TA, adding to the communication load on RSUs and vehicles. By contrast, certificate-less schemes require no communication with RSUs for regular pseudonym assignment, except for one time when vehicle acquires secret keys through a secure channel to TA through RSU.

Pseudonym Usage. As noted earlier, vehicles use pseudonyms to identify themselves to other vehicles and RSUs. Vehicles use pseudonyms when sending periodic safety messages and alerts about traffic or road conditions.

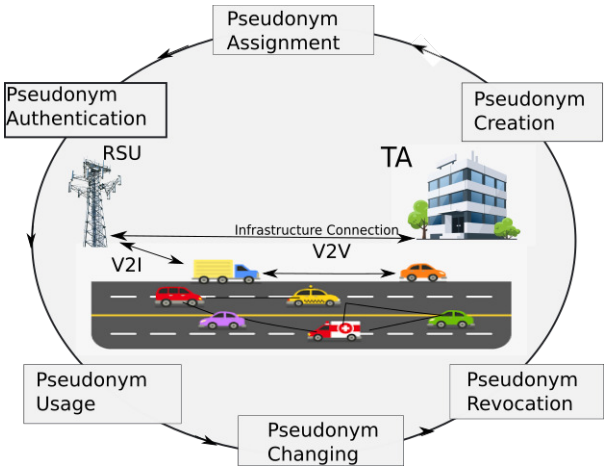

Fig. 2. Pseudonym Cycle - ITS Infrastructure

Changing Pseudonym. Vehicles need to change pseudonyms at intervals determined by the Location Privacy Protection Mechanisms (LPPMs). The certificate-less cryptographic approach has vehicles generate pseudonyms themselves. While this reduces the communication burden on the RSUs and TA, it imposes a computational burden on the vehicle computers, depending on the rate at which pseudonyms are consumed.

Timing, location, context, cooperation from neighboring vehicles, and the pseudonym-change mechanism of the protocol, together determine the success of pseudonym change in protecting privacy.

Revocation. The TA revokes the certificates associated with a vehicle in the following cases: out of commission, change of ownership, or repudiation due to malicious behavior. Certificate-based solutions have a communication-intensive method to revoke all vehicles' certificates. Moreover, broadcasting all vehicles' certificates to an RSU is an added burden. When an RSU detects malicious behavior from a registered vehicle, it connects with the tamper-proof device on the vehicle to eliminate its security credentials, the RID (Registration ID) [15].

Vehicular Network Characteristics. The challenges in maintaining a vehicular network are:

(1) External attacks: Vulnerability to misinformation or malfunction due to tampering. The cost of such malfunction is immense.
(2) Restricted mobility: Vehicles on roads with a strict rules of entering and exiting are easy to predict in terms of timing. For example, right only lanes near a traffic light intersection.
(3) Randomly changing network topology. At high speeds, the network topology formed by the vehicles can change rapidly.
(4) Limited Range: VANET operates under 2.4GHz or 5GHz frequencies with limited range.
(5) Dependency on external systems: VANET relies on RSUs, neighboring CAVs, connected traffic light systems, and GPS, which are all vulnerable to attacks.

Given these challenges, an ITS has to maintain security and preserve privacy, while supporting high traffic throughput and performing its primary function of enhancing the safety of vehicles on the road network.

3.3 Security Requirements

There are several security attacks possible in each phase of the pseudonym life cycle. The vulnerability arises both from within, and outside, the TA and RSUs.

The security requirements include:

(1) **Availability**: The ITS infrastructure has to be highly available, irrespective of the volume of the traffic. The ITS components should rapidly detect and adequately defend against any security threats to the infrastructure.
(2) **Integrity**: A third party should not be able to modify any message transmitted among the ITS participants without detection. Any message from an attacker with modified content should be easily detected and rejected.
(3) **Confidentiality, Privacy, and Anonymity**: The source and contents of a message should only be known to the intended parties.
(4) **Traceability and Revocability**: Only trusted authorities should be able to trace the source of a safety message and only authorized entities like law enforcement should have the ability to revoke security credentials.
(5) **Non-repudiation:** A vehicle cannot deny having sent any of its messages. This property ensures that a vehicle takes ownership of the messages it sends. When accidents happen this property prevents vehicles from sending malicious messages.
(6) **Scalability:** The system obviously has to scale efficiently to handle a large (and rapidly changing) volume of traffic.

(7) **Unforgeability:** This property secures a communication channel from attempts by an attacker to interrupt message transmission, read a message, and forge it using the security credentials of a different vehicle.
(8) **Unlinkability:** An attacker should not be able to link two messages from the same vehicle across pseudonym exchanges.
(9) **Transparency:** This property establishes the following critical steps to achieving transparency: information sharing, software accountability, security incident reporting, and disclosure of mitigation steps and fixes.

3.3.1 Security Attacks. An ITS offers a wealth of attack surfaces [13, 16, 17]. The more common attacks are as follows.

(1) Sybil Attack: A vehicle impersonates multiple vehicles by transmitting multiple messages with different IDs. Many countermeasures exist [18]; for example, an approach where each vehicle measures received signal strength and localizes the source of each safety message [19].
(2) Bogus Information Attack: Vehicles send bogus accident/congestion messages to divert traffic to other routes. Authenticating each message and its sender's ID, and verifying the information from other sources, such as crowdsourcing applications which report traffic, can defeat this attack.
(3) Impersonation Attack: An attacker steals a vehicle's identity. The attacker uses the stolen identity in message replay, fabrication, and alteration. By replaying old messages, an attacker can create an illusion of heavy traffic in a road segment. As other vehicles avoid taking that road (at the cost of increasing traffic along alternative routes), the attacker can clear its intended route of traffic. Also, a vehicle can impersonate an ambulance to get priority access to roads. A tamper-resistant OBU can protect against stealing security keys.
(4) ID Disclosure: Attackers might infect vehicles by sending malware. The infected vehicles periodically report their ID and location to a malicious entity. Monitoring a vehicle's network stack for security attacks can counter such malicious attacks. Furthermore, using AI/ML analysis on the cloud or an in-built model within the vehicle can investigate the outgoing traffic and reset its stack when it detects anomalous behavior. There is scope for future research to strengthen existing countermeasures.
(5) Fault-Injection: Due to attacks on a vehicle's sensors, the vehicle reports false information. This is a fault-injection attack. An effective countermeasure is to integrate information received from multiple sources to identify subsets of information which do not correlate with the majority. A vehicle may also take proactive measures to deal with suspicious data. For example, suppose a vehicle receives information from its sensors reporting multiple vehicles on the road. Before broadcasting a wrong message, the vehicle can validate the information by querying a nearby RSU about the traffic volume. There is scope for further research to improve this countermeasure.
(6) False GPS signal generation or GPS signal blocking: Using GPS signal simulation, an attacker can broadcast false GPS signals with higher signal strength. The presence of false high-strength signals misleads vehicles into reporting the wrong location. Also, an attacker can jam GPS signals. Lack of GPS signals may lead vehicles to, for instance, falsely report a tunnel or even entirely prevent them from reporting their location.
A defense against such an attack is to correlate recent vehicle positions. Given that the vehicle's velocity is known, it can flag instances where there is a non-credible change in its reported location. Also, preloaded maps in the vehicle can be used to corroborate information from GPS (e.g., to determine whether in fact the vehicle is in a tunnel).
(7) Delay Attacks: A malicious vehicle may simply delay forwarding status messages. A popular approach to counter such an attack is to use a tamper-proof software stack to broadcast such messages.
(8) Denial of Service (DoS) Attacks: DoS attacks can be mounted on a vehicle or an RSU. DoS attacks on a particular vehicle occur when it connects to an RSU. A malicious RSU retries a connection request multiple times. Such an attack prevents the vehicle connecting to a valid RSU. Alternatively, DoS attacks on RSU can happen by malicious vehicles repeatedly sending false authentication messages. The RSU has to validate each message in order to determine that it is a false message. An effective countermeasure should detect DoS attacks and disengage the malicious node.
(9) Black Hole Attack: Assume that a malicious vehicle has a few vehicles behind it and some vehicles ahead of it at a distance. The malicious vehicle creates a black hole by not forwarding traffic alert messages from the vehicles behind to the vehicles ahead. One way to counter such an attack is to use a trust management system to ensure the trust of surrounding vehicles. When a trust level of neighboring vehicles is below a threshold, the concerned RSU should forward such critical alerts even with some delay.
(10) Gray Hole Attack: The Grey Hole attack is similar to the Black Hole attack, with the difference that the malicious vehicle broadcasts a few messages while dropping others; this reduces the chance of the attack being rapidly discovered. Countermeasures include a reliable RSU as a backup to forward such alerts to vehicles.
(11) Man In The Middle (MITM) Attacks: A vehicle in the middle listens to two vehicles (one behind and the other in front) and passes incorrect information to each other. Robust integrity verification methods can subvert such attacks. One such method is to include a message-hash in the optional part of basic safety message.

Many countermeasures rely on robust and trustworthy RSUs near critical junctions. However, an insider attack can compromise an RSU. Therefore, ideally, two or more RSUs must cover each crucial region to provide corroboration.

3.4 Privacy Requirements

Privacy requirements include the standard ones of confidentiality and anonymity. In addition, an eavesdropper should ideally not be able to link any two messages from the same vehicle if these are separated by more than a certain duration. Furthermore, the process of revoking a vehicle's identity should not lead to revealing vehicle's other security credentials.

3.4.1 Privacy attacks. Several attacks are possible against an ITS.

(1) Trace Analysis Attack: In this type of attack, the attacker generates mobility patterns of vehicles using their publicly available security credentials.
(2) Colluding Attack: In a group-based or ring-based scheme, a group of vehicles are given privileges to encrypt messages and pass them on to the vehicles in the group or ring. For example, two vehicles can collude to spread misinformation, manipulate group processes, or disrupt communication.
(3) Location Linking: An attacker locates the target vehicle successfully across multiple road segments.
(4) Timing Attack: A vehicle frequently changes its temporary identity. During these changes, the vehicle maintains silence. However, an adversary observes the time of the entry and exit of a vehicle. Based on the timing information, the attacker can attempt to track the temporary identity change of a vehicle.
(5) Transition Attack: The adversary uses traffic statistics to estimate the probability for intersection behavior (e.g., the fraction of traffic that can be expected to turn left, right, or go straight). An attacker can track vehicles transitioned silently within a region based on timing (e.g., duration between entry to, and exit from, a given region).
(6) Inference Attacks: Adversaries trace past movements to predict the future locations of vehicles.

3.5 Safety Requirements

The ITS should be able to preserve safety even in the face of a security attack. Hence, each vehicle should have a dependable fallback system; autonomous systems fall back to semi-autonomous or manual systems in the event of disabled vehicle connectivity.

The following are some of the safety issues [16]. A lane changing alert is required if another vehicle is in the blind spot when changing lanes. If a vehicle is misbehaving (e.g., skips a red light), nearby vehicles must be suitably warned in time to take avoiding action. Similarly, impending collisions must be guarded against, either due to mismatched speeds on a road segment or carelessness at an intersection. Approaching emergency vehicles must be given adequate leeway.

The safety application requirements are [12]:

(1) Low Latency: The vehicles and neighboring RSUs should be alerted rapidly in the event of an emergency: the communication and computational burden should be low enough so that this can be achieved.
(2) Alert Validity: Alerts should be validated rapidly by either the local RSU or neighbouring vehcles. If neighboring vehicles provide proof-of-event, the validation process can be rendered lightweight.
(3) Infrastructure Availability: Vehicles should be able to broadcast safety or alert messages anytime except when they change pseudonyms (since the IP protocol has to reset during a pseudonym change). During such a change, vehicles cannot broadcast alerts. However, such silence should be overridden at the price of privacy in order to protect against imminent danger.
(4) Reliability: Groups of disparate sensors might be used, to ensure sufficient reliable sensing capability across a wide range of weather conditions.

3.6 The Attack Space

Researchers have categorized attacks along a number of dimensions.

(1) Side-Channel Attacks: Many viable side-channel attacks have been described. For example, Rouf et al. demonstrated that a tire pressure monitoring system could reveal the identity of vehicles and thus their visited locations [20].
(2) Insider vs. Outsider Attacks: The attacker's possession of access to the target system determines their classification as an insider or an outsider. An insider attacker gains access to the TA infrastructure by stealing a worker's password credentials. They have the ability to manipulate the equipment of various ITS nodes and their software systems. An authenticated vehicle can be used as a malicious vehicle to initiate insider attacks. An outsider attacker can hack into a vehicle's On-Board Unit and steal the vehicle's credentials in order to masquerade as a valid vehicle.
(3) Rational vs. Malicious Attacks: The attacker's intent determines whether they are rational or malicious. A rational attacker seeks personal gain, such as increased profit, which is their primary motive, while harm to the system is considered acceptable collateral damage. In contrast, a malicious attacker seeks disruption as an end in itself. For example, a rational attacker might exploit traffic information to target advertising, whereas a malicious attacker might aim to disrupt traffic for no reason other than causing harm.
(4) Active vs. Passive: An attack is classified as active or passive based on timing of disruption. Much of the location privacy research focuses on an active attacker. An active attacker participates in compromising the system through various means. For example, a malicious vehicle can block broadcasting a security alert in an active attack. A passive attacker listens to the network traffic, records it, and analyzes it to unravel vehicles' identity, route, and driver's habits. Many privacy attacks fall into this category.

(5) Local vs. Extended: The extent of access to network information distinguishes an attacker as local or extended. A local attacker can access information broadcast within a limited region of the network. The objectives of a local attacker may include disabling infrastructure, disrupting traffic near an intersection, inferring vehicles' turns, or identifying vehicles within that limited area. While local attacks can be potent, they are constrained to a specific region. In contrast, an extended attacker requires greater resources to launch a more expansive attack, gaining access to infrastructure through hacking and acquiring data across a broader region of interest.

A given attack can be categorized based on its position within the attack space. For example, we might have Local Passive Attacks (LPA), Global Passive Attacks (GPA), and Local Active Attacks (LAA).

3.7 Privacy Metrics

Privacy metrics measure the effectiveness of a system in preserving privacy in the face of attacks. For a general discussion of the merits and weaknesses of diverse privacy metrics, see [21]. We focus here on privacy metrics suitable for evaluating pseudonym-changing protocols.

(1) Uncertainty: Suppose the adversary is interested in tracking a particular vehicle. Such a target has to be identified from a set of nearby vehicles. The level of uncertainty in the identification is an indication of the resilience of the system to a privacy attack.
For example, suppose vehicles enter a parking lot, remain silent during parking, and then exit after a random parking duration. An eavesdropper has then no means (relying solely on listening to wireless messages) to identify with certainty the target vehicle from any of the others which were parked there at the same time. Privacy measures relevant to pseudonym-changing schemes include the following.
- Anonymity Set, $\mathcal{AS}$ and K-Anonymity: This metric defines the number of vehicles which can create uncertainty for the attacker, i.e., the number of vehicles in the anonymity set, denoted by $|\mathcal{AS}|$. Any vehicle in the group of vehicles $\mathcal{AS}$ may be the target vehicle. Clearly, the bigger the anonymity set, the greater the anonymity of the target vehicle. However, this is a good metric only when the members of the anonymity set have a roughly equally likely probability of being mistaken for a target vehicle. If $|\mathcal{AS}| = K$, the target vehicle is said to have K-anonymity.
Clearly, the attacker's capability affects the size of the anonymity set. A highly capable attacker can extract a great deal of information from multiple sources and with sophisticated algorithms will end up with a smaller set than an attacker with lower capability. This measure is hampered by having a 0-1 characteristic: fuzzy membership of the anonymity set is not part of the model.
- Entropy and Pairwise Entropy: This measure is based on information theory and is more expressive than the K-Anonymity Set. In particular, it removes the requirement of members of a set having roughly equal likelihood of being the target.
Suppose each vehicle $v_i \in \mathcal{AS}$ has probability p_i of being the target vehicle out of K vehicles in the anonymity set, $\mathcal{AS}$. The entropy $\mathcal{H}$ is given by Equation 1.

$$\mathcal{H}(\mathcal{AS}) = -\sum_{i=1}^{K} p_i \log_2 (p_i) \tag{1}$$

It is maximum when $p_i = 1/K$ for each vehicle. Related to this measure is the notion of *pairwise entropy*, which expresses the uncertainty of identifying the target between a given vehicle *pair*. For example, suppose vehicles v_i and v_j enter and exit an intersection with different identities v_i^* and v_j^* respectively. Let $p_{i,j}$ denote the probability that the attacker identifies incoming vehicle v_i as outgoing vehicle v_j^*; we have two possible identifications corresponding to the probabilities p_{i,i^*} and p_{j,i^*}. The former represents the correct matching of each outgoing member of the pair to its incoming; the latter the incorrect matching. The pairwise entropy $\mathcal{H}(i, j)$ is given by Equation 2.

$$\mathcal{H}(i, j) = -p_{i,i^*} \log_2 (p_{i,i^*}) - p_{j,i^*} \log_2 (p_{j,i^*}) \tag{2}$$

The uncertainty in correctly mapping i to its new pseudonym is the minimum of $\mathcal{H}(i, j)$ and $\mathcal{H}(j, i)$. A minimum of both entropy values is selected for conservative estimate of unpredictability.

(2) Attacker's Tracking Success: This is the percentage of vehicles tracked successfully over a given observation period, from the start of their journey to the end of it.
(3) Maximum Tracking Time (MTT) or Distance: This is the maximum cumulative time or distance an attacker can track a vehicle successfully.
(4) Time to Confusion: This is the total time over which the entropy with respect to a given target is below a specified threshold.

3.8 Traffic Efficiency Metrics

As noted earlier, a key goal of ITS is to enhance traffic efficiency. A system-focused metric for efficiency is the average traffic throughput, which represents the average number of vehicles passing through a set of points, like intersections, per hour. Average throughput can be employed to assess the influence of mix-zones on traffic flow. The throughput of a lane L_j in a mix-zone during an i^{th} interval of Δt minutes with $N_{L_j}^i$ vehicles traversed through the lane is given by $N_{L_j}^i/\Delta t$. The average throughput q_{L_j} observed during a set of k equally spaced intervals of Δt minutes each given by Equation (3).

$$q_{L_j} = \frac{1}{k} \sum_{i=1}^{k} \frac{N_{L_j}^i}{\Delta t} \tag{3}$$

The average throughput of an intersection with m outgoing lanes over k such intervals can then be calculated as

$$q_M = \sum_{j=1}^{m} q_{L_j} \tag{4}$$

A user-focused metric is the degree to which a vehicle is delayed by traffic, which is referred to as trip delay.

4 PSEUDONYM CHANGING STRATEGIES

A pseudonym exchange is considered successful when it is impossible (or very difficult) for an attacker to link the old and new pseudonyms of a vehicle, making it challenging for the attacker to determine with high probability that a particular pseudonym is the new name of a specific vehicle.

A vehicle periodically broadcasts its current behavior, including velocity, acceleration, and heading. When a pseudonym changes, the attacker tries to associate the new pseudonym with the previous one by matching the vehicle profile. Pseudonym-changing techniques aim to reduce the accuracy of such linkage by implementing pseudonym changes when the vehicle profile changes and/or when multiple vehicles coordinate their changes to increase pairwise entropy between vehicles. Pseudonym change algorithms can be characterized by their timing, location, and the level of inter-vehicle cooperation.

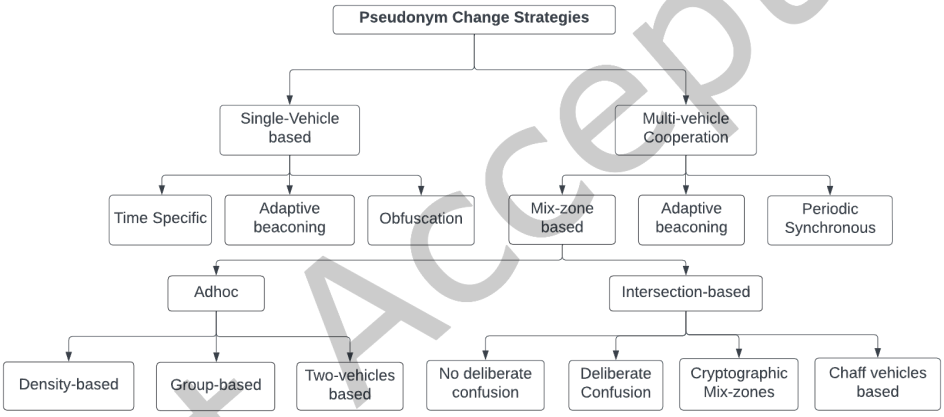

Fig. 3. Pseudonym changing strategies

Figure 3 provides a classification of pseudonym change strategies. The simplest to implement are those that require no explicit cooperation or coordination between vehicles; however, these strategies are also the most vulnerable. Recently, the focus has largely shifted towards coordinating pseudonym changes across a set of vehicles to enhance their effectiveness in confusing potential attackers.

After a brief discussion of uncoordinated techniques, we move to a more detailed look at coordinated multi-vehicle schemes.

4.1 Uncoordinated Pseudonym Changing Techniques

Time-Specific Schemes. The simplest approach of all is for a vehicle to change pseudonyms periodically [22]. An attacker can determine the periodicity of a pseudonym change by analyzing the timing and content of transmissions. A minor improvement on this is to have vehicles individually change pseudonyms at random times [23]. In many instances, such as vehicles on a highway or a single vehicle on a long road, t his protocol proves ineffective against a global passive attacker. Moreover, when a vehicle changes its pseudonym, the attacker becomes aware of the pseudonym change, resulting in spatiotemporal correlation almost as strong as periodic pseudonym changes, making tracking the pseudonym change a trivial task [24].

Introducing extended, randomly timed moments of silence during pseudonym changes can effectively diminish the association between a vehicle's old and new pseudonyms. This strategy also boosts the probability of multiple such periods coinciding [25]. Nevertheless, it is worth noting that this approach proves less effective in specific scenarios, such as on highways, sparsely populated roads, or situations where only one vehicle is changing pseudonyms, while all other vehicles retain their previous pseudonyms.

Mandating fixed intervals for vehicles to alter their pseudonyms presents a limitation, as it fails to adapt to fluctuating traffic conditions. When extended silent intervals coincide with pseudonym changes, it becomes essential to consider their potential impact on traffic safety. One proposed solution is to allow a vehicle to prematurely terminate its silence period in response to a safety-critical event [26]. Additionally,

many synchronized pseudonym changes can lead to confusion in densely populated areas with high traffic volume. While this confusion affects attackers and protects the privacy of vehicles, it can impact legitimate users of V2X messages, particularly safety applications. Such confusion poses a risk to safety since these applications often need more time to verify new pseudonyms before making critical decisions based on the received data. For example, suppose a vehicle receives a vital message from another vehicle that has just altered its pseudonym. The safety application can only act on the alert once the new pseudonym is validated.

Obfuscation-Based Schemes. The notion of disseminating deceptive information has been proposed as a tactic to confound potential attackers. This concept hinges on the understanding that pseudonym change algorithms exhibit their greatest vulnerability during periods of reduced traffic. Yet, it is crucial to note that such times often coincide with a decreased significance of safety messages. In these instances, when a vehicle perceives a minimal presence of neighboring vehicles, it may choose to transmit messages containing inaccurate details about its current location before executing a pseudonym change [27].. Employing obfuscation techniques proves practical in sparsely populated environments. However, since road traffic remains inherently unpredictable, these deceptive messages have the potential to misguide incoming vehicles to the same area.

Adaptive Beaconing. Many existing approaches assume that adversaries can successfully intercept all unencrypted V2X messages. However, a promising strategy involves diminishing transmission power, limiting the broadcast range to what is necessary for safety within the current traffic context. The aim is to render it significantly more challenging for attackers to eavesdrop on these low-power transmissions. An illustrative example of this approach is the Whisper algorithm, which dynamically adjusts transmission power based on factors like vehicle speed [28]. The underlying principle is that, during low-speed scenarios, a reduced reception range suffices. When the transmission range has remained suitably low for an extended period, it triggers a pseudonym change, as a smaller transmission range reduces the attacker's chances of intercepting messages. It is important to note that other V2X security schemes can seamlessly integrate this approach. For instance, research [4] has shown that this technique enhances the performance of CAPS [29] and SLOW [30] multi-vehicle cooperative algorithms, particularly in congested traffic conditions.

Discussion of Uncoordinated Schemes. Table 2 compares uncoordinated pseudonym-changing strategies (PCS), highlighting their advantages and disadvantages. In particular, it delves into their vulnerability to a potent attacker, a crucial aspect addressed in the last column of the table.

Table 2. Issues of non mix-zone specific pseudonym changing strategies

Type	Pseudonym Changing Strategy	Spatial Linking Effort	Temporal Linking Effort	Security Overload	Safety Efficiency	Traffic Efficiency	Attacker
Single-Vehicle	Time-based	Low	Low	Low	High	High	LPA and above
Single-Vehicle	Obfuscation Methods	Low	Low	Low	Low	High	GPA and above
Single-Vehicle	Adaptive Beaconing	Low	Low	Low	High	High	GPA and above
Single-Vehicle	Density-based	Low	Low	Low	Medium	Low	GPA, LPA, LAA
Multi-Vehicle	Vehicle-centric	Low	Low	Medium	High	High	GPA and above
Multi-Vehicle	Group-Based	Low	Low	Medium	High	High	Internal Attacker

As uncoordinated pseudonym change strategies mentioned above are vulnerable to a powerful attacker with machine learning (ML) capabilities, we explore mix-zone based pseudonym change techniques. Table 3 shows the evolution, over time, of pseudonym changing strategies. The focus is increasingly on coordinated multi-vehicle strategies.

5 PERIODIC SYNCHRONOUS MULTI-VEHICLE SCHEMES

When multiple vehicles change pseudonyms around the same time, it becomes more difficult for an eavesdropper to link the new pseudonym of a vehicle to its previous one. As might be expected, coordinated pseudonym change has the greatest privacy benefit in conditions of high traffic density, when the anonymity set is potentially large [24].

The time-based approach mentioned earlier can also be synchronized across vehicles. Assuming that vehicle clocks are sufficiently tightly synchronized (e.g., using GPS signals), the scheme can involve all vehicles being directed to change pseudonyms at synchronized points in time [26]. Thus, multiple changes take place in the traffic network at about the same time, thereby increasing the confusion to the attacker and reducing the probability that a vehicle's new pseudonym can be linked to its previous one. The sequential list of pseudonyms to be used can either be held in individual vehicles or in the RSU [31].

5.1 Mix-zones

The first mix-zone idea appears to have been pioneered in [32]. A mix-zone can be created either by the infrastructure or dynamically by participating vehicles. The effectiveness of a mix-zone in defeating attacks on privacy depends on its size, number of entry points and exit points, and location [37].

5.1.1 Ad-hoc Mix-zones. Vehicles form cooperating vehicle groups on the fly, effectively creating ad hoc mix-zones on demand. Any vehicle can initiate a request to form an ad hoc mix-zone, and participation in the mix-zone is voluntary. Each vehicle decides whether to change pseudonyms within it based on factors like trip anonymity and time since the last change. In the context of heavily trafficked

Table 3. Timeline of proposed pseudonym changing schemes

Year	Single vehicle				Multi-vehicle			
	Time-based	**Obfuscation**	**Vehicle centric**	**Adaptive beacon**	**Periodic**	**Mix-zone (Adhoc) Density based**	**Mix-zone (Group based)**	**Mix-zone (Infrastructure)**
2003								Beresford et al. [32]
2005	Huang et al. [25]						CARAVAN: Sampigethaya et al. [33]	
2006			Swing&Swap: Li et al. [34]				AMOEBA: Sampigethaya et al. [35], Gerlach and Guttler [24, 36]	
2007			Eichler [22], SLOW: Buttyan [30]				Mix Context: Gerlach and Guttler [24, 36]	Buttyan et al. [37], Eichler et al. [22], Freudiger et al. [38]
2008								
2009						Chaurasia et al. [39, 40], Liao and Li [41]		
2010	Rouf et al. [20]	Wei et al. [42]				DLP: Song et al. [43]	D-CMIX: Wasef et al. [44]	
2011					RPC: Pan et al. [23]		SPCP: Weerasinghe et al. [45]	MobiMix: Palanisamy et al. [46, 47]
2012			Freudiger et al. [48]			CPN: Pan and Li [49]		Lu et al. [50].
2013							DMLP: Ying et al. [51]	
2015						CAPS: Emara et al. [29]	Ying et al. [52]	
2016			SlotSwap: Eckhoff et al. [31]	Shah et al. [53]				Yu et al. [54], Boualouache et al.[55]
2017							TAPCS: Boualouache et al. s[56]	Zhang et al. [57], Boualouache et al.[58]
2018				ENeP-AB: Zidani et al. [59]	Eckhoff et al. [26]			Vaas et al. [60]
2019				Babaghayou et al. [28]				CPS: Wahid et al. in [61], AEMP: Ravi et al. [62]
2020		Benarous et al. [27]	PAPU: Li et al., [63]					
2021				WHISPER: Babaghayou et al.[64]			AGPC: Ullah [65]	Al-Marshoud et al. [66]

urban roads, there needs to be more control over the frequency with which vehicles establish ad-hoc mix-zones. Major cities like New York, for instance, feature numerous arterial roads. If mix-zones can spontaneously form without regulation, it can significantly disrupt traffic patterns and vehicular communication. In such a scenario, an attacker can easily exploit this lack of control by repeatedly initiating mix-zone requests as a disruptive communication attack. Ad-hoc and density-based mix-zones share similarities. One key difference is that ad-hoc mix-zones can come into existence even on highways. While group-based strategies effectively preserve privacy against local and global passive eavesdroppers, they exhibit susceptibility to internal attackers. Moreover, the group leader, responsible for communicating with RSUs on behalf of the group, may need to compromise their privacy as part of the process.

In the Swing algorithm, a vehicle initiates pseudonym change when its traffic characteristics (e.g., heading, speed) are changing, it detects other vehicles in the neighborhood, and its current privacy level is below a threshold or its pseudonym has not been changed for a long time [34]. If these conditions are met, it announces to its neighboring vehicles that it is changing its pseudonym before falling silent for a random period. Other vehicles in the neighborhood then decide, based on their own privacy levels, whether or not to update their own pseudonyms at this time. The hope is that enough vehicles change their pseudonyms at roughly the same time so that an attacker cannot readily link a vehicle's new pseudonym to its prior one.

The Swap scheme [34] also involves a vehicle initiating a potential round of pseudonym changes among a set of neighbors under the same conditions as for Swing [34]. It transmits an exchange request; other vehicles in the area then respond to indicate whether they are willing to participate. The initiating vehicle then selects one of its willing neighbors and initiates an exchange of pseudonyms with it. The exchanging node can be selected at random [34] or by identifying another vehicle whose similarity to itself (in terms of position, heading and velocity) is the greatest among the respondents [63]. A variation on this scheme involves randomly updating a pseudonym only when there are at least k other vehicles with similar position, velocity and heading characteristics for some predefined threshold, k; these vehicles all change their pseudonyms in a synchronized fashion [41, 49]. Other schemes involving pseudonym changes, also based on density considerations, are described in [24, 39, 40, 43].

The willingness of a vehicle to engage in a swap depends on whether its own assessed privacy level is below a predetermined privacy threshold: vehicles which already have a high degree of privacy (for instance, because they might have only recently changed pseudonyms) may be unwilling to participate. One can use game theory to model such behavior and design exchange protocols appropriately. For instance, one approach is to adapt the privacy threshold in Swing based on the estimated number of neighboring vehicles and their estimates of their current privacy level [48].

In the SLOW protocol, vehicles maintain silence when their speed is below some threshold, say 30m/s, except when needing to fend off an imminent collision [30]. A vehicle can change its pseudonym during such a silence period. The motivation for using a speed threshold is that safety benefits of inter vehicle communication are more pronounced at high speeds and drop off when traffic is moving slowly. Furthermore, such slow speeds are often due to traffic congestion; all the neighboring vehicles are likely to be similarly affected and traveling at low speeds, so that the common road congestion acts as an implicit synchronization mechanism and creates an impromptu mix zone.

TAPCS (Traffic-Aware Pseudonym Changing Strategy) can be regarded as following some of the principles of SLOW [56]. In TAPCS, a vehicle which is slowed by congestion to below a specified speed, broadcasts a notification of traffic congestion. To avoid a rogue vehicle triggering spurious activity, vehicles require a minimum number of such congestion reports before proceeding. An election is held to select a leader to notify all vehicles within a given region to maintain silence. (A new leader is elected if the leader exits the silence zone.) When vehicles exit the congested area, they resume broadcasting.

Another type of ad-hoc mix-zone scheme is platoon-based. In CARAVAN, proposed by Sampigethaya et al. [33], vehicles form a platoon. The car leading the platoon becomes the leader. All other vehicles can remain silent within the platoon. They use group navigation to counter simple and correlation tracking adversaries. A group leader establishes a secure channel with third party location-based application servers via an RSU. These third party location-based servers carry low trust as malicious actors can track users based on their queries. To avoid tracking using the source identity of a query, the group leader collects location based queries from the vehicles in the platoon. The leader then forwards them to relevant servers. After receiving responses from the servers, the leader disseminates the answers to respective vehicles in the platoon.

Another ad hoc mix-zone scheme was presented by Gerlach and Guttler [24, 36]. A trigger for forming a mix-zone occurs when vehicles sense a proper context in which to mix. A suitable mixing context consists of a threshold number of neighbors all with a desired speed and direction. First, each vehicle indicates its desire to change pseudonyms by setting a flag in BSM. When vehicles sense (by counting the flags in BSMs) a suitable mix-context, all vehicles change pseudonyms synchronously. This scheme provides 60% more privacy than random pseudonym change.

Another ad hoc group formation also uses on-the-fly group creation [45]. If a vehicle desiring to change its pseudonym does not find a suitable nearby vehicle group to join, it initiates a group forming action in collaboration with the RSU and acts as group leader. When a sufficient number of members is assembled in a group, the group leader picks a time to ask all group members to change pseudonyms. Note, however, that group-based protocols are vulnerable to insider attacks such as a malicious vehicle that makes itself group leader to unravel the privacy of the other vehicles in its group. Moreover, forming such ad hoc groups is time-consuming, which has an impact on safety [2].

Yet another approach is for vehicles to have a minimum and a target pseudonym lifetime [52]. Vehicles maintain a candidate location list based on safety messages received from the other vehicles. The safety beacons include the target expiry time of pseudonyms. A vehicle changes its pseudonym either a) at the minimum lifetime of its current pseudonym, or when b) at least one other vehicle has reached

its target pseudonym age. The expectation is that the expiry of a pseudonym will usually lead to multiple near-simultaneous changes of pseudonym, which create a dynamic mix-zone, thereby making pseudonym linkage difficult.

Vehicles can use their Basic Safety Messages to count the number of nearby vehicles which are ready to change their pseudonyms [59]. Pseudonyms become eligible for replacement when they have been used for a certain minimum period. A vehicle which is ready to change its pseudonym sets a bit in a designated field of its BSM to so inform its neighbors. This way, vehicles can check whether a given threshold of change-ready neighbors is available; if so, they change pseudonyms.

The DMLP (Dynamic Mix-Zone for Location Privacy in Vehicular Networks) scheme goes as follows [51]. In addition to RSUs, there are Control Servers (CS) as part of the fixed infrastructure, to mediate group setup. When a vehicle wishes to create a dynamic mix zone in which it can change its pseudonym, it sends a request to the nearest CS. It then sends out only encrypted messages for a specified period of time before resuming its usual messages in the clear. The CS, upon receipt of such a request, determines the appropriate area to be covered by the mix zone and notifies the RSUs covering that area. The RSUs, in turn, instruct all traffic in the designated just-created mix zone that they should also encrypt their safety messages for the prescribed duration. Note that encryption can impose a heavy computational burden and may well lead to some vehicles failing to cooperate and transmit as instructed. To deal with such recalcitrant selfish vehicles, one proposal is to have vehicles earn credits for cooperating; a vehicle would need a certain number of credits for its mix-zone requests to be honored in the first place [52].

Rather than maintain silence, one may use encryption when changing pseudonyms at opportune moments; hence a dynamic mix-zone is created [44]. Each OBU has a preloaded set of keys and corresponding certificates. A vehicle initiates a pseudonym change and attaches the secret key in a request message to attain a temporary group key. Vehicles change pseudonyms while continuing to broadcast encrypted safety messages among the group using the group key.

MixGroup by Yu et al. forms mix-zones when vehicles meet sporadically on the roads and in social spots such as parking spaces [54]. The considered attackers include a Global Passive Adversary (GPA), Global Tracking adversary (GTA), Internal Betrayal Adversary (IBA), and Internal Tracking Adversary (ITA). The mixing technique involves sensing enough vehicles in a mix-group, joining a group, selecting a candidate to exchange pseudonyms, and leaving a group. Vehicles assume several adversaries and estimate the benefit of exchanging pseudonyms. The benefit is calculated as pseudonym entropy using Equation 1. If the benefit is sufficiently large, vehicles proceed with the exchange.

5.1.2 Infrastructure-Based Mix Zones. Lu et al. included parking spaces as mix-zones in addition to traffic light intersections and stop intersections [50]. In a mix zone, each vehicle changes pseudonyms independently and does not involve the RSU. The authors assume a global passive attacker. They assign equal importance to all the vehicles, ignoring the pattern of vehicles arriving and leaving the mix zone. This entry/exit pattern can constrain the anonymity set size and thereby the guaranteed privacy. A more appropriate metric to use when an intersection is a mix-zone is the percentage of success for the attacker to spot the target vehicle.

The algorithm assumes a global passive attacker with the anonymity set as the performance measure of interest. (Recall that an assumption in using the anonymity set as a measure is that all its members are equally likely to be the target vehicle.) As with many other schemes, it suffers lower anonymity under light-traffic conditions; it is also vulnerable to FIFO attacks for linking pseudonyms of vehicles leaving a mix zone with those previously entering it.

Freudiger et al. in 2007 use message encryption while in a mix-zone. In their CMIX protocol, vehicles receive symmetric keys from the RSU using asymmetric cryptographic techniques [38]. It assumes an external passive attacker. Also assumed is that when vehicles change pseudonyms within an intersection, spatiotemporal correlation of the old and new pseudonyms is unlikely.

For evaluating performance, entropy and cumulative entropy (vs the number of intersections traversed) are used together with the success in tracking vehicles. While this protocol ensures safety within the mix-zone and continuity in accessing services, it is vulnerable to insider attacks.

The formal analysis of CMIX scheme by Dahl et al. shows that timing of key establishment is critical in protecting the privacy of vehicles [67]. Hence, authors suggest vehicles to acquire keys before entering a mix zone.

Zhang et al. modified the CMIX scheme with a group signature scheme in which an individual user cannot leak others' credentials or forge signatures [57]. This scheme uses bilinear pairings [68]. Bilinear pairings is a cryptographic method to generate shared secret key using a public key without sharing the secret key of each other. While this scheme adds strength to the CMIX zone, it does have a few drawbacks of its own. One major drawback is that bilinear pairings are more time-consuming than the other cryptographic solutions. Moreover, the scheme is vulnerable to modification attacks.

Vaas et al. introduce fake "chaff" vehicles as an extension to CMIX [60]. The primary goal of this protocol is to overcome preserving privacy challenges at low-density intersections. When traffic is light, the local RSU generates enough chaff vehicles (i.e., transmits BSMs pretending to be generated by vehicles) leaving the intersection. The OBUs of the real vehicles in the mix zones do need to be securely notified that these messages are fake, however. A cuckoo filter is used for this purpose [69]. Since these fake vehicles soon vanish from the road network, a capable global attacker can try to identify and eliminate these chaff vehicles. A major assumption is that no malicious vehicles in the mix-zone can leak the symmetric key used to encrypt transmission in a mix-zone.

A variation on the above approach is to have individual vehicles create chaff vehicles rather than have this done by an RSU [70]. In this strategy, vehicles take up more of the burden of transmitting fake chaff messages, thereby reducing the load on the RSUs. However, this scheme continues to have many of the same vulnerabilities as [60]. The authors use the anonymity set size and the linkability between the

new and old pseudonyms as their primary measures of privacy enhancement. Another similar scheme can be found in [71]. The variation suggested by Ali, et al., in [66] replaces the cuckoo filter with the more resilient adaptive cuckoo filter and also adds an RSU signature and timestamp to each message stored in the adaptive cuckoo filter.

This scheme has the following drawbacks: Overload on the network for additional encryption and pseudonym generation. The storage requirements for Cuckoo Filters are an added burden that increases exponentially with the increase in trip length.

MobiMix by Palanisamy et al. focuses on the architecture and placement of mix zones [46, 47]. The objective is to break the correlation between the incoming and outgoing timing sequence of vehicles. A simple rectangular region centered on an intersection does not usually have this property. Instead, a non-rectangular mix zone is suggested, which starts at the center of the intersection and ends at its various outgoing points. A key observation is that by suitably choosing the length of the mix zone along each of the outgoing roads and linking it to vehicle speeds along them, we can decrease the correlation between the arrival and departure points of vehicles, thereby making it more difficult for an attacker to link new pseudonyms with their corresponding previous pseudonyms.

The authors assume a global passive attacker using timing and transition information to link old and new pseudonyms. The metrics used are pairwise entropy and entropy.

Vehicular Location Privacy Zone (VLPZ) by Boualouache et al. uses roadside infrastructures like parking spaces, gas stations, and toll booths as mix zones [55]. The principle behind this protocol is that vehicles spend a random amount of time in the parking space. This helps delink the order in which vehicles exit from the order in which they entered. The authors divide each region into a grid structure. Each cell within the grid has at least one VLPZ maintained by the infrastructure authority. At the entry point, a router coordinates vehicles to respective parking or gas fueling stations. At the exit point, an aggregator will help vehicles exit in random order. The aggregator is needed to avoid vehicles exiting in the same order as they entered. The anonymity set size is used as a performance measure.

Boualouache and Moussaoui use signalized traffic intersections as mix zones [58, 72]. When vehicles are stopped at a red light, the RSU randomly selects vehicles to exchange pseudonyms. Obviously, this scheme only works well when the position and heading of vehicles emerging from the intersection cannot be well correlated with that of vehicles which recently entered it. Also, when exchanging pseudonyms, vehicles inform the RSU, creating a further avenue for attackers to link pseudonyms. Simulations show that a higher arrival rate of vehicles results in lower privacy as this reduces maneuvering space to change lanes in the intersection. Also, long trip distances make vehicles likely to traverse more intersections, resulting in greater privacy.

The Anonymity Enhancing Mix-zone Protocol (AEMP) uses mix-zones with vehicles encouraged to proactively approach mix-zones to confuse an attacker [62]. When in a mix-zone at a traffic light vehicles are encouraged to switch lanes upon entering the silence zone and choose random exit speeds. This aims to minimize the spatiotemporal correlation between entry and exit behaviors.

Table 4. Cryptographic schemes - Pseudonym Authentication - Tradeoffs

Cryptographic Solutions / Tradeoff Criteria	Is Certificate needed	Communication Load for Pseudonym Distribution	Computing load for Pseudonym Update	Pseudonym Change Effort	Ease of Revoking	Batch Pseudonym Verification	Privacy Efficiency	Security Efficiency	Enabling proof of event	Batch Message Verification
Symmetric Key [38]	No	High due to key transport	Low	High computing load on RSU to redistribute secret keys to all the vehicles	Easy	Easy	Low	Vulnerable to insider attacks	No	Not available
Asymmetric Key (PKI) [44, 54, 55, 58, 60, 70–72]	Yes	High due to certificate distribution	High	High load on RSU to redistribute certificates to all the vehicles	Easy	Hard	High	Vulnerable to insider attacks at RSU or TA	No	Not Available
Group-based Ring based [33, 44, 57]	No	High (due to key distribution)	High	NA	Easy	Easy	Medium	Vulnerable to a malicious vehicle in the group	Group can vote	Available
ID-based [50, 62]	No	Low	Low	Low	Easy	Hard	High	High	No	Available
Certificate-less [73]	No	Low	High (ECC based)	Low	Hard	Hard	High	High	No	Available
Blockchain [74]	No	Low	High (ECC based)	Low	Hard	Hard	High	High	Yes	Available

5.2 Evaluation of Selected Mix-zone Schemes

Now that we have described several mix-zone schemes, we can summarize their characteristics along several dimensions. In particular, we look at (*a*) the use of encrypted communications and (*b*) how spatiotemporal correlation between exiting and entering vehicles can be reduced.

5.2.1 Merits of Cryptographic Solutions for Pseudonym Change in a Mix-zone. We first explain the need for encryption in a mix-zone and explain the role of proof-of-event in group based cryptography. Silence within a mix-zone can impact safety, so encrypting V2X communication has been proposed as a solution [38].

In group-based cryptography, enabling proof-of-event refers to the capability of demonstrating that a specific event or action has occurred within a group in a way that members of the group or external parties can independently verify. This proof is typically related to events such as group membership changes, cryptographic operations, or certain conditions being met. In group-based cryptography, this overhead is unavoidable.

Table 4 compares the various available cryptographic schemes.

An ideal solution should have a computation load that can scale with traffic no more than linearly at the RSUs and vehicles. Computational load is due to security credential computation, distribution, and revocation.

5.2.2 Unlinking PCS Techniques.

Table 5. Techniques to unlink spatiotemporal correlation employed in various Mix-zones protocols

Mix-zone Protocol	Year	Mix-zone definition	Spatial Unlinking	Temporal Unlinking	Capability to break the protocol	Addressed Attacks
Beresford et al.[32]	2003	A space throughout which users stay silent (not access applications) and when users exit they are indistinguishable	User has more than one exit points	User spends unpredictable amount of time	An active adversary who can analyze patterns of entry and exit	Local Passive Listeners
Eichler et al. [22]	2007	A circular region of 100m located either at an intersection or crossover point. Vehicles stay silent.	Intersections and crossover points has more than one exit.	Vehicle stays silent for a period of time determined by its speed.	An active adversary who can analyze entry speed and guess exit speed and patterns of entry to exit, such as FIFO.	Local and Global Passive Listeners
Buttyan et al. [30]	2007	Traffic signal intersections when vehicles stay silent when their speed goes below a threshold value	Maintaining silence at traffic signal Intersection	Traffic light has structured signalling sequence. However, at some lanes vehicles cannot follow FIFO	Local/Global passive Attacker with machine learning capabilities.	FIFO based local/global adversary
CMIX: Freudiger et al. [38]	2007	CMIX: Vehicles do not follow silence. Encrypt the communication between vehicles at a traffic light intersection	Instead of silence, vehicles encrypt their communication and exit the intersection.	Traffic light has structured signalling sequence. However, at some lanes vehicles cannot follow FIFO.	a) Map pseudonyms outside mix-zones b) An inside attacker c) An attacker with AI/ML capabilities can map pseudonyms	Local/Global passive adversary
MobiMix: Palanisamy et al. [47]	2011	Define mix-zone dimensions in such a way that time to exit in each direction remains same. Vehicles maintain silence.	All vehicles with same speed exit mix-zones at the same time	Traffic light has structured signalling sequence. However, at some lanes vehicles cannot follow FIFO.	In spite of change in dimensions of a mix-zone an attacker with machine learning capabilities can map old and new pseudonyms successfully based on the training data.	Local/Global passive adversary
Social Spots: Lu et al. [50]	2012	Silence at social spots: parking spaces near Malls and road networks	Maintaining silence in Parking spaces	Entry time and exit time are not correlated in a parking space	Local/Global active attacker	Local/Global passive adversary
Yu et al., [54]	2016	No silence in mix-zones. Social spots such as parking spaces and dynamic mix-zones on the road.	Encryption in social spots, dynamic mix -zones. Vehicles exchange pseudonyms through encrypted messages.	Dynamic mix-zones on the road, vehicles exchange pseudonyms.	Vehicles do not follow FIFO or any other pattern at social spots. However, dynamic mix-zones on a road are easy to break the privacy. Vulnerable to inside attackers of social spots and dynamic zones as symmetric encryption can be easily leaked.	Local/Global passive adversary
VLPZ: Boualouache et al.[55]	2016	Silence in mix-zones. Parking spaces, gas stations, and toll booths.	Entry and exit order is random.	Time spent in a mix-zone is random	Inside attackers can compromise router and aggregator.	Local/Global passive adversary
S2SI: Boualouache et al. [72], [58]	2017	Vehicles are silent. Change or exchange pseudonyms waiting for a green signal.	Vehicles enter traffic light intersection in random order.	No mechanism to unlink temporal correlation.	Vehicles select lanes immediately after entering an intersection. Hence linking pseudonyms is easy.	Global passive adversary

Table 5. Techniques to unlink spatiotemporal correlation employed in various Mix-zones protocols

Mix-zone Protocol	Year	Mix-zone definition	Spatial Unlinking	Temporal Unlinking	Capability to break the protocol	Addressed Attacks
Chaff: Vaas et al.[60]	2019	Vehicles are not silent. Traffic light intersection is a mix-zone.	RSUs broadcast Chaff BSMs in directions other than vehicle's.	No mechanism to unlink temporal correlation.	An advanced attacker can listen to the BSM beacons outside the mix-zone and identify real vehicles.	Local/ weak adversary
Wahid et al.[61]	2019	Silence for 120s at traffic light intersections	Vehicles maintain silence at traffic light intersections.	No mechanism to unlink temporal correlation.	An attacker with machine learning capabilities can predict the exit location of vehicles.	Local passive attacker
AEMP: Ravi et al. [62]	2019	Silence at traffic light intersections	Vehicles change lanes outside the mix-zone to confuse the attacker.	Vehicles change speed while exiting and slow moving vehicles exit last even though they enter first	Has 60% protection against attacker with ML capabilities.	An attacker with machine learning capabilities, LPA, GPA, Internal attackers
Khodaei et al. [70]	2020	Vehicles are not silent. Traffic light intersection is a mix-zone.	Vehicles transmit chaff BSMs.	No mechanism to unlink temporal correlation.	A global adversary can listen to vehicles outside the mix-zone and identify real vs chaff vehicles. An Internal attacker can leak cuckoo filters.	Local weak adversary
Al-Marshoud et al. [66]	2021	Vehicles are not silent. Traffic light intersection is a mix-zone.	Vehicles transmit chaff BSMs and change pseudonyms after CMIX mix-zones	No mechanism to unlink temporal correlation.	A global adversary can listen to vehicles outside the mix-zone and identify real vs chaff vehicles. Internal attacker can leak cuckoo filters.	Local weak adversary

In Table 5, we summarize techniques used to reduce the spatiotemporal correlation of vehicles leaving, from vehicles entering, a mix zone.

5.2.3 Mix-zone vs Attacker Strength. Attackers can be of varying strength. We now consider the vulnerability of mix zone privacy techniques to each of the following passive (i.e., non-transmitting) attacker categories:

- An advanced attacker with machine learning capabilities.
- A global passive attacker who can monitor all communications throughout the network.
- A local passive attacker who can only monitor communications within a subset of the network.
- An internal attacker as some mix-zone protocols rely on cryptographic schemes while changing pseudonyms.

We introduced availability (of a mix-zone) as a criterion as some mix-zone protocols rely on parking spaces but parking spaces may not be available in every trip. As computation costs decrease, all current schemes will lose some of their effectiveness.

Table 6 demonstrates how mix-zone protocols perform when facing various types of attackers. We observe that most schemes which rely on pseudonym exchanges at a traffic light intersection without deliberately confusing an attacker are vulnerable to ML-capable attackers. In contrast, schemes that rely on parking spaces are less vulnerable to ML-based attackers but only if the schemes do not have systems that guide vehicles to specific parking spots. The schemes that employ chaff vehicles or BSMs can escape ML attackers only if the locations mentioned in the BSMs do not coincide with the other chaff messages or actual vehicles. Also, an attacker can listen to messages outside the mix-zone and separate chaff messages from real ones.

5.2.4 Mix-zones - Tradeoff Between Traffic Efficiency, Security, and Safety. Protecting the pseudonym change ensures privacy. Table 7 illustrates the tradeoff between privacy and safety, the associated security overhead, and the often overlooked factor, traffic efficiency. Safety takes precedence above all. As connected vehicles are vulnerable to cybersecurity threats [1], all CAVs should have reliable fallback technologies in place and activate them when active cybersecurity threats are detected in order to continue driving safely.

The following analysis assumes that fallback technologies will be in place for all mix-zone-based privacy-enhancing schemes. When a vehicle establishes a communication channel with another vehicle or infrastructure through V2V or V2I, each protocol layer is assigned an identity, such as a MAC ID, IP address, or session ID. A corresponding change in session identities for each layer should occur when a pseudonym change occurs. Failure to do so could allow an attacker to track the identities of the other layers and link pseudonym changes. Consequently, a pseudonym change interrupts user services in a mix-zone, regardless of whether vehicles maintain silence or use

Table 6. Mix-zone Protocol vs Attacker Strength

Mix-zone Protocol	Year	Attacker with ML	Global Passive	Local Passive	Internal Attacker at RSU	Internal Attacker at TA	Availability
Beresford et al.[32]	2003	×	✓	✓	✓	✓	✓
Eichler et al. [22]	2007	×	✓	✓	✓	✓	✓
Freudiger et al. [38]	2007	×	✓	✓	×	×	✓
Buttyan et al. [30]	2009	×	✓	✓	✓	✓	✓
MobiMix [47]	2011	×	✓	✓	×	×	✓
Lu et al. [50]	2012	✓	✓	✓	✓	✓	×
Yu et al., [54] Parking spaces	2016	✓	✓	✓	×	×	×
Yu et al., [54] Dynamic Mix-zones on roads	2016	×	✓	✓	×	×	✓
Boualouache et al. [55]	2016	✓	✓	✓	×	×	×
Boualouache et al. [72],[58]	2017	×	✓	✓	×	×	✓
Vaas et al.[60]	2019	×	✓	✓	×	×	✓
Wahid et al.[61]	2019	×	×	✓	×	×	✓
Ravi et al.[62]	2019	✓	✓	✓	✓	×	✓
Khodaei et al. [70]	2020	×	×	✓	×	×	✓
Al-Marshoud et al. [66]	2021	×	×	✓	×	×	✓

encryption before the pseudonym change [75]. The baseline protocol, when comparing different mix-zone protocols, is an intersection with no mix-zone and zero anonymity but has good traffic efficiency, safety, and no added computation load.

Table 7. Mix-zone protocols and Tradeoffs with Traffic Efficiency, Safety and Computation Load

Mix-zone Protocol	**Year**	**Silence in Mix-zone**	**Traffic Efficiency Compared to No mix-zone**	**Safety Compared to No mix-zone**	**Computation Load Compared to No mix-zone**
Beresford et al.[32]	2003	✓	Decreases	Decreases	No change
Eichler et al. [22]	2007	✓	Decreases	Decreases	No change
Buttyan et al. [37]	2007	✓	Decreases	Decreases	No change
Freudiger et al. [38]	2007	×	No change	No change	Increases
Palanisamy et al. [47]	2011	✓	Decreases	Decreases	No change
Lu et al. [50]	2012	✓	Decreases	Decreases	No change
Yu et al., [54]	2016	✓	Decreases	Decreases	Increases
Boualouache et al. [55]	2016	✓	Decreases	Decreases	No change
Boualouache et al. [72],[58]	2017	✓	Decreases	Decreases	No change
Vaas et al.[60]	2019	×	Decreases	No change	Increases
Wahid et al.[61]	2019	✓	Decreases	Decreases	No change
Ravi et al. [62]	2019	✓	Decreases	Decreases	No change
Khodaei et al. [70]	2020	×	Decreases	No change	Increases
Al-Marshoud et al. [66]	2021	×	Decreases	No change	Increases

Mix-zone protocols reliant on parking spaces exhibit resilience against internal attackers. Nevertheless, there is room for improvement in both safety and computational efficiency. Additionally, it is essential to acknowledge that parking spaces within a city are limited.

A straightforward mix-zone protocol, where vehicles maintain silence at traffic light intersections (referred to as the baseline protocol in [62], lacks resilience against sophisticated attackers equipped with machine learning capabilities. However, it is worth noting that such a protocol can effectively evade tracking by less capable global and local passive attackers [62]. Vehicles have lower safety and traffic efficiency when they maintain silence in the mix-zone. On the contrary, mix-zones with encryption have the same traffic efficiency and safety as traffic light intersections without a mix zone. However, they are vulnerable to internal attacks, passive global attacks outside the mix-zones, and advanced attackers with ML capabilities. Another set of mix-zones are those with chaff vehicles or RSUs broadcasting chaff messages. Introducing chaff vehicles is an innovative approach to maintaining safety while still gaining privacy by confusing local attackers. However, this scheme decreases traffic efficiency. An actual vehicle and a chaff vehicle cannot exit the intersection simultaneously, and from the same lane, so the actual vehicle must delay occupying the chaff vehicle's location. The delay will have a negative impact on traffic efficiency. Moreover, this scheme increases the computation load on all the nodes.

Safety takes precedence over privacy. When a vehicle detects a severe safety issue in a mix-zone, it must sacrifice its privacy and broadcast the safety message. Mix-zones decrease traffic efficiency, but infrastructure engineers can plan the placement of mix-zones to minimize

the loss of traffic efficiency. An ideal solution would achieve high privacy while being resilient to most attackers and would have low computation overhead cost, high safety, high traffic efficiency, and high availability.

Table 8 presents the attainable levels of anonymity for each mix-zone protocol, showcasing their performance under diverse conditions. We carefully chose the most critical parameters to evaluate the performance of each protocol, and these parameters are unique to the characteristics of each protocol. Typical variations in conditions encompass variables such as vehicle arrival rate, exit vehicle speed, mix-zone radius, number of chaff vehicles, and the number of listening antennas.

6 MIX-ZONE PLACEMENT

When mix zones are infrastructure-based and preplanned, instead of ad hoc gatherings of vehicles, the traffic engineer is responsible for their appropriate placement. The placement of mix-zones depends on the road topology and the traffic flow. Since traffic flow can change over time, it is worth considering whether dynamically adjusting their placement is warranted despite the added complexity.

Figure 4 presents a taxonomy of mix-zone placement algorithms. The literature predominantly features static placement algorithms, with only a few algorithms designed to adapt to changing traffic conditions.

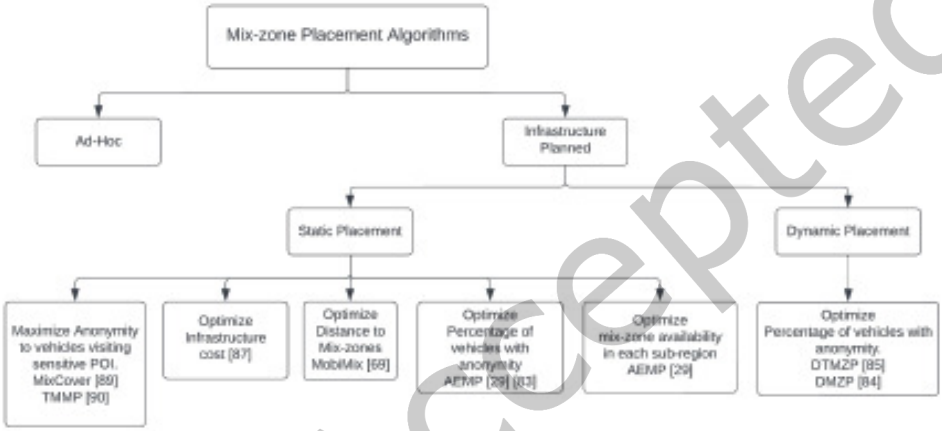

Fig. 4. Taxonomy of Mix-zone Placement Algorithms

We now outline some approaches to mix zone placement.

6.1 Static Positioning

One of the earliest contributions to the placement problem aimed at maximizing the probability of an attacker making a mistake when tracking vehicles [75]. Each mix-zone is subjected to multiple traffic flows in this approach, each with distinctive characteristics. The attacker's task is to classify exiting vehicles into one of these flows. Mix-zone placement aims to maximize the probability of the attacker making an error in such classification while adhering to two constraints. The first constraint requires the average distance over which an attacker can track any vehicle successfully to remain below a specified bound. Additionally, a cost is associated with passing through a mix-zone, modeled as a function of the silence period and the cost of using pseudonyms. The second constraint involves keeping this cost below a certain threshold.

Another approach involves having vehicles adjust their routes to pass through a mix-zone, and the mix-zones are strategically positioned to minimize the additional delay associated with this route adjustment [76]. A location qualifies as a mix zone if its average entropy exceeds a specified threshold. Here, entropy is determined based on the probability of correctly linking an outgoing pseudonym from the mix zone to an incoming one. A requirement to select mix zones from eligible intersections is that any travel exceeding a certain distance must pass through at least one mix zone, with the additional delay caused by route adjustment limited to a predetermined amount. The optimization problem aims to identify the smallest set of qualified intersections that can serve as mix zones while meeting the above-mentioned constraint.

In another scheme called MobiMix, the authors suggest two possible approaches [46]. One is to place mix zones at high-traffic intersections with reasonably random (unskewed) turn behavior as possible. Another is to superimpose a grid on the road network and maximize the average distance between any pair of mix zones within each grid cell.

A graph-theoretic scheme associated with the Mix Cover problem can be described as follows [77]. In the Mix Cover problem, we have a graph, denoted as G, where each node, labeled as v, possesses a specified capacity, $c(v)$, and a weight, $w(v)$. The weighted cost of each node, v, is determined as the product of its capacity and weight, namely $c(v) * w(v)$. Recall that a vertex cover in graph theory pertains to a set of nodes where each edge has at least one endpoint. The Mix Cover problem revolves around finding a vertex cover of a graph

Table 8. Mix-zone Protocols - Attainable Anonymity against a Strong Attacker

Author	Year	Minimum Assured Privacy	Maximum Achievable Privacy	Variable (low to high privacy)
Beresford et al.[32]	2003	entropy < 0.1	entropy ~ 1.0	Location update period within the mix-zone 1hour to 1s (for maximum walking speed of 1.2m/s)
Buttyan et al. [37]	2007	tracking success ~ 60%	tracking success ~ 10%	Number of listening antennas in a region 10 to 60
Freudiger et al. [38]	2007	80% < tracking success < 90%	20% < tracking success < 30%	Density Vehicle per intersection: 1 to 7
Palanisamy et al. [47]	2011	average pairwise entropy ~ 0.6	average pairwise entropy ~ 1	Average speed of exiting users (kmph): 70 to 10
Lu et al. [50]	2012	location privacy gain ~ 0.6	location privacy gain ~ 0.95	Vehicle arrival rate λ: 12s to 2s vehicle spends time in the mix-zone
Yu et al., [54]	2016	average pseudonym entropy ~ 65	average pseudonym entropy ~ 75	Sparse region 10, dense region 160 vehicles/street (time spent 50s in the mix-zone)
Boualouache et al. [55]	2016	Anonymity set ~ 4 (max size 16)	Anonymity set ~ 15 (max size 16)	Arrival rate (vehicles/min): 5 to 10
Boualouache et al. [72],[58]	2017	Probability of tracking ~ 0.6	Probability of tracking ~ 0.35	Short trip of 5 minutes. Density (vehicle/square km): 125 to 25 (low tracking)
Vaas et al.[60]	2019	Pseudonym change exposure/tracking ~ 0.1	Pseudonym change exposure/tracking ~ 0.001	Encryption radius is 50m to 250m
Wahid et al.[61]	2019	Entropy ~ 2	Entropy ~ 5	Max speed, low vehicle arrival rate vs. low speed, max arrival rate; Max vehicles: 100 vehicles
Ravi et al. [62]	2019	Probability of tracking ~ 95%	Probability of tracking ~ 65%	ML attacker, low vehicle arrival rate (20 vehicles/hour) vs. high vehicle arrival rate (750 vehicles/hour)
Khodaei et al. [70]	2020	Probability of linkability ~ 80%	Probability of linkability ~ 60%	100% honest but curious RSUs, 0% decoy traffic to 100% decoy traffic

wherein each node exhibits a sufficiently high capacity while minimizing the total weighted cost. In other words, given a bound, $b(v)$, associated with each node, it is required that $c(v)$ is greater than or equal to $b(v)$ for all v in the vertex cover, denoted as V_{MC}. Additionally, the objective is to minimize the sum of $c(v) * w(v)$ for all v in V_{MC}. Various heuristics are available to tackle this problem. When applied to the mix zone placement problem, the vertices represent intersections, and the edges represent roads. The capacity of each node (i.e., intersection) corresponds to the maximum demand that incoming traffic can impose on the edges connected to it. At the same time, the weight represents the cost associated with traversing the intersection. This approach guarantees that each road segment begins or ends at a mix-zone. The ratio of the heuristic's total weight to the optimal one and the execution time of the algorithm gives the algorithm's performance. Notably, this approach assures that any vehicle traversing at least one complete road segment will pass through a mix-zone.

The Traffic-Aware Multiple Mix Zone Placement (TMMP) scheme, described in [78], employs a graph representation of the road network. In this graph, predefined points of interest are the nodes, and the roads connecting them represent the edges. An infrastructure engineer can place a limited number of mix-zones. For two points of interest to be pairwise-associated, one can travel between them without passing through a mix-zone. The objective is to minimize the sum of all such pairwise associations. This algorithm considers side information, like an attacker observing a vehicle at a Point Of Interest (POI), which the attacker can potentially exploit. An essential constraint is that if two nodes are pairwise associated, at least one must be a mix-zone. Furthermore, additional constraints exist, such as setting lower bounds on the entropy associated with each mix-zone and the pairwise entropy between two nodes. Pairwise entropy between two nodes is the total entropy along all paths linking those nodes, accounting for the probability of side information being available on each path.

The Anonymity Enhancing Mix Protocol (AEMP) aims to minimize the probability of successfully piecing together a vehicle's end-to-end trajectory [62]. It assigns a *mixability* measure to each intersection to achieve this goal. This measure considers factors such as the traffic intensity at the mix zone, the number of mix zones a vehicle is likely to have passed through, the intersection's topology (including lanes in and out), and typical traffic turning behavior. Intersections are ranked in order of their mixability. A genetic algorithm selects an optimal set of mix-zones using the ordered list of intersections.

AEMP can be adapted to prioritize specific subregions [62]. For instance, there might be a greater need for privacy when traveling to and from hospitals. Therefore, the algorithm can be executed with an additional constraint, requiring a minimum number of mix zones to be placed in selected sensitive subregions. For example, the density of mix zones within a certain distance of a hospital may be specified as needing to be twice the average density to provide enhanced privacy for hospital patients and visitors.

6.2 Dynamic Positioning

The Dynamic Temporal Mix Zone Placement (DTMZP) algorithm [79] is a dynamic and temporal approach for positioning mix zones specifically designed for vehicles utilizing Location-Based Services. In this method, a predetermined quantity of mix zones must be allocated from many potential locations. These potential locations are initially organized into a chosen number of clusters via a standard clustering algorithm. By representing the road network as a graph with intersections as nodes and roads as edges, these clusters can be subsequently ranked in descending order based on eigenvector centrality. Then, the selection of the number of mix zones from each cluster is determined by utilizing traffic flow information over a specific time interval, and the mix zones are chosen accordingly.

The *Dynamic Mix-zone Placement* (DMZP) algorithm for VANET is another dynamic placement algorithm [80] that aids an infrastructure engineer with the placement of mix-zones in a road network. The algorithm has two components: an offline component and an online component. In the offline component, a suitable time slot calculates aggregate traffic flow, resulting in a traffic pattern associated with that time slot. Depending on the traffic engineer's preference, these time slots can vary from an hour to an entire day. Then, the DMZP algorithm calculates the optimal mix-zone placement for each traffic pattern. Over time, the algorithm builds a library of observed traffic patterns and optimal placement of mix zones. The algorithm updates the library periodically so that the optimization process is not on the critical real-time path of the placement algorithm.

The online component of DMZP consists of taking the currently prevailing traffic pattern as input and using Ensemble Kalman Filtering to predict the traffic for the next time slot. Then, the system finds the closest match to the patterns stored in the library. Once the algorithm finds a match, it retrieves the appropriate mix zone placement from the library.

Mix-zone placement is an NP-hard problem. We observe that dynamic mix-zone placement generally achieves better anonymity for most vehicles than static placement for the obvious reason that the latter cannot adapt to changes in traffic patterns. Low density traffic can have equally distributed mix-zones [46]. A conglomeration of sensitive points of interest should have regional priority [62]. It is difficult to determine the best algorithm among the static placement algorithms. A better way to compare the different algorithms is to simulate each for diverse road networks and compare the results. This can be an avenue for future research.

7 OPEN RESEARCH ISSUES

Despite considerable research on privacy in ITS, there are still several promising avenues for future research. We mention a few of them here.

7.1 Privacy Metrics

As we have seen, researchers have used many metrics for optimizing or evaluating vehicular privacy. Each of the metrics used can be justified on pragmatic bounds. However, it is not clear how correlated these metrics are to one another.

7.2 Inter-vehicular cooperation

Many schemes depend on the willingness of vehicles to change their pseudonyms when they pass through a mix zone. However, if a vehicle has only recently changed its pseudonym, it may be unwilling to go through the process again, since its own privacy will not be greatly improved. More research is needed on ways to incentivize vehicles for cooperating in the interests of the entire system.

7.3 Impact on Road Safety

The impact of mix-zones on road safety needs further study. For example, are there certain intersection topologies or locations which should not be mix-zones because that would greatly degrade safety? Which intersection topologies and locations offer the greatest privacy enhancement with the lowest impact on safety? How can ITS infrastructure generate proof of safety violations to minimize the time required for validating safety alerts?

7.4 Uninterrupted Services

Despite the omnipresence of diverse mobile networks, unavailability of RSUs and other network infrastructure can severely impact the usability of ITS from establishing secure connections to maintaining privacy [81]. Hence further research should explore non terrestrial communication to enable basic security and privacy features to vehicles where cellular networks are absent.

7.5 Traffic Simulation Tools

Low-overhead and easy-to-use traffic simulators (with user-friendly interfaces) are badly needed. These should ideally be accompanied by a sufficiently comprehensive library of traffic data in a wide variety of urban road networks.

8 CONCLUSION

With the advent of Intelligent Transportation Systems to improve throughput, reduce travel delays, save fuel, and improve safety, has come the need to protect against intrusions of privacy. Wireless V2X communication has long been recognized as a vulnerable attack surface. In this paper, we have looked at ways in which pseudonym-based systems are used to harden systems against breaches of privacy. As such systems become more widely used and the dangers to privacy become better understood, privacy enhancement will become an integral consideration in the design of modern urban transportation systems.

REFERENCES

[1] Dajiang Suo, John Moore, Mathew Boesch, Kyle Post, and Sanjay E. Sarma. 2022. Location-Based Schemes for Mitigating Cyber Threats on Connected and Automated Vehicles: A Survey and Design Framework. *IEEE Transactions on Intelligent Transportation Systems* 23, 4 (2022), 2919–2937. DOI: http://dx.doi.org/10.1109/TITS.2020.3038755

[2] Pravin Mundhe, Shekhar Verma, and S. Venkatesan. 2021. A Comprehensive Survey on Authentication and Privacy-Preserving Schemes in VANETs. *Comput. Sci. Rev.* 41, C (aug 2021), 18.

[3] Shawal Khan, Ishita Sharma, Mazzamal Aslam, Muhammad Zahid Khan, and Shahzad Khan. 2021. Security challenges of location privacy in VANETs and state-of-the-art solutions: A survey. *Future Internet* 13, 4 (2021), 96.

[4] Messaoud Babaghayou, Nabila Labraoui, Ado Adamou Abba Ari, Nasreddine Lagraa, and Mohamed Amine Ferrag. 2020. Pseudonym change-based privacy-preserving schemes in vehicular ad-hoc networks: A survey. *Journal of Information Security and Applications* 55 (2020), 102618.

[5] Hassan Talat, Tuaha Nomani, Mujahid Mohsin, and Saira Sattar. 2019. A survey on location privacy techniques deployed in vehicular networks. In *2019 16th International Bhurban conference on applied sciences and technology (IBCAST)*. IEEE, 604–613.

[6] Fengzhong Qu, Zhihui Wu, Fei-Yue Wang, and Woong Cho. 2015. A security and privacy review of VANETs. *IEEE Transactions on Intelligent Transportation Systems* 16, 6 (2015), 2985–2996.

[7] Abdelwahab Boualouache, Sidi-Mohammed Senouci, and Samira Moussaoui. 2017. A survey on pseudonym changing strategies for vehicular ad-hoc networks. *IEEE Communications Surveys & Tutorials* 20, 1 (2017), 770–790.

[8] J. Petit, F. Schaub, M. Feiri, and F. Kargl. 2015. Pseudonym Schemes in Vehicular Networks: A Survey. *IEEE Communications Surveys Tutorials* 17, 1 (2015), 228–255.

[9] Mohamed Amine Ferrag, Leandros Maglaras, and Ahmed Ahmim. 2017. Privacy-preserving schemes for ad hoc social networks: A survey. *IEEE Communications Surveys & Tutorials* 19, 4 (2017), 3015–3045.

[10] Philip Asuquo, Haitham Cruickshank, Jeremy Morley, Chibueze P Anyigor Ogah, Ao Lei, Waleed Hathal, Shihan Bao, and Zhili Sun. 2018. Security and privacy in location-based services for vehicular and mobile communications: an overview, challenges, and countermeasures. *IEEE Internet of Things Journal* 5, 6 (2018), 4778–4802.

[11] Zhaojun Lu, Gang Qu, and Zhenglin Liu. 2019. A Survey on Recent Advances in Vehicular Network Security, Trust, and Privacy. *IEEE Transactions on Intelligent Transportation Systems* 20, 2 (2019), 760–776. DOI: http://dx.doi.org/10.1109/TITS.2018.2818888

[12] Ruqayah Al-ani, Bo Zhou, Qi Shi, and Ali Sagheer. 2018. A survey on secure safety applications in VANET. In *2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*. IEEE, 1485–1490.

[13] Qazi Ejaz Ali, Naveed Ahmad, Abdul Haseeb Malik, Gauhar Ali, and Waheed Ur Rehman. 2018. Issues, challenges, and research opportunities in intelligent transport system for security and privacy. *Applied Sciences* 8, 10 (2018), 1964.

[14] Ikram Ali, Alzubair Hassan, and Fagen Li. 2019. Authentication and privacy schemes for vehicular ad hoc networks (VANETs): A survey. *Vehicular Communications* 16 (2019), 45–61.

[15] J. Huang, D. Fang, Y. Qian, and R.Q. Hu. 2020. Recent Advances and Challenges in Security and Privacy for V2X Communications. *IEEE Open Journal of Vehicular Technology* 1 (2020), 244–266. DOI: http://dx.doi.org/10.1109/OJVT.2020.2999885.

[16] Jin Cui, Lin Shen Liew, Giedre Sabaliauskaite, and Fengjun Zhou. 2019. A review on safety failures, security attacks, and available countermeasures for autonomous vehicles. *Ad Hoc Networks* 90 (2019), 101823.

[17] Vinh Hoa La and Ana Rosa Cavalli. 2014. Security attacks and solutions in vehicular ad hoc networks: a survey. *International journal on AdHoc networking systems (IJANS)* 4, 2 (2014), 1–20.
[18] Deepak Kushwaha, Piyush Kumar Shukla, and Raju Baraskar. 2014. A survey on Sybil attack in vehicular ad-hoc network. *International Journal of Computer Applications* 98, 15 (2014).
[19] Gilles Guette and Bertrand Ducourthial. 2007. On the Sybil attack detection in VANET. In *2007 IEEE international conference on Mobile Adhoc and sensor systems*. IEEE, 1–6.
[20] Ishtiaq Rouf, Rob Miller, Hossen Mustafa, Travis Taylor, Sangho Oh, Wenyuan Xu, Marco Gruteser, Wade Trappe, and Ivan Seskar. 2010. Security and Privacy Vulnerabilities of {In-Car} Wireless Networks: A Tire Pressure Monitoring System Case Study. In *19th USENIX Security Symposium (USENIX Security 10)*.
[21] Isabel Wagner and David Eckhoff. 2018. Technical privacy metrics: a systematic survey. *ACM Computing Surveys (CSUR)* 51, 3 (2018), 1–38.
[22] Stephan Eichler. 2007. Strategies for pseudonym changes in vehicular ad hoc networks depending on node mobility. In *2007 IEEE Intelligent Vehicles Symposium*. IEEE, 541–546.
[23] Yuanyuan Pan, Jianqing Li, Li Feng, and Ben Xu. 2011. An analytical model for random changing pseudonyms scheme in VANETs. In *2011 International Conference on Network Computing and Information Security*, Vol. 2. IEEE, 141–145.
[24] Matthias Gerlach and Felix Guttler. 2007. Privacy in VANETs using changing pseudonyms-ideal and real. In *2007 IEEE 65th Vehicular Technology Conference-VTC2007-Spring*. IEEE, 2521–2525.
[25] Leping Huang, Kanta Matsuura, Hiroshi Yamane, and Kaoru Sezaki. 2005. Enhancing wireless location privacy using silent period. In *IEEE Wireless Communications and Networking Conference, 2005*, Vol. 2. IEEE, 1187–1192.
[26] David Eckhoff and Christoph Sommer. 2018. Readjusting the privacy goals in vehicular ad-hoc networks: A safety-preserving solution using non-overlapping time-slotted pseudonym pools. *Computer Communications* 122 (2018), 118–128.
[27] Leila Benarous, Benamar Kadri, and Saadi Boudjit. 2020. Alloyed pseudonym change strategy for location privacy in VANETs. In *2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC)*. IEEE, 1–6.
[28] Messaoud Babaghayou and Nabila Labraoui. 2019. Transmission range adjustment influence on location privacy-preserving schemes in VANETs. In *2019 International Conference on Networking and Advanced Systems (ICNAS)*. IEEE, 1–6.
[29] Karim Emara, Wolfgang Woerndl, and Johann Schlichter. 2015. CAPS: Context-aware privacy scheme for VANET safety applications. In *Proceedings of the 8th ACM conference on security & privacy in wireless and mobile networks*. 1–12.
[30] L. Buttyán, T. Holczer, A. Weimerskirch, and W. Whyte. 2009. SLOW: A Practical pseudonym changing scheme for location privacy in VANETs. (2009), 1–8.
[31] David Eckhoff and Christoph Sommer. 2016. Marrying safety with privacy: A holistic solution for location privacy in VANETs. In *2016 IEEE Vehicular Networking Conference (VNC)*. IEEE, 1–8.
[32] A. R. Beresford and F. Stajano. 2003. Location privacy in pervasive computing. *IEEE Pervasive Computing* 2, 1 (2003), 46–55.
[33] K. Sampigethaya, L. Huang, Mingyan Li, R. Poovendran, K. Matsuura, and K. Sezaki. 2005. CARAVAN: Providing Location Privacy for VANET. *Proc. 3rd. Workshop ESCAR* (Nov. 2005), 1–15.
[34] Mingyan Li, Krishna Sampigethaya, Leping Huang, and Radha Poovendran. 2006. Swing & Swap: User-Centric Approaches towards Maximizing Location Privacy. *Proceedings of the 5th ACM Workshop on Privacy in Electronic Society* (2006), 19–28.
[35] K. Sampigethaya, Mingyan Li, Leping Huang, and R. Poovendran. 2007. AMOEBA: Robust Location Privacy Scheme for VANET. *IEEE J.Sel. A. Commun.* 25, 8 (Oct. 2007), 1569–1589.
[36] Matthias Gerlach. 2006. Assessing and improving privacy in VANETs. *ESCAR, Embedded Security in Cars* (2006).
[37] Levente Buttyán, Tamás Holczer, and István Vajda. 2007. On the effectiveness of changing pseudonyms to provide location privacy in VANETs. In *European Workshop on Security in Ad-hoc and Sensor Networks*. Springer, 129–141.
[38] Julien Freudiger, Maxim Raya, Márk Félegyházi, Panos Papadimitratos, and Jean-Pierre Hubaux. 2007. Mix-Zones for Location Privacy in Vehicular Networks. *Proc. ACM Workshop WiN-ITS* (08 2007), 1–7.
[39] Brijesh Kumar Chaurasia, Shekhar Verma, G. S. Tomar, and Ajith Abraham. 2009. Optimizing Pseudonym Updation in Vehicular Ad-Hoc Networks. *Transactions on Computational Science IV: Special Issue on Security in Computing* (2009), 136–148.
[40] B. K. Chaurasia, S. Verma, G. S. Tomar, and S. M. Bhaskar. 2009. Pseudonym Based Mechanism for Sustaining Privacy in VANETs. *2009 First International Conference on Computational Intelligence, Communication Systems and Networks* (2009), 420–425.
[41] Jianxiong Liao and Jianqing Li. 2009. Effectively changing pseudonyms for privacy protection in VANETs. In *2009 10th International Symposium on Pervasive Systems, Algorithms, and Networks*. IEEE, 648–652.
[42] Yu-Chih Wei and Yi-Ming Chen. 2010. Safe distance based location privacy in vehicular networks. In *2010 IEEE 71st Vehicular Technology Conference*. IEEE, 1–5.
[43] Joo-Han Song, Vincent WS Wong, and Victor Leung. 2010. Wireless location privacy protection in vehicular ad-hoc networks. *Mobile Networks and Applications* 15, 1 (2010), 160–171.
[44] Albert Wasef and Xuemin Sherman Shen. 2010. REP: Location privacy for VANETs using random encryption periods. *Mobile Networks and Applications* 15, 1 (2010), 172–185.
[45] Hesiri Weerasinghe, Huirong Fu, Supeng Leng, and Ye Zhu. 2011. Enhancing unlinkability in vehicular ad hoc networks. In *Proceedings of 2011 IEEE International Conference on Intelligence and Security Informatics*. IEEE, 161–166.
[46] B. Palanisamy and L. Liu. 2015. Attack-Resilient Mix-zones over Road Networks: Architecture and Algorithms. *IEEE Transactions on Mobile Computing* 14, 3 (2015), 495–508.
[47] Balaji Palanisamy and Ling Liu. 2011. Mobimix: Protecting location privacy with mix-zones over road networks. In *2011 IEEE 27th International conference on data engineering*. IEEE, 494–505.
[48] Julien Freudiger, Mohammad Hossein Manshaei, Jean-Pierre Hubaux, and David C Parkes. 2012. Non-cooperative location privacy. *IEEE Transactions on Dependable and Secure Computing* 10, 2 (2012), 84–98.
[49] Y. Pan and J. Li. 2012. An analysis of anonymity for cooperative pseudonym change scheme in one-dimensional VANETs. *Computer Supported Cooperative Work in Design (CSCWD), IEEE 16th International Conference* (2012), 251–257.
[50] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen. 2012. Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in VANETs. *IEEE Transactions on Vehicular Technology* 61, 1 (2012), 86–96.
[51] B. Ying, D. Makrakis, and H. T. Mouftah. 2013. Dynamic Mix-Zone for Location Privacy in Vehicular Networks. *IEEE Communications Letters* 17, 8 (2013), 1524–1527.
[52] Bidi Ying and Dimitrios Makrakis. 2015. Pseudonym changes scheme based on candidate-location-list in vehicular networks. In *2015 IEEE International Conference on Communications (ICC)*. IEEE, 7292–7297.
[53] Syed Adeel Ali Shah, Ejaz Ahmed, Feng Xia, Ahmad Karim, Muhammad Shiraz, and Rafidah Md Noor. 2016. Adaptive beaconing approaches for vehicular ad hoc networks: A survey. *IEEE Systems Journal* 12, 2 (2016), 1263–1277.

[54] R. Yu, J. Kang, X. Huang, S. Xie, Y. Zhang, and S. Gjessing. 2016. MixGroup: Accumulative Pseudonym Exchanging for Location Privacy Enhancement in Vehicular Social Networks. *IEEE Transactions on Dependable and Secure Computing* 13, 1 (2016), 93–105.

[55] Abdelwahab Boualouache, Sidi-Mohammed Senouci, and Samira Moussaoui. 2016. VLPZ: The vehicular location privacy zone. *Procedia Computer Science* 83 (2016), 369–376.

[56] Abdelwahab Boualouache and Samira Moussaoui. 2017. TAPCS: Traffic-aware pseudonym changing strategy for VANETs. *Peer-to-Peer networking and Applications* 10, 4 (2017), 1008–1020.

[57] L. Zhang. 2017. OTIBAAGKA: A New Security Tool for Cryptographic Mix-Zone Establishment in Vehicular Ad Hoc Networks. *IEEE Transactions on Information Forensics and Security* 12, 12 (2017), 2998–3010. DOI: http://dx.doi.org/10.1109/TIFS.2017.2730479

[58] Abdelwahab Boualouache and Samira Moussaoui. 2017. Urban pseudonym changing strategy for location privacy in VANETs. *International Journal of Ad Hoc and Ubiquitous Computing* 24, 1-2 (2017), 49–64.

[59] Ferroudja Zidani, Fouzi Semchedine, and Marwane Ayaida. 2018. Estimation of Neighbors Position privacy scheme with an Adaptive Beaconing approach for location privacy in VANETs. *Computers & Electrical Engineering* 71 (2018), 359–371.

[60] C. Vaas, M. Khodaei, P. Papadimitratos, and I. Martinovic. 2018. Nowhere to hide? Mix-Zones for Private Pseudonym Change using Chaff Vehicles. *2018 IEEE Vehicular Networking Conference (VNC)* (2018), 1–8.

[61] Abdul Wahid, Humera Yasmeen, Munam Ali Shah, Masoom Alam, and Sayed Chhattan Shah. 2019. Holistic approach for coupling privacy with safety in VANETs. *Computer networks* 148 (2019), 214–230.

[62] N. Ravi, C. M. Krishna, and I. Koren. 2019. Enhancing Vehicular Anonymity in ITS: A New Scheme for Mix Zones and Their Placement. *IEEE Transactions on Vehicular Technology* 68, 11 (2019), 10372–10381.

[63] Xinghua Li, Huijuan Zhang, Yanbing Ren, Siqi Ma, Bin Luo, Jian Weng, Jianfeng Ma, and Xiaoming Huang. 2020. PAPU: Pseudonym Swap With Provable Unlinkability Based on Differential Privacy in VANETs. *IEEE Internet of Things Journal* 7, 12 (2020), 11789–11802.

[64] Messaoud Babaghayou, Nabila Labraoui, Ado Adamou Abba Ari, Mohamed Amine Ferrag, Leandros Maglaras, and Helge Janicke. 2021. Whisper: A location privacy-preserving scheme using transmission range changing for internet of vehicles. *Sensors* 21, 7 (2021), 2443.

[65] Ikram Ullah, Munam Ali Shah, and Abid Khan. 2021. Adaptive Grouping and Pseudonym Changing Policy for Protection of Vehicles Location Information in VANETs. In *2021 IEEE Symposium Series on Computational Intelligence (SSCI)*. 1–7. DOI: http://dx.doi.org/10.1109/SSCI50451.2021.9659852

[66] Mishri Saleh Al-Marshoud, Ali H Al-Bayatti, and Mehmet Sabir Kiraz. 2021. Improved Chaff-Based CMIX for Solving Location Privacy Issues in VANETs. *Electronics* 10, 11 (2021), 1302.

[67] Morten Dahl, Stéphanie Delaune, and Graham Steel. 2010. Formal analysis of privacy for vehicular mix-zones. In *Computer Security–ESORICS 2010: 15th European Symposium on Research in Computer Security (Proceedings 15)*. Springer, 55–70.

[68] Antoine Joux. 2000. A One Round Protocol for Tripartite Diffie–Hellman. In *Algorithmic Number Theory*, Wieb Bosma (Ed.). Springer Berlin Heidelberg, Berlin, Heidelberg, 385–393.

[69] Bin Fan, Dave G Andersen, Michael Kaminsky, and Michael D Mitzenmacher. 2014. Cuckoo filter: Practically better than bloom. In *Proceedings of the 10th ACM International on Conference on emerging Networking Experiments and Technologies*. 75–88.

[70] Mohammad Khodaei and Panos Papadimitratos. 2020. Cooperative Location Privacy in Vehicular Networks: Why Simple Mix Zones are Not Enough. *IEEE Internet of Things Journal* 8, 10 (2020), 7985–8004.

[71] Nan Guo, Linya Ma, and Tianhan Gao. 2018. Independent Mix Zone for Location Privacy in Vehicular Networks. *IEEE Access* 6 (2018), 16842–16850. DOI: http://dx.doi.org/10.1109/ACCESS.2018.2800907

[72] A. Boualouache and S. Moussaoui. 2014. S2SI: A Practical Pseudonym Changing Strategy for Location Privacy in VANETs. (2014), 70–75. DOI: http://dx.doi.org/10.1109/INDS.2014.20

[73] Shalini Batra and Avleen Kaur Malhi. 2015. An efficient certificateless aggregate signature scheme for vehicular ad-hoc networks. *Discrete Mathematics & Theoretical Computer Science* 17 (2015).

[74] Qi Feng, Debiao He, Sherali Zeadally, and Kaitai Liang. 2019. BPAS: Blockchain-assisted privacy-preserving authentication system for vehicular ad hoc networks. *IEEE Transactions on Industrial Informatics* 16, 6 (2019), 4146–4155.

[75] Julien Freudiger, Reza Shokri, and Jean-Pierre Hubaux. 2009. On the Optimal Placement of Mix Zones. *Proceedings of the 9th International Symposium on Privacy Enhancing Technologies* (2009), 216–234.

[76] Yipin Sun, Bofeng Zhang, Baokang Zhao, Xiangyu Su, and Jinshu Su. 2015. Mix-zones optimal deployment for protecting location privacy in VANET. *Peer-to-Peer Networking and Applications* 8, 6 (2015), 1108–1121.

[77] Murtuza Jadliwala, Igor Bilogrevic, and Jean-Pierre Hubaux. 2013. Optimizing Mix-Zone Coverage in Pervasive Wireless Networks. *Journal of Computer Security* 21, 3 (May 2013), 317–346.

[78] Xinxin Liu, Han Zhao, Miao Pan, Hao Yue, Xiaolin Li, and Yuguang Fang. 2012. Traffic-aware multiple mix zone placement for protecting location privacy. In *2012 Proceedings IEEE INFOCOM*. IEEE, 972–980.

[79] A. R. Svaigen, H. S. Ramos, L. B. Ruiz, and A. A. F. Loureiro. 2019. Dynamic Temporal Mix-Zone Placement Approach for Location-Based Services Privacy. *2019 IEEE Latin-American Conference on Communications (LATINCOM)* (2019), 1–6.

[80] N. Ravi, C. M. Krishna, and I. Koren. 2023. Privacy and Traffic Efficiency under Dynamic Conditions in ITS. *Unpublished manuscript* (2023).

[81] Mishri Saleh AlMarshoud, Ali H. Al-Bayatti, and Mehmet Sabir Kiraz. 2022. Location privacy in VANETs: Provably secure anonymous key exchange protocol based on self-blindable signatures. *Vehicular Communications* 36 (2022), 100490.