People's Democratic Republic of Algeria
Ministry of Higher Education and Scientific Research
Mohamed El Bachir El Ibrahimi University of Bordj Bou Arréridj
Faculty of Mathematics and Computer Science
Department of Computer Science

DISSERTATION
Presented in fulfillment of the requirements of obtaining the degree
Master in Computer Science
Specialty: Networking & Multimedia

THEME

An Enhanced Pseudonym Change Scheme for Privacy Preservation in Vehicular Ad-Hoc Networks (VANETs)

Presented by:

AMMARI Mohammed EL Amine

MEGRAH Kaouther

Publicly defended on: 11/06/2025

In front of the jury composed of:

President: BELALTA Ramla

Examiner: FILLALI Ferhat

Supervisor: MOUSSAOUI Boubakeur

2024/2025

Dedication

For those who come after.

Mohammed

To my parents, for instilling in me the values of hard work and perseverance.
To my beloved mother, whose endless love, prayers, and sacrifices have been a guiding light through every challenge.
To my family, whose unwavering support and encouragement have formed the foundation of my journey.
To my dear friends, for your laughter, companionship, and motivation that helped me stay strong in difficult times.
And to everyone who believed in me when the road was uncertain—your faith carried me forward.
This achievement is as much yours as it is mine.

kaouthar

Acknowledgment

الحمد لله أولا وآخرا، ظاهرا وباطنا، على نعمه التي لا تُعد ولا تُحصى، والتي لولاها لما كان لهذا العمل أن يكتمل. نحمده سبحانه على توفيقه وتيسيره، ونسأله أن يتقبّل هذا الجهد خالصا لوجهه الكريم.

We would like to express our deepest gratitude to our beloved parents and siblings for their unconditional love, prayers, and unwavering support, which have been the foundation of our journey.

We sincerely thank our supervisor, Dr. Boubakeur Moussaoui, for his invaluable guidance and insight.

We thank our colleagues whose encouragement made this journey meaningful.

"May Allah bless everyone who supported us along this path and reward them generously in this life and the Hereafter."

ملخص

في شبكات المركبات اللاسلكية (VANETs)، تقوم المركبات بإرسال معلومات حساسة بشكل دوري، مثل الموقع والسرعة والاتجاه، إلى المركبات المجاورة. وعلى الرغم من أن هذه الاتصالات ضرورية لتطبيقات السلامة، إلا أنها تثير مخاوف جدية تتعلق بالخصوصية، خصوصاً خطر التتبع غير المصرح به للمركبات. في هذا العمل، نقوم بتحسين آلية موجودة لتغيير الأسماء المستعارة تُعرف باسم CPN (تغيير الاسم المستعار التعاوني اعتماداً على عدد الجيران)، من خلال إدخال شروط وخصائص جديدة، مثل فترة الصمت، بهدف تقوية عملية التغيير وضمان حدوثها فقط عند الضرورة. تم تنفيذ الحل المقترح باستخدام إطار المحاكاة PREXT، وتم تقييمه عبر مجموعة من المحاكاة. تُظهر النتائج أن النهج المقترح يحقق توازناً أفضل بين كفاءة استخدام الأسماء المستعارة وحماية الخصوصية، حيث يقلل من خطر تتبع المركبات دون التسبب في استهلاك غير ضروري للأسماء المستعارة.

الكلمات المفتاحية: VANET، الخصوصية، الأمان، تغيير الاسم المستعار، فترة الصمت، PREXT.

Abstract

In Vehicular Ad hoc Networks (VANETs), vehicles regularly broadcast critical information such as their position, speed, and direction to neighboring nodes. While essential for safety applications, this communication raises serious privacy concerns, particularly the risk of unauthorized vehicle tracking. To address this issue, various pseudonym change strategies have been proposed. In this work, we enhance an existing cooperative pseudonym change scheme, known as CPN (Cooperative Pseudonym Change based on the Number of Neighbors), by introducing new conditions and features, such as a silent period, that aim to strengthen the change process and ensure it occurs only when necessary. The proposed solution is implemented within the PREXT framework and evaluated through simulation. The results demonstrate that our approach achieves a better balance between pseudonym efficiency and privacy protection, reducing the risk of vehicle traceability while avoiding unnecessary pseudonym consumption.

Keywords: VANET, privacy, security, pseudonym change, silent period, PREXT.

Résumé

Dans les réseaux ad hoc véhiculaires (VANETs), les véhicules diffusent régulièrement des informations critiques telles que leur position, leur vitesse et leur direction aux nœuds voisins. Bien que cette communication soit essentielle pour les applications de sécurité, elle soulève de sérieuses préoccupations en matière de vie privée, notamment le risque de suivi non autorisé des véhicules. Pour remédier à ce problème, diverses stratégies de changement de pseudonyme ont été proposées. Dans ce travail, nous améliorons un schéma existant de changement de pseudonyme coopératif, connu sous le nom de CPN (Changement de Pseudonyme Coopératif basé sur le Nombre de Voisins), en introduisant de nouvelles conditions et fonctionnalités — telles qu'une période de silence — visant à renforcer le processus de changement et à s'assurer qu'il ne se produit que lorsque cela est nécessaire. La solution proposée est implémentée dans le cadre du simulateur PREXT et évaluée à travers des simulations. Les résultats démontrent que notre approche atteint un meilleur équilibre entre l'efficacité de l'utilisation des pseudonymes et la protection de la vie privée, en réduisant le risque de traçabilité des véhicules tout en évitant une consommation excessive de pseudonymes.

Mots-clés: VANET, vie privée, sécurité, changement de pseudonyme, période de silence, PREXT.

Table of Contents

Abbreviations list

BSM	Basic Safety Message
C-ITS	Cooperative Intelligent Transport Systems
CAM	Cooperative Awareness Messages
CPN	Cooperative Pseudonym Change based on Number of Neighbors
DENM	Decentralized Environmental Notification Messages
DSRC	Dedicated Short-Range Communications
E-CPN	Enhanced CPN
ETSI	European Telecommunications Standards Institute
I2I	Infrastructure-to-Infrastructure
IEEE	Institute of Electrical and Electronics Engineers
ITS	Intelligent Transport Systems
MANETs	Mobile Ad-Hoc Networks
NNPDA	Nearest-Neighbor Probabilistic Data Association
OBU	On Board Unit
OMNeT++	Objective Modular Network Testbed in C++
PREXT	Privacy Extension for Veins Framework
RSU	Road Side Unit
SUMO	Simulation of Urban Mobility
TA	Trusted Authority
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
VANETs	Vehicular Ad-Hoc Networks
Veins	Vehicles In Network Simulation
WAVE	Wireless Access in Vehicular Environments

List of Figures

List of Tables

List of Algorithms

General Introduction

Road traffic accidents continue to be a major concern worldwide, posing serious threats to both public safety and national economies. According to the World Health Organization (WHO), approximately 1.19 million people die each year as a result of road traffic crashes. In Algeria, the situation mirrors these global concerns. According to the National Delegation for Road Safety (DNSR), the country recorded 26,067 road accidents in 2024, which resulted in 3,740 deaths and 35,256 injuries. These figures represent a noticeable increase compared to previous years and highlight the urgent need for more effective solutions. The vast majority of these incidents were attributed to human error, including speeding, dangerous overtaking, and general negligence. In addition to the tragic loss of human life, the economic cost of these accidents is staggering, with estimates indicating an annual financial burden of over 100 billion dinars.

To tackle these issues, modern transportation research has increasingly focused on Intelligent Transportation Systems (ITS), which integrate communication and information technologies to improve road safety and traffic management. One of the most promising components of ITS is Vehicular Ad Hoc Networks (VANETs), which enable vehicles to exchange data with each other and with roadside infrastructure in real time. This real-time communication has the potential to prevent accidents, support safer driving behavior, and contribute significantly to building smarter and safer roads.

Although VANETs bring many benefits in terms of road safety and traffic flow, they also raise serious concerns about security and privacy. Vehicles regularly send out safety messages that include details like their location, speed, and direction. While this information helps avoid accidents and supports cooperative driving, it can also be misused by attackers to monitor and track vehicles over time. This kind of tracking puts driver privacy at risk and could even

lead to safety threats. To protect against this, vehicles often use pseudonyms instead of real identities. However, just using pseudonyms is not enough, because attackers can still follow the same vehicle by analyzing message patterns. That's why finding better ways to protect driver anonymity without affecting communication is a key challenge in VANET research. Solving this issue is important to help build trust in these systems and make sure they can be used safely in the real world.

As mentioned earlier, vehicles rely on pseudonyms—temporary identifiers—instead of their real identities to protect their privacy while communicating. This helps reduce the risk of being tracked. But if a pseudonym is used for too long, or if changes happen without coordination, it becomes easier for attackers to link those identities together and follow a vehicle over time. To make this harder, some strategies suggest that vehicles change their pseudonyms together, based on certain conditions like how many nearby vehicles are present. While these methods improve privacy compared to random or individual changes, they still face limitations in terms of efficiency, adaptability, or effectiveness in high-mobility scenarios. In this work, we propose an improved cooperative pseudonym change approach that aims to deal with those issues. Our method uses smarter coordination between vehicles and includes silent periods—short moments where communication is paused—to make it harder for attackers to follow and link messages

To explore and evaluate our proposed solution, this dissertation is organized as follows:

- **Chapter 1:** introduces Vehicular Ad Hoc Networks (VANETs), their main features, how they work, and the role they play in Cooperative Intelligent Transport Systems (C-ITS).
- **Chapter 2:** focuses on the security and privacy challenges in VANETs, with an emphasis on privacy threats and existing protection methods.
- **Chapter 3:** provides an overview of the related works, followed by a detailed description of our proposed solution, including its design, implementation, and the improvements it aims to bring.
- **Chapter 4:** presents the simulation setup, the evaluation process, and compares the performance of our approach to existing solutions.
- Finally, the dissertation ends with a conclusion that summarizes the work

Chapter 1

Overview of vehicular ad-hoc networks

1.1 Introduction

This chapter presents an overview of VANETs, a fundamental technology within Cooperative Intelligent Transport Systems (C-ITS). We introduce the basic architecture and describe the different types of communication between vehicles and infrastructure. The chapter also outlines the main types of messages exchanged in VANETs, highlights key applications in modern transportation, and explains how VANETs contribute to developing smarter, safer road systems.

1.2 Definition

VANETs are a specialized form of Mobile Ad-Hoc Networks (MANETs) that enable vehicles to communicate with each other and with roadside infrastructure without relying on fixed infrastructure. These networks are characterized by high mobility, dynamic topologies, and the ability to support a wide range of applications aimed at improving road safety, traffic efficiency, and passenger comfort. VANETs leverage advanced technologies such as onboard sensors, GPS, and wireless communication interfaces to facilitate real-time data exchange among vehicles and between vehicles and infrastructure. This capability is fundamental to the development of C-ITS, which aim to enhance transportation systems through increased connectivity and automation. [1]

1.3 Characteristics

- **High mobility and dynamic topology**

  In VANETs, nodes are vehicles that move at high speeds, resulting in frequent and rapid changes in network topology. This dynamic nature affects link stability and necessitates routing protocols that can adapt quickly to maintain reliable communication.

- **Road-constrained mobility**

  Unlike general mobile networks, VANET node movement is limited by road layouts, traffic signals, and legal constraints. This structured mobility enables trajectory estimation but also introduces unique constraints that influence communication patterns.

- **Intermittent connectivity**

  The combination of high mobility and variable vehicle density leads to unstable and short-lived communication links. This intermittent connectivity presents challenges for data delivery, particularly for time-sensitive applications.

- **Hybrid communication model**

  VANETs combine Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication to support both decentralized and infrastructure-assisted networking. This hybrid model enhances coverage and functionality but introduces dependencies on infrastructure availability.

- **Resource availability**

  Vehicles are generally equipped with ample processing power and a reliable energy source, allowing the execution of complex communication and computing tasks. This distinguishes VANETs from other ad hoc networks with stricter resource constraints.

- **Geographic awareness**

  Most VANET nodes possess positioning capabilities, such as GPS, enabling location-based services and geographic routing. This spatial awareness is a core feature that supports many VANET applications.

- **Scalability challenges**

  VANET environments vary from low-density highways to high-density urban roads, requiring network protocols to operate efficiently across different scales. Ensuring stable performance under diverse traffic conditions is a key design challenge.

1.4 Communication modes in VANETs

VANETs use distinct communication types to coordinate data exchange between vehicles, infrastructure, and traffic systems. These include:

1.4.1 Vehicle to vehicle communication(V2V)

V2V Communication is the primary mode used in VANETs. It allows direct wireless exchange of data such as position, speed, and direction between vehicles. These real-time updates help each vehicle build a dynamic view of its immediate surroundings, identify nearby vehicles, and adapt its behavior accordingly. V2V communication also enables the transmission of alerts about road conditions, obstacles, or incidents, which can be propagated to nearby vehicles for cooperative awareness.

1.4.2 Vehicle to infrastructure communication (V2I)

V2I communication refers to the wireless exchange of data between vehicles and roadside infrastructure elements such as Road Side Unit (RSU), traffic lights, and digital signage. Through this interaction, vehicles can receive dynamic information about traffic light phases, speed limits, construction zones, weather conditions, or detours. RSUs may also collect data from passing vehicles (e.g., congestion levels or environmental measurements) and relay it to traffic management centers for real-time analysis and decision-making. This bidirectional flow supports both driver assistance systems and infrastructure-side optimization of traffic flow.

1.4.3 Infrastructure to infrastructure communication(I2I)

Infrastructure-to-Infrastructure (I2I) communication enables data exchange between stationary network components, such as RSUs, surveillance cameras, environmental sensors, and traffic control systems. These connections often rely on high-speed wired or fiber-optic links to

ensure stable and fast communication. By sharing information like traffic density, signal timing, or detected incidents, different infrastructure nodes can synchronize actions — for example, adjusting traffic lights across intersections to reduce congestion or coordinating emergency response routes. I2I plays a key role in creating a unified, responsive urban mobility network.

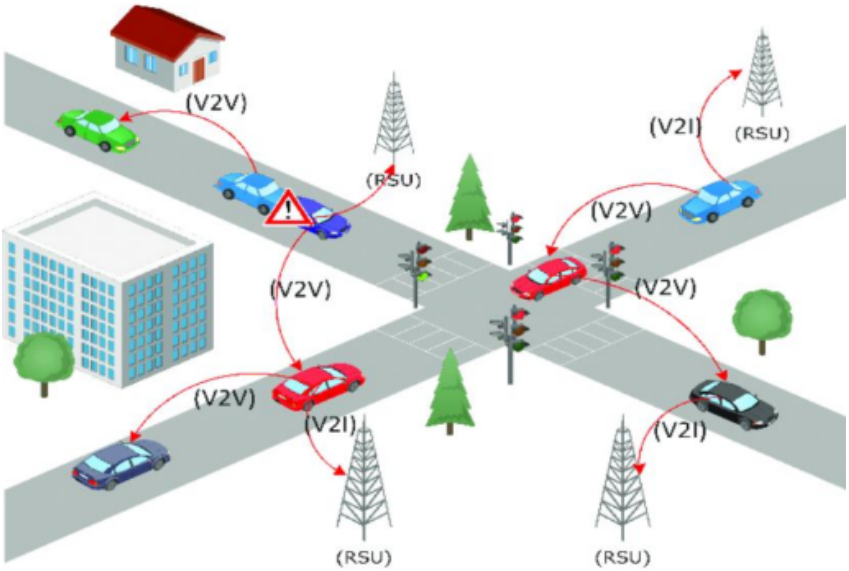

Figure 1: Key components in a VANET [2]

1.5 Key components in a VANET

The architecture of VANETs is built upon three fundamental components that enable communication and network functionality: On Board Unit (OBU), RSU. Through the coordinated interaction between these elements, VANETs can meet their objectives of providing safer roads, more efficient traffic management, and enabling the evolution of modern intelligent transportation systems.

1.5.1 On-board units(OBU)

OBU are embedded communication systems installed in vehicles, responsible for enabling wireless communication with other vehicles and roadside infrastructure. Each OBU typically includes a processor, memory, wireless interfaces, and positioning modules that allow vehicles to exchange real-time data such as traffic conditions, hazard alerts, and infotainment services. This capability supports the formation of highly dynamic networks in which vehicles frequently join and leave, requiring robust protocols to maintain consistent connectivity.

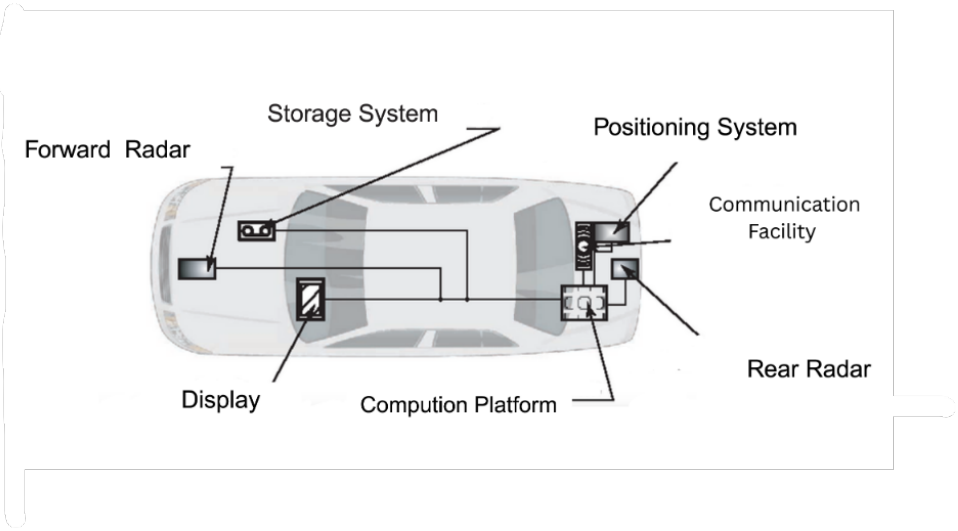

Figure 2: Elements of an intelligent vehicle[3]

1.5.2 Roadside units(RSU)

RSU are stationary infrastructure nodes deployed along highways, intersections, and urban roads. They support vehicular communication by relaying messages between vehicles, broadcasting critical information such as weather alerts or road closures, and occasionally serving as communication bridges to the Trusted Authority (TA). RSUs play a key role in extending network coverage and improving reliability, especially in situations where direct V2V communication is limited or obstructed.

Figure 3: Road side unit device [4]

1.6 WAVE: Architecture and communication standards

Wireless Access in Vehicular Environments (WAVE) architecture constitutes a foundational framework specifically designed to support communication systems in mobile environments, particularly within VANETs. Its primary objective is to enable reliable, real-time communication between vehicles V2V and between vehicles and infrastructure V2I, leveraging Dedicated Short-Range Communications (DSRC) technology.

Several international regulatory bodies have allocated spectrum in the 5.9 GHz band to support DSRC deployment. The U.S. Federal Communications Commission (FCC) designated 75 MHz in this band, while the European Telecommunications Standards Institute (ETSI) reserved 30 MHz. These allocations provide a dedicated frequency band for vehicular communications, minimizing interference and ensuring reliable, low-latency data exchange essential for safety-critical applications in VANETs.

The WAVE architecture comprises a suite of integrated standards developed by the Institute of Electrical and Electronics Engineers (IEEE), most notably the IEEE 802.11p standard[5], which is a tailored amendment to the original IEEE 802.11 protocol. It is optimized for high-mobility environments, addressing both the physical layer and the medium access control (MAC) sublayer. IEEE 802.11p enables direct data transmission between vehicles without the need for a fixed access point, with low latency to support time-critical applications.

Complementing this, the IEEE 1609.x family of standards extends the functionality of IEEE 802.11p and includes:

- **IEEE 1609.1**[6]: Specifies the architecture and management services for application development within the WAVE system. It defines interfaces for resource allocation, application prioritization, and data flow between the application layer and the rest of the stack, enabling modular and flexible application deployment.

- **IEEE 1609.2**[7]: Defines security services including encryption, authentication, and digital signatures to ensure message integrity and confidentiality. A detailed discussion of this standard will be provided in Section 2.2.2.2.

- **IEEE 1609.3**[8]: Covers network and transport layer services, supporting both IPv6 and WAVE Short Message Protocol (WSMP). WSMP is a lightweight, low-latency protocol

optimized for safety-critical messaging, allowing rapid broadcast of alerts without the overhead of traditional IP-based communication.

- **IEEE 1609.4**[9]: Enables multi-channel operation by managing the timing and synchronization between the control channel (CCH) and multiple service channels (SCHs). It supports channel switching, QoS prioritization, and channel coordination to balance safety and non-safety application demands efficiently.

This layered architecture enables a balanced approach to diverse communication requirements, such as low-latency safety messaging and support for traditional Internet Protocol (IPv6)-based services like infotainment or navigation. The WAVE suite integrates dedicated security mechanisms—primarily defined in IEEE 1609.2—including digital signatures, encryption, and certificate-based authentication, which serve as a defense against common threats such as eavesdropping, replay attacks, and identity spoofing. These protections enhance trust and resilience across the VANET ecosystem.

While the WAVE architecture generally aligns with the traditional OSI communication model, it extends beyond it by introducing cross-layer management and security components. For instance, IEEE 1609.1 addresses application and resource management, while IEEE 1609.2 defines out-of-band security services. This results in a flexible yet robust protocol stack that does not strictly adhere to the seven-layer model, enabling secure, efficient, and scalable communications tailored to the unique demands of vehicular environments.

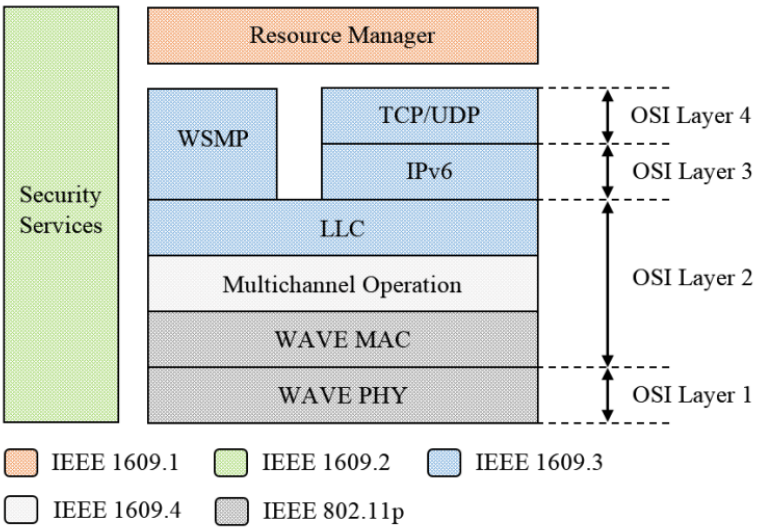

Figure 4: Structure of the DSRC/WAVE[10]

1.7 Types of messages in VANETs

In VANETs, vehicles and infrastructure exchange different types of messages to support real-time awareness, coordination, and service delivery. These messages generally fall into three categories:

1.7.1 Beacon messages

Beacon messages are periodically broadcast by vehicles to share their current position, speed, and direction. They are essential for maintaining awareness of surrounding vehicles and enabling mobility-related decisions. This message type is used in most communication protocols due to its role in building a dynamic network view. However, malicious actors can also exploit beacon messages to track vehicles or disrupt the network, making them a potential vector for privacy and security breaches.

1.7.2 Alert messages

Alert messages are sent in response to specific events like sudden braking, accidents, or unexpected obstacles. They are used to warn nearby vehicles and infrastructure of immediate hazards. These messages are time-sensitive and are prioritized to ensure quick dissemination in critical situations.

1.7.3 General purpose

General-purpose messages are used for non-safety communications such as navigation updates, infotainment, and interaction with roadside services. They are typically less urgent and are transmitted without interfering with safety-related messaging. Their role is to enhance the overall driving experience and system functionality.

1.8 Cooperative intelligent transportation systems

1.8.1 Definition

Intelligent Transport Systems (ITS) are infrastructure-centric platforms that apply information technologies (e.g., sensors, centralized traffic control) to monitor and optimize transportation networks. C-ITS extends this paradigm by enabling machine-to-machine coordination through direct V2V/V2I communication, primarily via VANETs (IEEE 802.11p/DSRC) using standardized messaging protocols. Unlike traditional C-ITS, which relies on human-mediated responses, C-ITS automates decision-making through the IEEE 1609.x family of standards (addressing security, networking, and resource management), creating a federated system where vehicles and infrastructure jointly process real-time data. This cooperative framework serves three fundamental objectives: enhancing road safety through proactive hazard prevention, optimizing network efficiency via coordinated vehicle routing, and enabling scalable mobility services while preserving compatibility with legacy infrastructure, ultimately delivering faster, safer, and more sustainable transportation ecosystems for all users [11]

1.8.2 Applications

C-ITS delivers real-world benefits through three main types of applications: safety systems that prevent accidents, traffic services that reduce congestion, and driver services that improve the travel experience. We now examine each category below:

- **Road safety applications:**

  C-ITS safety systems aim to prevent accidents by enabling vehicles and infrastructure to share critical warnings in real time. These systems alert drivers to immediate hazards—like sudden stops ahead, road obstacles, or emergency vehicles—giving them more time to react. For example, a car involved in a collision can automatically warn nearby vehicles to brake or change lanes, reducing the risk of further accidents.

- **Traffic management applications:**

  C-ITS traffic systems optimize vehicle flow and reduce congestion across both urban and highway environments. By coordinating real-time data between vehicles and smart infrastructure, these systems dynamically adjust routes and traffic signals based on current conditions. In cities, they might shorten red lights when roads are clear; on highways,

they could suggest alternate routes when accidents occur - all designed to cut travel time, reduce emissions, and keep traffic moving efficiently.

- **Comfort and smart services applications:**
  C-ITS enhances the driving experience through convenient services that go beyond safety and traffic needs. These include entertainment options like streaming music, real-time internet access, and location-based assistance such as finding and reserving parking spots. For example, vehicles can automatically locate and reserve parking spaces at destinations like shopping centers, with payment processed through C-ITS infrastructure.

1.8.3 User adoption barrier in C-ITS:

One of the key obstacles to the deployment of C-ITS lies in user acceptance. Encouraging drivers to equip their vehicles with OBU and actively participate in data-sharing networks is difficult. Privacy concerns, such as constant location tracking and potential misuse of personal data, lead to hesitancy. Additionally, many users may distrust the systems managing their information or may not perceive immediate personal benefits, making voluntary adoption a significant challenge for large-scale implementation.

1.9 Conclusion

In this chapter, we introduced VANETs, the definition, architecture, key characteristics, and application domains. We outlined how VANETs support real-time communication among vehicles and infrastructure, enabling various cooperative services aimed at improving road safety and traffic efficiency. This foundational overview sets the stage for the next chapter, which will focus on security and privacy aspects in VANETs.

Chapter 2

Security and privacy in VANETs

2.1 Introduction

This chapter provides an overview of the security and privacy foundations in VANETs. As vehicles become increasingly connected through real-time communication with infrastructure and other vehicles, ensuring secure and private data exchange becomes critical. The authors of [12] highlight that the unique characteristics of this type of network, such as high mobility, frequent topology changes, and decentralized operation, introduce complex challenges that demand robust solutions. In this chapter, we review the key security requirements, common threat models, and established architectures and standards. We also examine major privacy concerns and explore a range of protection mechanisms designed to mitigate them.

2.2 Security in VANETs

2.2.1 Security requirements

1. **Authentication:**

   Authentication serves as the primary defense against potential threats, ensuring that all messages originate from legitimate and verifiable sources. Each vehicle is assigned a unique identifier, such as a license plate or cryptographic certificate, to distinguish it within the network. This process prevents attackers from impersonating legitimate nodes

by verifying both the sender's identity and the vehicle's unique identifier. In the highly dynamic environment of VANETs, where rapid information exchange supports safety-critical applications, robust authentication is essential. Without it, malicious actors could inject false data, disrupt communication, and undermine the trust necessary for effective vehicular operations.

2. **Integrity and Consistency:**

   Integrity ensures that data remains unaltered from generation to reception. In VANETs, this means all information—safety alerts, traffic updates, or other messages—must be preserved exactly as transmitted. Since vehicles rely on this data for split-second decisions, even minor alterations could lead to critical errors, such as collisions or misdirected traffic. Maintaining integrity is crucial, as tampering—whether from sensor errors or malicious activity—can severely compromise vehicular communication safety and effectiveness.

   Consistency refers to the uniformity and logical coherence of data within the network. In the dynamic environment of VANETs, numerous nodes constantly share and update information, necessitating a synchronized perspective. In the absence of consistency, conflicting data, like varying reports on road conditions, can lead to confusion and potential hazards. Therefore, ensuring consistency is crucial for reliable decision-making, ultimately enhancing the safety and efficiency of the transportation system.

3. **Confidentiality:**

   Confidentiality refers to the protection of sensitive information from unauthorized access or disclosure, ensuring that only authorized entities can access the data. In the context of VANETs, confidentiality is of paramount importance, as vehicles and infrastructure continuously exchange sensitive information, including real-time location data, driver identities, and trip details. While the open communication framework of VANETs is essential for enabling safety and operational efficiency, this very openness creates vulnerabilities, exposing sensitive data to potential misuse.

4. **Availability:**

   Availability ensures that VANET services and resources remain accessible without disruption, enabling vehicles to exchange critical information in real-time. Given vehicles' rapid movement and the network topology's dynamic nature, uninterrupted communication is essential for maintaining road safety and traffic efficiency. If availability is compromised, time-sensitive safety messages, such as collision warnings or road hazard alerts, may fail to reach their intended recipients, significantly increasing the risk of accidents. Furthermore, disruptions in availability can impair navigation systems, traffic coordination, and emergency response services, rendering the network unreliable for its users.

5. **Access control:**

   Access control regulates which entities can participate in communication and access network resources within VANETs. Given these networks' open and dynamic nature, it is essential to implement mechanisms that restrict access to only legitimate vehicles and infrastructure components. Unauthorized access can result in data manipulation, service disruptions, or malicious activities, all undermining network reliability and safety. Effective access control mechanisms maintain structured communication by defining permission levels based on authentication credentials, ensuring that only verified and authorized entities can interact with the system.

6. **Non-repudiation:**

   Non-repudiation ensures that the origin and receipt of messages within VANETs are undeniable, providing accountability among participants. This is particularly critical for validating the source of information in scenarios such as traffic violations or accidents, where traceability is essential. By guaranteeing that messages, such as emergency alerts or traffic updates, can be traced back to their senders, non-repudiation facilitates accurate event reconstruction and supports legal proceedings. Without it, malicious actors could deny transmitting harmful or false data, undermining the network's reliability and the integrity of vehicular communications.

7. **Privacy:**

   Privacy in VANETs refers to protecting sensitive data related to vehicles and their occupants, ensuring that unauthorized entities cannot access or misuse this information. Since vehicle data, such as location, speed, and travel history, can be directly linked to individuals, compromising this information constitutes a breach of personal privacy. Unauthorized tracking and profiling could deter individuals from adopting VANET-based technologies, hindering the widespread implementation. Strong privacy protections are essential to fostering public trust and encouraging participation, as users must feel confident that their personal information will remain secure while benefiting from the network's safety and efficiency features.

2.2.2 Security architectures and standards

Vehicular networks require robust security frameworks to ensure that safety- and non-safety–critical messages are exchanged securely and reliably. In VANETs, public-key cryptography underpins centralized trust models, where Certification Authorities (CAs) and a top-level Root Certification Authority (Root CA) manage certificate issuance, revocation, and policy enforcement. This architecture addresses authentication, message integrity, and non-repudiation in a highly mobile and broadcast environment, while preserving privacy through mechanisms such as pseudonym rotation. In the following subsections, we first describe the Public Key Infrastructure (PKI) trust model and its key components, and then review the principal standards—IEEE 1609.2 and ETSI TS 102 940—that formalize security services, certificate lifecycles, and interoperability requirements for vehicle-to-everything (V2X) communications.[13]

2.2.2.1 Public key infrastructure(PKI)

PKI forms the foundation of centralized security architectures in VANETs, enabling authentication, key management, and secure communication. At the top of this hierarchical trust model, a Root CA serves as the ultimate trust anchor, responsible for overseeing policy enforcement, identity resolution, and coordination across subordinate Certification Authorities (CAs). These CAs issue, revoke, and manage digital certificates that bind a vehicle's identity to its public key. Each vehicle receives a unique public-private key pair and a CA-issued certificate to validate its identity. Messages are signed using the sender's private key and verified

using the corresponding public key. To bootstrap trust, every vehicle must pre-install and trust the Root CA's public key. While PKI enforces essential security properties—authentication, integrity, and non-repudiation—its centralized nature introduces potential privacy challenges if certificate usage is not properly anonymized. To mitigate this, VANETs employ short-lived certificates and pseudonym changes, concealing long-term identifiers while preserving traceability when necessary for accountability or safety. As the de facto trust framework in VANETs, PKI is standardized by IEEE 1609.2 and ETSI TS 102 940, which define certificate formats, revocation methods, and cross-domain interoperability.

2.2.2.2 Standards:

- **IEEE 1609.2:** Part of the IEEE 1609 WAVE suite (built on DSRC, 1.6), IEEE 1609.2 defines security services for V2X over IEEE 802.11p, including authentication, encryption, and certificate management. It specifies cryptographic algorithms (e.g., Elliptic Curve Digital Signature Algorithm (ECDSA) for signing, Advanced Encryption Standard (AES) for payload encryption), message formats for Basic Safety Message (BSM), and the use of short-lived pseudonym certificates to balance privacy with accountability. The standard also formalizes certificate revocation methods—both Certificate Revocation List(CRL) and Online Certificate Status Protocol (OCSP), to mitigate compromised nodes. Widely adopted in North America, it aligns with the U.S. Department of Transportation security requirements.[7]

- **ETSI TS 102 940:**

  As part of European Telecommunications Standards Institute (ETSI)'s ITS Security series, TS 102 940 builds on EN 302 637-2 by embedding General Data Protection Regulation (GDPR)-compliant anonymization into vehicular communications. It prescribes pseudonym lifecycle management—defining issuance intervals, pseudonym pools, and mandatory periodic changes—to prevent long-term tracking. Harmonized with the certificate framework of IEEE 1609.2, it adds data-minimization rules for Cooperative Awareness Messages (CAM) and Decentralized Environmental Notification Messages (DENM), ensuring sensitive data (e.g., precise location, speed) remains anonymous unless legal traceability is invoked.[14]

2.2.3 Threats and attack vectors

2.2.3.1 Nature of attackers:

1. **Attacker by affiliation:**

   These attackers are classified based on their network credentials. Insider attackers possess legitimate access and leverage it to manipulate communications or disrupt operations from within, while outsider attackers are unauthorized entities that attempt to penetrate the system without valid credentials, often employing methods to bypass existing authentication and security measures.

2. **Attacker by capability:**

   Attackers can be either passive or active based on their methods. Passive attackers observe network traffic to gather information without interfering, focusing solely on data collection and analysis. Active attackers, by contrast, modify, inject, or disrupt messages in real time, directly compromising the network's stability and reliability.

3. **Attacker by resources & scale:**

   Attackers are distinguished by their resources and the scale of their operations. Single-entity attackers consist of one compromised node acting independently to achieve its objectives, whereas distributed attackers involve multiple compromised entities collaborating in a coordinated manner to amplify the impact of their attack.

4. **Attacker by proximity:**

   Attackers can also be categorized based on their physical distance from the target. Local attackers operate within the immediate wireless range of the system, using direct access to interfere with communications, while global attackers act remotely, exploiting vulnerabilities in the network infrastructure or cloud systems without requiring physical proximity.

5. **Attacker by motivation:**

   Attackers can be driven by different motivations. Rational attackers act with clear objectives such as financial profit, strategic gain, or personal benefit. In contrast, malicious

attackers aim to disrupt network operations, spread misinformation, or undermine security without necessarily pursuing a tangible or personal reward.

2.2.3.2 Common attacks in VANETs:

1. **Spoofing attacks:**

   An adversary falsifies its identity by impersonating a legitimate vehicle or roadside unit. This undermines the authenticity of communications within the network, as the attacker uses fabricated identifiers or stolen credentials to mislead other participants, potentially causing vehicles to respond to false information.

2. **Sybil attacks:**

   A single malicious entity creates multiple fake identities within the network. This proliferation of counterfeit nodes disrupts trust and consensus mechanisms, as the attacker can manipulate network decisions by presenting a false image of widespread participation.

3. **Denial-of-service attacks:**

   The attacker overwhelms network nodes or the entire system by saturating communication channels with excessive traffic or exploiting vulnerabilities in network protocols. Such attacks lead to significant delays or complete interruptions in the transmission of safety-critical messages, thereby degrading overall vehicular communication and safety.

4. **Message tampering (replay & alteration attacks):**

   This category includes replay attacks, where valid messages are resent to disturb the normal flow of information, and alteration attacks, where the content of transmitted messages is modified during transit. Both forms compromise the integrity of data, leading to a breakdown in reliable communication between vehicles.

5. **Eavesdropping:**

   The attacker covertly intercepts and monitors network communications to collect sensitive information, such as vehicle locations and driver data. Although no alterations are made to the data, the information gathered can be exploited later for more targeted or disruptive activities.

6. **Black hole & Grey hole attacks:**

   In black hole attacks, compromised nodes deliberately drop all incoming packets instead of forwarding them, effectively creating a communication void. Grey hole attacks involve selective or intermittent packet dropping. Both strategies result in significant data loss and disrupt the network's normal operations.

7. **Jamming attacks:**

   Wireless signals used in VANETs are disrupted by transmitting interfering radio frequencies that block or degrade communication channels. This interference can severely impair the timely exchange of information, which is essential for the safe operation of vehicular networks.

8. **Man-in-the-middle attacks:**

   An adversary intercepts and potentially alters the communication between two legitimate parties without their knowledge. By inserting themselves into the communication chain, the attacker can manipulate, delay, or falsify the transmitted information, undermining both the confidentiality and integrity of the data exchanged.

2.3 Privacy in VANETs

2.3.1 Privacy requirements

1. **Anonymity:**

   Anonymity ensures that vehicles and users cannot be directly identified through their communications or interactions within the VANET. This requirement mandates the dissociation of vehicular data from real-world identities, preventing adversaries from linking transmitted messages to specific individuals or vehicles. In VANETs, where nodes frequently broadcast sensitive information, anonymity mitigates the risks of surveillance, stalking, or profiling.

2. **Unlinkability:**

   Unlinkability guarantees that distinct actions or communications generated by the same vehicle cannot be correlated over time or across contexts. This requirement ensures that pseudonyms, identifiers, or transactional data remain isolated across sessions, locations, and applications. Unlinkability preserves user privacy by preventing adversaries from reconstructing movement trajectories or behavioral profiles.

3. **Minimal disclosure:**

   Minimal disclosure restricts data sharing to the minimum necessary for specific interactions. This requirement prevents vehicular systems from exposing non-essential information that could reveal identities, locations, or behavior. By limiting data exposure in VANETs' open communication environment, minimal disclosure mitigates adversarial exploitation of aggregated or contextual data while preserving functionality.

4. **Conditional traceability:**

   Conditional Traceability allows authorized entities to revoke anonymity under legally defined conditions while preserving privacy during normal operations. This requirement balances accountability (e.g., post-incident investigations) with identity protection in daily interactions. In VANETs, conditional traceability ensures privacy mechanisms accommodate lawful oversight without compromising compliance or system integrity.

5. **Scalability and usability:**

   Scalability and Usability necessitate privacy mechanisms capable of operating efficiently in VANETs' large-scale, high-speed environment while ensuring minimal user intervention. These mechanisms must support rapid topology shifts, fluctuating node densities, and strict real-time constraints without degrading performance or introducing operational burdens.

2.3.2 Privacy concerns and challenges

1. **Identity and location tracking:**

   Vehicular networks continuously broadcast messages containing unique identifiers and location data, which, if not properly secured, can be exploited by adversaries to track vehicles over time. For instance, BSMs—transmitted at 10 Hz under IEEE 1609.2—often include static identifiers (e.g., temporary MAC addresses) that adversaries correlate with spatiotemporal data to reconstruct vehicle trajectories. Studies have shown that even with pseudonym rotation, re-identification rates exceed 80% over extended periods due to predictable rotation intervals in early implementations [15]. This persistent tracking compromises user privacy, allowing attackers to build movement profiles, monitor routines, and identify individuals. Such vulnerabilities enable predatory behaviors like route-based ambushes or corporate espionage, undermining trust in VANET technologies.

2. **Metadata leakage:**

   Metadata—non-content information like timestamps, message frequencies, and signal strength—can inadvertently reveal critical details about vehicular activity. For example, V2I interactions expose traffic density during rush hours or pinpoint high-value targets (e.g., armored vehicles) through transmission patterns. While standards like ETSI TS 102 940 acknowledge metadata risks, they lack enforceable guidelines for minimizing leakage in ITS implementations [14]. Even encrypted communications leak metadata, enabling adversaries to infer vehicle proximity, network topology, or emergency response routes. This vulnerability undermines system privacy by exposing exploitable patterns without requiring explicit personal data.

3. **Behavioral profiling:**

   Behavioral profiling involves analyzing vehicular data to infer patterns about a driver's habits, routines, and preferences. CAM, for example, inadvertently expose metadata such as lane-changing frequency or reaction times to hazards. Machine learning models trained on aggregated BSMs can de-anonymize drivers by analyzing speed, acceleration, and braking patterns. Wiedersheim et al. demonstrated that driving style alone uniquely

identifies 70% of drivers within a dataset of 1,000 vehicles [16]. Even anonymized data can reveal sensitive information, such as frequently visited locations or consistent travel times, which adversaries exploit for commercial gain (e.g., insurance premium discrimination) or targeted attacks (e.g., blackmail based on inferred habits).

4. **Legal and regulatory challenges:**

   The deployment of VANETs must comply with stringent privacy regulations, such as GDPR in the EU and California Consumer Privacy Act (CCPA) in the U.S., both of which mandate data minimization, user consent, and the right to erasure. However, the operational requirements of VANETs—such as maintaining immutable logs for accident forensics and enabling real-time data sharing for collision avoidance—often conflict with these privacy mandates. For instance, GDPR's "right to be forgotten" contradicts the need to retain vehicular data for liability investigations. At the same time, CCPA's opt-out provisions may impede the timely dissemination of safety-critical information. Moreover, regional regulatory differences further complicate compliance; EU standards (e.g., ETSI TS 102 940) emphasize pseudonymization to protect user privacy, whereas U.S. frameworks (e.g., IEEE 1609.2) focus on traceability to support law enforcement. These conflicting requirements create legal ambiguities, potentially slowing cross-border VANET deployments and increasing liability risks for manufacturers.[17][18]

2.3.3 Privacy-preserving solutions

1. **Cryptographic**:

   Cryptographic solutions in VANETs employ encryption, digital signatures, and secure key management to protect communication channels, ensuring confidentiality, integrity, and authenticity. These methods authenticate nodes and verify messages while preventing unnecessary disclosure of sensitive data. Cryptographic protocols enforce anonymity and unlinkability by dissociating vehicular identities from transmitted information, enabling secure exchanges under adversarial conditions. Their integration into VANETs preserves operational efficiency while ensuring reliable and privacy-compliant communications.

2. **Non-cryptographic**:

   - **Pseudonyms:**

     Pseudonyms replace real vehicle identities with temporary, situation-specific identifiers. Regular changes to these pseudonyms make long-term tracking difficult while still allowing trusted authorities to reveal identities when needed by law. This approach balances privacy with the need for accountability.

   - **Mix-zones:**

     Mix-zones designate geographic regions where multiple vehicles simultaneously change pseudonyms. By obscuring the linkage between old and new identifiers, mix zones prevent adversaries from correlating vehicular activity across spatial boundaries, enhancing unlinkability in dynamic environments.

   - **Silent periods:**

     Silent periods enforce temporary communication halts during pseudonym transitions. By avoiding overlapping transmissions of old and new identifiers, these periods eliminate temporal correlations that adversaries could exploit to track vehicles across pseudonym changes.

2.3.4 Limitations of the solutions

Privacy-preserving solutions in VANETs introduce computational and communication overhead, impacting latency-sensitive applications such as collision avoidance. Scalability challenges arise as the network grows, increasing the complexity of key management, pseudonym distribution, and cryptographic processing. Furthermore, privacy measures often conflict with regulatory and security requirements; strong anonymity can hinder traceability for legal investigations or malicious actor identification. Balancing privacy, efficiency, and accountability demands adaptive strategies that minimize trade-offs while ensuring system reliability.

2.4 Conclusion

In this chapter, we talked about the core security and privacy aspects of VANETs. We outlined the essential requirements, existing architectures, and widely recognized standards. We also reviewed common threats and attack types, followed by a discussion of the main privacy challenges and the available protection strategies. This foundation prepares us for the next chapter, where we will introduce our proposed enhancement to an existing privacy scheme.

Chapter 3

State of the art

3.1 Introduction

This chapter outlines the key concepts and existing research related to privacy protection in VANETs. It introduces the role of pseudonyms and digital certificates in securing vehicular communications. It then presents a structured review of pseudonym change strategies from the literature, categorized into static and dynamic approaches. Finally, it provides a comparative analysis of these strategies based on their design choices, limitations, and applicability.

3.2 Pseudonyms and certificates

Authentication plays a vital role in vehicular networks, as it enables the identification of message sources and helps maintain network integrity. However, to preserve user privacy, real identities must remain hidden from other vehicles and observers and only be accessible to a trusted authority. This dual requirement—ensuring both authentication and privacy—poses a major challenge in the deployment of vehicular communication systems. Using the real identity in transmitted messages is inappropriate. Yet, replacing it with a fixed pseudonym is also inadequate. For instance, if a vehicle follows a routine path—leaving from home in the morning and returning in the evening—an adversary could easily correlate location traces and infer the driver's identity based on behavioral patterns. This re-identification risk directly compromises the driver's privacy.

To address this, each registered vehicle is provided with a set of certified pseudonyms and their corresponding private keys by a trusted authority. Instead of using its true identity, the vehicle signs messages using the private key of the selected pseudonym. The authority remains the only entity capable of linking any pseudonym to the actual identity of the vehicle.

Nevertheless, pseudonym changes must be executed carefully. If not done properly, adversaries may still be able to correlate consecutive pseudonyms or associated certificates, thereby reconstructing the vehicle's trajectory. For this reason, several strategies have been proposed in the literature to determine when and where pseudonym changes should occur to ensure unlinkability and enhance privacy.

3.3 Pseudonym change strategies in the literature

Given the critical need to preserve vehicle anonymity, pseudonym change strategies have become a central focus in VANET privacy research. Numerous schemes have been proposed to address this challenge in a secure, efficient, and reliable manner. A recent survey [19] offers a classification of existing pseudonym change approaches, as illustrated in Figure 5.

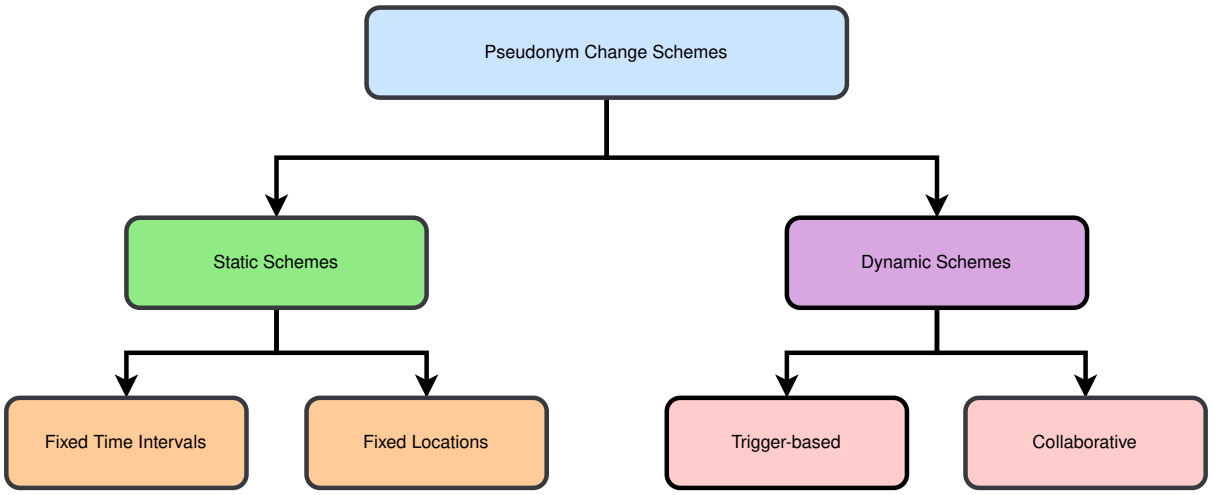

Figure 5: Pseudonym change schemes [20]

3.3.1 Static schemes

Static schemes rely on predefined rules for when or where pseudonym changes occur—either at fixed intervals or at specific locations. While this structure simplifies implementation, it introduces predictability, which adversaries can exploit. In many of these approaches, pseudonym

changes are preceded by silent periods, during which the vehicle disables its radio transmitter and temporarily stops broadcasting control messages.

3.3.1.1 Fixed location-based

A well-known family of static schemes leverages fixed locations for pseudonym change, often referred to as Mix-Zones. These zones are typically located at strategic and high-traffic areas, such as intersections, traffic lights, or commercial centers.

Deng et al.[21] introduced a protocol called PCP (Pseudonym Changing Protocol) designed to safeguard location privacy. Their model assumes the presence of base stations in addition to standard network entities like vehicles, RSUs, and a trusted authority. Each base station manages vehicle registration within its coverage area and, in cooperation with nearby RSUs, issues certified pseudonyms and a group key shared among all vehicles in that zone. This group key is used to sign messages during pseudonym changes. The protocol also considers vehicle density and behavioral variation. However, pseudonym changes are restricted to the base station's region—once a vehicle leaves this area, its keys and pseudonyms become invalid, requiring re-registration. While PCP aims to enhance privacy, it has notable drawbacks. The reliance on extensive infrastructure raises deployment costs and introduces scalability issues, which contrasts with VANETs' reliance on decentralized, vehicle-to-vehicle communication. Furthermore, even though pseudonym changes occur independently, vehicles within the same base station domain may not be physical neighbors, increasing the risk of syntactic or semantic linking attacks.

Another fixed-location approach is the Coupling Privacy with Safety (CPS) scheme by Wahid et al. [22]. In this method, vehicles reduce beaconing frequency when within the range of an RSU, aiming to obscure driver location. Upon entering an RSU zone, a vehicle authenticates using an identifier and a secret key assigned by the authority. The RSU verifies the ID against a stored list and computes a pseudonym to be used for the duration of the vehicle's stay in the region. However, the same pseudonym remains in use even after leaving the RSU area. This scheme treats the vehicle's identity as a simple identifier, not a certificate, which undermines security. Each time a vehicle interacts with an RSU, it reveals this identifier, allowing a passive adversary to track its movements across different RSU regions. Moreover, since the pseudonym is derived from both identity and location, an observer could potentially predict

or reconstruct future pseudonyms. CPS also shifts the responsibility for safety messaging to RSUs, assuming vehicles can remain silent. However, this overlooks the critical role of beacons in maintaining network topology awareness and supporting routing.

A more advanced strategy, proposed by [23], combines features from the CAPS and CPN schemes into a hybrid model called CCAPS. The idea is to leverage the strengths of both methods by defining three nested regions around each vehicle: R1 (radio range), R2 (CPN region), and R3 (CAPS region), where R1 > R2 > R3. These regions are standardized by the trusted authority to ensure consistency across the network. CCAPS prioritizes the density-based CPN strategy. When a vehicle nears the end of a pseudonym's validity, it scans its R2 region for neighbors willing to perform a coordinated change. If successful, a synchronous pseudonym change occurs. If no such neighbors are found, the vehicle monitors R3 for nearby nodes entering silent mode. It then follows suit, stopping message transmission temporarily, before switching its pseudonym. This hybrid approach shows promising results, as it mitigates some of the CAPS strategy's limitations without discarding its core strengths. Nonetheless, its reliance on silent periods remains controversial, as it contradicts the foundational goals of Intelligent Transportation Systems, where continuous broadcast of beacon messages is essential for real-time awareness and safety.

3.3.1.2 Fixed time intervals

The Periodical Pseudonym Change (PPC) [24] strategy was one of the earliest approaches to pseudonym alteration in vehicular networks. Under this scheme, each pseudonym is valid for a predefined period, after which it is replaced, either at fixed or randomly selected intervals. However, this predictable behavior exposes the system to linkage attacks, where an adversary can anticipate the next pseudonym change and correlate successive identifiers belonging to the same vehicle. To counter such linkability, the authors in [25] proposed the Random Silent Period (RSP) mechanism. RSP introduces a silent period composed of two components: a fixed duration and a variable one. The fixed portion disrupts the spatial link between the vehicle's original and new locations, while the variable portion confounds temporal correlations between the disappearance and reappearance events of the vehicle. This dual structure aims to break both spatial and temporal continuity from the perspective of the observer. Building upon RSP, the CARAVAN scheme [26] introduced a further enhancement. In CARAVAN, vehicles enter a random silent period before changing their pseudonyms. If multiple vehicles, such as A and B,

enter silence simultaneously and perform pseudonym changes during that period, it becomes significantly harder for an adversary to associate new identifiers with their prior ones, thus amplifying unlinkability through synchronized behavior.

Another approach, known as PCPPA [27], focuses on secure authentication between OBU and RSU. It relies on each vehicle internally generating a pool of pseudonyms and sharing them securely with the nearest RSU. Vehicles then change their pseudonyms at predetermined times. However, this non-cooperative, context-unaware timing risks compromising pseudonym independence. While the authors claim that consecutive pseudonyms remain unlinkable, it overlooks the potential for advanced tracking techniques that exploit structural or behavioral patterns in vehicular communications.

3.3.2 Dynamic schemes

Unlike static schemes, dynamic schemes take into account the vehicle's environment when performing a pseudonym change. The vehicle's environment includes factors such as the number of neighboring vehicles, their behavior, and so on. The strategies in this class promote the simultaneous pseudonym change of multiple vehicles.

3.3.2.1 Trigger-based

The core idea of these schemes is to satisfy specific traffic-related conditions, such as vehicles moving below a certain speed or encountering similar contextual situations, such as traffic congestion zones. A widely cited scheme published in [28], known as SLOW, avoids reliance on RSU infrastructure. Instead, vehicles autonomously create their mix-zones. The concept is simple yet effective from a privacy standpoint. Whenever a vehicle's speed drops below a predefined threshold, it disables its radio transmission (i.e., enters a silent period), remains silent for a duration, and changes its pseudonym before resuming communication. In these low-speed scenarios—typically associated with high traffic density—vehicles refrain from sending periodic or position-revealing messages, thereby taking advantage of the situation to perform a pseudonym change during the silence. Transmission resumes once the silent period ends. The same logic applies near traffic signals and congested intersections. The authors assume that vehicles in these contexts are moving slowly, reducing the risk of accidents or critical safety events. Although SLOW is simple to implement and effective in terms of privacy, assuming

optimal conditions, it has several limitations, among them we mention:

- **Unnecessary pseudonym changes:** Every drop below the speed threshold triggers a silent period and pseudonym change, which can lead to excessive pseudonym consumption and added computational overhead.
- **Contradiction with VANET safety objectives:** The primary goal of VANETs and intelligent transport systems (ITS) is real-time road safety and emergency alerts. Silent periods compromise this core functionality.

Another traffic-aware scheme was proposed in [29]. The authors introduced TAPCSa, a traffic detection protocol based on vehicle behavior. When a vehicle slows down, it sends a traffic detection message. It waits to receive a similar message from a neighboring vehicle to confirm congestion. A single vehicle is then elected, based on its relative position, as the initiator of the silent zone. The initiator disables its radio, changes its pseudonym, and periodically broadcasts congestion notifications. Vehicles receiving these notifications verify their speed and location; if certain conditions are met, they too enter silent mode. The vehicle directly behind the initiator, within signal range, is elected as the new initiator, maintaining zone continuity. The first initiator stops sending notifications once its successor takes over. Notifications cease when an initiator detects the end of congestion using a detection protocol.

Boualouache et al. [30] proposed a novel framework for pseudonym change. The network is divided into grid-based cells, each containing one or more logical zones known as Vehicular Location Privacy Zones (VLPZs). These are deployed by RSUs at infrastructure points such as service stations. RSUs periodically broadcast the availability of pseudonym change services. Upon entering the zone, a vehicle sends a request to the RSU, disables its radio, and follows a secure, randomized path directed by a router within the zone. The vehicle stays in the station for a service time, then exits with a new pseudonym. Service times vary by vehicle and service type. This approach ensures that silent periods do not disrupt safety-related applications.

Another contribution from [31] falls into this category. The authors proposed a scheme called ENeP-AB (Estimation of Neighbors' Position with Adaptive Beaconing), where vehicles estimate the number and positions of nearby neighbors. They reduce transmission range and change pseudonyms accordingly, making it harder for adversaries to distinguish between group members. A later enhancement of ENeP-AB, called E-ABRP, introduced variable intervals between beacon transmissions to further obscure vehicle identities.

3.3.2.2 Collaborative

In this category, pseudonym changes rely on coordination among multiple vehicles and are context-aware.

The scheme introduced in [32] proposes a novel approach based on pseudonym exchange between two vehicles. Each vehicle is issued a single pseudonym, along with its certificate and signature key, delivered securely via a trusted authority. The vehicles and RSUs are registered with the central authority beforehand. Pseudonym exchange occurs only when the contextual states of two encountered vehicles differ sufficiently. If both vehicles share similar movement patterns, such as traveling at the same speed, an exchange is deemed ineffective. When the condition is met, the initiating vehicle sends an encrypted request to the RSU containing both pseudonyms. The RSU authenticates the sender, forwards the request to the certification authority (CA), and updates the pseudonym database accordingly before notifying both vehicles of the successful exchange. This approach enhances privacy by decoupling pseudonyms through exchange rather than renewal. However, the strategy remains vulnerable to syntactic linking attacks, as only one vehicle effectively changes its identity, making it easier for an adversary to track changes. Moreover, the scheme introduces significant practical limitations. Frequent contact with RSUs and the central authority is required, which is challenging in high-speed vehicular environments where vehicles may quickly move in and out of RSU coverage zones. The additional cryptographic processing further adds to system overhead.

The authors of [33] proposed another scheme called CAPS, which supports pseudonym changes in a mixed context to break the spatial and temporal correlation of messages. Cooperation in this scheme comes from the fact that each vehicle monitors its neighbors; if one or more nearby vehicles stop sending beacon messages for a certain period, it enters a silent period. It resumes sending control messages with a new pseudonym once its real state could

be confused with that of a silent neighbor. While the pseudonym change is effective from a privacy perspective, safety applications are not considered—vehicles stop broadcasting safety messages during silence, which negatively impacts system functionality and compromises road safety, the core purpose of the vehicular ecosystem. Another limitation is that the scheme assumes that missing beacon messages indicate neighbors are in silence, which is not always true. For instance, vehicles at intersections or moving in the opposite direction may simply have left the communication range and are no longer neighbors.

Another scheme proposed in [34], called CPN, is a cooperative pseudonym change mechanism based on the number of neighbors. When the number of neighbors reaches a certain threshold, vehicles change their pseudonyms. This strategy is effective because it promotes simultaneous pseudonym changes by multiple vehicles, making it harder for a tracker to follow. When vehicles are in similar states, it becomes difficult to distinguish them. The main drawback is that the scheme performs many pseudonym changes even when they are not needed. Since the pseudonym pool is relatively limited, a vehicle may be forced to reuse a previously used pseudonym. Another limitation is the possible unavailability of the required number of neighbors. In low-density networks, such as when a driver intentionally avoids traffic by taking less congested roads, the pseudonym might never be changed, allowing a tracker to follow the vehicle and learn its entire route.

In [19], the authors proposed a new pseudonym change scheme called Context-Aware and Traffic Adaptive (CATA). This scheme leverages vehicle context information and current traffic models to select the optimal moment for pseudonym changes while preserving privacy. Within a region covered by the same RSU, multiple vehicles change their pseudonyms simultaneously using dynamic triggers, aiming to ensure privacy by maximizing anonymity. The timing of the changes is determined by the RSUs and communicated to all vehicles within their coverage. Each vehicle generates its pseudonym autonomously, provided it is registered with the RSU. Any unregistered vehicle is considered an intruder, and its pseudonym is broadcast to all vehicles in the region so they ignore messages received from it. Local pseudonym generation treats the pseudonym as a simple identifier, whereas in reality, it should be treated as a certificate to ensure accountability for malicious behavior.

Recently, the authors of [35] proposed a privacy scheme called “Safety-Related Privacy Scheme” (SRPS), which preserves privacy while meeting the requirements of VANET safety

applications. The core idea is to reduce silent periods. To change its pseudonym, a vehicle enters a silent phase while continuing to monitor its neighboring vehicles. If an accident is anticipated, it exits the silent period and resumes broadcasting safety messages. SRPS uses two algorithms based on the vehicle's state: one for the silent state and another for the active state. Both are built on a Multi-Target Tracking (MTT) [36] algorithm to identify effective contexts for pseudonym changes and avoid potential accidents. MTT helps the vehicle predict its next position and that of its active or silent neighbors, and stores these predictions. When a pseudonym is near expiration, the vehicle enters silence and compares its current state to its predicted state. If the distance is small, it keeps the same pseudonym; otherwise, it changes it. In this approach, detecting a silent neighbor is based on missing two consecutive beacons. This assumption is not always reliable — a neighbor may simply change direction at an intersection or stop. Another limitation is that emergency events do not necessarily concern all nearby vehicles. To avoid overloading the network, a vehicle must first determine whether it is involved or excluded from message dissemination before breaking silence.

Among recent approaches, the authors of [37] proposed an infrastructure-independent pseudonym exchange scheme called RIPS (RSU-Independent Pseudonym Swap Scheme), later improved in [38]. Unlike pseudonym change, RIPS uses exchange to reduce the number of pseudonyms required, as a pseudonym can be reused by another vehicle. However, treating pseudonyms as simple identities conflicts with security, privacy, and accountability requirements in vehicular networks. Most exchange schemes rely on RSUs, but RIPS enables cooperative exchange without RSUs, in mixed contexts that enhance location privacy. Each exchange is reported to the authority to ensure accountability and non-repudiation, though it still lacks a strong link between the vehicle and the pseudonym.

To ensure infrastructure independence, a trusted authority provides each vehicle with a set of swappable pseudonyms and one non-swappable pseudonym after registration. In favorable contexts, nearby vehicles exchange swappable pseudonyms in pairs. The current pseudonym is replaced by the partner's, and each vehicle synchronously selects a new pseudonym from its list. A report, including the non-swappable pseudonym for authentication, is then sent to the authority.[20]

3.4 Comparison

To conclude this chapter, we summarize the works cited above. Table 1 provides a comparison of these studies based on several criteria:

- **Scheme classification** This column identifies the category of each scheme based on the taxonomy adopted in this study.
- **Pseudonym change frequency** This metric refers to how often pseudonym changes occur. Since vehicles are issued a limited set of pseudonyms, excessive switching can lead to premature depletion, undermining long-term privacy. Efficient and judicious use of pseudonyms is therefore a key design consideration. The frequency is generally categorized as high (frequent and possibly unnecessary changes), medium (some redundant changes), or low (only necessary changes). In the case of RIPS [37], which relies on pseudonym exchange between vehicles rather than traditional replacement, this metric does not directly apply.
- **Decision authority** This specifies which entity initiates the pseudonym change, typically the vehicle itself, although some schemes delegate this decision to RSUs or other infrastructure components.
- **Pseudonym generation source** While a central trusted authority generally issues pseudonyms, alternative approaches exist where vehicles, RSUs, or base stations are responsible for generating them.
- **Silent period implementation** Some schemes introduce silent periods before pseudonym change events to enhance unlinkability. Others omit this step, potentially exposing patterns in communication.
- **Safety application consideration** An effective privacy strategy must not compromise the integrity of safety-critical applications. This metric evaluates whether each scheme interferes with real-time safety message delivery.
- **Computational overhead** This dimension assesses the processing load imposed on OBU. Lower computational demand is preferable for resource-constrained vehicular hardware.

- **Communication overhead** Due to bandwidth constraints in VANETs, privacy schemes should minimize additional communication between nodes. This metric reflects the extra messaging required by each scheme.

3.5 Conclusion

This chapter reviewed the use of pseudonyms and certificates in VANETs and surveyed existing pseudonym change strategies. It compared static and dynamic schemes and highlighted their trade-offs. These findings help motivate the improvements proposed in the next chapter.

Scheme	Scheme Classification	Pseudonym Change Frequency	Decision Authority	Pseudonym Generation Source	Silent Period Implementation	Safety Apps Consideration	Computational Overhead	Communication Overhead
PCP	Fixed Locations	Depends on visited locations	Vehicle	Roadside Unit	Grouped	Yes	High	High
CPS	Fixed Locations	Depends on RSU coverage	RSU	RSU	Yes	Yes	High	High
CCAPS	Fixed Locations	Medium	Vehicle	Trusted Authority	Yes	No	Medium	Low
RSP	Fixed Periods	High	Vehicle	Trusted Authority	Yes	No	Low	Low
CARAVAN	Fixed Periods	High	Vehicle	Trusted Authority	Yes	No	Medium	Medium
PCPPA	Fixed Periods	High	Vehicle	Vehicle	Yes	No	High	Medium
Trigger-based	Collaborative	Medium	Vehicle	Trusted Authority	No	No	High	High
CAPS	Collaborative	High	Vehicle	Trusted Authority	Yes	No	High	High
CPN	Collaborative	High	Vehicle	Trusted Authority	Yes	No	Medium	Medium
CATA	Collaborative	High	RSU	Vehicle	No	No	High	High
SRPS	Collaborative	Medium	Vehicle	Trusted Authority	Yes	Yes	High	High
RIPS	Collaborative	Exchange	Vehicle	Trusted Authority	No	No	High	High
SLOW	Trigger-based	High	Vehicle	Trusted Authority	Yes	No	Low	Low
TAPCS	Trigger-based	Medium	Vehicle	Trusted Authority	Yes	No	High	High
VLPZs	Trigger-based	Low	Vehicle	Trusted Authority	Yes	Yes	Low	Low
ENeP-AB	Trigger-based	High	Vehicle	Trusted Authority	Yes	No	Low	Low

Table 1: Comparison of Privacy Schemes in VANETs [20]

Chapter 4

Contribution

4.1 Introduction

This chapter presents an enhanced pseudonym change scheme designed to improve privacy protection in VANETs. The proposed mechanism builds on the original Cooperative Pseudonym Change based on Number of Neighbors (CPN) scheme by addressing its key limitations, including the lack of pseudonym lifetime awareness, the absence of silent periods, and insufficient handling of sparse traffic conditions. The enhancement introduces new decision criteria, incorporates silent periods for unlinkability, and defines emergency coordination protocols to ensure timely pseudonym updates. The chapter provides an overview of the enhancement, describes the implementation logic in detail, and introduces the algorithms for both the original and improved schemes to clarify the modifications made.

4.2 Overview of the proposed enhancement

Our scheme builds upon the original CPN scheme previously discussed in Section 3.3.2.2 by addressing several of its key limitations. Specifically, it introduces redefined conditions for pseudonym changes and incorporates silent periods to enhance privacy. The original scheme lacked pseudonym lifetime awareness, offered no fallback in sparse traffic, and did not use silent periods—factors which could reduce its robustness in real-world scenarios. In our approach, each vehicle monitors both its pseudonym lifetime and the number of surrounding neighbors. Two scenarios are identified: the normal case, where the pseudonym lifetime re-

mains valid and a change is not urgent, and the emergency case, where the pseudonym lifetime is approaching its maximum and a change becomes critical. In the normal case, once a pseudonym reaches half of its maximum lifetime and the number of neighbors meets or exceeds a predefined threshold k, the vehicle marks itself as ready to change. If it detects that at least k neighboring vehicles (including itself) are also ready, it enters a silent period before changing its pseudonym. During silent periods, vehicles halt outgoing communications while minimally processing incoming messages to maintain readiness coordination. In the emergency case, if the pseudonym exceeds a critical threshold before sufficient neighbors are ready, the vehicle activates an emergency flag and broadcasts it. Nearby vehicles receiving this flag also activate their own, allowing them to participate in a coordinated pseudonym change after a silent period. This dual-trigger mechanism enables vehicles to synchronize changes in dense traffic while ensuring timely changes in sparse scenarios, thereby enhancing privacy without disrupting unnecessary communication.

4.3 Implementation details

In this section, we present the implementation details of the proposed enhancement to the CPN scheme. We begin by outlining the limitations of the original CPN strategy, which motivates the need for improvement. Then, to support a clear understanding of the changes introduced, we include the algorithm of the original CPN scheme, followed by the enhanced mechanism. Due to its length, the enhanced pseudocode is divided into two parts, each presented on a separate page.

4.3.1 Original CPN Algorithm

Algorithm 1 CPN Algorithm

Input:
kNeighbors: neighbor threshold,
neighborRadius: maximum distance to consider a neighbor
Initialization:
$readyFlag = \text{false}$,
$setReadyFlagReceived = \text{false}$,
$nNeighbor = 0$

```
1  Function beaconToBeSent():
2      if readyFlag or setReadyFlagReceived then
3          Change pseudonym
4          readyFlag = false
5      end
6      else if nNeighbor ≥ kNeighbors then
7          readyFlag = true
8      end
9      Include readyFlag in beacon
10     Reset nNeighbor, setReadyFlagReceived
11 Function handleUpperMsg(msg) / handleUpperControl(msg):
12     if msg is WAVEBeacon then
13         Call beaconToBeSent()
14     end
15     Forward msg
16 Function msgArrived(msg):
17     if msg is not WAVEBeacon then
18         return
19     end
20     if distance to sender > neighborRadius then
21         return
22     end
23     if msg.readyFlag then
24         setReadyFlagReceived = true
25     end
26     nNeighbor++
27 Function handleLowerMsg(msg) / handleLowerControl(msg):
28     Call msgArrived(msg)
29     Forward msg
```

4.3.2 Limitations of the CPN scheme and motivations for enhancement

The original CPN scheme provides a valuable foundation by leveraging neighbor density for cooperative pseudonym changes. However, like many early privacy-preserving strategies in VANETs, it presents certain limitations that motivate further enhancement.

Specifically, CPN does not consider the remaining lifetime of a pseudonym, which may result in suboptimal change timing and affect long-term privacy. Additionally, the lack of silent periods during pseudonym transitions may expose vehicles to tracking through broadcast continuity. The scheme also assumes sufficient neighbor density, which limits its robustness in sparse or dynamic traffic scenarios where coordination becomes challenging. Moreover, CPN may initiate changes even when pseudonyms are still fresh, potentially leading to unnecessary consumption of pseudonyms. Finally, while cooperative, the original mechanism does not guarantee strict synchronization across participants, leaving room for linkability.

The proposed scheme builds upon these insights by integrating lifetime awareness, controlled silent periods, emergency coordination protocols, and stricter change conditions, thereby extending the applicability and strengthening the privacy guarantees of the original design.

4.3.3 Algorithm

The following algorithm outlines the implementation logic of our scheme, detailing how pseudonym changes are managed based on system conditions.

Algorithm 2 E-CPN (Part 1)

Input:
kNeighbors: neighbor threshold,
maxPsynmLifetime: pseudonym max lifetime,
neighborRadius: detection range,
silentPeriod: silent phase duration
Initialization:
$psynmLifetime = 0$,
$readyFlag =$ false,
$emergencyFlag =$ false,
$readyNeighborsCount = 0$,
$nNeighbor = 0$,
$bSilent =$ false,
Schedule *exitSilenceEvt*
Function `beaconToBeSent()`**:**
  if $\neg bSilent$ **then**
    Update *psynmLifetime*
    if $(readyFlag$ ***and*** $readyNeighborsCount + 1 \geq kNeighbors)$ ***or*** $emergencyFlag$ **then**
      $bSilent =$ true
      Schedule *exitSilenceEvt* after *silentPeriod*
    end
    else if $psynmLifetime \geq \frac{3}{4} \cdot maxPsynmLifetime$ **then**
      $emergencyFlag =$ true
    end
    else if $nNeighbor \geq kNeighbors$ ***and*** $psynmLifetime \geq \frac{1}{2} \cdot maxPsynmLifetime$ **then**
      $readyFlag =$ true
    end
    Include $readyFlag$, $emergencyFlag$ in beacon
    Reset $readyNeighborsCount$, $nNeighbor$
  end

Collectively, these steps define the complete sequence of operations for E-CPN scheme, as described in Algorithm 2. At the beginning of each journey, the algorithm initializes the pseudonym lifetime, neighbor counts, and state flags. The beacon transmission routine then updates the pseudonym lifetime, assesses readiness and emergency conditions based on predefined thresholds, and triggers silent periods when necessary. Incoming beacons are processed to increment neighbor counts and activate readiness or emergency flags, facilitating coordinated pseudonym changes.

When the silent-period timer expires, a self-message handler resets the flags and executes the pseudonym change. Upper-layer and lower-layer handlers maintain the silent period by either dropping or forwarding messages as appropriate. This implementation ensures synchronized pseudonym updates in dense traffic situations and timely changes in sparse environments, all without incurring excessive overhead.

Algorithm 2 E-CPN (Part 2)

```
Function msgArrived(msg):
    if msg is not a WAVEBeacon then
        return
    end
    if distance to sender > neighborRadius then
        return
    end
    if msg.readyFlag then
        readyNeighborsCount++
    end
    if msg.emergencyFlag then
        emergencyFlag = true
    end
    nNeighbor++
Function handleSelfMsg(msg):
    switch msg.kind do
        case EXIT_SILENCE do
            bSilent = false
            Change pseudonym
            Reset psynmLifetime, readyFlag, emergencyFlag, readyNeighborsCount
        end
        Log "Unknown self message"
    end
Function handleUpperMsg(msg) / handleUpperControl(msg):
    if bSilent then
        Drop msg
    end
    else
        if WAVEBeacon then
            Call beaconToBeSent()
        end
        Forward msg
    end
Function handleLowerMsg(msg) / handleLowerControl(msg):
    Call msgArrived(msg)  Forward msg
```

4.3.4 Flowchart

Figure 6 illustrates the flowchart of ECPN, providing a visual abstraction of its control logic and highlighting the key decision points and transitions in the pseudonym management process.

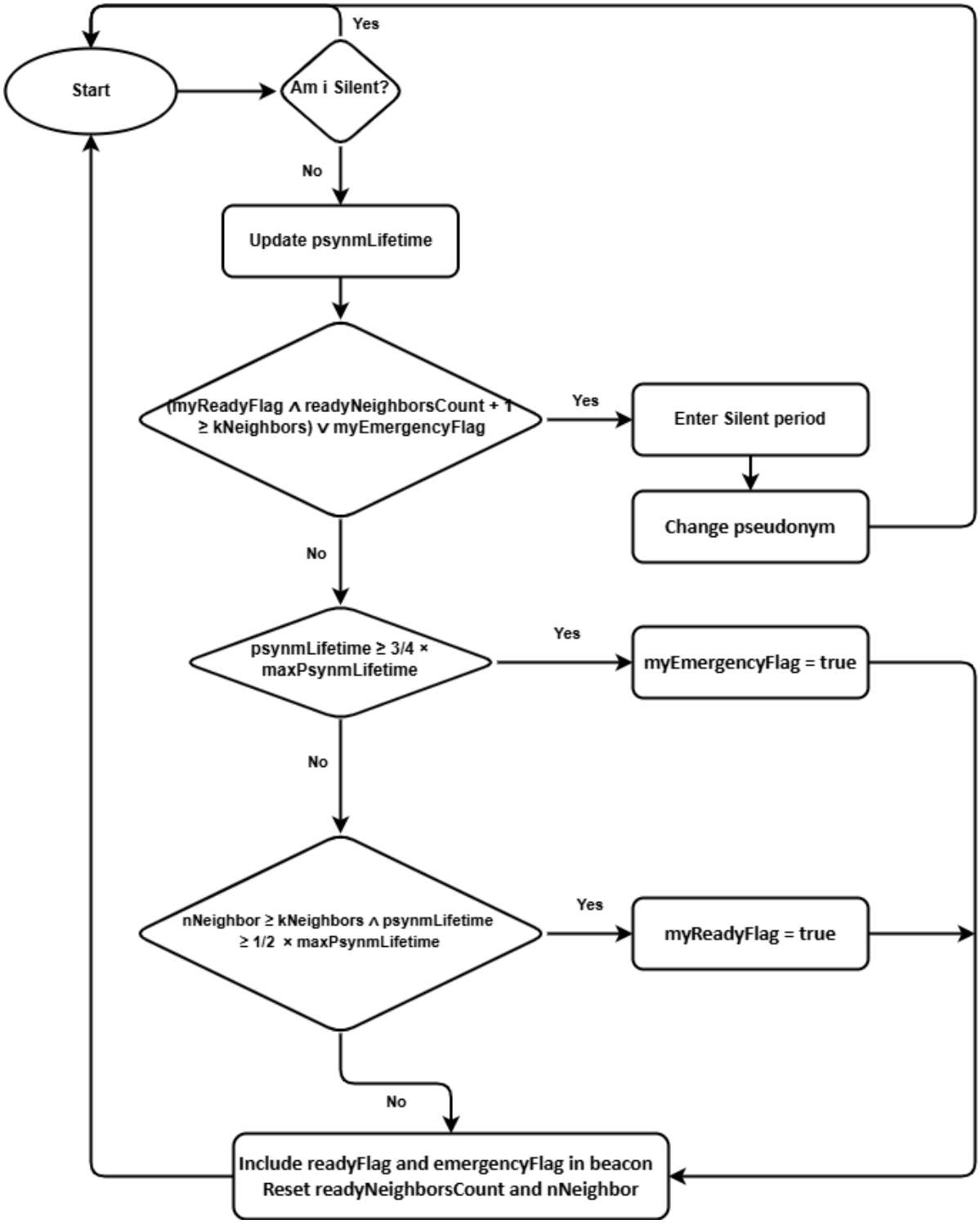

Figure 6: E-CPN flowchart

4.4 Conclusion

In this chapter, we introduce an enhanced pseudonym change scheme designed to improve privacy protection in VANETs. We detailed the modifications made, explained their implementation, and discussed the expected benefits. The next chapter presents the performance evaluation and simulation results of the proposed scheme.

Chapter 5

Simulation and performance evaluation

5.1 Introduction

This chapter outlines the simulation setup and evaluation process used to analyze the effectiveness of our proposed privacy scheme in VANETs. It introduces the simulation tools, the Privacy Extension for Veins Framework (PREXT) framework, and the privacy schemes used for comparison. Finally, it presents the performance metrics and discusses the results based on simulation outcomes.

5.2 Simulation setup

5.2.1 Simulation tools and environment

The simulation was conducted using the Vehicles In Network Simulation (VEINS) framework [39] version 4.4, and Objective Modular Network Testbed in C++ (OMNET++) version 5.0. PREXT framework served as the foundation for implementing and evaluating the proposed privacy scheme. Vehicle mobility was realistically modeled using the Simulation of Urban Mobility (SUMO)[40] version 0.25 to generate accurate traffic traces. This simulation environment enables comprehensive testing of pseudonym change strategies under practical VANET conditions, offering a controlled yet realistic setting to assess privacy protection mechanisms. Compared to earlier VANET simulation tools such as TraNS, VANET MobiSim, and iTETRIS, this setup, particularly with the inclusion of PREXT — provides a more unified,

extensible, and privacy-focused simulation environment. Thanks to PREXT's modular design, built-in privacy schemes, realistic adversary models, and diverse privacy metrics, the evaluation results obtained are more consistent and representative of real-world VANET behavior [41].

5.2.2 PREXT framework

5.2.2.1 The Role

The PREXT framework is used in this work as a dedicated privacy extension for the VEINS simulation platform. It was specifically designed to enable the realistic evaluation of privacy schemes in VANETs by combining accurate vehicular mobility from SUMO with detailed network communication models based on the IEEE 802.11p and IEEE 1609.4 standards, as provided by VEINS. This integration ensures that privacy solutions are tested under conditions that closely resemble real-world VANET deployments, rather than over-simplified simulation environments.

In addition to supporting the development and comparison of privacy-preserving mechanisms, PREXT incorporates several built-in privacy schemes based on silent periods, context-awareness, and mix zones. It also includes a configurable adversary model based on the Nearest-Neighbor Probabilistic Data Association (NNPDA) algorithm, capable of evaluating vehicle traceability under various attacker capabilities. Furthermore, PREXT provides multiple privacy metrics, including traceability, anonymity set size, entropy, and pseudonym statistics, offering a comprehensive evaluation framework.

An important feature of PREXT is its support for assessing not only privacy performance but also the potential impact of privacy schemes on communication protocols and safety applications. This capability, often neglected in other simulation tools, encourages the integration of privacy considerations during the design and evaluation of network protocols. For these reasons, PREXT was selected in this work to implement and evaluate the proposed privacy enhancement, ensuring a realistic and consistent comparison with other privacy strategies.

5.2.2.2 The Available Privacy Schemes

PREXT integrates seven privacy-preserving schemes to protect vehicular identities in VANETs. Some of these schemes—already discussed in Chapter 3—are briefly summarized here for completeness, while the others are introduced below.

1. **Periodical Pseudonym Change (PeriodicalPC)**

   This scheme changes the vehicle's pseudonym at regular time intervals. The change can occur at fixed or random times. Fixed intervals may lead to synchronized changes among vehicles, which can help with anonymity but also become predictable to adversaries. Random intervals reduce predictability but may lower the chance of simultaneous changes with other vehicles[24].

2. **Random Silent Period (RSP)**

   As explained in Chapter 3 (see Section 3.3.1.2), RSP introduces silent periods after pseudonym changes to break linkability. Vehicles stop beaconing for a randomly chosen interval, making identity tracking more difficult. In PREXT, this randomness increases entropy while still ensuring safety through bounded silence durations.

3. **Coordinated Silent Period (CSP)**

   CSP is a synchronized approach where all vehicles simultaneously enter silence and change pseudonyms. This maximizes the number of vehicles changing identities simultaneously, greatly enlarging the anonymity set. While effective in theory, CSP is difficult to apply in real-world scenarios due to the challenges of achieving global coordination and managing safety risks during simultaneous silences.[42]

4. **Silence At Low Speeds (SLOW)**

   Already covered in Chapter 3 (see Section 3.3.2.1), SLOW adapts beacon transmission based on vehicle speed. PREXT incorporates this strategy to exploit natural traffic patterns (e.g., traffic jams) as opportunities for pseudonym changes with minimal traceability.

5. **Cooperative Pseudonym Change based on neighbors (CPN)**

   Also detailed earlier (see Section 3.3.2.2), CPN detects opportunities for group-based pseudonym changes by evaluating vehicle density. In PREXT, it plays a key role in leveraging local context for coordinated anonymity.

6. **Context-Aware Privacy Scheme (CAPS)**

   Previously discussed in Chapter 3 (see Section 3.3.2.2), CAPS enhances pseudonym efficiency by selecting change moments based on situational awareness. PREXT uses CAPS to simulate realistic, non-deterministic behavior and avoid unnecessary pseudonym use.

7. **Mix-zone**

   Mix zones are virtual areas, typically placed at intersections, where vehicles become unobservable to external entities. When inside a mix zone, vehicles can change pseudonyms without being tracked, as their communication is either hidden or encrypted. The mix zone model assumes that adversaries cannot observe vehicle behavior within the zone, making it challenging to correlate identities before and after the vehicle passes through.

5.2.3 Simulation settings and map details

This section outlines the general simulation settings, the map's properties, and the tools used to generate the necessary files for conducting the simulation on the selected map.

5.2.3.1 General simulation settings

The simulation configuration is presented through three concise tables.Table 2 describes the adversary model provided by PREXT, Table 3 provides the network and communication settings used in the VEINS framework, including eavesdropper placement and tracking behavior.

Table 2: Adversary settings.

Parameter	Value
Eavesdropper range	300 m
Eavesdropper overlap	30 m
Track interval	1 s
Wait before delete	2 s
Type	Eavesdropping and tracking

Table 3: Veins settings.

Parameter	Value
Data rate	18 Mbps
Transmission power	20 mW
Beacon rate	1 Hz
Data length	100 bytes
Header length	256 bits
Simulation time limit	300 s
Network size	2.7 km × 2.9 km
Number of vehicles	(169 - 249)

5.2.3.2 Map details

The simulation utilizes a road map of central Munich, covering an area of approximately 2.67 km by 2.8 km, as illustrated in Figure 7. This map creates a realistic urban traffic environment and was used to evaluate the performance of the implemented privacy schemes. Vehicle movements were generated using the randomTrips.py script, allowing for varied traffic conditions through different arrival rates. The mobility settings follow standard SUMO configurations, including a maximum speed of 50 km/h and an acceleration range from -4.5 m/s² to 2.6 m/s². Vehicles transmit beacon messages at a rate of one per second. The median trace duration is approximately 290 seconds, with an average travel distance of about 2 kilometers. This map is included in the PREXT package and was initially extracted from OpenStreetMap. It was then converted into a SUMO-compatible format using the netconvert and polyconvert tools from SUMO version 0.25.0.

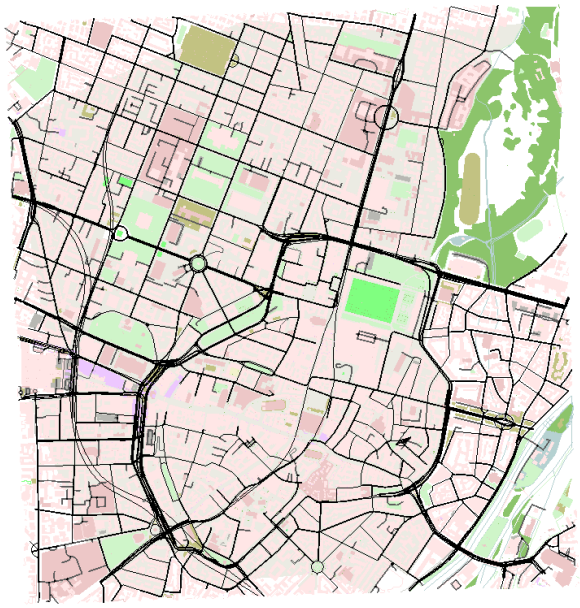

Figure 7: SUMO representation of the Munich map used in the simulation.

5.3 Comparison and discussion of results

5.3.1 Performance metrics

This section outlines the key metrics used to assess the effectiveness of the proposed privacy scheme. Derived from simulation results based on the setup discussed in Section 5.2, these metrics evaluate the level of protection offered against vehicle tracking in VANET environments.

1. **Traceability 90%**

   This metric measures the percentage of vehicle traces that an adversary can successfully track for at least 90% of their total duration. In other words, it reflects how persistent an adversary's tracking can be, even after vehicles change pseudonyms. A lower value of traceability indicates better privacy, as it means the privacy scheme is effective in preventing the adversary from maintaining continuous tracking.

2. **Normalized traceability 90%**

   This version of the traceability metric only considers vehicles that changed their pseudonyms at least once. It removes bias introduced by vehicles that never performed a pseudonym

change, which would otherwise be easily tracked. This normalized version gives a clearer picture of how effective the pseudonym change mechanism is in confusing the adversary.

3. **Average maximum anonymity set size per trace**

   The anonymity set refers to the group of vehicles that are difficult to distinguish from one another at a given time. This metric looks at the largest anonymity set size encountered in each vehicle's trace and averages it across all vehicles. Larger anonymity sets indicate better privacy, making it harder for an adversary to isolate and identify a single target vehicle.

4. **Average maximum entropy per trace**

   Entropy, in this context, measures the adversary's uncertainty in linking a vehicle's new pseudonym with its previous one. This metric records the highest entropy value observed during a trace, reflecting the peak level of confusion caused by the privacy scheme. A higher value means that, at some point, the adversary had a very low probability of correctly tracking the vehicle.

5. **Average sum entropy per trace**

   Unlike the maximum entropy, this metric sums the entropy values throughout a vehicle's trace, giving a global view of how uncertain the adversary was during the entire simulation period. A higher average sum entropy suggests that the adversary remained confused for a prolonged time, a desirable outcome in privacy protection.

6. **Average pseudonym changes per trace**

   This metric reports how often a vehicle changes its pseudonym on average during its journey. Pseudonym changes are the core mechanism in many privacy schemes, and their frequency directly influences privacy performance. While more changes can enhance privacy, they must be carefully balanced to avoid unnecessary overhead and ensure practical feasibility.

7. **Average confusions per pseudonym change**

   Confusion happens when the adversary incorrectly links a new pseudonym to the wrong vehicle. This metric measures the amount of confusion caused by each pseudonym

change. A high number indicates that the privacy scheme successfully deceives the adversary, making it harder for them to track vehicles across pseudonym changes.

8. **Average confusions per trace**

   This metric captures the total number of adversary confusions during a single vehicle trace, averaged across all vehicles. It provides an overall indication of how frequently the privacy scheme causes tracking errors during normal driving behavior. The higher this number, the more effective the scheme is at preventing accurate tracking.

5.3.2 Results discussion

This section presents a comparative analysis between our proposed privacy scheme and some existing schemes implemented in the PREXT extension, namely: Periodical Pseudonym Change, RSP, SLOW, CPN, and CAPS. The evaluation focuses on four representative performance metrics: Traceability, Normalized Traceability, Average Confusions per Trace, and Average Pseudonym Changes per Trace. These metrics collectively reflect the trade-offs between privacy protection and pseudonym usage. Each result represents the average across multiple simulation runs. The following discussion highlights the relative performance and effectiveness of our scheme in various traffic conditions. The simulation settings used for each scheme in the comparison are summarized in Table 4.

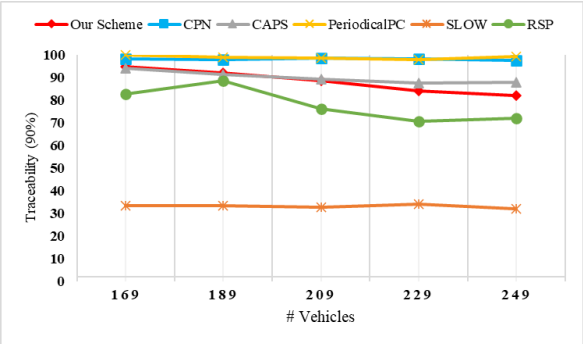

Figure 8: Traceability per trace.

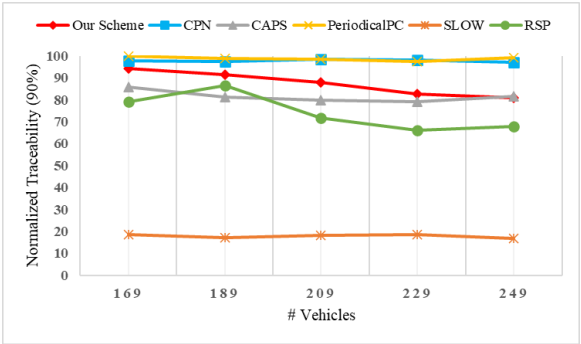

Figure 9: Normalized traceability per trace.

5.3.2.1 Traceability and normalized traceability (90%)

Figure 8 and Figure 9 illustrate the results for both traceability and normalized traceability across the evaluated schemes. These two metrics exhibit consistent trends and serve as key indicators of the effectiveness of privacy.

Table 4: Settings for each privacy scheme.

Scheme	Parameter	Value
PeriodicalPC	Pseudonym lifetime	60 s
RSP	Pseudonym lifetime	60 s
	Silent period	(3, 11) s
SLOW	Speed threshold	8 m/s
	Silent threshold	5 s
CAPS	Min pseudonym lifetime	60 s
	Max pseudonym lifetime	180 s
	Silence range	(3, 13) s
	Missed beacons silence threshold	2 beacons
	Neighborhood radius	50 m
CPN	Radius	100 m
	Neighbors threshold	2
Enhanced CPN	Radius	100 m
	Neighbors threshold	2
	Max pseudonym lifetime	60 s
	Silent period	2 s

In our scheme, the reduction in traceability compared to the original CPN is primarily driven by two enhancements: first, pseudonym changes are triggered only when coordination with neighboring vehicles is detected, or when a pseudonym is nearing expiration; second, silent periods are applied adaptively and only under these specific conditions. This reduces predictability while promoting synchronized changes, thus minimizing likability.

As vehicle density increases, traceability under our scheme decreases steadily. It eventually outperforms CAPS and reaches levels comparable to RSP. The PeriodicalPC scheme exhibits the highest traceability, mainly due to its static change intervals and lack of coordination among vehicles. The SLOW scheme achieves the lowest traceability overall by enforcing extended silent periods based on vehicle speed; however, this often leads to significant communication gaps. In contrast, our approach activates silence only when necessary and applies it for a limited duration, offering a more balanced trade-off between privacy and communication reliability.

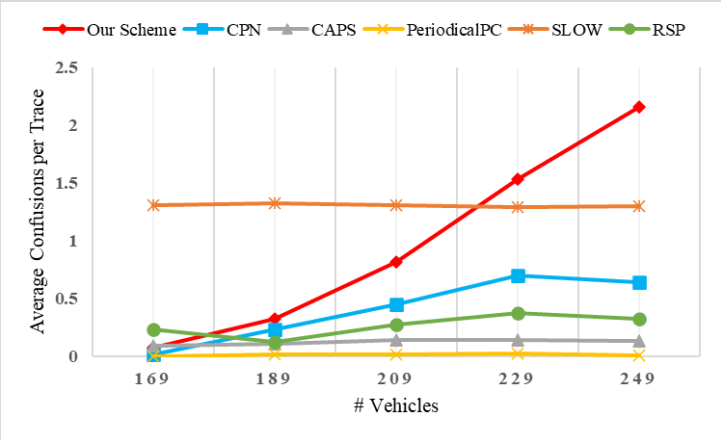

Figure 10: Average confusions per trace.

5.3.2.2 Average confusions per trace

Figure 10 illustrates the average number of confusions per vehicle trace, which serves as a key indicator of the privacy level achieved by each scheme. As explained earlier in Section 5.3.1, higher confusion values typically correspond to greater adversarial uncertainty in reconstructing vehicle identities.

Among the evaluated schemes, the proposed scheme demonstrates the most significant improvement in this metric as vehicle density increases. Unlike the original CPN, which shows only moderate gains, our approach scales more effectively and introduces greater ambiguity in denser scenarios. As a result, our scheme eventually outperforms all other evaluated methods, including RSP and SLOW, which yield solid results but tend to plateau at higher densities. In contrast, PeriodicalPC and CAPS exhibit consistently lower confusion values due to their fixed-timing or less adaptive coordination strategies.

The improvement in confusion levels observed in our scheme is a direct outcome of its dual-trigger coordination mechanism. The scheme leverages both readiness-based and emergency-triggered pseudonym changes to adapt its behavior to varying traffic densities. In denser environments, vehicles confirm mutual readiness before initiating a synchronized pseudonym change, followed by a silent period during which outgoing messages are temporarily suppressed. This process reduces message continuity and increases the likelihood of overlapping identity traces, complicating adversarial linking attempts. In sparse conditions, the emergency flag ensures that vehicles approaching the end of their pseudonym lifetime can still participate in coordinated changes.

This conditional and context-aware behavior introduces controlled randomness in change timing, which contributes to higher confusion levels, particularly as vehicle density increases. These results further confirm the effectiveness of our scheme in improving privacy.

5.4 Conclusion

This chapter presented the simulation setup and evaluation process used to assess the effectiveness of our proposed privacy scheme. By using realistic network scenarios and comparing multiple privacy strategies within the PREXT framework, we demonstrated our scheme's performance in terms of key metrics. The results confirm that our enhancement achieves a better balance between privacy protection and resource efficiency than the original approach.

General Conclusion

This work addressed a critical challenge in Vehicular Ad Hoc Networks: protecting user privacy through effective pseudonym change strategies. While pseudonyms are commonly used to anonymize vehicle identities, poorly timed or uncoordinated changes can still allow adversaries to track vehicles over time.

Among the most promising privacy solutions is the use of pseudonyms. Yet, without well-timed and coordinated changes, adversaries can still link them and compromise user anonymity. To address this issue, our work proposes an improved pseudonym change mechanism based on the CPN scheme. The enhancement introduces coordinated changes supported by controlled silent periods and pseudonym lifetime checks, which significantly hinder tracking attempts. While the approach improves vehicle anonymity, it introduces brief communication interruptions—a known trade-off in silent-period-based strategies.

The scheme was implemented and evaluated using the OMNeT++ simulator, the Veins framework, and the PREXT extension. Through realistic simulations, our mechanism demonstrated better performance than the original CPN scheme, particularly in dense traffic scenarios, and showed adaptability to different environments, including urban and highway settings.

Additionally, we aimed to reduce the pseudonym change rate, and although we achieved some improvement, the rate remains higher than in several existing schemes. We would like to continue working on this issue to bring the rate down further. Separately, we also recognize the limitations introduced by the use of silent periods, particularly the brief communication gaps they cause. In the future, we aim to explore alternatives to silent periods that would allow vehicles to remain fully connected without compromising privacy.

References

[1] H. Hartenstein and K. P. Laberteaux, "A tutorial survey on vehicular ad hoc networks," *IEEE Communications Magazine*, vol. 46, no. 1, pp. 164–171, 2008.

[2] H. Ouaomar and E. H. Nfaoui, "A framework for adaptive networked embedded transport systems," https://www.researchgate.net/figure/ANET-system-architecture-23_fig1_388370657, 2024, accessed: 2025-06-16.

[3] H. Jean-Pierre, C. Srdjan, and L. Jun, "The security and privacy of smart vehicles," *IEEE Security & Privacy*, no. 3, pp. 49–55, 2004.

[4] Traffic Products, LLC, "Connected vehicles and roadside units (rsus)," https://trafficproducts.net/connected-vehicles, 2024, accessed: 2025-05-16.

[5] IEEE 802.11 Task Group P, "IEEE P802.11p: Wireless Access in Vehicular Environments (WAVE)," https://www.ieee802.org/11/Reports/tgp_update.htm, 2006.

[6] IEEE Intelligent Transportation Systems Committee et al., "Trial-use standard for wireless access in vehicular environments (WAVE) - Resource Manager," IEEE Std 1609-1, 2006.

[7] IEEE, "IEEE Std 1609.2™-2016, IEEE standard for wireless access in vehicular environments (wave)–security services for applications and management messages," IEEE Standard 1609.2-2016, 2016.

[8] Intelligent Transportation Systems Committee et al., "IEEE Trial-use standard for wireless access in vehicular environments (WAVE) - Networking Services," IEEE Std 1609-3, 2007.

[9] ITS Committee et al., "IEEE Trial-Use Standard for Wireless Access in Vehicular Envi-

ronments (WAVE) - Multi-Channel Operation," IEEE Std 1609-4, 2011.

[10] R. A. Uzcátegui, A. J. De Sucre, and G. Acosta-Marum, "Wave: A tutorial," *IEEE Communications magazine*, vol. 47, no. 5, pp. 126–133, 2009.

[11] "Intelligent transport systems (its); vehicular communications; basic set of applications; definitions," https://www.etsi.org/deliver/etsi_tr/102600_102699/102638/01.01.01_60/tr_102638v010101p.pdf, ETSI, Tech. Rep. ETSI TR 102 638 V1.1.1, 2009, accessed: 2025-06-16.

[12] A. Ghosal and M. Conti, "Security issues and challenges in v2x: A survey," *Computer Networks*, vol. 169, p. 107093, 2020.

[13] B. Hammi, J.-P. Monteuuis, and J. Petit, "Pkis in c-its: Security functions, architectures and projects: A survey," *Vehicular Communications*, vol. 38, p. 100531, 2022.

[14] ETSI, "Intelligent transport systems (its); security; trust and privacy management," ETSI, Technical Specification ETSI TS 102 940, 2021, v2.1.1. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/102900_102999/102940/02.01.01_60/ts_102940v020101p.pdf

[15] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham *et al.*, "Experimental security analysis of a modern automobile," in *2010 IEEE symposium on security and privacy*. IEEE, 2010, pp. 447–462.

[16] B. Wiedersheim, Z. Ma, F. Kargl, and P. Papadimitratos, "Privacy in inter-vehicular networks: Why simple pseudonym change is not enough," in *2010 Seventh international conference on wireless on-demand network systems and services (WONS)*. IEEE, 2010, pp. 176–183.

[17] European Union, "Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (general data protection regulation)," Official Journal of the European Union, 2016. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj

[18] State of California, "California consumer privacy act (ccpa)," California Civil Code, Title 1.81.5, 2018. [Online]. Avail-

able: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.5.&part=4.&chapter=&article=

[19] I. Saini, S. Saad, and A. Jaekel, "A comprehensive pseudonym changing scheme for improving location privacy in vehicular networks," *Internet of Things*, vol. 19, p. 100559, 2022.

[20] B. Moussaoui, "Sécurité et protection de la vie privée dans les réseaux véhiculaires," Ph.D. dissertation, Université Mohamed Boudiaf - M'Sila, 2023.

[21] X. Deng, T. Gao, N. Guo, C. Zhao, and J. Qi, "Pcp: A pseudonym change scheme for location privacy preserving in vanets," *Entropy*, vol. 24, no. 5, p. 648, 2022.

[22] A. Wahid, H. Yasmeen, M. A. Shah, M. Alam, and S. C. Shah, "Holistic approach for coupling privacy with safety in vanets," *Computer networks*, vol. 148, pp. 214–230, 2019.

[23] P. K. Singh, D. Chourasiya, A. Singh, S. K. Nandi, and S. Nandi, "Ccaps: Cooperative context aware privacy scheme for vanets," in *2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall)*. IEEE, 2019, pp. 1–5.

[24] Y. Pan, J. Li, L. Feng, and B. Xu, "An analytical model for random pseudonym change scheme in vanets," *Cluster Computing*, vol. 17, no. 2, pp. 413–421, 2014.

[25] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki, "Enhancing wireless location privacy using silent period," in *IEEE Wireless Communications and Networking Conference, 2005*, vol. 2. IEEE, 2005, pp. 1187–1192.

[26] M. Li, R. Poovendran, K. Sampigethaya, and L. Huang, "Caravan: Providing location privacy for vanet," in *Proceedings of the Embedded Security in Cars (ESCAR) Workshop*, vol. 2, 2005, pp. 13–15.

[27] J. Qi, T. Gao, X. Deng, and C. Zhao, "A pseudonym-based certificateless privacy-preserving authentication scheme for vanets," *Vehicular Communications*, vol. 38, p. 100535, 2022.

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

[29] A. Boualouache and S. Moussaoui, "Tapcs: Traffic-aware pseudonym changing strategy for vanets," *Peer-to-Peer networking and Applications*, vol. 10, pp. 1008–1020, 2017.

[30] A. Boualouache, S.-M. Senouci, and S. Moussaoui, "Privanet: An efficient pseudonym changing and management framework for vehicular ad-hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 21, no. 8, pp. 3209–3218, 2019.

[31] F. Zidani, F. Semchedine, and M. Ayaida, "Estimation of neighbors position privacy scheme with an adaptive beaconing approach for location privacy in vanets," *Computers & Electrical Engineering*, vol. 71, pp. 359–371, 2018.

[32] S. Wang, N. Yao, N. Gong, and Z. Gao, "A trigger-based pseudonym exchange scheme for location privacy preserving in vanets," *Peer-to-Peer Networking and applications*, vol. 11, pp. 548–560, 2018.

[33] K. Emara, W. Woerndl, and J. Schlichter, "Caps: Context-aware privacy scheme for vanet safety applications," in *Proceedings of the 8th ACM conference on security & privacy in wireless and mobile networks*, 2015, pp. 1–12.

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

[35] R. Al-Ani, T. Baker, B. Zhou, and Q. Shi, "Privacy and safety improvement of vanet data via a safety-related privacy scheme," *International Journal of Information Security*, vol. 22, no. 4, pp. 763–783, 2023.

[36] K. Emara, W. Woerndl, and J. Schlichter, "Beacon-based vehicle tracking in vehicular ad-hoc networks," 2013.

[37] A. P. Mdee, M. T. R. Khan, J. Seo, and D. Kim, "Infrastructure-independent pseudonym swap protocol for vehicular networks," in *2022 Thirteenth International Conference on Ubiquitous and Future Networks (ICUFN)*. IEEE, 2022, pp. 351–356.

[38] ——, "Security compliant and cooperative pseudonyms swapping for location privacy preservation in vanets," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 8, pp. 10 710–10 723, 2023.

[39] C. Sommer, R. German, and F. Dressler, "Bidirectionally coupled network and road traffic simulation for improved ivc analysis," *IEEE Transactions on mobile computing*, vol. 10, no. 1, pp. 3–15, 2010.

[40] M. Behrisch, L. Bieker, J. Erdmann, and D. Krajzewicz, "Sumo–simulation of urban mobility: an overview," in *Proceedings of SIMUL 2011, The Third International Conference on Advances in System Simulation*. ThinkMind, 2011.

[41] K. Emara, "Poster: Prext: Privacy extension for veins vanet simulator," in *2016 IEEE Vehicular Networking Conference (VNC)*. IEEE, 2016, pp. 1–2.

[42] A. Tomandl, F. Scheuer, and H. Federrath, "Simulation-based evaluation of techniques for privacy protection in vanets," in *2012 IEEE 8th international conference on wireless and mobile computing, networking and communications (WiMob)*. IEEE, 2012, pp. 165–172.