7-29-2020

Towards a Framework for Preserving Privacy in VANET

Ikjot Saini
University of Windsor

Towards a Framework for Preserving Privacy in VANET

By

Ikjot Saini

A Dissertation
Submitted to the Faculty of Graduate Studies
through the School of Computer Science
in Partial Fulfillment of the Requirements for
the Degree of Doctor of Philosophy
at the University of Windsor

Windsor, Ontario, Canada

2020

Towards a Framework for Preserving Privacy in VANET

by

Ikjot Saini

APPROVED BY:

J. E. Martina, External Examiner
Federal University of Santa Catarina

M. Azzouz
Department of Electrical and Computer Engineering

R. Kent
School of Computer Science

S. Samet
School of Computer Science

A. Jaekel, Co-Advisor
School of Computer Science

S. Saad, Co-Advisor
School of Computer Science

May 28, 2020

DECLARATION OF CO-AUTHORSHIP/PREVIOUS PUBLICATION

I. Co-Authorship

I hereby certify that this dissertation incorporates material that is the result of my research conducted under the supervision of my advisors Dr. A. Jaekel and Dr. S. Saad. In all cases, the key ideas, primary contributions, experimental designs, data analysis, interpretation, and writing were performed by the author.

I am aware of the University of Windsor Senate Policy on Authorship and I certify that I have properly acknowledged the contribution of other researchers to my dissertation, and have obtained written permission from each of the co-author(s) to include the above material(s) in my dissertation.

I certify that, with the above qualification, this dissertation, and the research to which it refers, is the product of my own work.

II. Previous Publications

This dissertation includes the extended or original version of the papers that have been previously published/submitted for publication in peer reviewed conferences and journals, as follows:

- I. Saini, S. Saad, and A. Jaekel, "Evaluating the effectiveness of pseudonym changing strategies for location privacy in vehicular ad-hoc network," Security and Privacy, p. e68, May 2019, doi: 10.1002/spy2.68.

- I. Saini, S. Saad, and A. Jaekel, "Speed Based Attacker Placement for Evaluating Location Privacy in VANET," in Ad Hoc Networks, Cham, 2019, pp. 215–224.

- I. Saini, S. Saad, and A. Jaekel, "A Comprehensive Review of Pseudonym Changing Strategies in Vehicular Networks.," I. J. Network Security, vol. 21, no. 5, pp. 785–796, 2019.

- I. Saini, S. Saad, and A. Jaekel, "Identifying Vulnerabilities and Attacking Capabilities Against Pseudonym Changing Schemes in VANET," in Intelligent, Se-

cure, and Dependable Systems in Distributed and Cloud Environments, Cham, 2018, pp. 1–15.

- I. Saini, S. S. Ahmed and A. Jaekel, "Attacker Placement for Detecting Vulnerabilities of Pseudonym Change Strategies in VANET," 2018 IEEE 88th Vehicular Technology Conference (VTC-Fall), Chicago, IL, USA, 2018, pp. 1-5.

I certify that I have obtained a written permission from the copyright owner(s) to include the above published material(s) in my dissertation. I certify that the above material describes work completed during my registration as a graduate student at the University of Windsor.

III. General

I declare that, to the best of my knowledge, my dissertation does not infringe upon anyone's copyright nor violate any proprietary rights and that any ideas, techniques, quotations, or any other material from the work of other people included in my dissertation, published or otherwise, are fully acknowledged in accordance with the standard referencing practices. Furthermore, to the extent that I have included copyrighted material that surpasses the bounds of fair dealing within the meaning of the Canada Copyright Act, I certify that I have obtained a written permission from the copyright owner(s) to include such material(s) in my dissertation. I declare that this is a true copy of my dissertation, including any final revisions, as approved by my dissertation committee and the Graduate Studies office, and that this dissertation has not been submitted for a higher degree to any other University or Institution.

ABSTRACT

Vehicular Ad-hoc Network (VANET) is envisioned as an integral part of the Intelligent Transportation Systems as it promises various services and benefits such as road safety, traffic efficiency, navigation and infotainment services. However, the security and privacy risks associated with the wireless communication are often overlooked. Messages exchanged in VANET wireless communication carry inferable Personally Identifiable Information(PII). This introduces several privacy threats that could limit the adoption of VANET. The quantification of these privacy threats is an active research area in VANET security and privacy domains. The Pseudonymisation technique is currently the most preferred solution for critical privacy threats in VANET to provide conditional anonymous authentication. In the existing literature, several Pseudonym Changing Schemes(PCS) have been proposed as effective de-identification approaches to prevent the inference of PII. However, for various reasons, none of the proposed schemes received public acceptance. Moreover, one of the open research challenges is to compare different PCSs under varying circumstances with a set of standardized experimenting parameters and consistent metrics. In this research, we propose a framework to assess the effectiveness of PCSs in VANET with a systematic approach. This comprehensive equitable framework consists of a variety of building blocks which are segmented into correlated sub-domains named Mobility Models, Adversary Models, and Privacy Metrics. Our research introduces a standard methodology to evaluate and compare VANET PCSs using a generic simulation setup to obtain optimal, realistic and most importantly, consistent results. This road map for the simulation setup aims to help the research & development community to develop, assess and compare the PCS with standard set of parameters for proper analysis and reporting of new PCSs. The assessment of PCS should not only be equitable but also realistic and feasible. Therefore, the sub-domains of the framework need coherent as well as practically applicable characteristics. The Mobility Model is the layout of the traffic on the road which has varying features such as traffic density and traffic scenarios based on the geographical maps. A diverse range of Adversary Models are

important for pragmatic evaluation of the PCSs which not only considers the presence of global passive adversary but also observes the effect of intelligent and strategic 'local attacker' placements. The biggest challenge in the privacy measurement is the fact that it is a context-based evaluation. In the literature, the PCSs are evaluated using either user-oriented or adversary-oriented metrics. Under all circumstances, the PCSs should be assessed from both user and adversary perspectives.

Using this framework, we determined that a local passive adversary can be strong based on the attacking capabilities. Therefore, we propose two intelligent adversary placements which help in privacy assessment with realistic adversary modeling. When the existing PCSs are assessed with our systematic approach, consistent models and metrics, we identified the privacy vulnerabilities and the limitations of existing PCSs. There was a need for comprehensive PCS which consider the context of the vehicles and the changing traffic patterns in the neighbourhood. Consequently, we developed a Context-Aware & Traffic Based PCS that focuses on increasing the overall rate of confusion for the adversary and to reduce deterministic information regarding the pseudonym change. It is achieved by increasing the number of dynamic attributes in the proposed PCS for inference of the changing pattern of the pseudonyms. The PCS increases the anonymity of the vehicle by having the synchronized pseudonym changes. The details given under the sub-domains of the framework solidifies our findings to strengthen the privacy assessment of our proposed PCS.

DEDICATION

To my parents, family and mentors for their endless love, support, guidance and encouragement.

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to my advisors, Professor Dr. Arunita Jaekel and Dr. Sherif Saad, for their continuous support of my Ph.D. study and research, for their extensive professional guidance, and for their immense knowledge. I am thankful to my thesis committee members Dr. Robert Kent and Dr. Saeed Samet for their valuable comments and professional assistance. I would also like to thank the staff members of the School of Computer Science for their continuous support throughout the program. I would like to express my profound gratitude to my parents, family, mentors and friends who were the motivation and strength behind this work.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ADAS Advanced Driver-Assistance Systems

BSM Basic Safety Message

C-V2X Cellular-Vehicle to Everything

CA Certificate Authority

CATA Context-Aware and Traffic Adaptive

DSRC Dedicated Short Range Communication

EAS Entropy of Anonymity Set

FCC Federal Communications Commission

ITS Intelligent Transportation System

OBU On-Board Unit

PCS Pseudonym Changing Scheme

PETs Privacy Enhancing Technologies

PII Personally Identifiable Information

RSU Road Side Unit

TPD Tamper-Proof Device

V2V Vehicle to Vehicle Communication

V2X Vehicle to Everything Communication

VANET Vehicular Ad hoc Network

WAVE Wireless Access for Vehicular Environment

Chapter 1

Introduction

1.1 Vehicular Ad hoc Network

A Vehicular Ad hoc Network (VANET) consists of smart vehicles on the road and provides communication services among nearby vehicles and with roadside infrastructure [4]. The technology is dedicated to increasing the safety and prevention of traffic congestion due to the growing number of vehicles on the road. Wireless communication will enable the situational awareness of the vehicles. Today, the vehicles are equipped with Advanced Driver-Assistance Systems (ADAS) [5], which helps the driver by giving safety alerts and warnings. These electronic systems are equipped within the vehicle and are limited to the host vehicle for these alerts. As shown in Fig. 1.1, the drivers will be able to receive the safety alerts from the surroundings by providing connectivity among all the vehicles.

Figure 1.1: Vehicular Ad-hoc Network [1]

When crossing from an intersection, the nearby vehicles, traffic lights and pedestrians send their status messages, which allow the vehicle to make a safety-related decision based on safety applications. These applications take all received messages from the surroundings and generate safety-critical warnings and alerts.

This technology will revolutionize the transportation systems and will bring a safer experience for the drivers on the road. The communication among various entities in the vehicular network is generally called Vehicle to Everything Communication (V2X). As shown in Fig. 1.2, the communication can take place from a vehicle to infrastructure, another vehicle, pedestrian, a mobile device, grid and network. Dedicated Short Range Communication (DSRC) [6] is an IEEE 802.11p based wireless communication technology for Vehicle to Vehicle Communication (V2V) [7] to enable cooperative awareness. It provides high-speed direct communication for safety among vehicles and nearby infrastructure. DSRC is non-interoperable with cellular networks. The communication among the vehicles is carried out on a radio frequency band of 75 MHz on 5.9 GHz of radio spectrum. It is reserved for the use of Intelligent Transportation System (ITS).

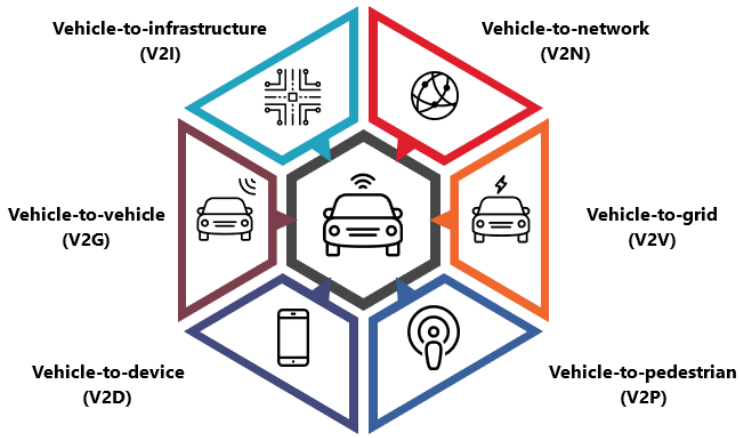


Figure 1.2: V2X Communication [2]

At the time of writing this dissertation, there is a new technology gaining momentum, known as Cellular-Vehicle to Everything (C-V2X) communication [8]. C-V2X is a 3GPP standard that is the alternative to IEEE802.11p for V2X communication, and it has an evolutionary path towards 5G. Many automakers in Japan, Europe and

North America, like Toyota, General Motors and Volkswagen, have started deploying with IEEE 802.11p based V2X technology in 2019. While automakers like Ford plan to integrate C-V2X in their new vehicles by 2022 [9]. Currently, the industry is waiting for the USA Federal Communications Commission (FCC) to make the final decision on the 5.9GHz band allocation. In this dissertation, our work is focused on using the DSRC protocol.

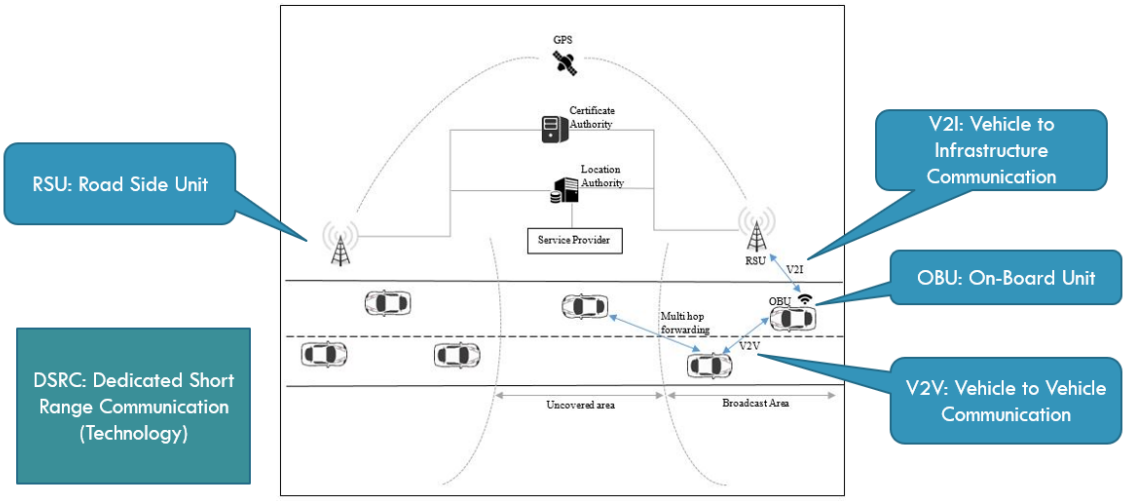


Figure 1.3: DSRC based Vehicular Communication

Fig. 1.3 shows various participating entities in the vehicular network and their communication. The vehicles have On-Board Unit (OBU), which enables DSRC communication with each other and the Road Side Unit (RSU) that constitute the infrastructure, including traffic signal controllers, roadside signage systems, cameras, and parking meters. These RSUs are directly connected to the back-end service providers such as Certificate Authority, which deals with short-term certificate provisioning, Location Authority and Law Enforcement Authority.

Fig. 1.4 illustrates the layered model of the Wireless Access for Vehicular Environment (WAVE) architecture [10] protocol system, which is a new standard for vehicular communication. IEEE 802.11P WAVE is only a part of a group of standards related to all layers of protocols for DSRC-based operations. The scope of IEEE 802.11 is strictly limited to MAC and PHY level standards with a single logical channel. The challenges and knowledge related to the DSRC channel plan and operational concept

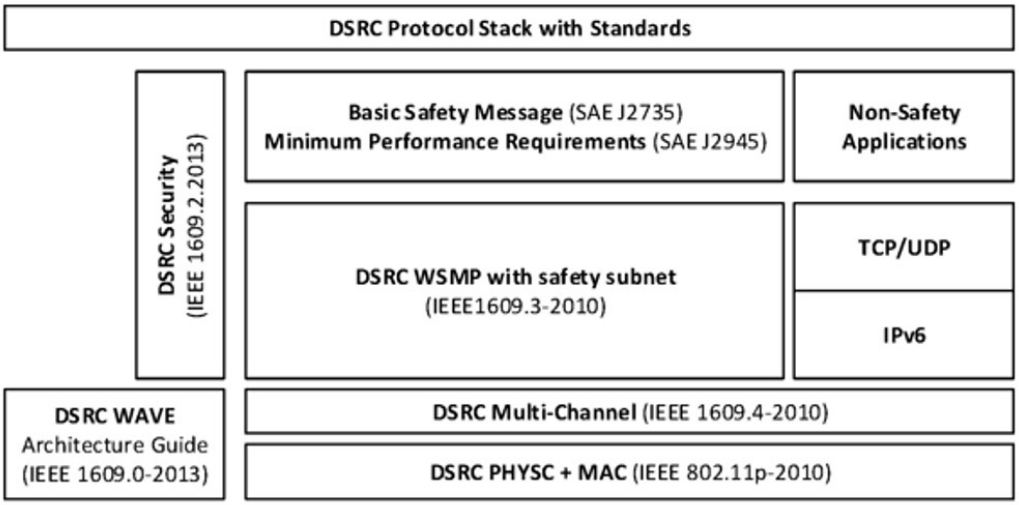


Figure 1.4: WAVE Architecture for VANET [3]

are controlled by upper layer IEEE 1609 standards. Especially, IEEE 1609.4 standard is right above IEEE 802.11p, which enables the operation of upper layers across multiple channels without requiring knowledge of PHY layer parameters. IEEE 1609.2 is dedicated to DSRC security, which runs along with IEEE 1609.3 and SAE J2735 and SAE J2945 for V2V communication.

This technology is still in development, and several issues need investigation and extensive analysis. There is a need for a realistic definition of security and privacy in the context of V2X communication, as it can have a direct impact on human lives. The user information is sensitive and prone to new security and privacy attacks in this evolving cyberspace.

1.2 Privacy in Intelligent Transportation Systems

ITS aims to have efficient traffic management and safer driving experience [11]. ITS applications rely on the real-time information of the vehicles on the road. Therefore, a wireless communication network is an essential requirement for data collection. The information associated with a car can be used to infer the driving behaviour when the vehicular sensor information is collected over time. It is predicted that future technologies will equip the vehicles with advanced navigation systems and will gather

sensor data from more than 200 sensors in a vehicle [12]. This information is primarily intended for communicating road conditions and driving preferences to manage traffic congestion and prevent collisions. However, the data collected with high precision and sensitive information such as location, timestamp and a vehicle identifier introduce a privacy threat. With this set of data, precise movement patterns can be inferred along with driving behaviour, which can lead to long term driver profiling and vehicle tracking. Many people are legitimately concerned about their privacy, and automobile manufacturers need to pay attention to the system design for privacy starting at the development phase. The easiest way to ensure privacy is not to share *any* driving information and operate as an isolated system, which is the case for most vehicles on the road today. However, this approach will fail to take advantage of the tremendous benefits that can be achieved in a connected vehicular environment. Therefore, a balance is required to determine what information can be shared and with whom.

1.2.1 What is Privacy?

Privacy Enhancing Technologies (PETs) [13] divide the privacy into five properties. *Anonymity* of the driver is the property that the target vehicle is indistinguishable from all the neighbouring vehicles. *Undetectability* is the property when the adversary fails to identify the existence of the target vehicle or a specific message that helps in recognizing the target vehicle. *Unlinkability* describes the inability to link temporary vehicle identifiers of the same vehicle *Plausible deniability* refers to the subject's ability to deny the performed action. *Confidentiality* describes the inability of the attacker to access the content of the messages that reveal sensitive information, e.g. in plain text.

The privacy of an individual is considered a fundamental right in most parts of the world. In 1948, the Universal Declaration of Human Rights [14] declares that everyone has a right to privacy at home, with family and in correspondence. The Global Internet Campaign [15] presented a report which classifies privacy in four categories: Information privacy, location privacy, the privacy of communication and territorial privacy. Generally, the privacy of the location information is about control-

ling access to this information. The user must know how much information is being collected, used and stored by the service providers. With technological advancements and pervasive computing, people often have to choose between using the services for convenience or sacrificing personal privacy.

Often, it is a general public consensus that information cannot be of any use for anyone. However, with the rise of personalized advertisements, a massive amount of data is already being collected and used for targeted ads. With information asymmetry [16], it becomes evident that individuals are often unable to see the extent to which various industries are using their data. Upon examining the profiling information, a significant amount of private information about an individual can be revealed, which cannot be otherwise obtained. One of the use cases is to have the frequently visited location map to know the activities of the person, further using this information in insurance cases, lawsuits, personal disputes. Vehicle tracking can be used legitimately for surveillance purposes by authorities. On the other hand, if an adversary starts vehicle tracking due to malicious intent, then it can escalate the level of the threat to the safety and security of the person in addition to the privacy. Dötzer [17] has discussed several examples of the VANET privacy problems related to the information used by police, private investigator, insurance companies and foreign secret services. As VANET requires the vehicles to broadcast the location information without encryption frequently, adversaries can easily eavesdrop this information and can track the driver. Therefore, the upcoming technologies must focus on the privacy aspects of using location information.

1.2.2 Privacy Challenge in Vehicular Networks

In V2V, the most important message is the *Basic Safety Message (BSM)*, which is defined by SAE J2735 Message Set Dictionary [18] and it conveys vehicle state information in the range of 300m for safety applications. BSM contains the data elements, including the vehicle status, position, size and other additional information as required by the type of safety application. BSMs consists of two parts: Part I contains critical state information sent to all the nearby vehicles every tenth of

a second, and Part II contains less important information, which is required less frequently and not present in every BSM transmission. Fig. 1.5 shows some of the properties included in each part of the BSM.

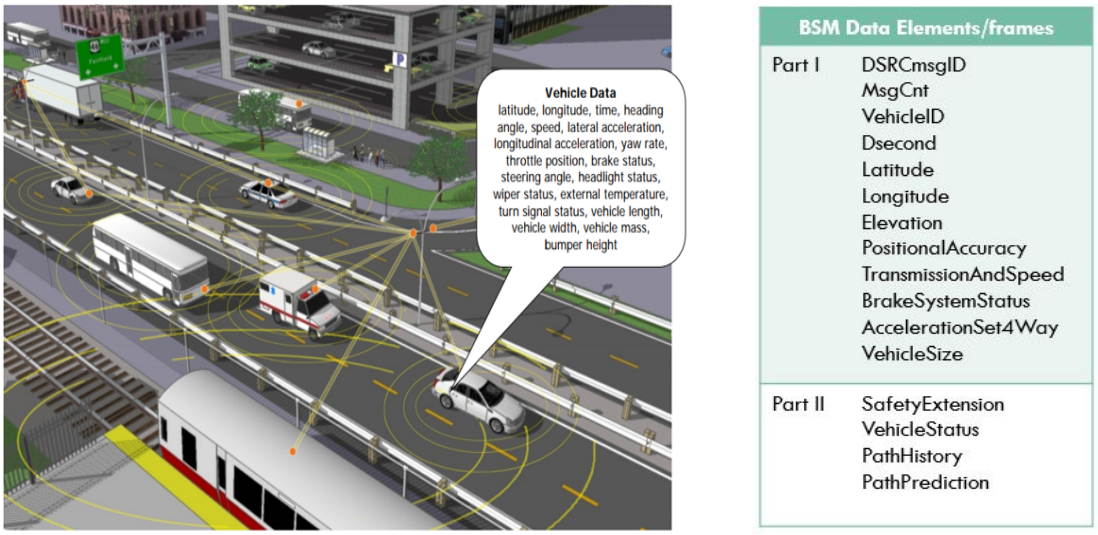


Figure 1.5: Basic Safety Message

Vehicles broadcast BSMs unlike any other one to one communication. In a mobile ad hoc network, the communication channel is secured for one to one wireless communication. Nevertheless, this is a new challenge in VANET, that the transmission of the safety messages is without encryption. It introduces the threat to the information associated with the vehicle, which can be collected over time and then aggregated to get useful knowledge. This knowledge can be of trips taken by a vehicle and would directly relate to frequently visited places like home, work or hospital. When the information can be deduced by listening to the safety messages, the vehicle can be tracked based on location, time, and fixed road network. In the connected vehicle environment, the vehicle joins the communication network and starts sending BSMs ten times per second message rate. The messages are not encrypted to increase computational performance in real-time. The message contains the geographical information as latitude and longitude, current time with a resolution of 1 millisecond, positional accuracy, and a temporary identifier to correlate the stream of BSMs from a given sender. This set of information can reveal Personally Identifiable Information (PII)

when the adversary collects BSMs over time. Another DSRC equipment can listen to the continuous broadcasting stream of BSMs and can gather the data based on location, time and temporary identifier. Over time, the data correlation may infer sensitive information such as the person's driving behaviours, driving patterns, frequently visited places. As the collected data has a high precision for position and time, there are significant chances for complete vehicle tracking and driver profiling.

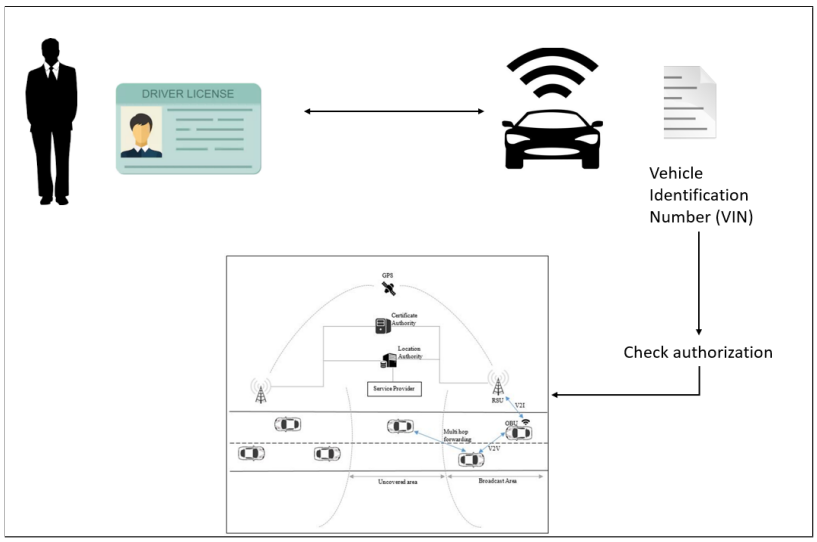


Figure 1.6: Authorized participation in VANET based on an original Vehicle Identifier

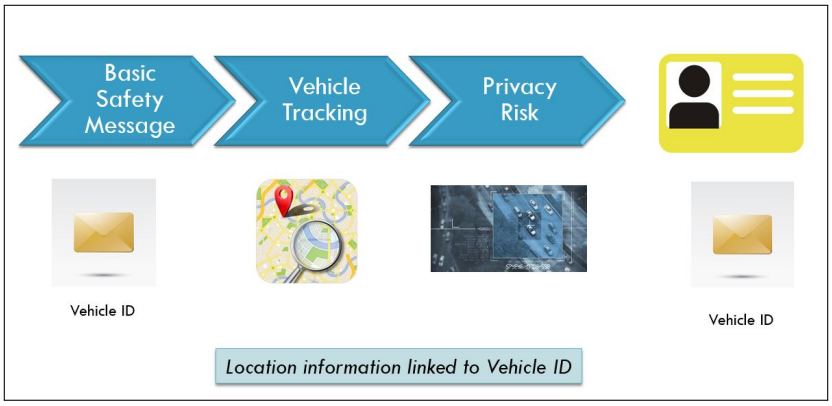


Figure 1.7: Current Location privacy Problem

The network of the connected vehicles is going to be vast, and the safety information broadcast among these vehicles will facilitate the location, situational and context awareness. These messages must be sent from an authorized, active vehicle, and the information in the message must be authentic. To have the authorization to

participate in the vehicular network, the vehicle will use an identifier given by the authorities, and this identification will be of the vehicle such as Vehicle Identification Number (VIN), as shown in Fig. 1.6. It will send the message using this identification once the vehicle is authorized and participates in the vehicle to vehicle communication. The problem of location privacy arises when a vehicle uses the same identifier, VIN, for all the messages with location and time information. Fig. 1.7, illustrates the general location privacy problem showing how the use of safety messages can lead to vehicle tracking when an original and static identifier (e.g. VIN) is always attached to streaming location information. As WAVE standard [10] has multiple layers, and each layer has multiple identifiers, there is a requirement that the identifiers on all of these layers are changed frequently to ultimately achieve the anonymity [19].

1.2.3 Current state of privacy in VANET

The privacy issues can arise as soon as the collected data forms the information trail with an identifier. To preserve privacy, the first step is to dissociate the identifier and information trail. Pseudonymization is a widely accepted approach to solve this problem of location privacy. Pseudonyms are the temporary identifiers that hide the vehicle's real ID and can be used to authorize a vehicle to be the part of the vehicular network. It is essential to change these temporary identifiers from time to time to disconnect the information stream associated with a specific identifier.

This changing of the pseudonym plays a vital role in preserving privacy, and the technique to change pseudonym is generally referred to as Pseudonym Changing Scheme (PCS). Several PCSs have been proposed in the last few years. They use many different approaches, such as changing pseudonyms based on the number of neighbouring vehicles, vehicle speed, area or zone, radio silence. The common idea is to maintain unlinkabiliy and untraceability. *Unlinkability* refers to the inability to relate two pseudonyms of a vehicle, and *untraceability* refers to the inability to correlate the location information with a set of pseudonyms to infer private information of vehicle's whereabouts. The primary objective of the PCSs is to determine an effective way to change pseudonyms in such a way as to create the maximum possible

confusion for the attacker. However, there are additional constraints that must be considered, e.g. changing pseudonyms at a rapid rate can impede tracking but may exhaust the given set of pseudonyms. Periodically changing pseudonyms are computationally simple but allows the adversary to predict and correlate the new and old pseudonyms. A suitable PCS should provide unlinkability of the pseudonyms with low communication overhead and without exhausting the available set of pseudonyms.

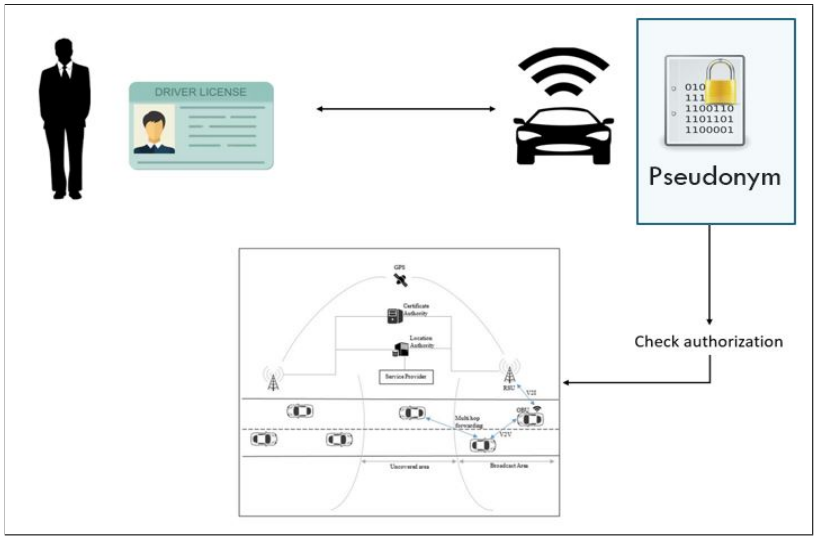


Figure 1.8: Authorized participation in VANET based on Pseudonym

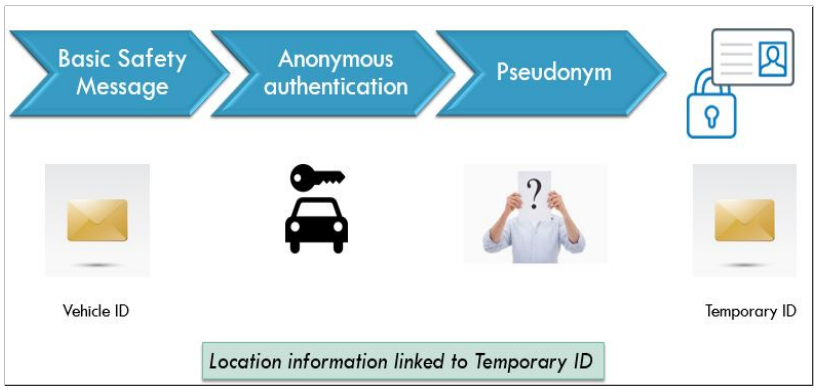


Figure 1.9: Use of the pseudonym (temporary identifier) is widely accepted approach to preserve privacy

A Security Credential Management System (SCMS) [20] can be used for managing all the credentials and identities of the vehicles. As all the vehicles in the network must be authorized participants, this process of assigning the pseudonyms to the ve-

hicles is carried out by Certificate Authority (CA). CA ensures that the vehicle has a legitimate vehicle identifier such as Vehicle Identification Number (VIN) to register on the communication network. Each vehicle receives a set of pseudonyms, and CA keeps a record of the association of real ID to these pseudonyms. Fig. 1.8 shows that the vehicle participates in the vehicular network using a pseudonym instead of an original identity. Fig. 1.9 demonstrates that the use of pseudonyms as the temporary identifiers can disrupt the direct inference of the location information associated with a vehicle. The adoption of a pseudonym for authentication of BSM leads to an increase in anonymity potentially. Due to the possibility of malicious vehicles in the network, it is essential to hold the vehicles accountable for their actions by keeping the record of their identities. This prevents the implementation of perfect privacy in vehicular communication as the authorities have private information. This kind of privacy is known as *conditional privacy*, which means that the real identification and the associated temporary identifiers of the vehicle are not revealed to any other participant of the communication network unless the vehicle has performed a malicious activity.

1.2.4 Open Challenges

The existing work on VANET privacy addresses some of the important challenges for pseudonym changing schemes. However, there are many open problems related to safety, scalability, flexibility, and applicability that still need to be resolved. In this section, we will identify the research gaps and discuss the potential areas where work is required.

Pseudonym reuse: Existing PCSs typically specify when and how to change pseudonyms but do not consider the frequency of this change. When the vehicle rapidly changes pseudonyms, the given set of pseudonyms may exhaust, and the vehicle is forced to repeat the given pseudonyms. This repetition increases traceability. Also, when a vehicle uses the pseudonym for a longer duration, it adds to traceability. There is a need to develop a mechanism that adequately deals with the number of changes required for optimal performance and privacy. Secondly, the reuse

of pseudonyms should be addressed carefully concerning location privacy. If the same pseudonym is used by a vehicle, it will likely increase the chances of being traced.

Fixed area: Many schemes use fixed area (e.g. traffic lights at intersections) to trigger pseudonym changes [21]. This has a limitation that such fixed areas for changing pseudonyms may not lie in the route of a vehicle. This will prevent the vehicle from changing pseudonyms for long periods and thus increase the traceability. More resilient schemes are needed so all the vehicles can change pseudonyms at an acceptable rate irrespective of trip route or location.

Safety/privacy trade-off: This is an issue for schemes that use radio silence [22] prior to pseudonym change. Radio silence helps to increase confusion for the attacker, but stopping communication at dense traffic areas increases the safety risk. Therefore, future research can be directed toward finding an alternative to radio silence for communication interruption or finding a trade-off between safety and privacy.

Security and Accountability: The exchange of the pseudonym increases location privacy and adds confusion to adversary tracking. However, it is necessary to balance strong privacy with the need to hold individuals accountable for malicious behaviour and misuse. So, mechanisms to report misbehaviour to the authorities for further processing must be implemented. When there is an internal adversary, then many of the schemes fail to preserve privacy, for example, group-based schemes and encryption schemes. Thus, future work should consider protection against attacks from an internal adversary.

Adaptive approaches: The flexibility and adaptability are essential as the vehicular environments are highly dynamic. Trigger-based approaches generally work well. However, these triggers should be applicable under dense and sparse traffic conditions and for different road networks.

1.3 Motivation

The quantification of privacy has been a challenging task, and a multitude of variables in the vehicular environment further complicate the evaluation and comparison.

The current state of the art pseudonym changing schemes lacks the consistent set of assessment elements. There is a wide variety of techniques to change the pseudonyms; however, the effectiveness of one PCS cannot be compared to another unless there is a unified framework that allows a fair comparison. The existing PCSs consider different road networks with changing traffic models, different adversary models with varying attacking strengths and distinct privacy metrics. Additionally, the simulation study of these PCSs has been carried out on different simulators. The inconsistency in the simulation parameters and the simulation setup also plays a vital role because it impacts the overall simulation mechanism. The majority of the existing schemes consider the presence of the global passive adversary as the worst-case scenario. However, a local passive adversary is a more realistic type of attacker, and the literature on PCSs lacks in evaluation in the presence of a local passive adversary.

We aim to bridge these gaps in the assessment of pseudonym changing schemes by providing a comprehensive framework which deals with a consistent set of realistic traffic and adversarial scenarios and uses common privacy metrics to compare the level of privacy. We determine the attacking capabilities of a local passive adversary and develop the intelligent attacker placement schemes accordingly. This strategic adversary placement helps in understanding the threat level in its region of interest. There is an absence of the intelligent local adversary in state of the art PCSs. The vehicular network is highly dynamic, and the traffic patterns change frequently; therefore, the mobility models are significant for the equitable assessment. In general, the underlying factors to change the pseudonyms are directly related to the traffic scenario or, in other cases, to the specific area. For this reason, the framework incorporates different mobility models, which generally are based on the region, which impacts the layout of the road network. Above all, the privacy assessment needs a consistent set of privacy metrics that not only quantify the anonymity of the individual but also measure the ability of the adversary to successfully track the vehicles when the vehicle is using a PCS. We also propose a context-aware and traffic adaptive pseudonym changing scheme aiming to increase the anonymity and minimize the tracking of the vehicle.

The inconsistency of the evaluation, as mentioned above, elements made it dif-

ficult to quantify and compare PCSs. The integration of these building blocks in a systematic manner helps in observing the differences, strengths and weaknesses when PCSs are tested under a variety of simulation scenarios with a consistent set of models and metrics. Eventually, this framework is a step towards supporting the industry standards in measuring privacy with the identified evaluation models, methods and metrics. As the auto industry enters the digital age, there will be an inherent conflict of a highly regulated industry with the least regulated one. In digital, self-regulation is the only approach to information security and privacy. In this case, an evaluation framework to assess privacy schemes becomes essential for the Intelligent Transportation System's ecosystem.

Our assessment led to identifying the privacy vulnerabilities and the limitations which are present in the existing PCSs. There are multiple factors involved in the evaluation, and when these PCSs are evaluated under similar circumstances, it reveals the weaknesses and strengths of PCSs. Hence, there is a need to have a comprehensive PCS which addresses these limitations and provides a higher level of privacy.

1.4 Research Contributions

The goal of this dissertation is essentially two-fold. First, it aims to develop a PCS that addresses the limitations and vulnerabilities of existing schemes. It has *better* performance under different traffic conditions and realistic adversary models in a vehicular network. The second purpose of this dissertation is to provide a systematic approach to help the research community for an equitable assessment of PCSs that will ensure an effective comparison of different schemes with consistent models and metrics. To accomplish this objective, the major contributions are summarized as follows:

- We reviewed the current state of the research for improving location privacy and determined the research gaps based on safety and privacy. After investigating the existing pseudonym changing schemes, we classified and compared these schemes to point out the differences, advantages and disadvantages. We

discussed the privacy vulnerabilities, characteristics and design requirements of pseudonym changing schemes.

- We constructed an equitable privacy assessment framework to compare a variety of PCSs with a consistent set of network models, adversary models, and privacy metrics. We proposed privacy metrics for evaluating the impact of the local passive adversary.

- We proposed two intelligent adversary placements that aim to maximize the degree of observation with limited capabilities. We evaluated the level of privacy provided by several PCSs in the presence of a local passive adversary. We assess the threat level, which indicates the effectiveness of the adversary.

- We proposed a pseudonym changing scheme that utilizes the context of the vehicle and traffic patterns to leverage the optimum situation for changing pseudonyms. We evaluated the privacy preserved by our proposed scheme as compared to the existing schemes in the presence of a local adversary. For this assessment, we have taken a consistent set of mobility models, adversary models, privacy metrics and simulation parameters.

From the aforementioned contributions, the following publications have been produced:

- I. Saini, S. Saad, and A. Jaekel, "A Comprehensive Review of Pseudonym Changing Strategies in Vehicular Networks.," I. J. Network Security, vol. 21, no. 5, pp. 785–796, 2019. *(Chapter 2)*

- I. Saini, S. Saad, and A. Jaekel, "Identifying Vulnerabilities and Attacking Capabilities Against Pseudonym Changing Schemes in VANET," in Intelligent, Secure, and Dependable Systems in Distributed and Cloud Environments, Cham, 2018, pp. 1–15. *(Chapter 2,3)*

- I. Saini, S. Saad, and A. Jaekel, "Evaluating the effectiveness of pseudonym changing strategies for location privacy in a vehicular ad-hoc network," Security and Privacy, p. e68, May 2019, doi: 10.1002/spy2.68. *(Chapter 3)*

- I. Saini, S. Saad, and A. Jaekel, "Speed Based Attacker Placement for Evaluating Location Privacy in VANET," in Ad Hoc Networks, Cham, 2019, pp. 215–224. *(Chapter 4)*

- I. Saini, S. S. Ahmed and A. Jaekel, "Attacker Placement for Detecting Vulnerabilities of Pseudonym Change Strategies in VANET," 2018 IEEE 88th Vehicular Technology Conference (VTC-Fall), Chicago, IL, USA, 2018, pp. 1-5. *(Chapter 4)*

1.5 Organization of the Dissertation

The rest of this dissertation is organized as follows:

- In chapter 2, we investigate the current schemes of changing pseudonyms for location privacy in VANET to identify the problems in different pseudonyms changing schemes. We classified these schemes into two categories based on infrastructure and user-based schemes. Also, we compared these schemes with respect to techniques used for pseudonym change.

- In chapter 3, we developed a comprehensive framework for Equitable Privacy Assessment Framework for simulation studies. We discussed various building blocks of the proposed framework. We then provided a simulation road map for the generation of consistent simulation results and one of the privacy assessments of the existing PCSs.

- In Chapter 4, we present our proposed Intelligent Adversary Placements for privacy evaluation under different traffic conditions.

- In Chapter 5, we introduce a new PCS, which is *Context-Aware and Traffic Adaptive*. We compare the performance of the proposed approach with existing techniques and in terms of both anonymity and tracking success rate.

- Finally, in Chapter 6, we present our conclusions and some directions for future research.

1.6 Conclusion

In this chapter, we introduced the Vehicular Ad hoc Network and the privacy challenges in this network. Using DSRC technology and wireless communication technology, the vehicles communicate directly with each other and their surroundings to provide safety and manage traffic congestion. The safety-critical messaging in this vehicular communication introduces privacy risk. Vehicles use pseudonyms for anonymous authentication of Basic Safety Messages. To preserve privacy, there is a need to change these pseudonyms. We discussed the vulnerabilities of current pseudonym changing schemes and the motivation of this work. Then, we stated the goal of this dissertation and summarized the research objectives.

Chapter 2

Literature Review

2.1 Background

2.1.1 Mechanism for preserving privacy: Anonymization

V2V communication uses a safety message broadcast, which must be sent to other vehicles while preserving the sender's privacy. The message contains sensitive information like personally identifiable information and real-time location. To prevent the tracking of vehicles and inference of personal information, there are various methods such as hiding events, adding dummy events, obfuscation, and anonymization. Among all these possible mechanisms, the only anonymization can be used for providing location privacy in vehicular networks. As for hiding, the events in V2V communication would result in safety problems. Similarly, adding dummy events will jeopardize the functioning of safety applications and increase security threats. Obfuscation of the location information has a direct impact on the working of V2V applications, as this is critical for various location danger warnings to notify the other vehicles in the vicinity. Therefore, anonymization is a suitable option for preserving privacy, which anonymizes the vehicle identities and prevents direct linking of the personal identification information to a vehicle.

2.1.2 Conditional Anonymous Authentication

Complete anonymization may allow malicious vehicles to become a part of the network, which directly affects the network's operability. Vehicle authentication supports the security requirements for authentication and non-repudiation. Anonymous authentication is a good idea because the users participating in the vehicular network

should be legitimate and must have specific credentials like driver's license, VIN, VID of OBU and License plate. This information is used for identification purposes and authenticates the user to be an authorized user. In this way, only the vehicles with credentials can participate, and this eliminates the risk of unauthorized users in the network. Therefore, the security risks for active security attacks are limited to insiders. In the connected and autonomous vehicles, where the traffic and users rely on trustworthy messages for the safety warnings, insider attacks from malicious users can cause significant damage. There is a need for accountability, so such vehicles can be tracked by the authorities and ultimately excluded from the network. Therefore, conditional anonymous authentication is needed for the privacy-preserving mechanism. It provides the network's reliability and trust by authenticating authorized vehicles while preserving their anonymity and also enables the revocation of the malicious vehicle in case of misbehaviour.

2.1.3 Pseudonym Lifecycle

The pseudonym is an identifier that is used in place of the real identification of the entity for anonymous communication. The pseudonyms in context to vehicular communication are the short-term identifiers that are used in place of vehicle identifier (VID), which is embedded in the On-Board Unit. Certificate Authority authorizes all the vehicles and provides a set of pseudonyms that are not linkable to each other. Still, the relationship among them can be proved by using the credential. Here, credential means that each pseudonym has a certificate issued with it, which enables the authentication of the vehicle and proves that this pseudonym is valid. In this way, the vehicle is authorized. The pseudonyms are not only the substitute for the real identity but also provide accountability to revoke the malicious users in the network. Unlike other anonymous authentication mechanisms, the authorities maintain the linking information of the real identity and the set of pseudonyms for each vehicle. Therefore, a pseudonym serves as the best solution for providing anonymity and unlinkability.

The general lifecycle of the pseudonym in the context of the vehicular environment

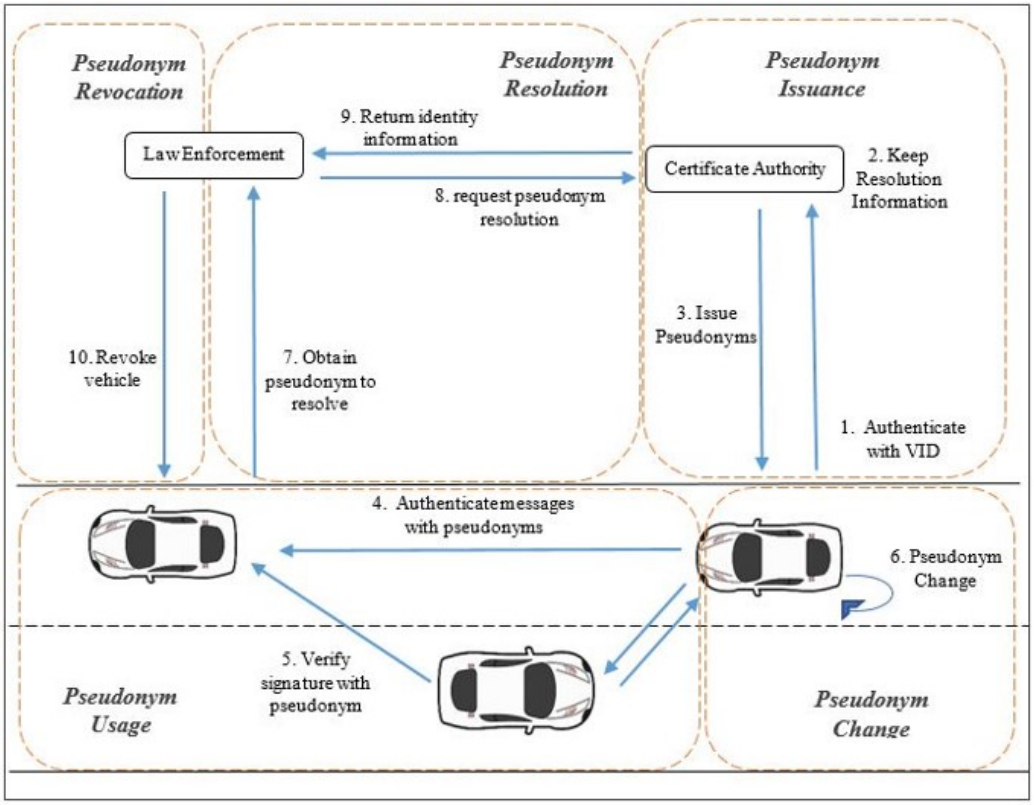


Figure 2.1: Pseudonym Lifecycle

involves pseudonym issuance, pseudonym usage, pseudonym change, pseudonym resolution and pseudonym revocation. These five phases are interdependent and affect the functioning of each other. The pseudonym issuance is implicitly dependent on pseudonym resolution and how these identifiers are revoked. The pseudonym issued to a vehicle should be accountable, pseudonym resolution and revocation work based on accountability while the pseudonym change is dependent on the pseudonym usage.

Pseudonym Issuance

The real identity of the vehicle is the vehicle ID (VID), and it is provided by the department of motor vehicles when the vehicle is registered [23]. VID is securely stored in the On-Board Unit of the vehicle [24]. VID is the signed certificate that allows the unique identification of the vehicle. This identity is associated with information about the driver and the vehicle. Therefore, the driver does not want to reveal VID and

pseudonyms are used to preserve privacy. VID is used to authenticate the valid vehicle, and after successful authentication, the vehicle can participate in the vehicular network. For the pseudonym issuance process, a Trusted Authority(TA) is responsible. This Trusted Authority can be a Certificate Authority(CA) or Pseudonym Provider(PP). It would be a good idea to not fully trust one authority and distribute the trust among different authorities, as a compromised, fully trusted authority can misuse the information. The pseudonym issuing authority authenticates the vehicle based on its VID and verifies the validity of the vehicle; that is, the vehicle should not be revoked; issues pseudonyms. The process of pseudonym resolution is closely related to the pseudonym issuance. Thus, the association of the pseudonym and identity is retained securely by a trusted authority [25]. More importantly, the resolution information is critical and must be strongly protected from the security attack on the infrastructure of authority. The pseudonyms have an expiry, which limits the activation time or usage time. This limited validity ensures the prevention of the Sybil attack.

Pseudonym Usage

The vehicle authenticates the message it sends, which helps the receiver to verify that the message is from a valid vehicle. The pseudonym should not be revoked or expired. The verification of the pseudonym is done locally, and most of the schemes allow the certificate attachment with the message. This certificate ensures that the vehicle is legitimate, and the pseudonym used by the sender is authentic. The verification process imposes a problem for the vehicles. The total number of messages for verification exponentially increases than the number of messages sent from the vehicle; in other words, the received messages will be more than the number of messages sent. Hence, the efficiency of real-time applications may be compromised.

Pseudonym Change

The vehicle cannot have a single pseudonym because it allows easy tracking. Also, when a single-vehicle changes its pseudonym, an adversary can quickly notice that

only one pseudonym is different and link the old and new pseudonyms [26]. The old and new pseudonyms associated with a vehicle can be linked based on the location, movement, actions and other parameters in the communication stack [27]. Therefore, to avoid linkability, not only the pseudonyms need to change but also other identifiers in the communication stack. The neighbouring vehicles can only provide sufficient confusion for the attacker when the pseudonym change occurs at the same time or in a synchronized manner. The frequency of the pseudonym change is crucial for real-time safety applications' performance, and it plays an essential role in the balance of privacy and safety [28]. The frequency, place, time and situation for changing pseudonyms are the open research issues that need more investigation [29].

Pseudonym Resolution

Trusted authority like Certificate Authority holds the resolution information (linking pseudonyms to actual IDs) that can be provided to law enforcement representatives when requested, e.g. in case of security attack and accidents. The trust can be distributed among various authorities, for more security. For instance, the Law Enforcement Authority (LEA) is responsible for requesting the Certificate Authority (CA) to provide the resolution information to the Law Enforcement Representative. This process may not be straightforward due to complex legal policies and laws.

Pseudonym Revocation

The pseudonyms of a misbehaving vehicle should be revoked, and the vehicle is excluded from vehicular communication [30]. Most of the existing schemes revoke only one pseudonym of the vehicle, which is known to LEA at that time. Therefore, other pseudonyms associated with the vehicle can still allow the vehicle to participate [31]. To revoke all the pseudonyms of the vehicle, VID of the vehicle should be revoked with further denial of refills. This scheme still allows the vehicle to participate until its current pseudonyms expire. Thus, effective pseudonym revocation is an open issue. The revoked pseudonyms are collectively kept in a Certificate Revocation List (CRL), and this list is distributed to all the authorized vehicles in the communication. If any

message is received from the revoked vehicle, then the message is dropped. But the management, distribution and update of CRL increase the complexity of the system. Currently, the researchers are investing in the balance of privacy and practicality in CRL management.

Pseudonym security requirements

There are various privacy attacks on the pseudonyms, which can be prevented if proper measures are taken. In this section, we identify some characteristics of PCSs to balance privacy requirements such as unlinkability and anonymity [32] with security and accountability.

Location Privacy

Location information of an individual can be used to determine more relevant information about that individual, which has a link to other services used by that individual. Therefore, real-time location sensing poses a significant threat to user privacy. The frequent trips to specific locations can reveal the home address and working place easily. At the same time, the frequently visited site may also include hospitals, police stations, or other destinations that show users' social and personal circumstances. Such information about the user's behaviour may be used by a third party like an insurance company for its benefits. To prevent the disclosure of information, either the minimum possible information should be revealed in the broadcasting safety messages, or the driver must have authority to the extent of the revelation of data.

Conditional Anonymity

Within a set of potential senders, the message sender should be anonymous, but the law enforcement should be able to resolve the identity in the case of misbehaviour. Hence, conditional anonymity allows the anonymous message transfer and at the same time ensures the identity resolution by law enforcement, which is needed for vehicular networks [33].

Accountability

The identity resolution mechanism can ensure the accountability of the vehicles participating in the vehicular network. Identity resolution is a crucial aspect of conditional anonymity. The anonymous authentication ensures that the participating vehicles are legitimate. But there may be a situation when the authorized vehicle misbehaves, and the authorities need to revoke this vehicle. The authorities must have a resolution mechanism to get the real identity of the anonymous vehicle from the current anonymous identity for obtaining the real identity of this misbehaving vehicle, .

Distributed Trust among authorities

The authorities which are responsible for the pseudonym issuance, resolution and revocation must not be fully trusted. The trust among these authorities should be distributed so that a single compromised authority cannot reveal the information of the vehicles [34]. The authorities may be a certificate authority, trusted authority, revocation authority, law enforcement authority, and resolution authority. As in some cases, there may be just one or two authorities that are fully trusted, and the information is stored in a centralized manner. This can be dangerous since the compromised centralized authority would reveal the information. Therefore, by distributing the trust among authorities, the data can be secured. Not just one authority has an entire set of information regarding a vehicle, and all the authority has a subset of information which can only be revealed when requested by another authority.

Unlinkability

The new and old pseudonyms associated with a vehicle must not be linkable. If the pseudonyms are linkable, then it may provide sufficient information to the adversary to recognize the vehicle, thus becoming traceable.

Fundamental Characteristics of a PCS

Unlinkability

Unlinkability is the anonymity property of two or more Items of Interest (IOI), which the attacker cannot sufficiently distinguish whether these IOIs are related or not [35]. In a vehicular network, the adversary must not be able to correlate the changing pseudonyms associated with the same vehicle. Pseudonyms of a vehicle must not show a direct correlation with each other. For instance, when a vehicle uses the pseudonym, say, 4321234, it changed it to 3421243 or changed from 212121 to 212122, 212123, and so on. These kinds of correlations lead to direct tracking of the vehicle without using the inference from other factors such as location information. Repetition of the limited pseudonyms also leads to compromise of unlinkability.

Untraceability

Untraceability can be seen as the next step to prevent the disclosure of personal information. Unlike unlinkability, this anonymity property addresses the association of pseudonyms of the target vehicle by inferring the location and other meaningful details in the vehicular communication. The determination of the correlation between location and pseudonyms of the vehicle leads to track. Therefore, untraceability is to keep this association unknown to the observer to inference attacks. Untraceability is achievable by introducing more confusion factors for the adversary.

Confusion Factor

This should be an integral part of the technique used for the pseudonym change, which prevents the direct inference of the location information of a vehicle. The streaming information makes it easier for the adversary to figure out the mobility tracks. Confusion factors introduce the required disruptions or alterations in the continuous transmission of the data. Some of the confusion factors are:

a) encryption or radio silence for varying time duration to disrupt the constant plain text message stream,

b) changing pseudonym simultaneously with neighbouring vehicles to increase the anonymity of the vehicle upon pseudonym change.

Safety-Privacy Trade-off

The balance of privacy and safety is essential. However, safety takes priority, which restricts the use of specific techniques like radio silence. Radio silence can be one of the most effective confusion factors as it breaks the stream of data. But the safety applications heavily rely on the redundant data in real-time for warnings and alerts. To use radio silence for PCS, one must carefully address its impact on the safety applications [36].

Computationally Feasible

The vehicular communication has real-time constraints, and the delay in the processing of computation of the safety messages has a direct implication on the safety of the passengers. Therefore, the pseudonym change technique should be computationally feasible as the OBUs have limited capacity compared to RSUs.

Compliance with Pseudonym Life cycle

Pseudonym change is a stage in the overall pseudonym life cycle, and the PCS should be compatible mainly with the process of generation and revocation of pseudonyms. Most of the existing schemes fit in the life cycle without any change. On the other hand, some schemes may introduce a different mechanism for pseudonym generation or may affect how pseudonyms are revoked from the network. In the latter case, it is necessary to provide the potential changes in the life cycle.

General Design Requirements of PCS

A PCS should:

- Prevent location tracking and profile generation

- Maintain untraceability, anonymity, unlinkability and perfect forward secrecy of pseudonyms
- balance the frequency of pseudonym change for every vehicular trip (to have multiple pseudonyms during a trip) and available number of pseudonyms (to avoid exhaustion of available pseudonyms)
- Prevent repetition or duplicates of the pseudonyms by the same vehicle
- Consider different traffic scenarios based on congestion (dense or sparse) and locality (urban or highway)
- Adaptive to the optimal level of privacy based on changing traffic environment
- Maintain the level of privacy in the presence of the intelligent passive adversary
- Preserve conditional privacy and provide accountability

Privacy Vulnerabilities

There are several vulnerabilities in the existing pseudonym changing schemes which compromise the privacy of the driver.

Linking ability of location updates

Pseudonyms may have resolved the problem of the authentication of safety messages. However, this temporary identifier can still link the location updates of the moving vehicle if the temporary identifier remains for a long time in the network. Even though the vehicle changes the pseudonym, the Spatio-temporal information helps identify the vehicle by correlating the pseudonyms. Hence, the mobility tracing can be prevented using an individual pseudonym for only a certain time during the trip and then by changing the given pseudonyms frequently on a longer trip. In the last decade, several PCS have been proposed. These schemes have different location privacy metrics and techniques. However, the effectiveness of these schemes has not been evaluated against the location privacy attacks in different traffic scenarios such

as urban, highway, or rural. It is important to determine which pseudonym changing scheme applies to what kind of traffic scenario.

Frequency of pseudonym change

The pseudonyms are required to change within a time duration so that a longer eavesdropping session does not disclose the information associated with a complete trip. If this happens often, the attacker can deduce the frequently visited places by a vehicle and, therefore, can profile the driver based on the mobility patterns and routine activities. Hence, the vehicles must change the pseudonym often so that attackers can not track complete trips. On the other hand, some existing pseudonym schemes allow the pseudonyms to change at a very high rate. This condition is suitable concerning privacy, but it creates problems with the issuance and re-issuance of the pseudonyms as every vehicle has a limited number of pseudonyms.

Effect of repetition

Many PCSs use a large number of pseudonyms as the changing frequency is higher. It is not practical to use such a large number of pseudonyms with the limited capacity of the OBU. The issuance of these temporary identifiers is also a major concern. It has been suggested [37] that in the initial phase, the set of pseudonyms issued to the vehicle must be valid for three years. Therefore, there is a limited number of pseudonyms. If used with higher frequency, then the vehicle will exhaust all the pseudonyms relatively sooner. Once the vehicle has used all the pseudonyms, it has to repeat as a new set of pseudonyms will be issued after three years. The repetition is a privacy concern because the attacker records all the pseudonyms associated with a vehicle, and repetition increases the tracking success. According to [37], 20 pseudonyms are active for a week. With the changing frequency of 5 minutes, all 20 pseudonyms will be within the knowledge of the attacker in continuous blocks of 100 minutes of eavesdropping.

Knowledge of Pseudonym Changing Scheme

The attackers can take advantage of having detailed information about PCS used by the vehicles. When the adversary knows regarding when and where the pseudonyms will be changed, it benefits the attacker in the placement of the equipment. If all the

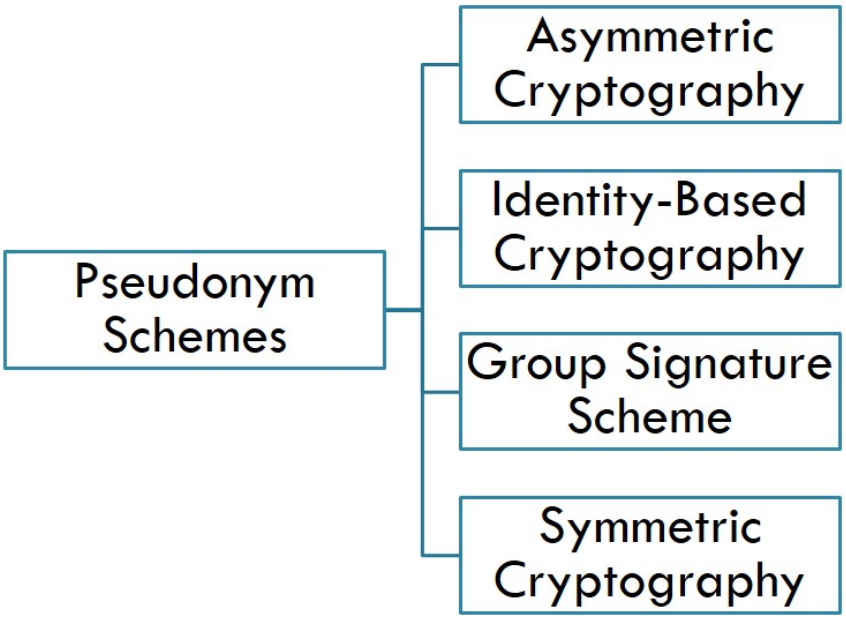


Figure 2.2: Classification of Pseudonym Schemes

vehicles are following the same scheme in all the scenarios, various factors like traffic congestion, the fixed time interval for the change and intersection mix zones helps the attacker to decide the most suitable location for placement for maximum coverage.

2.1.4 Classification of the Pseudonym Schemes

Based on the cryptographic mechanisms, the pseudonym schemes can be classified into four categories as shown in Fig.2.2. The schemes are Asymmetric cryptography, Identity-based cryptography, Group signatures, and Symmetric cryptography. Each cryptographic scheme has some advantages and disadvantages. Effective pseudonym schemes can be obtained by integrating the different schemes.

Asymmetric Cryptography

A set of public-key certificates is pre-loaded in the OBU with the corresponding key pairs by the pseudonym issuing authority [38]. In this case, public key certificates are used as pseudonyms after removing identifiable information. For authentication purposes, the vehicle signs the message with its private key corresponding to the

presently active pseudonym. Then, the message is sent along with the signature and pseudonym certificate. When it is received, the receiver checks the validity of the sender and its pseudonym by message signature, which can be obtained by the pseudonym certificate. Although the VID of the sender remains unknown in this process, which supports anonymity. The pseudonym issuance and refills depend on the backend connectivity to the Trusted Authorities [39]. This enforces the condition of the availability of the infrastructure all the time that may not be possible. The asymmetric key may cause the communication and computational overhead as it sends not only the message but also the signature and certificate. This overhead is relatively more than the identity-based scheme and group signature scheme. In the process of the revocation, the certificate revocation list is required. The problem may arise to manage this list due to the increase in the size of the list [40]. The major issues associated with asymmetric cryptography schemes are the scalability, increase of certificate revocation list, pseudonym linking, pseudonym refill, computational and communication overhead.

Identity Based Cryptography(IBC)

Identity-based authentication [41] allows implicit authentication as the vehicle's identity works as the vehicle's public key. It eliminates the requirement of the separate public key certificate for the authenticity of the vehicle [42]. The private key is generated from the vehicle's identifier, which is used to sign a message similar to the asymmetric cryptographic scheme. As the private key is a relative identifier of vehicle and vehicle may generate on its own, it needs accountability. Therefore, a centralized, fully trusted authority is responsible for the generation of the private keys and assignment to respective vehicles. This authority has complete knowledge of the vehicle and its system parameters. The authenticity of the vehicle is guaranteed because private keys are provided to only the authorized vehicles by the authorities. The authentication characteristics of IBC are similar to that of the asymmetric key scheme. Still, it does not involve certificates for essential public verification, and it cuts down the number of verification and computational overhead caused by the verification pro-

cess. The difference in two schemes lies in the mechanism of key generation. Hence, IBC becomes a preferable choice as compared to the public key scheme in vehicular networks [43]. However, the fully trusted authority may be vulnerable to security attacks. The significant problems with this scheme are related to the constant vehicle's identifiers, which are issues for revocation and computational overhead.

Group Signature Scheme

The group signature scheme reduces the overhead caused by public keys and the changing certificates [44]. Every group shares a common public key, and the group managers provide the private keys to each group member. When a vehicle sends a message, it sends the signature with it. This signature is verifiable with the group's public key, which ensures the validity of the vehicle. The anonymity preserves privacy within the group as the messages, and the sending vehicle is verified by the group signature [45] [46]. The Group signature scheme is similar to a public key scheme with the difference of the issuance of the private key [47]. There is no strict requirement of the availability of the infrastructure at all the time for the reason that the group manager handles this process [48]. However, the group manager can not be fully trusted as it can be part of the active security attack. The possession of complete information about the vehicles in the group is quite unsafe. Another problem can be noticed in the election of the group manager as the vehicles move at high speed; there will be a frequent change of the group manager, which can decrease the effectiveness of pseudonym management. The group signature scheme allows the scalability as a result of pseudonym management based on the group size. However, the vehicular environment is highly dynamic, causing critical computational overhead. Also, the revocation process may undergo a compelling change in the whole group to update the group public key.

Symmetric Cryptography Scheme

Unlike asymmetric cryptography, the symmetric cryptography is efficient with respect to the communication and computational overhead [45]. The process of the symmetric

key scheme is different and uses the message hash, and the secret key and issuance process may differ [49]. All the valid vehicles have the same secret key, which is used to verify the hash of the message. The method of obtaining a hash of the message is identical to the sender and receiver side. The efficiency, in this case, comes with some consequences. The secret key is common to the set of vehicles in vehicular communication, which expands the size of the anonymity set [50]. Further, since non-repudiation can not be achieved with secret key usage, accountability is not possible to maintain.

2.1.5 Location Privacy and Pseudonym Change

The pseudonyms are subjected to change frequently to maintain the untraceability, and this change should be carried out in a certain way, which supports the unlinkability of the pseudonyms. Many of the schemes are proposed in the last decade, but each of them has weaknesses which prevent the complete unlinkability, effects safety applications and cause communication and computational overhead. So, there is a need for a pseudonym changing scheme which addresses when, where and how to change the pseudonym without any such weakness. The pseudonym authentication is useful for privacy protection only when the pseudonyms change frequently and provide unlinkability. The unlinkability refers to the fact that the attacker should not be able to link two pseudonyms of the individual vehicles. However, the pseudonyms are the part of communication, and frequent changes of the pseudonym will adversely affect the overall performance of the network communication. There is a need for the development of PCS, which provides the unlinkability of the pseudonyms with optimal communication performance and provides optimum location privacy. To find a suitable approach, it is essential to find when, where, and how the pseudonyms should change. Many proposed strategies use radio silence, encryption, triggers, area-based mixing and context-based mixing. However, some schemes are not feasible due to overall performance and overhead, while others lack the balance of safety and privacy.

2.1.6 Existing Surveys

Several surveys for the security of the vehicular networks have been conducted. Several surveys exist on the VANET [51] [52] [53] its communication techniques and patterns [7], [54] requirements, architecture, challenges and standards [55], [51]. Most of these surveys focus on the security attacks, security and privacy requirements [56], intrusion detection systems [57], trust management [58], authentication schemes [59], and pseudonym schemes [32]. Privacy requirements in VANET are extensively given by Schaub [60]. Riley [59] has provided a survey of the authentication schemes for VANET and has analyzed the privacy-preserving schemes by considering privacy metrics as anonymity. Raya et al. [61] addressed the security and privacy issues and Krumm [26] outlined the issues of location privacy. Wiedersheim et al. [62] discussed the challenges and issues of the location privacy and provided the idea of the dynamic pseudonym schemes. Rebollo addresses privacy evaluation and metrics- Monedero et al. [24] which suggests the privacy measurement as there are no standardization of the privacy metrics in VANET. The location attacks are mentioned in [27] [28] [29]. The survey of the pseudonym schemes [32] focuses on the various pseudonym mechanisms with the complete pseudonym cycle, requirements, and challenges for each mechanism. Boualouache [30] surveyed the PCS and has given the comparison amongst them. We have presented the classification for the existing pseudonym changing strategies based on the mix zone and mix context which helps in understanding the difference of various strategies with respect to their approaches. For instance, some strategies are user-centric and do not rely on the specific areas and infrastructure for pseudonym change . In contrast, others use particular areas or road networks for pseudonym change. The techniques like radio silence, triggers, encryption have an impact on the performance as well as privacy. Therefore, we have discussed each of the strategies, its advantages and disadvantages briefly. We have identified that different pseudonym changing strategies are evaluating privacy based on various metrics. We have also discussed the research challenges of the pseudonym changing strategy and direction for future work. This classification and comparison can guide the new

researchers as well as help in the current research work to identify the drawbacks and advantages of different strategies.

2.2 Privacy Attacks and Adversary Models

The pseudonym authentication scheme is suitable for providing anonymous authentication to the nodes in a vehicular environment. It maintains anonymity and preserves the privacy of the user. However, the pseudonym schemes have certain loopholes which can provide the attacker sufficient window to execute many attacks. First of all, there are many proposed mechanisms for pseudonym issuance, usage, change, and revocation. Yet there is not one of the mechanisms which can provide a completely reliable and secure pseudonym lifecycle. There are different adversary models and security attacks on the linking of pseudonyms, which are discussed below.

Pseudonym Linking Attack

The pseudonym is used in the safety message broadcast, which implies that the frequent use of the same pseudonym can help identify the target vehicle. The linking property of old and new pseudonyms can reveal the vehicle's identity. Thus, the pseudonym must be changed in such a way that any two of the pseudonyms associated with an individual vehicle do not relate. The two types of linking are described in the next subsections.

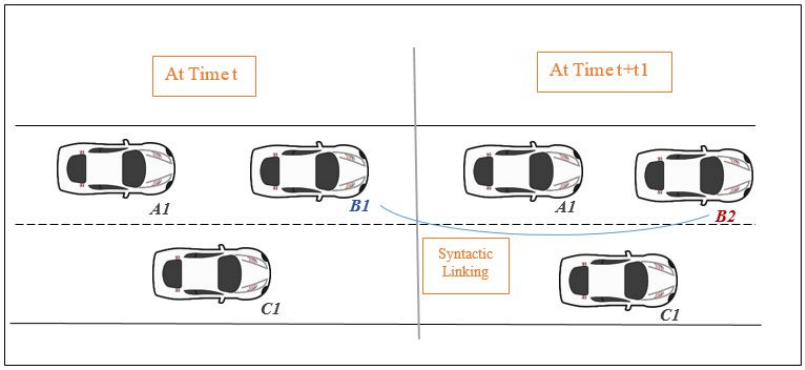


Figure 2.3: Syntactic Linking attack

Syntactic Linking

This type of linking is based on the neighbours of the vehicle. As illustrated in Fig 2.3, the vehicle has two other vehicles in its vicinity, but at time t+1, only one vehicle changes its pseudonym. The change in the pseudonym becomes obvious, and the attacker can determine the target vehicle effortlessly.

It can be solved by the synchronous pseudonym change and it can be further ensured that this change involves more vehicles. Since the vehicle density matters in the syntactic linking, it can not change when it is isolated and must guarantee that it has a certain number of vehicles around or passes through such areas where density is high.

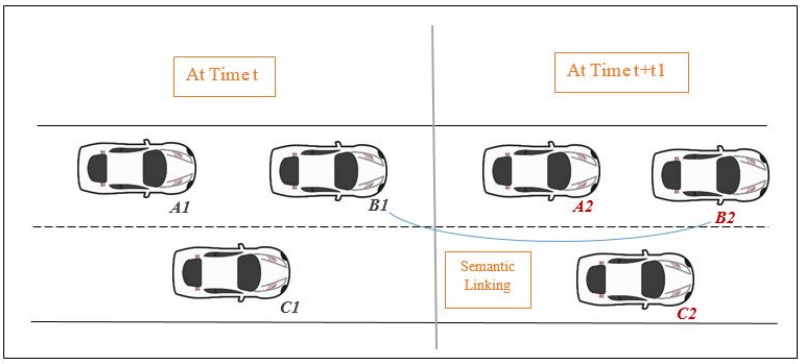


Figure 2.4: Semantic Linking attack

Semantic Linking

This type of linking is critical and involves the data in the message; therefore, it is difficult to prevent as compared to syntactic linking. The information used in the message is analyzed for finding the correlation between the two or more pseudonyms (Fig. 2.4). The system parameters, identifiers, location and the movement of the vehicle provide adequate information for linking the pseudonym. To avoid this linking, mechanisms are required which prevent the location prediction by limiting access to the safety messages for a specific time. This creates complications in the pseudonym schemes, especially in the pseudonym changing phase.

Classes of Adversaries

The adversary model is essential to consider the development of the robust pseudonym mechanism. The main aim of the adversary is to link the pseudonyms, despite their change, and break the anonymity of the user. The following are the types of adversaries.

Active vs Passive Adversary

The *active* adversary aims to alter the information in the message or inject new messages in the network. The examples of such attacks are Man-in-the-Middle attack, timing attack or broadcast tampering. The objective of the *passive* adversary, on the other hand, is to gain information to track and profile the drivers, by eavesdropping on messages. This kind of adversary is passive as it does not modify messages or the message stream. Although the passive adversary typically does not disrupt the ongoing communications in the network, the main concern with this kind of attack is that it is tough to detect, because the adversary is merely listening to the unencrypted messages and does not perform any alteration.

Global vs Local Adversary

The adversary can be *global* or *local*, based on the geographic area it can cover. The global adversary can eavesdrop all the messages from all vehicles at all times, without leaving any blind spot. In a real-world scenario, this would require the adversary to place the equipment to cover a target geographic area, e.g. a city completely. Considering the number of equipment that would be needed to achieve this, the global adversary scenario is unlikely due to the prohibitive cost. However, many privacy evaluation schemes adopt this model, as it is the strongest adversary and can be used to model the "worst-case" situation.

The local adversary only has access to a limited number of attacking equipment, each with a specified communication range. Therefore, it is generally not able to eavesdrop on all vehicles in the area of interest. This is a much more realistic sce-

nario, in terms of the adversary model. Due to the limitations on the number and communication range of the eavesdropping equipment, the local adversary needs to place these resources in a way that maximizes its attacking capabilities. Most PCSs reported in the literature use a simple random placement of listening equipment. In our work, we propose an *intelligent* local adversary model to investigate how the strategic placement of a limited number of eavesdroppers affects successful vehicle tracking in the presence of a local adversary.

Global Passive Adversary (GPA)

This adversary eavesdrops entire communication by using the radio receivers and the infrastructure like RSU [26]. These radio receivers are deployed in a vast area of interest. The adversary may also use cameras, but that will increase the cost significantly. The biggest threat to pseudonym schemes is the global passive adversary, as it is impossible to avoid this adversary to detect the changing pseudonyms. Each event and message are traceable. Even with Mix Zones [50], GPA can link pseudonyms semantically by predicting the location of the vehicle. It knows the location where it enters Mix Zone and based on this information; it can predict the time taken in the Mix Zone, and further, it can relate all the possible exit events to the expected event [45].

Local Active Adversary

The capability of this adversary is limited in the area based on the transmission range. The vehicles involved in vehicular communication are authenticated by an authority [21]. But there may be some selfish vehicles that intend to manipulate the messages or injects false information for their benefit. These are the participating vehicles and can not be directly identified unless the misbehaviour is detected [63]. The collusion of such an active local adversary with the global passive adversary brings the most challenging security problems. The privacy threats increase when the active local adversary provides information regarding other legitimate vehicles to the global passive adversary.

2.3 Classification of Pseudonym Changing Schemes

The **mix zone** is an unobserved zone where the vehicles cannot be eavesdropped due to radio silence and mix in such a way that after leaving the mix zone, they are indistinguishable. In 2003, Beresford [64] introduced this concept in the context of pervasive computing. To understand the mix zone, assume that the attacker has installed the radio receivers at specific points on the road. Now, the attacker can listen to network communication, especially the broadcasting beacons, which contain sufficient information to know the vehicle's movement and driving behaviour. This knowledge can help an attacker predict when the identifiers are changed, and the vehicles have different pseudonyms.

Mix Context: To mitigate the node movement's predictability, there are a few approaches; increasing the size of the mix zone, increasing silent periods, and increasing the frequency of updates. But these may not be either feasible or safety effective when implemented in the real world. In the case of longer silent periods, the chances of accidents increase exponentially. The larger mix zones would still not promise that all vehicles would pass through a certain area and be able to change the pseudonym. All these conditions are critically important to consider the development of PCS.

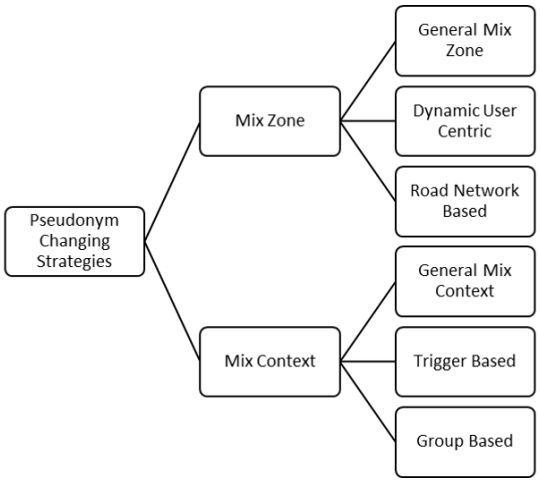


Figure 2.5: Taxonomy of Pseudonym Changing Schemes

2.3.1 General Mix Zone Schemes

The general mix zone schemes, as shown in Table 2.1, are infrastructure-based pseudonym changing schemes. We point out the key concept of the scheme along with the changing strategy. This strategy determines when, where and how the pseudonyms are changed. We indicate the evaluation method used in PCSs and inspect the problems associated with the changing strategy.

In 2007, Buttyan [63] introduced the first idea of using a mix zone in the context of vehicular networks. The mix zone is an area not controlled by the adversary, and the pseudonyms can be changed without eavesdropping the attacker. This provides unlinkability of the pseudonyms enabling location privacy. Buttyan evaluated the effectiveness of this kind of mix zone by using the success probability with the Bayesian decision algorithm. The success probability is the successfully mapped vehicles from the number of vehicles in the mix zone. The author emphasizes the minimum error probability, which is provided by the Bayesian decision algorithm. The results of the simulations carried out using MOVE and SUMO show that a stronger adversary can obtain higher success probability. Also, there is a saturation of success probability at 60 percent due to changing mobility patterns at junctions with half of the controlled junctions. In other words, if 50 percent of the intersections is compromised, then there is a 60 percent of success probability of the linking pseudonyms.

Freudiger [21] proposed the first implementation of the mix zone in vehicular ad hoc networks in 2007. According to Freudiger, the intersections are the mix zones that have infrastructure like RSU that assist in the pseudonym change. Additionally, the vehicles within mix zones encrypt the safety messages with the symmetric key provided by the RSU. Therefore, this mix zone is also known as Cryptographic Mix Zone(CMIX). The CMIX protocol has three phases in its life cycle: key establishment, key forwarding, and critical update. Also, it has a mix zone and extended mix zone. The entropy and success ratio of the vehicles are used as the privacy metrics. By simulation on MATLAB, the Manhattan network is assessed with a highly dense vehicular network. As entropy is used for evaluation, the tracking depends on the

traffic density and its delay characteristics. The success ratio is inverse to the entropy, which indicates that with increasing entropy, an attacker would not be able to link pseudonyms successfully. The anonymity of the vehicle increases linearly, while the success ratio of the adversary becomes negligible. This approach does not prevent internal adversary, and it is not scalable and adaptable.

Carianha [65] addressed the vulnerability in the CMIX protocol and proposed an effective approach that mitigates the risk. CMIX has encryption with the mixed zone, and the shared key is available to the participating vehicles. This increases the risk associated with the internal adversary who is authenticated for the vehicular network

Table 2.1: General Mix Zone Schemes

Author [ref]	**Year**	**Key concept**	**Changing Strategy**	**Privacy metric**	**Problems**	**Evaluation method**
Buttyan [63]	2007	First idea of Mix Zone in VANET	Intersection as Mix Zone	Success probability	Frequency of pseudonym change	Analysis, Simulation
Freudiger [21]	2007	First implementation of Mix Zone	Cryptographic Mix Zone (CMIX)	Entropy	prone to the internal adversary,Not scalable,Not adaptable	Simulation
Carianha [65]	2011	Eliminate risk of the internal adversary in CMIX	Extended secure CMIX	Success rate	Vehicles must pass at least one mix zone	Simulation
Scheuer [66]	2011	Communication proxy in mix zone with asymmetric key encryption	ProMix Zone(PMZ)	Number of vehicles (Anonymity Set Size)	Bandwidth overhead caused by increased beacon size	Simulation
Boualouache [22]	2014	Silence and Swap	Signalized Intersection as Mix Zone	Entropy of Anonymity Set Size	Silence cause problem in safety applications and vehicle may not pass a mix zone	Analysis, Simulation
Zhang [67]	2017	Does not rely on fully trusted authorities, group key instead of a shared key in CMIX	One Time Identity Based Authentication Asymmetric Group Key Agreement	Group Size (Anonymity Set Size)	Group key change and management	Simulation

and, therefore, can have the shared key. The proposed scheme consists of a status forwarding scheme limited to the neighbours and two of the overhead compensation strategies. The evaluation of the given scheme is carried out on OMNET, SUMO, and Veins based on the success rate. The results show that the success rate is directly proportional to the number of vehicles in the mix zone. As this scheme extends CMIX, it has a limitation of a fixed mix zone because vehicles may or may not pass through such a mix zone.

OTIBAAGKA is the strategy to eliminate the use of fully trusted authorities in the vehicular networks proposed by Zhang [67]. OTIBAAGKA stands for One Time Identity Based Authenticated Asymmetric Group Key Agreement. It is used to create CMIX while dealing with potential security attacks. He also suggested the benefit of using a group key rather than using a shared key in CMIX. It makes the network more dynamic and diverse. Even the internal adversary can have access to a few vehicles in that group. Unlike other group schemes, it does not force the group to change the group key when a vehicle leaves. The results based on the simulation on NS2 shows the effectiveness of this scheme.

In 2011, Scheuer [66] proposed the idea of ProMix Zone(PMZ) that is the communication proxy in the mix zone. The intersections of highways and crossroads are the mix zones with the infrastructure units dedicated to pseudonym change. These infrastructure units are proxies that are interconnected and have a pair of asymmetric keys with a CA certificate. This proposal does not involve the pseudonym distribution strategy. The simulation of PMZ on JAVA shows the results and dependencies. With the growing number of vehicles in PMZ, the performance increases. The problem may arise with the size of the beacon, which then causes bandwidth overhead. But the author suggested that it can be resolved by using ECC. PMZ is scalable, while its deployment is still fixed.

Boualouache [22] presented the idea of Silence and Swap at Signalized Intersection(S2SI), which would be the mix zone. The silence and swap are the two protocols that together form a mix zone. The silence protocol creates a secure silent mix zone, and swap protocol ensures the exchange of the pseudonyms within vehicles of that mix

zone under a controlled RSU. The author argued that the radio silence in the mix zone does not affect safety. Unlike other mix zones, it exchanges the pseudonyms among vehicles rather than changing them for an individual vehicle. This might increase the confusion for the adversary as tracking become difficult, but the communication stack parameters are not changed, which can still enable the tracking. In addition to that, there is another problem that may result in no change of pseudonym. There is a moderate probability of a vehicle to not pass through such a signalized intersection that prevent the vehicle from changing its pseudonym. The author evaluated the privacy based on the entropy of the anonymity set size and the attacker's success rate. More privacy is offered with lesser success rate and higher entropy of anonymity set size. The entropy of anonymity set depends on the arrival rate. With a small arrival rate, the number of vehicles at signalized intersection increases, which increases entropy. The simulation on OMNET, SUMO and VEINS gives the comparative analysis of the CMIX and S2SI. According to the author, this scheme can avoid more than 60 percent of the signature verification as compared to CMIX strategy.

2.3.2 Dynamic User-Centric Mix Zone

Dynamic user-centric mix zone PCSs are similar to the general mix zone as both types rely on infrastructure units for the pseudonym change. These PCSs have dynamic triggers as compared to the general mix zone PCSs. Similar to general mix zone PCSs, these PCSs have similar limitations based on the traffic situations.

Lu [68] suggested a pseudonym changing scheme using a mix zone where the social spot acts as a mix zone. The social spots are the temporary aggregation places where many vehicles stop by for a specific period. The locations can be the road intersection at a red light and parking lot in public places. The anonymity set size is the parameter for the evaluation of privacy. In the small social spot, the anonymity would increase with the increase of anonymity set size. In other words, more of the vehicles at intersection changing pseudonyms simultaneously, more the anonymity provided. On the other hand, the massive social spots provide more anonymity when the vehicle's inter-arrival time is less, and the duration of the vehicle to stay in the

Table 2.2: Dynamic User-Centric Mix Zone Schemes

Author [ref]	**Year**	**Key concept**	**Changing Strategy**	**Privacy metric**	**Problems**	**Evaluation method**
Lu [68]	2011	For city environment, scalable and adaptable	Social Spot as Mix Zone	Anonymity Set Size	Only applicable in dense scenarios	Analysis
Boualouache [69, 70]	2016	VLPZ, Prevent both linking attacks	Dedicated roadside infrastructure as Mix Zone	Anonymity Set Size	Every vehicle may not be able to visit such zone	Analysis, Simulation
Ying [71]	2013	DMLP, practical and simple to implement	Dynamic Mix Zone on demand of vehicle	Entropy of anonymity set size	Traffic density may not be enough to create mix zone	Analysis
Ying [72]	2015	Dynamic Mix Zone	Candidate Location List, defined timeslot for change	Anonymity Set Size and Success Rate	Sparse network	Analysis, Simulation
Arain [73]	2017	DPMM, use reported servers with RSU	Dynamic Pseudonym based on Multiple Mix zone (DPMM)	Delay and packet delivery ratio	No privacy evaluation for anonymiza-tion	Simulation

mix zone is higher. The author provided the analysis for the privacy provided by both the small and large social spots. Additionally, the numerical results are given for further validation. This scheme is useful in a city environment, and it is scalable and adaptable. However, it does not support the sparse vehicular networks.

Boualouache [69, 70] introduced another mix zone concept with the existing roadside infrastructure, which is dedicated to change the pseudonyms. The toll booth and gas stations are examples of such a mix zone as these places provide high traffic density, which helps in increasing anonymity set size. The scheme is named as Vehicular Location Privacy Zone(VLPZ). By interrupting the continuous tracking for some time, the pseudonyms can be changed securely without eavesdropping. The author has given the analytical model for the proposed scheme and further supported with the numerical analysis. In [70], the simulation results are presented based on a reputation mechanism. SUMO, OMNET++, and VEINS are used for the simulation.

The problem in this scheme can be caused by the silence provided within VLPZ, which jeopardizes the safety communication. There is a need for a balance of safety and privacy.

Ying [71] proposed a scheme that is user-centric and straightforward to implement. Dynamic Mix-Zone for Location Privacy(DMLP) enables the vehicle to create a mix zone on demand based on the traffic statistics, privacy level required and predicted location of the vehicle. It is more adaptable, scalable and performs well in sparse networks. The messages in mix zone are encrypted. The analysis shows the entropy of the anonymity set size of the mix zone varies with changing network size. As the scheme is compared with DLP, the size of the mix zone in DLP does not change, but in the case of DMLP, it changes and increases the location privacy.

Recently, Arain [73] proposed a PCS which outperforms RPCLP, EPCS, and MODP; this technique is known as Dynamic Pseudonym based multiple mix zone (DPMM). It uses roadside infrastructure as RSU and a network of reported servers. The method uses encryption and vehicle cooperation based on reputation techniques. On the SUMO simulator, the delay characteristics and packet delivery ratio are measured and compared with the existing methods. The outcome demonstrates the effectiveness of DMPP over RPCLP, MODP and EPCS.

2.3.3 Road Network Based Mix Zone

MobiMix is the idea presented by Palanisamy [74] in 2011 in the context of the anonymization effectiveness and attack resilience. The author argues that the placement of rectangular mix zones in the road network is vulnerable and careful measures should be taken before its installation. Palanisamy also proposed a method for road network mix zone placement, which provides location privacy. This method is evaluated on GTMobiSim with geographical maps on different scales. Besides, MobiMix offers a high level of resilience to timing and transition attack. Later in 2012, the author recognizes two significant vulnerabilities and evaluated the efficiency of the prevention measures [75]. The vulnerabilities are found in the user mobility, which, in some manner, is restricted as well as the road network characteristics and temporal

and spatial information. In 2013, Palanisamy [76] demonstrated the risks associated with the location privacy of the vehicles in the mix zones and how the location exposure can be restricted to prevent timing and transition attacks.

Table 2.3: Road Network Based Mix Zone Schemes

Author [ref]	**Year**	**Key concept**	**Changing Strategy**	**Privacy metric**	**Problems**	**Evaluation method**
Palanisamy [74–77]	2011-2015	Attack resilient, placement strategies	MobiMix	Information entropy	Difficult to compare with other schemes due to different evaluation metric	Analysis, Simulation
Liu [78]	2012	Three Placement constraints and two heuristic placement algorithms	Multiple mix zones preventing information attacks	Information entropy	Primarily focussed on placement, not the changing scheme	Analysis, Simulation

Liu [78] suggested the concept of using multiple mix zones to prevent attacks based on the side information provided by the user. Majorly, the author gives a method to place the mix zone in such a manner that it reduces the privacy risks. The idea of multiple mix zones is effective in breaking the continuity of the tracking more frequently. Liu indicated three placement constraints of the mix zone and two of the heuristic algorithms for the placement. The limitations are related to cost and service, graph, and traffic. The scheme is analyzed based on information entropy. The simulation analysis on CPLEX reveals that the traffic density increases the location privacy as there are more vehicles for finding the best match.

2.3.4 General Mix Context

The mix context concept is different from the mix zone with respect to the usage of infrastructure units. The Mix context schemes are independent of the specific location where the infrastructure units are responsible for pseudonym change. In Table 2.4, we discuss some of the early works in mix context schemes.

Li [79] proposed the idea of mix context for the first time in 2006. It is a user-

centric approach that does not rely on a particular location, as in the mix zone. The vehicles can independently determine when to change the pseudonyms. Unlike the mix zone, mix context allows vehicles to decide when and where to change pseudonyms. Now every vehicle on the road has a high probability of changing its pseudonym as it does not need to pass through a mix zone for the change and depending on user requirements for location privacy. The technique proposed by Li has two phases, namely, *swing* and *swap*. *Swing* enables vehicles to synchronize updates loosely during the change in their velocity, and *swap* is the extension of the *swing*. It facilitates the exchanging of the pseudonyms among vehicles to increase location privacy. The author evaluated the scheme with the entropy of anonymity set size as the privacy metric under the random and restricted pedestrian mobility. This scheme uses a random silent technique as the base and focuses on the prevention of the tracking mitigation. The drawbacks of this scheme are that it makes use of silent periods, and the exchange of pseudonyms needs accountability. Also, it is not reliable in a non-cooperative environment.

The first implementation of the mix context was done in 2007 by Gerlach [80]. The context mix models arguably prevent vehicle tracking better than mix zone as the vehicles are changing the pseudonyms independent of the location, which removes the certainty of change at a particular location. Now freely moving vehicles change pseudonyms while they are moving on the road and decide among themselves for synchronized change. The location privacy significantly increases as the number of vehicles increases. The observation from the simulation on JAVA using JIST/SWANS and STRAW shows that the tracking time is affected due to traffic density. The entropy of the anonymity set size is measured for the comparisons.

Liao [81] attempted to propose a scheme that allows the synchronous pseudonym change. In this approach, the status information of the vehicle and the simultaneity of the pseudonym change are considered. The author described the algorithm and supported it by giving simulation results. The simultaneous change ensures the prevention of the syntactic attacks in which the adversary cannot identify the vehicle if numerous vehicles are changing their pseudonyms altogether. There is no risk to

Table 2.4: General Mix Context Schemes

Author [ref]	**Year**	**Key concept**	**Changing Strategy**	**Privacy metric**	**Problems**	**Evaluation method**
Li [79]	2006	First idea of Mix Context	User centric, swing and swap	Entropy of Anonymity Set Size	Silent periods and exchange needs accountability	Simulation
Gerlach [80]	2007	First implementation of Mix Context	Vehicles cooperate, No infrastructure needed, No fixed places	Entropy of Anonymity Set Size	Non-cooperative behavior of vehicles	Simulation
Liao [81]	2009	Synchronous pseudonym change algorithm	Prevent semantic and syntactic attacks	Success Rate	In case other vehicles do not have similar status	Simulation

safety in this scheme as it does not use radio silence. The simulation is carried out on C++ and STRAW by utilizing the evaluation metric as a success rate.

2.3.5 Trigger Based Mix Context

The most popular and dynamic PCSs are the Trigger based mix context schemes. As shown in Table 2.5, the changing strategies of such PCSs vary based on the dynamic Trigger used by the vehicle. These PCSs can effectively be used in places where the infrastructure units are not present, and the vehicle has to protect itself from long term tracking. Some of the example triggers are based on speed and number of neighbouring vehicles.

Eckhoff [82] presented the usage of pseudonym pools, which enables the vehicles to change their identities autonomously. The scheme can be enhanced with the slotted time for static sized pseudonym pool. It also has an exchange of pseudonyms, which increases location privacy exponentially. The mapping and tracking of the vehicles become harder. The entropy of the anonymity set size is the privacy metric used for evaluation of the scheme. The simulation setup uses SUMO, OMNET, and INET. The drawback of the scheme is the accountability of the exchanged pseudonyms. The authorities must have a new mapping to revocate the malicious user.

Song [83] proposed the concept of location privacy based on vehicular density.

The pseudonyms of all the vehicles in vicinity change as the threshold reaches. There is a vehicular threshold, which is the triggering factor. It is defined as k-1; that is, if there are k-1 neighbours in the vicinity of the vehicle and they all can listen to each other, then they all change the pseudonyms altogether. This simultaneous change increases the confusion for the attacker. This scheme is evaluated based on the success rate of the adversary. The author has compared AMOEBA and CMIX schemes, and the simulation results support the comparison. It outperforms both schemes with respect to the success rate. The simulation using NS2, SUMO, and TRaNS shows the performance of the dense network. This scheme may not perform well in sparse networks as it requires a certain number of the vehicular density around the vehicle for pseudonym change. On the other hand, it applies to the vehicle to vehicle communication. Buttyan [84] proposed a scheme that uses silent periods based on the velocity of the vehicles. The pseudonym change would occur as the vehicles' velocity drops below 30 km/h, and the vehicles stop sending the beacons for the duration when the vehicle is moving slowly. It makes this scheme independent of the explicit synchronization and pseudonym change in a fixed place. This idea of an implicit trigger is applicable in the traffic jams and at the red light where the vehicle moves slowly; therefore, it is named as SLOW. The author also argues that this scheme has no problem with safety applications, as slow-moving traffic has fewer chances of accidents. The scheme's analysis shows that the success rate is directly related to the velocity and the density of the vehicles. The author has also shown the effects on safety and computational complexity. The drawback of this scheme is that the vehicles in the light traffic are more traceable as the change becomes obvious when there are no or a few vehicles in the vicinity.

Eckoff [85] presented *SlotSwap* which is the extension of the work in [82]. This scheme promises strong and affordable location privacy with consideration of the network and computational overhead. The time-slotted pseudonym pools are used, which regulate the change of the pseudonym based on the time slot and to make the synchronized change, GPS signal is used. In this type of pseudonym pool, the pseudonyms are reusable as they are bound to the particular time slot. The author

Table 2.5: Trigger Based Mix Context Schemes

Author [ref]	**Year**	**Key concept**	**Changing Strategy**	**Privacy metric**	**Problems**	**Evaluation method**
Eckhoff [82]	2010	Time slot synchronization	Use of static size pseudonym pools	Entropy of Anonymity Set Size	Accountability of exchanged pseudonyms	Simulation
Song [83]	2009	Trigger based on vehicular density	No effect of frequency of pseudonym change	Success rate	Inefficient in the sparse network and no semantic protection	Simulation
Buttyan [84]	2009	SLOW, implicit trigger	Change occurs as velocity drop down 30 km/h	Success rate	Traceable in light traffic	Analysis
Eckhoff [85]	2011	SlotSwap	extension of [28], strong and affordable	Entropy	Reusable pseudonym and swapping is not accountable	Simulation
Pan [86]	2013	Trigger based on number of neighbouring vehicles	Cooperative pseudonym scheme	Anonymity set	Inefficient in sparse network and number of updates regulation	Analysis, Simulation
Ying [72]	2015	Dynamic Mix Zone	Candidate Location List which implicitly has defined timeslot for change	Anonymity Set Size and Success Rate	Sparse network	Analysis, Simulation
Boualouache [87]	2017	TAPACS	Traffic awareness with radio silence	Entropy of Anonymity Set	Need congested area for change	Analysis, Simulation

has also proposed an idea of swapping the pseudonyms among the vehicles. But as the scheme is suitable for V2V communication and not depending on the infrastructure, this swapping may not be reported to the concerned authority for accountability purposes. The simulations of SUMO, OMNET++, and INET provide the analysis in two different urban and freeway scenarios. The results show that the sufficient level of privacy is achievable with this scheme in dense and sparse scenarios based on entropy, and the traffic overhead caused is insignificantly low.

Pan [86] proposed another trigger-based mechanism for pseudonym change, which

depends on the number of neighbouring vehicles. As the cooperation of the vehicles introduces higher anonymity, the author presented the idea of using the nearby vehicles' density as a trigger. Due to the reason that the synchronized change improves location privacy, the proposed scheme allows implicit synchronization on V2V communication. It is easy to implement, but it does not perform well in sparse networks. The author provided a comparison of the not cooperating vehicular network to the cooperative network in one and multi-lane. The results of the MATLAB simulations show that with the anonymity set increment, the unlinkability increases increases the location privacy. On the other hand, the scheme is deprived of the mechanism which regulates the number of required updates of a pseudonym, which may sometimes cause an overhead.

Ying [72] introduced a flexible approach that eliminates the problem of fixed mix zones. It is called Pseudonym Changes based on Candidate-location-list (PCC). This strategy uses the dynamic mix zones along with the candidate location list for changing the pseudonyms. The list has various identifiers, and one of them tells about the slot when the pseudonym is to be changed. As the vehicles maintain this location list, it changes pseudonyms at the same time due to this identifier. It works well in dense networks, but it may not be effective in light traffic as the adversary may identify the vehicle after its updating due to fewer vehicles around and position prediction. The author provided the beacon format for the candidate location list, algorithm, and scheme analysis. The size of the anonymity set and the success rate is used for the simulation comparison of the strategy CPN [86], DMLP [71], and PCC [72].

Boualouache [87] has provided the concept of traffic awareness, which is used along with radio silence. The scheme ensures safety and balances privacy and safety. The scheme proposed is closely related to SLOW [84] as it monitors the traffic and chooses a suitable place to change a pseudonym. The author suggests the congestion is the best opportunity for updating. In real-time, it may cause a problem for the vehicles which do not pass through a congested area and would not be able to change the pseudonym.

2.3.6 Group Based Mix Context

There is a set of PCSs in which the vehicles form a group on an ad hoc basis and then carry out the pseudonym change. Table 2.6 summarizes three such group-based mix context schemes. The common problem with these schemes is that it is challenging to manage a group in a vehicular network environment.

Table 2.6: Group Based Mix Context Schemes

Author [ref]	**Year**	**Key concept**	**Changing Strategy**	**Privacy metric**	**Problems**	**Evaluation method**
Sampigethaya [45, 46]	2005	CARAVAN/ AMOEBA	Group based, group manager is proxy for anonymous access	Anonymity Set Size	Group management is difficult in VANET	Analysis, Simulation
Wasef [88]	2010	Random Encryption Periods (REP)	PKI used with probabilistic symmetric key distribution	Anonymity Set Size	Group communication in VANET is difficult	Analysis, Simulation
Weerasinghe [89]	2011	Group based synchronization	Signal strength changes which change temporal and spatial properties	Anonymity Set Size, Entropy of Anonymity Set Size, and Tracking Probability	Group communication in VANET is difficult	Simulation

CARAVAN/ AMOEBA is the approach for the location privacy proposed by Sampigethaya [45] in 2005. The group of vehicles is formed based on broadcast listening. If vehicles can listen to each other's broadcasts, they will form a group with a group manager. The group manager is a proxy for anonymous access. It represents the entire group and communicates on behalf of its group as the group's vehicles are relative with respect to the velocity of the nearby vehicles. The analytical and simulation results show that average anonymity in the freeway model increases with an increase in anonymity set size [46]. The tracking time is reduced significantly with an increase in the number of vehicles as more number of vehicles increase the entropy. The author has presented a detailed mathematical analysis of the scheme and step by step explanations of the simulation, which would help understand the

scheme and its implementation. The only possible drawback of this scheme is the group formation and silence of the group members. The group management in the vehicular environment is challenging, and the silence risks safety even though it is for a short duration.

Wasef [88] has introduced Random Encryption Periods for enhancing location privacy. The strategy uses Public Key Infrastructure along with probabilistic symmetric key distribution. The symmetric key is the group based secret key, which is shared among the neighbouring vehicles. The scheme promises reliability, efficiency, and scalability. The author has provided a detailed analysis of the REP and supported with the simulation on MATLAB by using the evaluation metric as anonymity set size. The problem with this scheme arises with group communication, which is challenging to manage in vehicular environments.

Weerasinghe [89] introduced the concept of a group based synchronized pseudonym changing the protocol for the first time in 2011. The advantage of the scheme is that it takes a more extensive anonymity set and higher entropy during the pseudonym change. It is not only safety compliant but also prevents continuous tracking. The group manager decides the time to change the pseudonym, and other group members are informed, and after changing the pseudonym, the group is dissolved. Also, the signal strength is changed as the pseudonym is changed. Weerasinghe added an interesting idea of using a group identifier for a specific time between two of the pseudonyms. It changes temporal and spatial properties as it adds confusion and complicate the process for the tracking. The metrics used to evaluate the scheme were anonymity set, the entropy of anonymity set, and tracking probability. The simulation is performed on NS2 with Manhattan and the urban model.

2.4 Comparison of Pseudonym Changing Schemes

There are several schemes proposed for changing the pseudonym, but each scheme has certain advantages and disadvantages. Some of them are applicable only in urban areas, and some work well on freeways. Various mechanisms are used in the proposed

schemes, which affect not only the performance and overhead but also the safety of the vehicles. In this section, we discuss the different entities in the pseudonym change and their benefits and effects with respect to location privacy.

Radio silence is strongly emphasized as it disrupts the continuous, frequent broadcasts, which result in the untraceability of the vehicles if this silence period is used for the pseudonym change and status change. The radio silence is effective because the attacker can not use the information for linking two or more pseudonyms of the vehicles; thus, it gives high location privacy. The concept of radio silence was first introduced in 2006 by Li [74]and has been used in several other schemes in different manner [43,67,70,71,74,82,84]. This privacy-preserving technique of silence may have benefits. Still, it cannot avoid the risk posed by silence to the safety-related applications. The vehicular network aims to provide safety to the driver and passengers, which must not be compromised. Therefore, there is a need for a balance between privacy and safety.

Another significant factor which also disrupts the continuous eavesdropping and tracking is the encryption. Encryption is not proposed for the entire communication of the vehicular network. It is limited to certain zones or areas where all the vehicles are high and feasible to change the pseudonyms. The encryption in such areas provides a security layer over vehicular communication, which cannot be listened to by the attacker for some time. This idea of encryption is scalable, feasible to V2V communication and can eliminate the use of infrastructure if required. The only threat posed by encryption is an internal adversary. When the internal adversary helps a global adversary, the tracking can be possible with a high success rate. The schemes use encryption along with radio silence or in the mix zone [22, 66, 73, 79].

Some schemes propose the exchange of the pseudonyms among the vehicles, which helps in increasing the confusion for the adversary. These schemes do not give a suitable mechanism to report these exchanges to the authorities. There is a need to have the pseudonym to VID mapping for the revocation purpose in cases of security attack. Thus, using the swapping technique significantly impact the overall working of the pseudonym authentication. Accountability is mandatory, and there is a need

Table 2.7: Comparison among Pseudonym Changing Strategies

Scheme	**Category**	**Radio Silence**	**Infra-structure**	**Encryp-tion**	**Safety effect**	**Overhead**	**Syntactic Preven-tion**	**Semantic Preven-tion**	**Exchange**
CMIX	Mix Zone	No	Yes	Yes	No	Yes	+	+	No
Social-Spots	Mix Zone	No	Yes	No	No	No	+ + +	No	No
S2SI	Mix Zone	Yes	Yes	No	Yes	No	+ + +	+ +	Yes
VLPZ	Mix Zone	Yes	Yes	No	No	No	+ + +	+ +	No
DMLP	Mix Zone	No	Yes	Yes	No	Yes	+	+	No
PMZ	Mix Zone	No	Yes	Yes	No	No	+ +	No	No
Extended CMIX	Mix Zone	No	Yes	Yes	No	No	+ +	+	No
Swing-Swap	Mix Context	No	No	No	No	No	+ +	+ +	Yes
Mix Context	Mix Context	No	No	No	No	No	+ +	+ +	No
CARVAN/ AMOEBA	Mix Context	Yes	No	No	Yes	No	+ +	+ +	No
Liao	Mix Context	No	No	No	No	Possible	+ + +	+ +	No
DLP	Mix Context	No	No	No	No	No	+ +	No	No
SLOW	Mix Context	Yes	No	No	Yes	No	+ +	+ +	No
REP	Mix Context	No	No	Yes	No	Yes	+	+	No
Weerasin-ghe	Mix Context	No	No	No	No	Possible	+ +	+ +	No
CPN	Mix Context	No	No	No	No	No	+ +	No	No
SlotSwap	Mix Context	No	No	No	No	Yes	+ + + +	No	Yes
PCC	Mix Context	No	No	No	No	Yes	+ +	No	No
SPCP	Mix Context	No	No	No	No	Yes	+ +	No	No
TAPCS	Mix Context	Yes	No	No	No	No	+ +	+ +	No

to have swapping techniques with accountability. This may introduce a higher level of location privacy.

In the vehicular environment, group management is critical due to the highly dynamic network. The events of entering and exiting are fast and large in number, which complicates the group management processes. Therefore, it may not be a good idea to introduce grouping for the pseudonym change schemes as it then has to deal with different other problems regarding the group in the network performance. As many of the schemes are concerned with the anonymity set size, which is the number of neighbouring vehicles, the schemes apply to dense scenarios like urban and busy highways. There are no schemes that can protect the vehicles in light traffic areas, mainly, because the adversary can predict the next possible location of the vehicle and can relate the pseudonyms. Thus, there is a lack of location privacy in sparse networks. The trigger-based techniques are excellent because it enables implicit Trigger for a change of pseudonym. These are more effective as the adversary is not aware when vehicles are changing pseudonyms, and it can only see the change, and it is not easy to correlate after an implicit trigger. Another advantage is that even if the adversary is monitoring the information, it does not know when exactly and where the change is going to happen. Therefore, the prediction of such events is challenging, with no critical related information. These allow more flexibility and scalability to the pseudonym changing schemes. The possible drawback associated with this technique is that if there are not enough vehicles, an adversary may trace the vehicle. Therefore, the trigger technique is bound to the anonymity set size or the number of neighbouring vehicles.

The mixed context schemes are based on the cooperative behaviour of the vehicles, which is essential for V2V communication. Therefore, in such cases, if some of the vehicles refuse to cooperate, others suffer as they cannot change their pseudonyms. It is possible when there is a limit to the pseudonym change as the frequency of the change must be bounded; otherwise, the vehicle either runs out of the pseudonyms or may not be able to contact certificate authorities to obtain more of the pseudonyms. Thus, non-cooperative behaviour harms the mixed context schemes.

While comparing the schemes, it can be challenging to understand the effectiveness as different schemes use different privacy metrics. When the evaluation is carried out based on separate factors, it is a challenging task to analyze. There is no set of standardized evaluation privacy metrics that resolve this problem, so different schemes can be examined under a consistent set of metrics. Similarly, the schemes are analyzed in diverse simulation platforms with various mobility and adversary models, which cause the problem of understanding, evaluating, comparing and analyzing the underlying idea and algorithm.

2.5 Conclusion

In this chapter, we pointed out that *pseudonym change* is part of the pseudonym life-cycle, and the location privacy is dependent on how, when and where the pseudonyms are changed. Next, we explained the privacy attacks and the types of adversary models. We reviewed the current state of art pseudonym changing schemes and provided a taxonomy of these schemes. Next, we compared these schemes based on the factors which play a vital role in introducing or preventing the privacy risk.

Chapter 3

An Equitable Privacy Assessment(EPA) Framework

3.1 Need of EPA Framework

Many different PCSs have been proposed in recent years to determine under which situations and how often a vehicle, or group of vehicles, should change its pseudonyms. These schemes vary from one another in terms of their approaches and consider different privacy metrics, mobility models, adversary models and evaluation methods. The proposed schemes use different assumptions and limitations as well as various parameters and network models for simulations, making it very challenging to compare and evaluate these schemes consistently, under the same conditions. To carry out a fair and consistent evaluation of VANET location PCSs, it is necessary to have a systematic approach in which all the aspects mentioned above are taken into consideration. Currently, to the best of our knowledge, there is no suitable framework that allows comparison of the different schemes under the same mobility models and adversary models, using the same set of privacy metrics. Therefore, there is a need for a comprehensive simulation framework, where the feasibility and effectiveness of one scheme can be tested against others under the same conditions and vehicular environment. This will help identify the strengths and weaknesses of a particular scheme, under different conditions and determine the trade-offs that may be necessary for different contexts. In this chapter, we propose an equitable privacy assessment (EPA) framework for evaluating different pseudonym changing schemes. We first identify the various components needed to create such a framework. We discuss our implementation of these building blocks, and finally, we use the proposed EPA framework

to evaluate four existing PCSs.

Building Blocks of EPA Framework

Mobility Models: The mobility model describes the movement of vehicles in a vehicular network and is determined by two main factors - i) the road network topology and ii) the vehicular traffic pattern. The road topology includes not only the geographical locations and distances of road segments but additional features such as traffic lights, stop signs, speed limits etc. The traffic pattern is determined by the number of vehicles, their average trip times, routes and speeds. Both of these factors can have a significant impact on the performance of a PCS. The behaviour of the PCS heavily depends on the traffic models. The level of achievable privacy varies with the changing road network and the traffic situation.

Adversary Models: The adversary model describes the capabilities of the attacker. For example, its geographical range (global or local), type of attack (active or passive), amount of available equipment, tracking algorithms used, and awareness of traffic patterns and PCSs used to place attacking stations etc.

Privacy Metrics: The privacy metrics specify the criteria used to evaluate a PCS. Many different metrics that have been used in the literature and selecting a suitable metric is important as some PCSs perform well for one metric and may not perform so well when using a different one. So, to have a fair comparison, it is important to use a range of different metrics, rather than a single one.

3.2 Adversary model

In Vehicle to Vehicle (V2V) communication, the periodic safety messages sent in plain text can be captured using DSRC enabled devices. This information can be used in various ways, depending on the objectives and capabilities of the attacker. Effective PCSs should consider an accurate and realistic adversary model. The adversary can be modelled based on different characteristics, such as the attack methodology,

capabilities of the attacker and its geographical reach. In this section, we will consider some important parameters that are typically used for adversary modelling.

In Chapter 2, we discussed that adversaries could be classified as active vs passive or global vs local. The *active* adversary aims to alter the information in the message or inject new messages in the network; the objective of the *passive* adversary, on the other hand, is to gain information to track and profile the drivers, by eavesdropping on messages. The global adversary can eavesdrop all the messages from all vehicles at all times, without leaving any blind spot. In contrast, the local adversary has limitations in terms of listening range and duration. As mentioned earlier, the global adversary scenario is unlikely due to the prohibitive cost. However, many privacy evaluation schemes adopt this model, as it is the strongest adversary and can be used to model the "worst-case" situation. In the remainder of this thesis, we will be using the *local passive adversary* model for privacy evaluation.

3.2.1 Tracking Approach

All the listening stations, placed at different locations, collect safety messages on the channel and send it to a central vehicle tracker. The tracker uses the spatial-temporal information for the prediction. Generally, multi-target tracking is used for tracking and surveillance purposes. The idea is to sample the target positions periodically and estimate the track of the goal using the measurement sequence. The association of the position measurements reveal the track of the target. One such tracking algorithm is Multi- Hypothesis Tracking [90], which relies on Kalman Filter [91]. In our work, we have used a multi-target tracking algorithm, Nearest Neighbour Probabilistic Data Association (NNPDA) [92], to track vehicles with anonymous message collection. If a vehicle with the same pseudonym appears in the listening range of another eavesdropping station, the vehicle can directly correlate, thus, successfully track without spatial-temporal inference. On the other hand, if the pseudonym is changed, then the vehicle tracker predicts the target vehicle based on the location and time information. It may accurately identify the target vehicle (successful tracking) or may observe it as a new vehicle in the area as the vehicle is not identified with any of the previous

tracked vehicles (unsuccessful tracking).

3.2.2 Factors affecting tracking ability

For successful tracking, the adversary needs to collect the streaming beacons almost continuously. The link between the old and new pseudonyms can be lost with a disruption, which reduces the chances of accurately correlating vehicle pseudonyms. For the local passive adversary considered in this thesis, several essential factors can affect vehicle tracking, as identified below.

- The number of vehicles changing pseudonyms simultaneously: A vehicle changing pseudonym alone is relatively easy to recognize. Therefore, PCSs, where multiple vehicles cooperate to change pseudonyms together, tend to perform better.

- Knowledge of PCS and traffic analysis: If the PCS is known to the attacker, the attacker can exploit this knowledge to place the listening stations strategically. Also, stations can be placed in high-traffic areas, if traffic patterns are known, to eavesdrop on more vehicles. Certain PCSs lead to the repetition of pseudonyms, which can also be exploited by the adversary.

- Eavesdropping duration: The longer the period over which BSMs are collected, the more information is available to the attacker. Hence, tracking success increases with the extended duration of eavesdropping. The longer tracking allows the attacker to gain knowledge of the maximum possible number of pseudonyms, visited places and chosen routes. If a PCS with a high frequency of pseudonym change leads to the repetition of the pseudonyms, then the attacker can identify the vehicle with minimum effort.

- Communication range of listening stations: The farther the vehicles are from the attacking stations, the higher the chances of packet loss due to obstacle shadowing. The communication range of a typical RSU varies from 100 to 1000m. A communication range of 300m is considered reliable, with having a relatively

low packet drop ratio. On the other hand, a more extended communication range allows eavesdropping of more number of vehicles. Therefore, the attacker will select a listening radius, which drops very few packets, while still covering a sufficiently large area.

- number of listening stations: An increased number of listening stations results in complete coverage of the area of interest by reducing "gaps" where vehicles are not monitored. Therefore, reducing the number of stations or their listening range or both results in fewer BSM messages reaching the eavesdropping stations and reduces successful vehicle tracking. Preliminary traffic analysis can help an attacker, with a limited number of attacking equipment, to optimize the selection of eavesdropping locations with respect to an available number of equipment.

- Equipment placement Due to the limitations on the number and communication range of the eavesdropping equipment, the local adversary needs to place these resources in a way that maximizes its attacking capabilities. Most PCSs reported in the literature use a simple *random* placement of listening equipment. However, the strategic placement of a limited number of eavesdroppers can improve successful vehicle tracking in the presence of a local adversary. Therefore, a realistic approach to evaluating the performance of a PCS should incorporate *intelligent* adversary placement strategies.

3.3 Privacy Metrics

The evaluation of privacy for VANET is a challenging task as it demands the quantification of the context-based scenarios. Various metrics have been proposed for privacy assessment, and these can be broadly classified into two categories based on their perspective - the user/vehicle who seeks privacy or the adversary who attempts to track the vehicle. We have selected the following two metrics (one from each group) to evaluate the different PCS.

- entropy of the anonymity set, based on the vehicle's perspective
- tracking success rate (TSR), based on the adversary's perspective

3.3.1 Metrics Based on Vehicle's Perspective

Anonymity Set

According to Pfitzmann [35],"To enable anonymity of a subject, there always has to be an appropriate set of subjects with potentially the same attributes. This leads to the first kind of a definition: Anonymity of a subject means that the subject is not identifiable within a set of subjects, the anonymity set. The anonymity set is the set of all possible subjects. With respect to actors, the anonymity set consists of the subjects who might cause an action. With respect to access, the anonymity set consists of the subjects which might be acted upon. The anonymity of a set of subjects within a (potentially larger) anonymity set means that all these individual subjects are not identifiable within this anonymity set."

The Anonymity Set, AS, contains the number of vehicles among which the target vehicle is indistinguishable from other vehicles. In other words, AS consists of all the vehicles in the network scenario that could potentially be the target vehicle v. Typically, this includes a set of vehicles that are changing their pseudonyms at the same time. As the number of vehicles in this set increases, it is expected that it will be harder for the adversary to accurately identify the target vehicle. This metric is straightforward, can be easily calculated and is often used by region or infrastructure bases PCSs, where vehicles which are in the same "Mix-Zone" change their pseudonyms simultaneously [93]. On the other hand, AS is not an appropriate metric for Mix-Context PCSs, which do not depend on a geographical area or infrastructure unit but allows vehicles to change the identifiers independently. In this case, all vehicles that are changing the identifiers simultaneously, in the entire network, are considered to belong to the Anonymity Set irrespective of their distance from the target vehicle. The main drawback of using AS as a metric is that all vehicles in the AS [94] are considered to be equally likely to be the target vehicle. This is not

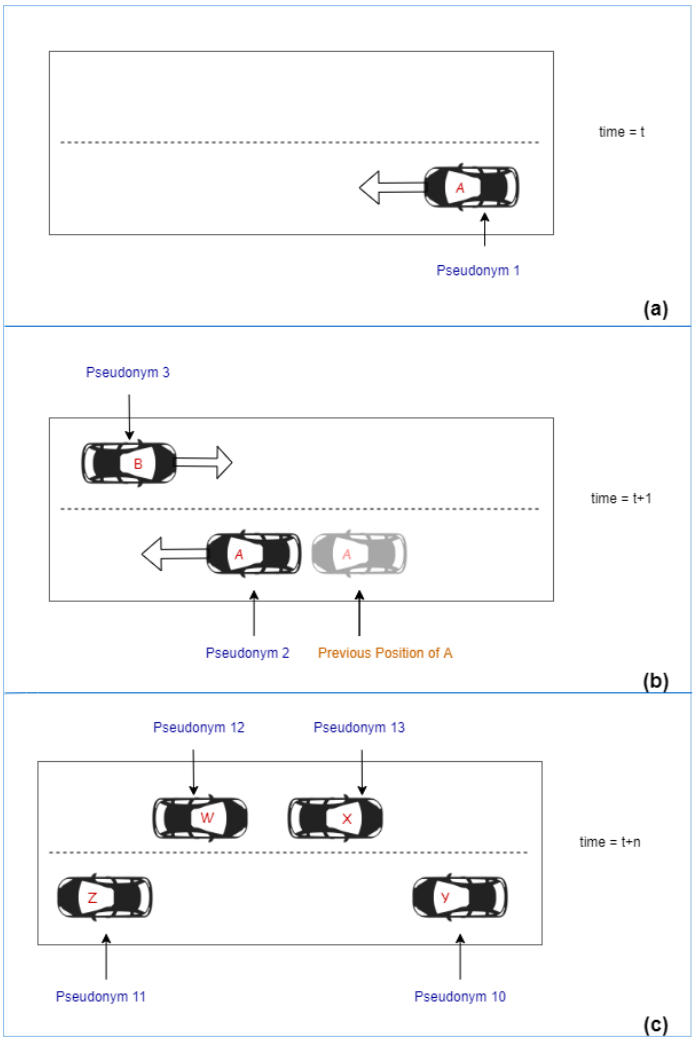


Figure 3.1: Example scenario to demonstrate Anonymity Set Size and Entropy of Anonymity Set Size

a reasonable assumption if two vehicles that are far away from each other happen to change their pseudonyms simultaneously. A vehicle that is far away but changing at the same time is highly unlikely to be the target vehicle v. In other words, AS evaluates the anonymity based only on the *number* of vehicles and does not use additional relevant information such as location, speed and direction.

Entropy of Anonymity Set Size

A more useful metric is the *entropy* of the anonymity set, which also considers the likelihood of a vehicle to be the target vehicle, and is based on the concept of entropy

of random variables and processes related developed by Claude Shannon [95].

The Entropy $H(v)$ of Anonymity Set for identifying a target vehicle $v \in AS$ is calculated using Eqn (1),

$$H(v) = -\sum_{i=1}^{|AS|} p_i * log_2\ p_i \tag{1}$$

where p_i is the probability of node i to be the target vehicle $v, \forall i \in |AS|$. Note that adversary observes the pseudonyms, therefore, a node i is identified using the pseudonym.

In the example of Fig. 3.1(a), the vehicle A is the only vehicle in the scenario and the adversary notice pseudonym PN_1. Here, i is the node as observed by an adversary, which is (pseudonym) 1 and p_i is the probability of 1 to be target vehicle A because in this case, $|AS| = 1$, therefore the entropy will be zero. This indicates that the adversary is certain that i is the identifier of A.

In Fig .3.1(b), we consider two vehicles, A and B, and the adversary observe new pseudonyms PN_A and PN_B. We assume PN_A and PN_B are associated with vehicles A and B, respectively. However, this is unknown to the adversary. A weak adversary would consider that all the vehicles in AS are equally likely to be the target vehicle irrespective of the distance, heading and other parameters. This means p_i= 0.5 for both vehicles and $H(v_A) = 1$. However, an intelligent adversary considers road network constraints and the vehicle's context, including location information. We consider the following example to demonstrate this scenario. With the knowledge of the previous position of A, the adversary can determine the likelihood of PN_A being the pseudonym of A is much higher (say 95%) than the chance of PN_B being the pseudonym of A (say 5%). Then $H(v_A)$, calculated using Eqn (1), will be approximately 0.28. This is a significant difference in the measurement of the level of privacy from the user's perspective.

In Fig. 3.1(c), we consider four vehicles, W, X, Y and Z, and calculate the entropy for vehicle W. After a simultaneous pseudonym change, let PN_W, PN_X, PN_Y and PN_Z be the new pseudonyms associated with W, X, Y, Z respectively (which is unknown to the adversary). For a weak adversary, all four pseudonyms

are equally likely to belong to the target vehicle W. Therefore, p_i is 0.25 for each pseudonym, resulting in $H(v_W) = 2$. On the other hand, a strong adversary observes and distributes the probability based on the heading and speed, in Fig. 3.1(c), W and X, are heading in the same direction, and W is right behind vehicle X. Taking this into consideration the adversary calculates the probability distribution of PN_W, PN_X, PN_Y and PN_Z being the new pseudonym of W, as p_i=0.90, 0.70, 0.20, 0, which results in $H(v_W)$= 0.53. From this example, we see that Entropy of Anonymity Set provides a more realistic measure when an intelligent adversary is considered, and we have used this metric in our simulations.

3.3.2 Metrics Based on Adversary's Perspective

In the literature, the proposed PCSs are evaluated using Success Rate, which is the rate of successful tracking events defined based on various conditions of the adversary model and proposed pseudonym changing schemes. Generally, the success rate is the probability that the estimated vehicle corresponds to the target vehicle based on the information collected from the collected safety messages. In [63], the adversary is designed according to the mix zone. Therefore, it computes the probability p for an existing event based on its entry and exit port.

Tracking Success Rate (TSR) and Global Tracking Success Rate (GTSR)

We define two metrics the *Tracking Success Rate* (TSR) and *Global Tracking Success Rate* (GTSR) to measure how well vehicles can be tracked while using various PCSs. These metrics are from the adversary's point of view, so a higher value of TSR or GTSR is better for the adversary and could point to a potential weakness in the PCS. We use the following notation to define our metrics:

- V: Set of all vehicles in the simulation
- N_v: Total number of vehicles in the simulation, i.e. $N_v = |V|$.
- N_a: Total number of vehicles that come within the listening range of at least

one attacking station. We note that for a global adversary $N_a == N_v$, while for a local adversary $N_a \leq N_v$

- PN_v: Set of distinct pseudonyms used by vehicle $v \in V$ over a complete trip from source to destination.
- c_v: Number of pseudonyms changes carried out by vehicle $v \in V$ over a complete trip from source to destination.
- $PN_{v,i}$: Specific pseudonym in use by vehicle $v \in V$ after the ith pseudonym change $1 \leq i \leq c_v$. $PN_{v,0}$ corresponds to the initial pseudonym used by vehicle v. We note that if a vehicle v does not repeat any pseudonyms over its entire trip, then $|PN_v| = c_v + 1$; however if pseudonyms are repeated then $|PN_v| \leq c_v$.

For a vehicle $v \in V$ undergoing a pseudonym change from $PN_{v,i}$ to $PN_{v,i+1}$, we consider the pseudonym change event to be tracked *successfully* if both the old and new pseudonyms are associated with the same vehicle by the adversary. On the other hand, an *unsuccessful* tracking event for vehicle v occurs if i) two pseudonyms used by vehicle v are not recognized as belonging to the same vehicle by the adversary or ii) a pseudonym belonging to a different vehicle is linked to vehicle v by the adversary.

We set $s_v = 1$ if a vehicle v is successfully tracked over its *entire* trip, i.e. if following conditions are both satisfied.

- There is a total of c_v *successful* tracking events associated with v and
- There are no *unsuccessful* tracking events associated with v.

Based on the above definitions, we calculate the overall tracking success rate for a simulation run as

$$TSR = \frac{\sum_{v \in N_a} s_v}{N_a} * 100 \tag{2}$$

Similarly, we calculate the overall global tracking success rate for a simulation run as

$$GTSR = \frac{\sum_{v \in N_a} s_v}{N_v} * 100 \tag{3}$$

We note that the impact of the intelligent placement strategies is expected to be reflected in terms of higher GTSR values (but not necessarily higher TSR) when using such schemes. This is because when listening stations are in areas with low vehicle density, it may be easier to track the limited number of vehicles in its range since fewer vehicles cause less confusion; however, overall, only a small percentage of vehicles are being eavesdropped.

3.4 Simulation Setup

The simulation environment needed to evaluate the different pseudonym management techniques (PMTs) consists of three main components:

- A network simulator
- A road traffic simulator (with the ability to communicate with the network simulator)
- A privacy evaluation module

In our work we have used the following existing tools for each component: i) OMNET++ [96], which is a discrete event simulator, for the network simulator, ii) Simulation of Urban MO-bility (SUMO) [97] as the road traffic simulator and iii) PREXT [98] for privacy evaluation. Fig. 3.2 shows a block diagram of our framework, and in this section, we will discuss each component in more detail.

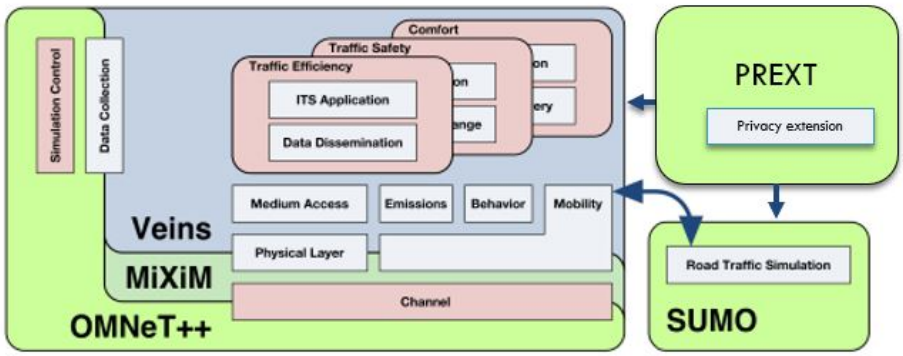


Figure 3.2: Vehicular Simulation Framework

3.4.1 Network Simulator

The communication model has the following four layers: Application layer, Privacy layer, Transport and Network layer, and Physical layer. For BSM, the application layer sends the packet to the privacy layer, and at this layer, the pseudonym is assigned to the packet. The pseudonym could be the same as in the previous BSM transmission or a new one. If a pseudonym change event is triggered based on the PCS parameters, it is generated at the privacy layer and appended to the outgoing BSM. When a packet is received, the receiver gets the safety message along with the pseudonym. Each vehicle is set to emit beacon with a frequency of 10 Hz, and the wireless communication is based on the IEEE 802.11p (DSRC) protocol. Several factors influence the quality of wireless communication, such as interference and channel fading. The BSM transmission may be affected by the signal shadowing effect in urban areas due to buildings and other vehicles on the road which block radio propagation. We have used the simple obstacle shadowing model [99] to represent interference in the communication channel due to buildings and other entities. This model assumes that there is a minimum effect of the obstacle shadowing caused by the buildings and infrastructures, allowing the eavesdropper to receive and track more messages.

3.4.2 Road Traffic Simulator

We considered two types of road topologies - i) urban and ii) highway. The urban setting has complex road topology, with many intersections and possible routes between two points compared to the highway scenario. For the highway scenario, we consider a single road segment with different entry and exit points. So, vehicle routes are more predictable in highway scenarios, as the vehicles do not have many options to change the trajectory except at an exit point. To obtain a realistic vehicle movement, we have used random trip generation for urban traffic, which initializes the vehicles of different origin/destination pairs and assigns routes for each trip. The movement of vehicles can be further fine-tuned based on various properties such as traffic lights

and high congestion areas. To connect network simulator and road traffic simulator, we use Veins [100], which couples both OMNET++ and SUMO bidirectionally. This allows direct control of the VANET communication not only on traffic levels but also on the network level.

3.4.3 Privacy Evaluation

PREXT [98] provides a unified framework for the simulation of the PCSs in vehicular networks. It contains the attacking modules that passively listen to all the safety messages sent by all the active vehicles in the network. The listening stations placed at different locations collect and send messages to a central vehicle tracker, where the attacker tries to link old and new pseudonyms used by the same vehicle. The adversary cannot receive all the messages from the vehicles, as each eavesdropping station only covers a limited area. The tracker also has the capability of estimating vehicle locations based on the spatial-temporal information, including speed, acceleration, heading etc. This allows the attacker to link two pseudonyms associated with the same vehicle potentially. However, this correlation is not always successful, and the adversary may incorrectly link the changed pseudonym to another vehicle than the target vehicle.

3.4.4 Observed PCSs

We have selected four of the leading pseudonym changing schemes for the analysis and comparison of privacy. These PCSs are different from each other and do not follow the same techniques for pseudonym change. There are many other proposed PCSs in the literature, and most of the schemes use the radio silence for pseudonym change. The use of radio silence in a PCS refers to the property that the vehicles do not broadcast the Basic Safety Message for a certain period before changing their pseudonyms. However, safety applications rely on a continuous stream of BSMs to alert the driver. If the radio silence is longer than the beacon frequency, then it directly impacts safety. We considered the PCSs, which either do not have radio silence or whose radio silence

period is less than the beacon frequency. We selected a Periodical scheme because it is one of the schemes with constant triggers, and also it is part of the proposed standard. To observe the impact of radio silence, we observed the SLOW scheme, which is also a User-oriented scheme. Cooperative is another user-oriented scheme that relies on neighbouring vehicles, and CAPS is the context-aware scheme that also uses radio silence. For the investigation of diverse schemes, we considered a range of different approaches such as radio silence, user-centric, cooperative and context-based. This allows examining the strengths and weaknesses of each scheme when tested with the same simulation environment.

Periodic Scheme

The periodical PCS, introduced by Brecht et. al [37], has a static time-based trigger and is proposed as an element of the emerging standards by USDOT. The vehicle changes pseudonyms after every five minutes and selects a new pseudonym from a pool of twenty active pseudonyms, which is valid for one week. The pool size is restricted, so the pseudonyms allocated to a vehicle are not exhausted too quickly. However, this means that if a vehicle is active for more than 100 minutes continuously, it is forced to reuse the pseudonyms, and all pseudonyms in its weekly pool are potentially disclosed to the adversary. Therefore, tracking becomes easier as the adversary does not have to correlate the location and time information when it can directly link the target vehicle using previously recorded pseudonyms. This scheme focuses primarily on the limitation of the pseudonym usage.

Speed-Based Scheme: SLOW

In 2006, Li [79] introduced an approach with a dynamic speed-based trigger, which allows moving vehicles to swap their identifiers. However, there is an accountability problem in this scheme, and in 2009, Buttyan et al. proposed SLOW [84], another speed based PCS, where pseudonym has changed the speed of the vehicle drops below 30 Km/hr. The vehicle uses radio silence for a short period before changing its

pseudonym. Since this is not based on a fixed place or time, it creates increased confusion for the adversary. The radio silence is not desirable for safety applications, but with respect to the attacker, it prevents the continuous information broadcast that reduces the success of the linking attack. One drawback of SLOW is that the vehicle changes its identifier independently, without considering any neighbouring vehicles. It is likely the vehicles in a congested area slow down together. However, the scheme itself does not consider the adjacent vehicles. SLOW is a user-centric and dynamic scheme, in which the vehicle changes the pseudonym without determining the fixed area or periodic change. Therefore, the timing of the pseudonym change is more randomized than the periodic changing scheme.

Density-based: Cooperative

The anonymity of a vehicle is directly related to the number of other vehicles in its neighbourhood. In 2009, Song et al. [83] introduced the first scheme with the vehicular density-based trigger. Later, Pan proposed a cooperative scheme called CPN [86] in which the vehicles require the cooperation of the nearby vehicles to change pseudonyms simultaneously. To increase anonymity, all the neighbouring vehicles should change the pseudonym at the same time. There has to be at least one other vehicle for this change to occur to mislead the tracker. As the number of vehicles in the changing event increases, the level of tracking drops significantly as the level of confusion increases. The main drawback of this scheme is that the pseudonym usage is very high as compared to other schemes. When a vehicle is ready to change its pseudonym, it sends the message for the change and forces nearby vehicles to change at the same time. With the increasing number of neighbouring vehicles triggered by the changing event, the same slot will have a larger anonymity set. This creates confusion for the attacker and is more effective in the dense traffic scenarios where vehicles are closer to each other. The changed pseudonym of the vehicle cannot be resolved or correlated by the attacker.

Context-based: CAPS

Context-based PCSs take into consideration the surrounding situation and change pseudonyms by adapting to the current situation. CAPS [101] is a context-aware scheme, where the vehicle decides when to change the pseudonym based on surrounding conditions and keeps radio silence for a limited time before the change. These schemes introduce a trade-off between quality of service and traceability, due to radio silence. Context-based PCSs can be regarded as more intelligent, and the identifiers' changes are less likely to correlate to the target vehicles. The vehicle indicates the need to change pseudonyms, and as soon as another vehicle agrees to change the pseudonym at the same time, two or more vehicles change the pseudonyms. It increases the confusion for the attacker as two or more neighbouring vehicles are changing the identifiers simultaneously.

3.5 Assessment of Existing Techniques

In this section, we have compared and analyzed four existing pseudonym changing schemes using the following two widely accepted performance metrics: i) Tracking Success Rate (TSR) and ii) Entropy of Anonymity Set. Such comparison is an important step that will ultimately allow a vehicle to choose the most appropriate approach to meet its current needs. Table 3.1 shows the simulation parameters used in evaluating each PCS.

The urban scenario, shown in Fig. 3.3 corresponds to a road network in the city of Berlin. It has 1388 edges, and 576 junctions with a total area of 4x4 Km^2 and the average speed of the vehicle in the urban scenario is 50 Km/hr.

The highway scenario consists of a single straight road segment of 6 Km, with multiple connecting edges, as shown in Fig. 3.4, with average vehicle speed set to 100 Km/hr. The average number of vehicles is 200, with a maximum trip time of 15 minutes per vehicle in both scenarios. This means that each vehicle remains active in the simulation for a maximum of 900 seconds, and the total simulation time is 1200 seconds. Vehicles join the network at different times, which means not all the vehicles

Parameter	Value
Traffic scenarios	Urban(U) and Highway(H)
Max. Speed	50Km/hr (U) and 100Km/hr(H)
Carrier frequency	5.890e9 Hz
OBU receiver sensitivity	-89dBm
Transmission power	20mW
Bitrate	18Mbps
Beaconing rate	10 Hz
Thermal noise	-110dBm
usePropagationDelay	True
Adversary placement	Random
Listening range	300m
Simulation time	1200 sec

Table 3.1: Simulation Parameters

are present at the beginning and the end of the simulation.

3.5.1 Vehicle Density

Fig. 3.5 shows how the TSR varies with vehicle density for different PCSs. For the periodic scheme, the TSR increases for both urban and highway scenario, since more vehicles come in contact with listening stations. Also, more vehicles lead to road congestion and slower speeds, making it more likely that pseudonyms will be repeated. The highest TSR is observed for the periodic scheme in the highway scenario. This is due to longer eavesdropping on the unidirectional traffic. The SLOW scheme has overall less TSR than a periodic scheme, except in the urban scenario with 100 vehicles. Generally, it is difficult for the adversary to track the vehicles with the SLOW scheme as there is radio silence. The tracking also becomes more difficult

Figure 3.3: Simulated Urban Road Scenarios

Figure 3.4: Simulated Highway Road Scenarios

for the SLOW scheme when there is a more significant number of vehicles clustering together as they are slowing down, e.g., 300 vehicles in urban scenarios. The TSR for SLOW is generally lower, for the same number of vehicles, on highways compared to urban roads. This is because, on highways, the vehicles do not slow down as much as in urban scenarios, leading to fewer chances of monitoring pseudonym changes. Therefore, the number of successful tracking events is relatively low in our simulations.

The *cooperative* scheme has moderate TSR in the urban scenario, and TSR decreases with vehicle density, as the increased number of vehicles introduces more confusion for the attacker when more vehicles change their pseudonyms at the same time. CAPS is a context-aware scheme that allows the change of pseudonym with high attacker confusion due to radio silence and large anonymity set. It has relatively lower TSR in the urban scenario with a sudden decline of TSR with high vehicle density. While TSR of highway increases gradually due to the overall increased number

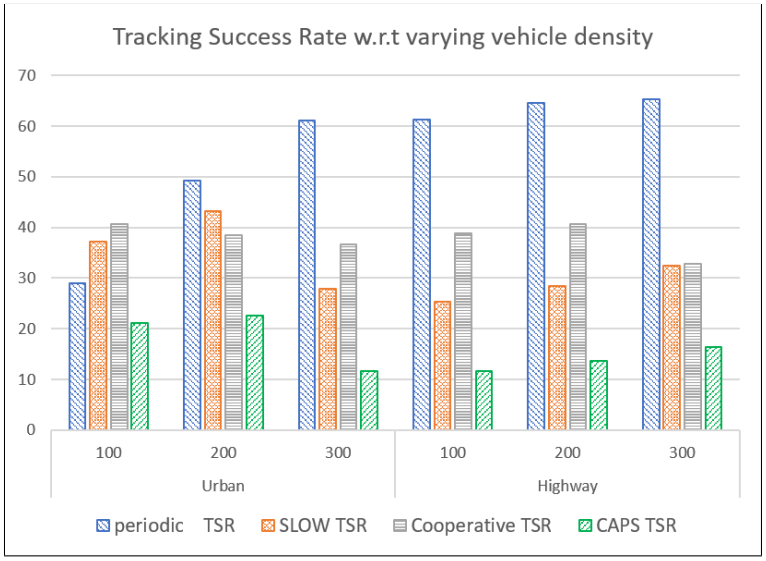


Figure 3.5: Tracking Success Rate with varying vehicle density

of successful tracking events, an increased number of vehicles are in the adversary's range. In general, TSR for CAPS scheme is the lowest of the four schemes; in both the scenarios, due to radio silence, there are more unsuccessful tracking events.

Fig. 3.6 shows how the entropy of the anonymity set AS varies with vehicle density for different PCSs. The entropy remains low for the SLOW scheme because the vehicles approaching the red lights and traffic congestion are the only vehicles that change the pseudonyms. With the knowledge of PCS used, the adversary would not have enough confusion as the vehicles are not surrounded by other slow vehicles due to random trips. Even with increased vehicle density, the entropy remains low. This is because our simulations have used random trips from different entry and exit points. Therefore, the vehicles are spread out over the whole road network. So when a vehicle is slowing in our mobility model, it is usually far from other vehicles, making the correlation of the new and old pseudonyms more predictable. The entropy would grow for the SLOW scheme if more number of vehicles in the mobility model are clustered together and always slow down together. This creates confusion for the attacker due to the radio silence of multiple vehicles within a short geographical distance. For the same reason, the cooperative and CAPS scheme's entropy remains high as the randomness is relatively high in these schemes when a target vehicle is tracked. This

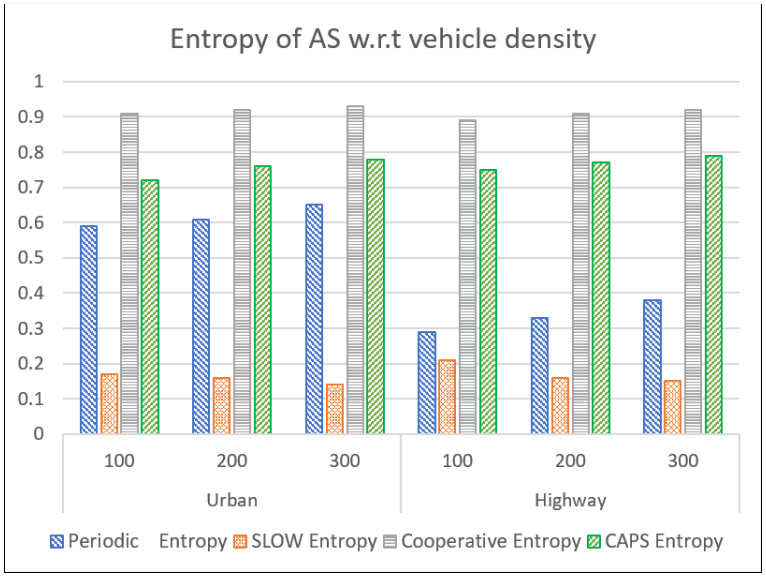


Figure 3.6: Entropy of AS with varying vehicle density

randomness is introduced by the set of vehicles changing pseudonyms together and the radio silence maintained by more than two vehicles in cooperative and CAPS schemes. For the periodic scheme, the anonymity set entropy is high in the urban scenario as the anonymity set consists of the total number of active vehicles that are changing pseudonyms nearly at the same time. The underlying traffic movement plays a role in this case. In our observation, there are sets of vehicles close to each other when they periodically change pseudonyms. In the highway scenario, the entropy is comparatively lower than the urban scenario because there is less randomness on the highway. The urban area consists of a mesh road network where more vehicles are moving in close range of each other, decreasing the predictability as compared to straight highway road where the predictability increases due to fixed speed of the vehicle. Therefore, even though the anonymity set contains all the moving vehicles, the distant vehicles from the target vehicle on the highway are less likely to be the estimated target vehicle.

3.5.2 Trip Time

The trip duration of the vehicle is another important factor in assessing privacy protection. For our simulations based on varying trip time, we considered 15, 30 and

60 minutes of average trip time in both urban and highway scenarios, with vehicle density of 200 and 5 attacking stations. Some trips are shorter, and others are longer than the considered average time. Therefore, the overall simulation time varies in this case. Fig. 3.7 shows how the TSR and entropy of the anonymity set AS vary with trip time for different PCS.

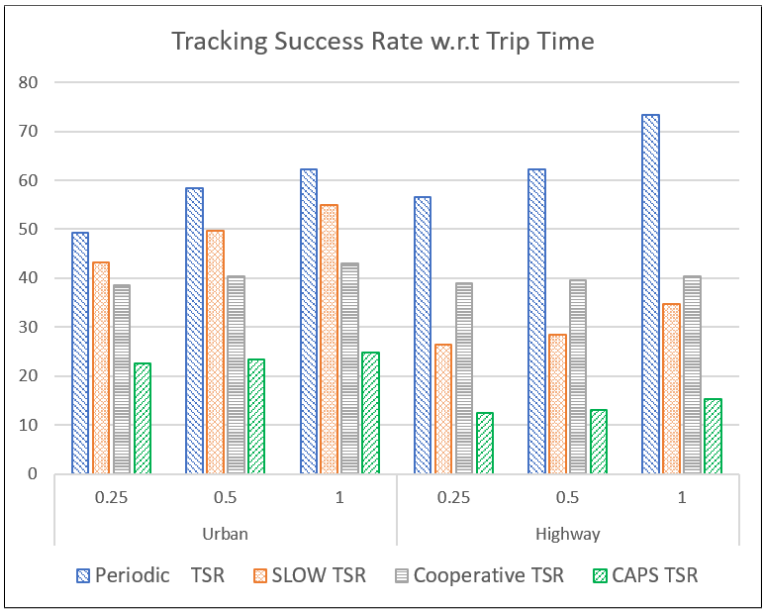


Figure 3.7: Tracking Success Rate with varying trip time

When the PCS allows the repetition of the pseudonyms due to a limited number of temporary identifiers, the attacker can accumulate knowledge of previously used pseudonyms, which increases TSR. In the periodic scheme, a limited number of pseudonyms are allotted to each vehicle to be used over time. The TSR for periodic scheme increases steadily with trip time and is significantly high when the trip time is longer since the likelihood of pseudonym reuse increases with trip duration. The SLOW scheme shows lower TSR compared to the periodic scheme, in both urban and highway scenario. The highways have relatively fewer pseudonym changes as vehicles slow down only due to congestion or after taking the exit. Therefore, the overall number of successful tracking events for SLOW is lower in random highway placement. For both cooperative and CAPS schemes, the trip time seems to have minimal effect on TSR. CAPS scheme results in the lowest TSR, with the cooperative scheme as the

next best case. In Fig. 3.8, we observe the entropy of anonymity set with varying

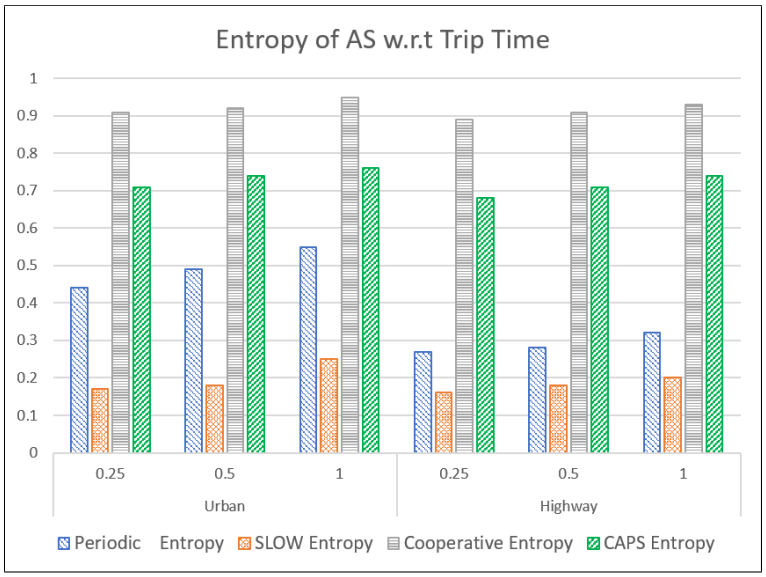


Figure 3.8: Entropy of AS with varying trip time

trip time. The entropy for the periodic case is moderate for the urban scenario but lower for the highway. This results in higher TSR for highways as the duration has no significant impact on the anonymity set size. The entropy remains low for all cases, with very little chance for the SLOW scheme. The cooperative scheme shows very high entropy in all the observed cases, due to the simultaneous change of the identifiers. The entropy for CAPS also remains consistently high, but lower than cooperative for all cases. In the cooperative scheme, the anonymity set includes all the vehicles changing pseudonyms and more vehicles involved than the CAPS scheme. This is why the entropy for cooperative is higher as compared to the CAPS scheme. Interestingly, TSR for the cooperative case is higher than CAPS with high entropy of AS; this is due to the radio silence of CAPS scheme, which introduces additional confusion for the adversary. This shows that more vehicles are suitable for increasing anonymity, which is good from the user's perspective. For the adversary, radio silence is more challenging, decreasing the tracking success rate.

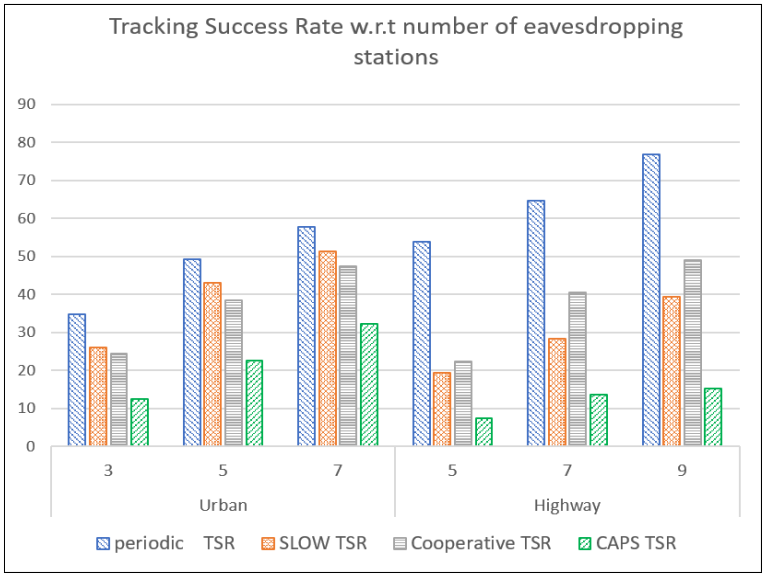


Figure 3.9: Tracking Success Rate with varying eavesdropping stations

3.5.3 Number of Eavesdropping Stations

Fig. 3.9 shows how the TSR of the anonymity set AS varies with the number of eavesdropping stations for different PCS. For these simulations, we considered 3, 5 and 7 eavesdropping stations for urban scenarios and 5, 7 and 9 for highway scenarios, each with each 300m of range. For both urban and highway, we simulated 200 vehicles with 15 minutes of trip time per vehicle.

With more eavesdropping stations, the attacker can expand its listening area and record the pseudonym changes, as vehicles broadcast their safety messages. As expected, the TSR increases consistently for all approaches, as the number of eavesdropping stations increases. As before, the CAPS scheme has the lowest TSR, followed by cooperative and SLOW schemes. The periodic scheme performs the worst in all cases.

The entropy of the anonymity set, in Fig. 3.10 remains high for the cooperative and CAPS scheme, while it is moderate for the periodic scheme and low for SLOW schemes. The context-aware scheme provides the best privacy protection level on the highways with high entropy and the lowest TSR with five attacking stations. The cooperative scheme has moderate TSR with high entropy of AS, which shows that the

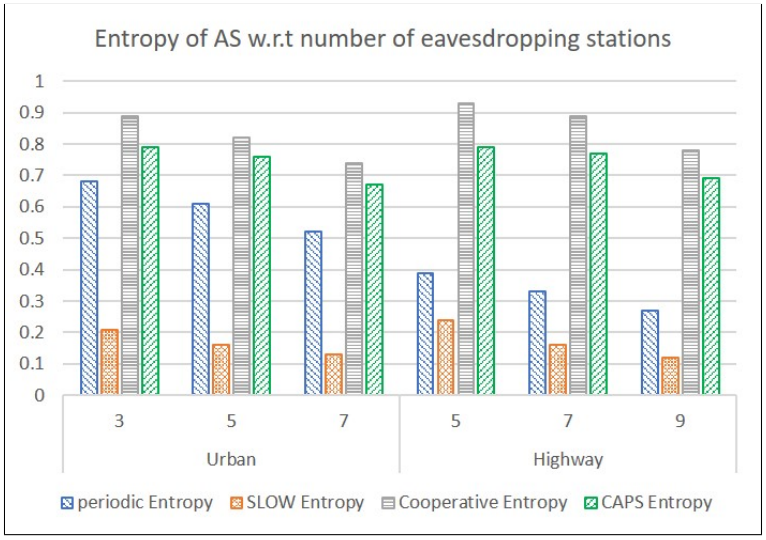


Figure 3.10: Entropy of AS with varying eavesdropping stations

scheme promises the anonymity on the user side. However, the way the pseudonyms are changed, the linkability of new and old pseudonyms becomes evident for the attacker in many cases. The context-aware approach (CAPS) gives a high entropy and low tracking rate. This is due to a reasonable time of radio silence, which provides confusion as well as randomness. In context-aware schemes, vehicles are usually surrounded by other vehicles, which will simultaneously change their identifiers. On the other hand, there is radio silence in SLOW, but the vehicle may be far from other vehicles when changing its pseudonym. This allows the attacker to track it more easily, compared to vehicles using a context-aware scheme.

3.6 Conclusion

In this chapter, we discussed the need for an equitable privacy assessment framework. We identified the building blocks of this framework. We described the adversary model, the tracking approach used for tracking the vehicles and the factors affecting the tracking ability. We explained the privacy metrics from vehicle's and adversary's perspectives. We presented a set of simulators that facilitate privacy evaluation in vehicular networks. Using this simulation setup, we compared and analyzed four existing pseudonym changing schemes using two of the privacy metrics.

Chapter 4

Intelligent Adversary Placements for Privacy Evaluation in VANET

4.1 Introduction

The existing attack modelling in PREXT [98] is the global passive adversary who can eavesdrop all the messages without packet loss. Such an adversary demands an extensive network of the roadside units, which would require either control on the existing infrastructure or deployment of the new equipment. Therefore, it is considered to be very challenging to execute a global passive adversary. On the other hand, local attacks are feasible with less equipment. Therefore, the scope of our observation is the local passive attacking scenarios. For local adversary, we have considered that the attacking stations are placed strategically so that the attacker can take advantage of the dense traffic and frequently chosen routes, which are usually in the center of the city. The limited capabilities of the attacker may affect the urban areas differently than the highways. Also, the local attacks are targeted to the busy areas within the city as the attacker wants to use a minimum number of attacking stations to reduce the overall cost. So we have simulated the local attack with varying number of attacking stations for different pseudonym changing schemes. It reveals the attacking capabilities and the level of privacy protection provided by various schemes. PREXT involves the global attacking module, which passively listens to the safety messages sent by vehicles. We have altered the attacking capabilities in this framework. We have placed the listening stations at the selected observation points based on preliminary traffic analysis. All the listening stations placed at different locations collect messages and send them to a central tracker where the attacker

determines the relation of the old and new pseudonyms used by the same vehicle. The attacker is not able to receive all the messages from the vehicles as one eavesdropping station covers a limited area; hence, when the vehicles are in the range of one of the attacking stations and change the pseudonym, then the attacker can directly correlate the changed pseudonym. The tracker also has the capability of estimating based on the spatial-temporal relation. As the vehicle moves on a road and in a specific direction at a time, the vehicle's speed helps in determining the vehicle's movement in a given time, which allows the determination of the same vehicle, which previously had a pseudonym P1. When it enters the range of the new attacking station, it has a new pseudonym P2. This correlation of the pseudonyms is observable only because of the continuous Basic Safety Messages and the smaller changing frequency of the pseudonyms.

We propose two traffic-aware attacker placement strategies that can be used to select the most advantageous eavesdropping locations for attacking stations intelligently. We show how intelligent attacker placements can affect the performance of different PCS and analyze the conditions under which privacy is most likely to be compromised.

Objectives

- A distance based attacker placement scheme (DBAP)
- A novel speed based attacker placement scheme (SBAP)
- A comprehensive comparative evaluation of different PCSs using the proposed schemes and random attacker placement, for different traffic conditions, using common metrics.

4.2 Intelligent Attacker placement

We consider a *local passive adversary*, with a limited number of eavesdropping stations that have a specified listening range. In this context, the goal of the adversary is

to target the positions with high vehicle density and eavesdrop on the maximum number of vehicles. The placement algorithms use knowledge of long term traffic patterns to help select potential locations for adversary placement. Such information can be easily obtained from public sources to retrieve real-time traffic information using a variety of web applications such as Google Maps, so the algorithms are not dependent on any specialized or proprietary data. The collected traffic information can include the most congested road segments or intersections, time of the day, the usual duration of congestion and length of the road segments with congestion. An adversary accumulates this information over time to understand the underlying traffic patterns in the region, which allows it to make *intelligent* choices when placing the listening stations. Furthermore, prior knowledge of the PCS being used can directly affect the strategic placement of the eavesdropping stations. For example, if the adversary is aware that *Periodic* scheme is being used and pseudonyms are changed every five minutes [37], the distance between stations can be adjusted for continuous linking of the changing pseudonyms.

Most PCSs reported in the literature typically assume a simplistic, random placement of attackers, which may not provide an accurate measure of its performance under more realistic conditions. In this section, we present two new attacker placement strategies - i) *distance based attacker placement* (DBAP) and ii) *speed based attacker placement* (SBAP) for selecting the locations where attacking stations should be placed to increase the chances of successful vehicle tracking. For both approaches, this is accomplished by selecting locations where

1. attacking stations can listen to beacons from many vehicles and

2. pseudonym changes are likely to occur

It is expected that an intelligent adversary can make use of publicly available information to improve its chances of successfully tracking vehicles. Therefore, the various PCSs need to be evaluated for such placement schemes, rather than simple random placement, for a more accurate measure of performance. Both approaches have an initialization step during which parameters such as the number of available

equipment, their communication range and the pseudonym change frequency (used for periodic pseudonym changes) are specified. Long term traffic patterns are also analyzed to guide attacker placement.

4.2.1 Distance Based Attacker Placement

A brief overview of our proposed *distance based attacker placement* (DBAP) algorithm is given below. In this approach, the attacker chooses certain road segments, based on traffic conditions and places attacking stations at specified distances along the selected segments.

Algorithm 1 Distance based attacking placement algorithm

Input: Number of available equipment for tracking the vehicles (n) and PN change frequency (f)

Output: Adversary spacing

1: Based on traffic patterns select
   a. Target destination (T)
   b. a set P of potential starting points for routes, where $|P| = k$ and $p_i \in P$ is the ith starting point.
2: Calculate spacing between adversary positions (d)
3: Calculate lower limit $N_{min} = \sum_{i=1}^{k} \lceil \frac{dist(p_i,T)}{d} \rceil$ for
4: number of adversaries to use.
5: **if** $n < N_{min}$ **then** a. calculate d', where d' is the smallest spacing for which $n \geq \sum_{i=1}^{k} \lceil \frac{dist(p_i,T)}{d'} \rceil$ b. Set d=d'
6: **for** $p_i \in P$ **do**
7: Place adversary equipment with space d along route from p_i to T.

First, we select a suitable target destination T (step 1a), which is likely to be visited by a large number of vehicles. T is typically a high-traffic road for urban scenarios, often near the city center, while it is always taken as the last segment of the highway for highways. Next we identify a set P of k potential starting points (step 1b), where $p_i \in P$ and $1 \leq i \leq k$. The road segments from p_i to T are selected for adversary placement. The goal is to select roads with high traffic so that more vehicles will be exposed to attacking stations. For highways, $k = 1$ and p_1 is the initial

segment of the highway under consideration. In other words, we do not consider the highway on or off-ramps, but rather treat it as a single road segment.

After selecting the routes, we determine the maximum distance (d) between successive attacking stations along the selected routes (step 2) to achieve full coverage along these routes. The value of d can depend on several factors, such as vehicle speeds, the frequency of pseudonym changes and the communication range of the attacking stations. Next, in step 3, we determine the minimum number of attacking stations (N_{min}) needed for covering the routes, based on d. If the number of available stations (n) is higher than N_{min}, then d is set to be the attacker distance. On the other hand, if $n \leq N_{min}$, we calculate an updated attacker spacing d' (step 4-5), where $d' > d$ and then set $d = d'$. It is important to note that increasing the attacker spacing may have a negative impact on the ability to track vehicles. Finally, the stations are placed along each selected route with a distance of d between two adjacent stations (step 6-7).

4.2.2 Speed Based Attacker Placement

The DBAP scheme in the previous section works well for periodic pseudonym change, but may not be effective for a speed-based PCS. In speed based PCS, the pseudonym changes when the speed falls below a given threshold, for example, at red light intersections and stop signs or along sections of roads that experience high traffic congestion. In the remainder of this paper, we refer to an intersection with a traffic light or stop sign as a Traffic/Stop Intersection (TSI) and congested road segments as high traffic sections (HTS). TSI and HTS are excellent candidate locations for placing attackers when vehicles are using speed based PCS. However, it might not be feasible to place attacking stations on all TSI or very closely spaced along with an HTS. The SBAP algorithm given below identifies potential attacker positions so that more vehicles can be tracked with relatively few attacking stations. Monitoring a longer stretch of the road helps in the correlation of the old and new pseudonyms of a vehicle, especially when the vehicles do not change the pseudonyms very frequently. Therefore, we consider relatively long segments (at least 15km) and have high traffic

density.

Based on the long term traffic patterns, two types of road segments are selected for monitoring:

- A set $S1$ of urban roads segments where attackers will be placed based on TSI locations, where $|S1| = k$ and $s_i \in S$ is the ith road segment and
- A set $S2$ of road segments (primarily highways, but may contain some urban roads as well), where attackers will be placed based on traffic congestion.

Algorithm 2 Speed based attacking algorithm

Input: Number (n) and Communication range (r_{comm}) of available attacking stations for vehicle tracking

Output: Adversary locations

1: Repeat steps 2 - 13 until all selected locations are covered or there is no more available attacker equipment
2: **for all** $s_i \in S1$ **do**
3: loc_A= location of the first TSI of s_i
4: Repeat steps 5-8 until $loc_A \in s_i$ == False:
5: Place attacker at loc_A
6: d_{next}=distance from loc_A to the next TSI on s_i after loc_A
7: d_{inter}= max{d_{next}, $2.r_{comm}$}
8: $loc_A = loc_A + d_{inter}$
9: **for all** $HTS_i \in S2$ **do**
10: loc_A=location of first attacker in HTS_i
11: Repeat 13-14 until $loc_A \in HTS_i$ == False
12: Place attacker at loc_A
13: $loc_A = loc_A + 2 \cdot r_{comm}$

Attacking stations are placed one by one on the selected road segments, based on TSI (steps 2-9) and HTS (steps 10-15), until all positions of interest have been covered or the maximum number of stations (n) have been used. For each selected road segment s_i on an urban road, the current attacker location is initially set to the first TSI segment (step 3). If the specified attacker location (loc_A) falls within the

current road segment s_i, (step 4) then attacking equipment is placed at loc_A (step 5). Once the equipment has been placed, steps 6-8 determine the next location be used for placing additional equipment on the current segment. If the distance from the current TSI to the next one is greater than $2.r_{comm}$, then an attacker is placed at the next TSI. Otherwise, next attacker is placed a location $2.r_{comm}$ from the current TSI on the road segment s_i. This placement strategy allows all the TSI along the road segment to be covered using the fewest possible attackers.

Once attackers have been placed at intersections, we try to place any additional equipment along with congested road segments, i.e. $HTS_i \in S2$ (steps 10-14). The first attacker along an HTS is placed at a location that is at a distance of $2 \cdot r_{comm}$ from the nearest station. Subsequently, equipment is placed uniformly at intervals of $2 \cdot r_{comm}$ along the entire segment.

4.3 Simulation and Analysis

The *objective* of this simulation is to compare four of the existing PCSs with consistent set of Mobility Models, Adversary Models and Privacy Metrics according to EPA framework as discussed in Section 3.1.

- Observed PCSs: Periodic [37], SLOW [84], CPN [86] and CAPS [101]
- Adversary Placement schemes: Random, DBAP and SBAP
- Mobility Model- Traffic Scenario: Urban or Highway
- Mobility Model- Vehicle Densities: 100, 200, and 300 vehicles
- Privacy Metrics: TSR and GTSR
- Number of Attacking Stations: 3
- Listening range of attacking stations: 500m, 700m and 1000m

For the urban scenarios, we considered 6500m x 6500m area in the city of London, Ontario, while for the highway scenarios, we considered a 26,000m by 11,000m area on the outskirts of London, Ontario. In both cases, OpenStreetMap [102] was used to obtain realistic geographical map files. We evaluated the effect of adversary placement on different PCSs, under different traffic conditions, attacker capabilities and eavesdropping duration, by varying the following parameters:

4.3.1 Number of eavesdropped vehicles

The objective of the placement strategies presented in this paper is to increase the number of "eavesdropped" vehicles, i.e. the set of vehicles (N_a) that come within the listening range of at least one attacking station. Fig. 4.1 and Fig. 4.2 compares the number of eavesdropped vehicles for different placement schemes. We see that both DBAP and SBAP significantly improve (by at least double) the chances that a vehicle will come within range of an attacking device. The performance of DBAP and SBAP is similar for the urban scenario, while SBAP performs better in highways.

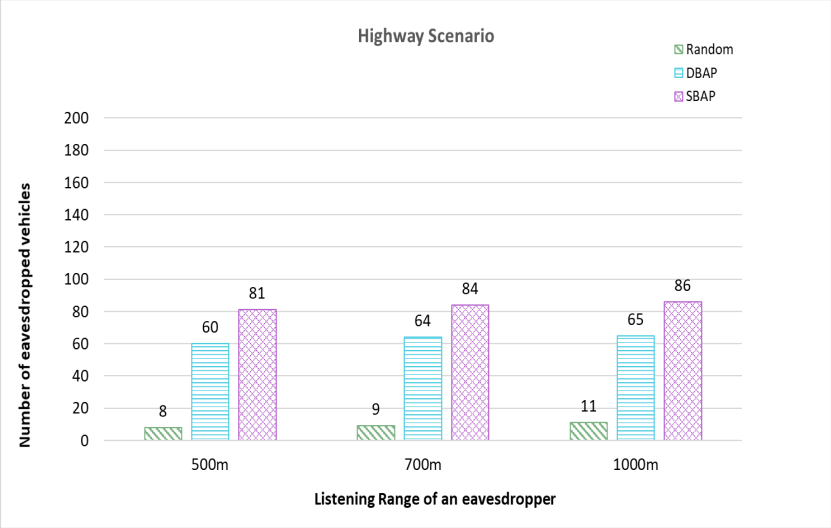


Figure 4.1: Impact of attacker placement assessed by N_a in Highway Scenario with varying listening range

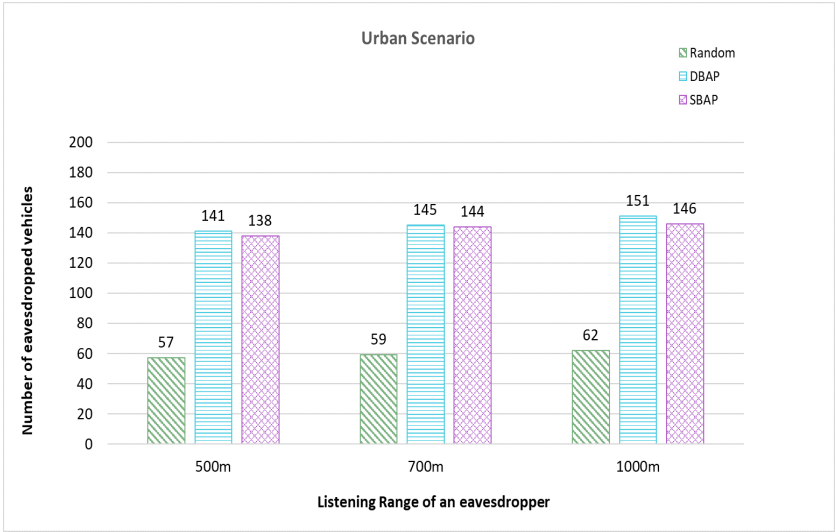


Figure 4.2: Impact of attacker placement assessed by N_a in Urban Scenario with varying listening range

4.3.2 Results for the base case

We selected a standard set of parameters to observe the "base case" performance of each PCS and placement scheme and then varied these to observe their effect on the adversary's tracking ability. For the base case, we simulated for 300 seconds with a vehicle density of 200 in the presence of 3 eavesdropping stations with a 500m listening range. The performance is measured in terms of the tracking success rate (TSR) and global tracking success rate (GTSR).

Fig. 4.3 shows the GTSR values for *highway* traffic using different PCSs, for random, DBAP and SBAP placement schemes respectively. The performance of PCS depends on placement schemes, based on their triggers and frequency of pseudonym change. This means that if the adversary is aware of PCS being used, this information can be exploited to use the placement strategy with the highest GTSR for that PCS. Overall, SLOW has the worst performance (i.e. highest GTSR) among the 4 PCSs for highway scenario, with GTSR values of 33%, 35% and 44% for random, DBAP and SBAP respectively. For periodic pseudonym changes, DBAP is the most effective scheme with a GTSR of 40%. For CAPS, both DBAP and SBAP perform similarly and much better than random placement, with GTSR values of 40% and

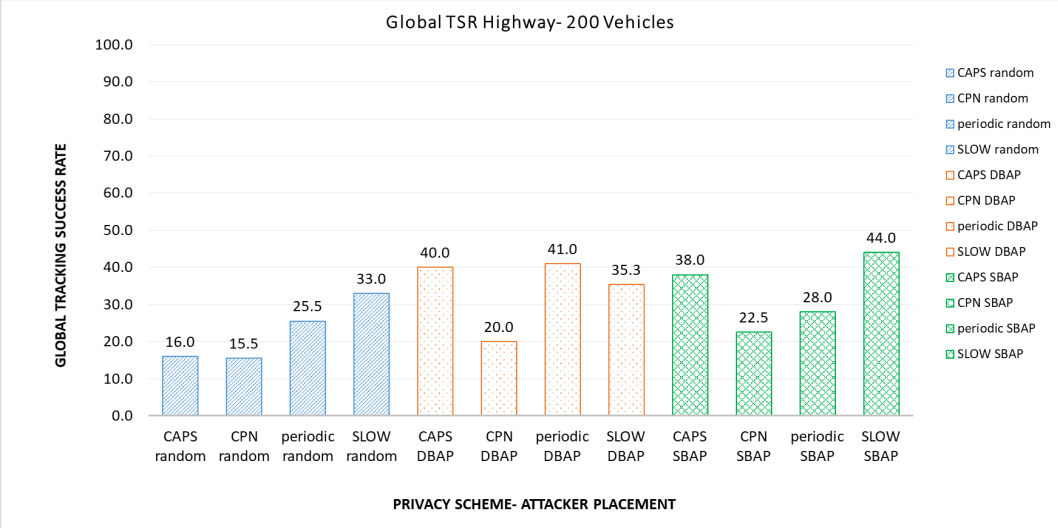


Figure 4.3: Global TSR Highway Scenario

38%, respectively. The CPN approach, which is a cooperative approach and relies on the neighbouring vehicles, works the best (has lowest GTSR) in the highway scenario for all three placement schemes, with GTSR values of 15% - 22%.

The average GTSR overall PCS approaches for DBAP placement are 34%, and SBAP placement is 33% as opposed to Random placement, which is 22.5%. Furthermore, regardless of PCS being used, random placement always has a lower GTSR, compared to both DBAP and SBAP. This shows that with limited resources, the strategic and intelligent placement of the eavesdropping stations can result in an increased rate of successful tracking. It is important to note that for highway scenario, three adversary stations with a listening range of 500m cover only a small fraction of the region of interest (26000m x 11000m) and can still achieve overall successful tracking of over 30%. By increasing the range or the number of stations, the coverage can be expanded, which directly impacts the Global Tracking Success Rate.

Fig. 4.4 shows the corresponding GTSR values for the base case, for *urban* traffic. The relative performance of PCSs is very similar to that for highway traffic, although there is some slight variation in the actual values. For random placement, we observed no significant differences between the highway and urban traffic. For DBAP, more vehicles were tracked for periodic PCS and fewer for CAPS, with urban traffic. Similarly, for SBAP GTSR value increased considerably for SLOW.

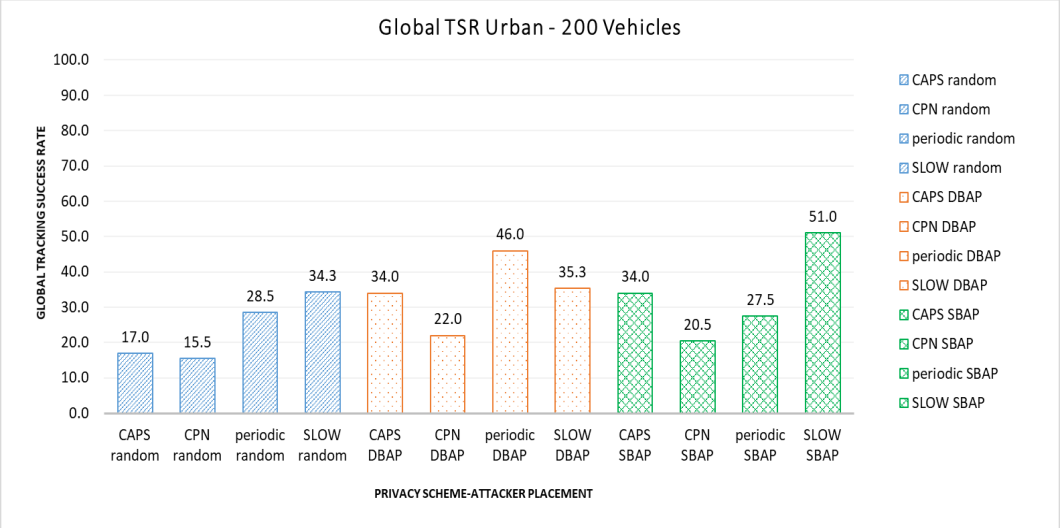


Figure 4.4: Global TSR Urban Scenario

Fig. 4.5 and 4.6 show the TSR values for different privacy approaches and placement schemes for highway and urban traffic, respectively. The TSR values are significantly higher than GTSR since they do not consider vehicles that are out of range of the eavesdropping stations. For example, for highway traffic, the GTSR values for a SLOW range from 33% - 44%, while the corresponding values for TSR are 85% - 94% and for CPN using DBAP, the TSR is 100%. It is interesting to note that there appears to be no clear correlation between the placement scheme and TSR. For example, in several cases, random placement results in higher TSR than in more informed schemes like DBAP or SBAP. Both of these observations can be explained by the fact that TSR calculations ignore all vehicles that are not 'observed' by any listening station. This means that if a listening station is in an area with very few vehicles, it will likely be able to successfully track those vehicles since fewer vehicles mean less confusion for the attacker. This will lead to a higher TSR, even though many vehicles are not being observed at all. In such cases, random placement will produce a higher TSR as the other approaches always try to put stations in the most congested locations. It can also lead to a TSR of 100% if very few vehicles appear within the stations' listening range, leading to easier tracking.

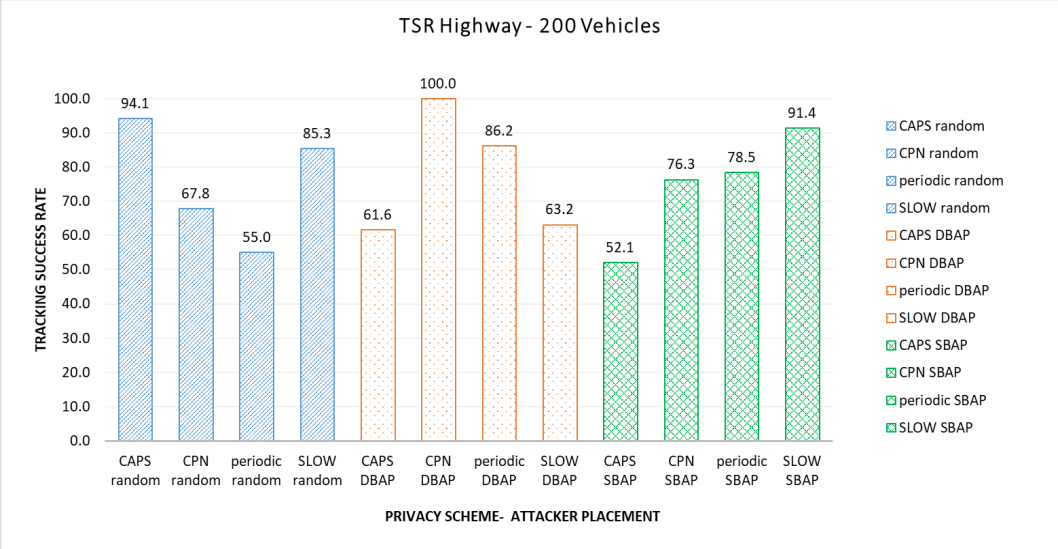


Figure 4.5: TSR Highway Scenario

4.3.3 Vehicle Density

Table 4.1: Urban Scenario: GTSR with Varying Vehicle Density

Number of Vehicles	Random				DBAP				SBAP			
	CAPS	CPN	PRD	SLOW	CAPS	CPN	PRD	SLOW	CAPS	CPN	PRD	SLOW
100	17	20	30.5	11.3	25	48	45.5	32.7	25	20	38.5	35.7
200	17	15.5	28.5	34.3	34	22	46	35.3	34	20.5	27.5	51
300	30	15.5	11.3	34.7	48	17	47	25.3	39	17.5	27	51.3

Tables 4.1, and 4.2 shows the performance of the different PCSs for different vehicle densities on the road network. PCSs may or may not directly rely on the number of neighbouring vehicles. For instance, CAPS is context-aware and relies on nearby vehicles for changing IDs. CPN also depends on the number of vehicles and leads to more frequent pseudonym changes as vehicle density increases. The vehicles using the CPN scheme would force the neighbouring vehicle to change the pseudonym simultaneously, irrespective of the delay between two consequent changes. SLOW and periodic schemes, on the other hand, are independent of the vehicle density. The urban road topology is complex and contains the intersections and traffic light rules.

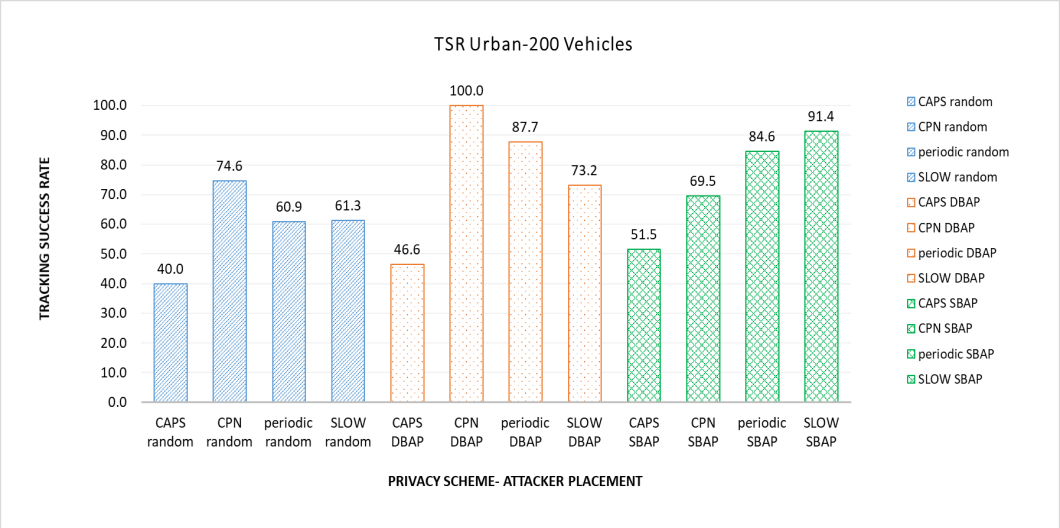


Figure 4.6: TSR Urban Scenario

Table 4.1 compares the GTSR for the different PCSs with 100, 200 and 300 vehicles in the urban road network. In this section, we discuss how the performance of each PCS varies with vehicle density.

CAPS: The context-aware scheme shows the highest tracking rate of 48% in the presence of 300 vehicles with a DBAP placement strategy and the least with random placement with a tracking rate of 17%. In general, the GTSR increases with vehicle density, irrespective of the placement strategy used. With more vehicles, there are more resulting pseudonym changes. The overall GTSR increases as the count of the successful tracking events increase with respect to the overall tracking events. When there are more vehicles around the target vehicle, it increases the frequency of pseudonym change with the CAPS scheme, and the distance-based attacker placement strategy can track these effectively. SBAP placement strategy will show the gradual decline in the tracking rate if the number of eavesdropping stations remains the same while the distance among these stations starts increasing. The performance of DBAP and SBAP is very similar for 100 and 200 vehicles.

CPN: The cooperative scheme has the highest tracking rate of 48% in the presence of 100 vehicles with a DBAP strategy. The GTSR decreases as the vehicle density increases. This scheme triggers a huge number of pseudonym changes as the number of vehicles increases, making it difficult to track the vehicles. The results are especially

Table 4.2: Highway Scenario: GTSR with Varying Vehicle Density

Number of Vehicles	Random				DBAP				SBAP			
	CAPS	CPN	PRD	SLOW	CAPS	CPN	PRD	SLOW	CAPS	CPN	PRD	SLOW
100	16	18	33	11	24	46.5	42.5	36	24	25	36	49.33
200	16	15.5	25.5	33	40	20	41	35.3	38	22.5	28	44
300	37	15.5	10.7	33.7	54	18	47	25.7	38	21	25.3	43.3

interesting when observed from the attacker's standpoint that the knowledge of traffic patterns (dense or sparse) in urban areas can allow the adversary to strategically use the placement strategy accordingly to achieve optimal tracking rate. In our mobility model with random trip-up, the growing number of vehicles was out of the observation of the eavesdropping station, causing a decrease in the overall tracking rate. This effect was particularly evident for DBAP placement.

Periodic: For a periodic scheme, the best placement strategy is DBAP, as it has the highest GTSR overall, regardless of the number of vehicles. Randomly placing the eavesdropper results poorly for the tracker while SBAP performs well with 38.5% of tracking with 100 vehicles and gradually shows the decline as the stations are separated.

SLOW: As expected, SBAP has the highest tracking rates (35% - 51%) for the SLOW scheme, as it places attacking stations where pseudonym changes are likely to occur. The tracking rate increases with several vehicles when using SBAP. The GTSR for DBAP (25% - 36%) and random placement (11% - 35%) is much lower since they do not allow the tracker to strategically cover high traffic areas or the areas with potential traffic jams. With DBAP, GTSR does not seem to correlate strongly with several vehicles, while it increases with vehicular density increases for random placement.

For the highway scenario, the GTSR values for each PCS followed a similar trend as for the urban roads, although there were some variations in the actual values.

4.4 Conclusion

To summarize the key findings of this chapter, we proposed two new intelligent adversary placement strategies- i) *distance based attacker placement* (DBAP) and ii) *speed based attacker placement* (SBAP) which aim to maximize the degree of observation with limited capabilities. We evaluated the privacy level provided by four observed PCSs in the presence of a local passive adversary. We assessed the threat level, which indicates the effectiveness of the adversary. We observed the total number of vehicles eavesdropped in the presence of these adversarial settings in different traffic scenarios. We then examined the successful tracking based on two metrics, Tracking Success Rate and Global Tracking Success Rate.

Chapter 5

A Context Aware and Traffic Adaptive PCS in VANETs

5.1 Introduction

There are various PCSs proposed in the last decade; however, these schemes have limitations. Several PCSs rely on radio silence, which is not a suitable choice for the safety-critical messaging [22] [79]. Some schemes work better in high vehicle density areas [68] [83] [72] [87] while others depend on specific zones [69] [73]. This dependency on the traffic scenario and zones within the road network impacts privacy. These schemes are not adaptive to the changing vehicular scenarios based on the region (city or highway). Li [79] proposed a scheme in which vehicles exchange pseudonyms and use radio silence when changing pseudonyms. In terms of preserving privacy, this scheme would perform better than other schemes. But the exchange of the identities conflicts with the requirement of conditional privacy [82] [85]. The cooperative [80] and synchronous [81] PCSs are the general mix context schemes where vehicles signal neighbouring vehicle(s) to change the pseudonyms simultaneously. For these schemes, the frequency of pseudonym change is usually very high. With rapid changes, the pseudonyms exhaust when provided in a limited number. Currently, the emerging standards have a limit for the number of issued pseudonyms to a vehicle that has a lifetime of three years. The current scheme in standards is the result of the availability of the limited number of pseudonyms. A vehicle periodically changes pseudonyms every five minutes, and once the allocated pseudonyms are exhausted, it is forced to reuse pseudonyms throughout the remaining period [37]. This introduces a privacy vulnerability because the repetition allows easy tracking as the Adversary has the

prior knowledge of the used pseudonyms. Among all the existing PCSs, context-aware schemes take advantage of the information about neighbouring vehicles. CAPS [101] is one such scheme in which the vehicle detects a nearby vehicle, and when both the vehicles agree, they stop BSM broadcasting for some time. This is an effective approach when viewed for privacy only; however, in terms of balancing safety and privacy, such schemes using radio silence are not very attractive. An intelligent passive adversary may also know about the PCS; therefore, one of the main limitations is the use of static triggers.

A comprehensive PCS should leverage different factors to increase anonymity in an ad-hoc environment with a defensive approach to protect from the tracking based on eavesdropping. Rapidly changing pseudonyms provide more privacy and can lead to a vehicle's being exhausted quickly, since only a limited number of pseudonyms are available, due to the limited memory of OBU. This leads to the reuse of previous pseudonyms, allowing easier tracking of the target vehicle. An ideal PCS should allow frequent pseudonym changes to preserved anonymity without being constrained by the number of available pseudonyms.

As mentioned earlier, using radio silence before pseudonym changes are effective in terms of the untraceability of vehicles but can compromise safety [36]. Therefore it is desirable to implement a PCS that can effectively maintain vehicle anonymity without requiring radio silence. The constant frequency and predictable timing for pseudonym change can be used by the Adversary to deduce a pattern over a period of eavesdropping. So, good PCS should use unpredictable triggers to initiate pseudonym changes.

In this chapter, we propose a new PCS that aims to benefit the most from the context of the vehicle and traffic patterns to leverage the optimum situation for changing pseudonyms. The vehicles change the pseudonym simultaneously in a region to increase privacy by maximizing the anonymity set.

5.2 System Architecture

Our model considers that the vehicles are equipped with DSRC enabled On-Board Units (OBUs), which facilitate the Vehicle to Vehicle (V2V) as well as Vehicle to Infrastructure (V2I) Communication. There are three main entities, namely, *Certificate Authority (CA), RSU, OBU* which communicate with each other. All the entities in this vehicular communication, including RSUs, CAs and vehicles, have a set of public and private keys for secure communication.

CA

CA in VANETs is responsible for issuance of a set of a public and a private key to the participating vehicles and RSUs in the vehicular network. RSUs and Vehicles have the public key of CA. CA also issues the initial seed to the authorized vehicles for pseudonym generation. CA maintains the database for the long-term accountability of the registered vehicles by keeping the original vehicle identification and the assigned seed along with the issuance time. CA is an integral part of the Security Credential Management System(SCMS), which has high computational facilities and extensive storage capabilities. The information from this database is used to investigate malicious activities. In this work, we are focusing primarily on the usage and change of the pseudonyms. Therefore, the generation and revocation of the pseudonym are not in the scope of this work. However, we indicate that law enforcement will contact CA and use this information from the database to identify or confirm the malicious vehicle. Our PCS assures the balance of accountability while providing conditional privacy. The database contains the following information, which enables accountability.

- Enrollment Certificate of Vehicle with assigned seed S and timestamp t
- RSU ID, Location Coordinates and range of RSU R
- Seed S, RSU ID which assigned S, timestamp t

- Currently active seed S with RSU IDs of encountered RSUs

RSU

The DSRC-based *RSUs* are interconnected to each other as well as with the back-end CAs via a wired network. This network of RSUs works as the backbone network architecture, helping in the fast intercommunication of RSUs. RSUs are responsible for the distribution of the seeds to the vehicles in their ranges and also for triggering pseudonym changes based on vehicle contexts and traffic. We assume that RSUs are trusted entities. RSUs are also useful in terms of computation; however, sometimes sending more data to process on the RSU can cause network congestion. We consider that the vehicles send BSM with the pseudonym. The validity of this pseudonym is verified by the RSU of that region so that vehicles do not have to perform additional computation. Each Vehicle v registers itself with its regional RSU when it enters the transmission range of the RSU, which monitors all the vehicles within its vicinity. Upon successful registration, RSU provides a time map of TM to the vehicle. This time map consists of randomly distributed timestamps for initiating the pseudonym change cycle. The RSU is responsible for verifying the pseudonyms used in BSMs, as opposed to all the vehicles. To check the validity of the pseudonym, RSU performs the same steps as the vehicle to obtain the pseudonym from the seed. RSU monitors BSM activity in its region and makes sure all the pseudonyms used in these BSMs are valid. When an unverified pseudonym is encountered in the range, RSU sends a message to all the vehicles in its range, informing about the untrusted vehicle. RSU is responsible for the coordinated pseudonym change based on the traffic and context information of all the vehicles in its range.

Vehicle/OBU

The *Participating Vehicle* is equipped with *OBU* which periodically broadcast the situational awareness information to its immediate environment for safety applications. It has a Tamper-Proof Device (TPD) for securing sensitive information on the

vehicle, such as credentials. The vehicle can participate in Vehicular Communication once CA authorizes the vehicle. Upon successful authorization, Vehicle V enrolls with CA and obtains a seed S for pseudonym generation, which is signed by CA_{PR} and contains timestamp t at which the seed is issued.

Pseudonym Generation and Usage The pseudonyms are generated by using the Hash-based Message Authentication Code (HMAC) [103], which takes a secret key and a cryptographic hash function. HMAC is used to ensure the authenticity and integrity of the message. However, we are using HMAC to generate pseudonyms as a hash chain. These pseudonyms are used for BSM authentication and misbehaviour reporting. The secret key is the seed value given by CA to the vehicle upon authorization to allow participation in a vehicular network. The vehicle can generate new pseudonyms using this secret key.

5.3 Proposed PN lifecycle

5.3.1 Initialization

The initial issuance of the seed to vehicle solely relies on CA that enrolls the vehicle based on the enrollment certificate of OBU and provides a *seed* for generating the pseudonyms. This enrollment is carried out once to join the vehicular network. The seed is provided to the vehicle for generating pseudonyms, and this seed is signed with the CAs private key to indicate the authenticity of the seed.

5.3.2 Vehicle registration

As soon as the vehicle encounters an RSU, it registers itself with this RSU by giving its seed for the time it is going to be in the range of this RSU. Fig. 5.1 demonstrates the registration process of the vehicle with the regional RSU. Each RSU sends a periodic announcement which contains RSU_{PK}, RSU ID and timestamp t. When a vehicle V receives this announcement, it sends the Registration Request to the RSU, which contains the seed S and timestamp t, as shown in Fig. 5.2.

Figure 5.1: Vehicle Registration with regional RSU

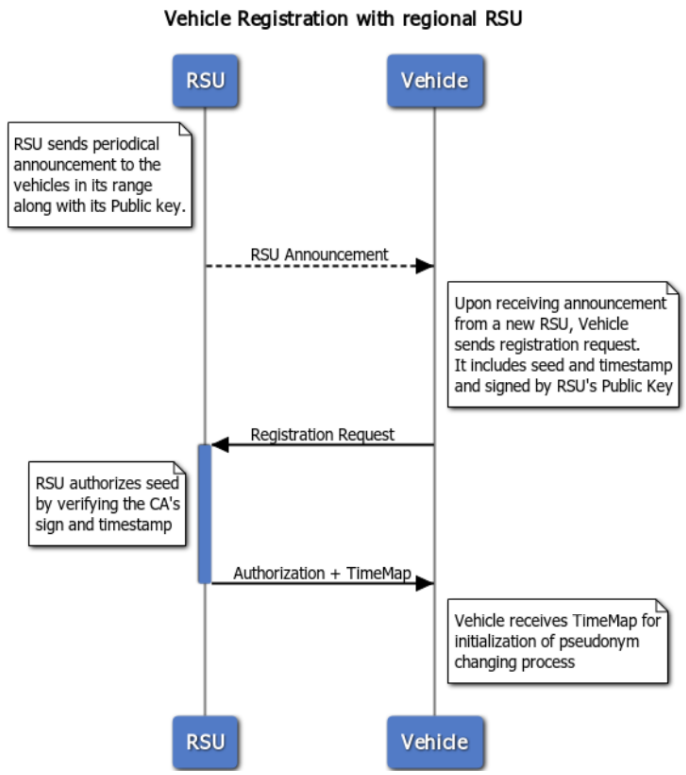


Figure 5.2: Message Structure for Vehicle-RSU communication

MESSAGE STRUCTURE

Sender Cert	Receiver Cert	Type of Message	Message Attributes

AUTHENTICATION

a) Vehicle request RSU to join its zone

Veh_{PR}	RSU_{PK}	**Reg. Rqst**	{Seed S, $T_{issuance}\}_{CA_{pk}}$, Current *Psnym*, Current timestamp *t*

b) RSU approves registration request and sends acknowledgement

RSU_{PR}	Veh_{PK}	**Reg. ACK**	{ Registration *ACK*, Time map *TM*, current index *i* in TM}

ALERT MESSAGE

RSU sends an alert message when an unverified (malicious) vehicle is encountered

RSU_{PR}	Veh_{PK}	**Alert**	{pseudonym(s) of Unverified vehicle }

This request message is encrypted using RSU_{PK}. Once the Road Side Unit receives the Registration Request, it verifies the seed S using CA_{PK}.

With this mechanism of seed registration, RSU holds the vehicles accountable at the regional level. It will also reduce the communication and computational overhead caused by the verification of the Basic Safety Messages by the receiving vehicles. RSU is responsible for verifying the pseudonyms used in the BSMs in its area. According to currently proposed standards, the receiving vehicle verifies the pseudonym. Considering the frequency of the BSMs and heavy traffic scenarios, a receiving vehicle has to verify a large number of pseudonyms. In our scheme, RSU takes care of verification and informs the vehicles about the malicious vehicle when encountered.

5.3.3 BSM broadcast

For safety purposes, the vehicles communicate the information related to situational awareness with each other. A vehicle sends the safety message with the pseudonym identity for BSM authentication. RSU authenticates the vehicles in its range and informs all the vehicles in case of misbehaviour detection. The receiving vehicles do not perform verification, which accelerates the processing of received BSMs.

5.3.4 Handling misbehaviour

With the registration of the vehicles, RSU can hold the vehicles accountable, which are in its region. If a vehicle fails to register, it is considered a malicious vehicle. RSU and other vehicles can receive BSMs from the unregistered vehicle. However, if RSU does not verify the sending vehicle, then RSU sends the alert message to the vehicles in its area. As shown in Fig. 5.2, RSU sends the unverified pseudonym to the registered vehicles so that the receiving vehicles do not process BSM as the pseudonym identity used in BSM matches the one in the alert message. The main advantage of this mechanism is that RSU can detect the misbehaviour immediately at the regional level. This mechanism partially supports the active attacks, which involve the alteration of the pseudonym, such as impersonation attack or replay attack. RSU

can detect if there are two copies of the same pseudonym or a vehicle that generates a fake pseudonym and has not registered with RSU. Both of these cases cause RSU to trigger a challenge and response in which RSU determines the authorization of the vehicle by asking the vehicle to generate the next possible pseudonym. In this case, only one can generate the correct pseudonym, and this accelerates the identification of the malicious node in the network at the regional level. The strength of using the HMAC-based pseudonym generation is that it prevents pseudonym repetition and supports the recognition of malicious vehicles. The active attacks are not in the scope of our work.

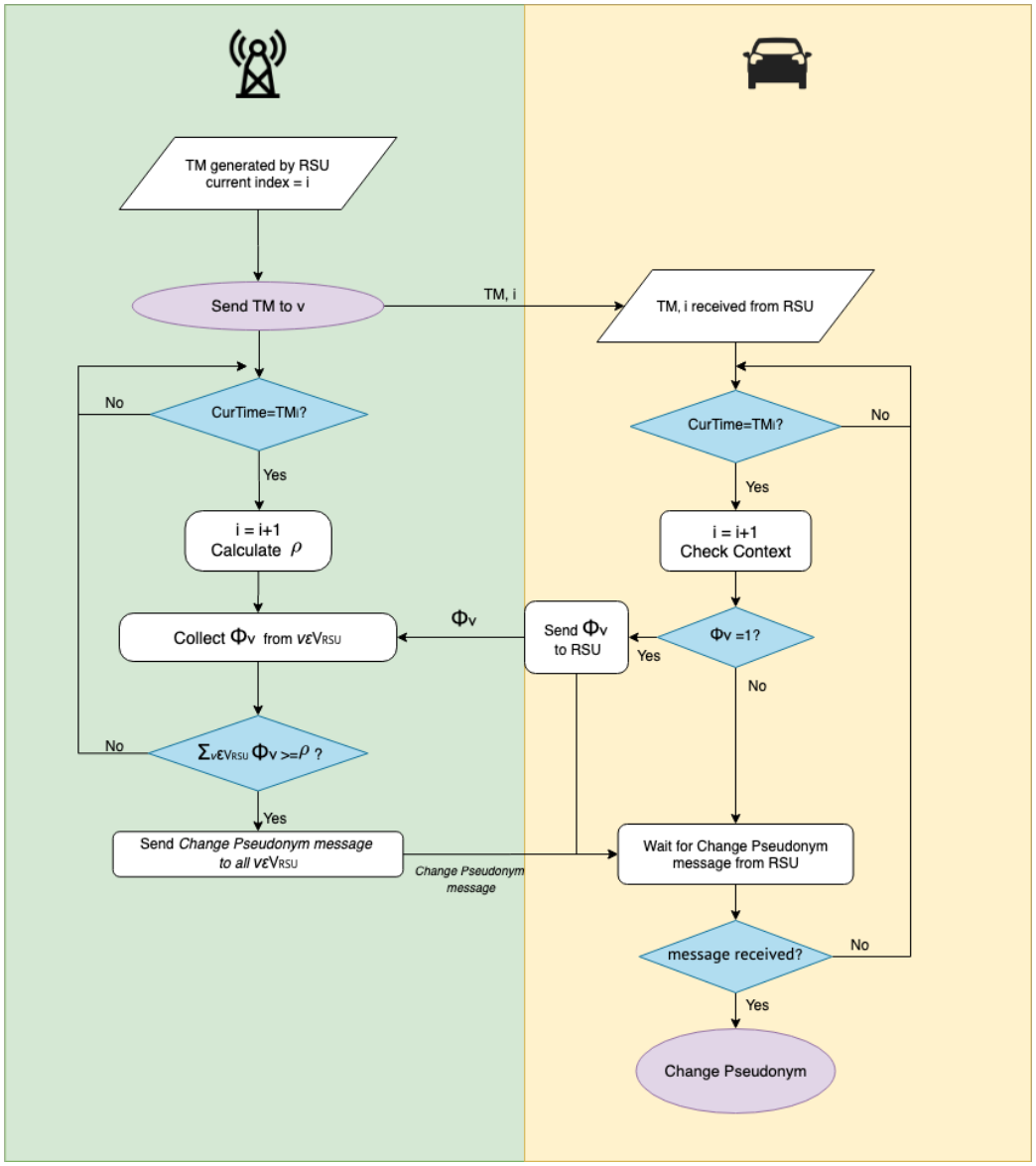
5.4 Proposed Pseudonym Changing Scheme

In this section, we present our proposed *Context-Aware and Traffic Adaptive (CATA)* pseudonym changing scheme. RSUs are responsible for initiating the process of pseudonym change and uses information about the *context* of vehicles in its range, to dynamically determine when pseudonym change should occur. Each vehicle calculates its context, which can include speed, direction and distance of neighbouring vehicles, and sends this information to the RSU. Based on the information received from vehicles and the current traffic density in its regions, the RSU decides if pseudonym change should occur and informs the vehicles accordingly.

When a vehicle changes pseudonyms, the surrounding traffic conditions have a significant impact on whether an adversary can link the old and new pseudonyms. The primary factors that affect this include the number of other vehicles near the ego vehicle, the distance from other vehicles, and the relative speed and direction of travel of the surrounding vehicles. We refer to these as the *context* of a vehicle. When several vehicles are moving in the same direction, with similar speeds and are close by each other, this situation serves as an ideal pseudonym changing condition. The proximity of many similar context vehicles changing pseudonyms simultaneously makes it difficult for the Adversary to link old and new pseudonyms to the same vehicle accurately. To have a strong PCS, a high degree of context match is essential

as it increases the anonymity of the vehicle while decreasing the Adversary's tracking success rate. The network of vehicles on the road changes rapidly based on the time of the day and locality/area. The traffic patterns can vary depending on the type of road segment (urban or highway), the number of vehicles (sparse or dense traffic), road conditions, etc. In our scheme, each RSU is aware of the current traffic patterns (TP_{RSU}) in its region and considers this in determining when vehicles should change pseudonyms.

Figure 5.3: Overview of CATA Pseudonym Changing Scheme



The proposed approach differs from CAPS based on the usage of the context information. In CAPS, the context information is used to detect a neighbouring vehicle in silence; it turns to silence as well. In case no vehicle in the immediate environment is silent, the vehicle sends BSMs until it reaches a maximum pseudonym time and then turns to silence. This radio silence is used to confuse the Adversary by disrupting the continuous stream of BSMs. In terms of safety and privacy trade-off, the radio silence provides privacy by putting safety at risk. Therefore, we avoid the radio silence to ensure that there is no disruption in the safety-critical messaging. This is the main reason that our scheme does not impact the frequency of BSMs; hence, it complies with the currently proposed rate of BSM transmission. In our proposed CATA pseudonym changing scheme, the context information is used to detect the neighbouring vehicle(s) with similar speed and heading. By determining at least one such vehicle close by, when the cooperative pseudonym change occurs, it not only maximizes the anonymity set but increases chances of the unsuccessful tracking events.

Table 5.1: Notations used in the proposed scheme

Notation	**Description**
CA	Certificate Authority
N_v	Set of neighbouring vehicles for node v
V_{RSU}	Set of vehicles in the range of a RSU
μ	Number of Vehicles with Context-Match
ϕ_v	Context Flag for vehicle v
ρ	Traffic Adaptive Threshold
RSU_v	RSU with which vehicle v is currently registered
dir_v	Direction of Vehicle (node)
$speed_v$	Speed of vehicle v
$dist_{u,v}$	Distance between vehicles u and v
d_{th}	Distance threshold for context similarity
s_{th}	Relative speed threshold for context similarity
i	Current index in time map (TM)
TM_i	time at which next pseudonym change cycle starts

The RSU has the record of all the vehicles in its range, and upon registration, RSU sends a time map (TM) and the current index i to the vehicle. TM contains a list of randomly distributed timestamps for triggering each successive round of the pseudonym change cycle. Both the RSU and the individual vehicles (after registration) in its range have access to the same TM and are responsible for carrying out their respective tasks and communicating with each other when the process is triggered, as shown in Fig. 5.3.

Algorithm 3 and 4 outline the steps carried out at the RSU and each vehicle $v \in V_{RSU}$ respectively. At the RSU (Algorithm 3), TM_i is the next time the pseudonym change cycle should start. In steps 1 and 2, the RSU simply waits until the process can start (i.e. $CurrentTime == TM_i$). Once the process starts, the index i is incremented (step 3) to point to the start time for the *next* round. Next, the RSU calculates the *traffic adaptive threshold* (ρ), which determines what percentage of vehicles in its region need to report a non-zero context flag to trigger pseudonym change. This threshold depends on the current traffic patterns and set of vehicles in the region. RSUs can frequently change this percentage to introduce more variability in terms of the conditions for triggering pseudonym change. The RSU then waits for half of the time before reaching the next cycle to receive context flags from the vehicles in its range (step 5) and calculates the total number of vehicles with a positive context match (μ) in step 6. If μ exceeds the value calculated using the threshold (ρ), then a message is sent to all vehicles in the range of the RSU to change their pseudonyms. Otherwise, no pseudonym change takes place in the current round.

Algorithm 3 RSU triggers pseudonym change if needed

Require: $\mu, TP_{RSU}, V_{RSU}, TM, i$

1: **for all** $CurrentTime <= TM_i$ **do**
2: Wait to initiate pseudonym change cycle
3: $i = i + 1$
4: $\rho = calc\_Traffic\_Threshold(V_{RSU}, TP_{RSU})$
5: Collect context flag (ϕ_v) messages from $v \in V_{RSU}$
6: $\mu = \sum_{v \in V_{RSU}} \phi_v$
7: **if** $\mu >= \rho \cdot |V_{RSU}|$ **then**
8: Send *Change Pseudonym* message to all $v \in V_{RSU}$

At each vehicle $v \in V_{RSU}$ (Algorithm 4), steps 1-3 to initiate pseudonym change are the same as in Algorithm 3. For the individual vehicles, the algorithm proceeds in two phases. During Phase 1, each vehicle v calculates its context flag (ϕ_v) and sends it to the RSU. This is done by checking the context similarity (steps 5 - 7) with each vehicle $u \in N_v$ in its neighbourhood. Two vehicles have similar contexts if they are close to each other, have similar speeds and are travelling in the same direction. As soon as the first similar-context vehicle is found in the neighbourhood, the context flag is set to 1 (step 8), and this information is sent to the RSU (step 9). No additional vehicles in the neighbourhood are checked, and Phase 1 ends. The concept of sensing the immediate environment of the vehicle before a change of pseudonym is an essential aspect of our CATA PCS. When the decision to change pseudonym is based on a dynamic and adaptive trigger, which takes context and situation of the vehicle into account, it promises more privacy than the predictable, known and constant triggers.

After Phase 1, the vehicle must wait for some time to receive a *Change Pseudonym* message. If the message is received, Phase 2 starts and v generates a new pseudonym

Algorithm 4 Vehicle v changes its pseudonym if directed by RSU

Require: $N_v, TM, i, d_{th}, s_{th}, dir_v, speed_v$
Require: $dir_u, speed_u, dist_{u,v} \forall u \in N_v, u \neq v$
1: **while** $CurrentTime <= TM_i$ **do**
2: Wait to start context check
3: i = i+1

Phase 1 - Vehicle v calculates its context flag

4: **for** all $u \in N_v$ **do**
5: **if** $dist_{u,v} <= d_{th}$ **then**
6: **if** $dir_u == dir_v$ **then**
7: **if** $|speed_u - speed_v| <= s_{th}$ **then**
8: Set $\phi_v = 1$
9: Send context flag (ϕ_v) to RSU_v
10: break

Phase 2 - Vehicle v updates pseudonym

11: **if** *Change Pseudonym* message is received from RSU_v **then**
12: $pseudonym_v$ = generate_PN($seed_v, pseudonym_{v-1}$)

based on its seed and a current pseudonym. Otherwise, the pseudonym changes cycle ends without any updates to the current pseudonym, and the vehicle waits for the next cycle to start.

Advantages of Proposed Scheme

The proposed scheme increases the anonymity of the individual and untraceability of the vehicle primarily because of the cooperative change of pseudonyms. There are two main factors: a) several vehicles, and b) context matching neighbouring vehicles, which increase the effectiveness of the pseudonym change concerning intelligent tracking. CATA adapts according to the traffic patterns, and this contributes to the dynamic nature of the trigger. An intelligent adversary may have prior knowledge of PCS, and when the scheme has static triggers, the Adversary can take advantage of it. Therefore, our scheme adapts the trigger based on the traffic patterns and does not reveal any direct information regarding when the next pseudonym change will occur. The trigger also needs to be random so that an intelligent adversary cannot deduce a pattern or guess the next changing event. Our scheme does not impact the frequency of BSM transmission, which ensures that there is no effect on the safety applications when preserving privacy. Another advantage of our scheme is that unlike other schemes, it does not allow the repetition of the pseudonyms due to the limited available set of pseudonyms. The vehicles do not verify the received BSMs while RSU monitors BSM transmission and verifies the sender's authenticity. Due to this reason, the misbehaving vehicles can be identified immediately, and this information can be sent to all the vehicles in the transmission range.

5.5 Experimental Results

Simulation Setup

For the urban scenarios, we considered a 6500m by 6500m area in the city of London, Ontario. In contrast, for the highway scenarios, we considered a 26,000m by 11,000m

area on the outskirts of London, Ontario. Our scheme utilizes infrastructure units. Therefore, the road network is accordingly covered in both scenarios using RSUs. In the Urban scenario, 12 RSUs are placed in the triangular pattern, while in Highway Scenario, it takes 13 RSUs with 50 m of overlap in the transmission range in both cases. We have used random trip generation for urban traffic for different origins and assign different routes to distinct destinations. We evaluated the level of privacy provided by the observed schemes with metrics based on the user's and Adversary's perspectives. For the assessment, we consider a local passive adversary with a limited number of equipment, in total six of the attacking stations. We assess our proposed PCS by comparing it with three other schemes in different adversary placements. These PCSs use different techniques to change the pseudonyms such as radio silence, constant rate of change, neighbouring vehicle and context. We measure the effect of adversary placements on different PCSs with two types of road networks (Urban and Highway) and attacker capabilities based on the following parameters, as discussed in Table 5.2.

Location Privacy Evaluation

The evaluation of privacy is subjected to the context and situation of the user. The anonymity of the individual in the network is based on the neighbouring vehicles, and it depends on the traffic patterns at the regional level. The uncertainty of de-identifying an individual is relative to the locality and road network. When a PCS takes into account the changing environment of the vehicle, the trigger to change pseudonym tends to be dynamic, and the scheme becomes user-centric. This means a vehicle finds an optimized situation to change the pseudonym simultaneously with neighbouring vehicles [86] [101]. When PCS is dependent on the neighbouring vehicles, the anonymity of the vehicle heavily depends on the traffic density and traffic patterns. With the increase in the number of vehicles, the uncertainty of recognizing the vehicle gets higher. Contrary to this case, PCS with the static triggers like a periodical change of the pseudonym [37] is independent of the traffic movement and the number of vehicles. However, the anonymity level still relies on these factors even

Table 5.2: Simulation Parameters

Parameter	***Value***
Simulation Framework	OMNET++, SUMO, VEINS, PREXT
Geographical Map Tool	OpenStreetMap
Traffic Scenarios	Urban, Highway
Urban region	City of London, ON, 6500 m x 6500 m
Highway Region	Outskirts of London, ON, 26,000 m x 11,000 m
Max. Speed	50Km/hr (U) and 100Km/hr(H)
Vehicles	200
Traffic model	Continuous broadcasting, no packet collisions, Minimum period between two broadcasts is 0.1 secs
Carrier Frequency	5.890e9 Hz
OBU Carrier Sensitivity	-89dBm
Transmission Power	20mW
Bitrate	18Mbps
Beaconing rate	10 Hz
Thermal Noise	-110dBm
usePropagationDelay	True
Obstacle Model	SimpleObstacleShadowing
Compared PCSs	Periodic, CPN, CAPS and our scheme CATA
Placement Scheme	Random, DBAP and SBAP
Number of Attacking Stations	6
Number of RSUs in Scenarios	12 (Urban) and 13 (Highway)
Listening Range of Adversary	1000m
Eavesdropping Duration	300 sec
Tracking	NNPDA [61]
Metrics	Entropy of Anonymity Set, Global Tracking Success Rate

though periodical PCS itself does not depend on the traffic. When assessing location privacy, we consider the user's as well as Adversary's perspectives to investigate the robustness of our CATA PCS in the presence of intelligent adversaries. To the best of our knowledge, this is the first evaluation to examine both points of view. This assessment reflects the level of privacy in terms of the randomness of the target vehicle within an anonymity set and the ability of the Adversary to identify the target vehicle successfully.

We note that the average number of pseudonym changing events occurring with each PCS differs. The cooperative scheme has the highest rate of change of pseudonyms followed by our scheme and then CAPS scheme in both scenarios. The periodic scheme is bound by the constant time period, and it directly depends on the length of the simulation rather than the traffic situation. In our evaluation, with the periodic scheme, the vehicles change pseudonyms one time during their trips. With a cooperative scheme, the vehicles are forced to change along with another vehicle that intends to change the pseudonym. Therefore, we observe a spike of 19 changing events on average. The rate of change of pseudonym with CAPS will increase with the dense traffic scenarios in which vehicles are moving close to each other. On the other hand, our scheme is adaptive to traffic density, which means the rate of change of pseudonym would not be affected by the number of vehicles. Also, due to the randomness introduced by the time map, the average number of pseudonym changes will vary because essentially, it is a time map that initiates the pseudonym change cycle. In this experiment, we observed an average of 14 changing events with the CATA scheme. With the CAPS scheme, on average, the vehicles changed pseudonyms six times. The higher frequency of change is an advantage if the pseudonyms are not repeated, and there are enough pseudonyms available. Our scheme covers this aspect; it not only has a high frequency of pseudonym change but also avoids repetition by generating a new pseudonym.

Another important observation is related to the number of vehicles that encountered the Adversary. Vehicular trips are random in all scenarios, and the vehicles on average encounter two attacking stations in an urban scenario and three to four in

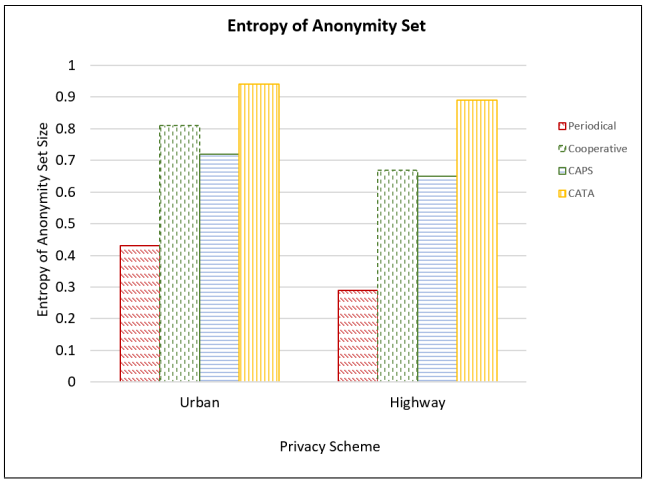
highway scenarios. The number of encountered stations rely on traffic modelling as well as the eavesdropping duration.

Privacy Evaluation: User's Perspective

We examined the Entropy of Anonymity Set for three of the existing PCSs and our proposed scheme. This privacy metric mainly relies on traffic movement and PCS. We observed the Urban and Highway traffic scenarios and noticed that the randomness varies in both of these scenarios but overall shows similar trends. The Urban scenario has relatively higher Entropy of Anonymity Set (EAS) because of the complex road network. Generally, the Periodical Scheme shows the lowest EAS because of the deterministic nature of PCS. Often, when a vehicle with Periodical PCS changes the pseudonym, it is carried out individually, which decreases the randomness significantly. The next higher EAS is of CAPS, which is moderately less than CPN in the Urban scenario and slightly lower in the Highway scenario. As the traffic movement remains the same for all the schemes, we observe that when PCS considers the neighbouring vehicle to carry out the pseudonym change, the vehicle enjoys a higher level of privacy with EAS in the range of 0.6 to 0.85. In the CPN scheme, the vehicles change pseudonyms with high frequency; it introduces additional advantage, thus, have higher EAS than CAPS. This frequency of changing the identifier is relative to the traffic density. With more neighbouring vehicles, the number of pseudonyms changing requests received by a vehicle increases; therefore, we observe rapid changes. These quick changes are responsible for the rise in EAS of CPN when compared to CAPS.

The underlying vehicular network remains the same when we assess all four PCSs with a consistent number of vehicles, road networks, traffic patterns for both scenarios. We noted the highest EAS for our proposed scheme in the Urban scenario with slightly lower EAS in Highway Scenario. The fundamental reason behind this trend is the impact of the large scale cooperative pseudonym change, which maximizes the anonymity set and increases the randomness. The uncertainty of determining a specific vehicle among a large number of vehicles with new identifiers cause more

Figure 5.4: Entropy of Anonymity Set: Urban and Highway Scenario



confusion for Adversary and affects the correctness of the tracking of the target vehicle. CATA has a regional cooperative pseudonym change, which is carried out once RSU determines the area's significant traffic density. It also considers the context of the vehicles in their area. Both traffic and context together become the key reason for the higher EAS. In the previous case of CAPS, the pseudonym change is carried out by using the context of the vehicle. However, it is subjected to the neighbouring vehicles only while CATA uses the context of the vehicles and uses this information at the regional level. When a sufficient number of vehicles indicates that they have at least one vehicle with matching context, RSU further decisions based on the traffic density when to change the pseudonym. The intricacies of the context of the vehicle and the traffic movement, as observed by RSU, results in higher EAS.

Privacy Evaluation: Adversary's Perspective

For privacy assessment, the Adversary's perspective is as significant as the user's point of view. When we discuss the privacy-preserving schemes, we are inherently aiming to prevent information loss, which can be used to infer the private information of an individual. Therefore, we emphasize that the PCSs need thorough investigation with a consistent set of traffic models and in the presence of intelligent adversary models. It allows the examination of how successfully an adversary can track and determine the target vehicles throughout their trips. The trends, as shown in Fig.

5.5 reflects the Global Tracking Success Rate (GTSR) in the presence of different adversary placements in the Urban Scenario. It is important to notice that GTSR is the tracking rate observed with respect to all the vehicles in simulation and not merely the Adversary's encountered vehicles. It is highly unlikely that the local passive Adversary eavesdrops all the vehicles in the scenario. It mainly depends on the number of attacking stations and the coverage of the road network. With different placement strategies, the coverage varies, which plays an important role in overall tracking. The assessment shows the percentage for GTSR always lower than 50%. This is because the attacking stations are disjoint, therefore when the vehicles are not in the Adversary's range, then that vehicular trip counts toward the unsuccessful tracking event. Another factor is that the vehicle may be re-identified as a new vehicle when it enters the next station range. With limited eavesdropping stations, the overall number of unsuccessful events increases, which leads to overall lower GTSR. When attacking stations are in areas with low vehicle density, it is easier to track the limited number of vehicles in its range since fewer vehicles cause less confusion. However, overall only a small percentage of vehicles are being eavesdropped.

Generally, Periodical PCS shows the highest GTSR because the vehicle changes the pseudonym irrespective of context and surrounding traffic. The highest GTSR is observed in the presence of distance-based attacker placement (DBAP) for the periodical scheme. This placement scheme is ideal for such PCS, which has a deter-

Figure 5.5: GTSR in Urban Scenario

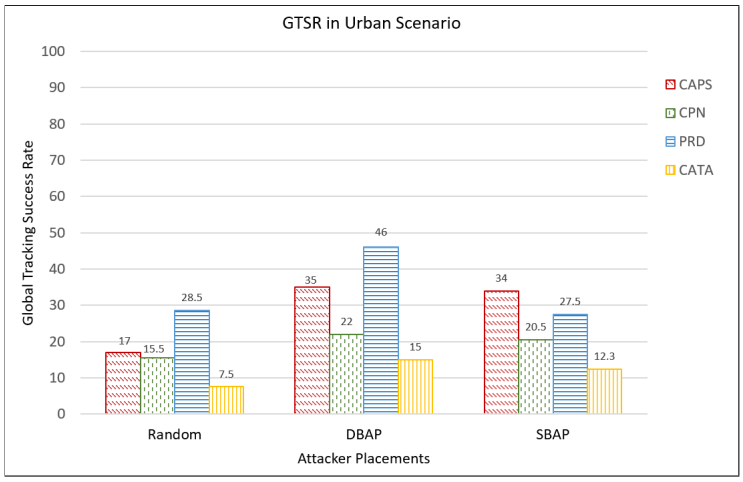
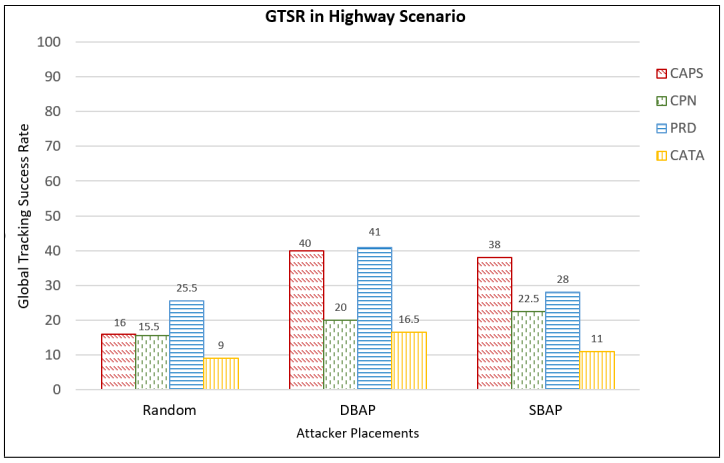


Figure 5.6: GTSR in Highway Scenario



ministic pattern for changing the pseudonym. An intelligent adversary with DBAP takes advantage of this fact and places the equipment by pacing out strategically in high-density areas. However, the random placement and SBAP show nearly the same GTSR as there is a rise of unsuccessful events mainly due to the gaps in the attacking stations. For the CAPS scheme, random adversary placement shows the lowest GTSR, while for SBAP and DBAP, there is a difference of 1%. CAPS is context-based PCS, from the observation in Fig. 5.5, we notice that GTSR is higher than CPN, which does not consider the context. This happens because the frequency of the change is lower in CAPS than CPN. In both cases, at least two vehicles change the pseudonyms simultaneously, yet the rapid changes in CPN become the advantage in terms of protecting against continuous tracking. CPN has the highest tracking success with DBAP placement, followed by SBAP and Random placement. Our proposed CATA scheme outperforms the observed PCSs with the lowest GTSR in all adversary placements. Our CATA PCS introduces a variety of factors which collectively prevent successful tracking. Primarily, the proposed PCS does not allow a deterministic pattern of the pseudonym change. When the PCS involves the dynamic triggers, which are random and remain unknown to the Adversary, we have seen in the case of CPN and CAPS that the tracking rate decreases. However, CATA prevents a higher level of tracking because of the cooperative regional pseudonym change. The vehicles in the RSU's area form larger anonymity set as the occurrence of pseudonym change

is a regional event. In this case, not only the vehicles have context matching vehicles, but also overall, RSU triggers the changing event based on the traffic density. These triggers are effective because these are based on the surrounding environment of vehicle and adaptation to the traffic scenarios. TM becomes the prominent factor of unpredictability as it is completely random, and there is no beacon broadcast for initiating the process. Therefore, the Adversary is left with no information regarding the next pseudonym change. All these factors neutralize the placement strategies as these strategies would need prior knowledge or deterministic patterns in PCS to best place the attacking stations to eavesdrop a maximum number of vehicles. However, we noticed that despite the intelligent placements, the overall tracking remains very low. In Fig. 5.6, we examined the Highway Scenario that the general trend remains similar to Urban Scenario. CATA shows the lowest GTSR for Random placement with a minor increase in SBAP placement and then rises for DBAP. In the highway scenario, the traffic patterns are relatively more predictable. But the limited attacking stations in the large area keeps overall GTSR lower. It becomes easier for the vehicles to find the context matching vehicle as compared to the Urban scenario. The road network in the Urban scenario is complex while on the highway, the vehicles move in either of the two directions, and overall it increases the percentage of vehicles moving in the same direction with similar speed and

5.6 Conclusion

We presented a novel PCS to maximize the level of location privacy in Vehicular Ad hoc Networks. This PCS has two main components, namely, Context and Traffic pattern. When these properties are taken into consideration for PCS, the vehicle is less likely to change the pseudonym when the Adversary can easily de-identify the target vehicle. By keeping in mind, the intelligent adversaries, we have systematically developed CATA PCS by integrating the best possible situational and methodical aspects. For the development of this scheme, we introduce some changes to the architecture model. Typically, a set of pseudonyms is assigned by the Certificate Authority while

we consider that CA issues a seed for the pseudonym generation. By introducing this factor, we aim to eliminate the problem of the frequency of pseudonym change. Usually, due to a limited number of pseudonyms, the vehicle restricted to use pseudonyms in a way that expands the duration of pseudonym usage. Another important reason for introducing this mechanism is that it preserves the conditional privacy and accountability at a localized level, which means that RSU can detect the malicious activities regarding the identity of the vehicles such as impersonation attack. Therefore, this mechanism has twofold benefits; it allows a multitude of pseudonym changes while enabling the detection of malicious vehicles at the perimeter.

We carried out simulation runs in different traffic environments and in the presence of various adversary placements to assess PCS. To determine the effectiveness of our scheme, we compared our scheme with the existing schemes. Our evaluation quantifies the privacy of Users and Adversary's perspectives. We analyzed that our PCS not only outperforms other schemes by promising a higher level of anonymity but also prevent the intelligent adversaries from de-identifying the user with the least global tracking success rate in both Urban and Highway Scenarios.

Chapter 6

Conclusions and Future Directions

Conclusions

Privacy is a rising concern for vehicular communication. Intelligent Transportation System aims to increase road safety with this evolving technology. However, it should not be at the cost of the privacy of the driver. In the near future, the connectivity of vehicles with the environment will be a part of the larger smart city ecosystem. There are emerging standards across the globe for Vehicle-to-Everything communication. Embedding privacy in the design of these systems is paramount, as it will be difficult to sufficiently modify once the systems are deployed.

Privacy is a concept that is not only difficult to define precisely but also presents challenges in terms of quantification. When it comes to putting a number on for the measurement, the concrete level of privacy becomes very dependent on the underlying measurement factors as well as the context. In this dissertation, we have developed the framework for the equitable privacy assessment, which provides a systematic approach for evaluating PCSs. It aims to help the academic research community in the future development and assessment of PCSs. The industry standard bodies can utilize it as a systematic method for privacy assessment of vehicular communication. It facilitates the assessment and comparison of the PCSs with a consistent set of parameters, models and metrics.

One of the major concerns in the privacy assessment is poor adversary modelling. When evaluating privacy, we aim to check the resilience of PCS against the local passive adversary, with reasonable capabilities to take advantage of known traffic patterns and calculate vehicle trajectories. To address this issue, we proposed two intelligent adversary placements algorithms that use prior knowledge of traffic activity in the

area. The strength of the adversary has a direct impact on the assessment. Therefore, it is essential to incorporate the strong adversary models in the assessments.

Finally, yet importantly, our privacy assessments of existing schemes revealed several vulnerabilities and shortcomings. We have developed a new comprehensive PCS in which we addressed the limitations of existing PCSs. Our PCS is context-aware and traffic oriented that focuses on the maximum achievable anonymity in order to minimize successful tracking. The proposed scheme allows a large number of vehicles to change pseudonym simultaneously and prior to this change, the ideal situation is decided based on the context of the vehicles and traffic in that area. The adversary heavily relies on the prior information to deduce the pattern. By knowing when and how the pseudonyms are being changed, the adversary can estimate when the next pseudonym change will happen. To counteract this, we introduced random triggers to initiate the pseudonym change process. After the process is initiated, a chain of events are put in place to decide the suitable situation for pseudonym change, and the final pseudonym change becomes harder to track for the adversary. We assessed our PCS from the user and adversary standpoint and compared it with the existing PCSs. The results indicate that the proposed scheme outperforms existing schemes and successfully keeps the driver anonymous at a higher degree and shows the minimal rate of tracking.

Future Work

There are several experiment adaptations which can be performed by altering the models and parameters. Future work concerns the deeper analysis of PCSs with more sophisticated and diverse traffic models, which are based on real traffic data or synthetic traffic data that closely resembles the realistic traffic patterns. Further, each of the elements of the privacy assessment framework comprises a subset of parameters, and their variation may have minor to a significant impact on privacy. The future work with respect to the proposed PCS is the development of the overall system architecture in which the proposed PCS becomes an inherent part of the pseudonym

life cycle. Our work primarily focused on the segment where the pseudonyms are changed. Also, we used HMAC based pseudonym generation mechanism, which is different than the traditional pseudonym generation as a part of the pseudonym life cycle.

We have also identified some of the future directions which are out of the scope of this dissertation. These are some of the relevant issues that require further consideration in future work. Our scheme is supported by infrastructure units. Hence, there will be a requirement of a backup plan for the pseudonym changing scheme in places where there is no infrastructure unit, or the vehicle does not encounter RSU. Ideally, the vehicle should be able to change the pseudonym independently using a user-oriented scheme that has dynamic triggers such as a cooperative scheme. It is also necessary to tackle the misbehaving vehicles in the network. To address this issue, there is a requirement of methods to detect misbehaviour and steps to revoke pseudonyms. Once a vehicle is revoked, all the vehicles in the network need to be informed about the blacklisted vehicles and their identifiers. The infrastructure units in the network, as well as certificate authorities, do not fully attack resistant. Therefore, there is further study required for handling the compromised RSUs and CAs.

BIBLIOGRAPHY

[1] Autotalks combines dsrc and c-v2x on one chipset. *https://www.eenewsautomotive.com/news/autotalks-combines-dsrc-and-c-v2x-one-chipset*, Accessed: 21 January, 2020.

[2] Tapping into the connected cars market: What you need to know. *https://www.accesspartnership.com/tapping-into-the-connected-cars-market-what-you-need-to-know*, Accessed: 21 January, 2020.

[3] V2x (vehicle-to-everything). *https://www.towardsautonomy.com/v2xt*, Accessed: 13 February, 2020.

[4] Hannes Hartenstein and Kenneth Laberteaux. *VANET: vehicular applications and inter-networking technologies*, volume 1. John Wiley & Sons, 2009.

[5] Felipe Jiménez, José Eugenio Naranjo, José Javier Anaya, Fernando García, Aurelio Ponz, and José María Armingol. Advanced driver assistance system for road environments to improve safety and efficiency. *Transportation Research Procedia*, 14:2245–2254, 2016.

[6] John B Kenney. Dedicated short-range communications (dsrc) standards in the united states. *Proceedings of the IEEE*, 99(7):1162–1182, 2011.

[7] Patcharinee Tientrakool Theodore. L. Willke and Nicholas F. Maxemchuk. A survey of inter-vehicle communication protocols and their applications. *IEEE Communications Surveys Tutorials*, 11(2):3–20, 2009.

[8] Cellular vehicle-to-everything (c-v2x) enabling intelligent transport. *https://www.gsma.com/iot/wp-content/uploads/2017/12/C-2VX-Enabling-Intelligent-Transport*$_2$*.pdf*, *Accessed* : 12*December*, 2019.

[9] The v2x (vehicle-to-everything) communications ecosystem: 2019- 2030- opportunities, challenges, strategies forecasts. *https://sites.google.com/snstelecom.com/new-website/v2x*, Library Catalog: www.snstelecom.com, Accessed: 2 February, 2020.

[10] *IEEE P1609.4-2016/Cor1/D3, April 2019*, page 1–12, Sep 2019. IEEE P1609.4-2016/Cor1/D3, April 2019.

[11] George Dimitrakopoulos and Panagiotis Demestichas. Intelligent transportation systems. *IEEE Vehicular Technology Magazine*, 5(1):77–84, 2010.

[12] Contreras-Castillo J. Guerrero-Ibáñez J, Zeadally S. Sensor technologies for intelligent transportation systems. Sensors (Basel), 2018 April 16. doi:10.3390/s18041212.

[13] Ian Goldberg, David Wagner, and Eric Brewer. Privacy-enhancing technologies for the internet. In *Proceedings IEEE COMPCON 97. Digest of Papers*, pages 103–109. IEEE, 1997.

[14] The United Nations. *Universal Declaration of Human Rights*. December 1948.

[15] David Banisar and Simon Davies. Privacy and data protection around the world. In *21st International Conference on Privacy and Personal Data Protection*, september 1999. http://www.pco.org.hk/conproceed.html.

[16] Masooda Bashir, Carol Hayes, April D Lambert, and Jay P Kesan. Online privacy and informed consent: The dilemma of information asymmetry. *Proceedings of the Association for Information Science and Technology*, 52(1):1–10, 2015.

[17] Florian Dötzer. Privacy issues in vehicular ad hoc networks. In George Danezis and David Martin, editors, *Privacy Enhancing Technologies*, page 197–209. Springer Berlin Heidelberg, 2006.

[18] Draft SAE. J2735 dedicated short range, communications (dsrc) message set dictionary, jun. 12, 2006, 167 pages, the engineering society for advancing mobility land sea air and space international. *Society of Automotive Engineers, Inc. USA*.

[19] Hassan Artail and Noor Abbani. A pseudonym management system to achieve anonymity in vehicular ad hoc networks. *IEEE Transactions on Dependable and Secure Computing*, 13(1):106–119, Jan 2016.

[20] William Whyte, André Weimerskirch, Virendra Kumar, and Thorsten Hehn. A security credential management system for v2v communications. Vehicular Networking Conference (VNC), 2013 IEEE, pages 1–8. IEEE, 2013.

[21] Julien Freudiger, Maxim Raya, Márk Félegyházi, Panos Papadimitratos, and Jean-Pierre Hubaux. Mix-zones for location privacy in vehicular networks. Number LCA-CONF-2007-016 in ACM Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS), 2007.

[22] Abdelwahab Boualouache and Samira Moussaoui. S2si: A practical pseudonym changing strategy for location privacy in vanets. Advanced Networking Distributed Systems and Applications (INDS), 2014 International Conference on, pages 70–75. IEEE, 2014.

[23] Jean-Pierre Hubaux, Srdjan Capkun, and Jun Luo. The security and privacy of smart vehicles. *IEEE Security & Privacy*, 2(3):49–55, 2004.

[24] David Rebollo-Monedero, Javier Parra-Arnau, Claudia Diaz, and Jordi Forné. On the measurement of privacy as an attacker's estimation error. *International journal of information security*, 12(2):129–149, 2013.

[25] Saif Al-Sultan, Moath M Al-Doori, Ali H Al-Bayatti, and Hussien Zedan. A comprehensive survey on vehicular ad hoc network. *Journal of network and computer applications*, 37:380–392, 2014.

[26] John Krumm. A survey of computational location privacy. *Personal and Ubiquitous Computing*, 13(6):391–399, 2009.

[27] Zhendong Ma, Frank Kargl, and Michael Weber. Measuring location privacy in v2x communication systems with accumulated information. Mobile Adhoc and Sensor Systems, 2009. MASS'09. IEEE 6th International Conference on, pages 322–331. IEEE, 2009.

[28] Amer Aijaz, Bernd Bochow, Florian Dötzer, Andreas Festag, Matthias Gerlach, Rainer Kroh, and Tim Leinmüller. Attacks on inter vehicle communication systems-an analysis. *Proc. WIT*, pages 189–194, 2006.

[29] Marius Wernke, Pavel Skvortsov, Frank Dürr, and Kurt Rothermel. A classification of location privacy attacks and approaches. *Personal and ubiquitous computing*, 18(1):163–175, 2014.

[30] Abdelwahab Boualouache, Sidi-Mohammed Senouci, and Samira Moussaoui. A survey on pseudonym changing strategies for vehicular ad-hoc networks. *IEEE Communications Surveys & Tutorials*, 2017.

[31] Emanuel Fonseca, Andreas Festag, Roberto Baldessari, and Rui L Aguiar. Support of anonymity in vanets-putting pseudonymity into practice. Wireless Communications and Networking Conference, 2007. WCNC 2007. IEEE, pages 3400–3405. IEEE, 2007.

[32] Jonathan Petit, Florian Schaub, Michael Feiri, and Frank Kargl. Pseudonym schemes in vehicular networks: A survey. *IEEE communications surveys & tutorials*, 17(1):228–255, 2015.

[33] Rongxing Lu, Xiaodong Lin, Haojin Zhu, P-H Ho, and Xuemin Shen. Ecpp: Efficient conditional privacy preservation protocol for secure vehicular communications. INFOCOM 2008. The 27th Conference on Computer Communications. IEEE, pages 1229–1237. IEEE, 2008.

[34] Ubaidullah Rajput, Fizza Abbas, and Heekuck Oh. A hierarchical privacy preserving pseudonymous authentication protocol for vanet. *IEEE Access*, 4:7770–7784, 2016.

[35] Andreas Pfitzmann and Marit Hansen. A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management, 2009.

[36] David Eckhoff and Christoph Sommer. Marrying safety with privacy: A holistic solution for location privacy in vanets. In *2016 IEEE Vehicular Networking Conference (VNC)*, pages 1–8. IEEE, 2016.

[37] Benedikt Brecht, Dean Therriault, André Weimerskirch, William Whyte, Virendra Kumar, Thorsten Hehn, and Roy Goudy. A security credential management system for v2x communications. *IEEE Transactions on Intelligent Transportation Systems*, pages 1–22, 2018.

[38] Panagiotis Papadimitratos, Levente Buttyan, Tamás Holczer, Elmar Schoch, Julien Freudiger, Maxim Raya, Zhendong Ma, Frank Kargl, Antonio Kung, and Jean-Pierre Hubaux. Secure vehicular communication systems: design and architecture. *IEEE Communications Magazine*, 46(11), 2008.

[39] Zhendong Ma, Frank Kargl, and Michael Weber. Pseudonym-on-demand: a new pseudonym refill strategy for vehicular communications. Vehicular Technology Conference, 2008. VTC 2008-Fall. IEEE 68th, pages 1–5. IEEE, 2008.

[40] Florian Schaub, Frank Kargl, Zhendong Ma, and Michael Weber. V-tokens for conditional pseudonymity in vanets. Wireless Communications and Networking Conference (WCNC), 2010 IEEE, pages 1–6. IEEE, 2010.

[41] Adi Shamir. Identity-based cryptosystems and signature schemes. Workshop on the theory and application of cryptographic techniques, pages 47–53. Springer, 1984.

[42] Shushan Zhao, Akshai Aggarwal, Richard Frost, and Xiaole Bai. A survey of applications of identity-based cryptography in mobile ad-hoc networks. *IEEE Communications Surveys & Tutorials*, 14(2):380–400, 2012.

[43] Chris Lai, Henry Chang, and Chei Chung Lu. A secure anonymous key mechanism for privacy protection in vanet. Intelligent Transport Systems Telecommunications,(ITST), 2009 9th International Conference on, pages 635–640. IEEE, 2009.

[44] Giorgio Calandriello, Panos Papadimitratos, Jean-Pierre Hubaux, and Antonio Lioy. Efficient and robust pseudonymous authentication in vanet. Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks, pages 19–28. ACM, 2007.

[45] Krishna Sampigethaya, Leping Huang, Mingyan Li, Radha Poovendran, Kanta Matsuura, and Kaoru Sezaki. Caravan: Providing location privacy for vanet. Technical report, Washington Univ Seattle Dept Of Electrical Engineering, 2005.

[46] Krishna Sampigethaya, Mingyan Li, Leping Huang, and Radha Poovendran. Amoeba: Robust location privacy scheme for vanet. *IEEE Journal on Selected Areas in communications*, 25(8), 2007.

[47] Yong Xi, Kewei Sha, Weisong Shi, Loren Schwiebert, and Tao Zhang. Enforcing privacy using symmetric random key-set in vehicular networks. Autonomous Decentralized Systems, 2007. ISADS'07. Eighth International Symposium on, pages 344–351. IEEE, 2007.

[48] Kewei Sha, Yong Xi, Weisong Shi, Loren Schwiebert, and Tao Zhang. Adaptive privacy-preserving authentication in vehicular networks. Communications and Networking in China, 2006. ChinaCom'06. First International Conference on, pages 1–8. IEEE, 2006.

[49] Chenxi Zhang, Xiaodong Lin, Rongxing Lu, and P-H Ho. Raise: An efficient rsu-aided message authentication scheme in vehicular communication networks. Communications, 2008. ICC'08. IEEE International Conference on, pages 1451–1457. IEEE, 2008.

[50] Christine Laurendeau and Michel Barbeau. Secure anonymous broadcasting in vehicular networks. Local Computer Networks, 2007. LCN 2007. 32nd IEEE Conference on, pages 661–668. IEEE, 2007.

[51] Mohammed Saeed Al-Kahtani. Survey on security attacks in vehicular ad hoc networks (vanets). Signal Processing and Communication Systems (ICSPCS), 2012 6th International Conference on, pages 1–9. IEEE, 2012.

[52] Yasser Toor, Paul Muhlethaler, and Anis Laouiti. Vehicle ad hoc networks: Applications and related technical issues. *IEEE communications surveys & tutorials*, 10(3), 2008.

[53] Hannes Hartenstein and LP Laberteaux. A tutorial survey on vehicular ad hoc networks. *IEEE Communications magazine*, 46(6), 2008.

[54] Elmar Schoch, Frank Kargl, and Michael Weber. Communication patterns in vanets. *IEEE Communications Magazine*, 46(11), 2008.

[55] Georgios Karagiannis, Onur Altintas, Eylem Ekici, Geert Heijenk, Boangoat Jarupan, Kenneth Lin, and Timothy Weil. Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions. *IEEE communications surveys & tutorials*, 13(4):584–616, 2011.

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

[57] Mohammed Erritali and Bouabid El Ouahidi. A review and classification of various vanet intrusion detection systems. Security Days (JNS3), 2013 National, pages 1–6. IEEE, 2013.

[58] Jie Zhang. A survey on trust management for vanets. Advanced information networking and applications (AINA), 2011 IEEE international conference on, pages 105–112. IEEE, 2011.

[59] Marshall Riley, Kemal Akkaya, and Kenny Fong. A survey of authentication schemes for vehicular ad hoc networks. *Security and Communication Networks*, 4(10):1137–1152, 2011.

[60] Florian Schaub, Zhendong Ma, and Frank Kargl. Privacy requirements in vehicular communication systems. volume 3 of *Computational Science and Engineering, 2009. CSE'09. International Conference on*, pages 139–145. IEEE, 2009.

[61] Maxim Raya and Jean-Pierre Hubaux. Securing vehicular ad hoc networks. *Journal of Computer Security*, 15(1):39–68, 2007.

[62] Björn Wiedersheim, Zhendong Ma, Frank Kargl, and Panos Papadimitratos. Privacy in inter-vehicular networks: Why simple pseudonym change is not enough. Wireless On-demand Network Systems and Services (WONS), 2010 Seventh International Conference on, pages 176–183. IEEE, 2010.

[63] Levente Buttyán, Tamás Holczer, and István Vajda. On the effectiveness of changing pseudonyms to provide location privacy in vanets. European Workshop on Security in Ad-hoc and Sensor Networks, pages 129–141. Springer, 2007.

[64] Alastair R Beresford and Frank Stajano. Location privacy in pervasive computing. *IEEE Pervasive computing*, 2(1):46–55, 2003.

[65] Antonio M Carianha, Luciano Porto Barreto, and George Lima. Improving location privacy in mix-zones for vanets. Performance Computing and Communications Conference (IPCCC), 2011 IEEE 30th International, pages 1–6. IEEE, 2011.

[66] Florian Scheuer, Karl-Peter Fuchs, and Hannes Federrath. A safety-preserving mix zone for vanets. International Conference on Trust, Privacy and Security in Digital Business, pages 37–48. Springer, 2011.

[67] Lei Zhang. Otibaagka: A new security tool for cryptographic mix-zone establishment in vehicular ad hoc networks. *IEEE Transactions on Information Forensics and Security*, 12(12):2998–3010, 2017.

[68] Rongxing Lu, Xiaodong Lin, Tom H Luan, Xiaohui Liang, and Xuemin Shen. Anonymity analysis on social spot based pseudonym changing for location privacy in vanets. Communications (ICC), 2011 IEEE International Conference on, pages 1–5. IEEE, 2011.

[69] Abdelwahab Boualouache, Sidi-Mohammed Senouci, and Samira Moussaoui. Towards an efficient pseudonym management and changing scheme for vehicular ad-hoc networks. Global Communications Conference (GLOBECOM), 2016 IEEE, pages 1–7. IEEE, 2016.

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

[71] Bidi Ying, Dimitrios Makrakis, and Hussein T Mouftah. Dynamic mix-zone for location privacy in vehicular networks. *IEEE Communications Letters*, 17(8):1524–1527, 2013.

[72] Bidi Ying and Dimitrios Makrakis. Pseudonym changes scheme based on candidate-location-list in vehicular networks. Communications (ICC), 2015 IEEE International Conference on, pages 7292–7297. IEEE, 2015.

[73] Qasim Ali Arain, Zhongliang Deng, Imran Memon, Asma Zubedi, Jichao Jiao, Aisha Ashraf, and Muhammad Saad Khan. Privacy protection with dynamic pseudonym-based multiple mix-zones over road networks. *China Communications*, 14(4):89–100, 2017.

[74] Balaji Palanisamy and Ling Liu. Mobimix: Protecting location privacy with mix-zones over road networks. Data Engineering (ICDE), 2011 IEEE 27th International Conference on, pages 494–505. IEEE, 2011.

[75] Balaji Palanisamy, Ling Liu, Kisung Lee, Aameek Singh, and Yuzhe Tang. Location privacy with road network mix-zones. Mobile Ad-hoc and Sensor Networks (MSN), 2012 Eighth International Conference on, pages 124–131. IEEE, 2012.

[76] Balaji Palanisamy, Sindhuja Ravichandran, Ling Liu, Binh Han, Kisung Lee, and Calton Pu. Road network mix-zones for anonymous location based services. Data Engineering (ICDE), 2013 IEEE 29th International Conference on, pages 1300–1303. IEEE, 2013.

[77] Balaji Palanisamy and Ling Liu. Attack-resilient mix-zones over road networks: architecture and algorithms. *IEEE Transactions on Mobile Computing*, 14(3):495–508, 2015.

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

[79] Mingyan Li, Krishna Sampigethaya, Leping Huang, and Radha Poovendran. Swing & swap: user-centric approaches towards maximizing location privacy. Proceedings of the 5th ACM workshop on Privacy in electronic society, pages 19–28. ACM, 2006.

[80] Matthias Gerlach and Felix Guttler. Privacy in vanets using changing pseudonyms-ideal and real. Vehicular Technology Conference, 2007. VTC2007-Spring. IEEE 65th, pages 2521–2525. IEEE, 2007.

[81] Jianxiong Liao and Jianqing Li. Effectively changing pseudonyms for privacy protection in vanets. Pervasive Systems, Algorithms, and Networks (ISPAN), 2009 10th International Symposium on, pages 648–652. IEEE, 2009.

[82] David Eckhoff, Christoph Sommer, Tobias Gansen, Reinhard German, and Falko Dressler. Strong and affordable location privacy in vanets: Identity diffusion using time-slots and swapping. Vehicular Networking Conference (VNC), 2010 IEEE, pages 174–181. IEEE, 2010.

[83] Joo-Han Song, Vincent WS Wong, and Victor CM Leung. Wireless location privacy protection in vehicular ad-hoc networks. *Mobile Networks and Applications*, 15(1):160–171, 2010.

[84] Levente Buttyán, Tamás Holczer, André Weimerskirch, and William Whyte. Slow: A practical pseudonym changing scheme for location privacy in vanets. Vehicular Networking Conference (VNC), 2009 IEEE, pages 1–8. IEEE, 2009.

[85] Christoph Sommer-Falko Dressler David Eckhoff, Reinhard German and Tobias Gansen. Slotswap: strong and affordable location privacy in intelligent transportation systems. *IEEE Communications Magazine*, 49(11), 2011.

[86] Yuanyuan Pan and Jianqing Li. Cooperative pseudonym change scheme based on the number of neighbors in vanets. *Journal of Network and Computer Applications*, 36(6):1599–1609, 2013.

[87] Abdelwahab Boualouache and Samira Moussaoui. Tapcs: Traffic-aware pseudonym changing strategy for vanets. *Peer-to-Peer Networking and Applications*, 10(4):1008–1020, 2017.

[88] Albert Wasef and Xuemin Sherman Shen. Rep: Location privacy for vanets using random encryption periods. *Mobile Networks and Applications*, 15(1):172–185, 2010.

[89] Hesiri Weerasinghe, Huirong Fu, Supeng Leng, and Ye Zhu. Enhancing unlinkability in vehicular ad hoc networks. Intelligence and Security Informatics (ISI), 2011 IEEE International Conference on, pages 161–166. IEEE, 2011.

[90] Robert J. Fitzgerald. Development of practical pda logic for multitarget tracking by microprocessor. In *1986 American Control Conference*, pages 889–898, June 1986.

[91] Kalman and Rudolph Emil. A new approach to linear filtering and prediction problems. *Journal of basic Engineering*, 82(1):35–45, 1960.

[92] Karim Emara, Wolfgang Woerndl, and Johann Schlichter. Vehicle tracking using vehicular network beacons. In *2013 IEEE 14th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM)*, pages 1–6, June 2013.

[93] Florian Scheuer, Karl-Peter Fuchs, and Hannes Federrath. A safety-preserving mix zone for vanets. In *Proceedings of the 8th International Conference on Trust, Privacy and Security in Digital Business*, TrustBus'11, page 37–48, Berlin, Heidelberg, 2011. Springer-Verlag.

[94] Andrei Serjantov and George Danezis. Towards an information theoretic metric for anonymity. In *Proceedings of the 2Nd International Conference on Privacy Enhancing Technologies*, PET'02, pages 41–53, Berlin, Heidelberg, 2003. Springer-Verlag. http://dl.acm.org/citation.cfm?id=1765299.1765303.

[95] Claude E. Shannon and Warren Weaver. *A Mathematical Theory of Communication*. University of Illinois Press, Champaign, IL, USA, 1963.

[96] András Varga and Rudolf Hornig. An overview of the omnet++ simulation environment. In *Proceedings of the 1st International Conference on Simulation Tools and Techniques for Communications, Networks and Systems & Workshops*, Simutools '08, pages 60:1–60:10, ICST, Brussels, Belgium, Belgium, 2008. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering). http://dl.acm.org/citation.cfm?id=1416222.1416290.

[97] Pablo Alvarez Lopez, Michael Behrisch, Laura Bieker-Walz, Jakob Erdmann, Yun-Pang Flötteröd, Robert Hilbrich, Leonhard Lücken, Johannes Rummel, Peter Wagner, and Evamarie Wießner. Microscopic traffic simulation using sumo. In *The 21st IEEE International Conference on Intelligent Transportation Systems*. IEEE, 2018. ¡https://elib.dlr.de/124092/.

[98] Karim Emara. Poster: Prext: Privacy extension for veins vanet simulator. In *2016 IEEE Vehicular Networking Conference (VNC)*, pages 1–2, Dec 2016.

[99] Hermann S. Lichte and Jannis Weide. Modeling obstacles in inet/mobility framework: Motivation, integration, and performance. In *Proceedings of the 2nd International Conference on Simulation Tools and Techniques*, Simutools '09, Brussels, BEL, 2009. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering). https://doi.org/10.4108/ICST.SIMUTOOLS2009.5680.

[100] Christoph Sommer, Reinhard German, and Falko Dressler. Bidirectionally coupled network and road traffic simulation for improved ivc analysis. *IEEE Transactions on Mobile Computing*, 10(1):3–15, Jan 2011.

[101] Karim Emara, Wolfgang Wörndl, and Johann H. Schlichter. Caps: context-aware privacy scheme for vanet safety applications. In *WISEC*, 2015.

[102] Openstreetmap. *https://www.openstreetmap.org/copyright*, Accessed: 5-January-2020.

[103] Hugo Krawczyk, Mihir Bellare, and Ran Canetti. Rfc2104: Hmac: Keyed-hashing for message authentication. 1997.

VITA AUCTORIS

Ikjot Saini was born in India in 1992. She obtained her Bachelor of Technology in Computer Science and Engineering from Rajasthan Technical University and Master of Technology in Computer Science and Engineering from Lovely Professional University in 2013 and 2015, respectively. Before starting her Ph.D. program in 2016, she completed One-Year Ontario College Graduate Certificate Program of Information Security Management from Fanshawe College in 2016. Her recent research interests are VANET Cybersecurity and Privacy, Location Tracking, V2X technology, Security Credential Management System, Connected and Autonomous Vehicle Security, and Network Security.