Towards Vehicle-to-Infrastructure Connectivity, Location Privacy and Trust Management in Vehicular Networks

Pranav Kumar Singh

Towards Vehicle-to-Infrastructure Connectivity, Location Privacy and Trust Management in Vehicular Networks

Thesis submitted in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

by

Pranav Kumar Singh

Under the Supervision of

Professor Sukumar Nandi

Department of Computer Science and Engineering
INDIAN INSTITUTE OF TECHNOLOGY GUWAHATI
Guwahati 781039, India
February 2021

In Memory of

Nana ji, Dada ji and Bade Pita ji

Dedicated to

My Teachers, Parents, Brothers, Wife and Son

For their blessings, constant inspiration, and love

Declaration

I certify that

a. The work contained in this thesis is original, and has been done by myself under the general supervision of my supervisor.

b. The work has not been submitted to any other institute for any degree or diploma.

c. Whenever I have used materials (data, theoretical analysis, results) from other sources, I have given due credit to them by citing them in the text of the thesis and giving their details in the references.

d. Whenever I have quoted written materials from other sources, I have put them under quotation marks and given due credit to the sources by citing them and giving required details in the references.

Place: IIT Guwahati
Date:

Pranav Kumar Singh
Research Scholar
Department of Computer Science
and Engineering,
Indian Institute of Technology Guwahati,
Guwahati 781039, India.

CERTIFICATE

*This is to certify that this thesis entitled "**Towards Vehicle-to- Infrastructure Connectivity, Location Privacy and Trust Management in Vehicular Networks**" being submitted by Mr. Pranav Kumar Singh to the Department of Computer Science and Engineering, Indian Institute of Technology Guwahati, is a record of bona fide research work under my supervision and is worthy of consideration for the award of the degree of Doctor of Philosophy of the Institute.*

The results contained in this thesis have not been submitted in part or full to any other university or institute for the award of any degree or diploma.

Place: IIT Guwahati

Date:

Professor Sukumar Nandi
Department of Computer Science and Engineering,
Indian Institute of Technology Guwahati,
Guwahati 781039, India.

Acknowledgements

At the very outset of submission of this thesis, I would like to extend my sincere thanks with a deep sense of gratitude to all who have helped and supported me directly or indirectly during my PhD process.

First, and most importantly, I want to thank my supervisor Prof. Sukumar Nandi Sir for his guidance throughout my PhD. I consider myself extremely fortunate to be supervised by the Sir. Sir has provided me all the support and given me the freedom to explore and pursue my research. He ensured that I do not deviate from my goal and the core of my research. I loved attending his classes, which helped me a lot in understanding the basics and advanced concepts of my selected research domains. His discussions on several other issues have helped me to grow professionally, which will be of the most generous help in my future career. I will always be thankful for all that I learned from him.

I also want to thank my Doctoral Committee members, Dr. Sanasam Ranbir Singh, Dr. John Jose, and Dr. Ashok Singh Sairam for their valuable comments and suggestions during my PhD. Dr John Sir's motivational lectures can never be forgotten, which has always inspired me to give my best throughout my PhD. I am grateful to Dr. Ranbir Sir for his helpful comments and constructive criticism throughout this entire process. I can never forget Dr. Ashok Sir's friendly nature, which helped me a lot during my progress. I have been fortunate to have such members in my Doctoral Committee. My thesis has been improved substantially from their insightful recommendations.

I am thankful to my host organization, Central Institute of Technology Kokrajhar for allowing me to carry out research work at IIT Guwahati by granting me QIP leave. A special thanks goes to Former Director CITK Prof. Mohammad Jawed Sir. I also want to thank present Director, and Registrar CITK. I have great pleasure in acknowledging my gratitude to all my colleagues, staff members, and students at CITK for their continuous support. Bundle of thanks also goes to all my colleagues in the Department of CSE, CITK for their support, advices and their friendship over the years. A special thanks to former Head, CSE Dr. Pankaj Pratap Singh and present Head CSE, CITK Dr. Amitava Nag for their support and encouragement.

Next, I would also like to express my sincere gratitude to the Director, the Deans, and other management of IIT Guwahati, whose collective effort

has made this institute a place for world-class studies and research. I am thankful to all the faculties, and the staffs of the Department of CSE for their cooperation and support. A special thanks to former Head CSE Prof. S. V. Rao and present Head CSE Prof. Jatindra Kumar Deka for their valuable support. Bundle of thanks also goes to B.Tech and M.Tech Students and research scholars of this institute, with whom I have closely worked.

I am indebted to all my friends and collaborators, Sunit, Roshan, Prof. Rawat, Dr. Kayhan, Sahil, Shivram, Tamilselvan, Anup, and Gaurav for helping me to complete this work. I am thankful to all my friends Sisir, Brijesh, Abhijit, Vijay, Arunangshu, Shrestha, Madhurima, Sikha, Partha, Subrata, Neelakshi, Palash, Aparajita, Anasua, Sheel, Pradeep, Ujjwal, Anirban, and Sukanta, for their support and to create a delightful learning ambiance. I am thankful to my seniors Rakesh Sir, Subhrendu Bhaiya, Niladri Da, and Satish Bhaiya for all their help and support. I owe thanks to a few special persons during my stay at IITG Nilima Nandi Ma'am and Sunit for their love and care towards me, Sisir, Lipa Bhabhi, and Duggu for their love and support and for considering me as their family member. I am lucky to have them in my life. I thank the doctors team and medical staffs at IITG for their healthcare services. A special thanks goes to Library and Computer Centre staffs for their support and making all the resources available to us for learning.

I feel a deep sense of gratitude for my teachers who taught me good things and making me what I am today. My heartfelt regards go to my Badi Amma, Uncles, Aunties, Mama, Maami, Mausa, Mausi, Bhaiya, Bhabhi, brothers, sisters, father-in-law, mother-in-law, nephews, nieces, Lalit, Amit, Rishabh, Jaya, Aadarsh, Puja, and Anurag for their love and support. I want to express my gratitude to my grandmother for her love and prayers. I am also grateful to my school and college friends for their love, and constant encouragement.

I appreciate my adorable son Arnav and my caring wife Neha for their sacrifice and patience throughout this PhD. Thanks for believing in me and supporting me during this long and challenging journey. In all those difficult moments, their smiles and embraces served as a booster, braced me to get back to work. Thank you for the special prayers that you made for me to complete this work. I am lucky to have such a lovely and caring family standing beside me with their unconditional love and support.

Finally, I would like to extend my heartiest gratitude to my parents, who mean a lot to me. I want to thank them for supporting me and showing

their faith in me. Thank you for your endless prayers and fast that you keep for me. I salute my parents for their selfless love, care and sacrifices. Both of you are very special and like God to me.

Place: IIT Guwahati
Date:

Pranav Kumar Singh

Abstract

The vehicular network is in its flourished stage, and its various applications related to safety, traffic efficiency, and infotainment have made it more appealing. Due to its unique applications and features, it is one of the leading research areas (under the various names of Internet of Vehicles (IoV), Vehicular Communication, Vehicular Adhoc Networks (VANETs)) of recent times, with the USA, Europe, and Japan as its leading participants. It has drawn considerable attention from academia, industry, and governments. In our recent survey, we find that providing seamless vehicle-to-infrastructure connectivity, dealing with security and privacy threats, and managing the trust are major concerns to widespread adoption of a vehicular network. This thesis explores the vehicular network in detail, associated challenges, existing solutions from the research community and standardization bodies, state-of-the-art solutions, and future research directions. The work in this thesis focuses on three key challenges related to seamless vehicle-to-infrastructure connectivity, location privacy, and trust management.

In this thesis, first, we present details (architecture, applications, key enablers, protocol stacks) of a vehicular network domain and highlight the major challenges. The first contribution of the thesis is towards the vehicle-to-infrastructure (V2I) connectivity issues. V2I connectivity enables a variety of safety, infotainment, and mobility applications. However, most of these applications require "always best and seamless connectivity," which constitutes a key challenge in the context of available radio access and core network technologies. We explore the amalgamation of the software-defined network and multipath TCP (MPTCP) in addressing the challenges. We test the performance of MPTCP for V2I connectivity in SDN controlled small cells of DSRC and Wi-Fi using the Mininet-WiFi emulator. The study identifies the advantages and issues in the integration of these two technologies. We highlight our observations that can significantly benefit V2I connectivity in small cells. We propose solutions to V2I connectivity in the software-defined vehicular network with MPTCP and highlighted future research directions in this domain.

The second contribution of the thesis is towards the location privacy issues

in a vehicular network. Preserving location privacy is an essential aspect of a vehicular network. First, we propose a scheme called masqueraded probabilistic flooding for source-location privacy (MPFSLP) that provides non-repudiation, message authentication, integrity, and non-traceability to a great extent. We also propose a second scheme named cooperative pseudonym exchange and scheme permutation (CPESP) with the same objective. The first scheme leverages the fact that an endpoint only requires the knowledge of the location and velocity of another endpoint and not its identity; thereby, our mechanism introduces confusion in the mapping form identity of nodes to packets. The second scheme leverages the idea of exchanging the pseudonyms and using multiple pseudonym change schemes, thereby protecting nodes from being tracked by the network operator and eavesdroppers. We test these two proposed schemes on the PREXT simulator and find that the first scheme reduces traceability by 6× compared to baseline pseudonym changing schemes. The second scheme also performs well in comparison to baseline schemes.

In this thesis, we also address another important challenge, trust management issue in a vehicular network. We propose a blockchain-based decentralized trust management system to address the critical challenges of existing and traditional centralized and decentralized solutions. We use smart contract to automate the process and implement accessibility and decentralized control and decision making. We introduce the concept of blockchain sharding to efficiently maintain and update reliable and consistent trust values across the network. We introduce an incentive scheme concept to encourage peers to perform well. We also conduct testbed-based experiments, which demonstrate the implementation feasibility of proposed mechanisms in the real world. With the proposed system, we achieve most of our design goals of decentralization, transparency, security scalability, reliability, availability, and resilience to failures.

Contents

List of Figures

List of Tables

List of Algorithms

List of Abbreviations

5G	5th Generation Mobile Network
ANDSF	Access Network Discovery and Selection Function
BSM	Basic Safety Message
CA	Certificate Authority
CAM	Co-operative Awareness Message
C-ITS	Co-operative ITS
DENM	Decentralized Environmental Notification Message
DSRC	Dedicated Short Range Communication
HetNet	Heterogeneous networks
IoV	Internet of Vehicles
ITS	Intelligent Transportation System
LTE-A	LTE Advanced
MA	Misbehavior authority
MIH	Media Independent Handover
MPTCP	MultiPath TCP
OBU	Onboard Unit
PKI	Public Key Infrastructure
PCA	Pseudonym Certificate Authority
QoS	Quality of Service
QoE	Quality of Experience
RA	Registration Authority
RSU	Roadside Unit
SDN	Software-Defined Networking
VANET	Vehicular Ad hoc Network
V2V	Vehicle-to-Vehicle
V2I	Vehicle-to-Infrastructure
WAVE	Wireless Access for Vehicular Environment

Chapter 1

Introduction

The increasing number of road accidents worldwide has motivated the research communities and automotive industries to propose solutions for road safety. Vehicular communication networks have been developed to connect vehicles wirelessly to provide road safety, improve traffic flow, and offer driving comfort. Indeed, the vehicular network enables various safety and non-safety applications and Intelligent Transportation System (ITS) services. In recent years, various advancements in the traditional Vehicular ad hoc networks (VANETs) [16] (initially driven by Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication) have drawn considerable attention from both academia and industry. In the Internet of Everything (IoE) era [17], the traditional VANETs have evolved to the Internet of Vehicles (IoV) [18]. As shown in Figure 1.1, in the IoV concept of vehicular networks, the smart and intelligent vehicles connect not only to other vehicles and roadside units but also to any entity such as pedestrians, networks, satellite, UAVs, gas stations, charging stations, clouds, etc. via the Vehicle-to-Everything (V2X) or Cellular Vehicle-to-Everything (C-V2X) technologies [19].

IoV is expected to solve the major challenges of our transportation by improving road safety, minimizing road congestion, reducing fuel consumption and CO2

Figure 1.1: Internet of Vehicles

emissions, solving parking issues, and minimizing expenses and space by enabling cab sharing, etc. The phenomenal advancements in vehicle's on-board capabilities (sensing, computation, storage, communication), network architectures, protocols, Radio Access Technologies (RATs) have enabled automated driving and platooning [20]. These advancements brought IoV to the center of Industry 4.0. and led to promising areas of intelligent transportation, vehicle manufacturing, payment services, predictive maintenance, usage-based insurance, intelligent parking, automation, infotainment, over-the-air software update, secure data sharing, data trading, vehicle life-cycle, etc. [18].

These promising IoV applications have varying Quality of Service (QoS) requirements. To support the diverse QoS requirements various RATs have been developed and some are under development, such as DSRC/IEEE 802.11p, IEEE 802.11 Next-Generation V2X (NGV) (amendments being prepared as IEEE 802.11bd) [21], WiFi, 4G, new 5G radio (NR), 6G [22], white space TV, millimeter

wave (mmWave) and Visible Light Communications (VLC) [23]. Three dedicated protocol stacks have been developed over DSRC to enable vehicular communications in the USA, Europe, and Japan, which are known as Connected Vehicle (WAVE), the Cooperative-ITS (C-ITS), and the ARIB STD-T109, respectively.

1.1 Challenges

The opportunities and benefits of deploying a vehicle network are enormous. However, a realistic and closer look at the existing protocol stack, security, trust, and privacy mechanisms reveals multiple issues. The vehicular network differs in terms of its connectivity, security, privacy, and trust requirements due to the network layout and dynamics, which calls for specialized mechanisms to cater to its needs.

1.1.1 Seamless V2I Connectivity

ITS has become an essential part of smart cities these days. We need seamless V2I/I2V connectivity to fulfill the QoS requirements of different ITS services. Vehicles must be enabled to run applications and use services seamlessly. Providing seamless V2I connectivity in a vehicular network with rapid topological changes, random vehicle speed, and variable node density is very challenging. The major challenges due to these characteristics are as follows.

- Dynamic topology: The vehicular network topology is highly dynamic in nature [24]. Vehicles in an urban scenario can have a velocity up to 50 km/h and more than 100 km/h on the highway. Vehicles can take different routes to their destination. The discovery of an appropriate target cell at high speed is a challenging task. The change in route and velocity may lead to frequent link disruption and disconnection.

- Radio Propagation: The radio propagation characteristics such as reflection, interference, multipath fading, and congestion also vary with mobility scenarios, affecting the overall performance. The frequently and time-varying radio wave propagation channel can create a dynamic scattering environment [25].

- Varying Density: The vehicular node density varies in a spatial-temporal manner, leading to dynamic variation in vehicular network connectivity such as sparse, semi-sparse, and dense networks. For example, during peak hours or traffic jam, a large number of vehicles can generate a heavy load on certain cells. In these extreme conditions the network may frequently disconnect and degrade the overall network performance [26].

- QoS Requirements: Providing QoS which is sufficient to meet different application (real-time, VoIP, audio, safety-related, etc.) requirements (delay, jitter, throughput) is one of the biggest challenges. The use of a single RAT may not be able to support various applications with diverse QoS requirements. Utilizing different RATs simultaneously, such as the combination of cellular (4G, 5G), Wi-Fi, and IEEE 802.11p/DSRC to meet the diversified QoS requirements, is expected to be a good solution [27]. However, it has not yet been widely explored. Cognitive radio-enabled vehicular communication in HetNets is another aspect that enables sensing, analyzing, and accessing the radio spectrum opportunities dynamically. Cognitive radio-enabled vehicular communication in HetNets [28–31] is another aspect that can enable sensing, analyzing, and accessing the radio spectrum opportunities dynamically. However, the main obstacles in adopting cognitive vehicular networks are interference (interference to primary users and due to other networks), mobility (speed and direction badly affect the performance), security, and privacy.

1.1.2 Preserving Location Privacy

A particular facet of vehicular networks is its beaconing mechanism, wherein each vehicle periodically broadcasts its position and velocity information. This knowledge is helpful for traffic management: mitigating traffic congestion, mitigating accidents, etc. [32]. However, there are multiple security issues with these beacon messages which need to be addressed. First, the beacon messages must have a mechanism to ensure their integrity as well as to authenticate them. Otherwise, an adversary can generate fake messages or alter messages to disrupt traffic flow. Second, a legal authority should be able to link a message to its sender in case of dispute; in other words, the system must ensure non-repudiation of messages. This is to ensure that the law is able to find out the misbehaving peer when some party sends fake messages or doesn't conform to the protocol. Thirdly, an eavesdropper should not be able to trace the path of vehicles using the beacon messages, which is equivalent to ensuring location privacy of the sources [33,34]. A vehicle is fundamentally linked to a driver, and being able to trace a vehicle is equivalent to being able to trace the person driving the car. This seriously invades the driver's privacy. Although various solutions have been proposed, developing an effective and better pseudonym-change-based privacy scheme to preserve location privacy without compromising with the security requirements is still an open research problem.

1.1.3 Trust Management

Various entities of a vehicular network (vehicles, roadside sensors (traffic detection units), RSUs, network elements, etc.) register themselves to trusted authority and get certificates (long-term and short-term) and cryptographic materials (key pairs). These materials are used for confidentiality (V2I/I2V, I2I), integrity, signing, verification, and authenticity. However, these certificates and materials do not protect the network against internal threats from compromised, malicious, and

misbehaving entities. For example, a vehicle in the network can disseminate false information about its kinematics, causing disruption and affecting road safety. Such actions are known as misbehavior. The malicious entities may intentionally transmit false information, and faulty or compromised entities may unintentionally send the wrong information. The misbehaving nodes hold the required certificates and cryptographic materials to communicate in a network and are considered insiders and active attackers. These attackers can modify the payload of its outgoing safety and awareness messages by gaining access to their vehicle's CAN bus (protocol is vulnerable). It is also possible that attackers can launch a MiM, replay attack and alter sensors data [35]. Trust management aims to allow each peer in a vehicular network to detect dishonest peers and malicious data sent by misbehaving or dishonest peers. There should be an incentive and penalty mechanisms to manage the reputations, encourage nodes/peers to behave honestly, and discourage self-gain and misbehavior. Based on the applications' critical nature, data and node-centric trust have been proposed in the literature. In the recent past, researchers have proposed various centralized and decentralized solutions for trust management. However, the unique characteristics of a vehicular network environment pose challenges to effectively model and manage trust in a decentralized, transparent, reliable, consistent, and scalable manner.

1.2 Motivation and Objectives

Vehicular networks are being deployed in various developed nations like the USA, Europe, and Japan. It is on the verge of real-world deployment in many developing nations. Table 1.1 shows that the USA, Japan, and Germany are the leading countries that contribute significantly to vehicular network-related research and development [12]. This network has a great potential to improve road safety, improve traffic management, minimize CO2 emissions, and offer new driving comfort levels.

We believe that developing nations' research and development communities should also contribute to this increasingly important research domain to take benefits from the network. We can be benefited from these vehicular network services and applications only when we are ready with the desired ecosystem and the latest technologies that can address the existing challenges. To identify the challenges and address them, we conduct a survey to have a more profound knowledge of the potential applications, architecture details, radio access technologies, existing protocol stacks, ongoing standardization and project activities, etc. From the survey, we select three major impediments to the adoption of the vehicle network, namely seamless V2I connectivity in small cells, privacy issues, and trust management, and we contribute towards them. Our approach in this thesis is different. Instead of focusing on one sub-domain and extending the same work, we select three sub-domains for our contributions. The motivation is to contribute to the major challenges of a vehicular network, which are critical and need to be addressed. We do not restrict ourselves to a particular sub-problem. This helped us learn the domain from different perspectives, identify gaps in the state-of-the-art standard solutions, and identify possible future research opportunities in communication, privacy, and trust-related issues of a vehicular network.

This thesis aims to investigate the theoretical and practical aspects of vehicle-to-infrastructure connectivity, privacy, and trust management issue keeping in view the challenges/hurdles discussed in the previous section. In particular, the objectives of this work may be summarized as follows:

- Acquiring a deep understanding of the vehicular network domain and exploring various research opportunities in its sub-domain of communication, security, privacy, trust, etc.

- Survey existing standard solutions and research proposals and find potential technology enablers for V2I connectivity in HetNet. Conduct a systematic

Continent	Country	Projects	Total by Continent
Asia	China	10	
	India	1	
	Israel	6	
	Japan	45	
	Singapore	4	
	South Korea	17	
	Taiwan	6	
	Turkey	1	
Europe	Austria	2	172
	Belgium	10	
	Finland	2	
	France	15	
	Germany	46	
	Greece	2	
	Italy	12	
	Netherlands	21	
	Norway	2	
	Portugal	1	
	Romania	1	
	Spain	6	
	Sweden	16	
	Switzerland	1	
	United Kingdom	10	
	Europe-Wide	25	
North America	Canada	6	176
	USA	170	
Oceania	Australia	8	10
	New Zealand	2	
Grand Total			**448**

Table 1.1: Geographical Summary of (Country-by-Country Count) of Connected Vehicle Projects [12]

study of potential enablers, namely SDN, small cells (Wi-Fi, DSRC/IEEE 802.11p), and MPTCP and their role in V2I connectivity. Setup of the SDN-based framework close to the real-world scenario using the emulation platform to demonstrate the effectiveness of MPTCP for a V2I communication in it. Finally, elaborating on the solution's feasibility and suggesting future works that can help improve V2I connectivity in SDN-controlled small cell deployment.

- Survey existing standard solutions and research proposals and find associated challenges in preserving privacy in a vehicular network. Propose novel privacy-preserving schemes to overcome the existing challenges. Evaluate the performance of proposed mechanisms using essential privacy metrics against the global adversary model and compare it with existing and popular systems to demonstrate their effectiveness.

- Survey existing standard solutions and research proposals for centralized and decentralized trust models in a vehicular network and find associated challenges. Based on challenges, list the desired properties of an effective trust management system to be incorporated for broader acceptance. Propose a solution for trust management to achieve desired goals and address existing challenges. Design and Implement it to demonstrate the feasibility of the solution.

1.3 Contributions of the Thesis

As discussed earlier, first, we survey the vehicular network domain that covers all the latest details. This survey presents state-of-the-art that covers the latest architecture, various applications, emerging radio access technologies, standardization, and project activities. We discuss different vehicular network protocol stacks devel-

oped in the USA, Japan, and Europe with their latest standards. We present major challenges related to seamless V2I connectivity, security, location privacy, and trust management. These are the topical subjects in the vehicular network domain and open problems for the research community to address. Our contributions to three sub-domains (connectivity, privacy, and trust) of a vehicular network are as follows.

It is well recognized that better and seamless V2I connectivity can serve consumer demands for safety, infotainment, and other services related to mobility, environment, infotainment, vehicular social networking, maintenance, payment, and so on. For example, the driver and occupants can access many services from their user interfaces, such as audio-video on-demand, live TV, software updates, route guidance, navigation, messaging, voice-over inter protocol (VoIP), and many more. The industry and academia focus on developing better RATs that can enable connectivity between vehicles and roadside communication infrastructures, which enables various services. The four leading RATs for V2I communication are Wi-Fi, DSRC, 4G/ long-term evolution advanced (LTE-A), and 5G. The seamless vehicular communication in HetNet implies switching or roaming between RATs, which should hardly be perceived by the driver and occupants of the vehicle while accessing various services. Therefore, the biggest challenge is how to switch seamlessly from one radio access technology to another. Switching across different RATs disrupts any ongoing communication, and it is one of the biggest challenges of making it transparent to transport and application layer protocols. The traditional way of V2I connectivity in the HetNet environment has to face diverse challenges in terms of faster discovery, selection of suitable network, fast handover, full-filling diverse QoS requirements, and better management and control of resources. If we go by the traditional architecture, it is very challenging to address the issues mentioned above. We need to have better technology integrations at the end-hosts, radio access network, and the core. Software-defined networks (SDNs) are promising

solutions and can address many of these challenges by separating the control plane from the data plane. To capitalize available interfaces for connectivity in HetNets, we need to have technologies like Multipath TCP (MPTCP), which can allow a vehicle to use multiple network interfaces and IP paths simultaneously. Most of the end-user devices are now equipped with multiple network interfaces. The legacy mechanism uses only one path even when more than one path is available between the vehicle and the corresponding node. MPTCP can help capitalize on all available network interfaces and benefit in terms of better performance and reliability. The biggest advantage of MPTCP is that there is no need to change the legacy backbone infrastructure (DSRC network, cellular, Wi-Fi network, and IP infrastructure). It only requires the end devices to be MPTCP capable. In the first contribution of the thesis, we test MPTCP in small cells (DSRC and Wi-Fi) under SDN controlled environment for V2I Connectivity. We provide a systematic study of these technologies in the context of a vehicular network and identify the advantages and issues in integrating these two technologies. We present our findings after the experiment that can significantly benefit V2I connectivity in small cells. We propose solutions to V2I connectivity in the software-defined vehicular network with MPTCP and highlight future research directions in this domain.

Basic Safety Messages (BSMs: SAE J2945.1-2.2) and Cooperative Awareness Messages (CAMs: ETSI 302637-20-v1.3.0) are the two popular periodic messages defined in the Wireless Access in Vehicular Environment (WAVE) and Cooperative-ITS (C-ITS) protocol stacks standards of the USA and Europe, respectively [36]. These standards mandate the periodic broadcasting (1 Hz-10 Hz) of BSM and CAM in an unencrypted form [37] that includes vehicle's identification information (temporary ID), speed, current location, direction, speed, acceleration, etc. The BSM and CAM contain valuable data that other vehicles utilize to decide to prevent any undesired situations from arising. Since these messages are transmitted over

a wireless medium, an adversary can passively eavesdrop on all such broadcasted messages within its area of interest. If these broadcast messages are massively captured and analyzed, a vehicle's location privacy can be compromised [38]. Although the standardization development organizations (SDOs) such as IEEE and ETSI suggest using a pseudonym-change-based strategy, neither recommended a specific pseudonym change strategy nor discussed existing solutions. The standards only specify the use of the pseudonym, and it must be changed frequently to avoid simple correlation, i.e., there is no standard strategy adopted by the SDOs until now [11]. The development of an effective and better pseudonym-change-based privacy scheme is still an open research problem. Motivated by these facts, we contribute to this vital area of the research and propose two new schemes to preserve location privacy in a vehicular network. In the second and third contributions of the thesis, we present two schemes named Masqueraded Probabilistic Flooding for Source-Location Privacy (MPFSLP) and Cooperative Pseudonym Exchange and Scheme Permutation (CPESP), respectively.

Our second and third contributions to the privacy issue in a vehicular network are summarized as follows:

- We present a systematic study of existing PKI-based pseudonyms authentication scheme of VANETs, existing works, and models related to privacy in VANETs such as system, communication, adversary models, pseudonyms linking attack, and privacy metrics.

- We propose a new mechanism, MPFSLP, which ensures source location privacy without compromising other security requirements. The key insight we leverage is that in VANETs, a node only requires to know the location and velocity information of other nodes and not which node is at a particular location with a particular velocity. We define the idea of re-sending, which replaces the concept of forwarding in the network.

- The proposed mechanism uses the probabilistic flooding model. Each node transmits packets of all other nodes from which it receives, in addition to its own packet, using masqueraded probabilistic flooding.

- We apply our proposed mechanism to existing pseudonym change schemes to further limit the adversary's tracking ability. We also introduce the concept of casual dependency and proof-of-claim mechanisms that ensures non-repudiation in our scheme.

- We evaluated our scheme over the Privacy Extension for Veins VANET (PREXT) simulator, a framework that allows the comparison of pseudonym-changing schemes. Our scheme reduces normalized traceability when coupled with a pseudonym changing scheme as opposed to running the baseline pseudonym scheme. We also conduct a security analysis of the proposed mechanism.

- We propose another novel privacy-preserving scheme named CPESP, which combines two techniques: cooperative pseudonym exchange and scheme permutation.

- We implement our proposed CPE, SP techniques, and their combination CPESP in the PREXT simulator with a realistic mobility map to demonstrate the claim. We evaluate our proposed mechanism using essential privacy metrics against the deployed adversary model.

- We also compare our proposal with some of the existing and popular schemes in the literature for comparative results.

In a vehicular network, when a vehicle receives a BSM and a Decentralized Environmental Notification Message (DENM) for awareness and some incident, it uses the information to avoid an unwanted situation such as accident, congestion,

or some dangerous situation by effectively reacting to it. Consequently, the received messages' reliability and trustworthiness are of paramount significance. The system's acceptance and efficacy depend on them because they can affect driving decisions, and any wrong decision can have disastrous consequences. Trust management in a vehicular network implements vehicles' reputation based on both the trust value scored from its past behavior (reputation) and neighbors opinion about the received message broadcasted by the alarmer vehicle for an event. Trust management can also facilitate incentive mechanisms for the peers who behave well in the system and have earned a better trust score. There can be punishments for the dishonest or misbehaving peers in terms of trust score reduction and revocation after a certain limit of misbehavior is crossed or a defined threshold has been reached [39]. IEEE 1609.2 and ETSI-TS-102 941 standards of WAVE and C-ITS protocol stacks focus on misbehavior detection and trust management. However, developments are in their early research stage.

The fourth contribution of the thesis contributes to the trust management issue in a vehicular network. We propose a blockchain and smart contract-based decentralized trust management system to address the challenges of traditional centralized and decentralized mechanisms. The proposed system inherits key features of blockchain, such as decentralization, availability, consistency, and immutability. Besides, we introduce the concept of sharding to solve the scalability problem while managing trust in a vehicular network. The smart contract ensures fraud-free contract execution without any trusted third party. We also introduce an incentive strategy for the vehicles participating in event detection, i.e., their contribution in detecting a true event. Its accurate reporting helps them get rewards, which they can redeem for various services and payments. The proposed incentive mechanism encourages participating peers to perform well and get wallet points. However, if they do not perform well, they can be revoked from the system.

We demonstrate our framework's performance in terms of average throughput and execution time by deploying the private blockchain on the testbed.

1.4 Organisation of the Thesis

The rest of the thesis is organized as follows:

Chapter 2 provides a brief background and state-of-the-art of a vehicular network. This chapter gives a thorough survey of a vehicular network that presents a vehicular network architecture, applications, radio access technologies, protocol stacks, standards, projects, and state-of-the-art of selected sub-domains.

Chapter 3 presents the first contribution of the thesis. The chapter discusses the challenges associated with the standard solutions for V2I connectivity in HetNets and several other research proposals to this end. This chapter presents the theoretical foundation of the proposed technologies in a vehicular network context and discusses the finding from emulation. The chapter discusses various advantages and challenges in the proposed technology integration. Finally, the chapter suggests a suitable framework.

Chapter 4 starts with an introduction to location privacy in a vehicular network then presents details of the PKI-based pseudonym authentication system. The chapter also discusses standard solutions and related works in this sub-domain. The system model of the chapter covers communication, adversary, and attack models. This is followed by the proposed MPFSLP scheme details. Finally, the chapter reports the simulation results and security analysis.

Chapter 5 presents the third contribution of the thesis, which is based on the theoretical foundations (state-of-the-art, related works, system model) of Chapter 4 and towards the same issue of location privacy in a vehicular network. The chapter provides the proposed CPESP scheme details. Finally, the chapter reports the simulation results and security analysis.

Chapter 6 presents the fourth contribution of the thesis. The chapter starts with the introduction of trust management issues in a vehicular network. It then discusses proposed technologies and provides a detailed survey of the existing literature. It is followed by the proposed blockchain-based framework details and various algorithms used. The chapter analyzes the performance of a testbed-based experiment and discusses the outcome.

Finally, **Chapter 7** concludes the thesis with a summary of the work done and suggests possible future research directions in these domains of the vehicular network.

Chapter 2

Background and State-of-the-art

This chapter presents background details of our selected research domain of this thesis that includes the architecture, characteristics, applications, radio access technologies, protocol stacks, standardization, and project activities. Finally, the chapter discusses the state-of-the-art of selected sub-domains of a vehicular network.

2.1 Vehicular Network Architecture

Vehicular networks are deployed to enable vehicle-to-everything communication. It facilitates communication of types Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Vehicle-to-Network (V2N), Vehicle-to-Pedestrian (V2P), Vehicle-to-Device (V2D), etc. These networks are the leading research areas under different names of Vehicular Ad-Hoc Networks, Vehicular Communication, Internet-of-Vehicles (IoV), etc. The vehicular network enables vehicles to exchange information for various safety and non-safety applications. Figure 2.1 shows various domains of a vehicular network and multiple forms of communication. The network architecture consists of four distinct domains In-vehicle domain, Adhoc domain, Infrastructure domain, and Services domain. In the following, we detail their components and communication

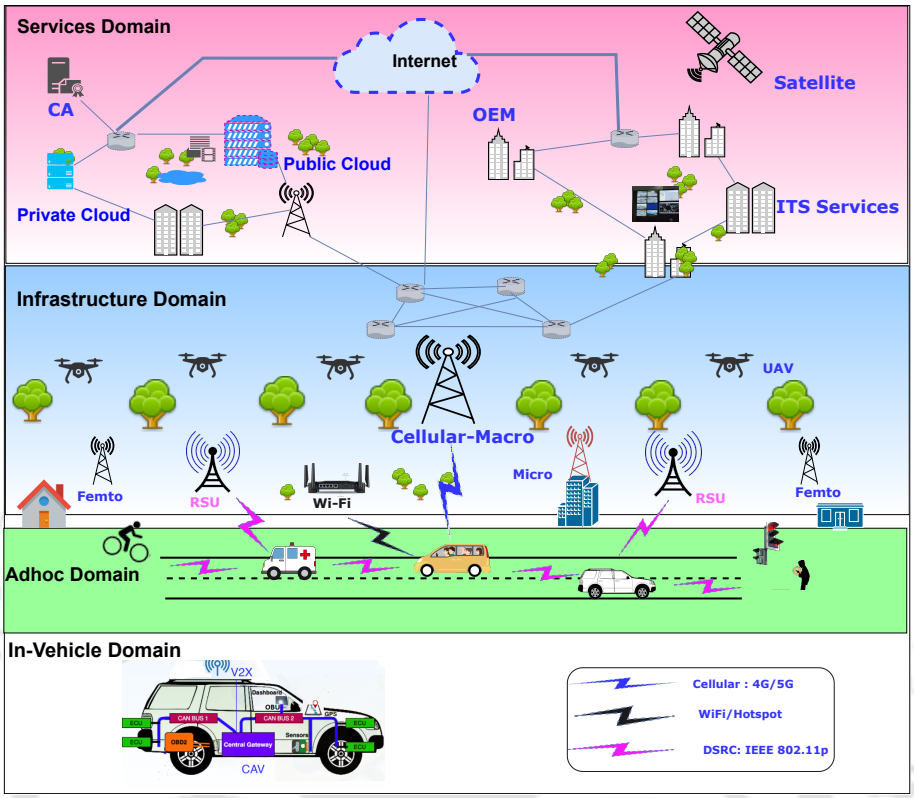


Figure 2.1: Vehicular Network Architecture

architectures.

2.1.1 In-Vehicle Domain

The in-vehicle components depend on the types of vehicle: connected vehicle or automated vehicle. Modern vehicles are called connected vehicles. They are equipped with complex mechatronic structures, sophisticated control, sensing, and communication capabilities, and over millions of lines of code for various automation and control functions [40]. Figure 2.1 illustrates the typical in-vehicle subsystem, which comprises sensors, actuators, Controller Area Network (CAN), Electronic Control Units (ECUs), GPS, Vehicle-to-Everything communication (V2X), On-Board Diagnostic (OBD) framework, Onboard Unit (OBU), central gateway, etc.

There are different protocols for data exchange between inter-subsystem (ECUs) and intra-subsystem (within each subsystem) such as CAN (powertrain sensors, transmission, engine controller), CAN with Flexible Data Rate (CAN-FD), FlexRay (Airbag, chassis, steering, brake control), Local Interconnect Network (LIN) (instrument cluster, door, seat, light, climate, seat, light, climate), Media Oriented Systems Transport (MOST) (phone, audio, display, navigation), and Ethernet. The V2X capability interface enables interactions with different radio access technologies such as Bluetooth, Wi-Fi (IEEE 802.11 a/b/g/n/ac/ad), Dedicated Short-Range Communication (DSRC), and cellular connectivity (3G /4G/ 5G). Integration of robust sensors such as Radar, LiDAR, Camera, and other advanced technologies to connected vehicles make them Connected and Automated Vehicles (CAVs).

The OBU is equipped with hardware (processing, memory, storage, and interfacing) and software to run various applications. It is also responsible for storing cryptographic materials and certificates for reliable data transmission, security, privacy, and other essential features [41]. The computing system is designed to support a wide variety of ITS applications and services such as hazard-warning, a navigation system, route information, traffic information, voice, and text messaging, infotainment, etc. The OBU provides an interface to the dashboard for driver interaction with the system. This dashboard incorporates a display, sound system, touch screen, gesture support, voice recognition, and other interfaces to provide better assistance and interaction.

2.1.2 Adhoc Domain

The adhoc domain is a special class of Mobile Ad-hoc Network (MANET), where the wireless network is created spontaneously for inter-vehicle communication. The two main components are vehicle and RSU. All the vehicles register themselves to the trusted or Certificate Authority (CA) to be part of the network. The communication

between vehicles can be one-hop or multi-hop and is of adhoc type. The presence of RSUs can sometimes help extend the range of communication and help in forwarding the messages to other vehicles. The communication in the adhoc domain is mainly V2V communication. Vehicles take the help of the infrastructure domain for its for V2I communication.

2.1.3 Infrastructure Domain

The infrastructure domain includes the roadside wireless infrastructure and the backbone wired network with middleboxes. The roadside wireless infrastructure can be RSUs (DSRC), Base Stations (eNB/gNB), and Wi-Fi Hotspots. The wired network infrastructure components can be access switches, routers, open flow switches and controllers (in case of Software Defined Network), edge nodes, fog nodes, gateways, and other required components. The fronthaul wireless infrastructures are connected to the backhaul wired infrastructures to connect vehicles and the services domain.

2.1.4 Services Domain

The services domain is the top layer of the architecture that provides services to the vehicles using the infrastructure domain via V2I/I2V connectivity. These services can be classified into two main categories:

- **Road Traffic-related services** provided by the road administration authorities in urban, rural, and highway zones. These services can be a part of the services provided by the ITS. Examples of services that can be deployed under this category are traveler information, traffic management, Map, electronic payment, emergency management, fleet management, parking management, etc.

- **Generic services** include the Internet service, subscription-based services, enterprise-based service (voice, video, data), equipment manufacturer-based services, energy services (from the smart grid), insurance, cloud-based services, etc.

Vehicular network with these domains has special characteristics which are discussed in the following section.

2.2 Characteristic

The vehicular network has unique characteristics that make it different than other traditional static networks. The network is dynamic and has different mobility models of urban, rural, and highway. The vehicle density and speed are not uniform; they vary considerably over time and space, which makes the topology very dynamic. The participating vehicles are resource-rich, and ample energy, computing, and storage power can be mounted or installed. The vehicle can be powered with more than one radio interface to enable V2X communication. All the vehicles need to broadcast event-driven messages and status information such as current location, speed, heading, acceleration, etc., periodically. These broadcasts are for delay-sensitive safety applications and happen in open communication. Vehicles run different types of non-safety applications and access the services while on the move. The QoS requirements for such V2I/I2V driven applications vary considerably. These important safety and non-safety applications are discussed in the following section.

2.3 Applications

In this section, we present various applications of vehicular network technologies. The primary goal of vehicular network deployment was to enable safety applications.

Nowadays, these networks are used for a wide variety of applications and services. The data from various studies, surveys, polls, and drivers' experience suggests hundreds of applications. All of these applications can be classified into two classes safety and non-safety applications. In the following, we briefly discuss each of these categories, using proper examples and illustrations.

2.3.1 Safety Applications

Safety applications advance drivers' knowledge of their direct environment, which helps prevent road accidents. Drivers' direct environment factors include road accidents, unexpected animals, obstacles, pedestrians, drivers going in the wrong direction, road construction and maintenance, road surface, road topology, legal speed limit, weather status, and other factors [42]. As shown in Figure 2.2, safety-critical applications such as post-crash, blind intersections, do not pass warnings are enabled mainly through V2V communication. The V2I mode of communication also helps in various safety-related applications such as curve-speed, pedestrian in signalized crosswalk, work zone warning, etc., as shown in Figure 2.3.

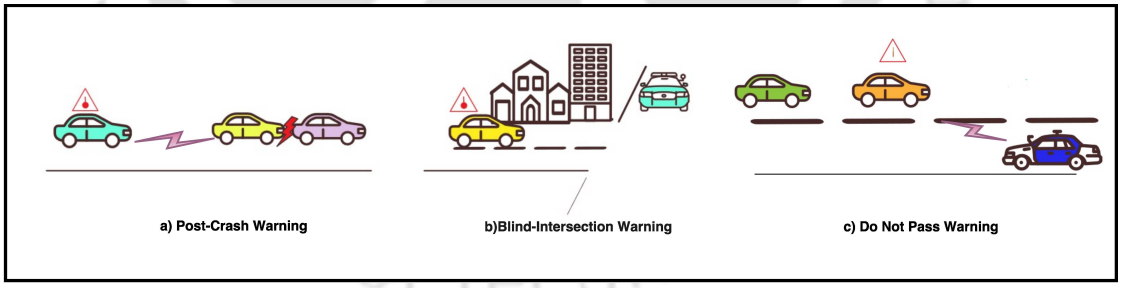


Figure 2.2: Safety Critical Applications enabled through V2V communication

Consider an example shown in Figure 2.2.a), a Post-crash or hazard warning. Assuming that a vehicle on the road encounters an accident with another vehicle, the automatic onboard sensor gets activated and broadcasts an alert or warning message to other vehicles. Vehicles approaching the crash site on the same route

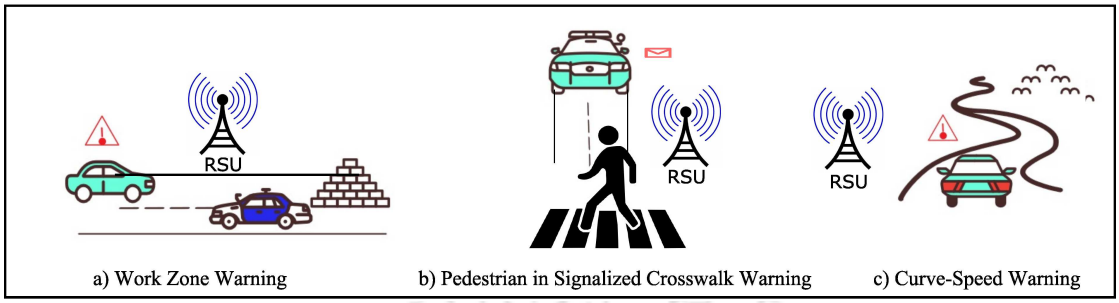


Figure 2.3: Safety Related Applications enabled through V2I/I2V communication

gradually decelerate and stop after receiving the warning message to avoid another crash. Such mishaps occur mainly on highways or expressways when visibility is low due to dense fog or bad weather. An accident in such a condition results in a series of vehicle collisions. Safety applications can play an immense role in safeguarding human lives under such circumstances.

2.3.2 Non-Safety Applications

In addition to safety applications, vehicular network technologies allow incorporating many other applications and services related to mobility, environment, infotainment, vehicular social networking, maintenance, payment, etc. [1]. We club all these services together into the non-safety applications category. Different types of non-safety applications are shown in Figure 2.4.

Figure 2.5 portrays few of these non-safety applications. Figure 2.5.c) illustrates traffic signal management and optimal speed advisory, which is based on Traffic-Light-To-Vehicle Communication (TLVC) [43]. In this method, a traffic light controller periodically broadcasts the light scheduling information to nearby vehicles in I2V mode. After receiving this information, drivers can adjust their speed to pass the traffic signal when it is green. This entire mechanism can help avoid stopping and braking and reduce fuel consumption and carbon emission [43].

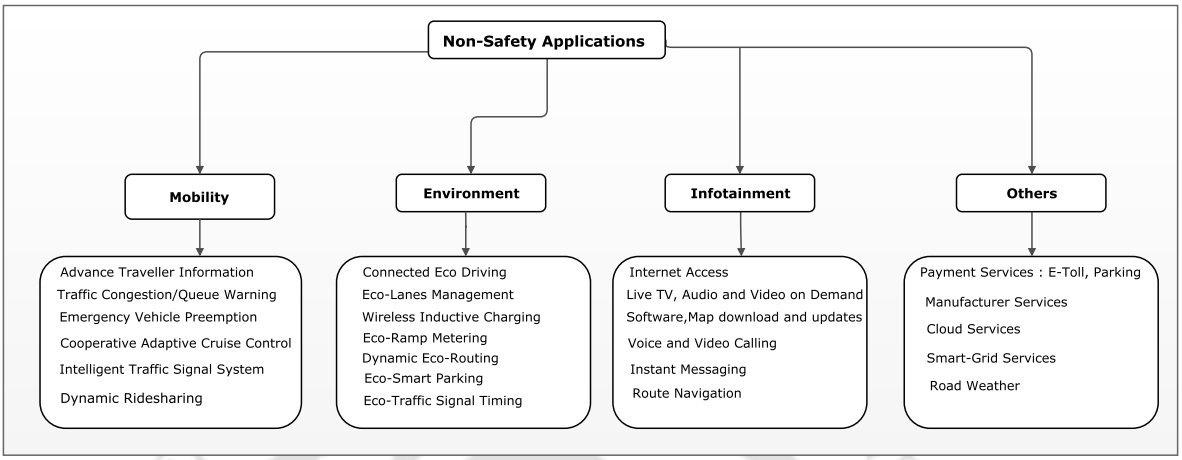


Figure 2.4: Non-Safety Application Types [1]

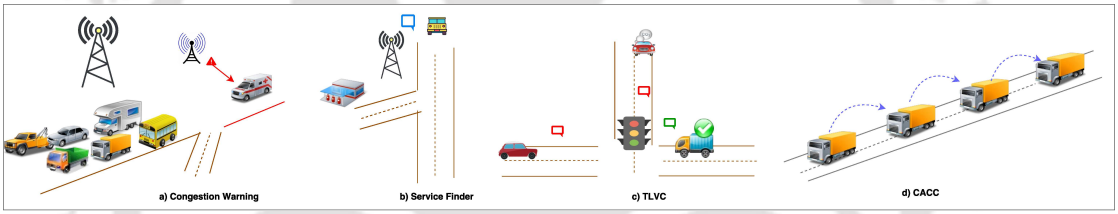


Figure 2.5: Illustration of few Non-Safety Applications

In infotainment services, the driver can access many services from its dashboard, such as audio, video on demand, live TV, software updates, route guidance, navigation, messaging, calling, and many more. Many of these applications are similar to the applications that we use on smartphones. However, meeting QoS requirements becomes challenging in a vehicular network because of its high mobility and dynamic network topology. The communication required for most of the non-safety applications is based on V2I or I2V mode. However, some applications in this category, such as Cooperative Adaptive Cruise Control (CACC), rely on V2V communications.

Various types of vehicular network applications discussed above are facilitated by radio access technologies, which are discussed in the next section.

2.4 Radio Access Technologies

Features	DSRC/IEEE 802.11p	Wi-Fi	VLC	LTE	LTE-A	5G Envisioned
Standard	IEEE 802.11p	IEEE 802.11	IEEE 802.15.7	3GPP Rel-8/9	3GPP Rel-10/11/12	3GPP Rel-15/16
Frequency Band(s)	5.86-5.92 GHz	2.4 GHz, 5.2 GHz	380-800THz	700 - 2690 MHz	450 MHz - 4.99 GHz	700 MHz - 100 GHz
Channel Width	10 MHz	20 MHz	NA	1.4, 3, 5, 10, 15, 20 MHz	Up to 100 MHz	NA
Bit Rate	3-27 Mbps	6-54 Mbps	11.67kbps - 96 Mbps	Up to 300 Mbps	Up to 1 Gbps	Up to 20 Gbps
Range	Up to 1 km	Depends on Protocol, and Device ; 100-500 meteres	<100m	Femto Cell Pico Cell, Macrocells; tens of meters to 30 KMs	Femto Cell Pico Cell, Macrocells; tens of meters to 30 KMs	Ubiquitous
Mobility Support	Medim : Up to 60 Km/h	Low	Low	Very high (up to 350 km/h))	Very high (up to 350 km/h)	Up to 500 km/h
QoS Support	Enhanced Distributed Channel Access (EDCA)	EDCA	NA	QCI and bearer selection	QCI and bearer selection	NA
V2V Support	Yes : Ad hoc	Yes : Ad hoc	Yes	No	Yes : Via D2D	Yes
V2I Support	Yes	Yes	Yes	Yes	Yes	Yes
Deployment	RSU	Hotspot , Access Points	Available Road Lights (LEDs)	May use the available eNodes B	May use the available eNodes B	NSA and SA mode
Market Penetration	Low	High	Low	Potentially high	Potentially high	NA
Broadcast/multicast support	Native broadcast	Native broadcast	Broadcast	Through eMBMS	Through eMBMS	NA

Table 2.1: Radio Access Technologies for Vehicular Communications, adapted from [13, 14]

The V2V mode of communication is a key enabler to provide safety applications. RATs such as DSRC [44], Cellular Vehicle-to-Everything (C-V2X) [45], and Visible Light Communication (VLC) are the potential candidates for V2V communication. Infrastructure and network connectivity is a crucial feature of connected vehicles. This connectivity is required for various non-safety applications mentioned

in the previous section. The telecom industry and academia focus on the development of better RATs that can enable connectivity between vehicles and roadside communication infrastructures. The RATs for V2V (DSRC, C-V2X, VLC) can also be capitalized for V2I/I2V driven non-safety applications. Apart from these RATs, Wi-Fi and cellular connectivity (4G and 5G) are the other two promising candidates for infrastructure-based communications. Many car-manufacturing companies such as BMW, Ford, Audi, Mercedes, Fiat, Toyota, Nissan, and General Motors are already experimenting with the available RATs to enable safety and non-safety (mainly Internet access) applications. Audi and General Motors have the most vehicles embedded in-car 3G or 4G/LTE-powered wireless access for the Internet. Various features of the RATs are listed in Table 2.1. A vehicular network needs to have well-defined wireless communication protocol stacks to utilize the underlying RATs for various applications and services. The following section discusses three dedicated protocol stacks for vehicular communication.

2.5 Protocol Stacks

Over the last decade, the vehicular network is shifted from pure research to deployments in the developed regions such as the USA, Japan, and Europe. In the USA, the research on the connected vehicle is entering into real-world deployments. Pilot projects in the Tampa, Wyoming, and New York regions are being rolled out [46]. The V2V communication over DSRC is likely to be mandatory in these regions. Japan is expanding its deployment of V2I to IVC, and Europe, in its Phase 1, is working to deploy connected driving in the EU. As shown in Figure 2.6, three dedicated protocol stacks (for vehicular communication over DSRC) have been developed in these regions: WAVE protocol stacks in the USA, the Cooperative-ITS (C-ITS) protocol in Europe, and the ARIB STD-T109 in Japan [47].

We provide an analogy analysis between Connected Vehicle, ARIB STD-T109,

and C-ITS protocol stacks.

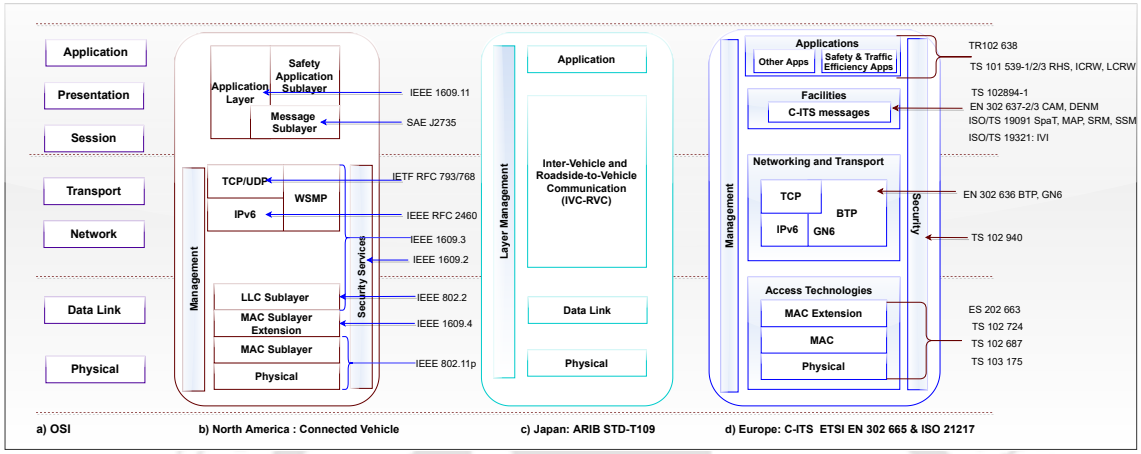


Figure 2.6: ITS Protocol Stack is the USA, Japan and Europe.

Lower Layer: The lower layers of these protocol stacks differ from each other. The Connected vehicle and C-ITS standards are based on WLAN Extension in OCB mode operating in the 5.9 GHz frequency band (IEEE 802.11p), which uses CSMA/CA to coordinate multiple access. However, ARIB STD-T109 uses the same physical layer but in the frequency band of 700MHz (center frequency of 760MHz) and employs an adapted MAC layer that mixes CSMA/CA with TDMA. The lower layer of the C-ITS protocol stack is referred to as an access layer that merges the physical and the data link layer corresponding to the OSI model. Details of the technology are specified in ETSI ES 202 663. It constitutes three parts: IEEE 802.11p, IEEE 802.2 LLC, and DCC. The lower layers of the connected vehicle follow a similar approach with MAC sublayer extension functionalities of multi-channel operation specified in IEEE 1609.4.

Network and Transport Layers: These two layers of these protocol stacks specify the required functionalities of layers 3, 4, 5, and 6 of the OSI reference model. In Connected vehicle and C-ITS protocol stacks, at these layers, we have two separate data planes; one with TCP/UDP over IPv6 for V2I communication,

and the other using WSMP (specified in IEEE 1609.3) and BTP with GN6 (defined in ETSI EN 302 636-4-1) for V2V communication, respectively. The WSMP is a highly efficient messaging protocol designed primarily for optimized operation in a vehicular mobility environment. WSMP is utilized mainly for safety and fee collection scenarios. It is well suited for message-based applications and in the case of intermittent connectivity. GN6 is used as a network protocol that facilitates both single-hop and multi-hop communication via geographical addressing. For multi-hop communication, it uses routing, which is based on geographic areas. The BTP is a connectionless, best-effort transport layer protocol explicitly designed for traffic safety applications that are delay-sensitive. It also facilitates the means for distinguishing between different protocols at the layer on top of it. In ARIB STD-T109, these two layers' functionalities are defined in the IVC-RVC Layer, which maintains channel access parameters, handles communication control, and synchronizes the clock. Time synchronization among vehicles is achieved via Over-The-Air (OTA) synchronization. IVC deals with V2V communication, i.e., the traffic between vehicles, whereas RVC defines I2V communication, i.e., the traffic sent to vehicles from RSUs.

Application Layer: This layer of these protocol stacks represents an interface for communicating with end-user applications. Various safety and non-safety applications and protocols have been developed in these regions. To name a few, BSM, CAM, DENM, etc., which use underlying layers to offer road safety, infotainment, payment, and commercial services in vehicular networks.

Security Framework: The security frameworks for connected vehicles and C-ITS are specified in IEEE 1609.2 and ETSI TS 102 940. However, the security details of ARIB STD-T109 are not available. In the USA, the NHTSA and ETSI in Europe define security architecture for vehicular communication based on Public Key Infrastructure (PKI). The PKI consists of hardware, software, policies, and

standards. They have a similar architecture with little variations in these two regions, and their mappings are available in ETSI TS 102 867. The security services provided by these two follow similar security mechanisms. For example, authenticity via signing, confidentiality via symmetric and asymmetric encryption, integrity via message authentication code and value of signed messages, and non-repudiation via EDR traces. The misbehavior detection and trust management in these regions are under development. For preserving Location privacy, they rely on the PKI-base pseudonym authentication mechanism. The following section reviews various standardization efforts for these protocols and research projects in vehicular network fields at the regional and international levels.

2.6 Standardization Activities

The standardization activities are carried out at international and regional level standardization developing organizations (SDOs). International SDOs work on vehicular network-related recommendations, reports, and standardization. Various studies on advanced radio and V2X communications are underway to improve road safety, transport efficiency, and comfort in many countries. At the regional level, the main developments emerge from the USA, Europe, and Japan. These countries are contributing significantly to the deployment. Figure 2.7 lists the main SDOs at the international and regional levels. Regional SDOs collaborate with International SDOs to develop the harmonized standard for vehicular network technologies. The main objective is to accelerate the vehicular network deployment process and provide harmonized standards across the globe by minimizing variations, reducing costs, and proving interoperability between architectures and equipment.

The U.S. Department of Transportation (USDOT) is an active participant in connected vehicle standardization in the USA. The connected vehicle technology standards are primarily released by IEEE, SAE International, and National

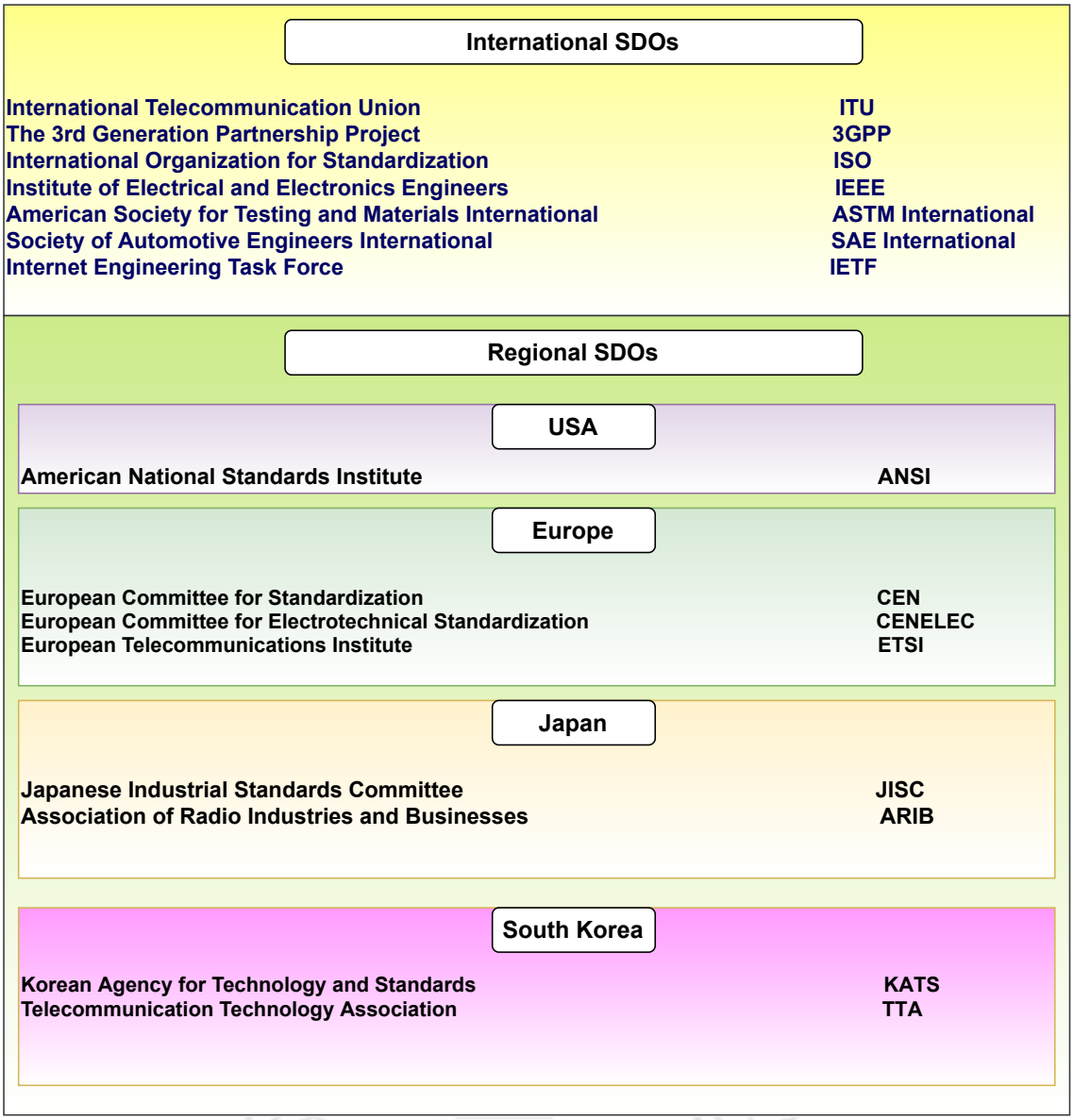


Figure 2.7: International and Regional SDOs for Vehicular Network Technologies

Transportation Communications for ITS Protocol (NTCIP). Various standards (shown in Figure 2.6.b)) that are used to deploy "Connected Vehicles" in the USA are listed as follows:

- SAE J2735 and SAE J2945/1.

- IEEE 1609 family Standard (Includes IEEE Std 1609.2, 1609.3, 1609.4, 1609.11 and IEEE 1609.12) [48].
- IEEE 802.11p [49, 50].

The U.S. DOT's ITS Joint Program Office (JPO), National Highway Traffic Safety Administration (NHTSA), and other SDOs, including the SAE, the IEEE, and the Crash Avoidance Metrics Partnership (CAMP), are working together to enhance and publish these connected vehicle standards.

In Japan, the SDO ARIB promotes research and development of new radio systems and advances the harmonization of international standards and related activities in the fields of telecommunications and broadcasting. The major activities of ARIB related to the ITS Japan are the development of DSRC standards. In Japan, the DSRC spectrum of 80 MHz (5.770-5.850 GHz) has been used with ARIB STD-T55 (ETC), ARIB STD-T75 (DSRC), and ARIB STD-T88 (DSRC Application Sub-Layer (ASL)). ARIB STD-T55 and STD-T75 are available for V2I communications and define standardization on layers 1, 2, and 7 of the base OSI reference model. At the physical (PHY) layer, ARIB STD-T75 uses 14 separate channels of 4.4 MHz widths each. Out of 14 channels, seven channels are used for the downlink and the remaining seven for the uplink. ARIB STD-T88 has been developed mainly to support applications based on V2V and V2I communication. In ARIB STD-T88, the new DSRC-ASL layer is added on top of the ARIB STD-T75 protocol stack. This new standard is primarily intended to provide multi-application services based on ARIB STD-T75 [51] more easily. The DSRC-ASL can handle both IP and non-IP applications. In addition to these three standards, a new standard ARIB STD-T109 (700 MHz Band Intelligent Transport Systems) has been developed for "Driving Safety Support Systems." In 2011, the new frequency range of 755.5-764.5 MHz is allocated to ARIB STD-T109 for various types of ITS applications.

In Europe, standards are being developed by the SDOs officially recognized

by the European Union (EU). These SDOs are known as European Standards Organizations (ESOs) and are CENELEC, CEN, and ETSI. These ESOs cooperate closely and work in close collaboration with other international SDOs, including ISO, IEEE, IEC, and SAE International. Their goal is to achieve internationally harmonized standards of ITS that are now essential to interoperability on a global scale. At the European level, technical committees of the ESOs for ITS related standardizations are given as follows:

- CEN: CEN/TC 278 for ITS and CEN/TC 226 Machine Readable cards
- CENELEC/TC 226 Road equipment
- ETSI - ETSI TC ITS (ETSI's Technical Committee for ITS)

Various standards developed to deploy "Cooperative-ITS" in Europe are shown in Figure 2.6.d.

2.7 Project Activities

Several research projects have been completed and are now being taken to the next level in the USA, Japan, and Europe. Various projects are in trial and dealing with next-generation vehicular networks. This section discusses those project activities.

The first research program, "California PATH Program" in North America was founded in 1986. In 1991, the U.S. Congress initiated the Intelligent Vehicle Highway Systems (IVHS) program via Intermodal Surface Transportation Efficiency Act (ISTEA). The main objectives of this program are to improve road safety, increase efficiency, conserve fossil fuel and reduce pollution of the U.S. national road infrastructure [52]. The United States Department of Transportation (U.S. D.O.T.) took the responsibilities of the IVHS program. In 1996, the IVHS service framework was prepared by the U.S. D.O.T., Intelligent Transportation Society of America

(ITSA), and finally named National Intelligent Transportation Systems Architecture (NITSA). To date, this framework is considered one of the master plans for ITS in the USA. NITSA acknowledged and accepted wireless communications as a key component in implementing ITS services [52]. Vehicle Safety Communications (VSC) [53], IntelliDrive(sm)/Vehicle Infrastructure Integration (VII) [54], Cooperative Intersection Collision Avoidance Systems (CICAS) [55] are some of the completed project. Safe and Efficient Travel through Innovation and Partnership for the 21st century (SafeTrip21) [56] and Vehicle-to-Vehicle (V2V) Communications for Safety [57] are some of the ongoing projects in the USA. Now, all R&D works associated with U.S. D.O.T. is managed and controlled by Research and Innovative Technology Administration (RITA) [58]. The two key priorities of U.S. D.O.T.'s current ITS research program are (i) Realization of Connected Vehicle implementation (ii) Advancement of Automation technology.

Japan has a long history of ITS and connected vehicle technology. The history of Japanese ITS research and development [12] [59] are:

- 1973: Comprehensive Automobile Traffic Control System (CACS)
- 1980: Trial operation of Highway Advisory Information Radio system (HAIR)
- 1984: Road Automobile Communication System (RACS)
- 1989: Advanced Mobile Traffic Information and Communication System (AMTICS)
- 1991: Advanced Safety Vehicle (ASV).

These projects have contributed to the development of the Vehicle Information and Communication System (VICS). Electronic Toll Collection (ETC) Systems [60] [61] [62], Advanced Safety Vehicle (ASV) [12] [63] [64], Smartway [12], Driving Safety

Support Systems (DSSS) [12] [65] [66], ITS-Safety 2010 [12] [67] and ITS Spot [68] are some of the major projects in Japan.

The Eureka PROMETHEUS Project (PROgraMme for a European Traffic of Highest Efficiency and Unprecedented Safety, 1987-1995) reported being the largest R&D project ever in the field of driverless cars [80] [81]. Car manufacturers from six European countries headed this research programme. The primary goal of PROMETHEUS is to create concepts and solutions (use of microelectronics, information processing, and artificial intelligence) for an efficient, safe, and eco-friendly road traffic system. The main instrument for funding research and development projects in the European Union is the Framework Programme (FP), and most of the ITS-related projects are funded under FP in the category 'ICT for Transport'. FP project information is available on the European Commission's community research and development information service web page at [82]. The main European ITS projects under FP6, FP7, Horizon 2020 (H2020) are as follows:

- FP6: COMeSafety [83], COOPERS [84], CVIS [85], SAFESPOT [86] , NoW [87], AIDE [88], APROSYS [89].

- FP7: PREDRIVE C2X [90], GeoNET [91], iTETRIS [92] [93], ROSATTE [94], PRESERVE [95], PRECIOSA [96], DRIVE C2X [97], COLOMBO [98]

- H2020: HIGHTS [99], CIMEC [100], CODECS [101] 5GCAR [102].

Over the years, various advancements have been made in the field of vehicular networking. A large number of industrial trials and initiatives indicate the shift of the technology from academia to field trials and real-world deployments. We list some of the latest industry trends/projects/trials in Table 2.2.

2.7 Project Activities

Projects / Trials	Description	Comm. / App.	Start
C-V2X trials in Japan [69]	The trial was conducted with a joint collaboration among Nissan, Ericsson, Continental, NTT DOCOMO, OKI, and Qualcomm Technologies. Companies claimed the trial to be the first C-V2X testing in Japan. The trial focused on sending messages under varying conditions such as in the presence of high buildings and with vehicles moving at high speed,	LTE / 5G	2018
Bosch-Daimler fully automated and driverless driving system [70]	Bosch and Daimler has joined hands to bring fully automated (SAE 4) and driverless system (SAE 5) on the road. The project aims to develop software and algorithms for autonomous driving systems for improving traffic flow and enhancing driver safety.	Automated and Driverless systems	2018
Intel-Mobileye 100-car autonomous vehicle (AV) fleet in Israel [71]	Intel and Mobileye began operating a 100-car autonomous vehicle (AV) fleet in Jerusalem. Each vehicle in the fleet is powered with 12 cameras in a 360* configuration. The goal of the initial phases of the project is to create a comprehensive end-to-end solution from processing only the camera data.	Autonomous Vehicle	2018
Multi-party 5G trials for connected cars [72]	NTT DOCOMO in collaboration with Toyota, Ericsson, and Intel performed a trial of 5G technologies for automobiles. The trial achieved data speeds of up to 1 Gbps for 4K-resolution video communications with a vehicle traveling at 30 km/h. Companies are planning further trials for testing the practicality of 5G technology for connected car applications.	5G	2017
AT&T, Ford, Nokia, Qualcomm C-V2X trials in the USA [73]	*AT&T*, Ford, Nokia, Qualcomm announces C-V2X trials for demonstrating its potential in automotive safety and driving. The trials were made in San Diego.	4G LTE	2017
LG Electronics partners with HERE Technologies on autonomous cars [74]	LG Electronics partners with HERE cars for building telematics solutions for location-based services and high-quality maps. The partnership combines LG's advanced telematics technology with HERE's Open location platform.	Location-based Services	2017
Telefonica-SEAT assisted driving use case with V2X [75] in Spain	Telefónica and SEAT presented use case within the framework of 5G Technological cities project by equipping a vehicle and an RSU both with C-V2X technology for information exchange. The use case was presented for a city named Segovia in Spain.	5G	2018
C-MOBILE Project [76] in Europe	C-MOBILE project envisions to provide C-ITS related services to urban users on European road networks. The project aims to provide interoperable services with large-scale deployments. The C-MOBILE pilot sites span overs Denmark, Spain, France, and some other countries	C-ITS	–
Toyota Friend Project by Toyota [77]	Toyota Friend allows drivers receive messages from their cars such as car health status. It supports cloud communications allowing drivers to communicate with the service centers.	V2V and V2I	2011-Ongoing
BMW: Application for Automotive Projects [78]	The goal of the project is to allow seamless integration of smartphone applications with the BMW vehicles allowing BMW group to provide fast infotainment services to their customers.	Infotainment Services	Ongoing
Toyota-Grab Data Collaboration Initiative for Connected Car Services [79]	The project aims to use data analysis to improve access to connected car services that will improve the fleet customers' experience.	Customer Services	2017-Ongoing

Table 2.2: Latest Industry Trends/Trials

2.8 State-of-the-Art

In the previous sections, we saw that considerable efforts had been made at the regional and global levels to shift the technology from academia to real-world deployments. However, recent studies and surveys [11, 40, 103–105] have reported concerns with standard solutions for V2I connectivity in HetNet, security, privacy, and trust management. As these issues are turning out to be the main obstacles to a broader acceptance of a vehicle network, further efforts must be made to address them. Therefore, these standard solutions need to be thoroughly reviewed, tested and improved. In this part of the thesis, we summarize the state-of-the-art solutions to the selected issues.

2.8.1 Seamless V2I Connectivity in HetNets

The seamless V2I Communication in HetNet is an important aspect of the vehicular network. It implies switching or roaming across different radio access technologies (RATs), which should hardly be perceived by the driver and occupants of the vehicle while accessing various services. Therefore, the switching across different RATs should be transparent to transport and application layer protocols. With advances in user equipment, radio access, core networks, applications and services, and various usage models, the multi-RAT operation is likely to become the norm. Figure 2.8 illustrates the V2I connectivity in HetNets.

There have always been trade-offs between capacity, coverage, latency, data rate, mobility, spectral efficiency, and reliability in a wireless network. It is nearly impossible for a single RAT to fulfill the requirements. For example, the IEEE 802.11p/DSRC has been designed explicitly for vehicular communications and provides seamless handovers. However, it has low market penetration and suffers in terms of data rate support (capacity). Wi-Fi has the largest market penetration and supports better speed and capacity; however, it suffers in terms of coverage, delay

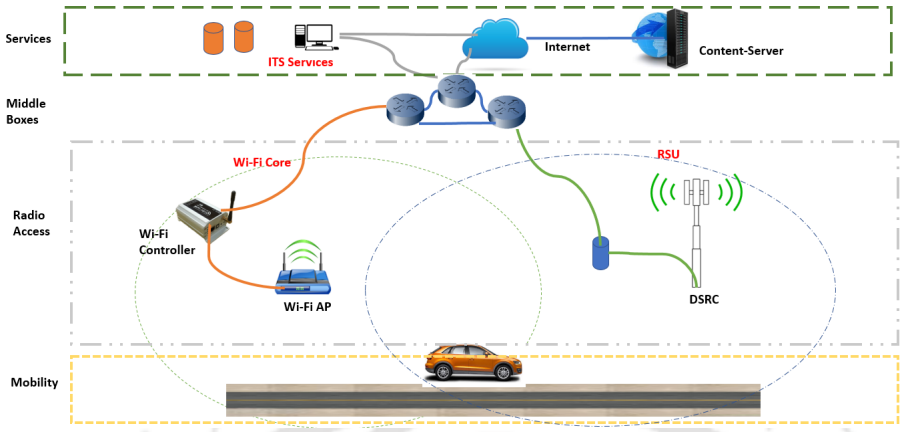


Figure 2.8: Illustration of V2I Connectivity in HetNets [2]

spread, high handover latency, and fading in the context of vehicular communication. Cellular networks such as long-term evolution (LTE), LTE-advanced, and LTE-pro also have advantages and limitations. The new generation network 5G IMT-2020 [106] is envisioned as a potential solution.

A considerable amount of research works have been carried out in the HetNet context. The two well-known mechanisms are the vertical handover-based mechanism and the multipath-based approach. In the former approach, only one RAT is used at any instant of time; however, in the latter approach, multiple RATs are utilized simultaneously. Figure 2.9 illustrates the horizontal and vertical handover concepts.

The two well-known standard solutions for V2I connectivity in HetNet are (1) media-independent handover (MIH) by IEEE (IEEE 802.21) [3] and (2) access network discovery and selection function (ANDSF) [107] by 3GPP.

The MIH protocol

It facilitates handover initiation (network discovery, selection, and handover negotiation), handover preparation (layer-2 and layer-3 connectivity), and interface activation in HetNet [3]. MIH is required in the existence of a heterogeneous network

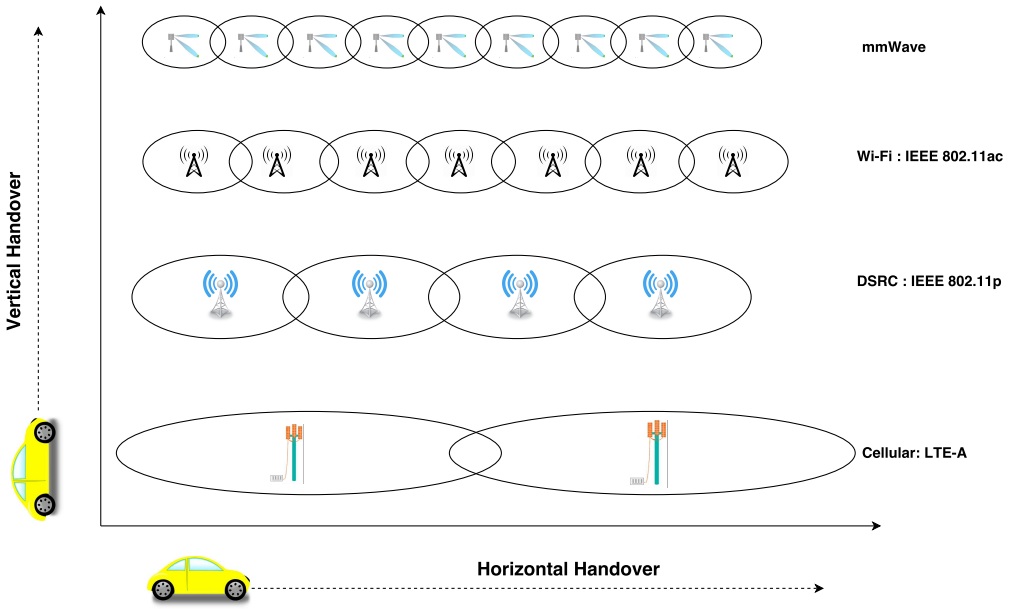


Figure 2.9: Illustration of horizontal and vertical handover [2]

(HetNet). It provides the mobile terminal the capability of discovering wireless networks of diverse technology in its vicinity and allows them to select the best network depending upon the gathered information. The MIH specification enables handovers between heterogeneous technologies such as IEEE 802.x and cellular technologies, making it one of the leading V2I communication candidates. Concerning V2I in HetNet, MIH can provide not only the list of available RATs but also the relevant information, which allows the vehicle to select a suitable target RAT.

Figure 2.10 illustrates the general architecture of IEEE 802.21. This framework allows higher levels to interact with lower layers to enable session continuity independent of underlying media or RAT. As shown in Figure 2.10, the IEEE 802.21 specifies a middleware protocol called media-independent handover function (MIHF) that encapsulates different underlying RATs (e.g., 802.x, 3GPP, and 3GPP2) to the upper layers. This allows the handover management process to operate independently of the data link layer and physical layer. MIHF provides services

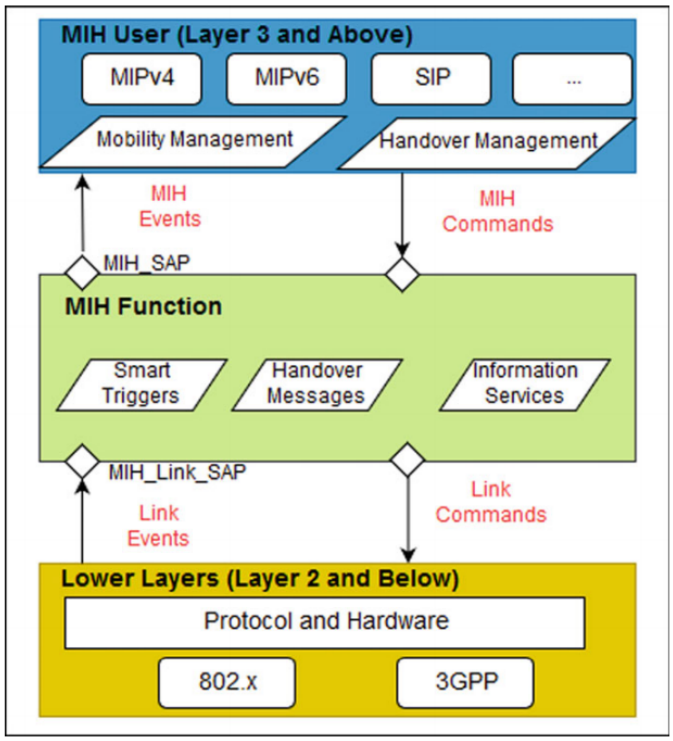


Figure 2.10: IEEE 802.21 MIH Architecture [3]

to both the lower and upper layers. These layers communicate with the MIHF via the service access points (SAPs). MIHF communicates with the link-layer (L2) via a technology-dependent interface called MIHF_LINK_SAP. However, communication between the MIHF and the media-independent handover user (MIHU) takes place via an independent technology interface called MIHF_SAP. These two SAPs aim to collect information and control the behavior of the link during handovers. To implement the vertical handover, the MIHU of the mobile node queries its MIHF for further information. The specification provides three major services to the users, namely Media-Independent Event Service (MIES), Media-Independent Command Services (MICS), and media-independent information services (MIIS). These services enable the MIHUs to access handover-related information and to deliver commands to the link layer.

IEEE 802.21 has been subject to various amendments by the IEEE after initial standardization in 2008. These are listed as follows.

- **IEEE 802.21a-2012:** This is the first amendment and an extension of the initial IEEE Std 802.21-2008. Security mechanisms have been introduced to protect MIH services. Another mechanism has been introduced, which uses MIH in assisting proactive authentication so that latency in media access authentication and key establishment with the target network can be reduced.

- **IEEE 802.21b-2012:** This amendment discusses handovers with downlink only technologies.

- **IEEE 802.21c-2014:** Additional IEEE 802(R) media access independent mechanisms have been specified to optimize handovers between heterogeneous IEEE 802 systems and cellular systems and enable improved handover performance for single-radio devices.

- **IEEE 802.21d-2015:** This standard specifies mechanisms to enable multi-cast group management for MIH services. It defines management primitives and a set of messages that can enable a user to join, leave, or update group membership. It also specified security mechanisms to protect multi-cast communication.

- **IEEE 802.21-2017:** Now, in this series, the standard IEEE 802.21-2017 is presently active, which defines media access independent services framework including its function and protocol that enables the optimization of services including handover and other key services when performed between heterogeneous networks.

ANDSF

It enables a mobile node to discover and select the most appropriate underlying RATs based on certain policies predefined by the network operators. It supports the discovery, selection, and connection to both 3GPP and non-3GPP access networks. ANDSF provides the mobile node a list of radio access networks that may be available in its vicinity and mobility domain, along with their deployment coordinates. This may help the mobile node to preselect and store the target network for its handover.

ANDSF is an entity within the Evolved Packet Core (EPC) introduced in 3GPP Release-8. It aims to assist UE in the discovery and selection of non-3GPP access networks such as Wi-Fi and provide them with rules and policies for connection to these networks. This non-3GPP access then can also be used for data communications in addition to 3GPP access networks. User Equipment (UE) may then employ IP FlOw Mobility (IFOM), multiple-access PDN connectivity (MAPCON), or non-seamless Wi-Fi offload according to operator policy and user preferences.

The ANDSF client-server interaction happens using the Open Mobile Alliance Device Management (OMA-DM) protocol over the S14 interface. This interface is an IP-based interface that supports pull and push communication mechanisms. Based on the operator configuration, the following category of information is provided to UE by the ANDSF server: discovery information, inter-system mobility policy (ISMP), inter-system routing policy (ISRP), inter-APN routing policy (IARP) rule selection information, WLAN selection policy (WLANSP), home network preferences, visited network preferences, and so on. The ANDSF-based architecture employs various ANDSF objects for smooth communication between the ANDSF client and the ANDSF server.

ANDSF was introduced in Release-8 to discover non-3GPP access networks

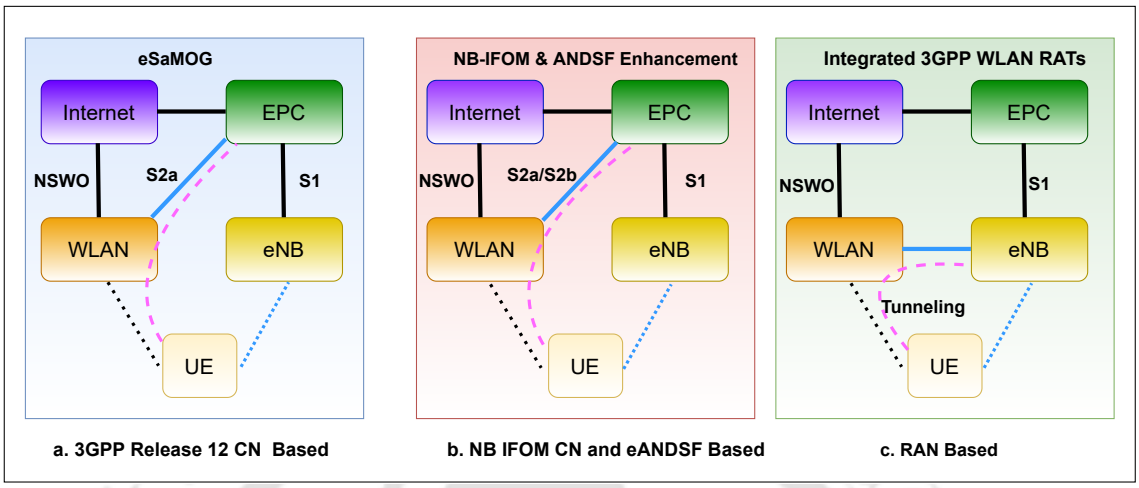


Figure 2.11: ANDSF for 3GPP and non-3GPP internetworking [4]

such as Wi-Fi and WiMAX; however, in the last 3GPP Releases 10–12, it has been enhanced to enable the UE to discover, select, and connect not only non-3GPP but also 3GPP access networks (UTRAN, HSPA, and LTE) [4]. The 3GPP Release 14 introduces the radio-level integration (RLI) of LTE and Wi-Fi, which enhances the capability of inter-working between LTE and Wi-Fi. To this end, LTE Wi-Fi radio-level integration with IPSec tunnel (LWIP) and LTE Wi-Fi Aggregation (LWA) have been proposed. In Release 14, the RLI architectures have been further enhanced to support mobility, uplink aggregation, and enable Wi-Fi inter-working in high-frequency bands (60 GHz). Figure 2.11 shows 3GPP and non-3GPP inter-networking architectures and their evolution in later 3GPP releases.

The existing RATs and techniques, including 4G (up to Release 14), do not support latency (1 ms), reliability (nearly 100 percent), and data rate (in Gbps) required to exchange information between the fully automated vehicle and the infrastructure. We need to have a highly reliable, scalable, available, and flexible network for driverless vehicles in diverse geographies and road conditions. 5G is intended to meet the requirements of autonomous vehicle communication for different services, which are impossible with the technologies we have today. The

5G details are discussed in the following section.

2.8.2 5G (Release 15 to 17):

This section provides details of the new generation RAT 5G (Release 15 to 17).

5G Technical Requirements

The 5G network has the capabilities to support the extremely diverse set of V2X use cases, applications, and services. It is expected to meet QoS and QoE to various applications and services and is considered to be reliable and secure. In its vision document "IMT-2020 Vision" [5], ITU-R defines 5G communication capabilities for its intended use cases in terms of latency, mobility, peak data rate, spectrum efficiency, and so on. The IMT-2020 (envisioned 5G) capabilities in comparison to IMT-Advanced (existing 4G) capabilities are shown in Figure 2.12.

The key performance indicators (KPI) define the technical requirements and depend on the particular use case. IMT-2020 use cases, such as enhanced mobile broadband (eMBB), requires higher network capacity and a higher peak data rate, ultra-reliable and low latency communications (URLLC) communications requires very low latency and high reliability and massive machine type communications (mMTC) demands energy efficiency and connection density.

5G for V2X

The D2D interface PC5 introduced in Release 12/13 was not suitable for V2X services and needed modification. Thus, to enable V2V communication and address the two main challenges of a vehicular network: high-speed (up to 250Kph) and high density (thousands of nodes) [108], a new interface is introduced in Release 14 with changes at the link and system level [109]. The study of the potential requirements of 5G New Radio (NR) started in 2015, and standardization activity began in March

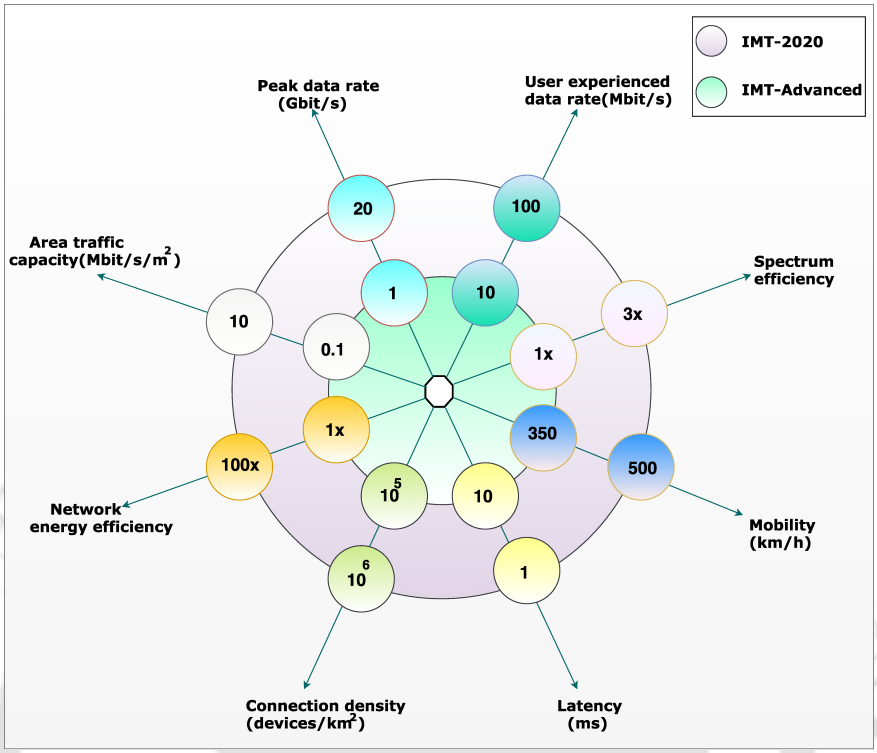


Figure 2.12: Key capabilities of IMT-2020 : Comparison to IMT-Advance [5].

2017 as 3GPP Release 15 [110]. It focuses primarily on all use cases of eMBB and some portion of URLLC (mission-critical applications). It introduced 5G NR for the Uu interface and various other enhancements for V2X communication of Release 14. The introduction of 5G NR can provide new levels of efficiency and capacity and ultra low-level latency to V2X communication in Non-Standalone (NSA) or Standalone (SA) modes of operation. It can support high throughput and a vast amount of data transfer in a reliable manner.

Phase 2 of the 5G development corresponds to 3GPP Release 16 [111]. It is considered to be the full compliance with ITU IMT-2020 requirements that can support all identified use cases (eMBB, mMTC, and URLLC). It enhances the capabilities and features of the Release 15 developments for V2X communication.

To satisfy a wide variety of requirements to the services deployed in diverse

scenarios, several technological transformations at the RAN, and in the NGC network of the 5G has taken place [112–116] in Phase 1 and Phase 2. In Release 17, new features for eMBB, URLLC, and mMTC are introduced.

Various transformations in Release 15 to Release 17 for 5G RAN include :

- Utilization of new spectrum above 6 GHz (mmWave up to 100 GHz) [117].
- Advanced beamforming [118] and tracking.
- Advanced channel coding (LDPC codes for data channels and Polar codes for control channels) [119].
- Massive MIMO [114].
- Advanced multiple access mechanisms (non-orthogonal multiple access (NOMA) [120, 121] and contention-based protocols).
- Enhanced frame structure design (low latency and self-contained sub-frame) [122].
- Advanced interference management [123–125](coordinated multipoint (CoMP) communication).
- Scalable radio numerology [126, 127].
- Supporting NR from 52.6 GHz to 71 GHz.
- Sidelink relaying.
- Support for multi-SIM.

The Phase 2 RAT includes common design for uplink, downlink, backhaul and sidelink, unlicensed spectrum access, D2D communication etc. The RAN facilitates new features to be added to the 5G NGC network. New features of the 5G core network that are being studied and expected to be included are as follows:

- Network slicing [128];
- Network Function Virtualization (NFV) [129, 130].
- Software Defined Network (SDN) [130].
- Self Organizing network (SON: Self-Configuration, Self-Optimization and Self-Healing)
- Integration of edge and fog computing [131].
- Flexible QoS support [132].
- Multi-connectivity [133, 134] support across 5G, DSRC, LTE, and Wi-Fi.
- Multi-RAT, multi-tier handover (intra-5G and inter-RAT handover) support [135, 136].
- Multi-vendor interoperability support [137, 138].
- Operator-controlled sidelink (D2D) and operation support (in-coverage and out-of-coverage) [139].
- Rapid and efficient deployment of network and services and ultra-dense networks [140, 141].

5G technology is envisioned to provide better vehicle automation and connectivity for transportation operation and infotainment services. 5G features such as ultra-low latency, high mobility, and high bandwidth make it more appealing for automotive use cases. In particular, the mmWave-based 5G can be beneficial for raw sensor data exchange, high-definition streaming, 3D map downloading, and many more applications. However, 5G is widely unexplored for V2I connectivity. It would be interesting to see whether the 5G is going to fulfill their claims of high throughput, ultra-low latency, high reliability, availability in different traffic conditions or

not. Heterogeneous connectivity based on multi-RAT is now essential to provide the best connectivity at all times.

As mentioned earlier, V2I and V2V are the two main communication modes of the vehicular network. Both of these communication modes pose a set of challenges. Ensuring seamless connectivity is the biggest challenge for V2I connectivity in HetNets; similarly, ensuring privacy and trust are the two major challenges of V2V communications. The following subsections discuss these two challenges, requirements, and standard solutions in detail.

2.8.3 Privacy in a Vehicular Network

The privacy risks include location tracking by dumping V2V safety messages (Basic Safety Messages) and performing a syntactic and semantic linking attack. The delay-sensitive safety messages are disseminated in V2V mode as plaintext (as encryption is not recommended to avoid delay). Thus, an adversary can easily eavesdrop on the broadcasted safety messages and extract sensitive Spatio-temporal info. The location of the driver and occupants can be revealed by using powerful tracking algorithms on that collected information, which poses a serious threat to their privacy. Vehicle-generated data, which is uploaded to cloud platforms via secure V2I and shared with service providers (manufacturer, the insurance company, service center, map provider, etc.) to benefit from various services such as predictive maintenance, usage-based insurance, payment services, and infotainment, also poses risks to privacy. Figure 2.13 depicts the privacy risk in a vehicular network.

Privacy Requirements:

There is a need for a strong privacy protection mechanism, which can prevent adversaries from exploiting private data related to vehicles, drivers, and occupants. Three distinguished classes of privacy protection in IoV are as follows: (1) Protection

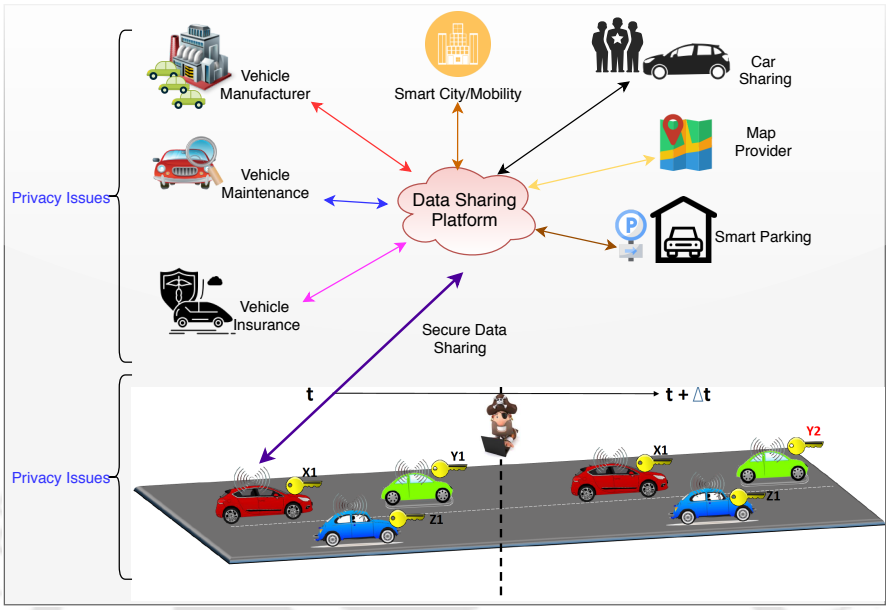


Figure 2.13: Privacy Risks in a Vehicular Network

of the vehicle's identity, (2) Protection of the vehicle's location and (3) Protection of the data exchanged in IoV. Key privacy requirements of IoV are as follows [11]:

Minimum disclosure: Minimal information about a user should be revealed, which is very necessary to ensure IoV's functionalities.

Anonymity: Anonymity is one of the standard methods to protect privacy, provided by the use of pseudonyms. The messages sent by a vehicle should not contain the real identity and should be anonymous within a set of subjects, i.e., potential vehicles.

Unlinkability: The use of a pseudonym helps in authentication without revealing the real identity. However, if the same pseudonym is used for a long time in a given context, it becomes linkable. Therefore, a set of pseudonyms are used to achieve the unlinkability of pseudonyms. These pseudonyms must be changed over time to combat linkability in that context.

Standard Solution for Privacy

To secure the vehicle network and fulfill the above-mentioned requirements, a consensus is reached on using the Public Key Infrastructure (PKI) based pseudonym authentication system based on Public Key Cryptography (PKC). The standards IEEE 1609.2 [142] and ETSI 102-941-v1.1.1 [143] describe the PKI-based architectures of security and privacy for connected vehicle and C-ITS protocol stacks, respectively. Figure 2.14 illustrates a simplified view of the PKI-based pseudonym authentication system. The PKI-based system for a vehicular network constitutes a set of Certification Authorities (CAs) such as Registration Authority (RA), Linkage Authority (LA), Misbehavior Authority (MA), Pseudonym Certificate Authority (PCA), and Root Certificate Authority (RCA). Various network entities such as vehicles, pedestrians, roadside units, and other infrastructures first register themselves to ECA in a secure out-of-band manner and then send requests for pseudonyms to RA via the Edge Certificate Management (ECM). All these entities become trusted after the registration. PCA issues certificates to all vehicles in an encrypted form using vehicles' private keys. These certificates are long-term and set of short-term certificates. The short-term certificates are termed pseudonyms or anonymous credentials. As a result, each registered vehicle in the network is securely provisioned with a set of short-lived pseudonym certificates. Vehicles use one of these short-term certificates and sign the BSM using its private key. Therefore a digital signature is attached to each outgoing BSM. Each vehicle that receives this signed BSM verifies the validity of the pseudonym first by checking the signature in the certificate using the public key of PCA. Then, verify other necessary fields of the certificate. Finally, it checks the signature of the message for its correctness. Vehicles use each pseudonym for a short period and switch from one pseudonym to a non-previously used one to ensure the unlinkability of digitally signed BSMs, which improves the privacy of vehicular communication. As a result, this PKI-based

system enforces authentication, authorization, and privacy in a vehicular network.

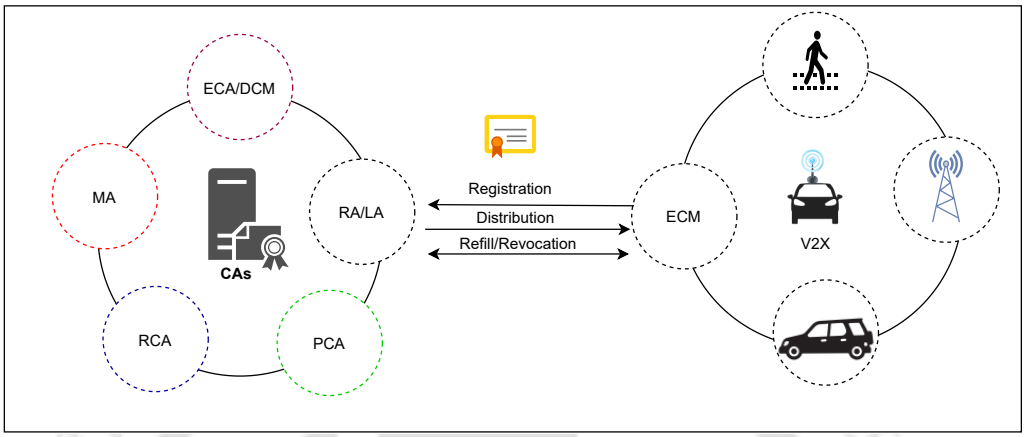


Figure 2.14: Simplified view of Standard Public Key Infrastructure

2.8.4 Trust Management in a Vehicular Network

Trust management is yet another biggest challenge of the vehicular network. It is an important concept in a vehicular network to identify and revoke malicious and misbehaving nodes. The use of appropriate trust models helps to evaluate the trustworthiness of the received message and its sender. The key functions of trust management in a vehicular network are as follows:

Misbehavior Detection: Detecting malicious and misbehaving nodes is one of the primary tasks of trust management. It aims to monitor the system to detect potential misbehaving nodes and prevent the IoV from deviating from its normal behavior. The misbehavior detection system operates in four steps [144]: local detection of the misbehaving entity, misbehavior reporting to the Misbehavior Authority (MA), an investigation by MA is sent to the root certificate authority to determine whether the entity is really misbehaving or just faulty, and finally, action by RCA to protect the system.

One such misbehavior of type position falsification attack is shown in Figure

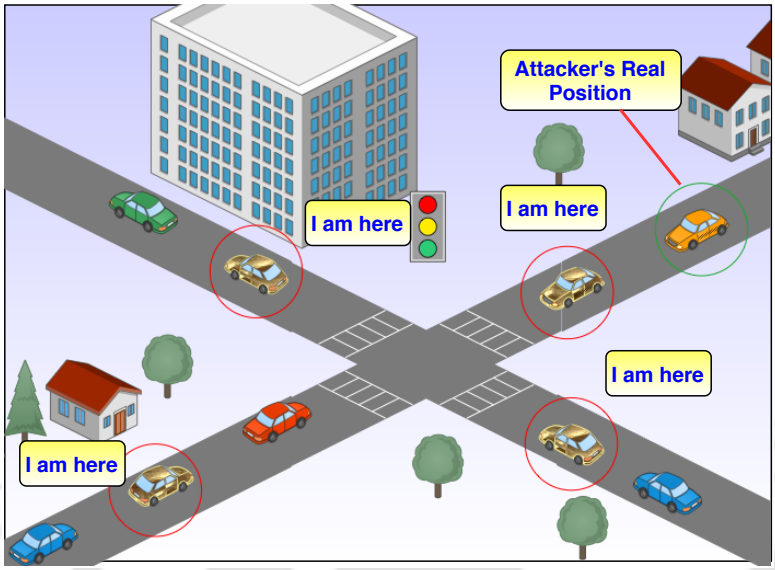


Figure 2.15: Misbehaviour (Position Falsification Attack) in a Vehicular Network [6]

2.15. The vehicle misbehaves by altering the safety message payload to produce false positions and broadcast it through V2V. As can be seen in Figure 2.15, the misbehaving node may overwhelm false position information when it is close to the intersections and confuse other vehicles [6]. Such misbehavior can have an adverse impact on critical safety applications, and it may be hazardous for other neighboring nodes. Since the message is produced from an insider (authorized node), other receiving vehicles that are part of the same authentication system verify the message and accept it for processing. Consequently, this can significantly affect a broad range of safety-related applications that rely on actual position information.

Accountability and Traceability: The specific action should be unambiguously assigned to an individual entity using a fair protocol to ensure accountability. In a vehicular network, this can be facilitated by traceability. Only privileged and highly trusted authorities must be allowed to trace a pseudonym and map to the user's real identity. Such authorities must try to trace or map a pseudonym to a real

identity under specific conditions only. For example, only MA should be allowed to perform traceability to detect the actual misbehaving entity.

Revocation and CRL Distribution: Trust management must have a fair revocation process that can respond better when misbehavior is detected. There should be some reputation-building mechanisms that have a reward and penalty system. If misbehavior is intentional, the corresponding vehicle needs to be penalized and loses its reputation score. A warning should be given to such misbehaving entities. After crossing the threshold, active revocation (current certificates revoked) or passive revocation (should not be able to request more certificates) must be invoked. Based on the decision, a list of revoked certificates called Certificate Revocation List (CRL) should be created and distributed efficiently.

Standard Solution for Trust Management

The centralized Public Key Infrastructure (PKI) based system discussed in the previous section is responsible for trust management also. The standards IEEE 1609.2 [142] and ETSI TS 102-941-v1.1.1 [143] specify the trust management in the connected vehicle and C-ITS protocol stacks, respectively. The Security Credential Management System (SCMS) is a large-scale PKI with several enhancements and specifies trust management in a vehicular network. Whyte et al. [145] established it first, and the Crash Avoidance Metrics Partnership (CAMP) improved it further.

The standard IEEE 1609.2.1 has adopted the specifications published by CAMP. A similar specification has also been considered in the ETSI TS 102-941 for trust management in C-ITS. For misbehavior detection and trust management, the SCMS consists following sequence of steps. Misbehavior detection and response consist of a sequence of steps [146]:

- Detection at the vehicles or infrastructure level.
- Reporting to the MA.

- Analysis and correlation by the MA.
- Taking a decision: 1. A request for linkage information from the LAs. 2. Blacklisting the misbehaving entity at the RA. 3. Revoking the entity (invalidating pseudonyms given)

2.9 Summary

In this chapter, we discussed the main research domain of this thesis more clearly by giving an overview of the vehicular network architecture, applications, radio access technologies, protocol stacks, standardization, and project activities. We discussed the state-of-the-art solutions of our selected sub-domains of a vehicular network. From the discussions of state-of-the-art solutions on seamless V2I connectivity in HetNet, privacy, and trust management in a vehicular network, we can conclude that considerable standardization efforts have been made in all these sub-domains. It would be interesting to know the challenges associated with these proposed standard solutions and the research proposal to address them. We discuss each one of them in subsequent chapters and our contributions towards them. In the next chapter, we start with the first issue, which is towards V2I connectivity in HetNets.

Chapter 3

Towards V2I Connectivity

A Multipath Approach in SDN Controlled Small Cells

3.1 Introduction

Vehicle-to-Infrastructure connectivity remains a hot topic due to the growing demand for infotainment applications and services on the move. The evolution in radio access and core network technologies make it more appealing. Given the positives and negatives of each RAT for V2I communication, a combination of RATs forming the HetNets approach might ultimately be an ideal solution for V2I connectivity. HetNets approach can utilize the pros of each RAT to result in a more robust solution. The promising solution in the future may likely utilize the benefits of the cellular, DSRC, and Wi-Fi deployments for better coverage, connectivity, and speed. Besides, the V2I connectivity must also be able to cope with the challenges in dense and small cell deployment due to the high mobility of the vehicle. At the same time, it has to deliver high-speed and reliable V2I connectivity. Consequently, the traditional V2I connectivity must be designed using a new mechanism, devising a new control paradigm that can minimize the impact of disconnections, utilize multiple interfaces, provide the quality of service, allocate the resources efficiently,

and ensure reliability and security. It must also ensure that new applications, rules, and policies can be integrated easily.

The state-of-the-art solutions based on the vertical handover approach proposed by IEEE and 3GPP have laid down stones for seamless V2I connectivity in HetNet. It is continuously being enhanced amended for better performance in new RATs. However, with the evolution of more applications and integration of various features by automotive industries, much effort needs to be put in. Still, there is a long way to go. This section discusses some of the significant challenges associated with ANDSF and MIH solutions for HetNet.

Concerning V2I connectivity over HetNet using MIH, it can provide not only the list of available RATs but also other relevant information that can enable vehicles to select the best and appropriate target network. However, the MIH functions and features in the current state may not be able to assist the vehicle in getting the prioritized list of candidates RATs which it may encounter toward its moving direction. Consequently, a vehicle needs to spend much time discovering target RATs by scanning all available candidate RATs. Therefore, during handover, finding a potential candidate RAT to which the vehicle should handoff is time-consuming and one of the biggest challenges. This may cause higher handover latency and packet loss that can affect the QoS severely. Thus, the current MIH standard needs major modifications to fit in for V2I communications requirements.

In contrast to the MIH protocol, ANDSF provides the mobile node with a list of target networks that may possibly be present in its service area. It also provides the geographical coordinates of those target networks. These characteristics of ANDSF may enable the mobile node to pre-select and store potential target RATs, to which it may likely handover to in the near future. However, most of the solutions proposed by 3GPP support non-seamless WLAN offload (NSWO) and has the ability for a mobile node to offload traffic directly to the Wi-Fi access

network. ANDSF can be considered more promising than the MIH. Having said this, a considerable amount of work is still needed to design and develop mechanisms for network discovery, association, authentication for seamless connectivity that would meet QoS requirements of high-speed mobile nodes moving in a multi-RAT and small cell-based HetNets.

In addition to these standard solutions for HetNet connectivity, various other research proposals and solutions can be found in the literature. Huawei introduced a single radio controller (SRC) entity for unified radio resource and traffic management in a HetNet environment. The SRC consists of an integrated radio network, base station, and Wi-Fi controller to facilitate handover in HetNet and reduce vertical handover latency [147]. Haziza et al. [148] proposed the integration of software-defined radio (SDR) in vehicles for seamless V2V and V2I connectivity across DSRC/IEEE 802.11p and LTE. SDR is a wireless system driven by software routines to support various wireless radios by the same hardware based on software changes. Software-defined network (SDN) is a new network paradigm introduced in 2014 for the vehicle network [149]. Another possible solution for the seamless connectivity in HetNet could be implementing fast vertical handoff between 3GPP and non-3GPP networks. The two popular strategies for inter-networking of 3GPP and non-3GPP networks are tight coupling [150] and loose coupling [151]. In the multipath approach category, the two best candidates at transport layer protocol for multi-RAT connectivity are stream control transport protocol (SCTP) [152,153], and multipath TCP (MPTCP) [154,155].

SRC and SDR solutions have not been able to gain much attention due to their specific hardware and software requirements. In a tight coupling-based solution, the non-3GPP (WiMAX/WLAN) is integrated as part of the 3GPP network (UMTS/3G/4G), and the entire traffic (data and signal) are transferred through 3GPP networks. In dense conditions, the high traffic generated from vehicles is

received by high-speed non-3GPP networks (WLAN) that it passes through the 3GPP network (cellular), which can be a bottleneck due to congestion in the 3GPP network. In the case of loose coupling, the integration between 3GPP and non-3GPP is done via gateway nodes. The underlying RATs functions autonomously, and the traffic of non-3GPP does not pass through the 3GPP network. This solution is cost-effective and simple but increases the handover delay due to signaling between gateway nodes. This might not be suitable for delay-sensitive applications via V2I connectivity such as VoIP. The SCTP deployment requires many middleboxes of the Internet to be changed or upgraded.

Despite various standard solutions and research proposals, seamless V2I connectivity in HetNet remains an open research problem. It is currently a hot topic due to its diverse challenges in the form of faster network discovery, selection of suitable network, fast authentication and handover, meeting QoS requirements, multipath utilization, quick integration of new services, rapid configuration, management, and control of the system, flexibility, programmability, mobility management, and better network resources utilization.

3.1.1 Motivation

From the list of solutions that have been discussed in the previous section, we believe that an amalgamation of MPTCP and SDN could be a potential solution to address most of the existing V2I connectivity challenges in HetNets. This section discusses the key motivation behind selecting these two technologies and testing them in a small cell deployment of Wi-Fi and DSRC.

Wi-Fi and DSRC/IEEE 802.11p are two leading small cell technologies of smart cities. Wi-Fi has high market penetration globally, whereas DSRC/IEEE 802.11p is popular in the USA, Europe, and Japan and has now become mandatory in many cities. DSRC/IEEE 802.11p is mainly designed for vehicular context to provide

safety and non-safety applications. Wi-Fi is primarily an indoor technology for high-speed connectivity, which is now an integral part of the smart cities to offer various services. These two technologies can be utilized for V2I connectivity in smart cities.

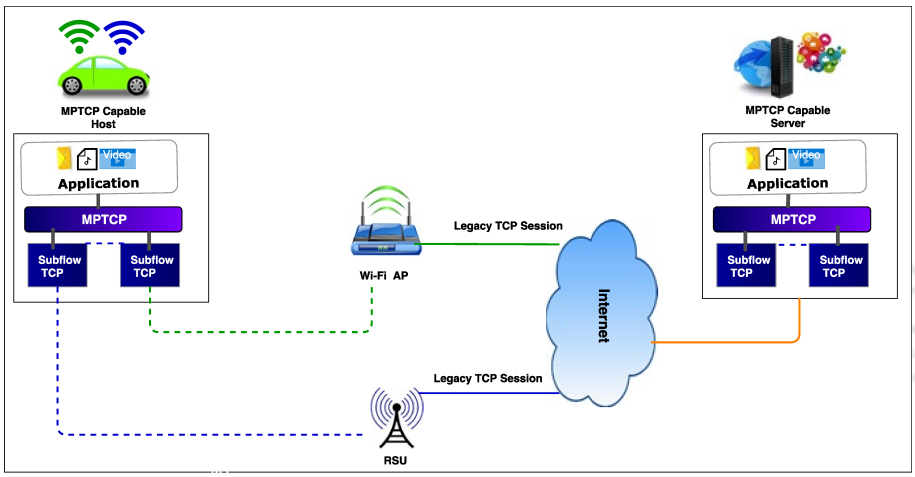


Figure 3.1: MPTCP Capable Host and Server

Most of the end-user devices are now equipped with multiple network interfaces, including the vehicle's OBU. The legacy TCP mechanism uses only one path, even when more than one path between a vehicle and the corresponding node. The MPTCP can enable a vehicle to use multiple network interfaces and IP paths simultaneously. The most significant advantage of MPTCP is that there is no need to change the legacy backbone infrastructure (DSRC, WiFi network, and IP infrastructure). As shown in Figure 3.1, the only requirement is that the end devices need to be MPTCP capable. Unlike the vertical handover approach, it can help to aggregate the available bandwidths of multiple links. It eliminates the need for external gateway nodes or integration of different RATs and, as a result, minimizes additional overhead. It is also resilient to failures; if one path is down or congested, then an alternate path can be utilized. Data transmitted through different paths also helps in providing better confidentiality.

Software-defined Network (SDN) is envisioned as a promising candidate for Intelligent Transportation Systems (ITS) deployment in smart cities. SDN decouples the control plane (network control functions) from the data plane (forwarding functions). The centralized controller implements the control functions, and switches/APs/RSUs are only responsible for data forwarding. The decoupling of the control plane and the data plane makes SDN a desirable technology to efficiently manage, control, monitor, and configure vehicle networks. It brings flexibility, programmability and offers a birds-eye view of the entire network. The application plane facilitates authorities and network operators to set policies and integrate services in a better way. The SDN enables efficient resource allocation and optimization and can deal with heterogeneity. With all these features, SDN is one of the potential enablers for V2I connectivity in small cells.

The traditional TCP cannot benefit from multi-RAT availability. Even in a single RAT, TCP may suffer from high delay and packet loss caused by the frequent handover (in Wi-Fi) or low throughput (in DSRC). MPTCP can address the issues mentioned above. However, when these two small cell technologies are under SDN, the primary challenge is capitalizing on them in the best possible way to deliver V2I-based services. Although SDN and MPTCP in a vehicular network have been investigated separately, they are not applied together concerning vehicular mobility impacts in small cell deployments to the best of our knowledge. Better performance, secure and reliable V2I connectivity is of prime importance in smart cities. The impact of MPTCP and SDN technologies integration needs to be studied extensively. Motivated by all these factors, in this chapter, we analyze and evaluate how MPTCP and SDN together deliver services to the vehicle while moving across small cell deployments of a smart city.

The rest of the chapter is organized as follows. The background details of selected technologies and related works are discussed in Section 3.2. Section

3.3 discusses the experimental setup and provides details of the emulation setup, reference scenario, mobility, and emulation parameters. It also presents the obtained results and discusses the feasibility of the proposed setup. Section 3.4 discusses the proposed mechanism to address the issues observed after the experiment. Finally, Section 3.5 concludes the chapter.

3.2 Background and Related Work

This section presents a systematic study of selected technologies, i.e., small cells (Wi-Fi, DSRC/IEEE 802.11p), MPTCP, and SDN in the context of V2I connectivity. We also discuss previous studies that have used MPTCP or SDN for V2I connectivity.

3.2.1 Background

Small Cells: DSRC/802.11p and Wi-Fi

Hyperdense small-cell deployment is one of the promising solutions to meet the capacity and QoS requirement for various services [156]. Small cells can be categorized into two major categories [156, 157]:

- Small cells of the cellular technology (same technology): micro-, pico-, or femtocells.
- Small cells of different technologies: LTE-femtocells, DSRC/IEEE 802.11p, Wi-Fi, and so on.

In this work, we use DSRC/IEEE 802.11p RSUs and Wi-Fi APs deployments as small cells and refer to them as the multi-radio access technology-based network (Multi-RAT Network). Although these technologies have many similarities, these two differ in frequency allocation, coverage, and connectivity. We present the details of these selected technologies.

Wi-Fi

With the urbanization and development of smart cities, Wi-Fi deployments are rapidly growing, making Wi-Fi a complimentary and low-cost solution for V2I/I2V connectivity. Using massively deployed APs of a smart city to provide V2I connectivity can save considerable deployment costs of any new technology.

Wi-Fi is used within the unlicensed spectrum and operates widely in 2.4 GHz and 5 GHz. In 2.4 GHz, 11 channels are allowed in the USA with a bandwidth of 20/22 MHz and a channel separation of 5 MHz. Wi-Fi has undergone a significant transformation since its conception. For example, IEEE 802.11a/b/g/n/ac/ad are incremental standards that define enhancements mostly in terms of speed [158]. Frequency bands, carrier aggregation mechanisms, spread spectrum techniques, modulation and coding schemes, medium access mechanisms, antenna technologies (such as multiple-input and multiple-output (MIMO)), interference cancellation techniques, and so on are the key elements of enhancements made. Wi-Fi has also seen several security standards enhancements, mainly for authentication and encryption. It starts from wired equivalent privacy (WEP) and then enhanced in an incremented way to Wi-Fi protected access (WPA), WPA2, WPA2-pre-shared key (PSK), WPA2-enterprise (802.1X) [159], and IEEE 802.11i [160] Now the management frames can also be protected using IEEE 802.11w. Wi-Fi is also evolving for fast transition or handover/roaming in addition to speed and security enhancements. For example, IEEE 802.11r for fast transition (FT) roaming via the over-the-air or over-the-distribution system [161].

It should be noted that IEEE 802.11 protocols are not designed to support high mobility network services. Using Wi-Fi to support seamless connectivity for different services presents several challenges. Vehicles may travel at 50 km/h in urban scenarios. Since Wi-Fi coverage is small, the residence time of a vehicle in an AP would be of very short duration. The discovery of the appropriate access

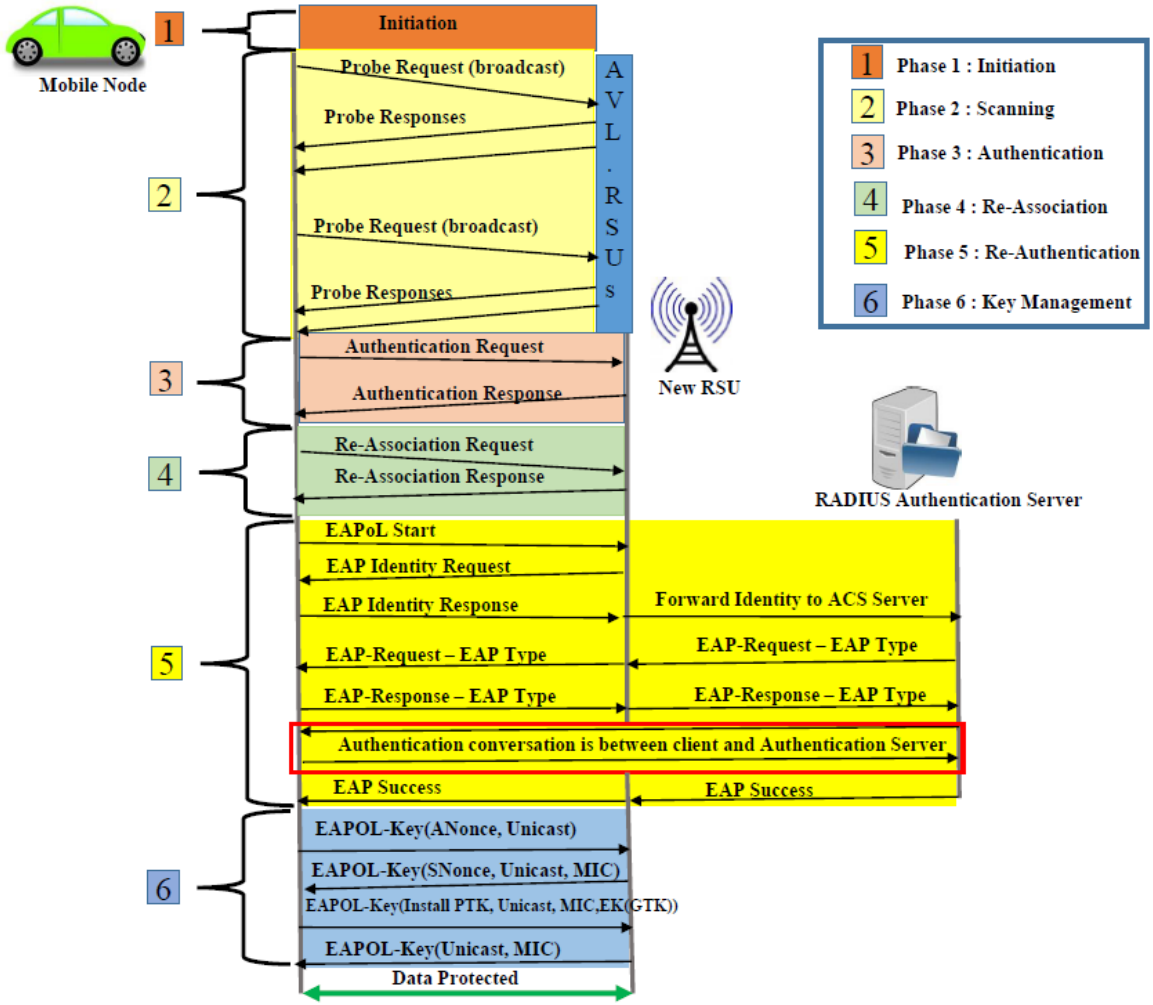


Figure 3.2: Management frame exchange during handover in Wi-Fi using IEEE 802.11i based security [7]

point in the least amount of time is a challenging task. Dense deployment of APs in the urban scenario (due to small coverage) may cause frequent handover and interrupt ongoing communications. Layer-2 and Layer-3 handover latency in Wi-Fi may disrupt several delay-sensitive applications. It may also increase the interference, and this can reduce the handover decision quality. In this work, we focus mainly on intra-domain handover. The intra-domain handover is also referred to as a Layer-2 handover or Link Layer Handover. The intra-domain handover is

Basic Service Set (BSS) transition within the same Distribution System (DS). All-access points (APs) in the distribution system (DS) are configured with the same IP subnet mask.

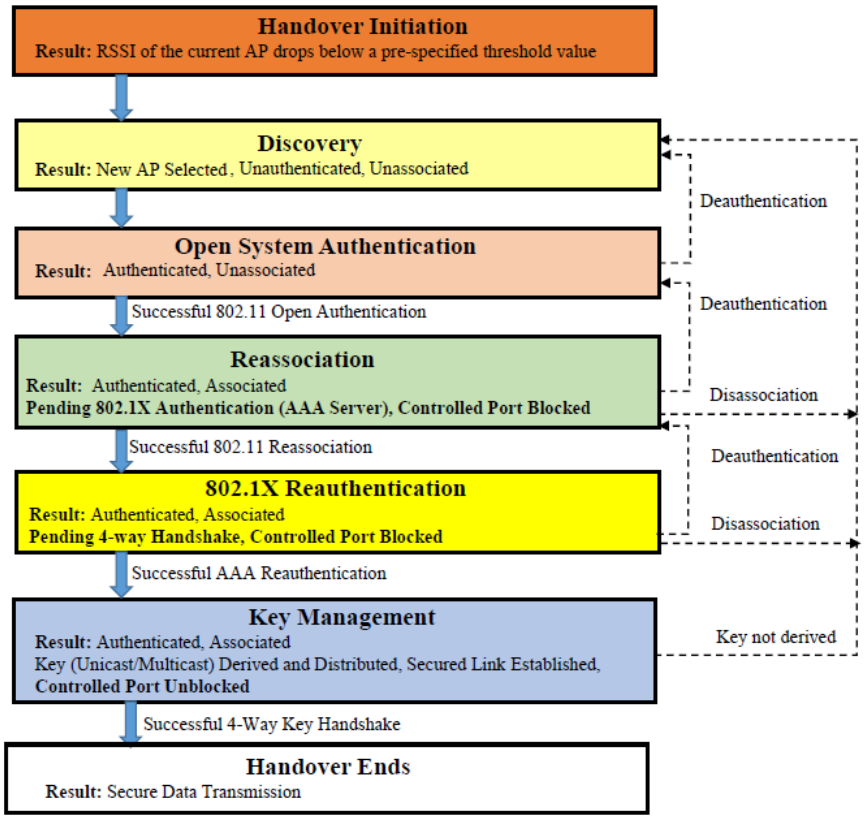


Figure 3.3: Phase Transition during handover in Wi-Fi using IEEE 802.11i based security [8]

Layer-2 handover process based on the 802.1X/EAP security framework could consist of 6 phases: initiation, discovery, 802.11 open authentications, Re-association, Re-authentication, and the key handshake. The set of management frames that are exchanged during handover in IEEE 802.11i is shown in Figure 3.2 and detail of Layer-2 phase transition in Figure 3.3. From Figure 3.2, it is clear that the total Layer-2 Handover time TL2Handover can be estimated as follows:

$$T_{L2Handover} = Time_{Phase2} + Time_{Phase3} + Time_{Phase4} + Time_{Phase5} + Time_{Phase6} \tag{3.1}$$

Only two management frames are exchanged between the station and an AP in Phase 3 and Phase 4. Delay incurred in these two phases is negligible and can be neglected. Three main contributors to the handover delay are Phase 2, Phase 5, and Phase 6. The discovery delay is the dominating component of the Layer-2 handoff delay [162] [163]. The re-authentication phase that includes key-handshaking is equally time-consuming. It varies between few milliseconds to the second [162], depends on which authentication mode (Pre Shared Key (PSK) or 802.1X/EAP) and protocol used. Therefore, the Layer-2 handover itself can severely affect QoS and quality of experience (QoE) for real-time applications and ITS services in the 802.11i enterprise-based security framework.

DSRC

As shown in Figure 3.4, the allocated DSRC licensed spectrum of the 75 MHz (5.850-5.925 GHz) is divided into seven 10 MHz channels in the USA. One of which is a control channel (CCH), the other six are service channels (SCH). In addition to these seven channels, 5 MHz is reserved for future use [164]. The CCH is assigned number 178, which is the default and highest priority channel and is mainly used for critical safety applications. SCH channels can be used for safety as well as non-safety applications. The DSRC uses a channel width of 10 MHz that supports a bandwidth of 3 Mbps to 27 Mbps. It also allows two SCHs to be combined to form a 20 MHz channel width to provide a higher data rate of 54 Mbps. For example, channels 174 and 176 (used for medium-range services) and channels 180 and 182 (short-range services) may be combined to form a single 20 MHz channel supporting high data rates.

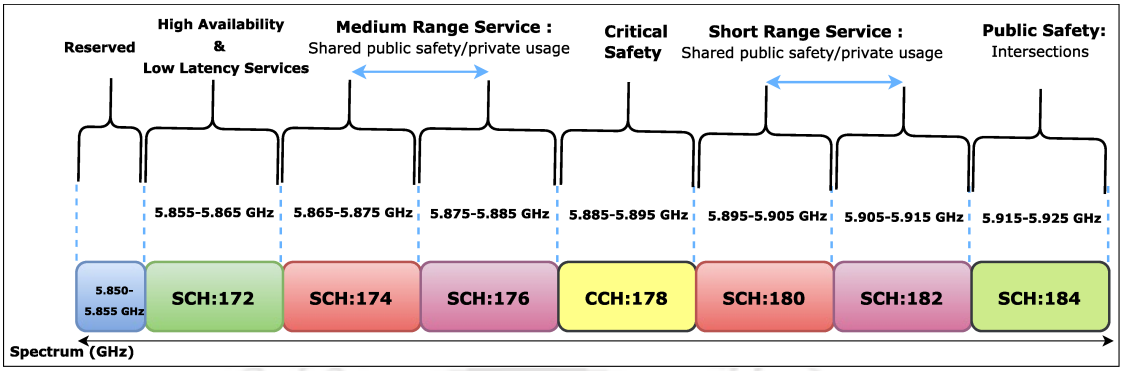


Figure 3.4: USA DSRC spectrum allocations and its applications [9]

The physical (PHY) and lower-Media Access Control (MAC) layers of the WAVE protocol stack are defined in the IEEE 802.11p standard. IEEE 802.11p is an enhancement of IEEE 802.11a (amendment to IEEE 802.11-2007) to support vehicular communication using DSRC. The differences between IEEE 802.11p and IEEE 802.11a at the PHY are shown in Table 3.1. IEEE 802.11p runs at half the clock rate of IEEE 802.11a (channel of 10MHz), which helps to resist the effects caused by the Doppler spread (due to high mobility and other factors) and reduces inter-symbol interference in a channel. The transmission power output of IEEE 802.11p (2-30W) is much greater than IEEE 802.11a (less than 200mW) and provides broader coverage (approx. 1000 meters in the line of sight) than Wi-Fi. The effects of Orthogonal Frequency Division Multiplexing (OFDM) on Vehicle-to-Everything (V2X) communication can be found in [165].

The WAVE protocol stack uses the IEEE 802.11e Enhanced Distributed Channel Access (EDCA) protocol to prioritize the traffic based on its category at the lower-MAC layer. The four access categories(ACs) defined in IEEE 802.11e are Voice (VO), Video (VI), Background (BK), and Best Effort (BE). The queues are assigned to each access class and serviced as per the priority of the AC. Each queue is assigned contention parameters Arbitration Inter-Frame Spacing (AIFS) and Contention Window (CWmin and CWmax). The highest priority AC uses

Parameters	**IEEE 802.11a**	**IEEE 802.11p**	**Changes**
Channel Width (MHz)	20	10	Half
Signaling	OFDM	OFDM	No Change
Bit rate (Mbps)	6,9,12,18,24,36,48,54	3,4.5,6,9,12,18,24,27	Half
Modulation mode	BPSK, QPSK,16QAM, 64QAM	BPSK, QPSK,16QAM, 64QAM	No change
Code rate	1/2, 2/3, 3/4	1/2, 2/3, 3/4	No change
Number of subcarriers	52	52	No change
Symbol duration	4μs	8μs	Double
Guard time	0.8μs	1.6μs	Double
FFT period	3.2μs	6.4μs	Double
Preamble duration	16μs	32μs	Double
Subcarrier spacing	0.3125MHz	0.15625MHz	Half

Table 3.1: IEEE 802.11a/p PHY parameter comparison [15]

smaller contention parameter values.

Some of the important changes made at layer-2 of the 802.11 communication protocol stack that eliminates or shorten phases of layer-2 handover. The mobile nodes using IEEE 802.11p over 5.9 GHz DSRC band in the USA or EU send data frames outside the context of a BSS (OCB), thus avoiding the authentication, association, or data confidentiality phases of layer-2. Since the OCB communication of V2V and V2I occurs in a dedicated frequency band for safety and non-safety, there is no need to scan the channel. Therefore, IEEE 802.11p eliminates the layer-2 handover delay due to discovery, authentication, association, and key establishment phases. However, there is a provision to secure the V2I communication outside the MAC layer.

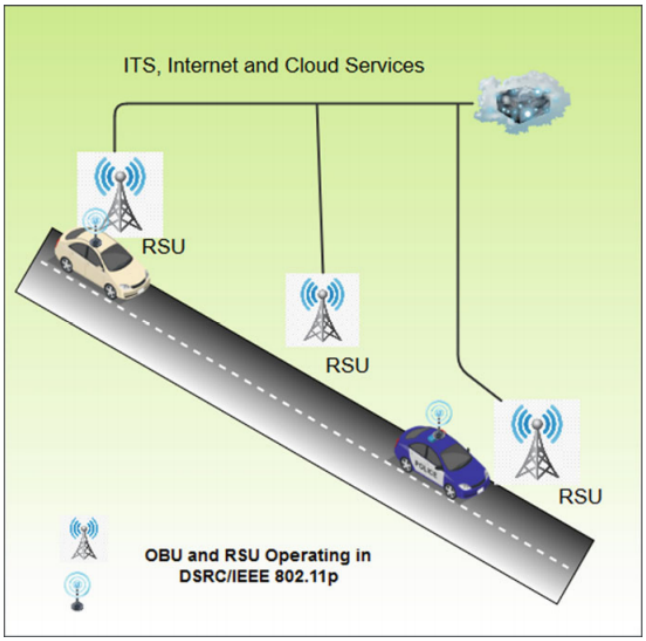


Figure 3.5: V2I Connectivity in DSRC/IEEE 802.11p

As shown in Figure 3.5, the RSUs deployed alongside the road also act as an infrastructure router. In IEEE 802.11p, deployment and movement detection between two adjacent RSUs are harder for the mobile nodes because it does not rely on layer-2 triggers (unlike IEEE 820.11 association and dissociation phase). In OCB mode, it is difficult to detect when they are about to leave the associated RSU and move to another RSU. In such a context, there is a need for a movement detection mechanism that can utilize other triggers and detect handovers. One such mechanism can be taking advantage of positioning data (latitude and longitude) broadcasted in various messages. MIPv6 specifies a new option for router advertisement (RA) called the "advertisement interval option (AI)." Using this option, an RSU can indicate the maximum interval between two consecutive unsolicited router advertisement messages broadcasted by this RSU. This allows a mobile node to learn when it is supposed to get the next RA from the same RSU and, in turn, can help in detecting the movement. When specified time interval elapses

without the mobile node receiving any RA from that RSU means that the RA has been lost. Now, it is up to the mobile node to decide how many lost RAs from that RSU can be considered as a handover trigger. If RA frequency is increased, it reduces the discovery delay of the target RSU and enables faster detection of potential RSUs. When multiple RSUs are detected, it is recommended that the mobile node should consider better signal quality for a handover decision. Once target RSU has been selected, the optimistic DAD is recommended to speed up the auto-configuration to reduce layer-3 handover delay. Therefore, a combination of all these mechanisms for IEEE 802.11p ensures faster layer-2 and layer-3 handover for V2I communication. These overall changes make the IEEE 802.11p standard fast and suitable for V2I communication [166].

MPTCP

The main motivation for MPTCP design is to enhance resource utilization and resilience to failures. MPTCP uses multiple available interfaces in order to aggregate the bandwidth and hence provide better QoS. The necessary condition for this protocol to work is that both server and client need to be MPTCP capable, and at least one of them is multi-homed. It is backward compatible and provides at least the same as what best is possible when the connection is a single path. MPTCP differs from the previous Stream Control Transmission Protocol (SCTP) technology of IETF that has more features. However, SCTP deployment requires many middleboxes of the Internet to be changed or upgraded.

MPTCP is a transport layer protocol, and an extension of TCP [167]. It is a layer between the application and network layer, as shown in Figure 3.6. It aggregates several TCP connections, called "subflows". A subflow is a same as TCP connection characterized by same tuple ($Source_{IP}$, $Source_{TCP-port}$, $Destination_{IP}$, $Destination_{TCP-port}$). Each subflow is assigned a unique identifier called subflow-id,

which is generated by the MPTCP stack. The subflow-id is used to inform subflow related advertisements. Steps involved in MPTCP session initiation and sub-flow establishment are shown in Figure 3.7 and details are summarized as follows:

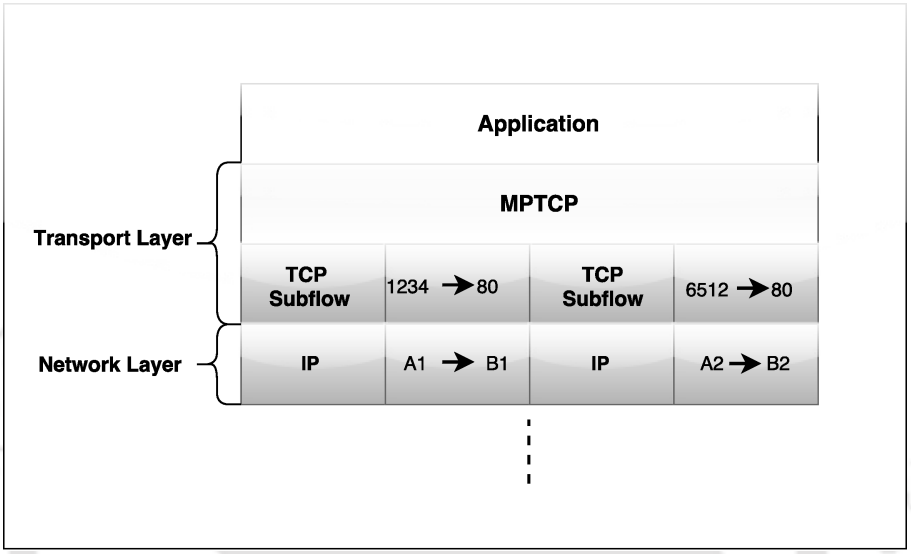


Figure 3.6: MPTCP Stack

MPTCP Session Initiation With the help of DNS, a vehicle checks that the server is reachable from any of its interfaces (say from interface A). A three-way handshake is performed, which is similar to the simple TCP; however, at the options field, it carries $MP\_CAPABLE$ options that are only understood by the MPTCP stack. With this $MP\_CAPABLE$ option, both vehicle and server come to know that they have MPTCP capabilities. In order to begin the MPTCP session, the first handshake SYN with an $MP\_CAPABLE$ from the vehicle(V) to the server (S) is sent to notify the server that it has MPTCP capability. It also sends Key_V (random key generated by the V) in the first handshake. Upon reception of the first message, the S responds with an SYN/ACK, with the $MP\_CAPABLE$ option and Key_S (random key generated by the S). The Key_S is reflected by the V in the final TCP handshake A along it's with Ack, $MP\_CAPABLE$, and Key_V. At the end of the handshake server, S creates the state and exchanges the random keys.

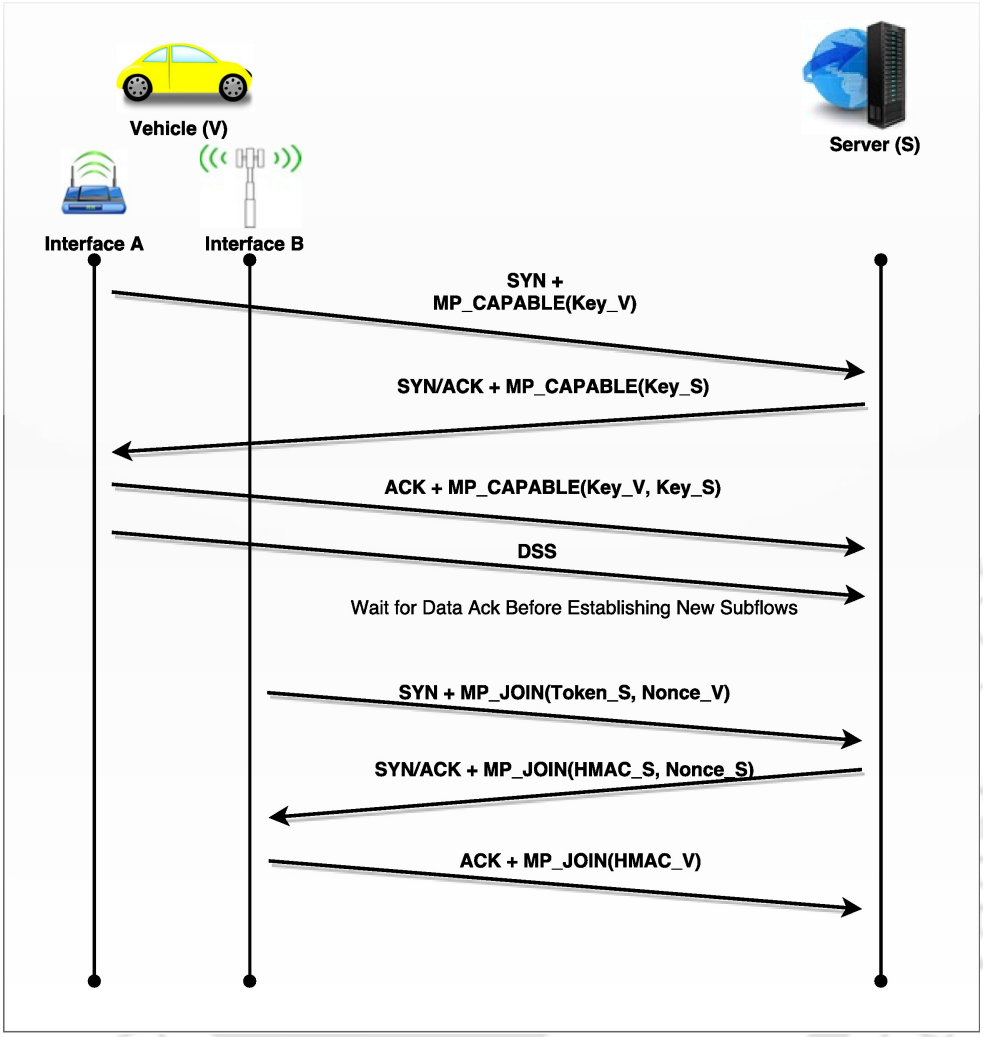


Figure 3.7: MPTCP Session Initiation and sub-flow establishment

The keys Key_V is later hashed and used by MPTCP to authenticate additional sub-flows. This Key_S allows the S to operate in a stateless mode.

Addition of subflows: Once the MPTCP session is completed, vehicle V can add a new subflow as soon as a Data Sequence Signal (DSS) option with a Data Ack is received (requires at least two RTTs). At any point, either end device (S or V) can try to add new subflows. Assume that V wants to create a subflow between its interface B (Address 2) and S's interface. Again a new MTCP three-way handshake

starts with the MP_JOIN option. This time the option is different because now, new subflows to be created need to be attached to the existing MPTCP session. Vehicle V can establish a new sub-flow using the same connection but has to join to the correct context in server S. V attaches $Token\_S$ to the MP_JOIN option. The token is the hash of the key generated during session initiation. Upon reception, the Server S responds with SYN/ACK, with MP_JOIN option but without a token, because V already has a state for that subflow. Then vehicle V acknowledges with ACK with the MP_JOIN, in the context of server S. And subflow is ready for use.

Each session in MPTCP is carried by several subflow if the two communicating nodes have multiple end-to-end paths. Each sub-flow is similar to an independent regular TCP connection on one of the available paths. TCP segments generated at the sender end are transmitted to different subflows over different paths. At the receiver end, all the segments coming from different subflows are reassembled to construct the original data stream. Therefore, it allows all the applications based on TCP to take benefit from the multipath gain in a transparent manner.

Connection Management: MPTCP provides path management (fullmesh, ndiffports, etc.) to detect and use available paths between two communicating devices. It uses a packet scheduler to control transmission over the available paths and reorder segments. The default scheduling of MPTCP is Lowest-RTT-First (LowRTT); another well-known example of scheduling is round-robin. MPTCP supports a fallback mechanism, i.e., upon failure, it falls back to legacy TCP. Different congest control mechanisms have been developed, such as Linked-Increases Algorithm (LIA), Opportunistic Linked-Increases Algorithm (OLIA), Balanced Linked Adaptation (BALIA), etc., to achieve fairness, resource pooling, and stability.

SDN

In this section, we systematically define the flow setup (reactive rule installation) of the SDN architecture for V2I connectivity (Figure 3.8). In SDN controlled wireless environment, the APs and RSUs work as OpenFlow switches. These devices exchange OpenFlow messages with the controller (via control plane) whenever they see data traffic for which they do not already have flows established. All these devices consist of hardware and software. The hardware contains flow tables and other components, and the software must have OpenFlow Agent (OFA) that implements communication with the controller using the OpenFlow protocol. In our SDN-based V2I communication scenario, the rules are installed reactively, as it is explained below.

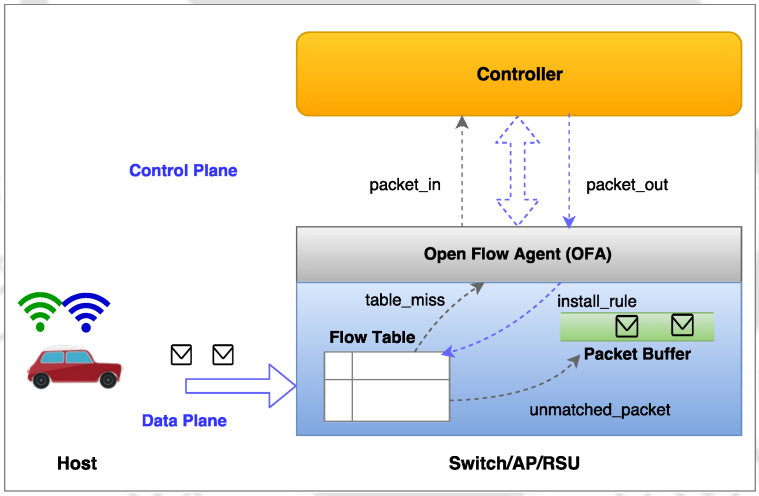


Figure 3.8: OpenFlow Switches/APs/RSUs with Controller in SDN

Reactive Rule Installation: This is an on-demand approach, and APs/RSUs and Switches explicitly request the controller to define the rules for them. For example: When AP received a new request from the hosts (no entry in Flow Table), AP may ask the controller to define the new rule. The details of the processes involved in the installation of the reactive rules at AP/RSU/ are as follows [168,169]:

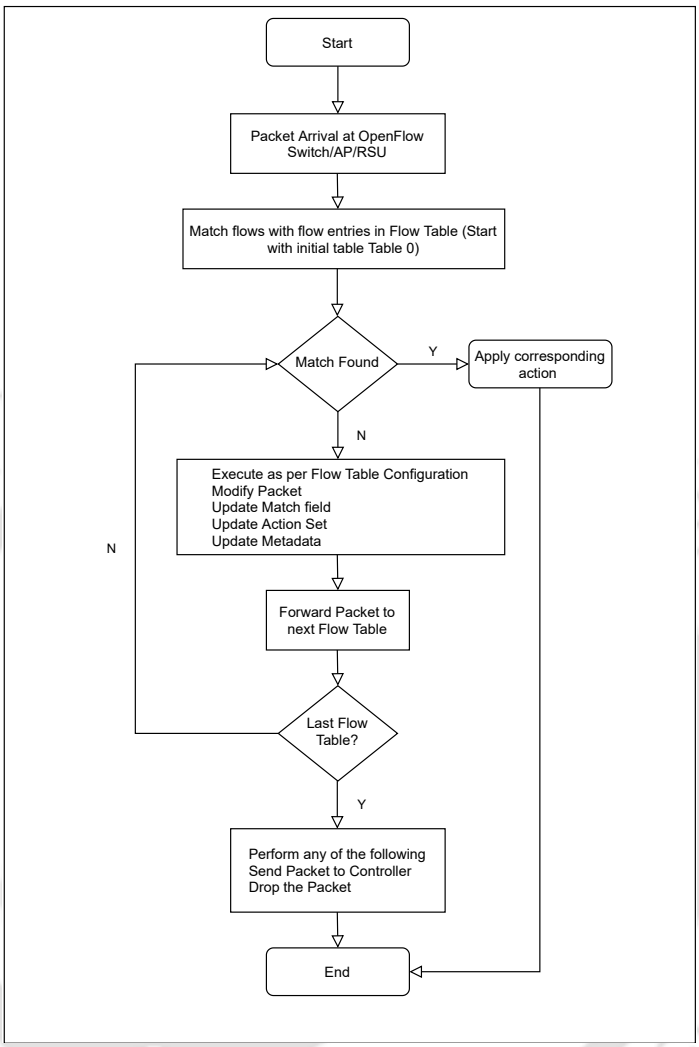


Figure 3.9: Flow chart for packet processing in OpenFlow Switches/APs/RSUs [10]

Figure 3.9 shows the process on an arrival of a packet to OpenFlow devices. The first step is establishing the connection via the Layer-2 association. Once the host is associated with the AP/RSU, it generates data traffic, requesting certain services from the corresponding server/node. When a packet generated from the host arrives at an AP, the AP first parses the header and looks up in its flow table using the header fields and the input port (Matched against flow entries). If a flow entry is found, where the header field wildcard matches the header, that particular

entry is considered to update the associated counters and apply the corresponding action (forward the packet to a port). In case of several such entries (one or more) are already present in the flow table, matching of the packet is done based on the priority, i.e., the entry with the highest priority is selected for packet forwarding. If no matching entry is found in the Flow Table, it triggers the table_miss event to the OFA. If AP has Packet Buffer, it stores the packet in the buffer, encapsulates a fraction of the packet (first byte) into a packet_in (flow request), and sends it to the controller via the control plane. If AP is not capable of buffering or its Packet Buffer becomes full, the OFA encapsulates the entire packet into packet_in and sends it to the controller.

Upon receiving a packet_in message, the controller identifies the required action for the packet and sends a set of rules (appropriate entries) to the requesting AP (via packet_out). Usually, the controller sets up the entire path for the packet_in the distribution system by modifying the flow tables of all APs on the path. Upon receiving a rule from the controller, the AP's OFA checks whether its Flow Table is full. If there is space, the rule is inserted and forwards the buffered packets as per the defined rule; otherwise, the rule is dropped, and an error message is sent to the controller. Each rule (entries in the Flow Table) is assigned a HARD_TIMEOUT and IDLE_TIMEOUT that jointly determine how long the flow entry (rule) can exist.

3.2.2 Related Work

Previous studies for V2I connectivity used legacy TCP in DSRC/IEEE 802.11p [170], Wi-Fi [171–175] and, LTE technologies [176–179], while others have studied MPTCP either in fixed or low mobility scenarios such as walking speed environments.

MPTCP is new in the context of V2I communication, and we could find only two sound research studies. The authors of [180] investigated the use of MPTCP for

V2I communication in Wi-Fi (802.11n), DSRC and 3G. They observed that when MPTCP is used across similar characteristics links, throughput in most cases is at least as good as single-path TCP. However, when paths are asymmetric (regarding RTT and bandwidth), the MPTCP performs worse than single-path TCP. They tested MPTCP with a single mobile node accessing the RSU and a single low priority traffic class. The impact of Layer-2 handover between access points is not that much reflected in this study. In [154], the authors investigated the performance of MPTCP in V2I and V2V under distinct velocities in LTE and Wi-Fi access networks. They observed that the MPTCP maintains comparable performance to simple TCP. MPTCP can replace vertical handover technologies [181, 182], allowing vehicles to connect to different RATs available on the path simultaneously. However, MPTCP is not much explored in the V2I context.

The work by Ku et al. [149] in 2014, the first work to introduce SDN into VANET. The authors demonstrated how SDN as an emerging network paradigm with its flexibility and programmability features could facilitate new services to VANETs. The authors compare SDN-based routing with traditional MANET/VANET routing protocols using simulation. In 2016, the authors [183] proposed a software-defined vehicular network (SDVN) framework to enable vehicular communication in HetNets. The authors presented the opportunities and challenges of applying the SDN to a vehicular network scenario. They proposed an approach to mitigate the heterogeneity of the vehicular network that abstracts all the networking components in a unified manner. In [184], the authors performed offloading from the cellular network to 802.11p network under SDN architecture. They proposed Offloading with Handover Decision based on SDN (OHD-SDN) scheme. The controller collects all vehicles' and RSUs' contexts such as speed, geographical position, direction, and sensed neighboring RSUs' IDs and then decides whether it is valuable to offload or not. The proposed scheme considers both the

quality of the network and the estimated residence time of a vehicle in the RSU to make a decision. In the literature [185–188], the researchers have also tried to explore how emerging technologies such as fog computing, network function virtualization (NFV), mobile edge computing (MEC), named data network [189] and artificial intelligence can play a role in the SDVN to facilitate quality of service and quality of experience requirements. We found two good studies [190, 191] that attempted to address the issues that arose due to vehicular mobility in SDVN. In [190], the authors proposed software-defined IoV (SDIV) architecture to address the increased complexity issues and problems related to scalability and services deployments. They also developed a novel mechanism for rule installation that reduces the number of rules required for services in SDIV. In [191], authors designed and implemented various mobility management approaches (reactive, proactive, and delegated approach) in SDNized wireless networks. They also investigated the impact of the overall handover delays and tried to address the scalability issue with a specific focus on mobility management.

An amalgamation of MPTCP and SDN can play a crucial role in improving the V2I connectivity in a heterogeneous network scenario. Before proposing improvements and enhancements, such technology integration needs to be tested with vehicular mobility. We need to explore how it works in the default setup. We test the default MPTCP performance in small cells under SDN, then measure the effects of handover and flow setup, which is not much reflected in the previous works. To the best of our knowledge, this is the first study in which both MPTCP and SDN are explored for V2I communication in small cells.

3.3 Experimental Evaluation

The performance of the proposed technology integration for V2I connectivity is evaluated through an emulation setup. This section summarizes the experimental

setup and then provides the details of the reference scenario used in the experiment. We list emulation parameters used for performance analysis in a tabular form. Further, the emulation results are used to demonstrate the feasibility of the proposal.

3.3.1 Emulation Setup

The emulation setup we use incorporates most of the component which is deployed in the real-world scenarios. We found that many simulation/emulation-based studies miss the important elements and factors and fail to map to practical deployments. The details of our emulation setup are summarized as follows.

We use Mininet-WiFi emulator [192], which is a fork of the Mininet SDN network emulator that extends the functionality of Mininet. It facilitates users to create virtualized Wi-Fi stations and APs by using standard Linux wireless drivers and the 80211_hwsim wireless driver. We use background scanning for scanning the deployed Wi-Fi APs and OCB mode for the IEEE 802.11p setup. The resemblance of OCB mode is done in such a way that a vehicle can directly communicate to the RSUs without any Layer-2 handover delay due to scanning and re-authentication. It allows data frame exchange establishment in milliseconds. To implement the layered security method that can provide Authentication, Authorization, and Accounting (AAA) in smart city Wi-Fi deployment, we use the Remote Access Dial-In User Service (RADIUS) protocol. The IEEE 802.11r as Fast Basic Service Set Transition (FT-BSS) Over-the-DS FT-BSS for fast re-authentication is used. In over-the-DS FT, the host credentials are passed from one AP to the others in the mobility domain using action frames (management frame) over the DS (wired network interconnecting APs). The complete handshaking for re-association (Phase 3, 4, 5, and 6 of Figure 3.2) is done only once with the first AP during its initial joining. Later on, First AP "vouches" for the host to the other APs in the mobility domain. Now, the remaining APs need not re-verify again, and with only four management frames

(Passing seeds, verification and key generation, re-association request (verification of encryption key), and re-association response) exchange host can easily connect to the target AP. There is an alternative method called over-the-Air (OTA) FT, where the host directly communicates with the target AP over the air. However, the host needs to leave its active channel to negotiate on another channel during scanning, which can interrupt ongoing communication if the host is already at the edge of the AP coverage.

We use MPTCP Linux Kernel to make vehicle and corresponding node MPTCP capable (Figure 3.1) and enable the vehicle to use both interfaces simultaneously. For SDN integration, the POX SDN controller, a simple-to-use SDN controller coupled with a Mininet-WiFi SDN network emulator. This SDN controller programs the OpenFlow-enabled switched and APs deployed in our reference scenario using the Mininet-WiFi network emulator. The components of the POX controller are Python programs. By invoking the POX components, we implement networking functions. We modified the stock components of POX *l2_learning* to set HARD_TIMEOUT and IDLE_TIMEOUT and for communication to AAA server in Wi-Fi. The setup has been implemented in the Mininet-WiFi userspace, which allows us to implement our specifications and modifications, but it is not faster or almost slower than kernel space.

Reference Scenario

As depicted in Figure 3.10, we consider two RATs DSRC/IEEE 802.11p and smart city Wi-Fi setup for V2I based services and applications. We select the urban road segment for the experimental study. RSUs (IEEE 802.11p) and Wi-Fi APs are deployed in an umbrella fashion and cover the entire road segment. Wi-Fi APs belong to the same ESS, and vehicles perform intra-domain handover (same mobility domain). The corresponding node is MPTCP capable and represents the server

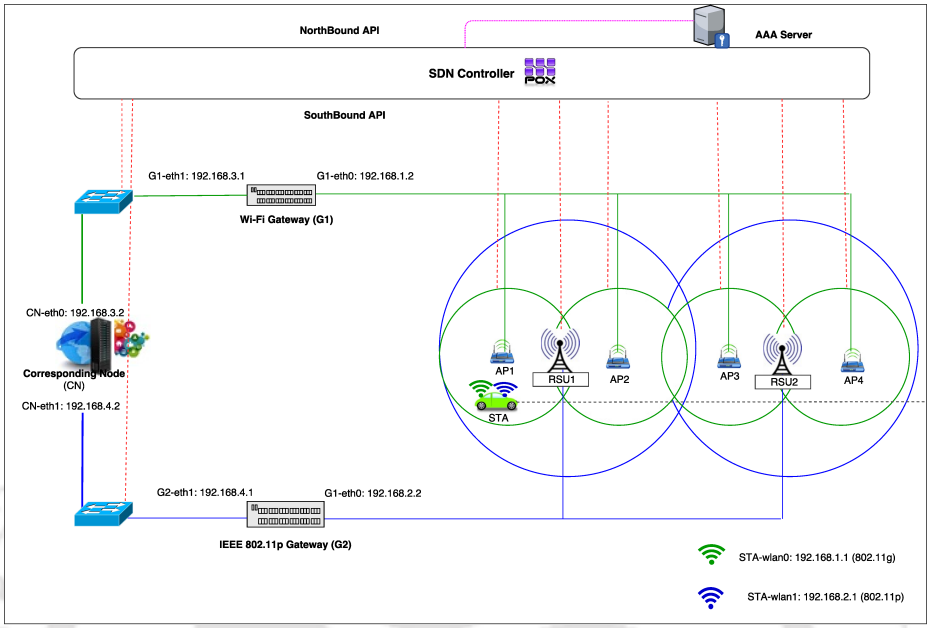


Figure 3.10: Reference Scenario: V2I Connectivity in SDN controlled Small Cells

installed at smart-city road authority to maintain real-time traffic information. The vehicles' onboard unit is equipped with two wireless interfaces: IEEE 802.11p and Wi-Fi. The vehicle drivers try to fetch traffic data from the server using MPTCP while moving across RSUs and APs in the selected road segment. The AAA server is installed by the road administration authority to allow an authorized vehicle to access applications and services in a secured manner via Wi-Fi APs. The security features in IEEE 802.11p are provided by the security entities defined in IEEE 1609.2.

Vehicular Mobility using SUMO

In this subsection, we present the real road network segment of the USA city Brooklyn obtained using the OpenStreetMap (OSM) [193]. This road segment from OSM is imported to Simulation of Urban Mobility (SUMO) [194] using an application called the NETCONVERT. SUMO is one of the most popular traffic

simulators, and it has a large number of features built-in. Figure 3.11 shows the procedure involved in obtaining real-world traffic using SUMO. Figure 3.12.a, and 3.12.b show the OSM file and the corresponding SUMO NET file of the Brooklyn city.

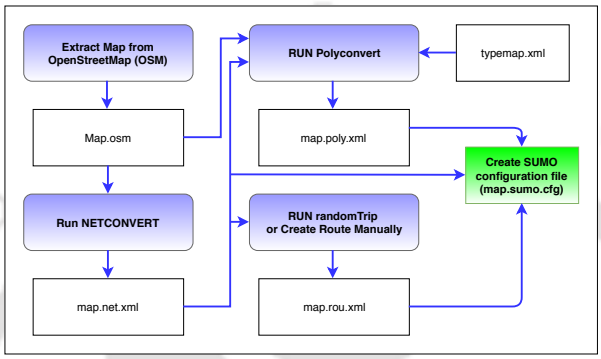


Figure 3.11: Overview of the steps involved in road traffic generation using SUMO

As a traffic simulator integrated with Mininet-WiFi emulator, SUMO helped us map our experiment close to a realistic scenario. The snapshot of network emulation on Mininet-WiFi for corresponding road traffic of SUMO is shown in Figure 3.13.

Emulation Parameters

Table 3.2 list details of parameters used in our emulation setup.

3.3.2 Results and Discussion

We investigate two SDN-controlled scenarios for performance evaluation: Single path TCP performance over Wi-Fi deployment (four APs) and MPTCP performance with 802.11p (two RSUs) and Wi-Fi (four APs) with vehicular mobility generated from SUMO. In each of these experiments *IPerf* [195], is used to measure the performance. *Tcpdump* packet analyzer is used to capture the communication details in pcap format, and Wireshark and *Synthetic Packet Pair* [196] tools for packet loss and

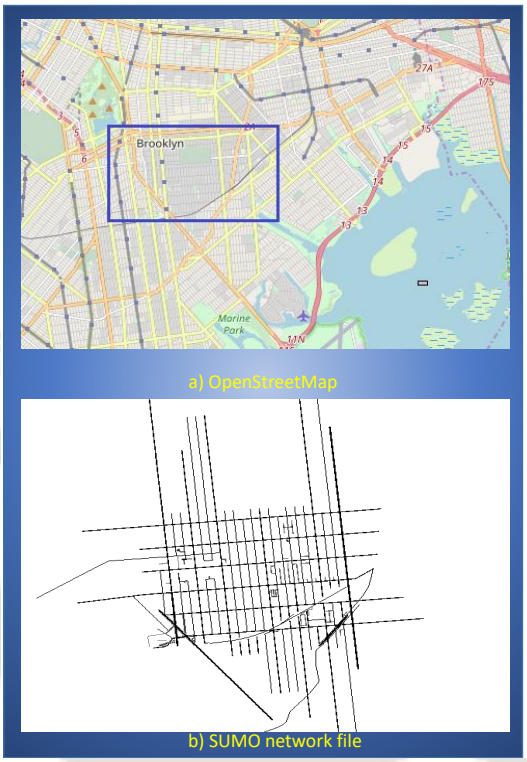


Figure 3.12: a. Map of Brooklyn city obtained from OpenStreetMap. b. SUMO network file corresponding to OSM of Brooklyn city road segment

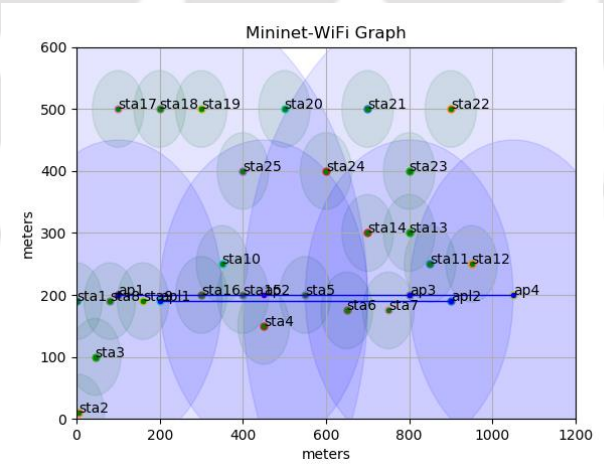


Figure 3.13: Network Topology on Mininet-WiFi Emulator

Parameters	Values
Operating System	Ubuntu 16.04-LTS
AAA Server	FreeRADIUS Version 2.1.12
Wi-Fi Emulator	Mininet-WiFi
SDN Controller	POX Controller
RSU Antenna Type	Omnidirectional
Propagation Model	Log Distance Propagation Loss Model
Path Loss Exponent	3.5 (Urban)
Area	Urban Approx. 1.5 x 1.5 km^2
Mobility	SUMO (Traffic Simulator)
Number of WiFi APs	4
Number of RSUs	2
Maximum Velocity	Approx 14 m/s
Radio Range of WiFi APs	250 m
Radio Range of RSU	500 m
Wireless Mode	IEEE 802.11g (54 Mbps), OCB (27 Mbps)
Authentication Mode	WPA-Enterprise: 802.1X/EAP and FT-EAP
Authentication Protocol	EAP-TLS
Traffic Generation	Simple HTTP, IPerf
Protocols Used	ICMP, TCP, MPTCP
MPTCP Connection	Scheduler: default, Path-manager: fullmesh
WLAN Security Framework Tested	IEEE 802.11r FT over-DS
Emulation Duration	120 second
Performance metrics	Packet Loss, Round Trip Time (RTT) and Avg.Throughput

Table 3.2: Emulation Parameters

Round trip time (RTT) measurement. We captured the throughput values for each interface via *ifstat* while *IPerf* was running and verified it with the Wireshark throughput graph for each data stream.

Challenges due to mobility in SDN-based deployments

In this section, we discuss and demonstrate the challenges due to mobility in the SDN-based framework. We take a simple example of single-vehicle mobility, in which a vehicle moves across different APs, and while moving from one AP to another, it pings the corresponding node continuously. The vehicle re-associates with multiple APs (Wi-Fi) and connects to CN using only one interface (STA-wlan0). When the

vehicle under AP1 initially connects to it and transmits messages to the CN (after Layer-2 handover), the first packet received by AP1 is transmitted to the controller due to table_miss event (no entry in Flow Table). As the controller is aware of the direction in which the packet has to be sent, it generates flows to be added to AP's. The rules are installed to just AP1, and now the vehicle can communicate to the corresponding node using rules present in AP1. There are two timeouts defined in the controller, which are :

- IDLE_TIMEOUT : A flow entry is deleted if it was inactive for IDLE_TIMEOUT period.
- HARD_TIMEOUT : A flow entry is deleted irrespective of its activity after HARD_TIMEOUT.

When due to mobility, vehicle handover from AP1 to AP2, AP2 initially has no flow entries for vehicle's communication to CN. A packet destined to the CN is sent to the controller first. In response, the controller sets rules in AP1 and AP2 for the STA to CN communication. AP1 now has two entries for packets coming from the Wi-Fi gateway (G1). In the framework, the controller assigns the same priority to both the flow entries and is queued one after another. The incoming packets are matched against the flow entries created first. This implementation and TIMEOUT's of the controller cause the problem in a data flow. If IDLE_TIMEOUT is small and HARD_TIMEOUT is very large (which is a common implementation in controllers), and the vehicle is connected to AP2, AP1 still has previous flow entry for a packet coming from the Wi-Fi gateway (G1). The incoming packet from G1 is directed to the vehicle's Wi-Fi interface (STA-wlan0) via AP1 port, which was present earlier before the vehicle disconnected from AP1. However, a vehicle has moved to AP2 and is not connected with AP1; no reply packet reaches the vehicle. As IDLE_TIMEOUT is small, no packet is sent to the flow from AP1 to AP2, and the corresponding flow entry gets deleted. The final flow entries in AP2 are from

STA-wlan0 to AP1 and AP1 to STA-wlan0, and in AP1, the entries are from AP2 to G1 and G1 to STA-wlan0. No packet reaches the corresponding node till the G1 to STA-wlan0 entry gets deleted after HARD_TIMEOUT. This problem arises during every handover.

The solution to this problem is matching the incoming packet's header with the flow entry corresponding to the header (if multiple matching entries are present), which is inserted most recently or deleting the flows frequently. We implemented the later solution at the controller by assigning IDLE_TIMEOUT and HARD_TIMEOUT 1ms each. This leads to very frequent deletion of flow entries, and older flows do not sustain for a longer duration. As new flows are present after a HARD_TIMEOUT period, the system works perfectly, and STA is reachable. However, this implementation leads to an increase in the average RTT value.

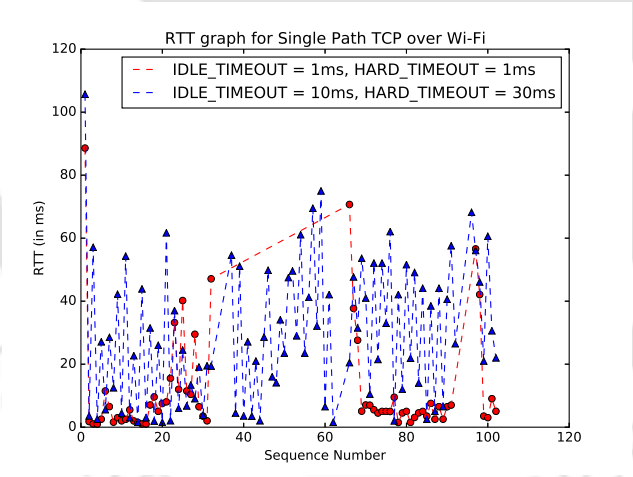


Figure 3.14: RTT Graph over Wi-Fi with ICMP (Ping) traffic

We analyze the impact of IDLE_TIMEOUT and HARD_TIMEOUT with default values (10ms and 30ms respectively) and keeping 1ms each. We use single node mobility and generated ping traffic to the CN node from that STA. The RTT plot is shown in Figure 3.14 with ping traffic (ICMP packet from STA to CN and vice versa) over the Wi-Fi network. With default values, the flows

stay for the defined duration in AP's, and the average RTT value remains low. However, packets are dropped after a certain period due to the problem stated above. In case of 1 ms duration, the flow entries are deleted frequently (after every HARD_TIMEOUT), the new incoming packet to AP is sent to the controller, which takes its time to create new flows, and then packets to CN are directed according to the flow entries. Although with this approach, a single node can communicate, the performance (RTT, packet loss, throughput) may degrade severely when more nodes are requesting the services. This part we demonstrate in the next subsection.

Performance of TCP and MPTCP for V2I Connectivity

After a discussion and demonstration of the SDN-related issues in mobility conditions, we evaluate the performance of TCP and MPTCP for V2I connectivity using a reactive rule installation mechanism by the controller. The IDLE_TIMEOUT and HARD_TIMEOUT limit is 1ms each, and performance is evaluated with varying node density of the SUMO mobility pattern.

As shown in Figure 3.10, all vehicles (STAs) have two physical interfaces, Wi-Fi (STAs-wlan0: connectivity in green color) and 802.11p (STAs-wlan1: connectivity in blue color) through which it can connect to the multi-homed corresponding node (CN) or server. First, we present the results of a simple TCP connection in Wi-Fi only for the V2I scenario under SDN.

Single-path TCP performance over Wi-Fi in SDN: In Figure 3.15 and Figure 3.16, we see the RTT graph and packet loss graph for Simple TCP over Wi-Fi respectively. The average RTT with fewer vehicles (4 only) remains under approximately 110ms in general except during the handover and after every HARD_TIMEOUT value when the RTT value gets between 125 and 140ms. However, as the number of nodes increases and more nodes request rules and do the handover, the sudden rise in RTT values can be seen and reaches up to approximately

600ms when there are 20 vehicles. We can see from Figure 3.16 that the percentage of packet loss is increasing as the number of nodes is increasing. This is a noticeable effect in the case of 15 and 20 vehicles. Since there are more handovers in these two scenarios, the RTT increases, and the average packet loss goes high, which is 28% and 38%, respectively.

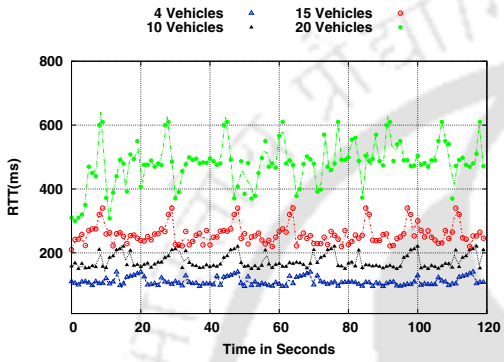


Figure 3.15: RTT for TCP over Wi-Fi with IPerf

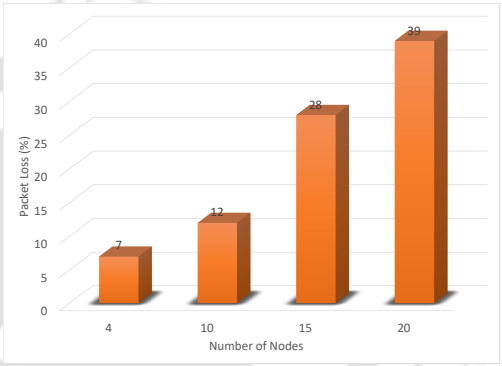


Figure 3.16: Packet Loss for TCP over Wi-Fi with IPerf

Figure 3.17 and Figure 3.18 shows the throughput performance of SimpleHTTP and Iperf server for Simple TCP over Wi-Fi. The performance is similar, and hence we choose to do further experiments with the Iperf server only. In both graphs, we see an average throughput decreases as the number of nodes increases. The average throughputs are approximately 10, 7, 4, and 1.5 Mbps for 4, 10, 15, and 20 vehicles, respectively. In the graph, we can see that there are places where throughput reaches 0 Mbps; this is because of packet loss and high RTT during the handover and rule installation.

MPTCP performance over Wi-Fi and DSRC in SDN: In this setup, vehicles are MPTCP capable, and their interfaces STAs-wlan0 and STAs-wlan1 are connected to Wi-Fi via APs and 802.11p via RSUs, respectively. Figure 3.19 and Figure 3.20 shows the RTT value for MPTCP over Wi-Fi and 802.11p respectively. The trend for the RTT graph in Wi-Fi for MPTCP is similar to the RTT graph of

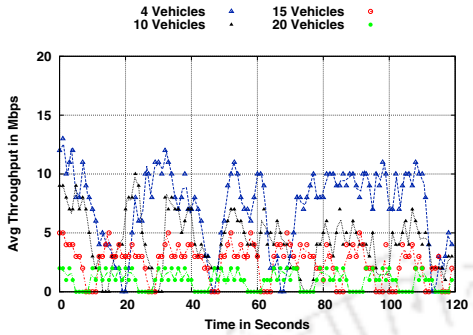


Figure 3.17: Throughput for TCP over Wi-Fi with IPerf

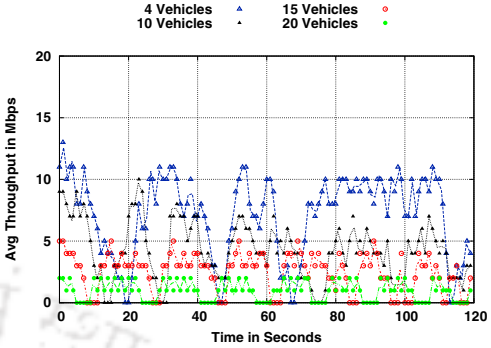


Figure 3.18: Throughput for TCP over Wi-Fi with SimpleHTTP

single-path TCP. However, the RTT graph for 802.11p is stable for 4, 10, and 15 nodes, and average RTT values are also lower than Wi-Fi. In the case of 20 nodes, we can see from the graph that RTT in 802.11p also increases and reaches an average value of 510 ms. The stability in less density is mainly due to its special mode of association and better coverage. The peaks in the graph represent time variations in flow setup from STAs to CN during re-associations. We found almost similar trends in packet loss for MPTCP over Wi-Fi. Figure 3.21 shows packet loss for MPTCP over Wi-Fi and 802.11p on Iperf server. The loss of packets on the 802.11p interface is comparatively lower than that of Wi-Fi.

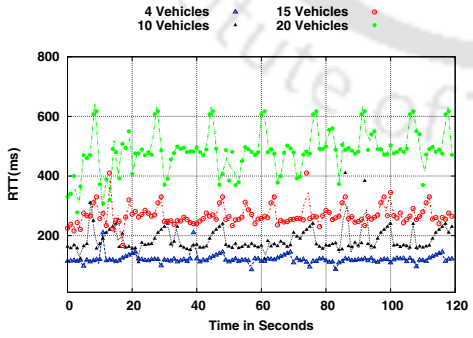


Figure 3.19: RTT Graph for MPTCP over Wi-Fi with Iperf

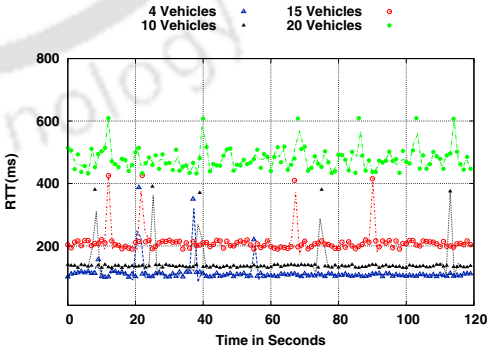


Figure 3.20: RTT Graph for MPTCP over 802.11p with Iperf

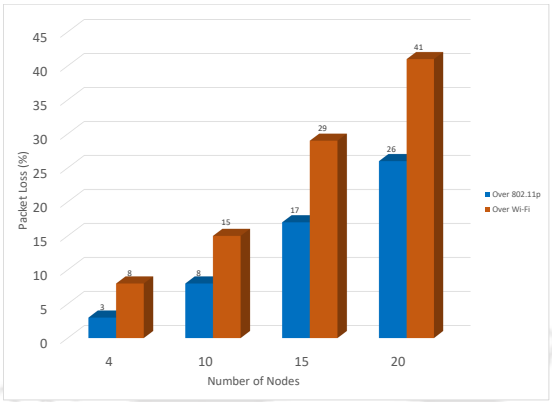


Figure 3.21: Packet Loss for MPTCP over Wi-Fi and 802.11p with IPerf

The average throughput graph of MPTCP for 10 vehicles and 15 vehicles communication are shown in Figure 3.22, and Figure 3.23, respectively. These figures consist of independent and combined throughput of both the paths with MPTCP enabled on vehicles. These two graphs give the trend of MPTCP performance in SDN-controlled V2I connectivity. We can see in Figure 3.22 of 10 vehicles, MPTCP gives a better performance than simple TCP with an average throughput of approx 10 Mbps. However, with a small increase in the number of vehicles (Figure 3.22), the average throughput is similar to simple TCP performance. In our experiment, we also observe that in MPTCP, most of the time (except few places due to handover at the same time), whenever the throughput of one path starts degrading, the other path throughput starts increasing. Therefore, MPTCP in small cells under SDN can be beneficial over simple TCP for vehicular mobility of varying density only if SDN has a proper flow setup, association, scheduling, and congestion control mechanisms. The flow setup is one of the major concerns and must be addressed to enhance the performance of simple TCP and MPTCP for V2I connectivity in small cells.

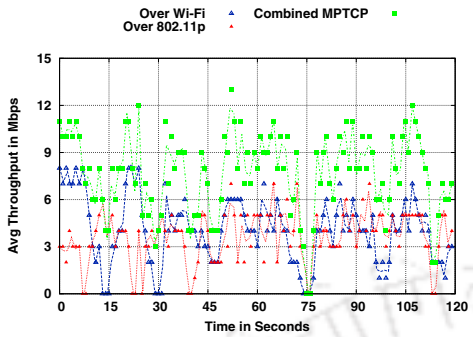


Figure 3.22: Avg Throughput for MPTCP over Wi-Fi and 802.11p with Iperf with 10 Nodes

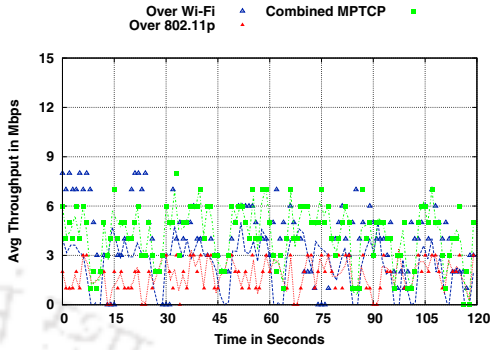


Figure 3.23: Avg Throughput for MPTCP over Wi-Fi and 802.11p with Iperf with 15 Nodes

Discussion

The role of the SDN controller in our work is to install rules reactively, which is an on-demand approach. When requests are generated from vehicles and corresponding matches not present in the data plane, the controller resolves the rules (flows) for destination and installs it on the open flow devices. However, this approach has serious implications for both the TCP and MPTCP performance in mobility conditions. Our experiment demonstrated that even MPTCP is not that beneficial under SDN as it can be in a traditional network. We tested with reduced flow lifetime entries set by the SDN controller; however, it does not help much, and with varying density, it becomes more problematic (high RTT and packet loss). This study is a preliminary analysis of the use of SDN with MPTCP for V2I communication. The SDN solution for reactive rule installation that we implemented has its consequences: Frequent deletion of flow entries causes multiple requests to the controller for the flow entries. When multiple vehicles are present, it creates a large overhead to the controller. After every HARD_TIMEOUT, a new request (packet_in) for flow entries reaches the controller, and the controller becomes busy installing flows(by packet_out) for multiple vehicles to corresponding nodes communication.

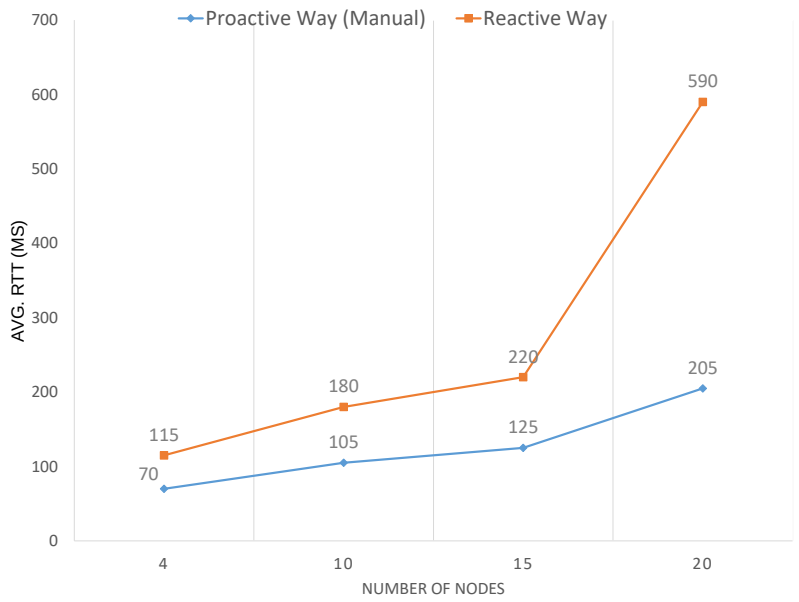


Figure 3.24: Avg RTT for MPTCP over Wi-Fi with Proactive Rule Installation (Manual)

We need a mechanism implemented at different planes of the SDN, which makes it possible to define the rules for "V2I under SDN" efficiently and proactively to improve TCP and MPTCP performances. The proactive way of installing the flows under the SDN framework in exiting mobility scenarios can be beneficial. We dumped all the flows and analyzed connectivity and flow requests generated by the vehicles in the data plane to demonstrate this. After our analysis, we manually installed the rules in the data plane for all requests made corresponding to the mobility scenario of SUMO. We plot the graph of RTT for MPTCP over WiFi, which is shown in Figure 3.24 and we can see that results are outstanding. However, such an approach of manually installing rules (flows) in SDN is not a practical approach for vehicular mobility. We need to have some mechanism deployed at

the SDN planes that can predict the next point of association of vehicles and trigger the SDN controller to install rules on the target path (in the data plane) in advance. However, it requires learning user behavior, application, mobility, etc., to take proactive actions. In the next section of the chapter, we propose one such solution.

3.4 Proposed Mechanism

In this section, we propose a mechanism to address the QoS issues due to flow setup (rule installation) in SDVN, which is inspired from [190]. Since a vehicle's residence time in small cells is very short, we need to have a rule installed by the time it completes the association with the target cell. The penalty for flow miss is very high and can severely affect the QoS for V2I connectivity and overall network performance. To address this issue, we propose some features in the application and data planes of the SDVN shown in Figure 3.25.

Application Plane: In the application plane, we propose to use Google Map API as a service. As overwhelming research is happening in the field of self-driving vehicles, eventually, every vehicle uses Google maps to reach its destination.

Data plane: In the data plane, we propose an edge node that maintains information about small cells locations, coverage details, and vehicles path to the destination. It uses the current position information of the vehicle to predict the subsequent association. Several such edge nodes can be deployed in the data plane based on road traffic analysis.

3.4.1 Flow setup in proposed approach

The detail of proposed rule installation for V2I connectivity under SDVN is given as follows and expressed in Algorithm 3.1.

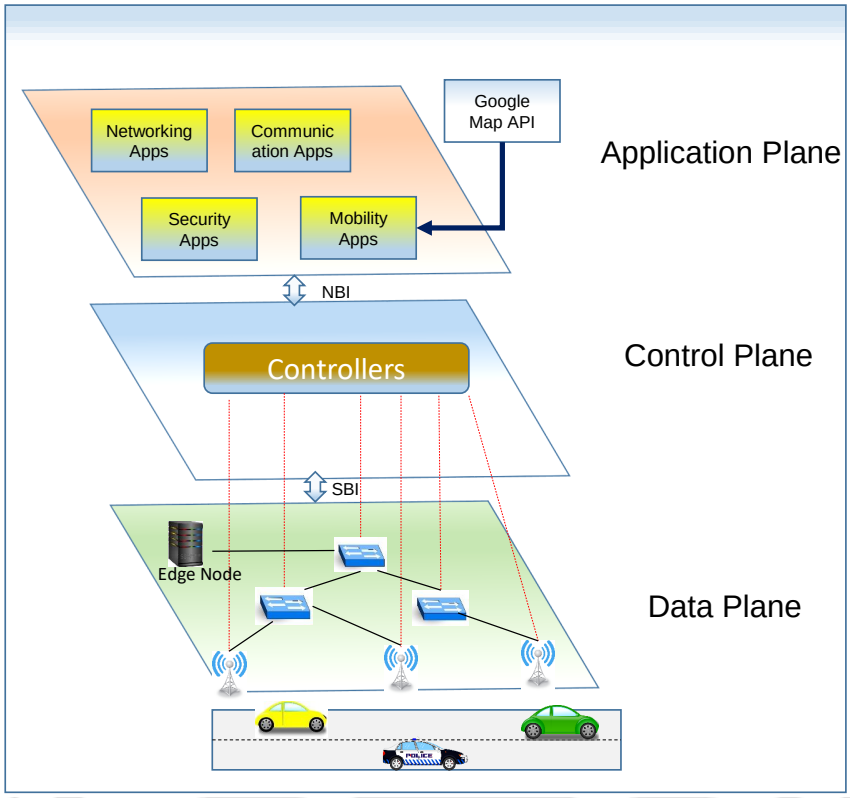


Figure 3.25: Proposed Edge-Based Mechanism for SDVN

Step 1. At the start of the journey, a vehicle, after association with a small cell, sends a packet to the controller containing the current location and destination location.

Step 2. This packet is then used by the controller to fetch map details from google API, and then brought details are sent to the edge node in the data plane. This initial packet is a special packet sent to use the northbound API of the SDN.

Step 3. After getting the initial packet, the controller also set up flow entries for that vehicle to the edge node in the data plane directly. This flow can be used to send GPS data regularly from the vehicle to the edge node.

Step 4. The edge node has coverage range information of deployed small cells, path information that the vehicle may follow, content to be fetched, and the

vehicle's current location. The edge node uses this information to trigger proactive flow installation to the target small cell just before it initiates the handover.

Step 5. As the vehicle is about to get out of the coverage range of an associated cell, the edge node proactively initiates new flows creation. These flows are cached (not in the flow table, a separate cache) in the target small cell to which the vehicle gets connected after the handover. Also, the flow for the vehicle to edge node communication is cached to the target small cell.

Step 6. The proactive flows which are cached in the target small cell have high timeout values. For a new request from the vehicle, if table_miss event happens, it checks its cache entries for matching rules instead of sending a request to the controller.

Step 7. If flow matches in the cache, that flow is updated in the flow table and gets deleted from the cache. If no match in the cache is found, then only OFA sends the request to the controller, and the controller accordingly installs flows in the respective cell using the on-demand approach.

Step 8. The flows present in cache also gets deleted after a TIMEOUT value (TIMEOUT >> max(IDLE_TIMEOUT,HARD_TIMEOUT)).

Step 9. After the handover, the vehicle's earlier flow entries present in the flow table of the previously associated cell gets deleted, and new entries are taken from its cache.

This proposed approach can help to reduce RTT, as packets are not sent to the controller for creating flows for those new requests. Our proposed method can reduce the load on the controller and also help to minimize congestion on the common physical control channel through which all the small cells and switches communicate. Since new requests are going to have matching flows, packet loss can also be minimized. Also, connectivity remains persistent that increases the average throughput. The proposed approach can help enhance overall QoS by increasing

throughput, minimizing packet loss, and reducing RTT. Using MPTCP in such an SDN setup can be very beneficial for persistent and seamless V2I connectivity.

Algorithm 3.1: Proposed Mechanism

Require: Application Plane (AP has Google_API); Edge Node (Ei) at Data Plane (DP)

Ensure: Enhance overall QoS

```
for each vehicle Vi do
    if Vi is associated with Small Cell (SCi) then
        Packet_Sent (Current location, destination location) {Vi to CP}
        Request_Map_Details from Google API {CP to AP}
        Forward_to_Edge node {CP to DP (Ei)}
        Setup_flow_entries for V_i {CP to DP (Ei)}
        Send_GPS_Data {Vi to DP (Ei)}
    end if
    if Vi is at the edge of (SCi) then
        Create(New_Flow) {Ei initiates Proactively}
        Cache(New_Flow) In Separate cache at Target SCi+1
        Cache(Vehicle_to_Ei_Flow at SCi+1)
    end if
    if Table_Miss==True then
        Check_Cache
        if Flow_Match==True then
            Update_Flow_Table
        else
            Request_Flow_Installation {DP to CP}
        end if
        Delete_Flows at Cache After Timeout
    end if
    if Handover_to_SCi+1==True then
        Delete_Flow_Entries at SCi
        Lookup_Cache at SCi+1
    end if
end for
```

3.5 Summary

This chapter contributed towards V2I connectivity in small cells and selected the multipath approach under emerging SDN architecture. The chapter discussed the problem associated with the state-of-the-art solutions and motivation for selecting MPTCP and SDN in small cell deployment. The performance evaluation of the proposed MPTCP approach is done in small cells (using Wi-Fi and its extension (similar) 802.11p technology) and SDN architecture setup with vehicular mobility scenario generated from SUMO. Measurements performed on emulated platform Mininet-WiFi with a framework implemented very close to a realistic scenario. The performance was measured in terms of packet loss, RTT, and throughput in single-path TCP and MPTCP. It is observed that when using MPTCP across paths of similar characteristics (almost symmetric path), throughput in high density is at least as good as simple TCP. The key observation was that MPTCP is helping resilience to failures very well. Since Wi-Fi has small coverage and due to the frequent handover of vehicles, the Wi-Fi interface goes down frequently, that time MPTCP enabling another interface of 802.11p tries to provide persistent connectivity. Wi-Fi complements the 802.11p for better bandwidth support whenever the vehicle's Wi-Fi interface has a good signal level. For TCP connections to various V2I based services, MPTCP is a feasible approach and could provide additional bandwidth support. The performance degradation was observed due to flow setup in SDN and handover delay in W-Fi. The overall performance can be improved with better flow management policies at SDN and fast handover mechanisms in Wi-Fi. To this end, we have also proposed a mechanism to install the required rules efficiently and proactively. This chapter opens a door as a new research area for V2I connectivity in small cells. The MPTCP and SDN amalgamation in such a setting needs to be explored widely. The next chapter of the thesis contributes towards a location privacy issue in vehicular networks. This is found to be another

biggest obstacle in the broader adoption of vehicular networks.

Chapter 4

Towards Location Privacy

A Masqueraded Probabilistic Flooding Approach

4.1 Introduction

The previous chapter contributed towards V2I communication in small cells under SDN architecture. The V2V communication of vehicular networks is also challenging, and the open nature of communication makes it vulnerable to active and passive attacks. The V2V wireless communication poses location privacy risks because it can be exploited to collect the vehicle's trajectories. In this chapter, we contribute towards the privacy issue of V2V communication in vehicular networks. In recent years, there has been considerable research on location privacy issues in a vehicular network. Special attention is given to it because privacy is the primary concern for the real-world deployment of vehicular networks. Vehicles broadcast beacon messages periodically that contain their status information [197]. The safety messages disseminated in a vehicular network are of two types: Event-driven and Periodic messages [198]. Basic Safety Messages (BSMs: SAE J2945.1-2.2) and Cooperative Awareness Messages (CAMs: ETSI 302637-20-v1.3.0) are the two popular periodic messages defined in the Wireless Access in Vehicular Environment

(WAVE) and Cooperative-ITS (C-ITS) protocol stacks standards of the USA and Europe, respectively [36]. These standards mandate the periodic broadcasting (1 Hz-10 Hz) of BSM and CAM in an unencrypted form [37] that includes vehicle's identification information (temporary ID), speed, current location, direction, speed, acceleration, etc. The BSM and CAM contain valuable data that other vehicles utilize to take appropriate decisions to prevent any undesired situations from arising. Since these messages are transmitted over a wireless medium, an adversary can passively eavesdrop on all such broadcasted messages within its area of interest. If these broadcast messages are massively captured and analyzed, the location privacy of a vehicle can be compromised [38]. Therefore preserving location privacy in a vehicular network is very important.

Privacy issue in a vehicular network has been reported in various studies [11, 199–201], and over the last decade, many privacy-preserving schemes have been proposed. In a vehicular network, authenticity and integrity are the essential requirements for security [202]. In addition to these, anonymity is another requirement to protect privacy. The existing system ensures that all received safety messages are authenticated, unmodified, and do not contain the real identity of the sender. Various anonymous authentication schemes have been proposed to meet the requirements mentioned above, which are divided mainly into three broad categories [11,203] group signatures based schemes [204–206], PKI-based pseudonym authentication schemes [207, 208], and hybrid schemes [203, 209].

Group signatures have huge communication overhead and are not scalable [11]. They require the formation of groups; ideally, each vehicle should be in the same cryptographic group, but this is not feasible in a highly dynamic topology. It also introduces high cryptographic processing overhead, which may not be suitable for critical safety-related applications [205, 210]. The hybrid approach inherits the high communication and computation overhead problem in the verification

of signatures from the group signature-based approach [211]. Although various diversities exist for security and privacy schemes in a vehicular network, there is a consensus from both academia and industry to adopt a public key infrastructure (PKI) based system to implement pseudonymous authentication scheme [37]. The PKI-based pseudonym authentication schemes facilitate message authentication, integrity and non-repudiation but often don't provide significant protection against tracing. Despite multiple mechanisms to change pseudonyms on the fly, the state of the art mechanisms either provide limited prevention of traceability [212], rely on long silence periods [213], or rely on certain traffic configurations for changing pseudonyms [214], which might not be very frequent and limiting privacy protection.

4.1.1 Motivation

The work towards location privacy in this chapter is motivated by the following observations.

So far, no standard privacy-preserving mechanism approach has been specified by any standard developing organizations (SDOs) such as IEEE and ETSI. They specified to use PKI-based pseudonym authentication but do not suggest adopting any specific pseudonym change strategy to deal with location tracking. Therefore from a standard point of view, it remains an open research problem to be addressed. A good amount of works [103,104,215,216] have been published in the last few years, which shows that this research topic is still attractive and cutting-edge.

The main motivation for the proposed scheme stems from a key limitation of pseudonym changing strategies, i.e., even if a sender changes its pseudonym frequently in broadcast messages still if an adversary gets sufficiently high fidelity of Spatio-temporal vehicle data, the adversary can construct the road map with vehicle locations and velocities, in turn computing their paths. Therefore what is required is un-linking the relation between vehicles and messages in the eyes of an

eavesdropper. The only way around it is that vehicles transmit fake information, but as established earlier, this is a dangerous proposal for a vehicular network, and further fake data come with other issues. Hence, as we don't require the knowledge of the sender, a node can send some other node's beacon masqueraded as its own. Given the mode of communication in a vehicular network is flooding, we get the name masqueraded probabilistic flooding for source-location privacy (MPFSLP). The proposed scheme is viable as nodes in the network don't require knowledge of the source of the message, as stated earlier.

This chapter proposes a new mechanism, MPFSLP, which ensures source location privacy without compromising with other security requirements. We apply our proposed mechanism to existing pseudonym change schemes to further limit the adversary's tracking ability. We also introduce the concept of casual dependency and proof-of-claim mechanisms that ensures non-repudiation in our scheme. We evaluated our scheme over the Privacy Extension for Veins VANET (PREXT) [217] simulator, a framework that allows comparison of pseudonym changing schemes.

The rest of the chapter is organized as follows. The background detail and a brief survey of related work are discussed in Section 4.2. Section 4.3 defines the problem. The proposed mechanism is discussed in Section 4.4. The evaluation of the proposed mechanism and obtained results are discussed in Section 4.5. Section 4.6 and conduct security analysis. Finally, the chapter is concluded in Section 4.7.

4.2 Background and Related Work

This section of the chapter provides details of the standard PKI-based pseudonymous authentication system in a simplified way. This section also discusses privacy-preserving mechanisms that have been proposed to decide when to change a pseudonym in the related work.

4.2.1 PKI-based Pseudonym Authentication System

Figure 4.1 depicts the working principle of the system, which is the basis for privacy protection through authenticated pseudonyms in PKI-based vehicular networks. The pseudonym life cycle of this system is shown in Figure 4.2. We describe these steps in the following subsections [11, 202, 218].

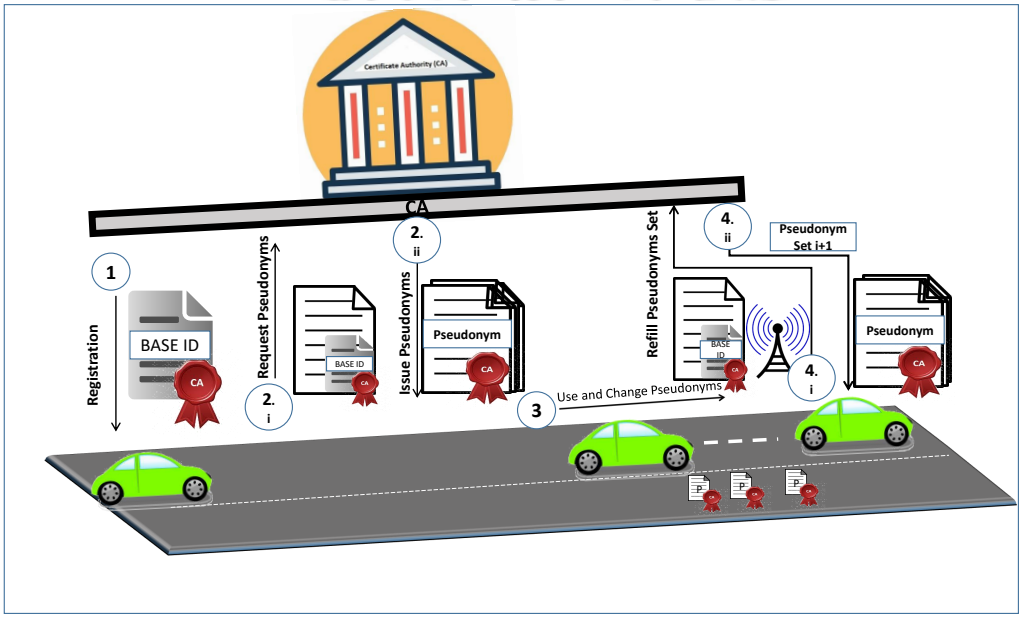


Figure 4.1: A simplified view of PKI defined by IEEE and ETSI

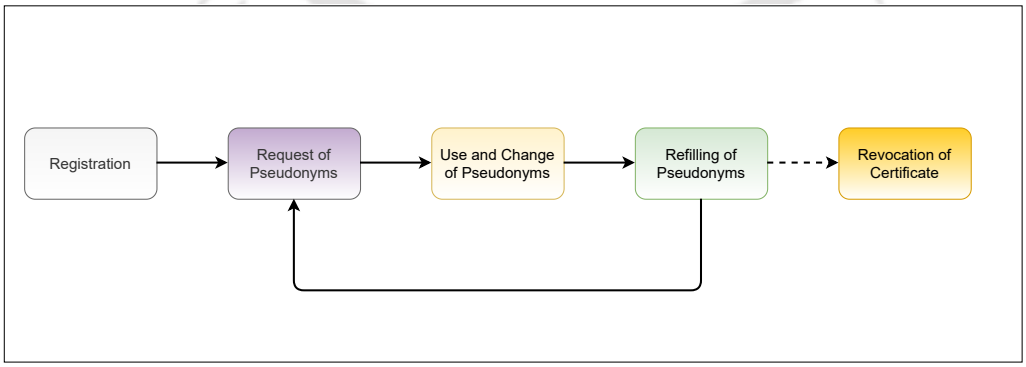


Figure 4.2: Pseudonym Life Cycle

Registration

Each vehicle has to register itself with Enrollment CA (ECA) to become part of the deployed vehicular network. The registration process takes place before the vehicle starts operation. This process initiates bootstrapping of the vehicle at the OEM. Vehicle establishes an out-of-band communication channel to the Device Configuration Manager (DCM) in a secure manner during manufacture. The DCM acts as an interface between the vehicle and the ECA and ensures that only authorized vehicles can submit a registration request. The registration certificate serves as an entry ticket for the vehicle to request pseudonym certificates. These registration certificates can also be blacklisted to prevent the vehicle from requesting pseudonym certificates to Registration Authority (RA).

Request of Pseudonyms

After successful registration, each vehicle is equipped with a base identifier and a key pair (public and private), using which it generates a request for a set of pseudonyms to RA. If the base identity is valid (long-term certificate not in the revoked list) and information present in the request for the pseudonym is correct, the RA forwards the pseudonym request to PCA. The PCA collects the information for certificates, signs, and encrypts, and gives it to the requesting vehicle through RA. A pseudonym is a public key (short-term identifier) that is certified by the PCA. It does not consist of any information about the real identifier of the vehicle. The PCA can see pseudonym certificates; however, it does not know which vehicle is requesting them. The mapping from a short-term identifier to a real identifier is resolved with the help of LAs and other CAs in case of misbehavior.

Use of Pseudonym

At this stage, all registered vehicles are equipped with a base identifier and set of signed pseudonyms. These identities ensure authenticity and anonymity at the same time. Figure 4.3 illustrates the use of pseudonyms in the vehicular plane [218].

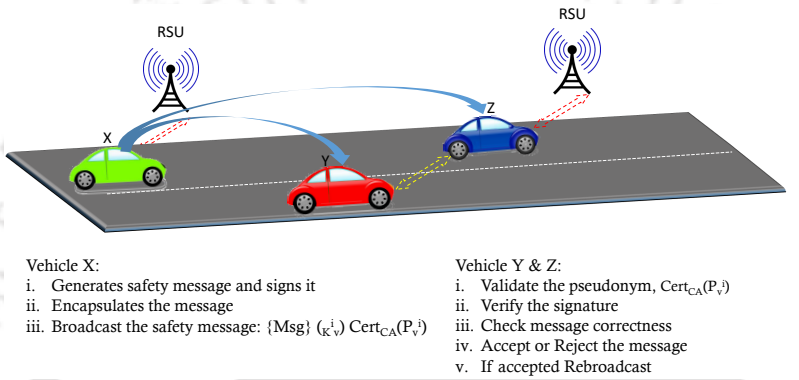


Figure 4.3: Use of Pseudonym for Security and Privacy

Each vehicle selects an unused pseudonym from its pseudonyms pool and uses it as its visible address. Each pseudonym (P_V^i) from the pseudonym pool are certified by PCA using its own digital signature: $Cert_{CA}(P_V^i)$. Before broadcasting a message (geo and time-stamped), the vehicle X digitally signs it using its private key K_R^V ($Msg_{K_R^V}$) corresponding to the pseudonym P_V^i. To facilitate verification at the receiver end, the $Cert_{CA}(P_V^i)$ is attached with the signed message $Msg_{K_R^V}$. Receiving vehicles Y and Z first check pseudonym P_V^i validity by checking the signature in $Cert_{CA}(P_V^i)$ using the public key of the CA. They also verify other necessary fields of $Cert_{CA}(P_V^i)$ for its validity. Then, Y and Z check the signature of the received message $Msg_{K_R^V}$ for its correctness. Therefore vehicles Y and Z consider received messages only if they are signed with under a valid pseudonym. These steps ensure the authenticity and integrity of the received message.

Change of Pseudonym

Vehicles use each pseudonym for a short period and change it from one to another (not previously used). Since the messages are anonymized with the short-term certificates, it does not reveal the real identity of the sender vehicle X. Safety messages with different pseudonyms help to achieve unlinkability. However, it is unclear (no standard approach) how pseudonym pools can be organized, how effectively the pseudonym should be used for transmission, and how pseudonym changes should be made to preserve privacy in a vehicular network. Towards this end, various proposals for change of pseudonym exist in the literature that we discuss in the next section.

Note: It is also recommended that the change of pseudonym should be accompanied by a change of all other identifiers used in communication such as MAC and the IP addresses [219].

Pseudonym Refilling

Each pseudonym has its lifetime; therefore, any vehicle, before consuming all its pseudonyms from the received set i requests a new set $i + 1$ (set of signed pseudonyms) from the PCA via RA using its base identifier. This process of generating the request for a new set of pseudonyms and obtaining it from PCA is referred to as pseudonym refilling. All information exchanged between the vehicle and the PCA during the refilling process is encrypted.

Revocation of Certificate

The revocation of the certificate given to any vehicle may take place in the following given cases: *i.* OBU of the vehicle has been compromised. *ii.* The vehicle is sold or broken. *iii.* When a vehicle misbehaves and its trust score is below a defined threshold. If the MA determines that any of that situation has occurred,

then revocation and blacklisting processes are carried out. In this process, the invalidation of a given enrollment certificate is done. The MA takes the help of LA and provides sufficient information to RA for determining which enrollment certificate to be invalidated and instructs the RA to blacklist that certificate. Once a vehicle is blacklisted, it no longer gets service from the RA. This prevents the vehicle from requesting or refilling pseudonyms. As a result, the blacklisted vehicle is not able to communicate with the PKI system. Other participants in the network get the information about this revocation through Certificate Revocation List (CRL) distribution that contains the list of revoked certificates [220].

4.2.2 Related Work

Multiple privacy-preserving methods have been proposed which decide when to change a pseudonym. We implement our scheme over seven existing state-of-the-art schemes, which we briefly elucidate as follows:

1. Periodical Pseudonym Change (PeriodicalPC): Initially, there was a Periodical Pseudonym Change (PeriodicalPC) scheme in which each pseudonym can be used for a specified period. In PeriodicalPC, a vehicle performs pseudonym changes operation either at a fixed or random interval. A fixed period may increase the number of simultaneous pseudonym changes among nearby vehicles. Nonetheless, an adversary could easily anticipate when pseudonyms would be changed by correlating old and new pseudonyms messages. A random change period can address this prediction issue; however, it may reduce the number of simultaneous pseudonym changes [221].

2. Random Silent Period (RSP): In [222], the authors proposed a silent period-based mechanism to enhance wireless location privacy and considered as a better solution than the PeriodicalPC. The authors in [223] extended this work

and adopted a random silent period to provide location privacy for VANET. After a specified pseudonym time, the RSP requires a vehicle to change its pseudonym and to remain silent for a time chosen from a uniform distribution within a predetermined range (e.g., from 5 to 15 s).

3. Coordinated Silent Period (CSP): The CSP scheme proposed in [224] coordinates all vehicles to remain silent and change pseudonyms synchronously in the network. CSP has been regarded as a theoretical technique since the global silence coordination among vehicles is very difficult and challenging to maintain. Also, more investigation is required to study the possible implications or attacks. For example, packet delivery and handling safety-critical situations during the scheduled silence may make CSP implementation quite challenging in real-world scenarios. Nevertheless, CSP enhances privacy as it maximizes the size of anonymity set at each pseudonym change.

4. SLOW: In [225], the authors proposed a SLOW scheme, which does not require any explicit synchronization among vehicles for pseudonym change. In SLOW, vehicles continuously check their current velocity and enter into the silent period if their velocity falls below a given threshold (say 40 Kmph) and change their pseudonym for each such silent period. For example, suppose vehicles stop at a traffic light intersection or move slowly in a traffic jam. In that case, they may enter into the silent period by refraining from beacon broadcasts and change their pseudonyms almost at the same time and location, i.e., at the same instant.

5. Cooperative Pseudonym Change (CPN): The CPN scheme proposed in [212] is based on the number of neighbors of a vehicle. In CPN, each vehicle monitors its neighbors within a radius R of itself and waits until the number of vehicles reaches a threshold K. When this threshold is exceeded, the vehicle sets an

internal flag $readyFlag$. Within the beacon, the vehicle broadcasts $readyFlag$ and changes the pseudonym with the next beacon. If a vehicle receives a beacon that is set to $readyFlag$ or if its internal flag is already set, it changes its pseudonym instantly.

6. Context-Aware Privacy Scheme (CAPS): The basic concept of CAPS [226] is that a vehicle decides the appropriate context to change its pseudonym. To do so, each vehicle employs an internal vehicle tracker to track the neighboring vehicles' state and enters into a silent period when one or more neighbors are silent. The vehicle resumes its communication with a new pseudonym when there is a chance to mix its actual state with a silent neighbor state. The CAPS approach increases the robustness of pseudonym changes against tracking and avoids wasting pseudonyms in easily traceable conditions.

7. Mix Zones: A mix-zone is an unobservable or anonymized region [214] where an adversary cannot eavesdrop on the messages broadcast by vehicles. It is typically located at road intersections to make the movement of the vehicle difficult to predict. When vehicles change their pseudonyms within a defined mix zone, the adversary would not be able to correlate the leaving vehicles with those entering the zone earlier due to hidden messages and unpredictable vehicle movement. In a mix zone, message hiding is implemented by freezing all communication, i.e., enter into silent mode or by encrypting messages using a shared symmetric key obtained from an RSU.

4.3 Problem Definition

This section of the chapter briefly elucidates a general system model, communication model and then presents the privacy issues that arise due to the presence of adversaries.

4.3.1 System Model

Vehicles that are part of the network have all connected vehicle components and features discussed in Section 2.1.1. The OBUs run the corresponding region's protocol stack. In this chapter, we consider WAVE protocol stacks of the USA. It facilitates V2V and V2I communication over DSRC. The OBU is also a tamper-proof device. In the infrastructure plane, we consider the RSUs to be the key infrastructure alongside the roads using DSRC and act as gateways between the vehicular and services plane. The services plane consists of entities that manage the traffic and also offer external services. Major entities are car manufacturers, certificate authorities of PKI, and service providers. The PKI-based pseudonym authentication system discussed in the previous section has been used to provide security and privacy services to the network. The CAs of PKI take care of pseudonym life cycle, i.e., registration, issuing certificates, key pairs, pseudonym sets, refilling pseudonyms, credential management (reputation and trust), and misbehavior detection revocation of certificates, etc. Both manufacturers and the legal authority are connected with the CA to help each other whenever the need arises.

4.3.2 Communication Model

Although there exist other types of communication patterns (V2X) in a vehicular network, such as those related to access different kinds of services such as infotainment, location, payment, etc., however, V2V communication is the most challenging and significant from security as well as privacy point of view. Thus, we focus on V2V communication, which has been found vulnerable to location tracking attacks. We consider BSMs, periodic beacons (1 Hz-10 Hz) that are broadcasted over safety channels of DSRC by vehicles and contain temporary ID, timestamp, cryptographic materials, and motion vector details as speed, location, acceleration, direction, etc.

4.3.3 Adversary Model

The adversary model that we consider in this chapter is of type external and performs a passive attack and can monitor the entire network. The adversary has the tracking capabilities to eavesdrop on all messages exchanged in the network by deploying low-cost receivers. Our main aim is to protect the location privacy against the adversary. We consider the state-of-the-art adversary model supported by the PREXT simulator [217]. The details of the model are as follows:

- ***Coverage:*** The simulator supports both local and global adversaries. We consider a global adversary that can cover the entire simulation region, which is realized by deploying wireless receivers alongside the road in listening mode (passive mode).

- ***Components:*** The adversary model has two components eavesdropper and vehicle tracker. The functionality of the eavesdropper is to listen to the wireless medium for beacons and send them to the vehicle tracker. The vehicle tracker is a central entity that collects beacons from deployed eavesdroppers, removes duplicates, and exports the collected information. On the collected information from beacons, the vehicle tracker runs the tracking algorithm to trace the vehicle location by reconstruction.

- ***Tracking Algorithm:*** The vehicle tracker employs a tracking algorithm, which consists of four iterative phases [227]: 1. State estimation (uses Kalman filter to obtain an actual state for vehicles from inaccurate measurements obtained from beacons and estimated states derived from a predefined kinematic model). 2. Gating (to prevent unnecessary computations for unlikely associations). 3. Data association (uses nearest-neighbor probabilistic data association (NNPDA) to associate each beacon to its originating vehicle with the help of assignment probability matrix calculation). 4. Track

maintenance (to the track initiation, its confirmation, and deletion).

We assume that participating vehicles and RSUs are honest (i.e., trusted entities). We consider external adversaries having wireless receivers to eavesdrop on V2V communication to infer user-sensitive information for harming the privacy of the user. These adversaries cover all entry and exit points to passively eavesdrop on the V2V communication of all the vehicles entering their zone. They try to link pseudonyms in that particular zone based on information derived from safety messages such as velocity, timing, and location. We consider that RSUs and VPKI are honest entities, i.e., they comply with PKI-based security protocols and policies. We also consider registered vehicles do not cooperate in any activities that can affect the security and protection of the system.

4.3.4 Attack Model

As already mentioned, BSM messages rely on a beaconing approach, which is periodically broadcasted and contains sensitive information. However, a passive adversary can easily exploit this over-the-air transmission by eavesdropping on broadcast messages and launch a pseudonym linking attack. The adversary uses spatiotemporal information in the linking attack when vehicles change their anonymous identity (pseudonym). Buttyán et al. [225] have identified two forms of pseudonyms linking attack syntactic and semantic linking, which are described as follows.

As shown in Figure 4.4, in a syntactic linking of pseudonyms, the adversary can easily link the pseudonym change (from Y1 to Y2) performed by only one vehicle (Y) among a set of vehicles (e.g., one out of three vehicles running on that zone) during Δt time. In the case of semantic linking (Figure 4.5), the adversary exploits the mobility information of beacon messages to predict the next location of vehicles via tracking methods. The information helps the adversary to link the pseudonym

(from Y1 to Y2) even if more than one vehicle (all three) performs pseudonym change during Δt time. Semantic linking is more powerful than syntactic linking.

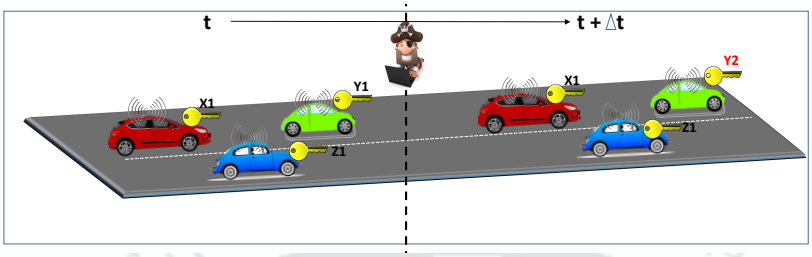


Figure 4.4: Syntactic Linking [11]

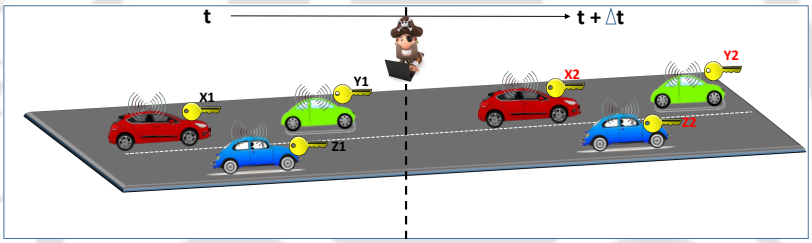


Figure 4.5: Semantic Linking [11]

4.3.5 Design Goals

Under the above system, communication model, adversary, and attack model, our design goal is to develop a solution for preserving the source-location privacy for vehicles in a vehicular network. In general, we want to accomplish the following goals:

- For all the vehicles in the network, their location information is sensitive, and their privacy must be preserved. Therefore, the proposed scheme should provide non-traceability against the attacks by the adversary mentioned in the above subsections.

- Although preserving location privacy is our primary goal, but at the same time, it should not compromise with the security requirements. Accountability has to be ensured in case of dispute and misbehavior. Therefore the proposed scheme should be fair in terms of security, trust, and privacy.

- The proposed scheme should not increase communication overhead and add high computational complexity. It can be efficiently run on the OBUs with their available computational capacity.

4.4 Proposed Mechanism

This section of the chapter describes the proposed masqueraded probabilistic flooding mechanism for source-location privacy (MPFSLP).

4.4.1 Working Principle

Since our proposed mechanism utilizes the underlying PKI-based authentication system, all vehicles must comply with its security requirements such as registration, certificate store, use of a pseudonym, signing, verification of safety messages, etc. With the example illustrated in Figure 4.6, we describe the working principle in a simplified manner as follows.

- The vehicle which generates a safety message (BSM/DENM) is considered as a source (Vehicle X in Figure 4.6).

- The source vehicle selects a pseudonym from its pool that it got after registration/re-filling and uses it as its visible address. These pseudonyms are certified by CA using the digital signature.

- The generated safety message (geo and time-stamped) is digitally signed

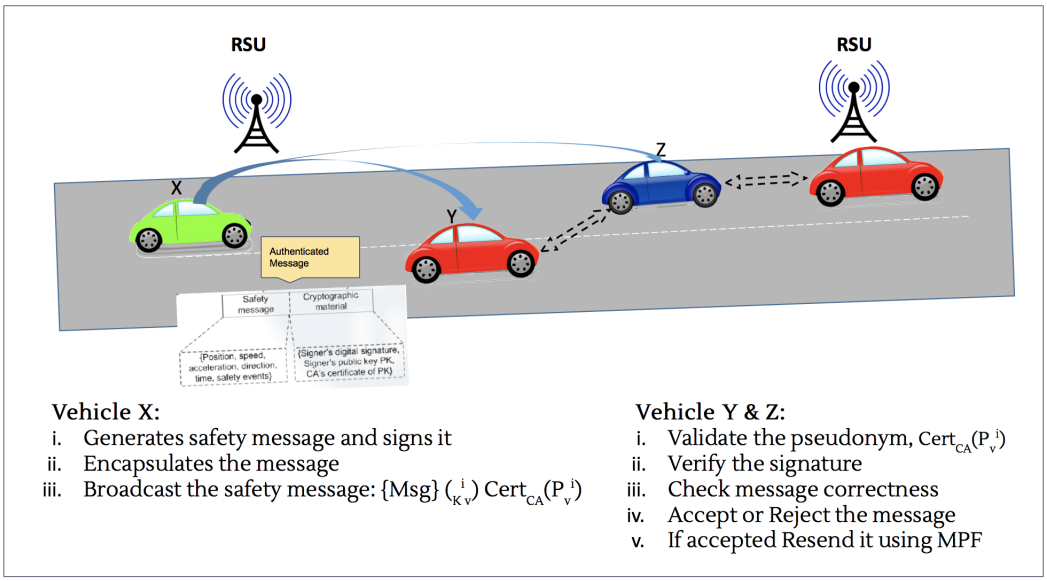


Figure 4.6: An Example of Masqueraded Probabilistic Flooding (MPF)

by the source using its private key and encapsulated with the header and cryptographic materials (such as a certificate of CA).

- After signing and encapsulation, the safety message is broadcasted over DSRC.
- The receiver(s) (Vehicle Y and Z in Figure 4.6) after receiving the message, checks the validity of the pseudonym and also verifies other necessary fields of the certificate for its validity.
- The receiver(s) also verifies the signature of the received message to ensure integrity and correctness.
- If all are valid and correct, receivers resend it using masqueraded probabilistic flooding method, which is explained below.

We swap the concept of forwarding in traditional networks sense with the idea of resending, which means that an intermediate node that forwards a packet replaces the senders' identity (IP and pseudonym) with its own identity to distort

Algorithm 4.1: Resending Routine

Require: Obtain Following from the network and pseudonym changing layers

Current node's IP : ip;

Current node's current pseudonym ps = (PrivateKey = kr, PublicKey = kv);

1: Resend($p = PACKET(m = MESSAGE(SourceIP = S\text{ip}, Location = l, Velocity = v, TTL = ttl), Pseudonym = P\text{kv}, Hash = h, Signature = s)$

2: $check = VERIFY(Message = (m|h), s, P\text{kv})$;

3: **if** (not check) or ttl == 1 **then**

$return$;

4: **end if**

5: $h' = SHA256(p)$;

6: $m' = MESSAGE(ip, l, v, ttl - 1)$;

7: $s' = SIGN(Message = (m'|h'), PrivateKey = ps.kr)$;

8: $p' = CREATEPACKET(m', ps.kv, h', s')$;

9: $BROADCAST(p')$;

10: **for** each incoming packet p **do**

11: $RESEND(p)$;

12: $STORE2DB(p)$;

13: **end for**

14: **for** every timer event **do**

15: $RemoveStalePacketfromDB()$;

16: $p = GetRandomPacketFromDB()$;

17: $RESEND(p)$;

18: **end for**

the relationship between a message and its origin, each node which is forwarding a message masquerades as the sender of a message even though it did not create the message. This weakens the link between the identity (IP, MAC address, a

pseudonym used) of a vehicle and its Spatio-temporal data (location, velocity). In our work, each node transmits packets of all other nodes from which it receives, in addition to its own packet using masqueraded probabilistic flooding. Also, the use of pseudonyms ensures that the identity of the packet sender remains concealed. Resending basically means that a node forwards a message that it received but replaces the details of the source with its own (similar to switching in link layer) (this includes a re-evaluation of any cryptographic hashes/digital signatures using the private parameters of the node forwarding the message) thus masquerading itself as the sender of the message. Apart from this, the nodes maintain a list of recent messages received, and they may probabilistically resend previous messages to further complicate the relationship between messages and the sender's identity. Therefore, the resending routine is run probabilistically over the set of recent messages received to further convolute the relation between the sender and the message. Algorithm 4.1 presents this resending routine of the proposal.

The proposed protocol with these specifications is still not sufficient as a malicious node can generate fake packets (as we have weakened the relation between sender and message). To ensure non-repudiation, we introduce a causal relation between the multiple re-sendings of the same message and proof-of-claim, which we discuss in the next subsections.

4.4.2 Casual Dependency

To ensure non-repudiation, we introduce a causal relation between the multiple re-sendings of the same message. The node which is resending a message appends the hash of the entire packet it received (including the digital signature and hash). This way, if the node retains the message it originally received and the message that it resent, it can prove that it, in fact, resent a message of another node rather than generating a message of its own. Figure 4.7 illustrates the causal dependency for

further clarity.

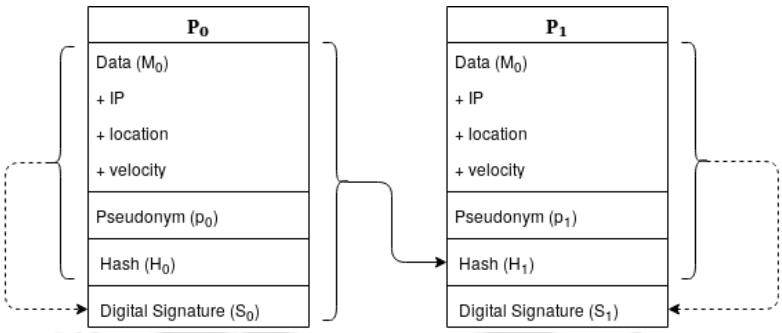


Figure 4.7: P_0 is the packet originally sent by origin, P_1 is formed when a node re-sends the packet received. The node has to recompute hash and signature as depicted in the figure. NOTE: H_0 is a dummy hash.

More formally, the process of introducing causal dependency is further described by the equations 4.1:

$$\begin{aligned} P_0 &= [M_0|p_0|H_0|S_0] \\ S_0 &= Sign_{p_0}([M_0|p_0|H_0]) \\ H_1 &= Hash(P_0) \\ P_1 &= [M_0|p_1|H_1|S_1] \\ S_1 &= Sign_{p_1}([M_0|p_1|H_1]) \end{aligned} \tag{4.1}$$

Note that both packet P_0 and P_1 contain the same message M_0.

4.4.3 Proof-of-Claim

Note that since a node does not broadcast the message it received (it only stores it for possible future verification), an eavesdropper cannot know the identity of the original sender as all the eavesdropper sees is a message broadcast-ed and signed by the node, which is resending. Only when asked to present a proof, a node shall reveal

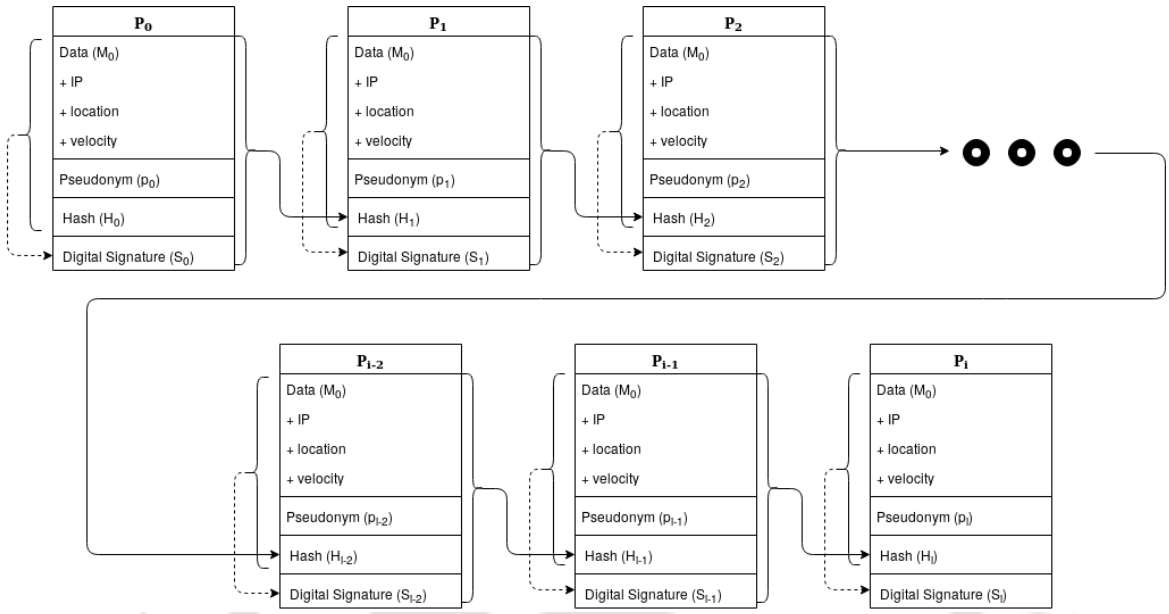


Figure 4.8: **The chain of proofs formed by from node i to the node 0 (original sender).** – Each node i proves that it received the message from node $i-1$ up till node 0 which can't use the same proof.

the identity of the node from which it received the message along with the proof-of-claim. Furthermore, when there is a chain of re-sends (a message generated from a particular source is resent successively multiple times), an intermediate node only knows about its immediate predecessor in the chain and can only prove the identity (pseudonym, IP) from whom it immediately received the message, and it has no information about the original source of the message. Therefore when it comes to determining the original sender of the message, all nodes of the chain up to the node told to prove the whereabouts/lineage of the message need to be involved. This is similar to a distributed blockchain, the difference being in a blockchain, each element of the chain refers to a previous element, and this reference is known and can be verified publicly. Whereas in our scheme, the reference is only known by the entity which resents the message (or, in other words, the entity which created the reference in the first place) and can only be proved by the same entity. Figure 4.8

illustrates the proof mechanism for further clarity.

Formally, the process of proving the identity of the original sender is described by equations 4.2. The idea is that each node proves the identity of the node from which it received the packet and this trails up to the original sender. In essence, node i in the chain proves that the message that it received is causally dependent on the message generated and signed by node $i-1$. This is because P_i contains the hash of P_{i-1} and the contents of P_{i-1} have been signed by node $i-1$. Therefore it cannot happen that packet P_i was generated before P_{i-1}. Hence the burden of proof moves to node $i-1$ from node i. This proof trickles through the chain until the turn of node 0 comes to prove the identity of the sender. Node 0, however, cannot claim that P_0 contains the hash of some other message as the hash contained in the first message is a dummy hash. Therefore all nodes in the chain except node 0 (the original sender) can prove that they are not the initiator of the message. This, coupled with the fact the contents of P_0 have been signed by node 0, proves that in fact node 0 is the initiator of the message.

$$\begin{aligned} P_{i-1} &= [M_0|p_{i-1}|H_{i-1}|S_{i-1}] \\ S_{i-1} &= Sign_{p_{i-1}}([M_0|p_{i-1}|H_{i-1}]) \\ H_i &= Hash(P_{i-1}) \\ P_i &= [M_0|p_i|H_i|S_i] \end{aligned} \tag{4.2}$$

4.5 Experimental Evaluation

This section of the chapter presents the experimental details that we performed on the PREXT simulation framework and discuss the obtained results.

(a) (b)

Figure 4.9: (a) Munich city center map (OSM). (b) Accumulative vehicle positions extracted from their unencrypted beacons with the existence of 6 circular mixzones (blue circles).

4.5.1 Simulation Setup

For simulating the traffic scenario, we employed a road map of Munich city center whose of size 2.67 km X 2.8 km, as shown in Figure 4.9. We used 250 vehicles on the selected road map. This map is used in the default simulation in PREXT using the Simulation of Urban Mobility (SUMO) framework [217]. We set the trace lifetime to 170 s for all simulations.Table 4.1 and Table 4.2 list the simulation parameter details of the experiment.

4.5.2 Results

For each of the seven schemes, we compare two values: the value of a metric obtained by implementing the scheme without MPFSLP and with MPFSLP. Figure 4.10 and Figure 4.11 compare the performance of the seven schemes with and without MPFSLP based on the metrics traceability and normalized traceability, respectively.

Module	Parameter	Values
Hardware Details	HP Inc	Intel(R) Core(TM) i7-8700 CPU @ 3.20 GHz 16 GB RAM
Operating System	Ubuntu	Version 16.04 64-bit
Simulator	PREXT	Version 1.0
Veins	Transmission power (Tx Power in mW)	20
	Bit rate (Mbps)	18
	Thermal noise (dBm)	-110
	Length of Packet Header (bit)	256
	Length of Beacon Payload (Byte)	100
	Beacon Rate (Hz)	1
	Traffic Simulator	SUMO 0.25.0
	Coupling using	TraCI
	Simulation Time (s)	1000
Adversary	Type	Passive (Evasdroping and Tracking), Global
	Range (m)	300
	Overlap (m)	30
	Tracking Interval (s)	1
Schemes		
PPC	Pseudonym Lifetime(s)	60
RSP	Pseudonym Lifetime(s), Min Silent Time(s), Max Silent Time(s)	60 3 9
SLOW	Silent Time threshold (s) Speed threshold (m/s)	5 8
CAPS	Min Pseudonym Lifetime(s), Max Pseudonym Lifetime(s), Min Silent Time(s), Max Silent Time(s), Missed Beacon Threshold, Neighborhood Threshold(m)	60 180 3 13 2 50
CPN	Radius(m) Neighbor Threshold	100 2
Mix-Zone	Interval for Advertising (s) Shape of the Zone Radius of the Zone (m) No. of Zones Zone Location	3 Circular 150 6 Figure 4.9

Table 4.1: Simulation Parameters

Comparison of Schemes

From Figure 4.10 and Figure 4.11 it can be observed that our scheme, when implemented along with an existing privacy scheme, always results in superior performance, as measured by the traceability. This shows that our scheme preserves privacy in a reliable manner.

Parameter	Definition	Default Value
MAX_TTL	The maximum time to live of a packet. It helps in reducing the redundant re-sending of old packets	4
prob_send	Probability of sending a packet	0.3

Table 4.2: Simulation Parameters for MPFSLP

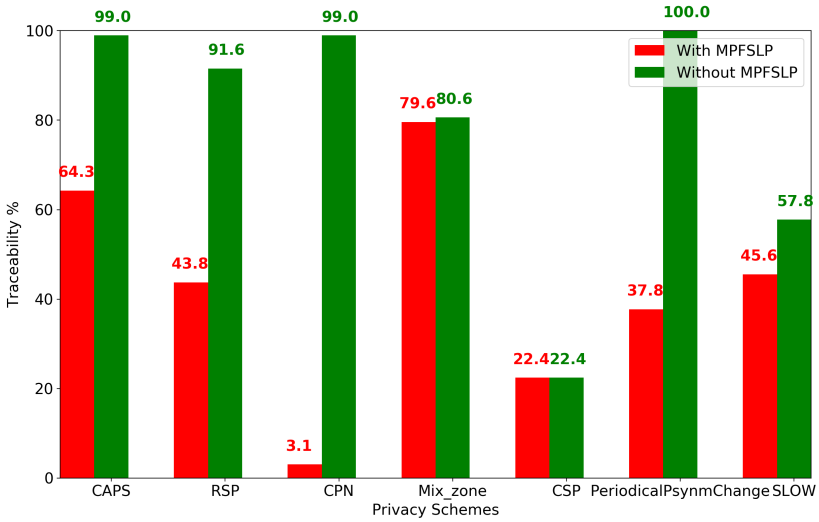


Figure 4.10: Traceability of the privacy schemes with and without using MPFSLP.

Particularly, it can be seen that the difference in the values of traceability is quite large in some cases, such as in CPN. Also, the reason for no difference in performance when MPFSLP is implemented over CSP is that in CSP, there is a coordinated silent period when no node is transmitting any data, and during this time pseudonym is changed, this means that after this silent period, each packet has a similar probability of being linked to every other pseudonym. Our approach also achieves a similar scenario but without the burden of global synchronization, which has high computation overheads.

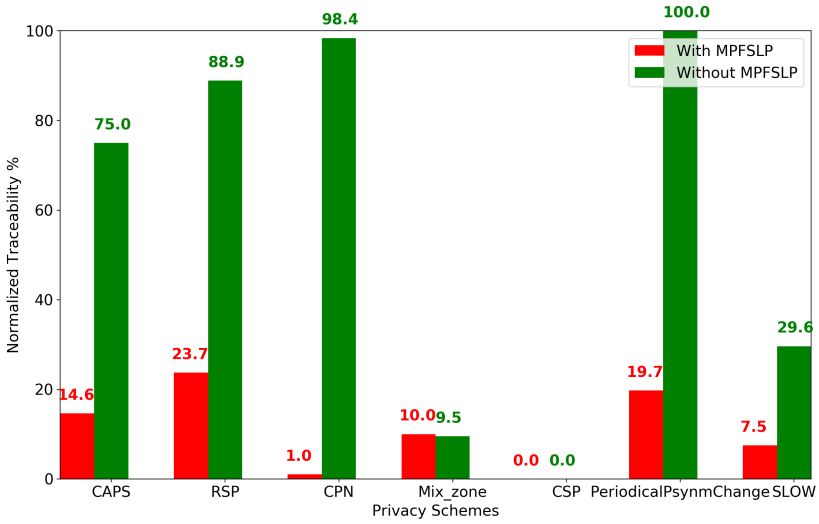


Figure 4.11: Normalized Traceability of the privacy schemes with and without using MPFSLP.

Discussion

In this section, we analyze our system for security and privacy. For a better understanding, we illustrate it in Figure 4.12. At level 0, we have vehicles running WAVE protocol stack and use the security module specified in IEEE 1609.2 standard [228].

At level 1, we use the PKI-based authentication system, which ensures security in a vehicular network. The PKI-based system protects the network from external attacks because entities that do not have valid certificates from PKI can't participate in the communication.

At level 2, we suggest using a pseudonym change strategy (any effective strategy from the literature) that effectively changes the pseudonym from the pool obtained from PKI to avoid location tracking and guarantee drivers' and occupants' privacy. The security standard suggests that pseudonyms should be frequently changed by vehicles but do not specify the context. Therefore we recommend using one such

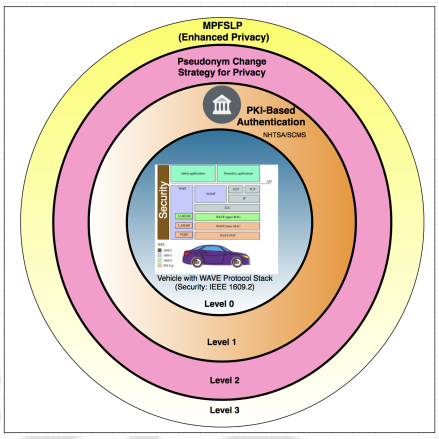


Figure 4.12: Security and Privacy after MPFSLP.

strategy for maintaining anonymity to some extent.

From all this, we learn that the best way to fool an adversary is to distort the relationship between vehicle data and the sender's identity. The best distortion is anyone can be anyone. If we allow each vehicle to send any other vehicle's beacons masqueraded as their own beacons (rather than routing beacons), an adversary can't link the identity of the sender with the velocity and location information. Thus, we add another level (level 3), where we propose our MPFSLP scheme as another shield to combat tracking and enhance privacy without compromising with the underlying security.

4.6 Security Analysis

This section of the chapter analyses the proposed scheme against different possible attacks.

4.6.1 External Attacks

Our proposed scheme is supposed to be run over a scheme that fulfills vehicular network security requirements using a PKI-based authentication system. As discussed, this system is immune to external attacks and provides a mechanism for authentication and integrity. The sign ensures that the message was sent or verified by an authenticated entity. For example, to ensure integrity, the sender must first verify the integrity of the message (as shown in Figure 4.6) it is forwarding and then re-calculate the digital signature using its private key.

4.6.2 Non-repudiation

Allowing vehicles to send other vehicle's messages affects non-repudiation. We rectify this requirement by introducing *causal dependence* between messages which are resent by vehicles. A node can falsely claim that it resents someone else's message when, in fact, it was its own message. In our scheme, to make this claim, the node would have to show the original message and show that hash H matches the hash of the original message received. This can't be forged, relying on the security of digital signatures.

4.6.3 Side Channel Attack

We note that side-channel attacks by sophisticated adversaries are possible that can use receivers to make an angle of arrival estimation etc. To mitigate these, senders can probabilistically change signal strength and transmit signals in some directions only at some periods of time if they have directional antennas.

4.6.4 Attack from the Internal Entity

Although the current system is immune to external attacks and with the internal entities of the PKI system, malicious activities by internal entities such as compromised or misbehaving vehicles are possible. One such example is a Sybil attack [35, 229] in a vehicular network. This attack takes place when a vehicle simultaneously uses pseudonyms from the pool to disturb the system. The attacker periodically broadcasts safety messages with random data and signing each of them with a different pseudonym. Such an attack may overwhelm the misbehavior detection module. Sybil attack of data replay is also possible. Someone sending data from one vehicle to another (as in our case) may be malicious and perform a data replay attack. Although such misbehavior detection is out of the scope of this work, our idea of casual dependency and proof-of-claim can be capitalized and extended to help the authority trace and catch such misbehaving entities. The chain can reveal the forwarder who replayed the data.

4.7 Summary

This chapter is the first contribution towards the location privacy issue in a vehicular network that proposed masqueraded probabilistic flooding-based approach. The proposed mechanism leverages the fact that a node only needs to know that the message is signed by an honest vehicle and is not forged; a node is not required to know the identity of a vehicle for applications like collision warnings, etc. The idea of re-sending is used, which convoluted the relation between the identity of a sender and the message. A concept of causal dependency has been introduced between the generated messages and resent messages to maintain non-repudiation. The proposed scheme used the same message authentication schemes as used for pseudonym changing schemes and works on top of these techniques. In addition

to providing background details and discussing the research proposal, the chapter defined the problem using different models. The chapter provided simulation setup details on which the proposed scheme was tested in a global adversary setup equipped with powerful tracking algorithms. The result section of the chapter discussed the resilience of the proposed system from tracing. The chapter also discussed the security analysis of the proposed mechanism against different possible attacks. The privacy scheme for a vehicular network must be evaluated against proper privacy metrics and using realistic mobility models. However, devising appropriate privacy metrics that can eliminate inconsistencies and demonstrate actual comparison performance is one of the areas open for research. The concept of pseudonym exchange and the use of scheme permutation can also be helpful in preventing location tracking performed by adversaries. The next chapter of the thesis explores this approach in a vehicular network and tests it against few appropriate privacy metrics.

Chapter 5

Towards Location Privacy

A Cooperative Pseudonym Exchange and Scheme Permutation Approach

5.1 Introduction

This chapter of the thesis is based on the theoretical foundation of the previous chapter and contributes to vehicular networks' privacy issues. In the last chapter, we added an outer layer shield (level 3 of Figure 4.12) against privacy threats. This chapter contributes one level down (level 2 of Figure 4.12) to demonstrate the impact of using pseudonym exchange and pseudonym change scheme permutation. With the emerging advancements in a vehicular network, preserving location privacy has become a vital requirement. In the previous chapters, we have seen a considerable amount of work reported by the research community and standard developing organizations towards this end. Many regions have reached a consensus to adopt a PKI-based pseudonym authentication system to ensure security, privacy, and trust [11,230]. The standard mechanism suggests changing the pseudonym after a specific interval to avoid location tracking. Researchers have proposed various privacy preservation schemes based on pseudonym change in the past few years to address these concerns. Most privacy schemes focus on changing the pseudonyms after a

specific interval of time or in some particular scenarios (can be mix-context or mix-zone) to avoid linking messages [208, 212–214, 222, 226]. However, a consensus could not be reached to adopting a specific pseudonym change-based scheme. There is a need for a better approach under a PKI-based pseudonyms authentication system, which can leverage the power of baseline mechanisms to prevent location tracking.

Motivated by the facts discussed above, this chapter contributes to this vital area of the research and proposes a new scheme called Cooperative Pseudonym Exchange and Scheme Permutation (CPESP). In the proposed scheme, vehicles are allowed to exchange their pseudonyms cooperatively. Since the proposed mechanism allows an exchange of pseudonyms between vehicles, it also eliminates location tracking by service providers. Vehicles are also allowed to change (permute) schemes depending on a context that can help create confusion for the adversary to improve privacy further. The motivation behind CPE is that privacy can be improved when a lot of vehicles are involved in pseudonym exchange. Although PKI ensures that identity mapping (a pseudonym to real identity) is concealed, the pseudonym exchange can build trust among vehicles about their privacy in a centralized security system. The objective behind introducing SP is that a single scheme may not fit in a different mobility context. When random schemes are used to change pseudonyms, it becomes harder for an adversary to track. The adversary cannot apply a scheme-based tracking algorithm since it does not know for sure which scheme is used.

The chapter is based on the theoretical foundation of the previous chapter that includes detail of the PKI-based pseudonyms authentication system and related works. The problem definition is the same and based on a similar system, communication, adversary, and attack models. This chapter proposes a new privacy-preserving scheme named CPESP, which combines two techniques: cooperative pseudonym exchange and scheme permutation. The proposed techniques CPE, SP, and their combination CPESP are implemented in the PREXT simulator with a

realistic mobility map to demonstrate their performance. The proposed mechanism is evaluated using some of the essential privacy metrics against deployed adversary model. The performance of the proposed mechanism is compared with some of the existing and popular baseline schemes (discussed in the previous chapter) for comparative analysis.

The rest of the chapter is organized as follows. This chapter does not cover the background detail, a brief survey of related work, and problem definition as it has been already discussed in the previous chapter. The next section, Section 5.2, presents the proposed mechanism. The evaluation of the proposed mechanism and obtained results are discussed in Section 5.3. Section 5.4 conducts the security analysis. Finally, the chapter is concluded in Section 5.5

5.2 Proposed Mechanism

One of the standard methods for implementing privacy in a vehicular network is using the PKI-based pseudonym system to create a virtual identity for a user to hide the original identity. Previous studies have tried to preserve privacy from adversaries by implementing a pseudonym change approach. The main disadvantage of this method is that creating multiple pseudonyms for a single vehicle is computationally heavy, and still, vehicles can be tracked after analyzing their messages and communication patterns over a period and linking the pseudonyms. Using only one approach to change pseudonyms is also vulnerable to tracking. We wish to implement a system different than this traditional approach, which improves over the previous strategies in providing enhanced user privacy and prevents tracking. We propose a system that can work in varying mobility conditions. The proposed mechanism has two parts cooperative pseudonym exchange and scheme permutation, which are described in the following subsections.

5.2.1 Cooperative Pseudonym Exchange

The pseudonym exchange method is an implementation of the simple transaction of pseudonyms between two nearby vehicles so that the identities of the two vehicles become indistinguishable after the transaction hence hinders the tracking activities by any adversary in the network. The abstract analysis is as follows. When a vehicle wishes to exchange its pseudonym with its neighbor vehicle, it sends an exchange request beacon to the neighbor. The receiver checks whether it has been changing its pseudonym frequently by keeping a timeout for exchanging. When the timeout is reached, the receiver accepts a request for the exchange and carries the process forward. The two users exchange the pseudonyms, and new pseudonyms are assigned. The entire exchange happens under encryption so that adversaries don't resolve the pseudonym exchanges.

The objective of this method is achieved when both vehicles are similar in driving characteristics such as travel direction, speed, etc. Exchanging pseudonyms without taking care of such parameters may fail to trick the adversary, whereas keeping a considerable bound on these parameters for an exchange can significantly increase the intractability of the vehicle; hence adversary may not succeed in tracking and linking. Our proposed strategy is inspired by [231], which offers a considerable amount of privacy from the network operators because it does not involve CA in the exchange process.

In the proposed method, instead of involving only two participants in the exchange process, the number of participants can be determined by the nearness of neighbors. Also, each vehicle independently keeps changing its pseudonym, as described below. In dense traffic areas, exchanging pseudonyms increases non-traceability. Based on the traceability of the current pseudonym, the node may wish to change its identity. Each node keeps broadcasting safety message beacons. The beacon has a flag, *readyToExchange*, saying whether the vehicle is ready to

exchange pseudonyms with neighbors. Previous works have suggested that too frequent pseudonym change affects the performance of VANETs. Hence in the proposed system, a node becomes ready for exchange only after 60 seconds since the previous time the node was involved in some exchange.

Each node has a set of unused pseudonyms and also has a current pseudonym using which it is communicating for authenticity. The scheme permutation (SP) part of CPESP replaces the current pseudonym with one of the unused pseudonyms when required. The node of interest (NIS) maintains a list of neighbors of its neighbors, which are within a threshold distance from the NIS. The neighborhood information can be maintained by listening to the beacon messages. When the number of neighbors is beyond a threshold ($kNeighbours$), the node starts the exchange process.

Say $PK_1, PK_2, ..., PK_n$ are the public keys of the neighbors (including the NIS itself). The NIS creates a random permutation (shuffle) of these public keys. Now, if at the i_{th} position, if PK_j is present (where PK_i was present initially), it means that the i_{th} vehicle should send its set of pseudonyms to the j_{th} vehicle. The NIS sends $n-1$ messages, one for each neighbor. The i_{th} message is encrypted using PK_i so that only that particular neighbor can decrypt it. These messages are called $CHANGE\_INSTR$ messages. The i_{th} message contains the public key PK_j, which is present at the i_{th} position in the random permutation. The job of NIS in the exchange process ends here.

When a vehicle receives a $CHANGE\_INSTR$ message, it decrypts (tries to) the message using its private key. After decryption, the node reads the public key (PK_j) present in it. The node can choose not to send any pseudonyms to the j_{th} vehicle if it is running out of unused pseudonyms. If it has a large enough number of unused pseudonyms, it selects some and sends them to the j_{th} vehicle. This message is encrypted using the public key PK_j so that only the j_{th} vehicle can read it. This

message type is called $PSYNM\_SET\_MESSAGE$.

When a vehicle receives a $PSYNM\_SET\_MESSAGE$ message, it decrypts (tries to) the message using its private key. After decryption, the node also adds the pseudonyms present in the set to its set of unused pseudonyms. The vehicle changes its pseudonym after this process.

5.2.2 Scheme Permutation

After having studied the existing schemes and having tested them on simulations, we realized that if the change of pseudonym in sparse traffic is carried out with the same scheme, it becomes easy for an adversary to track it. Thus, to address this problem, we introduced a unique strategy and named it schemes permutation.

The network consists of vehicles as nodes, with each node possessing a set of pseudonyms. The existing works suggest following their schemes; however, only one scheme may not fit in the different and dynamic context of the vehicular network. In the proposed method, the nodes can use a random pseudonym change scheme in fixed time slots. This change happens within its own set, i.e., it chooses a new pseudonym from the set it currently has. At the beginning of each time slot, a node selects one of the given schemes at random. In this chapter, two baseline schemes have been considered, namely, Random Silent Period (RSP) and Periodical Pseudonym Change (PPC). After choosing the scheme for the time slot, the node follows that scheme to change its pseudonym in that time slot.

The nodes achieve enhanced privacy by using these two schemes at random. Since the choice of scheme is random, the pattern in pseudonym change becomes random and harder to trace over a long period. Also, since the adversary may not be able to figure out the scheme the vehicle is using, it becomes tougher to trace. Therefore these two features of cooperative pseudonym exchange and scheme permutation can help preserve location privacy in an enhanced manner than the

existing solutions.

5.2.3 Algorithms

This section of the chapter presents the algorithms that have been used to implement the proposed strategy.

The Algorithm 5.1 takes as input a list of public keys of neighboring vehicles (and the vehicle itself) that are willing to exchange pseudonyms set. Then it assigns t to a random shuffle of the list. The *send_change_instr* function sends a message to the vehicle having *sendTo* as its public key to send pseudonyms to the vehicle having *value* as its public key.

Algorithm 5.1: exchangePsynm (pkList)

1: $t \leftarrow random\_shuffle(pkList)$
2: **for** i : 0 to size(t) - 1 **do**
3: $\quad send\_change\_instr(sendTo = pkList[i], value = t[i])$
4: **end for**

The procedure is given in the Algorithm 5.2 run just before a beacon is to be sent. It checks if the number of neighbors has reached the required threshold ($kNeighbours$) for exchange and the vehicle itself is also ready. In that case, it calls the $exchangePsynm$ procedure with the neighbors' public key list and even its own public key. Then it sets the ready flag of the beacon based on whether $thresExchange$ amount of time has passed since the last exchange. Finally, the procedure clears the $neighbourPKList$.

The vehicle using Algorithm 5.3 tries to decrypt the instruction using the private key. If it fails, then it assumes that the message is not intended for it. Hence, it ignores and returns. If not, it checks if enough pseudonyms are left using the utility function $notEnoughPsynmsLeft()$. Then it chooses a subset of unused pseudonyms

Algorithm 5.2: beaconToBeSent(bcn)

```
1: if nNeighbours ≥ kNeighbours and this.readyToExchange then
2:     exchangePsynm(neighbourPKList + self.PK)
3:     this.lastExchangeTime = currentTime()
4: end if
5: if this.lastExchangeTime + thresExchange ≥ currentTime() then
6:     readyToExchange ← true
7: else
8:     readyToExchange ← false
9: end if
10: bcn.setreadyflag(readyToExchange)
11: nNeighbours ← 0
12: neighbourPKList ← NULL
```

Algorithm 5.3: handleChangeInstr (instr)

```
1: instr ← decrypt(instr)
2: if failureToDecrypt then
3:     RETURN
4: end if
5: if notEnoughPsynmsLeft() then
6:     RETURN
7: end if
8: lastChangeTime ← currentTime()
9: psynmSendList ← pickFromUnusedPsynms()
10: sendPysnmSet(sendTo = instr.PK, list = psynmSendList)
```

using *pickFromUnusedPsynms*. After that, it sends these pseudonyms to the vehicle having the public key *instr.PK*. The function *sendPysnmSet* sends the

list of pseudonyms to the vehicle having PK *sendTo*. The message is encrypted using this PK itself.

Algorithm 5.4 is used to handle received messages. If the message type is $CHANGE\_INSTR$, then *handleChangeInstr* is called. If it is $PSYNM\_SET\_MESSAGE$, then the node tries to decrypt the message. If decryption succeeds, then it adds the pseudonym list in the message to its set of unused pseudonyms and the vehicle changes its pseudonym. It is also used to maintain the neighbor list. If the node is farther than *neighbourRadius* from the current vehicle or its ready flag is not set, it is ignored. Else, it is added to the neighbor list.

The Algorithm 5.5 is the scheme permutation(SP) algorithm that runs parallelly along with CPE. The *state* is periodically updated between $CHANGE\_SCHEME$, $CHANGE\_PSYNM$ (end of periodical PC) and $EXIT\_SILENCE$ (end of RSP). When an update of *state* happens, the *schemePermutation*() procedure is invoked just after. During the $CHANGE\_SCHEME$ state, a random scheme is chosen, either RSP or pediodicalPC. The required setup for that scheme is done. In the end, a state change to the same state ($CHANGE\_SCHEME$) is invoked after *schemePeriodTime*.

Definition of some of the variables used in algorithms are as follows:
i) ***nNeighbors***: Number of neighbors (Active, ready to exchange). ii) ***readyToExchange***: Flag indicating whether the vehicle is ready to participate in exchange. iii) ***lastExchangeTime***: The time at which the vehicle last participated in an exchange. iv) ***neighbourPKList***: List of public keys of the neighbours. v) ***state***: Represents the current state of vehicle wrt SP algorithm. vi) ***bSilent*** : Whether the vehicle is in silent mode (for RSP).

Note: In this work, the broadcast beacons have been used to find k neighbors, which is enabled by the vehicle's V2V connectivity feature. We use V2V connectivity because all vehicles in the network need to have this feature. However, If we

Algorithm 5.4: msgArrived(msg)

```
1: if msg.type == CHANGE_INSTR then
2:     handleChangeInstr(msg)
3:     RETURN
4: end if
5: if msg.type == PSYNM_SET_MESSAGE then
6:     msg ← decrypt(msg)
7:     if failureToDecrypt then
8:         RETURN
9:     end if
10:    addToUnusedPsynms(msg.psynmList)
11:    changePsynm()
12:    RETURN
13: end if
14: bcn ← (BEACON)msg
15: if !bcn then
16:    RETURN
17: end if
18: if distance(bcn.position,this.position) > neighbourRadius then
19:    RETURN
20: end if
21: if !bcn.readyflag() then
22:    RETURN
23: end if
24: neighbourPKList.add(bcn.getPK())
25: nNeighbour ← nNeighbour + 1
```

Algorithm 5.5: schemePermutation()

```
1: if state = = CHANGE_SCHEME then
2:   curScheme ← random_scheme(RSP, periodicalPC)
3:   if curScheme = = RSP then
4:     Silent_period ← uniform_random (MinSilent_Time, MaxSilent_Time)
5:     bSilent ← true
6:     Schedule state change to EXIT_SILENCE after Silent_period
7:   else
8:     PseudonymLifeTime ← uniform_random (minPseudonym_Life,
       maxPseudonym_Life)
9:     Schedule state change to CHANGE_PSYNM after PseudonymLifeTime
10:  end if
11:  Schedule state change to CHANGE_SCHEME
     after schemePeriodTime
12: else if state = = CHANGE_PSYNM then
13:  changePsynm()
14: else if state = = EXIT_SILENCE then
15:  bsilent ← false
16:  changePsynm()
17: end if
```

take advanced features into consideration, such as Light Detection and Radar (LiDAR), RADAR, visual cameras, high precision position estimators, visible light communication, and other powerful sensors (features available with leading brands and automated vehicles), it is easy to find k neighbors of similar driving characteristics. These considerations of advanced features are out of the scope of this work.

5.3 Experimental Evaluation

This section of the chapter presents the experimental details that we performed on the PREXT simulation framework [217] and discusses the obtained results. It uses Veins framework [232] which is based on OMNET++ and Simulation of Urban Mobility (SUMO) [194]. This section also presents the comparison results of the proposed mechanism with some other popular schemes and discusses the advantage and limitations of the proposed system.

5.3.1 Simulation Setup

Simulation Parameters

The key parameters and their corresponding values used in the simulations are listed in Table 5.1. The global adversary model of the PREXT covers the whole road network and eavesdrop beacon messages for tracking. The adversary uploads the received beacons to a central entity called the vehicle tracker. The tracking algorithm used by the vehicle tracker has four iterative phases State estimation using Kalman filter, Data association using nearest neighbor probabilistic data association (NNPDA) algorithm, Gating phase, and Track maintenance phase [217].

Mobility on Real Road Map

The real road map of Munich city was obtained using the OpenStreetMap (OSM) [193]. This road map from OSM is imported to SUMO using an application called the NETCONVERT. Then POLYCONVERT tool of the SUMO is used. Then, we used the randomTrips python script to generate random vehicle trips. We generated a trip of 100 and 300 vehicles. Since we have taken an urban road segments, the max speed is set to $50km/h$ with an acceleration range varying from $-4.5m/s^2$ to $2.6m/s^2$. Figure 5.1.a and 5.1.b show the OSM file and the corresponding SUMO

Module	Parameter	Values
Hardware Platform	System	Intel(R) Core(TM) i5-6300HQ CPU @ 2.30 GHz 8 GB RAM
Operating System	Ubuntu	Version 16.04 64-bit
Simulator	PREXT	Version 1.0
Veins	Transmission power (Tx Power in mW)	20
	Bit rate (Mbps)	18
	Thermal noise (dBm)	-110
	Length of Packet Header (bit)	256
	Length of Beacon Payload (Byte)	100
	Beacon Rate (Hz)	1
	Traffic Simulator	SUMO 0.25.0
	Coupling using	TraCI
	Simulation Time (s)	1000
Adversary	Type	Passive (Evasdroping and Tracking), Global
	Range (m)	300
	Overlap (m)	30
	Tracking Interval (s)	1
Schemes		
PPC	Pseudonym Lifetime(s)	60
RSP	Pseudonym Lifetime(s), Min Silent Time(s), Max Silent Time(s)	60 3 11
SLOW	Silent Time threshold (s) Speed threshold (m/s)	5 8
CAPS	Min Pseudonym Lifetime(s), Max Pseudonym Lifetime(s), Min Silent Time(s), Max Silent Time(s), Missed Beacon Threshold, Neighborhood Threshold(m)	60 180 3 13 2 50
CPN	Radius(m) Neighbor Threshold	100 2
CPESP	Neighbor Threshold Scheme Period Time (for SP) (s) MinSilTime,MaxSilTime(RSP)(s) Pseudonym life time Exchange Threshold	2 60 (3, 11) 58 60

Table 5.1: Simulation Parameters

NET file of the Munich city. As a traffic simulator integrated with the PREXT simulator using TraCI, SUMO helped us map our experiment close to a realistic scenario.

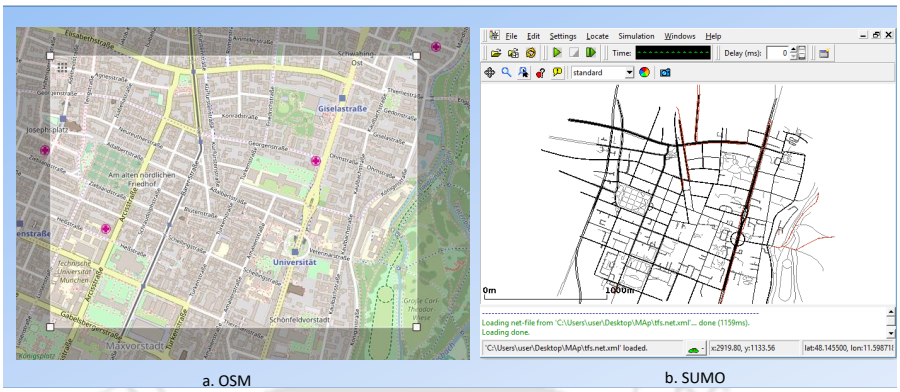


Figure 5.1: (a) OSM of Munich city (b) Corresponding SUMO Road Network

5.3.2 Results and Discussion

This section of the chapter presents the performance evaluation in terms of various vital metrics.

Traceability and Normalized traceability

Traceability denotes how effective the vehicle can be tracked by the adversary for more than 90% of the trace [226]. The continuous tacking of vehicles is necessary to breach privacy practically because the traces de-anonymization needs to have complete trajectories with allowable errors around endpoints. The calculation of Normalized traceability is done in a similar way; however, it neglects traces that never changed pseudonym.

Figure 5.2 and 5.3 depicts the traceability with 100 and 300 vehicles of our proposal and other schemes tested, respectively. Figure 5.4 and 5.5 depicts the normalized traceability with 100 and 300 vehicles, respectively. Periodical PC, RSP have poor performance because the scheme doesn't take into consideration the surroundings of the vehicle. RSP is a little better due to the silent periods. SLOW has very low traceability as the vehicle remains silent most of the time. This affects the safety and performance of the vehicular network. The proposed scheme CPE

performs better than most schemes like RSP, CAPS, CPN, etc. The performances of SP and CPESP are much better than all the other schemes for both metrics. Since the exchange happens at the vehicular plane, there is no overhead as well.

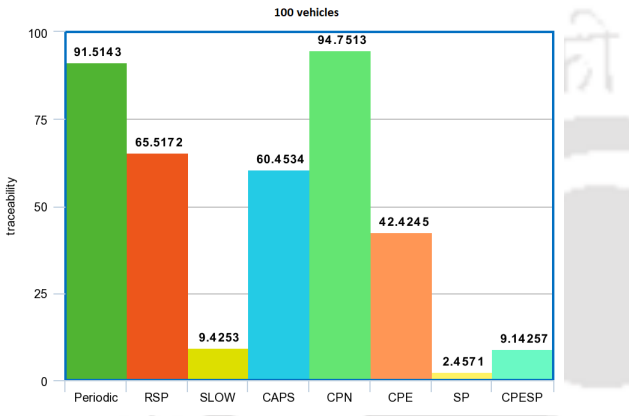


Figure 5.2: Traceability with 100 Vehicles

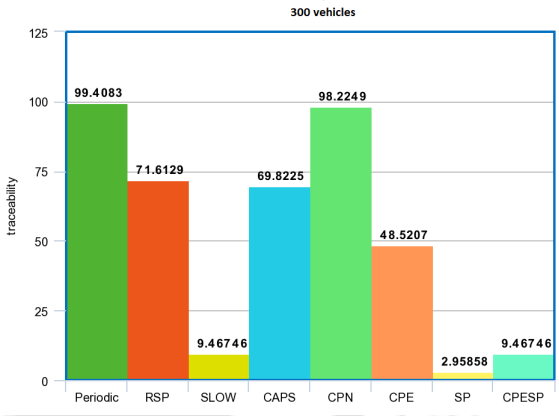


Figure 5.3: Traceability with 300 Vehicles

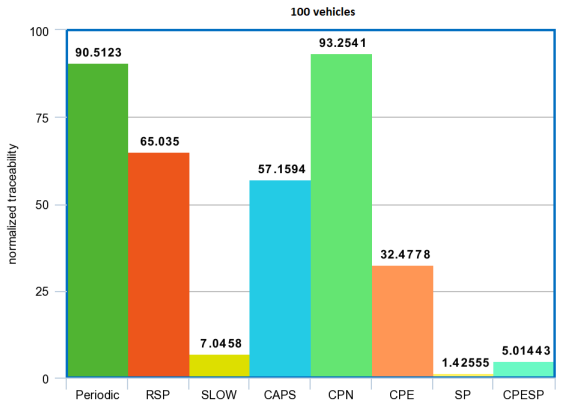


Figure 5.4: Normalized Traceability with 100 Vehicles

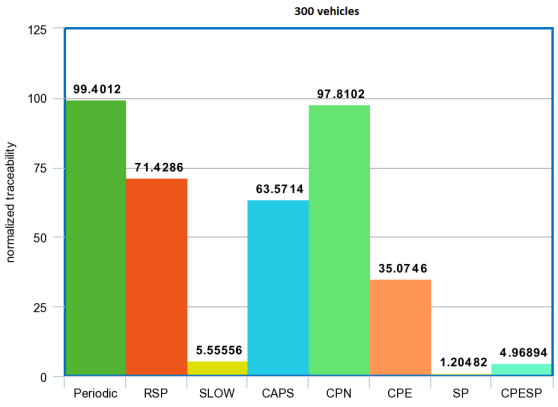


Figure 5.5: Normalized Traceability with 300 Vehicles

Avg Pseudonym Change Per Trace

As depicted in Figure 5.6 and Figure 5.7 the histogram denotes the number of times a vehicle tracked by the adversary changes its pseudonym for each scheme. The larger the value, the better the scheme is. Naturally, it is harder to trace vehicles that change their pseudonym more often. However, frequent pseudonym change also has a bad impact on safety applications. The proposed scheme performs better than all the other schemes in this metric. Most of the schemes have around 4.5 pseudonyms per trace, while ours (SP) has 64. Also, CPESP has a change of approx 9.11 per trace, CPE has 5.55, both better than the other schemes.

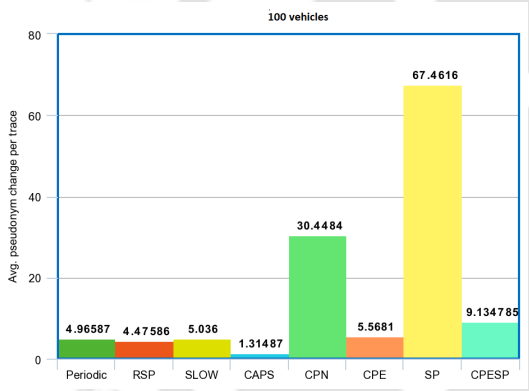


Figure 5.6: Avg Pseudonym Change Per Trace with 100 Vehicles

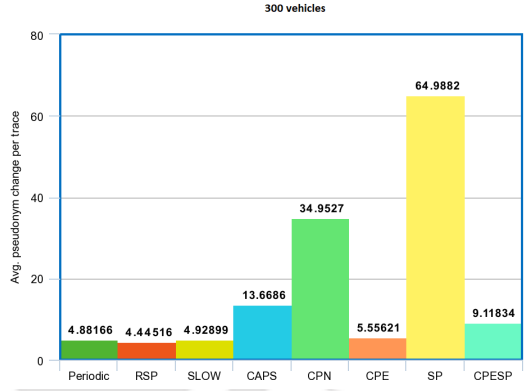


Figure 5.7: Avg Pseudonym Change Per Trace with 300 Vehicles

Average Confusion Per Trace

As the name of the metric suggests, it is related to how much the scheme confuses the adversary. We got similar trends in sparse and dense vehicular density conditions of 100 and 300 nodes, respectively. More the value, the better the scheme is. Figure 5.8 and Figure 5.9 shows the average confusion per trace for each scheme tested for 100 and 300 vehicles, respectively. SP outperforms all the other schemes by a wide margin in both the sparse and dense conditions. CPESP and SLOW have almost

equal values, while all other schemes (including CPE) have lower values.

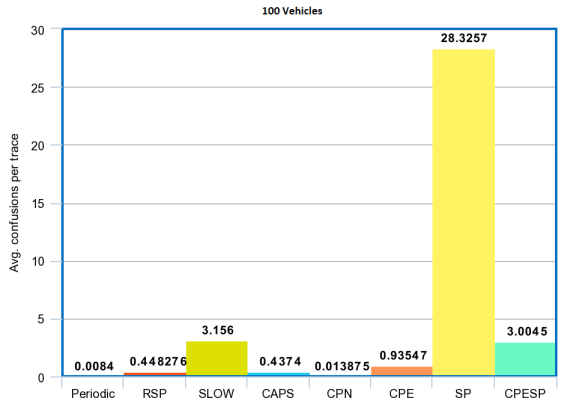


Figure 5.8: Avg Confusion Per Trace with 100 Vehicles

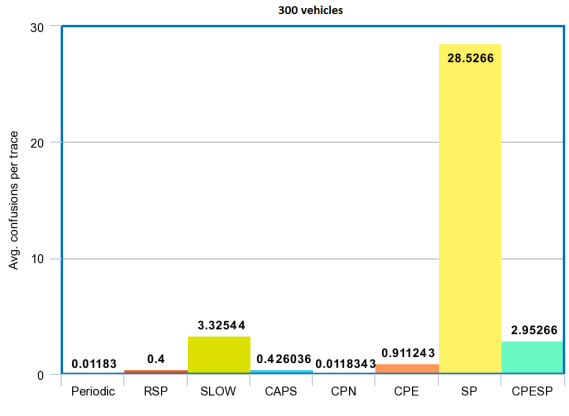


Figure 5.9: Avg Confusion Per Trace with 300 Vehicles

Average Confusions per Pseudonym Change

Figure 5.10 and Figure 5.11 represent an average number of confusion that happens per pseudonym change in case of sparse and dense conditions, respectively. This metric is the ratio of average confusions per trace and average pseudonyms per trace. The proposed schemes have comparable performance in terms of this metric.

Anonymity Set Size

The anonymity set size is defined as: Among how many other vehicles the target vehicle is indistinguishable to an adversary. Therefore it takes into account the number of potential vehicles linked to the sought one and the probabilities assigned to the vehicles.

Let N be the total number of vehicles that are linked to the item of interest with a non-zero probability ($p_i > 0, i = 1..N$). The anonymity set size is defined as the entropy H(X) of the distribution X of probabilities that link the vehicles

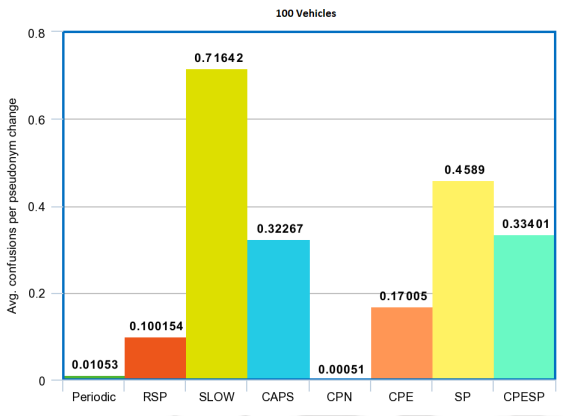


Figure 5.10: Avg. Confusion per Pseudonym Change with 100 Vehicles

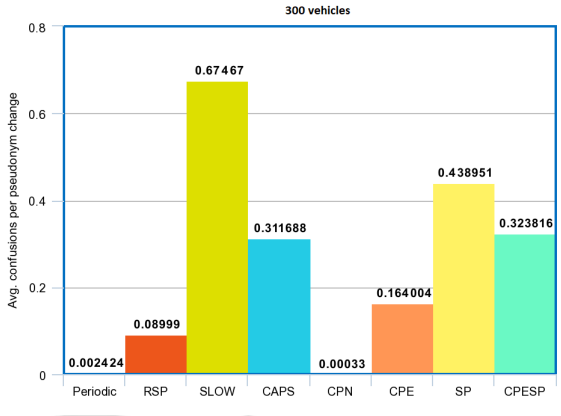


Figure 5.11: Avg. Confusion per Pseudonym Change with 300 Vehicles

of the anonymity set to the target vehicle. Based on the information obtained by the adversary, different vehicles may appear to have different probabilities (higher or lower) of link with the target vehicle. The more equitably distributed the probabilities attributed to the subjects of the anonymity set, the higher the anonymity set size. Assuming each vehicle in the set is targeted with equal probability, the larger the set size, the better is the scheme. The proposed scheme SP has a larger value of this metric than any other scheme in sparse as well as dense conditions. As shown in Figure 5.12 and 5.13, proposed schemes perform better or similar to all other schemes. CPE and combined approach CPESP also have comparable performances.

Average Max Entropy

The assumption that all vehicles in this set are targeted equally likely may not be a practical assumption because the adversary may observe some vehicles more likely than others. Apart from this, we also consider entropy as a metric to measure the strength of the scheme. The entropy of a message source was defined by Claude E.

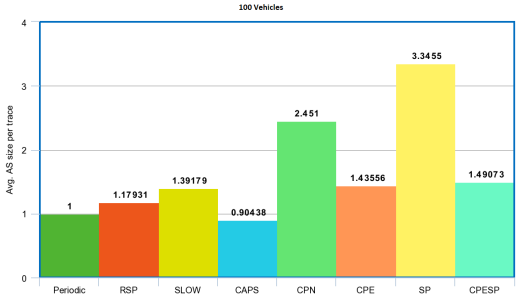


Figure 5.12: Anonymity Set Size with 100 Vehicles

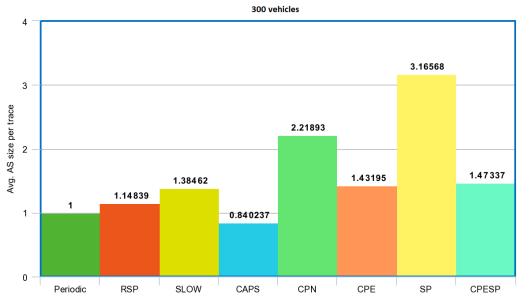


Figure 5.13: Anonymity Set Size with 300 Vehicles

Shannon [233] and found to be an appropriate metric to measure global anonymity.

Let i corresponds to a vehicle (subject) of the anonymity set N. N represents the number of vehicles to be analyzed (number of subjects), whereas p_i represents the probability that a certain vehicle i is the target one. The entropy H of identifying an individual vehicle in the anonymity set N can be calculated as:

$$H = -\sum_{i=1}^{|N|} p_i log_2(p_i)$$

Figure 5.14 shows the performance in terms of Average Max Entropy. With respect to this metric, our scheme SP outperforms all the other schemes. Our other two schemes, CPE and CPESP, also perform comparably to other schemes.

Discussion

The proposed scheme has two parts pseudonym exchange and scheme permutation. The pseudonym exchange can be used for non-safety critical messages only so that any misuse can be avoided; however, scheme permutation can be used for both the safety and non-safety broadcast messages. The pseudonym exchange process may create trouble not only for an adversary to trace but also to a trusted third party or service providers. However, vehicles can periodically upload the log file of

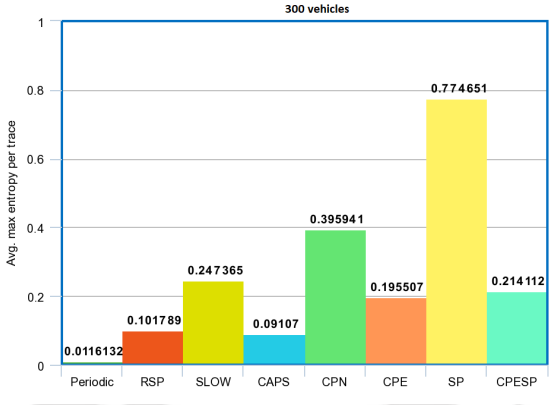


Figure 5.14: Average Max Entropy with 300 Vehicles

pseudonym exchange to the Certificate authorities (CAs), i.e., informing the CAs with whom, which pseudonyms, at what time the exchange happens so that CAs can do the traceability for trust management.

The existing pseudonym exchange method had one drawback; the number of swaps that are required to exchange the pseudonym of a given set of nodes is large. This is because only two vehicles can be involved in one swap. The proposed pseudonym exchange method improves over this by including multiple nodes in the exchange process. By this method, the number of exchanges happening to reduce significantly. To do good amount of exchange between N vehicles, slot swap needs $O(N^2)$ swaps while CPE does this with one exchange. Also, exchanging among a larger set (greater than size two) increases the entropy of the system and hence reduces traceability even further. Since exchange happens in CPE, the relatively smaller set of a pseudonym can do the job. CPE also eliminates the need for RSU/CA in the exchange process and hence is faster and protects vehicles from internal adversaries. Also, all computations happen at a vehicular level rather than at the RSU/CA. This significantly reduces network overhead. Since the exchange scheme is running simultaneously with the scheme permutation method, the user's privacy is enhanced, and non-traceability is further increased. We also argue that

if we change the pseudonym in a mix-context to preserve privacy in a vehicular network, we can allow vehicles to use multiple schemes and permute the schemes depending on the context to create confusion for the adversary. It can be seen from the result graphs that the scheme permutation (SP) has outperformed many schemes against the important metrics.

5.4 Security Analysis

This section of the chapter presents a security analysis of the proposed mechanism against linking attacks and assesses the level of anonymity in terms of anonymity set size.

5.4.1 Analysis Against Linking Attacks

To explain this, let us assume that an attacker knows the current pseudonym of the target. Once the attacker observes encrypted network traffic (pseudonym change instruction or pseudonym set messages) in the vicinity of the target vehicle, it cannot continue to track this vehicle. The details are as follows.

- An external attacker cannot decrypt the pseudonym change instruction or pseudonym set messages and cannot even distinguish between the two of them. The attacker cannot know if the target vehicle exchanged pseudonyms or not. Multiple vehicles change their pseudonyms at the same time after the exchange. This makes the linking attack harder to succeed. Hence the attacker cannot continue to link the pseudonyms used by the target vehicle.

- If the attacker is one of the nodes exchanging pseudonyms along with the target vehicle (but not the central node/node of interest), then the attacker can only decrypt the change instruction message sent to it. Thus, the attacker can continue to keep track of this vehicle only if the instruction tells it to

send pseudonyms to the target vehicle. Let there be N vehicles shuffling pseudonyms. The probability for this event is $(N-1)!/N! = 1/N$. For the attacker to successfully link the pseudonyms at least k times, P(k links) = $(1/N)^k$. This exponentially decreases as k increases; hence the attacker cannot continue the linking attack for a long time.

- If the attacker is the node of interest (NIS), then it can always send the pseudonym set to the target vehicle as it controls the random shuffling. But in this case, the target vehicle knows that it received the pseudonym set from the NIS as it can match the sender pseudonym of CHANGE_INSTR and PSNM_SET_MESSAGE it received. Therefore if the attacker does this continuously for k times, the target vehicle may suspect that it is being tracked as the probability that the NIS sends the pseudonyms k times continuously is very low ($(1/N)^k$). Hence the target vehicle can stop participating in CPE for some time if it suspects tracking.

In all possible cases, we can see that the proposed cooperative pseudonym exchange is robust against such attacks. The proposed mechanism works well against semantic linking because pseudonyms of vehicles with similar mobility are shuffled, and all vehicles change their pseudonyms simultaneously. The tracking algorithm applied in semantic linking cannot account for this shuffling. As previously stated, the tracking becomes harder when anonymity size increases.

In sparse density areas where CPE is not possible, SP can be targeted for linking attacks. However, the strength of the SP depends on the schemes used, and most of the schemes are strong enough against syntactic linking. The SP can be prevented against semantic linking attacks by considering schemes that use a better synchronization mechanism. Such schemes try to ensure that all vehicles change pseudonyms at the same time, which makes tracking difficult for the adversary. The

permutation of such schemes makes it stronger and more resistant to linking attacks, even in sparse conditions.

Correlation tracking is powerful if the adversary knows the scheme used by the vehicles as it can set the value of t1 accordingly. This is straightforward in the case of Periodical PC. In the case of RSP, the adversary can set t1 between minSilentTime and maxSilentTime. In the case of Slow, based on the current speed, the adversary can estimate the time at which the vehicle may speed down below the slow speed threshold and set t1 accordingly. The SP reduces the power of such an attack by randomizing the scheme. The attacker cannot predict the scheme used by the vehicle and thereby cannot evaluate t1 properly.

5.4.2 Analysis for Anonymity Set Size

The anonymity set introduced by Chaum [234] has been found useful in various studies to assess the level of anonymity and unlinkability, especially when the elements of the set have a uniform distribution. This section considers the anonymity set with the same consideration.

When analyzing the CPE, the scheme permutation is not considered, i.e., keep the scheme fixed. Let's consider the following denotations.

A_S: Anonymity Set

$|A_S|$: Size of Anonymity Set

K: Threshold for neighbors

t_{ex}: Threshold time for exchange

N_R: Neighborhood radius

δ: vehicle density and

$v(A)$: vehicles in area A, where $A = \pi * (N_R)^2$.

Considering vehicles are uniformly distributed, the $v(A)$, distributes according to spatial Poisson process [235]:

$$Pr\{v(A) = i\} = \frac{(\delta A)^i}{i!} e^{-\delta A} \tag{5.1}$$

CPE exchange occurs if atleast K neighbors are willing to exchange pseudonyms.

$|A_S|$ can take values from the set $\{1, K+1, K+2, ...\}$. A node can be ready to exchange if it has spent at least t_{ex} time since the last exchange. Let P_{ex} be the probability for this.

$$Pr(|A_S| = n)(n \geq K+1)$$

$$= \sum_{i=n}^{\infty} \{Pr(|A_S|) = n | v(A) = i\} \{P(v(A) = i) | v(A) \geq 1\}$$

$v(A) \geq 1$ because the target vehicle is present in the area.

$$= \sum_{i=n}^{\infty} \binom{i-1}{n-1} P_{ex}^{(n-1)} (1 - P_{ex})^{(i-n)} \left\{ \frac{P(v(A) = i) \cap v(A) \geq 1}{P(v(A) \geq 1)} \right\}$$

$$= \sum_{i=n}^{\infty} \binom{i-1}{n-1} P_{ex}^{(n-1)} (1 - P_{ex})^{(i-n)} \left\{ \frac{P\{v(A) = i\}}{1 - P\{v(A) = 0\}} \right\}$$

$$= \sum_{i=n}^{\infty} \binom{i-1}{n-1} P_{ex}^{(n-1)} (1 - P_{ex})^{(i-n)} \left\{ \frac{(\delta A)^i e^{-\delta A}}{i!(1 - e^{-\delta A})} \right\}$$

Expected size of anonymity set is

$$E(|A_S|) = \sum_{n=K+1}^{\infty} n * P(|A_S| = n) + 1 * (1 - \sum_{n=K+1}^{\infty} P(|A_S| = n))$$

Estimation of linking probability P_{link}, that an adversary can link two pseudonyms of the target.

$$P_{link} = P(|A_S| = 1) = 1 - \sum_{n=K+1}^{\infty} P(|A_S| = n)$$

5.5 Summary

This chapter is the second contribution towards the privacy issue in a vehicular network that proposed a CPESP approach to enhance the level of location privacy in a vehicular network. The scheme has two parts CPE and SP, which give three options CPE, SP, and CPE plus SP (CPESP). The suitable option can be capitalized by the users of the vehicular plane depending on the available context and type of applications. The chapter discussed the proposed mechanism in detail and presented various algorithms that have been used. The simulation-based experiment was conducted, and the performance of the proposed schemes was evaluated against some of the vital privacy metrics. To demonstrate the improvement, the proposed schemes are compared against some of the well-known mechanisms. Finally, the chapter analyzed the security of the proposed mechanism against possible internal and linking attacks. The chapter demonstrated how to deal with the powerful external adversary who captures the safety messages broadcasted using V2V for location tracking. Dealing with internal adversaries or misbehaving nodes is also very challenging in vehicular networks. Such nodes may try to gain over others by disseminating fake or false information over V2V communication. There is a need for a decentralized, efficient, salable trust management system to deal with malicious activities and misbehavior in vehicular networks. The next chapter of the thesis contributes towards this end.

Chapter 6

Towards Trust Management

A Blockchain and Smart Contract Based Decentralized Approach

6.1 Introduction

In addition to preserving users' privacy, building trust among all the users is another crucial requirement of vehicular networks. In a vehicular network, the vehicles use the information present in the received safety message to avoid an unwanted situation such as an accident, congestion, or some dangerous situation by effectively reacting to it. For example, other road users use the data of BSMs such as the speed, acceleration, heading, brake status, and other telemetry information about the vehicle to make smarter decisions for safety [146]. Therefore the accuracy and trustworthiness of the received data are of paramount significance. Vehicular network acceptance depends on the trustworthiness of data and entities sharing it because it affects driving decisions. The wrong decision taken on incorrect or false data can have disastrous consequences. As discussed earlier, the vehicular network is exposed to a range of threats to security and privacy. The presence of dishonest and misbehaving peers in the system is of a major concern, which may put lives in danger. Therefore establishing trust among these probable untrusted vehicles is one

of the most significant challenges of such a network.

As discussed earlier, in regions like the USA and Europe, a consensus is reached towards a PKI-based authentication system for ensuring security, privacy, and trust in a vehicular network. The standard IEEE 1609.2 and ETSI-TS-102 941 specifies misbehavior detection and trust management in protocol stacks of these regions. Although these systems have a great deal of attention, a critical portion of misbehavior detection and trust management remains relatively undeveloped. These developments are in their early research stage. To this end, a fair amount of research can also be found in the literature, which can be broadly categorized into centralized and decentralized solutions. In a centralized solution, central servers are utilized to collect, calculate, and store the trust values of all vehicles in a global scenario. The system is assumed to be a secure and fully trusted system. However, such assumptions are impractical and challenging to deal with a large number of vehicles, single-point of failure, performance issues, and security and trust-related issues. In a traditional decentralized solution, the system is deployed either at a vehicular plane or the RSU plane. The decentralization at the vehicular plane is impractical due to vehicles' highly dynamic nature, which may cause inconsistency and availability issues. The decentralization at the RSU level is also challenging in dealing with consistency, completeness, and reliability.

Trust management in a vehicular network needs to implement misbehavior detection, analysis efficiently, and decision making on reward and revocation [39]. There should be a mechanism to implement a reputation system of vehicles based on their trust value scored from their past behavior (reputation) and neighbors opinion about the received message broadcasted by the alarmer vehicle for an event. There is a need to integrate an incentives mechanism for the peers who behave well in the system so that they can earn a better trust score. There should be a proper punishment mechanism for the dishonest or misbehaving peers in terms

of trust score reduction and revocation after a certain limit of misbehavior. Most of the processes should be automated and decentralized in nature so that peers can trust the system. The deployed system needs to consider scalability, reliability, availability, accessibility, transparency, consistency, and immutability-related issues.

Motivated by the fact mentioned above, this chapter contributes towards trust management and proposed a blockchain and smart contract-based decentralized system. The blockchain is one of the disruptive technology in the financial industry, first proposed as the underlying technology for Bitcoin by Satoshi Nakamoto in 2008 [236]. Blockchain has become one of the driving forces of industrial IoT or Industry 4.0 [237] [238]. It is attracting a lot of attention from industries, academia, and research organizations. Its remarkable features such as high security (Merkel tree, hash function), decentralization, consensus (Proof of Work (PoW)), consistency, and reliability make it one of the potential candidates for establishing and managing the trust model in a vehicular network [239]. The use of blockchain technology inherits most of its useful characteristics in the proposed system. The use of smart contracts can automate entire functionalities and help to ensure fraud-free contract execution without involving a trusted third party. The introduction of a public blockchain makes the system decentralized, increasing the availability and enhancing the security of the system. The concept of sharding is introduced to solve the scalability issues. The proposed system tries to address the existing challenges of traditional centralized and decentralized trust management systems in a vehicular network. The chapter also introduces an incentive strategy for the vehicles participating in event detection, i.e., their contribution in the detection of a true event and its accurate reporting, which they can redeem for various services and payments. The revocation mechanism is also considered to blacklist the misbehaving vehicles. The proposed system is implemented on a testbed setup, using an open-source platform, Ethereum blockchain, and writing smart contracts to demonstrate

the feasibility, strength, and limitations.

The outline of the rest of the chapter is as follows. Section 6.2 present the background and survey on various techniques of trust management used in a vehicular network. Section 6.3 discusses the system model. Section 6.4 provides the detail of the proposed trust management framework. Experiment details and results are discussed in Section 6.5. Finally, Section 6.6 concludes the chapter.

6.2 Background and Related Work

This section of the chapter provides details of the technologies used in the proposed framework and provides a literature survey of trust management in a vehicular network.

6.2.1 Background

The chapter proposes a decentralized system for trust management, taking into account the core concepts of the blockchain. The core contribution of this work is designing, implementing, and evaluating a trust management system in a vehicular network using blockchain and smart contracts. Before providing details of implementation, the chapter provides an abstract overview of the blockchain, smart contract, sharding, and ethereum platform and discusses some key blockchain features.

Blockchain

A blockchain is a decentralized, distributed, unalterable, and append-only ledger that guarantees transparency in the chain's transactions. Blockchain can be used as a platform to build trust among untrusted parties. It facilitates storing the state in a distributed fashion among nodes of the network and continues to exist as long as

a network of nodes exists.

Smart Contract

A smart contract is a component of blockchain 2.0 that extends the capability of the earlier use-case specific blockchain by allowing code snippets defining business logic to be deployed on top of the blockchain. The smart contract ensures fraud-free contract execution without any trusted third party. It is a programmed logic having a predefined set of rules [240]. It enables users to execute a script in a verifiable manner on a blockchain network. It enables several issues to be solved in a way that minimizes the need for trust. In essence, smart contract functions as an autonomous entity on the blockchain and can execute logic deterministically as a function of the data provided to the blockchain.

Sharding in Blockchain

The current blockchain-based system with Proof-of-Work as the consensus mechanism faces the problem of scalability. The two most popular public blockchain platforms, Bitcoin and Ethereum, have an average transaction throughput of 8 txps (transactions per second) and 15 txps, respectively. In contrast, its counterpart VISA offers a transaction throughput of around 1700 txps. Blockchain sharding is an upcoming blockchain research domain that aims at improving the blockchain scalability in terms of transaction throughput by dividing the transaction loads on the full blockchain into several sub-blockchains where each sub-blockchain maintains a localized set of transactions. In blockchain sharding, the entire blockchain network is divided into some shards. A shard is a sub-blockchain maintained by a subset of nodes, also known as the committees from the global blockchain network. Each shard collects and processes a disjoint set of transactions. A shard is maintained by a committee of k members. Generally, k is significantly small in number as

compared to the participants in the global blockchain network. Having a smaller k facilitates to execute BFT based consensus algorithms; however, challenge-response-based consensus algorithms can also be used here. Smaller k also facilitates better use of network bandwidth for propagating the blocks as the committee members are mostly localized.

Ethereum Platform

Ethereum is an open-source blockchain platform that supports smart contracts. The platform facilitates the use of various programming languages to write the smart contract [241]. These smarts contracts can be converted into bytecode and are executed on Ethereum Virtual Machine (EVM). Ethereum facilitates the execution of its private and permissioned blockchain instance. In such an instance, only peers that are allowed to enter the network can view transaction data. Among those, only nodes that are granted special rights can participate in the mining.

Ethereum Blockchain Accounts: An entity holding an internal state is associated with an account in Ethereum. Ethereum distinguishes between two kinds of accounts, accounts owned externally and contract accounts. An externally owned account contains a private key making it a personal account. The key owner can send transactions to other externally held accounts or contract accounts from his/her account.

Key Features

Decentralization: Decentralization is one of the primary objectives of blockchain technology. Blockchain inherently keeps its data stored in multiple copies over multiple geographical locations making it highly available and lowering any successful attempts to modify chained data. It requires a malicious entity to have a hold on at least 51% of computing power in the blockchain network to execute a data alteration

attempt successfully [242].

Irreversibility and Immutability: Transactions once recorded in the blockchain cannot be reversed. The immutability property of the transactions recorded on the chain increases with each successive block being added to the chain. Once committed, the transactions can not be altered.

Digital Signature: Digital Signature is a facility provided by PKI that allows a party to prove the authenticity of data. Data is digitally signed by the sender party with their private key and is verified by the receiving party by the globally available public key of the sender. Each transaction in the blockchain network is digitally signed by the executor's private key and is verified by the miners with the available executor's public key ensuring non-repudiation against the execution of the transaction. The elliptic curve digital signature algorithm (ECDSA) is the standard algorithm used in blockchain [243].

6.2.2 Related Work

This section of the chapter discusses research contributions to misbehavior detection and trust management. As illustrated in Figure 6.1, research studies on trust models that include misbehavior detection in vehicular networks can be classified into three types [39, 244]: data-centric, entity-centric, and hybrid or combined. Similarly, deployment strategies for trust management can be broadly categorized into centralized and decentralized types.

Misbehavior Detection

Data-centric trust models concentrate on data trust calculation, while entity-centered trust models focus on a vehicle's trustworthiness computations. The characteristics of both data-centric and entity-centric are combined in hybrid trust models to assess the trust of a vehicle (entity) and the information (data) it transmits

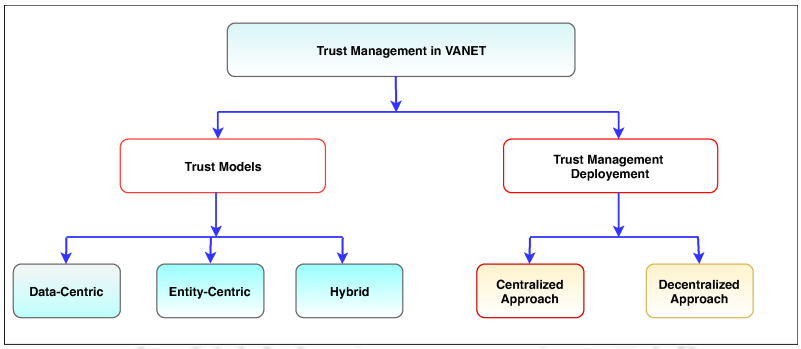


Figure 6.1: Trust Management in Vehicular Networks

[245].

Data-Centric: In a data-centric approach, the trustworthiness of data in terms of correctness, authenticity, and accuracy is computed. Since data plays a crucial role in such networks, it is assessed for trustworthiness before propagating it to others. Trust models using the data-centric approach are often based on the context of the event and considers location and time proximity, reports of the same event, and event types. Raya et al. have identified five popular techniques for data-centric trust models [246]: Most Trusted Report (MTR), Weighted Voting (WV), Majority Voting (MV), Bayesian Inference (BI), and the Dempster-Shafer Theory (DST). Various research studies [35, 246–250] exist in the literature that uses data-centric trust models in a vehicular network, each having their strength and weaknesses. However, the common deficiency is that making a trust decision takes a longer time. Two other major concerns are flooding of duplicate data in dense traffic conditions and performance issues in sparse traffic conditions.

Entity-Centric: In an entity-centric approach, the trustworthiness of entities (vehicles) plays a major role rather than the data. In vehicular networks, the trustworthiness of the entities has been considered as the basis for secure routing and reliable data delivery. There exist various entity-centric trust models in the literature that evaluate trustworthiness using the following methods: multifaceted approach

(experience, role, priority and majority opinion) [251], infrastructure-based trust and reputation approach (recommendation given by vehicles and RSUs) [252], cluster-oriented approach [253], dynamic entity-centric trust based on weight (application data and node) [254], etc. Three critical issues associated with entity-centric trust models are as follows. First, this model does not consider the data for assessing trust, which is an essential object. Therefore even if the transmitter is trustworthy, the correctness of received data in the presence of attackers remains uncertain. Secondly, it can perform well in low mobility and high vehicle density scenarios. Still, in high mobility and sparse traffic conditions, it may fail to obtain adequate data necessary for trust assessment. Third, this model depends heavily on the central authority to verify trust, which is the bottleneck. For example, in the case of role-based trust models [251].

Hybrid: Trust assessment is performed on the basis of the trustworthiness of the vehicles and the data they exchange. In the literature, very few hybrid trust model-based proposals are available, which are as follows. In the literature, very few hybrid trust models [255–257] based proposals are available, which are as follows. The complexity of implementing existing hybrid trust models is very high because a significant amount of messages need to be exchanged for data and entity trust assessment.

Trust Management

In vehicular networks, trust management architecture can either be centralized or decentralized. This relies on how trust models are implemented to establish trust, manage reputation, store, update, evaluate, verify, propagate it, etc.

Centralized: In a centralized architecture, a central trusted entity or server deployed in a secure zone is responsible for trust management. For example, a trusted third party (such as MA) is deployed in a PKI-based security framework of

the vehicular network. Trust management schemes based on a centralized approach have been proposed in [258–262]. In [258], the authors proposed TRIP, a novel mechanism to counter the attacks of dropping rational and irrational packets. Most of the processes of the proposed mechanism, such as receipts session processing, credit account update, state update, and eviction of a malicious node, are executed at a centralized trusted third party end. In [259], the authors proposed a centralized evaluation entity that processes locally created misbehavior reports of the vehicular and RSU plane. The central entity uses the reputation and trust information present in received reports to ensure the long-term functionality of the system. Li et al. [260] proposed a reputation system-based announcement scheme. The sensed data for traffic-related events are announced to neighbors by the vehicles. These messages are evaluated for their credibility, and generated feedback reports are uploaded to the centralized entity for reputation updates. In [261], authors proposed a reputation-based global trust establishment (RGTE) scheme for VANETs. This scheme allows for sharing the trust information safely by applying statistical laws. There is a centralized reputation management center (RMC) that gathers trust from all authorized nodes. It calculates the reputation of a vehicle but first filters out any suspicious trust messages.

In general, the schemes mentioned above need to have a centralized reputation management server to evaluate trust, establish a global reputation, and implement incentive strategies. However, such centralized trust management systems are impractical for a highly dynamic network like vehicular networks. It is challenging for such systems to deal with scalability, fault-tolerance, robustness, performance, and security and trust-related issues.

Decentralized: Various research studies have introduced a decentralized system for trust management to address the challenges associated with the above-mentioned centralized mechanisms.

The data-centric trust model introduced by Gurung et al. [249] relied on a decentralized approach: the trustworthiness of the message is evaluated in the vehicular plane without the need for any additional centralized architecture. The proposed model takes into account factors such as similarity of content, the similarity of the route, and conflict of content. Huang et al. [250], in its data-centric approach, used the voting-based system in a vehicular plane. The authors [263] proposed a conditional probability-based approach to detect malevolent vehicles at the vehicular plane. In this approach, the generated rating for a particular event is uploaded to the nearby RSU to maintain the trust information at the RSU plane. In the same line of thought, the authors [264] proposed the Distributed Reputation Management System (DREAMS) and introduced Vehicular Edge Computing (VEC) to execute vehicle reputation management functions (maintenance, manifestation, update, and usage) locally. The decentralization at the vehicular plane and RSU plane is very challenging in terms of availability, consistency, and resiliency.

Blockchain Related Works

This is not the first work that leverages blockchain technology. There are other works [265–268] in the literature that proposed frameworks based on this technology. In [265], the authors proposed a trust model from data-centric category and decentralized trust management using blockchain for vehicular networks. They used the Bayesian Inference model to assess the trustworthiness of the messages received from neighboring peers. In [266], the authors proposed an anonymous reputation system based on blockchain (BARS) to establish trust and preserve privacy in VANETs simultaneously. In [267], authors propose an intelligent vehicle trust point system for vehicle communication using vehicular cloud computing and blockchain technologies. Proof-of-Driving (PoD) was used as a consensus mechanism at the vehicular plane to reach the consensus among the vehicles. In [268], the

authors proposed a blockchain-based data sharing and trust management system in VANETs.

However, existing works emphasized mainly misbehavior detection and preserving privacy, not much on the maintained blockchain's internal aspects. Many important features are not covered, such as the node characteristics, transaction types, use of smart contracts for analysis, accessibility, incentive, revocation, etc. How to deal with scalability and roaming is not covered.

6.3 System Model

The system model considered in this chapter is similar to Chapter 4, with few changes at the RSU plane. This chapter considers the flourished stage of a vehicular network. RSUs are equipped with powerful computing and storage capacity, reliable and secured backhaul links to service plane, sensors, and secure wireless communication technologies for V2I/I2V connectivity. We can refer to it as the edge node, which can facilitate required caching, storage, communication, and computation to the proposed blockchain-based mechanism. It is also responsible for updating vehicle categories based on their sensing capacity, profile, and past behavior.

The vehicle's capabilities remain the same as the connected vehicle discussed in previous chapters. It runs WAVE protocol stacks for vehicular communication. In this work, the Traffic Authority (TA) is the supreme authority and plays a crucial role in registering the vehicles and deployment of the Regional Authorities (RAu). TA collects the information from the vehicles and issues them certificates via the PCA. It also assigns an initial trust value to the registered vehicles. In any system, there is always a hierarchy of trust levels. Vehicles can earn trust value by performing well. Vehicles that behave badly in the network are put into the Misbehaving Vehicle (MV) category.

The entire vehicular environment is divided into a number of regions based upon the geo-locations. RAu works in accordance with the TA and is responsible for deploying and maintaining the infrastructure in its territory. RAu is also responsible for providing vehicles entering its territory with a set of short-term keys for communications within the territory.

6.4 Proposed Framework

This section of the chapter discusses the proposed blockchain-based decentralized trust management module proposed at the edge nodes (RSU plane) of the vehicular network. The proposed blockchain-based framework for trust management is shown in Figure 6.2.

6.4.1 Initialization

The initialization processes of the proposed system are as follows.

Responsibility Assignment and Infrastructure Setup

The Traffic Authority initializes the system by deploying a Certificate Authorities and assigning a number of Regional Authorities in the network. Once the regional authorities are assigned by the TA, each regional authority deploys the necessary infrastructures such as the RSU edges for the functioning of the network. The maintenance and control of a territory's infrastructure is the exclusive responsibility of the Regional Authority concerned.

Vehicle Registration

A vehicle(V) generates its temporary public

$$PU_t^v$$

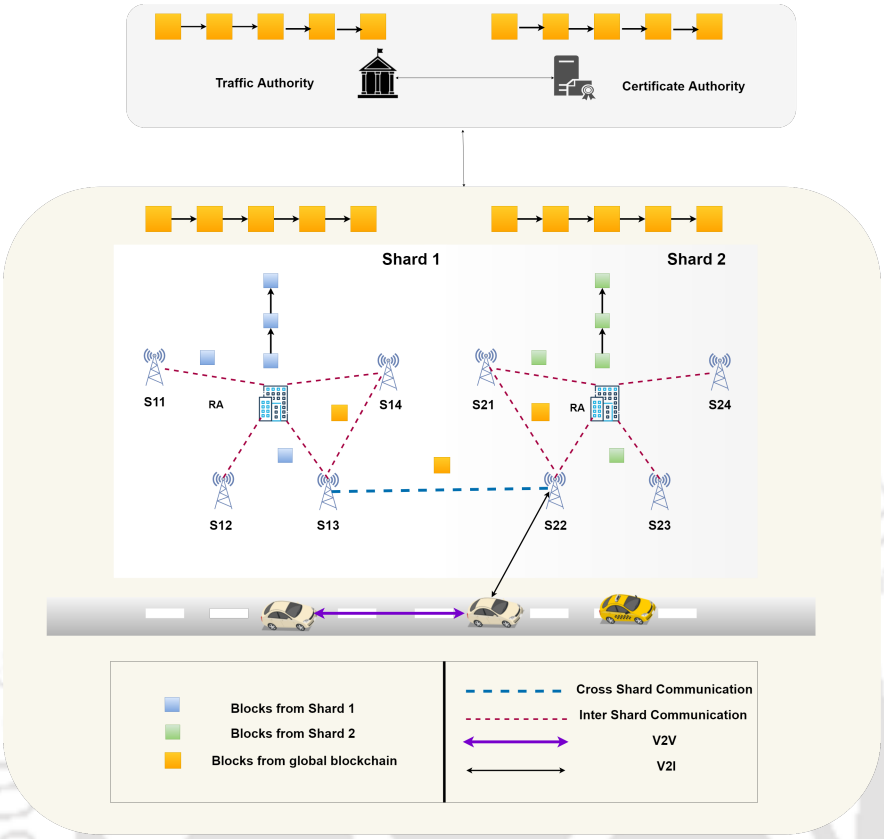


Figure 6.2: Proposed Blockchain Based Framework for Trust Management

and private

$$PR_t^v$$

key and send it to the Traffic Authority (TA).

$$SEND[E(PU_t^{TA}, details|PU_t^v)]$$

. The TA after verifying the details generate a pseudonym for the vehicle

$$V_{pseudo}$$

and SEND it to the Certificate Authority CA,

$$SEND[V_{pseudo}]$$

if the details are found to be valid and authentic. CA, PCA generates a certificate

$$Certificate^V$$

for the received

$$V_{pseudo}$$

, signs and writes the public key onto the ***globalBC*** (global blockchain) denoting it to be a valid public key and sends

$$Certificate^V$$

to the TA. The TA passes the certificate to the $\boldsymbol{V}$ further by

$$SEND[E(PU_t^v, Certificate^V)]$$

The mapping of the

$$V_{pseudo}$$

to the actual identity of the vehicle V lies with the TA only. The sequence diagram for obtaining a certificate by $\boldsymbol{V}$ is shown in Figure 6.3.

Short Term Key Distribution by Regional Authorities

Whenever a vehicle passes through different regions, the vehicle is provided with a set of short-term key pairs valid for that region only based upon the information available from the public blockchain. The Regional Authority gets the Trust Value of the vehicle and Wallet Score and stores these values against the temporary allocated address of the vehicle onto the local blockchain within the region. All the communications within that region take place with those sets of local key pairs only. When the vehicle is set to leave the region, it executes a transaction when the transaction gets minted onto the sharded blockchain. The Regional Authority executes a global transaction against the permanent public address of the vehicle that updates the score value of the vehicle on the ***globalBC*** (global blockchain).

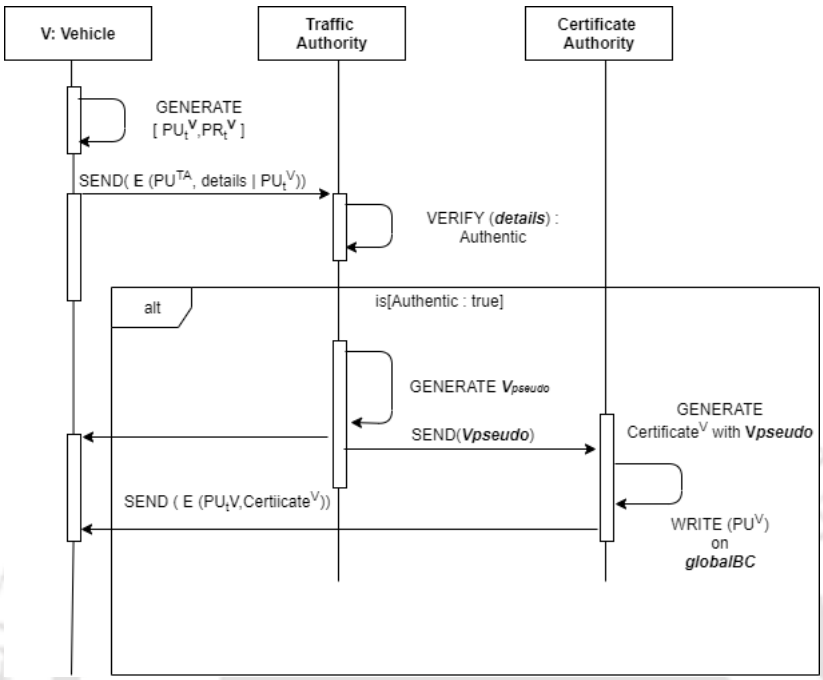


Figure 6.3: Sequence diagram for obtaining certificate

Blockchain Setup

The proposed framework set up a global blockchain along with the localized blockchain, also known as shards at various places, for improving the transaction throughput. The global blockchain is maintained by the TA, CAs, and the RAu(s) in the network and is open and decentralized. Because of the open and permissionless nature of participants of the blockchain network, the blockchain use PoW (Proof-of-Work) as the consensus mechanism. The true sense of decentralization of the global blockchain comes with the notion of allowing the participation of the RAu(s) along with the TA and the CA. As an RAu is free to deploy its infrastructure or RSUs, it gives the RAu(s) the freedom to deploy as many infrastructures as per its need and capacity, hence increasing the difficulty of competition. An RAu can decide the amount of computational allowable for the mining as per its flexibility. Whereas each RAu maintains a blockchain shard for processing the localized transactions

generated in its territory. The responsibility of maintaining the localized blockchain lies with the RAu and the infrastructure deployed in its territory. Due to the nature of being permissioned and closed, it is possible to execute an authoritative consensus mechanism within the localized blockchain network or the shard.

We used two different types of blockchains at two different levels is made with the underlying objective of reducing the transaction processing loads on a single blockchain. The concept of sharding in blockchains, along with the choice of using an authoritative consensus mechanism, has been utilized for localized transaction processing under each Regional Authority, which significantly reduces the transaction processing load. Also, data is generated under a particular RA may not be much significant to other RA's, and putting such information on the globalBC will put extra load on a single blockchain which may result in a blockchain bloat. Therefore, we made a separation of localized data processing from the global data processing on the blockchains. Also, the choice of using the consensus mechanism is made accordingly. A fast transaction processing algorithm is used in the local blockchain to handle the faster processing of a large number of localized transactions being generated. For interaction among the top-level entities (Figure 6.2), public/permissioned blockchain can be used. At the regional level, we use open and permissionless at the global level(globalBC) and private permissioned blockchain at the local level (localBC).

A shard exists in each territory. The maintenance of the shard lies with the RAu and its deployed infrastructure, RSUs. We choose to use an authoritative consensus mechanism in the shard. The authoritative consensus mechanism lies with a set of validators, in our case, the RAu, and its RSUs. The RAu is the initial validator and is authorized to allocate and deallocate the validation right to its RSUs. The consensus is achieved in rounds, where in each round, a validator proposes a block with the localized transactions coming from the shard. Other validators in the shard

check for the authenticity and validity of the block and accept and add the block to the blockchain if it is found valid. In the event that a block is found invalid, validators in the shard call to vote against the faulty validator, and if a majority votes against the validator, the validator is removed from the list.

6.4.2 Preliminaries

In the proposed framework of trust management, the TA governs the deployment of smart contracts. Each Regional Authority (RAu) deploys the same version of the smart contract, as mentioned by the TA. The RAu puts the hash of each of the deployed smart contracts onto the public blockchain. Therefore a vehicle, before interacting with the smart contract in an RAu, can verify the credibility of the contract. Road Side Units (RSUs) are configured and added to the blockchain by the TA calling *configureRSU:*. RSUs are the entity responsible for analyzing the reports. TA is also responsible for adding new vehicles into the system by calling *configureVEH*. At the time of registration, the TA provides the vehicle with a set of private/public key pairs before it enters the road. This can be done within an authoritative domain. The vehicles registered to the system are termed as *intelligentVehicle* in the smart contract analogy. An *intelligentVehicle* senses from its environment and participates in various events at the vehicular plane. In each event, a set of messages are exchanged among the vehicles, and many of these messages are incorrect and are generated from the misbehaving vehicles. Each event has a unique id, which we term as the session in our smart contract analogy. An *intelligentVehicle* reports about any suspicious activity on the road by calling *reportSuspicion*. Before calling *reportSuspicion* an *intelligentVehicle* checks for any unclaimed rewards that it has earned for participating in some earlier reporting. If yes, then it calls *claimReward* and claims the reward. RSUs call *analyseReports* with an arbitrary interval of time to analyze the reports given by a set of vehicles

for a particular session.

The smart contract maintains a set of registers with the help of mappings provided in solidity. The mapping is a hash table, which consists of key types and value type pairs.

- **Personal Transaction Register (PTR):** It keeps track of the information of the vehicle participating in a reporting session, the reporting that they make, and the status of the rewards to be received by them.

- **Score and Status Register (SSR):** It maintains the score of the reported vehicle from a session and also the verification status of those reports by the RSU.

- **Vehicle Register (VR):** VR maintains the information specific to a vehicle, such as an account no., credit score, trust value (TV), revocation status, claimed rewards and rewards yet to claimed.

- **Session Register (sessionRegister):** sessionRegister stores all the necessary information corresponding to a session such as total no. of vehicles participated, addresses of participating vehicles, address of alarmer vehicle (i.e., the first vehicle reporting a particular session), vehicle enrollment status (i.e., whether or not a vehicle is already enrolled in the session).

- **Vehicle in Session Register (VISR) and Claimable Reward Register (CR):** VISR is used by the report analyzing entities at the time of analyzing the reports. CR keeps track of all the vehicles eligible for getting a reward for their participation in a certain session.

6.4.3 Access Rights and other Logics

The framework provides appropriate access modifiers in the smart contract restricting a set of entities to execute certain functionalities of the contract. Like only an *intelligentVehicle* can call *reportSuspicion*. Similarly, only the TA can call *configureRSU* and only RSUs can call *analyseReports*. The snippet of modifiers that we implemented in the smart contract for various access rights is shown in Figure 6.4.

```
1
2  modifier intelligentvehicle (address _acno){
3      bool is_veh_intelligent = false;
4      if(vr[_acno].acno == _acno){
5          is_veh_intelligent = true;
6      }
7      require(is_veh_intelligent == true, "Not an intelligent vehicle");
8      _;
9  }
10
11 modifier onlyTA {
12     bool auth = false;
13     if(msg.sender == TAaddress){
14         auth = true;
15     }
16     require(auth == true, "You are not the traffic authority");
17     _;
18 }
19
20 modifier onlyRSU{
21     bool flag =  false;
22     for (uint i=0; i<roadsideunits.length; i++){
23         if(msg.sender == roadsideunits[i]){
24             flag = true;
25         }
26     }
27     require(flag == true, "You are not a RSU");
28     _;
```

Figure 6.4: Smart Contract Logics for Access Rights

The smart contract, besides managing the trust and detecting the false reporting of the vehicle, also takes care of the revocation of the vehicles relaying

falsified messages. Two types of revocation have been considered, which are listed below.

Soft Revocation: Each time a vehicle detected as misbehaving, it gets its TV deducted by 1. It gets itself blocked for a fixed interval of time during which it cannot execute any transactions on the blockchain.

Hard Revocation: Vehicles whose TV (trust value) falls below a threshold automatically get revoked from the system. This revocation is permanent, and only the TA has the authority to bring the revoked vehicles back into the system, which it can do within an authoritative domain. The snippet of these logics of the smart contract is shown in Figure 6.5.

There are various other important logics considered in this work to deal with situations that may arise in the real-life framework when dealing with trust management. For example, an appropriate logic in the smart contract to take care of duplicate submission of response by vehicles, etc.

```
modifier notblocked(address suspected_vehicle){
    bool flag = false;
    if(vr[suspected_vehicle].time > now){
        flag = true;
    }
    require (flag == false, "You are blocked for 1 minute");
    _;
}

modifier notrevoked(address _acno){
    bool statusrevocation = false;
    for (uint i=0; i<revocationlist.length; i++){
        if(revocationlist[i] == _acno){
            statusrevocation = true;
        }
    }
    require(statusrevocation == false, "Your vehicle is revoked");
    _;
}
```

Figure 6.5: Revocation Status of an Vehicle

6.4.4 Main Procedure

We consider the use case of earning reputation by a vehicle through their contribution to misbehavior detection. An intelligent vehicle participates in various events at the vehicular plane. For an event, a set of messages are exchanged between an event generating vehicle and other vehicles in its range.

Step 1. Transaction collection and Validation: Vehicles participating in the event check the validity (authenticity and integrity) of the received message. The framework assumes that the intelligent vehicles are running sophisticated models (discussed in the literature) that help them detect the truthfulness of the received messages in the vehicular plane.

Step 2. Report Suspicion: An intelligent vehicle reports suspicious behavior from its peer vehicles by analyzing their responses to an event. An intelligent vehicle reports the suspicion by calling *reportSuspicion*, which in turn results in a transaction.

Step 3. Block Sealing: RSUs in the region check the validity of the transaction upon receiving the transactions and seal the transaction in a block, which is eventually committed onto the sharded blockchain.

Step 4. Report Analysis by the RSU: RSUs at some random interval of time execute the *analyseReports* function. By executing the function, RSU checks for the correctness of the claim by an intelligent vehicle against another, suspecting it of a misbehaving one. Since RSUs execute these functions at a certain random duration, the duration should be such that by the time an RSU calls the function, all the transactions from that event have got mined into some blocks and are added to the blockchain. After the execution of the function, the suspecting vehicle gets punished if the claim turns out to be true, and the reporting vehicles get rewarded for their contribution.

Step 5. Mining: RSUs at the RSU Plane receive the transactions

corresponding to the ***globalBC*** and checks for its validity. RSUs acting as miner nodes bundle these received transactions together to form a block and perform a rigorous Proof-of-Work to get the block on the blockchain. Upon finding a block, a miner broadcasts the block to his peers. Since all the nodes in the network agree on this block, a consensus is reached, and that block is added to the blockchain.

Step 6. Claim of Reward by the vehicles: Once the RSU analyses the responses for an event and the reporting turns out to be true. Then the participating vehicles who honestly reported for the event can claim the rewards by calling *claimReward*. A vehicle needs to claim its reward from any previous event before participating in the next event.

Step 7. Vehicle leave from a Region: In case a vehicle leaves a region and tries to enter another region, it executes a `LEAVE-REGION` transaction.

Once the transaction is successfully minted onto the local blockchain maintained in the region, the corresponding RAu executes a transaction that updates the score values on the global blockchain taking the current values of the Trust Value and Wallet Score from the Smart Contract. The RAu maps the temporary credentials of the leaving vehicle to its actual permanent address. This updates the score values of the leaving vehicle V.

6.4.5 Algorithms

The three algorithms implemented in the smart contract to deal with reporting, analyzing, updating the trust score (increasing, decreasing putting in a revocation list), and providing incentives are given as follows.

In Algorithm 6.1, an *intelligentVehicle* calls *reportSuspicion* for reporting suspicious activities around itself. The reporting vehicle includes the session ID and suspected vehicle address in the transaction and sends it to the network to get it mined. The mining RSUs include these transactions to form a block and attempt

to add the blocks in the blockchain.

In Algorithm 6.2, RSUs call *analyseReports* at random interval of time different for each RSU. On being called, the module analyses the responses received within a particular session. The module gets the session to be analyzed from the RegisteredSession list. The module checks the score of each vehicle reported as suspicious in a session. The minimum number of vehicles needed to participate in an event is considered to be 4. The consideration is made to handle a scenario where an attacker vehicle creates a session and reports against a benign vehicle. Since no other vehicle will be reporting for the same session and by the 51% rule used in our analyzing module, the report is considered as true, resulting in an undesired punishment to the benign vehicle. Otherwise, if the majority of the participating vehicles identifies a vehicle to be suspicious, the reporting is considered to be true, and the TV of the suspected vehicle is decremented by 1 and is blocked for a minute. If the suspicious activity of the vehicle continues, the vehicle is revoked from the system.

In Algorithm 6.3, *claimReward* is called by an *intelligentVehicle* for claiming the rewards to be received for participating in true reporting in some earlier season. For true reporting, the TV of the reporting vehicle is incremented by 1, and the credit score of the vehicle is incremented by 5. If the reporting vehicle was the first one to report the suspicious activity, then the vehicle is considered as an alarmer vehicle, and the account of the vehicle is credited with two more credit points. Once *inteliigentVehicle* executes it, a transaction is generated, which gets mined by the RSU/miner.

Algorithm 6.1: Handle Reporting of an Event

Require: x (session ID), *suspectedVehicle* (Suspected Vehicle Address)

Ensure: Suspicion Reported

1: ***Require:*** msg.sender (*Reporting Vehicle*) is an intelligentVehicle, msg.sender is notRevoked, suspected Vehicle is an intelligent Vehicle, msg.sender is not Blocked
2: $s \leftarrow sessionRegister[x]$
3: **if** x is a new session **then**
4: Add x to *RegisteredSession* list
5: $s.alarmer \leftarrow msg.sender$
6: $s.count \leftarrow 1$
7: **end if**
8: $V \leftarrow VISR[x][s.count]$
9: $P \leftarrow PTR[msg.sender][x][suspectedVehicle]$
10: $S \leftarrow SSR[x][suspectedVehicle]$
11: $v \leftarrow VR[msg.sender]$
12: $C \leftarrow CR[v.reportNumber]$
13: **if** The session is in *RegisteredSession* and the report is not duplicate **then**
14: $V.registeredAddress \leftarrow msg.sender$
15: $V.doubtyVehicle \leftarrow suspectedVehicle$
16: $S.score \leftarrow S.score + 1$
17: $P.isrewardReceived \leftarrow false$
18: $P.submitted \leftarrow true$
19: $C.session \leftarrow x$
20: $C.suspectedVehicle \leftarrow suspectedVehicle$
21: $v.reportNumber \leftarrow v.reportNumber + 1$
22: $s.count \leftarrow s.count + 1$
23: **end if**

Algorithm 6.2: Analyzing Report and Trust update

Ensure: Analysed reports

Require: There must exist some session in *RegisteredSession* list which reports are not yet analyzed, msg.sender is RSU

Select an unprocessed session x from *RegisteredSession* list

$s \leftarrow sessionRegister[x]$

for Each participating vehicle i in the session x **do**

  $V \leftarrow VISR[x][i]$

  $suspectedVehicle \leftarrow V.doubtyVehicle$

  $S \leftarrow SSR[x][suspectedVehicle]$

  $v \leftarrow VR[suspectedVehicle]$

  if s.count >= 4 **and** S.score > s.count/2 **then**

    $v.TV \leftarrow v.TV - 1$

    $v.time \leftarrow v.time + 1minutes$

    if v.TV < 0 **and** v.Revoked ! = true **then**

      Put *suspectedVehicle* into *RevocationList*

      $v.Revoked \leftarrow true$

    end if

    $S.verificationResult \leftarrow true$

  end if

end for

Algorithm 6.3: Reward Claim by an Intelligent Vehicle

Ensure: Reward claimed credited to msg.sender account

Require: msg.sender (*Claiming Vehicle*) is $intelligentVehicle$, msg.sender is notRevoked
$v \leftarrow VR[msg.sender]$
$C \leftarrow CR[v.claimNumber]$
$x \leftarrow C.session$
$suspectedVehicle \leftarrow C.suspectedVehicle$
$S \leftarrow SSR[x][suspectedVehicle]$
$P \leftarrow PTR[msg.sender][x][suspectedVehicle]$
$s \leftarrow sessionRegister[x]$
if *msg.sender* has not claimed rewards for session x **then**
  if The reports of the session x is analysed by the RSU **then**
    if $P.submitted == S.verificationResult$ **then**
      $v.creditScore \leftarrow v.creditScore + 5$
      $v.TV \leftarrow v.TV + 1$
      $v.claimNumber \leftarrow v.claimNumber + 1$
      if s.alarmer == msg.sender **then**
        $v.creditScore \leftarrow v.creditScore + 2$
      end if
      $P.isrewardReceived \leftarrow true$
    end if
  end if
end if

6.5 Experimental Evaluation

This section of the chapter provides experimental setup details and discusses the results obtained after the experiment.

6.5.1 Prototype Detail: Testbed Setup

Figure 6.6 illustrates the prototype and the small scale testbed setup (Figure 6.7) corresponding to it for the proposed blockchain framework for trust management in a vehicular network. The experiment demonstrates the maintenance of the ***globalBC***.

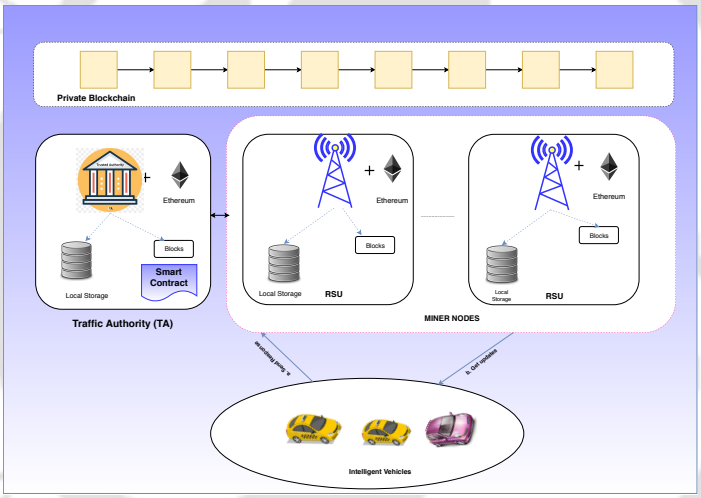


Figure 6.6: Blockchain Prototype of IoV

To implement the decentralized approach using a smart contract, the framework use a private permissioned Ethereum blockchain [269]. Private blockchain handles the flow of data based on the TA's specified and deployed smart contract or authorized policies. We use the cryptocurrency ether, which is provided in the core of the ethereum client, as a medium of exchange. Credit scores earned by the *intelligentVehicles* can be redeemed as the ether, which can be utilized by them for accessing various ITS-related services. The network proposed consists of three node types: full nodes, light nodes, and miner nodes.

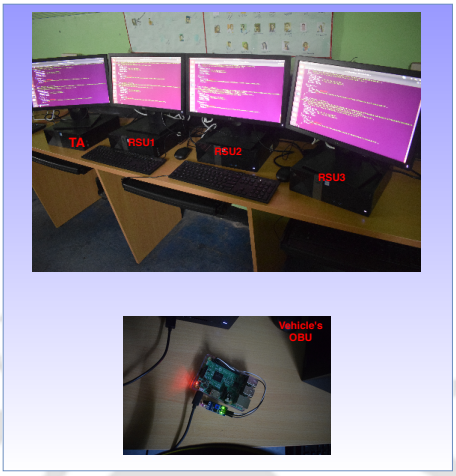


Figure 6.7: Testbed Setup

i) Full Node: A full node is a node that has the complete blockchain downloaded and available on the network. A full node fully enforces all of the rules of the blockchain.

ii) Light Node: A light node does not maintain an entire ledger of records on the blockchain; however, it gets the information of its interest from its peer trusted full nodes. This facilitates low-capacity end devices to participate in the blockchain network without downloading an entire copy of the chain locally. The trusted peer nodes act as an endpoint for the light nodes.

iii) Miners: Miners are the maintainers of a blockchain network that hold a full copy of the blockchain and are responsible for verifying the validity and authenticity of each incoming transaction in the network. They execute computationally expensive mathematical operations, also known as mining, prior to adding a block onto the chain.

In the private blockchain, the TA is a full node that may act as a miner or may not. RSUs act as a miner, whereas the vehicles are considered to be light nodes. Miners and full are preferred to be always active.

The testbed details are as follows: All PCs are of hardware configuration CPU:

Intel $Core^{TM}$ i7-7700 3.60GHz, 8 GB RAM, the hard drive of 1 TB, and running OS Ubuntu 18.04.1 LTS. Each full node, including the TA runs Ethereum's geth 1.8.17-stable client. We used 4 PCs with the above configurations, out of which one takes the role of TA, and the other three are RSUs. We use Raspberry Pi 3.3 PC as an OBUs of vehicles. They report the misbehavior detection to one of the RSU. Raspberry Pi 3 also runs Ethereum's geth 1.8.18 ARMv7 stable release and can work as a light node for executing the transactions. Raspberry Pi 3 node interacts with the RSU in wireless infrastructure mode. The backbone connectivity of TA and RSUs is wired network. For writing and compiling the contract, we used the Remix integrated development environment(IDE) and for Solidity, a browser-based IDE.

We conducted testbed experiments where the Raspberry Pi 3 node (vehicle) sends a set of the transaction of type *reportSuspicion* to our private blockchain platform in an asynchronous manner, i.e., all transactions are transmitted without waiting for a blockchain response. We implemented it to create the scenario of multiple vehicles reporting about the misbehavior to RSU after local detection. The no. of requests was set to 1, 100, 500, 750, and 1000. The obtained experimental results averaged over three independent runs. The transactions are placed in a javascript file and executed from the Raspberry Pi 3 light node. The interaction between the nodes in the private blockchain is accomplished with HTTP connections and web3.js and node.js API.

6.5.2 Results

The performance of the blockchain testbed is presented in this section. It shows the average throughput and execution time of the decentralized approach that uses a smart contract on Ethereum Blockchain for trust management at the RSU plane of the network.

Performance Evaluation

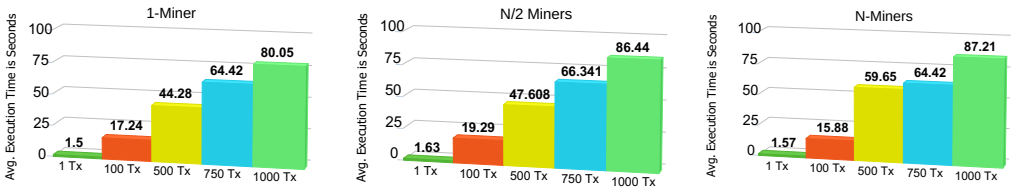
Values collected for each transaction in order to assess the performance of our configured private blockchain are as follows. Transaction (Tx) Deployment Time (t1): Unix time when transactions have been deployed. Transaction (Tx) Completion Time (t2): Unix time when the blockchain confirmed transactions. The transaction completion time was collected through web3.js APIs that return transaction details. We choose transaction execution time and throughput as parameters for evaluating our set up of the private blockchain.

Execution Time: The execution time is the total amount of time (seconds) during which all transactions in the dataset get executed and confirmed by the blockchain. It is the duration of time elapsed when the first transaction was deployed to the time when the last transaction is mined.

Throughput: It is defined as the number of successful transactions per second from the first deployment time of the transaction. Average throughput is the average over execution time.

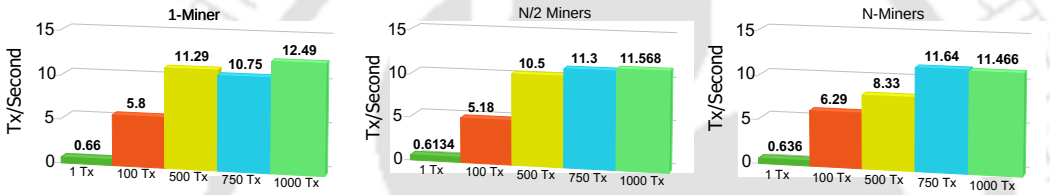
Comparing Average Execution Time: The performance is compared to the differences in execution time of varying transactions with three distinct sets of miners: 1, N/2, and N (in our case, N=4), as shown in Figure 6.8a, Figure 6.8b, and Figure 6.8c, respectively. The execution time grows as the number of transactions in the dataset increases. For a batch of 1000 transactions, the blockchain takes 80.05, 86.44, and 87.21 seconds with 1, N/2, and N miners.

Comparing Average Throughput: Figure 6.9a, Figure 6.9b, and Figure 6.9c shows the average throughput plot for varying sets of transactions with 1, N/2, and N miners, respectively. For a batch of 1000 transactions, the average throughput is found to be 12.49, 11.568, 11.466. Besides, one can see that as the number of transactions in a set increases, the rate of throughput decreases. Therefore for a huge set of transactions, the average throughput becomes some constant value.



(a) Avg. Execution Time with 1-Miner (b) Avg. Execution Time with N/2 Miners (c) Avg. Execution Time with N Miners

Figure 6.8: Avg. Execution Time Performance



(a) Avg. Throughput with 1-Miner (b) Avg. Throughput with N/2 Miners (c) Avg. Throughput with N Miners

Figure 6.9: Average Throughput Performance

6.5.3 Discussion

As we can see from the average execution time plot and the average throughput plot, increasing the number of miner nodes does not have a significant impact on improving system performance. However, an increased number of miner nodes definitely helps in making the system decentralized in a true manner, which comes at the cost of higher power consumption.

What we achieved?

Through the proposed framework for trust management using blockchain, we achieved the following goals.

- **Decentralized Approach:** In the proposed mechanism, most of the tasks such as verification, computation, result calculation, proof of work, mining, etc., are done at the edge level of the vehicular network in a decentralized manner, i.e., in a distributed fashion at the RSU plane. This approach minimizes the delay incurred in communication between vehicle and CA or TA, maximizes scalability, reliability, and can deal with fault tolerance.
- **Consistency:** The distributed RSUs executing blockchain technology maintain a consistent trust database. Any changes made in the database at any RSU propagated across all other RSUs via the blockchain in the network.
- **Availability:** Consistent information about the trust and its reward is always available at the edge of the network. Vehicles requesting that information can easily access them.
- **Encourage to behave well:** The framework introduced an incentive mechanism for vehicles behaving well and helping in the detection of misbehavior and reporting of true information to RSU. The incentives scored can be redeemed for various services such as insurance premiums, maintenance, etc.
- **Revocation:** Authorized peers who misbehave continuously lose their reputation in terms of trust score and are eventually removed from the system. However, the TA can take the help of other CAs to do the root cause analysis for misbehavior, and if it finds that it was intentional, then appropriate action must be taken.

6.6 Summary

The chapter proposed a decentralized trust management framework for a vehicular network that leverages blockchain and smart contracts to address the challenges

associate with traditional mechanisms. The chapter provided a survey of existing works available in this increasingly important area. In the proposed blockchain-based decentralized approach, the TA deploys the smart contract, and all RSUs work in a distributed manner to maintain a consistent vehicular trust database and enhance reliability, availability, and consistency. The idea of maintaining sharded blockchains has been introduced to reduce the propagation delay of transactions and to provide scalability. The framework also introduced an incentive strategy for the vehicles participating in event detection, i.e., their contribution in the detection of a true event, and its accurate reporting helps them to get rewards, which they can redeem for various services and payments. The proposed incentive mechanism encourages participating peers to perform well and get wallet points. However, if they do not perform well, they can be revoked from the system. The performance of the framework was evaluated on a small-scale testbed setup in terms of average throughput and execution time by deploying the private blockchain on the testbed, demonstrating its feasibility.

Chapter 7

Conclusion and Future Directions

Seamless V2I connectivity, privacy protection, and trust management are essential factors for public acceptance and the successful deployment of a vehicular network. These are the sub-problems of a vehicular network domain, where more efforts need to be put in. The thesis work focuses on highlighting various solutions for these problems from the SDOs and research communities, finding the gaps, and proposing solutions to them. This thesis also highlights our proposals' limitations and the possible future research directions in these three sub-domains of a vehicular network. The contributions of this thesis and future directions are summarized in the following sections.

7.1 Summary of Contributions

The first contribution of the thesis proposed a multipath approach under the new network paradigm of SDN to utilize multiple interfaces and better V2I connectivity in small cells. The main objective of such a proposal is to address issues of the traditional way of vehicle-to-infrastructure connectivity in small cells. The state-of-the-art solutions are discussed in detail. The challenges associated with these

solutions are also discussed. Existing solutions are not well suited to better and seamless V2I connectivity in HetNets and mainly focus on using a single RAT, either by offloading from one to the other or by coupling through additional nodes. The work discussed the motivation behind selecting MPTCP and SDN technologies and testing them in small cell deployments of Wi-Fi and DSRC. The results demonstrated the feasibility of the proposed solution through emulation-based experimentation and highlighted the limitations of these emerging technologies in a vehicular network context. A suitable mechanism is also proposed to address the challenges of seamless V2I connectivity in such setups.

The second and third contributions of the thesis tried to address the location privacy issue of a vehicular network. Preserving location privacy is one of the important factors for vehicular network acceptance. Since there is no standard solution available, this area is green and still open for the research community to contribute. Towards this end, an MPFSLP scheme is proposed in the fourth chapter that has been found resilient to tracking when applied on baseline schemes. The experiment is carried out on a PREXT simulator with mobility generated from SUMO. The proposed approach is analyzed against different types of attacks such as internal, external, and Sybil. The concept of casual dependency and proof-of-claim addressed the implications of the masqueraded approach. The theoretical foundation of this chapter is capitalized to extend the work, and a new scheme, CPESP, is proposed in the fifth chapter. Here the idea of pseudonym exchange and the use of multiple schemes are proposed. This scheme performed well in terms of important privacy metrics when evaluated against a global adversary on a simulation platform. The proposed CPESP scheme is compared against existing schemes and analyzed against different attacks.

The fourth contribution of the thesis focused on the trust management issue, which is another major obstacle in adopting the vehicular network. The blockchain

and smart contract-based decentralized trust management system is proposed in chapter 6 to address the challenges associated with state-of-the-art solutions. A comprehensive survey of the existing solutions is presented, and associated problems are also discussed. Trust management is still under development, and it is observed that the centralized solutions approach might not be practical for such a dynamic environment. The proposed mechanism focused on the decentralized trust management system and tried to provide a scalable, reliable, and immutable framework. The power of smart contracts is capitalized to eliminate the need for manual interventions and build trust among peers. The feasibility of the proposed approach is demonstrated through a small-scale testbed setup. It is also discussed how the proposed blockchain and smart contract-based setup could help achieve the design goals of trust management in vehicular networks.

7.2 Future Directions

The first contribution in chapter 3 can be extended in numerous ways, which can help to evolve MPTCP and SDN for V2I connectivity. The key areas related to MPTCP for V2I connectivity to which one can contribute are better congestion control, packet scheduling, synchronizing asymmetric paths, path management, subflow management, and dealing with lower layer handovers (e.g., layer-2 of WLAN). The SDN controller can have global knowledge of the available physical radio resources of each RAT along with the vehicle's mobility information such as speed, location, and anticipated heading. How intelligent vertical handover can be accordingly employed for switching purposes is one of the important areas to be considered for future research. The proactive rules for flow installation of anticipated data traffic to provide faster content delivery is another important area to be explored. Since this domain is totally new and wide open for research, the researchers can explore how such SDN-based intelligence can be deployed and tested for seamless

V2I connectivity in HetNet using emerging technologies such as network function virtualization, slicing, and edge computing. Machine learning-based approach can also be explored for path prediction. The role of edge and fog computing with SDN can be tested to minimize the delay and provide better content delivery services. There is a need to adopt better RSUs and APs placement mechanisms so that they can complement each other. A better mechanism needs to be devised to minimize the Wi-Fi handover delay for seamless and persistent connection. There is a need to improve rule installation (flow setup) by the SDN for high mobility and dense traffic scenarios. The performance of MPTCP for V2I in the presence of asymmetric paths such as Multi-tier and Multi-RAT (LTE-A, Wi-Fi, DSRC) can be another important research area.

The second and third contributions in chapter 4 and chapter 5 can be extended in numerous ways. The work in chapter 4 posits that the proposed MPFSLP scheme can also be applied natively or can be modified to cater to the security requirements of the Internet of Things. The impact of MPFSLP on ensuring accountability in vehicular networks needs to be explored. The details of these aspects can be explored in the future. The CPESP scheme proposed in chapter 5 can be extended by integrating more powerful schemes and synchronizing the pseudonym change to preserve location privacy. The cooperation in pseudonym exchange can also be enhanced by considering other important mobility parameters. Since safety applications are the top priorities in vehicular networks, analyzing the impact of the proposal on safety applications is another important area of research. One can explore the role of advanced sensors and powerful technologies in synchronizing the pseudonym change to enhance location privacy. The privacy issues associated with V2I communication are unexplored and must be considered in future research work. Devising appropriate privacy metrics, which can eliminate inconsistencies and demonstrate actual performance, is another area to be researched.

The fourth contribution in chapter 6 uses the concept of shards; however, the evaluation results do not analyze the benefit and impact on the number of shards on the performance. It can be considered as one of the important research areas in case of dynamic vehicular environment. The work does not consider the misbehavior detection at the vehicular plane using plausibility factors, filters, consistency (position, speed, heading), beacon frequency, etc. The misbehavior detection in a vehicular plane and ensuring anonymity and unlinkability in a blockchain-based system are important research areas. The role of AI in misbehavior detection and efficient consensus algorithms in the RSU plane for decentralized trust management are some other areas to be explored. Although blockchain features have been capitalized for solving the existing issues, blockchain integration in a vehicular network is found to be very challenging. Some of the major challenges are as follows. *(1). Maintaining performance to the allowable latency threshold and throughput. (2). Ensuring anonymity of users' identity and providing unlinkability of transactions. (3). Dealing with security flaws of blockchain setup. (4). Dealing with HetNets, different data formats, and semantics.* These areas can be considered interesting research avenues for blockchain adoption in vehicular networks to ensure enhanced security, privacy, and trust.

References

[1] G. Cordahi, R. Kamalanathsharma, J. Kolleda, D. Miller, S. Novosad, T. Poling, and S. Sundararajan, "Connected Vehicle Pilot Deployment Program Phase 1, Application Deployment Plan–Tampa (THEA)," Tech. Rep., 2016.

[2] M. Khan and K. Han, "A survey of context aware vertical handover management schemes in heterogeneous wireless networks," *Wireless Personal Communications*, vol. 85, no. 4, pp. 2273–2293, 2015.

[3] A. De La Oliva, A. Banchs, I. Soto, T. Melia, and A. Vidal, "An overview of ieee 802.21: media-independent handover services," *IEEE Wireless Communications*, vol. 15, no. 4, 2008.

[4] T. V. Pasca and B. R. Tamma, "Traffic steering in radio level integration of LTE and Wi-Fi networks," Ph.D. dissertation, Indian institute of technology Hyderabad, 2019.

[5] I. WP5D, "IMT-Vision-Framework and Overall Objectives of the Future Development of IMT for 2020 and Beyond," 2015.

[6] C. A. Kerrache, C. T. Calafate, J.-C. Cano, N. Lagraa, and P. Manzoni, "Trust management for vehicular networks: An adversary-oriented overview," *IEEE Access*, vol. 4, pp. 9293–9307, 2016.

[7] M. S. Bargh, R. Hulsebosch, E. Eertink, A. Prasad, H. Wang, and P. Schoo, "Fast authentication methods for handovers between ieee 802.11 wireless lans," in *Proceedings of the 2nd ACM international workshop on Wireless mobile applications and services on WLAN hotspots*, 2004, pp. 51–60.

[8] P. Machań and J. Wozniak, "Performance evaluation of ieee 802.11 fast bss transition algorithms," in *WMNC2010*. IEEE, 2010, pp. 1–5.

[9] N. Gupta, A. Prakash, and R. Tripathi, "Medium access control protocols for safety applications in Vehicular Ad-Hoc Network: A classification and comprehensive survey," *Vehicular Communications*, vol. 2, no. 4, pp. 223–237, 2015.

[10] I. Z. Bholebawa, R. K. Jha, and U. D. Dalal, "Performance analysis of proposed openflow-based network architecture using mininet," *Wireless Personal Communications*, vol. 86, no. 2, pp. 943–958, 2016.

[11] A. Boualouache, S.-M. Senouci, and S. Moussaoui, "A survey on pseudonym changing strategies for vehicular ad-hoc networks," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 770–790, 2017.

[12] J. Cregger, V. Brugeman, and R. Wallace, "International survey of best practices in connected and automated vehicle technologies: 2014 update," *Center for Automotive Research, Transportation Systems Analysis Group*, 2014.

[13] G. Araniti, C. Campolo, M. Condoluci, A. Iera, and A. Molinaro, "LTE for vehicular networking: a survey," *IEEE Communications Magazine*, vol. 51, no. 5, pp. 148–157, 2013.

[14] C. M. Silva, B. M. Masini, G. Ferrari, and I. Thibault, "A survey on infrastructure-based vehicular networks," *Mobile Information Systems*, vol. 2017, 2017.

[15] R. F. Atallah, M. J. Khabbaz, and C. M. Assi, "Vehicular networking: A survey on spectrum access technologies and persisting challenges," *Vehicular Communications*, vol. 2, no. 3, pp. 125–149, 2015.

[16] H. Hartenstein and L. Laberteaux, "A tutorial survey on vehicular ad hoc networks," *IEEE Communications magazine*, vol. 46, no. 6, pp. 164–171, 2008.

[17] J. Iannacci, "Internet of things (IoT); internet of everything (IoE); tactile internet; 5G–A (not so evanescent) unifying vision empowered by EH-MEMS (energy harvesting MEMS) and RF-MEMS (radio frequency MEMS)," *Sensors and Actuators A: Physical*, vol. 272, pp. 187–198, 2018.

[18] J. Contreras-Castillo, S. Zeadally, and J. A. Guerrero-Ibañez, "Internet of vehicles: architecture, protocols, and security," *IEEE internet of things Journal*, vol. 5, no. 5, pp. 3701–3709, 2017.

[19] H. Abou-Zeid, F. Pervez, A. Adinoyi, M. Aljlayl, and H. Yanikomeroglu, "Cellular V2X Transmission for Connected and Autonomous Vehicles Standardization, Applications, and Enabling Technologies," *IEEE Consumer Electronics Magazine*, vol. 8, no. 6, pp. 91–98, 2019.

[20] S. P. Mohanty, "Consumer electronics is the driver of smart car," *IEEE Consum. Electron. Mag.*, vol. 7, no. 5, p. 3, 2018.

[21] G. Naik, B. Choudhury, and J.-M. Park, "IEEE 802.11 bd & 5G NR V2X: Evolution of radio access technologies for V2X communications," *IEEE Access*, vol. 7, pp. 70 169–70 184, 2019.

[22] F. Tang, Y. Kawamoto, N. Kato, and J. Liu, "Future intelligent and secure vehicular network toward 6G: Machine-learning approaches," *Proceedings of the IEEE*, vol. 108, no. 2, pp. 292–307, 2019.

[23] C. B. Liu, B. Sadeghi, and E. W. Knightly, "Enabling vehicular visible light communication (V2LC) networks," in *Proceedings of the Eighth ACM international workshop on Vehicular inter-networking*, 2011, pp. 41–50.

[24] F. Domingos, L. Villas, and A. Boukerche, "Data communication in vanets: Survey, applications and challenges," *Ad Hoc Networks*, vol. 44, no. C, pp. 90–103, 2016.

[25] L. Azpilicueta, C. Vargas-Rosales, P. Lopez-Iturri, E. Aguirre, and F. Falcone, "Characterisation of radio wave propagation in vehicular environments through deterministic methods," in *2017 IEEE International Symposium on Antennas and Propagation & USNC/URSI National Radio Science Meeting*. IEEE, 2017, pp. 613–614.

[26] W. Wu, Z. Yang, and K. Li, "Internet of vehicles and applications," in *Internet of Things*. Elsevier, 2016, pp. 299–317.

[27] K. Zheng, L. Hou, H. Meng, Q. Zheng, N. Lu, and L. Lei, "Soft-defined heterogeneous vehicular network: Architecture and challenges," *IEEE Network*, vol. 30, no. 4, pp. 72–80, 2016.

[28] D. B. Rawat, Y. Zhao, G. Yan, and M. Song, "Crave: Cognitive radio enabled vehicular communications in heterogeneous networks," in *2013 IEEE Radio and Wireless Symposium*. IEEE, 2013, pp. 190–192.

[29] S. Shetty, K. Agbedanu, and R. Ramachandran, "Opportunistic spectrum access in multi-user multi-channel cognitive radio networks," in *2011 19th European signal processing conference*. IEEE, 2011, pp. 1229–1233.

[30] D. B. Rawat, S. Reddy, N. Sharma, B. B. Bista, and S. Shetty, "Cloud-assisted gps-driven dynamic spectrum access in cognitive radio vehicular networks for transportation cyber physical systems," in *2015 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, 2015, pp. 1942–1947.

[31] K. D. Singh, P. Rawat, and J.-M. Bonnin, "Cognitive radio for vehicular ad hoc networks (cr-vanets): approaches and challenges," *EURASIP journal on wireless communications and networking*, vol. 2014, no. 1, pp. 1–22, 2014.

[32] H. Zhu, S. Chang, M. Li, K. Naik, and S. Shen, "Exploiting temporal dependency for opportunistic forwarding in urban vehicular networks," in *2011 Proceedings IEEE INFOCOM*. IEEE, 2011, pp. 2192–2200.

[33] S. Tangade, S. S. Manvi, and P. Lorenz, "Decentralized and scalable privacy-preserving authentication scheme in VANETs," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 9, pp. 8647–8655, 2018.

[34] S. Chang, X. Liu, H. Zhu, M. Dong, K. Ota, and T. Lu, "Where were you yesterday: Privacy risk of published anonymous trajectories," in *2016 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2016, pp. 1–6.

[35] J. Kamel, F. Haidar, I. Jemaa, A. Kaiser, B. Lonc, and P. Urien, "A misbehavior authority system for sybil attack detection in c-its," 2019.

[36] C. Campolo, A. Molinaro, and R. Scopigno, "From today's VANETs to tomorrow's planning and the bets for the day after," *Vehicular Communications*, vol. 2, no. 3, pp. 158–171, 2015.

[37] D. Eckhoff and C. Sommer, "Driving for big data? Privacy concerns in vehicular networking," *IEEE Security & Privacy*, vol. 12, no. 1, pp. 77–79, 2014.

[38] C. Bernardini, M. R. Asghar, and B. Crispo, "Security and privacy in vehicular communications: Challenges and opportunities," *Vehicular Communications*, 2017.

[39] J. Zhang, "Trust management for VANETs: challenges, desired properties and future directions," *International Journal of Distributed Systems and Technologies (IJDST)*, vol. 3, no. 1, pp. 48–62, 2012.

[40] Z. El-Rewini, K. Sadatsharan, D. F. Selvaraj, S. J. Plathottam, and P. Ranganathan, "Cybersecurity challenges in vehicular communications," *Vehicular Communications*, vol. 23, p. 100214, 2020.

[41] "Car 2 Car - Communication Consortium: Manifesto," Available at https://www.car-2-car.org/index.php?id=31.

[42] "Safespot :Integrated Research Project," Available at http://www.safespot-eu.org/.

[43] C. Suthaputchakun, Z. Sun, and M. Dianati, "Applications of vehicular communications for reducing fuel consumption and CO2 emission: the state of the art and research challenges," *IEEE Communications Magazine*, vol. 50, no. 12, pp. 108–115, December 2012.

[44] J. B. Kenney, "Dedicated short-range communications (DSRC) standards in the United States," *Proceedings of the IEEE*, vol. 99, no. 7, pp. 1162–1182, 2011.

[45] E. Uhlemann, "Initial steps toward a cellular vehicle-to-everything standard [connected vehicles]," *IEEE Vehicular Technology Magazine*, vol. 12, no. 1, pp. 14–19, 2017.

[46] K. Thompson *et al.*, "Connected vehicle pilot deployment program: Driving towards deployment: Lessons learned from the design/build/test phase," United States. Department of Transportation. Intelligent Transportation ..., Tech. Rep., 2018.

[47] K. Abboud, H. A. Omar, and W. Zhuang, "Interworking of DSRC and cellular network technologies for V2X communications: A survey," *IEEE transactions on vehicular technology*, vol. 65, no. 12, pp. 9457–9470, 2016.

[48] IEEE-1609.0, "IEEE Guide for Wireless Access in Vehicular Environments (WAVE) - Architecture," *IEEE Std 1609.0-2013*, pp. 1–78, March 2014.

[49] IEEE-802.11-2010, "IEEE Standard for Information Technology–Telecommunications and information exchange between systems–Local and metropolitan area networks–Specific requirements–Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 6: Wireless Access in Vehicular Environments," *IEEE Std*, vol. 802, no. 11, 2010.

[50] IEEE-802.11-2012, "IEEE Std 802.11-2012 IEEE Standard for Information Technology–Telecommunications and information exchange between systems–Local and metropolitan area networks–Specific requirements–Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 6: Wireless Access in Vehicular Environments," *IEEE Std*, vol. 802, no. 11, 2012.

[51] "DSRC APPLICATION SUB-LAYER ARIB STDT88, ARIB STANDARD-Ver.1.0 ARIB STD-T88, Version 1.0 MAY 25, 2004," Available at http://www.arib.or.jp/english/html/overview/doc/5-STD-T88v1_0-E2.pdf.

[52] R. A. Uzcátegui, A. J. De Sucre, and G. Acosta-Marum, "WAVE: A tutorial," *IEEE Communications magazine*, vol. 47, no. 5, 2009.

[53] "Vehicle Safety Communications Project Task 3 Final Report, March 2016 ," Available at https://www.nhtsa.gov/DOT/NHTSA/NRD/Multimedia/PDFs/Crash%20Avoidance/2005/CAMP3scr.pdf.

[54] I. JPO, "Vehicle safety applications. US DOT IntelliDrive(sm) Project-ITS Joint Program office," Technical report, Tech. Rep., 2008.

[55] "Cooperative Intersection Collision Avoidance Systems (CICAS)," Available at http://www.dot.state.mn.us/guidestar/2006_2010/cicas.html.

[56] "SafeTrip-21 Initiative," Available http://www.dot.ca.gov/ctjournal/2009-3/InnovTrans.html.

[57] "RITA - Intelligent Transportation Systems - Vehicle-to-Vehicle (V2V) Communications for Safety Fact Sheet," Available at http://www.its.dot.gov/factsheets/v2v_factsheet.htm.

[58] "Research and Innovative Technology Administration (RITA)," Available ar https://www.rita.dot.gov/.

[59] "Presentation on "ITS initiatives in Japan", by MLIT : Ministry of Land, Infrastructure, Transport and Tourism," Available at http://www.mlit.go.jp/road/ITS/pdf/ITSinitiativesinJapan.pdf.

[60] H. Makino and H. Tsuji, "Electronic Toll Collection System of Japan," in *PIARC International Seminar on Intelligent Transport System (ITS) In Road Network Operations*, 2006.

[61] H. Tsuji, "ETC and Smartway in Japan," in *2nd Thailand ITS Seminar. Thailand ITS Conference*, 2007.

[62] "To Use ETC 2.0 Services - ETC portal site," Available at http://www.go-etc.jp/english/etc2/use.html.

[63] H. Watanabe, S. Kondo, and K. Hirano, "Introduction to Suzuki ASV technologies," in *Intelligent Vehicles Symposium, 1996., Proceedings of the 1996 IEEE*. IEEE, 1996, pp. 219–223.

[64] I. Paromtchik and C. Laugier, "The Advanced Safety Vehicle Programme," *Scientific Commons*, 2007.

[65] T. Aotani, S. Yamaoka, and T. Tajima, "Research development of driving safety support systems," in *Proceedings of the 41st SICE Annual Conference. SICE 2002.*, vol. 3, Aug 2002, pp. 1792–1797 vol.3.

[66] M. Sugimoto, "Driving safety support system: DSSS," in *Vehicle Electronics Conference, 1999.(IVEC'99) Proceedings of the IEEE International*. IEEE, 1999, pp. 480–484.

[67] "ITS-Safety 2010," Available at http://wiki.fot-net.eu/index.php/ITS-Safety_2010#Objectives.

[68] "ITS (Intelligent Transport System) Spot Services — International Transport Forum 2012 Summit," Available at http://www.mlit.go.jp/kokusai/itf/kokusai_itf_000006.html.

[69] "C-V2X trials in Japan ," Available at https://site.ieee.org/connected-vehicles/2018/12/13/leading-automotive-telecom-and-its-companies-successfully-carry-out-first-/cellular-v2x-trial-in-japan/.

[70] "Bosch-Daimler fully automated and driverless driving system," Available at https://www.daimler.com/innovation/case/autonomous/bosch-cooperation.html.

[71] "Intel-Mobileye 100-car autonomus vehicle (AV) fleet," Available at http://sites.ieee.org/connected-vehicles/2018/05/17/intel-and-mobileye-begin-testing-their-autonomous-fleet-in-jerusalem/.

[72] "Multi-party 5G trails for connected cars," Available at http://sites.ieee.org/connected-vehicles/2017/11/06/1675/.

[73] "AT&T, Ford, Nokia, Qualcomm C-V2X trails," Available at http://sites.ieee.org/connected-vehicles/2017/10/31/att-ford-nokia-qualcomm-launch-cellular-v2x-connected-car-technology-trials-u-s/.

[74] "LG Electronic partners with HERE Technologies on autonomus cars," Available at http://sites.ieee.org/connected-vehicles/2017/12/27/lg-electronics-technologies-partner-autonomous-cars/.

[75] "Telefónica-SEAT assisted driving use case with V2X," Available at http://sites.ieee.org/connected-vehicles/2018/07/24/telefonica-and-seat-present-the-first-use-case-of-assisted-driving-via-the-mobile/-network-in-a-real-setting-in-segovia/.

[76] "C-MOBILE Project," Available at https://c-mobile-project.eu/pilot-sites/.

[77] "Toyota Friend Project by Toyota," Available at https://adage.com/creativity/work/toyota-toyota-friend/23372.

[78] "BMW : Application for Automotive Projects," Available at http://www.bmw-carit.de/projects/applications-for-automotive.php.

[79] "Toyota-Grab Data Collaboration Initiative for Connected Car Services," Available at http://sites.ieee.org/connected-vehicles/2017/08/30/toyota-grab-launch-data-collaboration-initiative-connected-car-services/.

[80] "Programme for a European traffic system with highest efficiency and unprecedented safety — EUREKA," Available at http://www.eurekanetwork.org/project/id/45.

[81] M. Xie, L. Trassoudaine, J. Alizon, M. Thonnat, and J. Gallice, "Active and intelligent sensing of road obstacles: Application to the European Eureka-PROMETHEUS project," in *1993 (4th) International Conference on Computer Vision*, May 1993, pp. 616–623.

[82] "European Commission : CORDIS : Projects & Results Service : Home," Available at http://cordis.europa.eu/projects/home_en.html.

[83] R. Bossom *et al.*, "D31 European ITS Communication Architecture-Overall Framework-Proof of Concept Implementation, March 2009," *COMeSafety deliverable*.

[84] "Co-operative Systems for Intelligent Road Safety, presentation of COOPERs project, 026814 Funded under: FP6-IST," Available at http://cordis.europa.eu/project/rcn/79301_en.html.

[85] "CVIS Co-operative Vehicle-Infrastructure Systems, 027293 Funded under: FP6-IST," Available at http://cordis.europa.eu/project/rcn/79316_en.html.

[86] F. Bonnefoi, F. Bellotti, and T. Schendzielorz, "From User Needs to Applications: The Safespot Approach Based on Road Accident Data Analysis," in *Proceedings of the 6th European Congress and Exhibition on Intelligent Transport Systems and Services*, 2007.

[87] A. Festag, G. Noecker, M. Strassberger, A. Lübke, B. Bochow, M. Torrent-Moreno, S. Schnaufer, R. Eigner, C. Catrinescu, and J. Kunisch, "'NoW–Network on Wheels': Project objectives, technology and achievements," 2008.

[88] "AIDE: Adaptive integrated driver-vehicle interface, 507674 Funded under: FP6-IST," Available at http://cordis.europa.eu/project/rcn/71446_en.html.

[89] "APROSYS: Advanced Protection Systems (APROSYS), 506503 Funded under: FP6-SUSTDEV," Available at http://cordis.europa.eu/project/rcn/74297_en.html.

[90] "PRE-DRIVE, 224019 Funded under: FP7-ICT," Available at http://cordis.europa.eu/project/rcn/87604_en.html.

[91] "GeoNet : Geoaddressing and Georouting for vehicular communications, 216269 Funded under: FP7-ICT," Available at http://cordis.europa.eu/project/rcn/85551_en.html.

[92] M. Rondinone, J. Maneros, D. Krajzewicz, R. Bauza, P. Cataldi, F. Hrizi, J. Gozalvez, V. Kumar, M. Röckl, L. Lin *et al.*, "iTETRIS: a modular simulation platform for the large scale evaluation of cooperative ITS applications," *Simulation Modelling Practice and Theory*, vol. 34, pp. 99–125, 2013.

[93] "iTETRIS Platform," Available at http://www.ict-itetris.eu/itetris_platform.html.

[94] "ROSATTE:ROad Safety ATTributes exchange infrastructure in Europe, 213467 Funded under: FP7-ICT," Available at http://cordis.europa.eu/project/rcn/85524_en.html.

[95] "PRESERVE: Preparing Secure Vehicle-to-X Communication Systems,269994 Funded under: FP7-ICT," Available at http://cordis.europa.eu/project/rcn/97466_en.html.

[96] "PRECIOSA: Privacy Enabled Capability In co-Operative systems and Safety Applications, 224201 Funded under: FP7-ICT," Available at http://cordis.europa.eu/project/rcn/86606_en.html.

[97] "DRIVE C2X - Accelerate cooperative mobility," Available at http://www.drive-c2x.eu/project.

[98] "COLOMBO:Cooperative Self-Organizing System for low Carbon Mobility at low Penetration Rates," Available at http://www.colombo-fp7.eu/.

[99] "High precision positioning for cooperative ITS applications: HIGHTS," Available at https://cordis.europa.eu/project/rcn/193407/factsheet/en.

[100] "Cooperative ITS for Mobility in European Cities: CIMEC," Available at https://cordis.europa.eu/project/rcn/196891/factsheet/fr.

[101] "Cooperative ITS Deployment Coordination Support: CODECS," Available at https://cordis.europa.eu/project/rcn/194851/factsheet/fr.

[102] M. Fallgran, M. Dillinger, Z. Li, G. Vivier, T. Abbas, J. Alonso-Zarate, T. Mahmoodi, S. Alli, T. Svensson, and G. Fodor, "On Selected V2X Technology Components and Enablers from the 5GCAR Project," in *2018 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB)*. IEEE, 2018, pp. 1–5.

[103] A. Boualouache, S.-M. Senouci, and S. Moussaoui, "Privanet: An efficient pseudonym changing and management framework for vehicular ad-hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, 2019.

[104] D. Manivannan, S. S. Moni, and S. Zeadally, "Secure authentication and privacy-preserving techniques in vehicular ad-hoc networks (vanets)," *Vehicular Communications*, p. 100247, 2020.

[105] X. Liu, H. Huang, F. Xiao, and Z. Ma, "A blockchain-based trust management with conditional privacy-preserving announcement scheme for vanets," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4101–4112, 2019.

[106] A. Osseiran, J. F. Monserrat, and P. Marsch, *5G mobile and wireless communications technology*. Cambridge University Press, 2016.

[107] G. T. 23.402, "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Architecture enhancements for non-3GPP accesses (Release 10)," Tech. Rep., 2012.

[108] Dino Flore, 3GPP RAN Chairman , "Initial Cellular V2X standard completed," 2016, http://www.3gpp.org/news-events/3gpp-news/1798-v2x_r14.

[109] LG Electronics, Huawei, CATT, "Revised WI proposal: LTE-based V2X Services, RP-161894," 2016, ftp://ftp.3gpp.org/TSG_RAN/TSG_RAN/TSGR_73/Docs/ RP-161894.zip.

[110] "3GPP : RP151660, Further Planning on Next Generation Radio Access Technology," Available at http://www.3gpp.org/ftp/tsg_ran/TSG_RAN/TSGR_70/Docs/, 2016.

[111] 3GPP TS 22.186 v16.2.0, "Partnership Project; technical specification group services and system aspects; study on enhancement of 3GPP support for 5G V2X services (Release 16)," Tech. Rep., 2019.

[112] S. Chen and J. Zhao, "The requirements, challenges, and technologies for 5G of terrestrial mobile telecommunication," *IEEE Communications Magazine*, vol. 52, no. 5, pp. 36–43, 2014.

[113] T. Nakamura, A. Benjebbour, Y. Kishiyama, S. Suyama, and T. Imai, "5G radio access: Requirements, concept and experimental trials," *IEICE Transactions on Communications*, vol. 98, no. 8, pp. 1397–1406, 2015.

[114] V. Jungnickel, K. Manolakis, W. Zirwas, B. Panzner, V. Braun, M. Lossow, M. Sternad, R. Apelfrojd, and T. Svensson, "The role of small cells, coordinated multipoint, and massive MIMO in 5G," *IEEE Communications Magazine*, vol. 52, no. 5, pp. 44–51, 2014.

[115] C.-X. Wang, F. Haider, X. Gao, X.-H. You, Y. Yang, D. Yuan, H. Aggoune, H. Haas, S. Fletcher, and E. Hepsaydir, "Cellular architecture and key technologies for 5G wireless communication networks," *IEEE Communications Magazine*, vol. 52, no. 2, pp. 122–130, 2014.

[116] I. Parvez, A. Rahmati, I. Guvenc, A. I. Sarwat, and H. Dai, "A Survey on Low Latency Towards 5G: RAN, Core Network and Caching Solutions," *arXiv preprint arXiv:1708.02562*, 2017.

[117] T. S. Rappaport, S. Sun, R. Mayzus, H. Zhao, Y. Azar, K. Wang, G. N. Wong, J. K. Schulz, M. Samimi, and F. Gutierrez, "Millimeter wave mobile communications for 5G cellular: It will work!" *IEEE access*, vol. 1, pp. 335–349, 2013.

[118] S. M. Razavizadeh, M. Ahn, and I. Lee, "Three-dimensional beamforming: A new enabling technology for 5G wireless networks," *IEEE Signal Processing Magazine*, vol. 31, no. 6, pp. 94–101, 2014.

[119] R. G. Maunder, "The 5G channel code contenders," *AccelerComm White Paper*, pp. 1–13, 2016.

[120] L. Dai, B. Wang, Y. Yuan, S. Han, I. Chih-Lin, and Z. Wang, "Non-orthogonal multiple access for 5G: solutions, challenges, opportunities, and future research trends," *IEEE Communications Magazine*, vol. 53, no. 9, pp. 74–81, 2015.

[121] Z. Ding, Z. Yang, P. Fan, and H. V. Poor, "On the performance of non-orthogonal multiple access in 5G systems with randomly deployed users," *IEEE Signal Processing Letters*, vol. 21, no. 12, pp. 1501–1505, 2014.

[122] T. A. Levanen, J. Pirskanen, T. Koskela, J. Talvitie, and M. Valkama, "Radio interface evolution towards 5G and enhanced local area communications," *IEEE Access*, vol. 2, pp. 1005–1029, 2014.

[123] N. Bhushan, J. Li, D. Malladi, R. Gilmore, D. Brenner, A. Damnjanovic, R. Sukhavasi, C. Patel, and S. Geirhofer, "Network densification: the dominant theme for wireless evolution into 5G," *IEEE Communications Magazine*, vol. 52, no. 2, pp. 82–89, 2014.

[124] E. Hossain, M. Rasti, H. Tabassum, and A. Abdelnasser, "Evolution toward 5G multi-tier cellular wireless networks: An interference management perspective," *IEEE Wireless Communications*, vol. 21, no. 3, pp. 118–127, 2014.

[125] W. Nam, D. Bai, J. Lee, and I. Kang, "Advanced interference management for 5G cellular networks," *IEEE Communications Magazine*, vol. 52, no. 5, pp. 52–60, 2014.

[126] J. Vihriala, N. Ermolova, E. Lahetkangas, O. Tirkkonen, and K. Pajukoski, "On the waveforms for 5G mobile broadband communications," in *Vehicular Technology Conference (VTC Spring), 2015 IEEE 81st.* IEEE, 2015, pp. 1–5.

[127] A. A. Zaidi, R. Baldemair, H. Tullberg, H. Bjorkegren, L. Sundstrom, J. Medbo, C. Kilinc, and I. Da Silva, "Waveform and numerology to support 5g

services and requirements," *IEEE Communications Magazine*, vol. 54, no. 11, pp. 90–98, 2016.

[128] X. Foukas, G. Patounas, A. Elmokashfi, and M. K. Marina, "Network Slicing in 5G: Survey and Challenges," *IEEE Communications Magazine*, vol. 55, no. 5, pp. 94–100, 2017.

[129] H. Hawilo, A. Shami, M. Mirahmadi, and R. Asal, "NFV: state of the art, challenges, and implementation in next generation mobile networks (vEPC)," *IEEE Network*, vol. 28, no. 6, pp. 18–26, 2014.

[130] P. Demestichas, A. Georgakopoulos, D. Karvounas, K. Tsagkaris, V. Stavroulaki, J. Lu, C. Xiong, and J. Yao, "5G on the horizon: key challenges for the radio-access network," *IEEE Vehicular Technology Magazine*, vol. 8, no. 3, pp. 47–53, 2013.

[131] K. Zhang, Y. Mao, S. Leng, Q. Zhao, L. Li, X. Peng, L. Pan, S. Maharjan, and Y. Zhang, "Energy-efficient offloading for mobile edge computing in 5G heterogeneous networks," *IEEE Access*, vol. 4, pp. 5896–5907, 2016.

[132] V. Tikhvinskiy and G. Bochechka, "Prospects and QoS requirements in 5G networks," *Journal of Telecommunications and Information Technology*, no. 1, p. 23, 2015.

[133] E. Dahlman, G. Mildh, S. Parkvall, J. Peisa, J. Sachs, Y. Selén, and J. Sköld, "5G wireless access: requirements and realization," *IEEE Communications Magazine*, vol. 52, no. 12, pp. 42–47, 2014.

[134] M. Giordani, M. Mezzavilla, S. Rangan, and M. Zorzi, "Multi-Connectivity in 5G mmwave cellular networks," in *Ad Hoc Networking Workshop (Med-Hoc-Net), 2016 Mediterranean.* IEEE, 2016, pp. 1–7.

[135] O. Galinina, A. Pyattaev, S. Andreev, M. Dohler, and Y. Koucheryavy, "5G multi-RAT LTE-WiFi ultra-dense small cells: Performance dynamics, architecture, and trends," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 6, pp. 1224–1240, 2015.

[136] R. Wang, H. Hu, and X. Yang, "Potentials and challenges of C-RAN supporting multi-RATs toward 5G mobile networks," *IEEE Access*, vol. 2, pp. 1187–1195, 2014.

[137] A. De La Oliva, X. C. Pérez, A. Azcorra, A. Di Giglio, F. Cavaliere, D. Tiegelbekkers, J. Lessmann, T. Haustein, A. Mourad, and P. Iovanna, "Xhaul: toward an integrated fronthaul/backhaul architecture in 5G networks," *IEEE Wireless Communications*, vol. 22, no. 5, pp. 32–40, 2015.

[138] F. Granelli, A. A. Gebremariam, M. Usman, F. Cugini, V. Stamati, M. Alitska, and P. Chatzimisios, "Software defined and virtualized wireless access in future wireless networks: scenarios and standards," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 26–34, 2015.

[139] S. Mumtaz, K. M. S. Huq, and J. Rodriguez, "Direct mobile-to-mobile communication: Paradigm for 5G," *IEEE Wireless Communications*, vol. 21, no. 5, pp. 14–23, 2014.

[140] A. Osseiran, F. Boccardi, V. Braun, K. Kusume, P. Marsch, M. Maternia, O. Queseth, M. Schellmann, H. Schotten, H. Taoka *et al.*, "Scenarios for 5G mobile and wireless communications: the vision of the METIS project," *IEEE Communications Magazine*, vol. 52, no. 5, pp. 26–35, 2014.

[141] X. Ge, S. Tu, G. Mao, C.-X. Wang, and T. Han, "5G ultra-dense cellular networks," *IEEE Wireless Communications*, vol. 23, no. 1, pp. 72–79, 2016.

[142] IEEE-1609.2a, "IEEE Standard for Wireless Access in Vehicular Environments–Security Services for Applications and Management Messages - Amendment 1," *IEEE Std 1609.2a-2017 (Amendment to IEEE Std 1609.2-2016)*, pp. 1–123, Oct 2017.

[143] T. ETSI, "ETSI TS 102 941 v1. 1.1-intelligent transport systems (ITS); security; trust and privacy management, Standard, TC ITS, 2012."

[144] J. Kamel, M. R. Ansari, J. Petit, A. Kaiser, I. B. Jemaa, and P. Urien, "Simulation framework for misbehavior detection in vehicular networks," *IEEE Transactions on Vehicular Technology*, 2020.

[145] W. Whyte, A. Weimerskirch, V. Kumar, and T. Hehn, "A security credential management system for v2v communications," in *2013 IEEE Vehicular Networking Conference*. IEEE, 2013, pp. 1–8.

[146] K. Henry, "Misbehavior Detection in V2X Communications," in *Transportation Association of Canada and ITS Canada 2019 Joint Conference and Exhibition*, 2019.

[147] P. Xing, L. Yang, C. Q. Li, P. Demestichas, and A. Georgakopoulos, "Multi-rat network architecture," in *Wireless World Research Forum, White Paper, Version*, vol. 2, 2013.

[148] N. Haziza, M. Kassab, R. Knopp, J. Härri, F. Kaltenberger, P. Agostini, M. Berbineau, C. Gransart, J. Besnier, J. Ehrlich *et al.*, "Multi-technology vehicular cooperative system based on software defined radio (sdr)," in *International Workshop on Communication Technologies for Vehicles*. Springer, 2013, pp. 84–95.

[149] I. Ku, Y. Lu, M. Gerla, R. L. Gomes, F. Ongaro, and E. Cerqueira, "Towards software-defined vanet: Architecture and services," in *2014 13th annual*

Mediterranean ad hoc networking workshop (MED-HOC-NET). IEEE, 2014, pp. 103–110.

[150] F. A. Phiri and M. Murthy, "WLAN-GPRS tight coupling based interworking architecture with vertical handoff support," *Wireless Personal Communications*, vol. 40, no. 2, pp. 137–144, 2007.

[151] Y. Li, K.-W. Lee, J.-E. Kang, and Y.-Z. Cho, "A novel loose coupling interworking scheme between umts and wlan systems for multihomed mobile stations," in *Proceedings of the 5th ACM international workshop on Mobility management and wireless access*, 2007, pp. 155–158.

[152] C.-M. Huang and M.-S. Lin, "RG-SCTP: Using the relay gateway approach for applying SCTP in vehicular networks," in *The IEEE symposium on Computers and Communications*. IEEE, 2010, pp. 139–144.

[153] K. Katsaros and M. Dianati, "A cost-effective SCTP extension for hybrid vehicular networks," 2017.

[154] J. Mena, P. Bankole, and M. Gerla, "Multipath tcp on a vanet: A performance study," in *Proceedings of the 2017 ACM SIGMETRICS/International Conference on Measurement and Modeling of Computer Systems*. ACM, 2017, pp. 39–40.

[155] A. Ford, C. Raiciu, M. Handley, S. Barre, J. Iyengar *et al.*, "Architectural guidelines for multipath TCP development," *IETF, Informational RFC*, vol. 6182, pp. 2070–1721, 2011.

[156] J. Rodriguez, *Fundamentals of 5G mobile networks*. John Wiley & Sons, 2015.

[157] G. Gódor, Z. Jako, A. Knapp, and S. Imre, "A survey of handover management in LTE-based multi-tier femtocell networks: Requirements, challenges and solutions," *Computer Networks*, vol. 76, pp. 17–41, 2015.

[158] M. Mueck, V. Ivanov, S. Choi, J. Kim, C. Ahn, H. Yang, G. Baldini, and A. Piipponen, "Future of wireless communication: Radioapps and related security and radio computer framework," *IEEE Wireless Communications*, vol. 19, no. 4, pp. 9–16, 2012.

[159] I. . W. Group *et al.*, "Standard For Port-Based Network Access Control. IEEE Draft P802. 1x, March 2001," 2001.

[160] IEEE Std 802.11i, IEEE Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer Specifications, "Amendment 6: Medium Access Control Security Enhancements."

[161] IEEE Std 802.11r /D01.0, Draft Amendment to Standard for Information Technology – Telecommunications and Information Exchange Between Systems – LAN/MAN Specific Requirements Part 11, " Wireless Medium Access Control (MAC) and Physical Layer Specifications: Amendment 8: Fast BSS Transition."

[162] A. Mishra, M. Shin, and W. Arbaugh, "An Empirical Analysis of the IEEE 802.11 MAC layer handoff process," *ACM SIGCOMM Computer Communication Review*, vol. 33, no. 2, pp. 93–102, 2003.

[163] S. Shin, A. G. Forte, A. S. Rawat, and H. Schulzrinne, "Reducing MAC layer handoff latency in IEEE 802.11 wireless LANs," in *Proceedings of the second international workshop on Mobility management & wireless access protocols*. ACM, 2004, pp. 19–26.

[164] Y. J. Li, "An overview of the DSRC/WAVE technology," in *International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness*. Springer, 2010, pp. 544–558.

[165] S. Arslan and M. Saritas, "The effects of OFDM design parameters on the V2X communication performance: A survey," *Vehicular Communications*, vol. 7, pp. 1–6, 2017.

[166] A. Petrescu, N. Benamar, J. Haerri, C. Huitema, J. Lee, T. Ernst, and T. Li, "Transmission of IPv6 Packets over IEEE 802. 11 Networks in mode Outside the Context of a Basic Service Set (IPv6-over-80211ocb)," *Internet-Draft draft-ietf-ipwave-ipv6-over-80211ocb-04, Internet Engineering Task Force*, 2017.

[167] A. Ford, C. Raiciu, M. Handley, and O. Bonaventure, "TCP extensions for multipath operation with multiple addresses," Tech. Rep., 2013.

[168] P. Zhang, H. Wang, C. Hu, and C. Lin, "On denial of service attacks in software defined networks," *IEEE Network*, vol. 30, no. 6, pp. 28–33, 2016.

[169] O. TS-006, "Specification, OpenFlow Switch V1. 3.1," 2012.

[170] J. Gozálvez, M. Sepulcre, and R. Bauza, "IEEE 802.11p vehicle to infrastructure communications in urban environments," *IEEE Communications Magazine*, vol. 50, no. 5, 2012.

[171] M. Mouton, G. Castignani, R. Frank, and T. Engel, "Enabling vehicular mobility in city-wide ieee 802.11 networks through predictive handovers," *Vehicular Communications*, vol. 2, no. 2, pp. 59–69, 2015.

[172] P. Deshpande, A. Kashyap, C. Sung, and S. R. Das, "Predictive methods for improved vehicular WiFi access," in *Proceedings of the 7th international*

conference on Mobile systems, applications, and services. ACM, 2009, pp. 263–276.

[173] A. Balasubramanian, R. Mahajan, A. Venkataramani, B. N. Levine, and J. Zahorjan, "Interactive wifi connectivity for moving vehicles," *ACM SIGCOMM Computer Communication Review*, vol. 38, no. 4, pp. 427–438, 2008.

[174] T.-Y. Wu, M. S. Obaidat, and H.-L. Chan, "QualityScan scheme for load balancing efficiency in vehicular ad hoc networks (VANETs)," *Journal of Systems and Software*, vol. 104, pp. 60–68, 2015.

[175] S. F. Hasan, N. H. Siddique, and S. Chakraborty, "Developments and constraints in 802.11-based roadside-to-vehicle communications," *Wireless personal communications*, vol. 69, no. 4, pp. 1261–1287, 2013.

[176] Z. H. Mir and F. Filali, "LTE and IEEE 802.11p for vehicular networking: a performance evaluation," *EURASIP Journal on Wireless Communications and Networking*, vol. 2014, no. 1, p. 89, 2014.

[177] W. Chen, *Vehicular communications and networks: Architectures, protocols, operation and deployment*. Elsevier, 2015.

[178] A. Vinel, "3GPP LTE versus IEEE 802.11p/WAVE: Which technology is able to support cooperative vehicular safety applications?" *IEEE Wireless Communications Letters*, vol. 1, no. 2, pp. 125–128, 2012.

[179] K. C. Dey, A. Rayamajhi, M. Chowdhury, P. Bhavsar, and J. Martin, "Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication in a heterogeneous wireless network–Performance evaluation," *Transportation Research Part C: Emerging Technologies*, vol. 68, pp. 168–184, 2016.

[180] N. Williams, P. Abeysekera, N. Dyer, H. Vu, and G. Armitage, "Multipath TCP in Vehicular to Infrastructure Communications," *Grenville Armitage Centre for Advanced Internet Architectures. Technical Report A*, vol. 140828.

[181] J. Márquez-Barja, C. T. Calafate, J.-C. Cano, and P. Manzoni, "An overview of vertical handover techniques: Algorithms, protocols and tools," *Computer communications*, vol. 34, no. 8, pp. 985–997, 2011.

[182] E. Ndashimye, S. K. Ray, N. I. Sarkar, and J. A. Gutiérrez, "Vehicle-to-infrastructure communication over multi-tier heterogeneous networks: a survey," *Computer Networks*, vol. 112, pp. 144–166, 2017.

[183] Z. He, J. Cao, and X. Liu, "SDVN: enabling rapid network innovation for heterogeneous vehicular communication," *IEEE network*, vol. 30, no. 4, pp. 10–15, 2016.

[184] C.-M. Huang, M.-S. Chiang, D.-T. Dao, H.-M. Pai, S. Xu, and H. Zhou, "Vehicle-to-Infrastructure (V2I) offloading from cellular network to 802.11 p Wi-Fi network based on the Software-Defined Network (SDN) architecture," *Vehicular Communications*, vol. 9, pp. 288–300, 2017.

[185] J. Nobre, A. M. de Souza, D. Rosário, C. Both, L. A. Villas, E. Cerqueira, T. Braun, and M. Gerla, "Vehicular Software-Defined Networking and Fog Computing: Integration and Design Principles," *Ad hoc Networks*, 2018.

[186] J. Liu, J. Wan, B. Zeng, Q. Wang, H. Song, and M. Qiu, "A scalable and quick-response software defined vehicular network assisted by mobile edge computing," *IEEE Communications Magazine*, vol. 55, no. 7, pp. 94–100, 2017.

[187] S. H. Ahmed, S. H. Bouk, D. Kim, D. B. Rawat, and H. Song, "Named data networking for software defined vehicular networks," *IEEE Communications Magazine*, vol. 55, no. 8, pp. 60–66, 2017.

[188] C.-C. Lin, H.-H. Chin, and W.-B. Chen, "Balancing latency and cost in software-defined vehicular networks using genetic algorithm," *Journal of Network and Computer Applications*, vol. 116, pp. 35–41, 2018.

[189] M. Chen, D. O. Mau, Y. Zhang, T. Taleb, and V. C. Leung, "VENDNET: Vehicular named data network," *Vehicular Communications*, vol. 1, no. 4, pp. 208–213, 2014.

[190] X. Wang, C. Wang, J. Zhang, M. Zhou, and C. Jiang, "Improved rule installation for real-time query service in software-defined internet of vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 2, pp. 225–235, 2017.

[191] M. A. Khan, X. T. Dang, T. Dörsch, and S. Peters, "Mobility management approaches for SDN-enabled mobile networks," *Annals of Telecommunications*, pp. 1–13.

[192] R. d. R. Fontes and C. E. Rothenberg, "Mininet-WiFi: A platform for hybrid physical-virtual software-defined wireless networking research," in *Proceedings of the 2016 ACM SIGCOMM Conference*. ACM, 2016, pp. 607–608.

[193] M. Haklay and P. Weber, "Openstreetmap: User-generated street maps," *Ieee Pervas Comput*, vol. 7, no. 4, pp. 12–18, 2008.

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

[195] V. GUEANT, "iPerf - The ultimate speed test tool for TCP, UDP and SCTPTest the limits of your network Internet neutrality test." [Online]. Available: https://iperf.fr/

[196] "Synthetic Packet Pairs (SPP) - Tool for passive round trip time measurement." [Online]. Available: http://caia.swin.edu.au/tools/spp/

[197] Z. Doukha and S. Moussaoui, "An SDMA-Based Mechanism for Accurate and Efficient Neighborhood-Discovery Link-Layer Service." *IEEE Trans. Vehicular Technology*, vol. 65, no. 2, pp. 603–613, 2016.

[198] M. C. Weigle and S. Olariu, *Vehicular networks: from theory to practice*. Chapman and Hall/CRC, 2009.

[199] D. A. Rivas, J. M. Barceló-Ordinas, M. G. Zapata, and J. D. Morillo-Pozo, "Security on VANETs: Privacy, misbehaving nodes, false information and secure data aggregation," *Journal of Network and Computer Applications*, vol. 34, no. 6, pp. 1942–1955, 2011.

[200] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on VANET security challenges and possible cryptographic solutions," *Vehicular Communications*, vol. 1, no. 2, pp. 53–66, 2014.

[201] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym Schemes in Vehicular Networks: A Survey," *IEEE Communications Surveys Tutorials*, vol. 17, no. 1, pp. 228–255, Firstquarter 2015.

[202] D. Eckhoff and C. Sommer, "Readjusting the privacy goals in Vehicular Ad-Hoc Networks: A safety-preserving solution using non-overlapping time-slotted pseudonym pools," *Computer Communications*, vol. 122, pp. 118 – 128, 2018.

[203] F. Qu, Z. Wu, F.-Y. Wang, and W. Cho, "A security and privacy review of VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 6, pp. 2985–2996, 2015.

[204] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "On the performance of secure vehicular communication systems," *IEEE transactions on dependable and secure computing*, vol. 8, no. 6, pp. 898–912, 2010.

[205] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: A secure and privacy-preserving protocol for vehicular communications," *IEEE Transactions on vehicular technology*, vol. 56, no. 6, pp. 3442–3456, 2007.

[206] J. Guo, J. P. Baugh, and S. Wang, "A group signature based secure and privacy-preserving vehicular communication framework," in *2007 Mobile Networking for Vehicular Environments*. IEEE, 2007, pp. 103–108.

[207] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of computer security*, vol. 15, no. 1, pp. 39–68, 2007.

[208] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen, "Pseudonym changing at social spots: An effective strategy for location privacy in vanets," *IEEE transactions on vehicular technology*, vol. 61, no. 1, pp. 86–96, 2011.

[209] D. Liao, H. Li, G. Sun, M. Zhang, and V. Chang, "Location and trajectory privacy preservation in 5G-Enabled vehicle social network services," *Journal of Network and Computer Applications*, vol. 110, pp. 108–118, 2018.

[210] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in *IEEE INFOCOM 2008-The 27th Conference on Computer Communications*. IEEE, 2008, pp. 1229–1237.

[211] M. Khodaei, A. Messing, and P. Papadimitratos, "Rhythm: A randomized hybrid scheme to hide in the mobile crowd," in *2017 IEEE Vehicular Networking Conference (VNC)*. IEEE, 2017, pp. 155–158.

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

[213] K. Emara, W. Woerndl, and J. Schlichter, "Context-based pseudonym changing scheme for vehicular adhoc networks," *arXiv preprint arXiv:1607.07656*, 2016.

[214] J. Freudiger, M. Raya, M. Félegyházi, P. Papadimitratos, and J.-P. Hubaux, "Mix-zones for location privacy in vehicular networks," in *ACM Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS)*, no. CONF, 2007.

[215] S. Chang, C. Li, H. Zhu, T. Lu, and Q. Li, "Revealing privacy vulnerabilities of anonymous trajectories," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 12, pp. 12 061–12 071, 2018.

[216] Q. Mei, H. Xiong, J. Chen, M. Yang, S. Kumari, and M. K. Khan, "Efficient certificateless aggregate signature with conditional privacy preservation in iov," *IEEE Systems Journal*, 2020.

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

[218] M. Khodaei and P. Papadimitratos, "The key to intelligent transportation: Identity and credential management in vehicular communication systems," *IEEE Vehicular Technology Magazine*, vol. 10, no. 4, pp. 63–69, 2015.

[219] P. Papadimitratos, L. Buttyan, J.-P. Hubaux, F. Kargl, A. Kung, and M. Raya, "Architecture for secure and private vehicular communications," in *7th International Conference on ITS Telecommunications*. IEEE, 2007, pp. 1–6.

[220] P. P. Papadimitratos, G. Mezzour, and J.-P. Hubaux, "Certificate revocation list distribution in vehicular communication systems," in *Proceedings of the fifth ACM international workshop on VehiculAr Inter-NETworking*. ACM, 2008, pp. 86–87.

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

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

[223] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki, "Caravan: Providing location privacy for vanet," Washington Univ Seattle Dept of Electrical Engineering, Tech. Rep., 2005.

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

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

[226] K. Emara, W. Woerndl, and J. Schlichter, "CAPS: Context-aware privacy scheme for VANET safety applications," in *Proceedings of the 8th ACM conference on security & privacy in wireless and mobile networks*. ACM, 2015, p. 21.

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

[228] C. Mandy and I. Mahgoub, "Implementation of the wave 1609.2 security services standard and encountered issues and challenges," in *2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*. IEEE, 2018, pp. 13–18.

[229] S. Chang, Y. Qi, H. Zhu, J. Zhao, and X. Shen, "Footprint: detecting Sybil attacks in urban vehicular networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 6, pp. 1103–1114, 2011.

[230] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "VANet security challenges and solutions: A survey," *Vehicular Communications*, vol. 7, pp. 7–20, 2017.

[231] D. Eckhoff, R. German, C. Sommer, F. Dressler, and T. Gansen, "SlotSwap: strong and affordable location privacy in intelligent transportation systems," *IEEE Communications Magazine*, vol. 49, no. 11, 2011.

[232] C. Sommer, R. German, and F. Dressler, "Bidirectionally coupled network and road traffic simulation for improved ivc analysis," *IEEE Transactions on Mobile Computing*, vol. 10, no. 1, pp. 3–15, 2011.

[233] C. E. Shannon, "A mathematical theory of communication," *Bell system technical journal*, vol. 27, no. 3, pp. 379–423, 1948.

[234] D. Chaum, "The dining cryptographers problem: Unconditional sender and recipient untraceability," *Journal of cryptology*, vol. 1, no. 1, pp. 65–75, 1988.

[235] A. M. Mathai, *An introduction to geometrical probability: distributional aspects with applications*. CRC Press, 1999, vol. 1.

[236] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[237] J. Huang, L. Kong, G. Chen, M.-Y. Wu, X. Liu, and P. Zeng, "Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3680–3689, 2019.

[238] J. Huang, L. Kong, H.-N. Dai, W. Ding, L. Cheng, G. Chen, X. Jin, and P. Zeng, "Blockchain based mobile crowd sensing in industrial systems," *IEEE Transactions on Industrial Informatics*, 2020.

[239] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "Blockchain: A distributed solution to automotive security and privacy," *IEEE Communications Magazine*, vol. 55, no. 12, pp. 119–125, 2017.

[240] N. Szabo, "Formalizing and securing relationships on public networks," *First Monday*, vol. 2, no. 9, 1997.

[241] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum project yellow paper*, vol. 151, pp. 1–32, 2014.

[242] C. Dannen, *Introducing Ethereum and Solidity*. Springer, 2017.

[243] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," *International journal of information security*, vol. 1, no. 1, pp. 36–63, 2001.

[244] S. A. Soleymani, A. H. Abdullah, W. H. Hassan, M. H. Anisi, S. Goudarzi, M. A. R. Baee, and S. Mandala, "Trust management in vehicular ad hoc network: a systematic review," *EURASIP Journal on Wireless Communications and Networking*, vol. 2015, no. 1, p. 146, 2015.

[245] F. Ahmad, J. Hall, A. Adnane, and V. N. Franqueira, "Faith in vehicles: A set of evaluation criteria for trust management in vehicular ad-hoc network," in *IEEE International Conference on iThings, GreenCom, CPSCom, SmartData*. IEEE, 2017, pp. 44–52.

[246] M. Raya, P. Papadimitratos, V. D. Gligor, and J.-P. Hubaux, "On data-centric trust establishment in ephemeral ad hoc networks," in *INFOCOM: The 27th Conference on Computer Communications*. IEEE, 2008, pp. 1238–1246.

[247] N.-W. Lo and H.-C. Tsai, "A reputation system for traffic safety event on vehicular ad hoc networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, p. 9, 2009.

[248] A. Wu, J. Ma, and S. Zhang, "RATE: a RSU-aided scheme for data-centric trust establishment in VANETs," in *7th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM)*. IEEE, 2011, pp. 1–6.

[249] S. Gurung, D. Lin, A. Squicciarini, and E. Bertino, "Information-oriented trustworthiness evaluation in vehicular ad-hoc networks," in *International Conference on Network and System Security*. Springer, 2013, pp. 94–108.

[250] Z. Huang, S. Ruj, M. A. Cavenaghi, M. Stojmenovic, and A. Nayak, "A social network approach to trust management in VANETs," *Peer-to-Peer Networking and Applications*, vol. 7, no. 3, pp. 229–242, 2014.

[251] U. F. Minhas, J. Zhang, T. Tran, and R. Cohen, "A multifaceted approach to modeling agent trust for effective communication in the application of mobile ad hoc vehicular networks," *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 41, no. 3, pp. 407–420, 2011.

[252] F. G. Mármol and G. M. Pérez, "TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks," *Journal of Network and Computer Applications*, vol. 35, no. 3, pp. 934–941, 2012.

[253] U. Khan, S. Agrawal, and S. Silakari, "Detection of malicious nodes (dmn) in vehicular ad-hoc networks," *Procedia computer science*, vol. 46, pp. 965–972, 2015.

[254] X. Yao, X. Zhang, H. Ning, and P. Li, "Using trust model to ensure reliable data acquisition in VANETs," *Ad Hoc Networks*, vol. 55, pp. 107–118, 2017.

[255] Y.-M. Chen and Y.-C. Wei, "A beacon-based trust management system for enhancing user centric location privacy in VANETs," *Journal of Communications and Networks*, vol. 15, no. 2, pp. 153–163, 2013.

[256] H. Sedjelmaci and S. M. Senouci, "An accurate and efficient collaborative intrusion detection framework to secure vehicular networks," *Computers & Electrical Engineering*, vol. 43, pp. 33–47, 2015.

[257] W. Li and H. Song, "ART: An attack-resistant trust management scheme for securing vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 4, pp. 960–969, 2016.

[258] M. E. Mahmoud and X. Shen, "An integrated stimulation and punishment mechanism for thwarting packet dropping attack in multihop wireless networks," *IEEE Transactions on Vehicular Technology*, vol. 60, no. 8, pp. 3947–3962, 2011.

[259] N. Bißmeyer, J. Njeukam, J. Petit, and K. M. Bayarou, "Central misbehavior evaluation for vanets based on mobility data plausibility," in *Proceedings of the ninth ACM international workshop on Vehicular inter-networking, systems, and applications*. ACM, 2012, pp. 73–82.

[260] Q. Li, A. Malip, K. M. Martin, S.-L. Ng, and J. Zhang, "A reputation-based announcement scheme for VANETs," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 9, pp. 4095–4108, 2012.

[261] X. Li, J. Liu, X. Li, and W. Sun, "RGTE: A reputation-based global trust establishment in VANETs," in *Intelligent Networking and Collaborative Systems (INCoS), 2013 5th International Conference on*. IEEE, 2013, pp. 210–214.

[262] C. Lai, K. Zhang, N. Cheng, H. Li, and X. Shen, "SIRC: A secure incentive scheme for reliable cooperative downloading in highway VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 6, pp. 1559–1574, 2017.

[263] J. Oluoch, "A distributed reputation scheme for situation awareness in Vehicular Ad Hoc Networks (VANETs)," in *International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA)*. IEEE, 2016, pp. 63–67.

[264] X. Huang, R. Yu, J. Kang, and Y. Zhang, "Distributed reputation management for secure and efficient vehicular edge computing and networks," *IEEE Access*, vol. 5, pp. 25 408–25 420, 2017.

[265] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. Leung, "Blockchain-based Decentralized Trust Management in Vehicular Networks," *IEEE Internet of Things Journal*, 2018.

[266] Z. Lu, W. Liu, Q. Wang, G. Qu, and Z. Liu, "A Privacy-preserving Trust Model based on Blockchain for VANETs," *IEEE Access*, 2018.

[267] M. Singh and S. Kim, "Intelligent vehicle-trust point: Reward based intelligent vehicle communication using blockchain," *arXiv preprint arXiv:1707.07442*, 2017.

[268] U. Javaid, M. N. Aman, and B. Sikdar, "DrivMan: Driving trust management and data sharing in VANETS with blockchain and smart contracts," in *2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring)*. IEEE, 2019, pp. 1–5.

[269] S. Pongnumkul, C. Siripanpornchana, and S. Thajchayapong, "Performance analysis of private blockchain platforms in varying workloads," in *Computer Communication and Networks (ICCCN), 2017 26th International Conference on*. IEEE, 2017, pp. 1–6.

Publications Related to Thesis

Published/Accepted

Book Chapters

1. **Pranav Kumar Singh**, Roshan Singh, Sunit Kumar Nandi, Kayhan Zrar Ghafoor, and Sukumar Nandi. "Seamless V2I Communication in HetNet: State-of-the-art and Future Research Directions." In Connected Vehicles in the Internet of Things, pp. 37-83, Springer, Cham, 2020.

2. **Pranav Kumar Singh**, Roshan Singh, Sunit Kumar Nandi, and Sukumar Nandi. "Integrating Blockchain With CACC For Trust and Platoon Management." Cryptocurrencies and Blockchain Technology Applications, pp. 77-97, Wiley Online Library, 2020.

Journals

1. **Pranav Kumar Singh**, Sunit Kumar Nandi, Sukumar Nandi, "A Tutorial Survey On Vehicular Communication State of the Art, and Future Research Directions", Vehicular Communications, Volume 18, 2019, pp. 100164.

2. **Pranav Kumar Singh**, Sahil Sharma, Sunit Kumar Nandi, Sukumar Nandi, "Multipath TCP for V2I communication in SDN controlled small cell

deployment of smart city", Vehicular Communications, Volume 15, 2019, pp. 1-15.

3. **Pranav Kumar Singh**, Shivram N Gowtham, Tamilselvan S, Sukumar Nandi, "CPESP: Cooperative Pseudonym Exchange and Scheme Permutation to preserve location privacy in VANETs", Vehicular Communications, Volume 20, 2019, pp. 100183.

4. **Pranav Kumar Singh**, Anup Agarwal, Gaurav Nakum, Danda B. Rawat, and Sukumar Nandi. "MPFSLP: Masqueraded Probabilistic Flooding for Source-Location Privacy in VANETs." IEEE Transactions on Vehicular Technology Volume 69, no. 10 ,2020, pp. 11383-11393.

5. **Pranav Kumar Singh**, Roshan. Singh, S. K. Nandi, K. Z. Ghafoor, D. B. Rawat and Sukumar Nandi, "Blockchain-Based Adaptive Trust Management in Internet of Vehicles Using Smart Contract," in IEEE Transactions on Intelligent Transportation Systems, doi: 10.1109/TITS.2020.3004041.

Conference Proceedings

1. **Pranav Kumar Singh**, Chourasiya, D., Singh, A., Nandi, S. K., & Sukumar Nandi, "CCAPS: Cooperative Context Aware Privacy Scheme for VANETs", In 2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall), September, 2019, September, pp. 1-5.

2. **Pranav Kumar Singh**, Dash, M. K., Mittal, P., Nandi, S. K., & Sukumar Nandi, "Misbehavior detection in C-ITS using Deep Learning Approach", In International Conference on Intelligent Systems Design and Applications, September, 2019, pp. 641-652. Springer, Cham.

3. **Pranav Kumar Singh**, Jha, S. K., Nandi, S. K., & Sukumar Nandi, "ML-Based Approach to Detect DDoS Attack in V2I Communication Under SDN Architecture", In TENCON IEEE Region 10 Conference, October, 2018, pp. 0144-0149.

4. **Pranav Kumar Singh**, Tabjul, G. S., Imran, M., Nandi, S. K., & Sukumar Nandi, "Impact of Security Attacks on Cooperative Driving Use Case: CACC Platooning", In TENCON IEEE Region 10 Conference, October, 2018, pp. 0138-0143.

5. **Pranav Kumar Singh**, Chattopadhyay, S., Bhale, P., & Sukumar Nandi, "Fast and secure handoffs for V2I communication in smart city Wi-Fi Deployment", In International Conference on Distributed Computing and Internet Technology, January, 2018, pp. 189-204. Springer, Cham.

6. **Pranav Kumar Singh**, Sharma, S., Nandi, S. K., Singh, R., & Sukumar Nandi, "Leader Election in Cooperative Adaptive Cruise Control Based Platooning", In Proceedings of the 1st International Workshop on Communication and Computing in Connected Vehicles and Platooning, October, 2018, October, pp. 8-14. ACM Mobicom.