The Key to Intelligent Transportation Systems: Identity and Credential Management for Secure and Privacy-Preserving Vehicular Communication Systems

MOHAMMAD KHODAEI

Doctoral Thesis
Stockholm, Sweden 2020

KTH Royal Institute of Technology
School of Electrical Engineering and Computer Science
Division of Communication Systems
Networked Systems Security Group
SE-164 40 Stockholm
SWEDEN

TRITA-EECS-AVL-2020:32
ISBN 978-91-7873-564-8

Akademisk avhandling som med tillstånd av Kungliga Tekniska högskolan framlägges till offentlig granskning för avläggande av doktorsexamen måndag den 15 juni 2020 klockan 14.00 i Electrum, Kungliga Tekniska högskolan, Kistagången 16, Kista.

Tryck: Universitetsservice US AB

Abstract

Vehicular Communication (VC) systems can greatly enhance road safety and transportation efficiency and enable a variety of applications providing traffic efficiency, environmental hazards, road conditions and infotainment. Vehicles are equipped with sensors and radars to sense their surroundings and external environment, as well as with an internal Controller Area Network (CAN) bus. Hence, vehicles are becoming part of a large-scale network, the so-called *Internet of Vehicles (IoV)*. Deploying such a large-scale VC system cannot materialize unless the VC systems are secure and do not expose their users' privacy. On the one hand, vehicles could be compromised or their sensors become faulty, thus disseminating erroneous information across the network. Therefore, participating vehicles should be held *accountable* for their actions and credentials (their Long Term Certificates (LTCs) and their pseudonyms) can be efficiently revoked and disseminated in a timely manner throughout a large-scale (multi-domain) VC system. On the other hand, user privacy is at stake: according to standards, vehicles should disseminate spatio-temporal information frequently, e.g., location and velocity. Due to the openness of the wireless communication, an observer can eavesdrop the vehicular communication to infer users' sensitive information, and possibly profile users based on different attributes, e.g., trace their commutes and identify home/work locations. The objective is to secure the communication, i.e., prevent malicious or compromised entities from affecting the system operation, and ensure user privacy, i.e., keep users anonymous to any external observer but also for security infrastructure entities and service providers. This is not very straightforward because accountability and privacy, at the same time, appear contradictory.

In this thesis, we first focus on the identity and credential management infrastructure for VC systems, taking security, privacy, and efficiency into account. We begin with a detailed investigation and critical survey of the standardization and harmonization efforts, along with industrial projects and proposals. We point out the remaining challenges to be addressed in order to build a central building block of secure and privacy-preserving VC systems, a Vehicular Public-Key Infrastructure (VPKI). Towards that, we provide a secure and privacy-preserving VPKI design that improves upon existing proposals in terms of security and privacy protection and efficiency. More precisely, our scheme facilitates multi-domain operations in VC systems and enhances user privacy, notably preventing linking of pseudonyms based on timing information and offering increased protection in the presence of *honest-but-curious* VPKI entities. We further extensively evaluate the performance, i.e., scalability, efficiency, and robustness, of the full-blown implementation of our VPKI for a large-scale VC deployment. We provide tangible evidence that it is possible to support a large area of vehicles by investing in modest computing resources for the VPKI entities. Our results confirm the efficiency, scalability and robustness of our VPKI.

As a second main contribution of this thesis, we focus on the distribution of Certificate Revocation Lists (CRLs) in VC systems. The main challenges here lie exactly in (i) crafting an efficient and timely distribution of CRLs for

numerous anonymous credentials, *pseudonyms*, (ii) maintaining strong privacy for vehicles prior to revocation events, even with *honest-but-curious* system entities, (iii) and catering to computation and communication constraints of on-board units with intermittent connectivity to the infrastructure. Relying on peers to distribute the CRLs is a double-edged sword: *abusive peers* could ''pollute'' the process, thus degrading the timely CRLs distribution. We propose a *vehicle-centric* solution that addresses all these challenges and thus closes a gap in the literature. Our scheme radically reduces CRL distribution overhead: each vehicle receives CRLs corresponding only to its region of operation and its actual trip duration. Moreover, a ''fingerprint'' of CRL 'pieces' is attached to a subset of (verifiable) pseudonyms for fast CRL 'piece' validation (while mitigating resource depletion attacks abusing the CRL distribution). Our experimental evaluation shows that our scheme is efficient, scalable, dependable, and practical: with no more than 25 KB/s of traffic load, the latest CRL can be delivered to 95% of the vehicles in a region (15×15 KM) within 15s, i.e., more than 40 times faster than the state-of-the-art. Overall, our scheme is a comprehensive solution that complements standards and can catalyze the deployment of secure and privacy-protecting VC systems.

As the third main contribution of the thesis, we focus on enhancing location privacy protection: vehicular communications disclose rich information about the vehicles and their whereabouts. Pseudonymous authentication secures communication while enhancing user privacy. To enhance location privacy, cryptographic mix-zones were proposed to facilitate vehicles covertly transition to new ephemeral credentials. The resilience to (*syntactic* and *semantic*) pseudonym linking (attacks) highly depends on the geometry of the mix-zones, mobility patterns, vehicle density, and arrival rates. Our experimental results show that an eavesdropper could successfully link ≈73% of pseudonyms (during non-rush hours) and ≈62% of pseudonyms (during rush hours) after vehicles change their pseudonyms in a mix-zone. To mitigate such inference attacks, we present a novel *cooperative mix-zone* scheme that enhances user privacy regardless of the vehicle mobility patterns, vehicle density, and arrival rate to the mix-zone. A subset of vehicles, termed *relaying vehicles*, are selected to be responsible for emulating non-existing vehicles. Such vehicles cooperatively disseminate decoy traffic without affecting safety-critical operations: with 50% of vehicles as relaying vehicles, the probability of linking pseudonyms (for the entire interval) drops from ≈68% to ≈18%. On average, this imposes 28 ms extra computation overhead, per second, on the Roadside Units (RSUs) and 4.67 ms extra computation overhead, per second, on the (relaying) vehicle side; it also introduces 1.46 KB/sec extra communication overhead by (relaying) vehicles and 45 KB/sec by RSUs for the dissemination of decoy traffic. Thus, user privacy is enhanced at the cost of low computation and communication overhead.

Keywords: Security, Privacy, Vehicular PKI, VPKI, Identity and Credential Management; Vehicular Communications, VANETs; Availability, Scalability, Resilient, Efficiency, Micro-service, Container Orchestration, Cloud; Certificate Revocation List; Location Privacy, Mix-zones, Pseudonymity, Anonymity, Untraceability, Pseudonym Transition, Pseudonym Unlinkability.

Sammanfattning

Fordonskommunikationssystem (FKS) kan förbättra transportsäkerhet och effektivitet genom att möjliggöra många applikationer, till exempel inom trafikflöde och risker i omgivning. Fordonen utrustas med sensorer och radar och blir därmed en del av ett storskaligt nätverk, så kallade Fordonens internet. När system som FKS impementeras måste användarens säkerhet och integritet säkerställas. Å ena sidan kan fordons sensorer bli felaktiga, vilket kan leda till att falsk information sprids i nätverket. Å andra sidan kan användarens integritet sättas i fara eftersom fordonen enligt standarder måste dela information, t.ex. position, fart, och riktning. Eftersom trådlös kommunikation används så kan betraktare avlyssna fordons kommunikation, vilket kan leda till att viktig information avslöjas. På det visat kan användarna profileras baserat på olika attribut, t.ex. individer som pendlar kan spåras och det gör så att deras hem och arbetsplats kan lokaliseras. För att implementera FKS är det avgörande att säkra kommunikationen och garantera användarnas integritet, dvs. att användarna förblir anonyma.

Denna doktorsavhandling fokuserar på infrastruktur för förvaltning av identitet- och behörighetsuppgifter och tar hänsyn till säkerhet, integritet, och effektivitet. Utmaningar identifieras för att skapa den viktigaste delen av säkra och integritetsbevarande FKS, så kallade Vehicular Public-Key Infrastructure (VPKI). Vårt system underlättar en säker och integritetsbevarande FKS, och utgör en förbättring över befintliga förslag i säkerhet, skydd av integritet samt effektivitet. Vi utvärderar vårt systems prestanda på ett omfattande sätt. Vårt resultat bekräftar effektiviteten, skalbarheten och robustheten av vårt system.

Nyckelord: Säkerhet, personlig integritet, identitet- och behörighetsuppgifter, tillgänglighet, skalbarhet, motståndskraftig, effektivitet, moln, pseudonymitet, anonymitet, ospårbarhet.

Acknowledgements

First and foremost, I would like to express my sincere gratitude to my advisor, *Prof. Panos Papadimitratos*, for his supervision, support, and excellent guidance. His advice and technical criticism helped me understand the problem in depth. Thank you for giving me the opportunity to work with you and be a member of your team, in the stimulating research environment of the Networked Systems Security (NSS) group.

I am thankful to all of my friends and collaborators: my especial regards go to my friend, *Hamid Noroozi*, for all the fruitful discussion we had. I would like to thank my friends, *Kewei Zhang* and *Hongyu Jin*, for all the pleasant times we had throughout the PhD journey. Also, I would like to thank *Andreas Messing* for all of his time and efforts. I would like to thank *Ida Pinho* and *Jacob Wahlgren* for proofreading the Swedish abstract. I would also like to thank the former and the current members of NSS for all the interesting discussions and useful interactions: *Syed Muhammad Zubair*, *Mahtab Mirmohseni*, *Somayeh Salimi*, *Moritz Wiese*, *Thanassis Giannetsos*, *Stylianos Gisdakis*, *Marco Spanghero*, and *Cihan Eryonucu*.

I would like also to thank my friend, *Hossein Shokri*, for all interesting discussion we had at division of Network and Systems Engineering. Also, I would like to thank all my friends, administrators and faculty at division of Network and Systems Engineering and division of Communication Systems for all the useful interactions, help, and friendly environment. I feel happy to be a member of such academic environments. I also would like to thank my friends, *Behdad*, *Hamed*, *Alireza*, *Kaveh*, and *Franzi* for all the good times we had and their supports.

To my wife and family, who helped me through all the hard times: To my beloved wife, *Nazila*, I dedicate my heartfelt appreciation for all of your support, love, motivation, and patience during my study. Thank you very much for all the happiness you brought to my life. I would like to express my gratitude to my lovely parents, *Reza* and *Zohreh*, and my sister, *Hoori*, for all of their support throughout this long journey of my PhD.

Mohammad Khodaei
Stockholm, June 2020

Bekräftelse

Jag vill tacka för stödet från min handledare, *Prof. Panos Papadimitratos*, som har hjälpt mig med min avhandling. Han vägledde mig under hela arbetet. Jag är uppriktigt tacksam för alla intressanta diskussioner vi har haft. Tack så mycket för möjligheten att ha fått studera i denna grupp.

Dessutom skulle jag vilja säga tack till mina vänner och kollegor: *Hamid Noroozi*, *Kewei Zhang*, *Hongyu Jin*, *Hossein Shokri*, *Andreas Messing*, *Syed Muhammad Zubair*, *Mahtab Mirmohseni*, *Somayeh Salimi*, *Moritz Wiese*, *Thanassis Giannetsos*, *Stylianos Gisdakis*, *Marco Spanghero*, och *Cihan Eryonucu* för alla intressanta diskussioner som vi har haft. Jag vill tacka *Ida Pinho* och *Jacob Wahlgren* för korrekturläsning av den svenska sammanfattningen. Jag vill även tacka alla medlemmar i avdelningen för nätverk och systemteknik och avdelningen för kommunikationssystem. Tack så mycket för alla trevliga interaktioner vi har haft. Jag vill även tacka mina vänner, *Behdad*, *Hamed*, *Alireza*, *Kaveh*, och *Franzi* för alla de goda tider vi hade och deras stöd.

Till sist skulle jag vilja tacka min älskade fru, *Nazila*, som har uppmuntrat och motiverat mig att fortsätta min utbildning. Dessutom skulle jag vilja säga tack till mina föräldrar, *Reza* och *Zohreh*, och särskilt min syster, *Hoori*, från djupet av mitt hjärta vill jag tillägna dem min kärleksfulla uppskattning. De har alltid varit med mig i alla situationer, och de har stöttat mig i varje aspekt.

Mohammad Khodaei
Stockholm, juni 2020

Develop a passion for learning. If you do, you will never cease to grow.

Anthony J. D'Angelo

Contents

List of Figures

List of Tables

List of Algorithms

Acronyms

AAA Authentication, Authorization and Accounting.

AES-CCM Advanced Encryption Standard in Counter Mode with a Cipher Block Chaining Message Authentication Code.

BF Bloom Filter.

BSM Basic Safety Message.

C2C Car-to-Car.

C2C-CC Car2Car Communication Consortium.

CA Certification Authority.

CAM Cooperative Awareness Message.

CAMP VSC3 Crash Avoidance Metrics Partnership Vehicle Safety Consortium.

CAN Controller Area Network.

CDF Cumulative Distribution Function.

CF Cuckoo Filter.

CMIX Cryptographic Mix-Zone.

CP Chaff Pseudonym.

CRL Certificate Revocation List.

CSR Certificate Signing Request.

DDoS Distributed DoS.

DENM Decentralized Environmental Notification Message.

DL/ECIES Discrete Logarithm and Elliptic Curve Integrated Encryption Scheme.

DoS Denial of Service.

DoT Department of Transportation.

DSRC Dedicated Short Range Communication.

DSS Digital Signature Standard.

DTLS Datagram Transport Layer Security.

ECA Enrollment Certification Authority.

ECC Elliptic Curve Cryptography.

ECDSA Elliptic Curve Digital Signature Algorithm.

ECIES Elliptic Curve Integrated Encryption Scheme.

ECU Electronic Control Unit.

ETSI European Telecommunications Standards Institute.

EV Electric Vehicle.

F-LTCA Foreign-Long Term CA.

FOT Field Operational Testing.

GCP Google Cloud Platform.

GKE Google Kubernetes Engine.

GM Group Manager.

GNSS Global Navigation Satellite System.

GPA Global Passive Adversary.

GPS Global Positioning System.

GS Group Signatures.

GS-VLR Group Signatures with Verifier Local Revocation.

H-LTCA Home-Long Term CA.

HCA Higher-level Certification Authority.

HPA Horizontal Pod Autoscaler.

HSM Hardware Security Module.

IEEE Institute of Electrical and Electronics Engineers.

IoT Internet of Things.

IoV Internet of Vehicles.

ITS Intelligent Transport System.

LBS Location Based Service.

LDAP Lightweight Directory Access Protocol.

LTC Long Term Certificate.

LTCA Long Term CA.

LTE Long Term Evolution.

LuST Luxembourg SUMO Traffic.

MAC Media Access Control.

MAC Message Authentication Code.

NIC Network Interface Card.

OBU On-Board Unit.

OCSP Online Certificate Status Protocol.

OEM Original Equipment Manufacturer.

PCA Pseudonym CA.

PKC Public Key Cryptography.

PKCS Public Key Cryptosystem.

PKI Public-Key Infrastructure.

PRESERVE Preparing Secure Vehicle-to-X Communication Systems.

PS Participatory Sensing.

RA Resolution Authority.

RCA Root CA.

RF Radio Frequency.

RPC Remote Procedure Call.

RSSI Received Signal Strength Indication.

RSU Roadside Unit.

SAML Security Assertion Markup Language.

SCMS Security Credential Management System.

SeVeCom Secure Vehicle Communication.

TLS Transport Layer Security.

V2I Vehicle-to-Infrastructure.

V2V Vehicle-to-Vehicle.

V2X Vehicle-to-Vehicle (V2V) and/or Vehicle-to-Infrastructure (V2I).

VANET Vehicular Ad-hoc Network.

VC Vehicular Communication.

VM Virtual Machine.

VoI Vehicles of Internet.

VPKI Vehicular Public-Key Infrastructure.

VPKIaaS VPKI as a Service.

VSN Vehicular Social Network.

WAVE Wireless Access in Vehicular Environments.

XML Extensible Markup Language.

Chapter 1

Introduction

1.1 Background

The concept of smart cities is shaping future urban infrastructure and influences transportation systems. Smart vehicles, as the principal building block of Intelligent Transport Systems (ITSs), are on the way and car-makers are mandated to equip vehicles with new communication technologies [1, 2]. Meanwhile, Field Operational Testing (FOT) for self-driving cars is on-going [3]. These set the ground for the emergence of innovative applications to improve road safety, transportation efficiency, and driving experience[1]

In Vehicular Communication (VC) systems, vehicles are to be provided with special-purpose sensors and equipments to monitor their operation and surrounding. A smart vehicle will be equipped with Radar, Electronic Control Unit (ECU), sensors and Global Positioning System (GPS). Vehicles are to be fitted with On-Board Units (OBUs) to facilitate Dedicated Short Range Communication (DSRC), over ITS-G5 (i.e., IEEE 802.11p [5, 6]) or leveraging the cellular infrastructure, e.g., Long Term Evolution (LTE) [7] and 3G/4G, with other OBUs or Roadside Units (RSUs). Vehicles periodically disseminate messages about their actions, e.g., lane changing and emergency braking notifications, and their whereabouts containing location, velocity, and acceleration. As a result, neighboring vehicles will be informed about possible unexpected incidents or objects. Typical use cases of such safety-related applications are *''intersection collision warning''* and *''motorcycle approaching indication''* [8]. VC systems are not limited to safety-related applications; it also entails Location Based Services (LBSs) [5, 9, 10, 11, 12] and Vehicular Social Networks (VSNs) [13] which provide efficiency and infotainment in the VC systems. All these facilitate the emergence of next generation of connected vehicles, what one can call the *Internet of Vehicles (IoV)*.

[1]The contents of the introduction section of this compendium rely on the licentiate thesis [4] of the author of this dissertation.

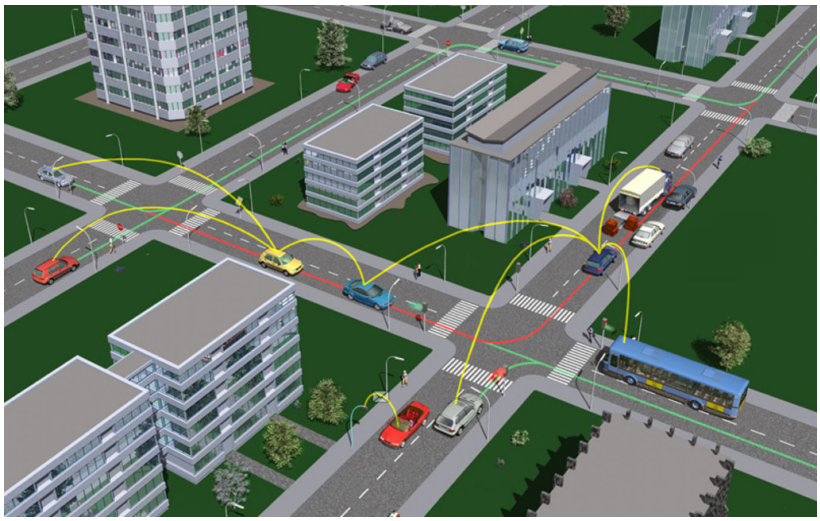


Figure 1.1: A Vehicular Communication Network [Source: C2C-CC [16]].

Fig. 1.1 illustrates a vehicular communication network: vehicles can directly communicate with each other, using Vehicle-to-Vehicle (V2V) communication across one or multiple hops, or they can exchange information with RSUs using Vehicle-to-Infrastructure (V2I) communication. Vehicles beacon Cooperative Awareness Message (CAM) [8] and Decentralized Environmental Notification Message (DENM) [14] frequently [5]; these messages disseminate valuable information on potentially dangerous vehicle movement, environmental hazards, or even assist regulating traffic [9]. More precisely, CAMs provide road safety by means of periodic beaconing of vehicle trajectory information to neighboring vehicles. Such beaconing messages include vehicle type, location, velocity, acceleration, vehicle length, width, and curvature [8]. Safety applications built on top of CAMs provide *''emergency vehicle warning''*, *''intersection collision warning''*, *''motorcycle approaching indication''*, and *''speed limits notification''* [8]. On the contrary, dissemination of DENMs is only triggered upon detection of an event: under specific circumstances, the vehicle broadcasts a DENM to its neighboring vehicles. The vehicle continues broadcasting as long as the event is present, or within a predefined expiry time [14]. DENMs can be triggered in environmental hazard events, e.g., *''precipitation''*, *''road adhesion''*, *''visibility''*, and *''wind''* [14], or in traffic events [15], e.g., *''road-work warning''*, *''traffic condition warning''*, and *''stationary vehicle''* [14].

1.2 Challenges and Problem Statements

As a result of such a paradigm shift, user privacy is highly at risk: by periodically beaconing information across the open wireless network, user private information is exposed potentially to everyone. An eavesdropper could collect user-identifying information to harm user privacy: by cross-referencing the time, location, and other

external information, e.g., local hospital admissions and driving patterns [17, 18, 19], it would be feasible to track and identify a vehicle. The experience from mobile applications and LBSs [20, 21, 22] hints that this is a realistic threat to user privacy, aggravated, of course, by the recent stream of disclosures on mass surveillance [23, 24]. Thus, vehicles should participate in the VC system and communicate with each other (ideally) anonymously. To further enhance their privacy, vehicles should communicate anonymously with the security infrastructure entities and service providers.

By the same token, the security of the VC system is paramount: an attacker could contaminate large portion of the system with false information, or meaningfully forge a message or impersonate an identity to mislead other vehicles [25]. The importance of secure communication in the VC systems is due to the risk for physical damages and injuries to the human safety: a fatal crash could threaten human safety [26] as vehicles could be compromised or their sensors become faulty. Anonymity may be abused by faulty (compromised or malfunctioning) vehicles to corrupt system operations by disseminating bogus information across the network. Thus, vehicles should be held accountable for their operations and actions, and the system should detect and evict misbehaving vehicles [25]; otherwise, the reliability and robustness of the entire system might be compromised, eventually, perhaps, jeopardizing human safety. But, accountability and strong privacy preservation, at the same time, appear at a first glance contradictory; the question this raises is: *how to design a secure VC system that ensures accountable vehicle identification while protecting user privacy.*

It has been well-understood that VC systems are vulnerable to attacks and that the privacy of their users is at stake. As a result, security and privacy solutions have been developed by standardization bodies (IEEE 1609.2 WG [6] and ETSI [5]), harmonization efforts (C2C-CC [16, 27]), and projects (SeVeCom [15, 28, 29], PRESERVE [30], and CAMP [31, 32]). A consensus towards using Public Key Cryptography (PKC) to protect V2V and/or V2I (V2X) communication is reached: a set of short-lived anonymized certificates, termed *pseudonyms*, are issued by a Vehicular Public-Key Infrastructure (VPKI), e.g., [31, 33, 34, 35], for registered vehicles. Vehicles switch from one pseudonym to a non-previously used one towards message unlinkability, as pseudonyms are per se inherently unlinkable. Pseudonymity is conditional, in the sense that the corresponding long-term vehicle identity can be retrieved by the VPKI when needed, e.g., if vehicles deviating from system policies.

Deploying a VPKI differs from a traditional Public-Key Infrastructure (PKI), e.g., [36, 37, 38]. One of the most important factors is the PKI dimension, i.e., the number of registered ‘‘users’’ (vehicles) and the multiplicity of certificates per user. According to the US Department of Transportation (DoT), a VPKI should be able to issue pseudonyms for more that 350 million vehicles across the Nation [39]. Considering the average daily commute time to be 1 hour [39] and a pseudonym lifetime of 5 minutes, the VPKI should be able to issue at least 1.5×10^{12} pseudonyms per year, i.e., 5 orders of magnitude more than the number of credentials the largest

current PKI issues (10 million certificates per year [31]). Note that this number could be even greater for the entire envisioned ITSs ecosystem, e.g., including pedestrians and cyclists, LBSs [5, 9, 40] and vehicular social networks [13]. More so, outside the VC realm, there is an ongoing trend towards leveraging short-lived certificates [41] for the Internet: web servers request new short-lived certificates, valid for a few days [41]. This essentially diminishes the vulnerability window, e.g., if a single Certification Authority (CA) were compromised [41], or if a large fraction of certificates needed to be revoked after the latest Certificate Revocation List (CRL) was distributed among all entities [42, 43, 44, 45].

With emerging large-scale multi-domain VC environments [5, 6, 9, 16, 46], the efficiency of the VPKI and, more broadly, its scalability are paramount. Vehicles could request pseudonyms for a long period, e.g., 25 years [47]. However, extensive pre-loading with millions of pseudonyms per vehicle for a long period is computationally costly and inefficient in terms of utilization [35]. Moreover, in case of revocation [42, 43, 44], a large, or very large, CRL should be distributed among all vehicles due to long lifespan of the credentials, e.g., [47]: a sizable portion of the CRL is irrelevant to a receiving vehicle and can be left unused, i.e., wasting of significant bandwidth for CRL distribution [44, 48]. Alternatively, each vehicle could interact with the VPKI regularly, e.g., once or a few times per day, not only to refill its pseudonym pool but also to fetch the latest revocation information[2]. However, the performance of a VPKI system can be drastically degraded under a clogging Denial of Service (DoS) attack [34, 35], thus, compromising the availability of the VPKI entities. Moreover, a *flash crowd* [52], e.g., a surge in pseudonym acquisition requests during rush hours, could render the VPKI unreachable, or drastically decrease its quality of service.

The cost of VPKI unavailability is twofold: security (degradation of road safety) and privacy. An active malicious entity could prevent other vehicles from accessing the VPKI to fetch the latest revocation information. Moreover, signing CAMs with the private keys corresponding to expired pseudonyms, or the Long Term Certificate (LTC), is insecure and detrimental to user privacy. Even though one can refill its pseudonym pool by relying on anonymous authentication primitives, e.g., [53, 54, 55, 56], the performance of the safety-related applications could be degraded. For example, leveraging anonymous authentication schemes for the majority of vehicles results in causing 30% increase in cryptographic processing overhead in order to validate CAMs [56]. Thus, it is crucial to provide a highly-available, scalable, and resilient VPKI design that could efficiently issue pseudonyms in an *on-demand* fashion[3] [57, 58].

Considering a multi-domain development of VC systems, with a multiplicity of service providers, each vehicle could obtain pseudonyms from various service

[2]Note that Cellular-V2X provides reliable and low-latency V2X communication with a wide range of coverage [49, 50, 51]; thus, network connectivity will not be a bottleneck.

[3]Unlike issuing short-lived certificates [41] for the Internet that responses can be cached, issuing on-demand pseudonyms cannot be precomputed: each vehicle requests new certificates with a different public key, important for privacy (unlinkability).

providers. The acquisition of multiple simultaneously valid (sets of) pseudonyms would enable an adversary to inject multiple erroneous messages, e.g., hazard notifications, as if they were originated from multiple vehicles, or affect protocols based on voting, by sending out false, yet authenticated, information. Even though there are distributed schemes to identify Sybil [59] nodes, e.g., [60, 61], or mitigate this vulnerability by relying on Hardware Security Modules (HSMs) [29], a VPKI system should prevent such credentials misuse on the infrastructure side, e.g., [34, 35]. However, when deploying such a system, e.g., [62, 63, 64, 65, 66], on the cloud, a malicious vehicle could repeatedly request pseudonyms; in fact, requests might be delivered to different replicas of a micro-service, releasing multiple simultaneously valid pseudonyms. Mandating a centralized database, shared among all replicas to ensure *isolation* and *consistency* of all transactions, would mitigate such a vulnerability. However, this contradicts highly efficient and timely pseudonyms provisioning for large-scale mobile systems.

From a different viewpoint, vehicles can be compromised or faulty and disseminate erroneous information across the V2X network [67, 68]. They should be held *accountable* for such actions and credentials (their LTCs and their pseudonyms) can be revoked. To efficiently revoke a set of pseudonyms, one can disclose a single entry for all (revoked) pseudonyms of the vehicle [69, 70, 71, 72]. However, upon a revocation event, all non-revoked (but expired) pseudonyms belonging to the ''misbehaving'' vehicle would also be linked. Linking pseudonyms with lifetimes prior to a revocation event implies that all the corresponding digitally signed messages will be trivially linked. Even if revocation is justified, this does not imply that a user *''deserves''* to abolish privacy prior to the revocation event. Avoiding such a situation, i.e., achieving what is termed in the literature as *perfect-forward-privacy* [73], can be guaranteed if the VPKI entities are *fully-trustworthy* [74]. However, we need to guarantee strong user privacy even in the presence of *honest-but-curious* VPKI entity; recent revelations of mass surveillance show that assuming service providers are fully-trustworthy is no longer a viable approach.

From the privacy point of view, an observer could eavesdrop communications in VC systems towards inferring vehicle-sensitive information. Although pseudonymous authentication is a promising approach to protect user privacy, an adversary, eavesdropping all traffic in an area, could link successive pseudonymously authenticated messages. An adversary might observe an isolated pseudonym change, and associate the old and new pseudonymous identifiers through *syntactic linking*, e.g., [75, 76, 77]. Alternatively, an adversary could leverage physical constraints of the road layout [18], and message payload, e.g., location, velocity, time, the confidence levels of heading, acceleration, the length and width[4], of a victim's vehicle to predict its trajectory towards linking messages *semantically*, e.g., [18, 76, 81, 82]. Such information could be unique, or one of few, and thus, can be easily linked by an external observer. While appropriate pseudonym provisioning policies alleviate syntactic linking through issuing timely-aligned pseudonyms [34, 35], compromising

[4]Length and width of vehicles are specified with a precision of 10 centimeters [78, 79, 80].

user privacy by conducting semantic linking attacks is still feasible[5].

Contributions: This thesis makes an effort to pave the way for deployment of secure and privacy-protecting VC systems presenting an identity and credential management infrastructure that builds upon past efforts and developed understanding. This work raises a number of open questions to be addressed to achieve enhanced protection (of the system and its users) and scalability. We propose comprehensive security and privacy-preserving solutions to address the aforementioned challenges that improve upon existing proposals in terms of security and privacy protection, and efficiency. More specifically, this thesis addresses the following aspects of VC systems:

- We propose SECMACE, a comprehensive security and privacy-preserving architecture for VC systems, contributing a set of novel features: (i) multi-domain operation, (ii) increased user privacy protection, in the presence of honest-but-curious system entities even with limited collusion, and by eliminating pseudonym linking based on timing information, (iii) thwarting Sybil-based misbehavior, and (iv) multiple pseudonym acquisition policies. Beyond these features, we provide an extensive survey of the prior art and a detailed security and privacy analysis of our system. We further provide an extensive evaluation of the overall system performance including alternative pseudonym acquisition policies, and assessing its efficiency, scalability, and robustness based on an implementation of our VPKI and two large-scale mobility traces.

- We show how to efficiently revoke a very large volume of pseudonyms while providing strong user privacy protection, even in the presence of honest-but-curious VPKI entities. Our system effectively, resiliently, and in a timely manner disseminate the authentic CRL throughout a large-scale (multi-domain) VC system. Moreover, we ensure that the CRL distribution incurs low overhead and prevents abuse of the distribution mechanism. Furthermore, our flexible design allows to temporarily evict a vehicle from the system without compromising user privacy. At the same time, it facilitates rejoining the system as a legitimate participant upon resolving the issue without imposing unnecessary workload on the VPKI entities, by frequently refilling pseudonyms pool, and, most important, shields the system from clogging DoS attacks leveraging the CRL and Δ-CRL distribution.

- We show how to enhance user privacy, notably in low-density areas and non-rush hour periods, and mitigate syntactic and semantic linking attacks without affecting the operation of safety applications. Our scheme efficiently, effectively, resiliently, and in a fine-grained manner, enhances user privacy.

[5]Note that connecting such anonymous location profiles to real identities of vehicle owners is the final step, e.g., tracing their commutes and identify home/work locations [83, 84, 85], the information obtained from VSNs [13], or full de-anonymization of vehicles by *honest-but-curious* VPKI entities [35].

Further, we ensure that our scheme incurs low (computation and communication) overhead and prevents abuse of the mechanism towards diminishing the performance of the system or harming user privacy.

1.3 Thesis Structure

The structure of the thesis is as follows: we first present the state-of-the-art security and privacy for the VC systems in Chapter 2. We then describe the security and privacy requirements and the adversaries in Chapter 3. In Chapter 4, we present our contributions, followed by Chapter 5 in which we give a summary of the papers in the context of this thesis along with the contribution of the author for each paper. We conclude this thesis with a discussion on future research directions in Chapter 6.

The aforementioned six chapters are followed by an appendix including the accepted or published papers and one in submission, in chronological order, all involving the author of this thesis. The contents of the introduction of this compendium (Chapters 1– 5) rely on the licentiate thesis [4] and prior publications, with all parts explicitly cited. More specifically, the introduction section of this compendium (Sec. 1.1 and Sec. 1.2) significantly relies on the introduction section in [4]. The contents in Chapter 2 draw on the related work section in [4, 35, 44, 45, 86]. The texts in Chapter 3 rely on the system model, requirements, and adversarial model sections in [35, 44, 86]. The contents in Chapter 4, which addresses the challenges and outlines the results in a concise manner, rely on [35, 44, 45, 86, 87], with all parts and figures explicitly cited. Finally, Chapter 5 provides a verbatim copy of the abstract for each publication.

Chapter 2

Current Status of Security and Privacy for Vehicular Communication Systems

Standardization bodies (IEEE 1609.2 WG [6] and European Telecommunications Standards Institute (ETSI) [88, 89, 90]) and harmonization efforts (C2C-CC [27, 91, 92]) have reached a consensus towards deploying a VPKI in order to protect V2X communication with the help of public key cryptography. These efforts unfolded in parallel by academic works that developed the same concepts, e.g., [15, 29, 93]. A set of Certification Authorities (CAs), constituting the VPKI, provide credentials to registered (thus legitimate) vehicles. Each legitimate vehicle is equipped with a LTC to ensure accountable identification of the vehicle. A set of short-lived anonymized certificates, termed *pseudonyms*, are used to enhance privacy, i.e., achieving unlinkability of messages originating the same vehicle, while maintaining non-repudiation, authenticity and integrity. The VPKI maintains a mapping of these pseudonyms to the corresponding LTC the vehicle is registered with. These ideas were elaborated by the Secure Vehicle Communication (SeVeCom) project [15, 28, 94] as well as in subsequent projects, e.g., Crash Avoidance Metrics Partnership Vehicle Safety Consortium (CAMP VSC3) [31, 32] and Preparing Secure Vehicle-to-X Communication Systems (PRESERVE) [30, 95, 96, 97, 98, 99].

2.1 Identity and Credential Management Systems

In VC systems, each vehicle is registered to one Long Term CA (LTCA), the identity provider, which is responsible for issuing the LTC for each vehicle; any legitimate, i.e., registered, vehicle is able to obtain pseudonyms from any Pseudonym CA (PCA), the pseudonym provider (as long as there is a trust established between the two CAs). Fig. 2.1 shows an overview of a VPKI with three domains, A, B and C. Domains A and B have established trust (security association) with the help

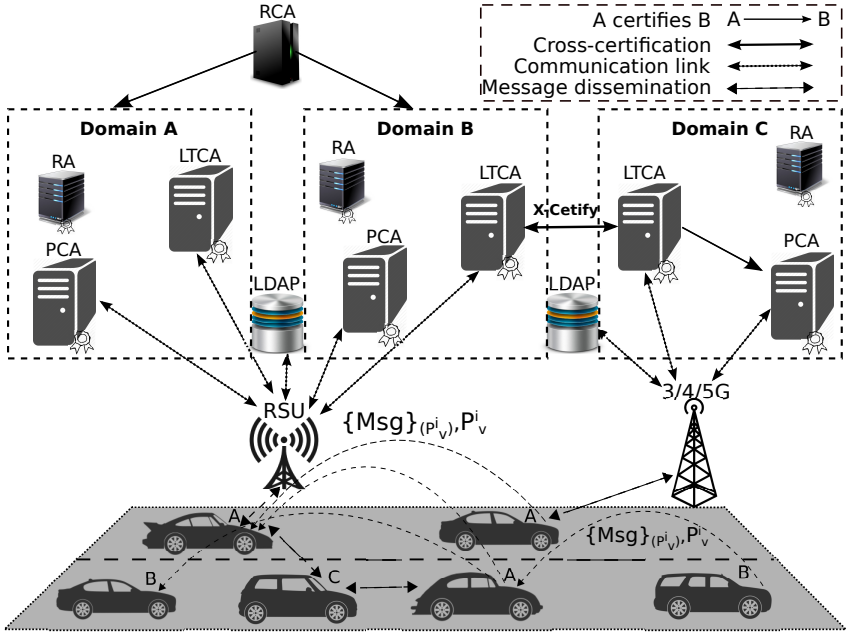


Figure 2.1: A Vehicular Public-Key Infrastructure (VPKI) Overview [taken from [87]].

of a higher-level authority, i.e. the Root CA (RCA) while domains B and C have established security association by cross certification. The vehicles in the figure are labeled with the domains they are affiliated to. In the VC systems, a domain is defined as a set of vehicles registered with an identity provider, with communication independent of administrative or geographical boundaries [25, 46, 100]. In case of misbehavior, the Resolution Authority (RA) is the responsible entity to initiate a process to resolve a pseudonym, i.e., revealing the real identity of a misbehaving or malfunctioning vehicle [67].

Each vehicle interacts with the VPKI entities to obtain a batch of pseudonyms, each having a corresponding short-term private key, to sign and disseminate their mobility information, e.g., CAMs or DENMs, time- and geo-stamped, periodically or when needed as a response to a specific event. As illustrated in Fig. 2.1, a vehicle registered in domain A digitally signs outgoing messages with the private key, k_v^i, corresponding to P_v^i, which signifies the current valid pseudonym signed by the PCA. The pseudonym is then attached to the signed messages to enable verification by any recipient. Upon reception, the pseudonym is verified (assuming a trust relationship with the pseudonym provider) before the message itself (signature validation). This process ensures communication authenticity, message integrity, and non-repudiation. Vehicles switch from one pseudonym to another one (ideally, non-previously used) to achieve unlinkability, thus protecting sender's privacy, as the pseudonyms per se are inherently unlinkable.

Several proposals are compatible with the C2C-CC security architecture (pilot PKI [27, 92]), e.g., PRESERVE [95], in which the direct LTCA-PCA communication is involved in the pseudonym acquisition process. Because of the direct communication at the time of pseudonym provision, the LTCA learns the targeted PCA; moreover, the LTCA could link the real identity of the vehicle with its corresponding pseudonyms according to the timing information of the credentials, i.e., pseudonym issuance and expiry times.

A ticket based approach is proposed in [101]: the LTCA issues authenticated, yet anonymized, tickets to the vehicles to obtain pseudonyms from the PCA. There is no direct LTCA-PCA communication and the PCA does not learn any user-related information through pseudonym process. However, the LTCA can learn from pseudonym acquisition process: when and from which PCA the vehicle will obtain pseudonyms since the Security Assertion Markup Language (SAML) token is presented to the LTCA. The exact pseudonym acquisition period could be used to infer the active period of the vehicle operation, and the targeting PCA could be used to infer the approximate location (assuming the vehicle chooses the nearest PCA) or the affiliation (assuming the vehicle can only obtain pseudonyms from the PCA in the domain it is affiliated to, or operating in) of the vehicle.

Several proposals [53, 54, 55, 102, 103] leverage anonymous authentication with Group Signatures (GS) in the context of VC systems. Each vehicle is equipped with a group public key, which are common among all the group members, and a distinct group signing key. Then, each vehicle in the group can sign its messages with its own group signing key and the recipients are able to verify those messages with the common group public key. The signer is kept anonymous since the signatures (even the signatures of two exactly same messages) cannot not be linked. However, GSs incur high (computational) overhead [55]. For example, the signing delay with Group Signatures with Verifier Local Revocation (GS-VLR) [104] (a representative GS algorithm) is around 67 times higher than that with Elliptic Curve Digital Signature Algorithm (ECDSA)-256, and the verification delay with the former one is around 11 times higher than the latter one (with the same security level, i.e., 128 bits) [55]. [105] proposes a fully anonymous scheme using zero-knowledge proofs for the vehicle-PCA authentication with the consequence that compromised OBUs can be revoked only *''manually''* with involvement of the owners.

[53, 54, 55] propose hybrid schemes by combining GS and traditional public/private keys. A vehicle can generate public/private key pairs and signs the public keys with its own group signing key. Then, a public key with an attached GS can be used as a pseudonym. Such schemes eliminate the need to request pseudonyms from the PCA repeatedly. Upon reception of messages signed under a new pseudonym, both the GS (of the pseudonym) and the message signature need to be verified; if the pseudonym is cached, only the message signatures need to be verified for the following messages signed under the cached pseudonyms (further optimizations can be found in [55]). Such performance improvement relies on the lifetime of each pseudonym, and it can be applied to all pseudonym-based authentication schemes: the longer the pseudonym lifetime is, the more pseudonym verification can be omitted. The

overall efficiency of VC systems, in fact, its scalability, is important. Adaptation can be beneficial [106], while cooperative approach and additional optimizations can render secure and privacy-preserving VC systems scalable and resilient to clogging DoS, e.g., [107, 108].

Sybil-based [59] misbehavior, based on the acquisition of multiple simultaneously valid pseudonyms, has not been considered by a number of proposals for identity and credential management infrastructure [31, 92, 101, 109, 110]. Consider an attacker that has multiple simultaneously valid pseudonyms and starts disseminating hazard notifications, each signed under a different pseudonym. Any recipient would interpret that the messages come from different vehicles while in reality, they all come from a single entity. These proposals either do not enforce issuing pseudonyms with non-overlapping lifetimes [31, 92, 109, 110] or the security infrastructure does not prevent a vehicle from obtaining simultaneously valid pseudonyms via multiple pseudonym requests [101]. This leaves a gap for vehicles equipped with multiple valid identities to affect the output of protocols by sending out redundant false, yet authenticated, information, e.g., fake traffic congestion alerts or fake misbehavior detection votes [111]. By providing vehicles with HSMs, the usage of pseudonyms can be regulated [29], which guarantees all outgoing signatures are signed under the private key of a single valid pseudonym at any time; thus mitigating Sybil attacks. [55, 105] prevent Sybil-based misbehavior by leveraging ''periodic n-show credentials'' [112], thus restricting the credentials usage and ensuring that each legitimate vehicle can only have one valid pseudonym at any time.

Although pseudonymous authentication is the most promising solution to enhance user privacy in Vehicular Ad-hoc Networks (VANETs), it could jeopardize user privacy if not properly used. Timing and location information of pseudonymously authenticated messages could help an adversary, who eavesdrops all traffic through an area, to link pseudonyms based on this information [18]. There are different strategies for pseudonyms transition, i.e., changing the currently used (or expired) pseudonym to a new one. Some proposals [113, 114] suggest changing pseudonyms at appropriate places, e.g., at an intersection or a parking lot, to make it more difficult for an observer to link two successive pseudonyms belonging to the same vehicle. To enhance user privacy, i.e., to increase the probability of unlinkability between two pseudonyms, [115] suggests that each vehicle should be silent, i.e., not beaconing, for a *quiet-time* interval, or if the speed is below a threshold [76]. However, vehicle transceivers cannot be simply switched off [116] as they could cause fatal accidents, thus seriously jeopardizing human safety. [117, 118] suggest cooperative pseudonym changing process: multiple OBUs cooperate with each other to determine the exact time of pseudonym transition so that they simultaneously change their pseudonyms. Without loss of generality, user traceability is orthogonal to the process of obtaining pseudonyms; nonetheless, it is related since all of the above-mentioned proposals require multiple valid pseudonyms at any given point in time. Thus, enabling these proposals requires issuing pseudonyms with overlapping lifetimes from the side of the security infrastructure. However, as explained earlier, this sets the ground for Sybil-based misbehavior.

Deploying a VC large-scale multi-domain environment shed the light on extensive experimental validation of the VPKI. In the light of a large-scale VC system, the performance, i.e., the efficiency, scalability, and robustness, of the VPKI are paramount. Beyond our work, very few schemes have evaluated aspects of performance of the implementation of their VPKI to some extent [101, 105]. We need to extensively evaluate the efficiency and scalability of any scheme we design to ensure that the system would scale up and it does not cause excessive delays in provisioning vehicles with pseudonyms.

2.2 Certificate Revocation List Distribution

The need to evict misbehaving or compromised [67] vehicles from a VC system is commonly accepted, because such vehicles can threaten the safety of vehicles and users and degrade transportation efficiency. CRL distribution is of central importance and it is the final and definitive line of defense [5, 6, 29, 111, 119]: only the VPKI can *''ultimately''* revoke a vehicle by including its unexpired certificates' serial numbers in a CRL.

The literature proposes distribution of the CRL via RSUs [120] and car-to-car epidemic communication [71, 72, 74], with enhancements on the distribution of pieces [121, 122] evaluated in [123]. A naïve solution would be to digitally sign the entire CRL and broadcast it; however, it imposes difficulties in downloading a large CRL file and exchanging it over short contact period (with an RSU or a peer). Splitting the digitally signed CRL into multiple pieces is vulnerable to *pollution* attacks: in the absence of fine-grained authentication, per CRL piece, an adversary can delay or even prevent reception by injecting fake pieces. Thus, the straightforward solution is to have the VPKI prepare the CRL, split it into multiple pieces, sign each piece, and distribute all of them across the VC system. RSUs can broadcast CRL pieces randomly or in a round-robin fashion [120], and vehicles can relay pieces until all vehicles receive all pieces necessary to reconstruct the CRL [71]. Erasure codes can be used to enhance the fault-tolerance of the CRL piece distribution in the highly volatile VC environment [120, 124].

Signing each CRL piece so that it is self-verifiable, incurs significant computation overhead, which grows linearly with the number of CRL pieces, both for the VPKI and for the receiving vehicles. Furthermore, an attacker could aggressively forge CRL pieces for a DoS attack leveraging signature verification delays [125] that can prevent vehicles from obtaining the genuine CRL pieces. A *''precode-and-hash''* scheme [126] proposes to calculate a hash value of each pre-coded piece, sign it, and disseminate it with higher priority. Each relaying node can apply a different precode to the original CRL and act as a secondary source. However, by applying different encodings to the original CRL file, another receiver cannot reconstruct the entire CRL from the pieces, encoded differently by various relaying nodes. To mitigate pollution and DoS attacks, we propose to piggyback a fingerprint (a Bloom Filter (BF) [127, 128]) for CRL pieces into a subset of pseudonyms to validating

CRL pieces ''for free''.

To efficiently revoke an ensemble of pseudonyms, one can enable revocation of multiple pseudonyms with a single CRL entry, to reduce the CRL size, e.g., [71, 72, 129]. Despite a huge reduction in size, such schemes do not provide *perfect-forward-privacy* [73]: upon a revocation event and CRL release, all the ''non-revoked'' but previously expired pseudonyms belonging to the evicted entity would be linked as well. Although forward-privacy can be achieved by leveraging a hash chain [74], the pseudonyms' issuer can trivially link all pseudonyms belonging to a vehicle, and thus the pseudonymously authenticated messages [77, 130, 131, 132], towards tracking it for the entire duration of its presence in the system [69, 70, 71, 72, 74]. More precisely, the CA specifies a *''time interval''* so that each vehicle receives $\mathbb{D}$ pseudonyms during the pseudonym acquisition process [74]. As a result, for each batch of revoked pseudonyms, a single key is disclosed. But, upon a revocation event, all pseudonyms within an interval are linked, because one can decrypt all pseudonym serial numbers; thus, no *perfect-forward-privacy* is achieved for that period. On the contrary, in our scheme, upon a revocation event and CRL release, it is infeasible to link the previously non-revoked (but expired) pseudonyms belonging to a misbehaving vehicle. This is so due to the utilization of a hash chain during the pseudonym issuance process, thus achieving perfect-forward-privacy [44, 45].

Compressing CRLs using a BF was proposed for compact storage of revocation entries [111], or to efficiently distribute them across the network [68, 111, 133]. However, the challenge is twofold: scalability and efficiency. Their CRL size still grows linearly with the number of revoked pseudonyms, while a substantial portion of the compressed CRL can be irrelevant to a receiving vehicle and be left unused. Moreover, compressing CRLs using a BF does not necessarily reduce the size of a CRL as vehicles can be provided with possibly hundreds of pseudonyms [6, 44, 45, 48]. Unlike such schemes [68, 111, 133], we do not compress the CRL: our scheme disseminates only trip-relevant revocation information to vehicles and it utilizes a BF to provide a condensed authenticator for the CRL pieces. Our scheme leverages and *enhances* the functionality of the state-of-the-art VPKI system [35] towards efficiently revoking a batch of pseudonyms without compromising user privacy backwards: upon a revocation event, all pseudonyms prior to the revocation event remain unlinkable.

Alternatively, vehicles could validate pseudonym status (revocation) information through Online Certificate Status Protocol (OCSP) [134]. However, due to intermittent VC network connectivity, significant usage of the bandwidth by time- and safety-critical operations, and substantial overhead for the VPKI (assuming the server is reachable), OCSP cannot really be used as a standalone solution [68]. A hybrid solution could rely on distributing certificate status information to other mobile nodes [135, 136, 137, 138, 139]; however, the system would be subject to the reachability (of sufficiently many cooperative) and the trustworthiness of such nodes. In our scheme, we ensure that the latest CRL is efficiently, effectively, and timely distributed among all vehicles without any assumption on persistent reachability and trustworthiness of specific mobile nodes.

Research efforts also focused on how to protect the VC systems from misbehaving nodes, by temporarily ''revoking'' (isolating) them from further access to the system [68, 111, 140, 141, 142] until connection to the VPKI is established and they are fully evicted from the system. Before the VPKI performs the ''actual'' eviction and CRL distribution, these protocols build evidence, in fact local agreement, that a given wrongdoer is present. This can serve towards isolating misbehaving vehicles before the corresponding VPKI entity takes the *''ultimate''* decision and commences the latest CRL distribution.

C2C-CC [27] and V-token [110] propose to revoke only the LTC of vehicles and let the pseudonyms expire. PUCA [105] requires the owner of the pseudonym to trigger revocation, i.e., the system cannot evict a misbehaving entity from the system. Clearly, leaving it up to the misbehaving entity, or allowing it to act for a significant period till pseudonyms expire, creates an unacceptable vulnerability window. Another line of studies proposes geo-casting a *''self-revocation''* message, by the VPKI, across a region, to wipe out the credentials from the HSM of a misbehaving vehicle [15, 68, 111, 143]. However, an adversary could control incoming messages, and prevent the *''self-revocation''* instruction from reaching the HSM, i.e., such schemes alone cannot guarantee the trustworthiness of the system against misbehavior unless the VPKI distributes the CRL enabling legitimate vehicles to defend themselves against misbehavior or faulty peers.

Alternatively, the VPKI could provide vehicles for a long period, e.g., 25 years, worth of pseudonyms with a decryption key for, e.g., a weekly batch of pseudonyms, delivered periodically [47]. This would eliminate the need for bidirectional connectivity to the VPKI to obtain pseudonyms. To evict a vehicle, the VPKI can stop delivering the corresponding decryption key to the vehicle HSM. Still, it is imperative to distribute the CRL and cover the (weekly) period and the corresponding revoked pseudonyms. Furthermore, having released a CRL towards the end of a week, signed messages with the private keys corresponding to the recently revoked pseudonyms (included in the CRL) can be linked, i.e., backwards-trackable for a week (no *perfect-forward-privacy* for that period) [39].

Outside the VC realm, a recent comparative evaluation of classic Internet schemes is available [43]. Such schemes, e.g., [144, 145, 146, 147, 148, 149, 150], cannot be leveraged due to the nature of VC systems, i.e., short-lived pseudonyms, highly dynamic intermittent connectivity, and resource constraints. For example, CRLite [150] stores CRLs in a *filter-cascade* BF without any false positive or false negative; however, this necessitates little change in the set of revoked and non-revoked certificates. Obviously, this contradicts *on-demand* pseudonym acquisition strategies for VC systems, e.g., [34, 35, 57, 58, 87, 105, 109, 110], which are more efficient (than preloading pseudonyms for a long duration, e.g., [47]) in terms of pseudonym utilization and revocation, thus more effective in fending off misbehavior.

Temporal eviction of a misbehaving or malfunctioning vehicle from the VC system has received limited attention. There are several situations that a vehicle should be temporarily evicted from the system until the issue is resolved and the vehicle can rejoin the system, e.g., in case a malfunctioning sensor disseminating false

information. Security Credential Management System (SCMS) [31, 47] supports only permanent eviction of a misbehaving vehicle by including a linkage seed into a CRL. Towards temporal revocation of credentials, [151, 152] propose a *linkage hook* between any *linkage seed* and the corresponding *pre-linkage values* in the original SCMS design. Thus, in order to temporarily revoke the credentials, the linkage hook is disclosed (instead of the linkage seed, used for permanently revoking the credentials). Temporal eviction of a subset of the certificates requires additional layers to be added to the tree. However, the disclosure of linkage hooks would trivially link all pseudonyms inside a given subtree. Our scheme facilitates eviction of a misbehaving vehicle temporarily, i.e., for a fine-grained interval, until the issue is resolved without compromising user privacy (prior to the revocation event).

2.3 Location Privacy Protection

Due to the openness of wireless transmissions and dissemination of basic safety messages in plaintext (as confidentiality is not needed in VC systems [6, 25, 80, 153, 154, 155]), an external entity can arbitrarily eavesdrop VC systems [156, 157, 158]. With advances in broadcast technology to extend the transmission range of OBUs [159], VANET messages become increasingly accessible for an attacker. This information allows semantic linking attacks that rely on location and heading information of continuously broadcast CAMs [18]. Prior works, e.g., [113, 131], assume that the system entities that are fully trustworthy, i.e., RSUs and VPKI entities, could link successive pseudonyms belonging to a given vehicle. However, recent revelations of mass surveillance, e.g., [23, 24], show that assuming service providers are fully-trustworthy is no longer a viable approach. Thus, in [113, 160, 161, 162], the VPKI entities can easily link pseudonyms issued for the vehicles, thus tracking them for the entire trip duration. Unlike the chaff-based Cryptographic Mix-Zone (CMIX) scheme [131] that requires vehicles provide their intended trajectory path to the RSUs, our scheme does not provide additional information and maintains strong user privacy protection upon pseudonym change in the presence of *honest-but-curious* system entities.

There are different solutions for location privacy: *K-anonymity* [163] ensures that a target node is not distinguishable from at least *K-1* nodes within an *anonymity set* with respect to the information each node disseminates. However, safety applications require precise information to operate correctly, e.g., *intersection collision warning* [164]. Alternatively, one can rely on group signature schemes, e.g., [53, 54, 55, 56, 165], to enhance user privacy. However, the performance of safety-related applications could be degraded. For example, leveraging such anonymous authentication schemes by the majority of vehicles results in a 30% increase in cryptographic processing overhead [56]. Moreover, with all vehicle-sensitive information in CAMs and DENMs, e.g., location, velocity, and acceleration, a targeted node could be unique, or one of few, and thus, successive messages could be linked sequentially by an external observer.

Different pseudonym transition strategies, to prevent an attacker from inferring such information, have been proposed. To evade correlation attacks, each vehicle could turn its wireless transmitter off for a randomly chosen interval and change pseudonym within that silent period [118, 166, 167]. Even though such schemes could improve user privacy, they impose a performance penalty on safety applications [168], thus jeopardizing human safety. To mitigate such a problem, vehicles could become silent and change their pseudonyms when their speed drops below 30 km/h since the risk of a fatal accident at a slow speed is expected to be low [76]. However, an adversary can still conduct syntactic linking attacks due to a lack of synchronization among vehicles [77], or track vehicles across pseudonym changes by predicting their trajectories [169].

Another line of study proposes pseudonym transitions strictly within CMIX [113], which does not impair transportation safety applications. A cryptographic mix-zone was initially proposed [113] in the VC systems to establish a cryptographically protected region at appropriate times and places, e.g., at intersections. When crossing these regions, vehicles change their pseudonyms privately while their communication is encrypted, which prevents syntactic and semantic linking attacks. However, the achieved privacy protection highly depends on the number of vehicles participating in the mix-zone, i.e., user privacy is degraded under low traffic density, e.g., in a highway scenario [170]. Moreover, an attacker could compromise unlinkability within a mix-zone based on the traffic mobility pattern and vehicle speed [171]. To counter this, vehicles could randomly switch lanes and speed prior to entering and/or crossing the mix-zones to confuse an adversary [172, 173]. However, such schemes would not be practical as they could seriously jeopardize human safety. Unlike such schemes, we provide privacy protection without affecting the operation of safety applications and regardless of variations in road layout, vehicle density, and mobility patterns.

Another alternative approach is to participate into a dynamic mix-zone, e.g., [172]: each OBU is provided with a global symmetric key, using it to initiate a pseudonym change process. However, an internal attacker could terminate the encryption period on behalf of any vehicle; this impairs the functionality and operation of the scheme, thus eliminating user privacy protection. A dynamic cooperative location privacy protection scheme was proposed [132]: time-aligned pseudonyms are issued for all vehicles to facilitate synchronous pseudonym changes. Upon reaching a pseudonym transition process, a dynamic mix-zone formation is initiated by a vehicle and all CAMs within each mix-zone is encrypted using a distinct symmetric session key [132]. However, in a low traffic density area where there are very few vehicles to cooperatively change pseudonyms, vehicles could be semantically linkable. Unlike such schemes, our system ensures that user privacy is strongly protected even in situations with inherently low traffic density, e.g., suburban areas, and during low traffic periods.

MobiMix [174, 175] shows that an adversary could infer user-sensitive information based on the vehicle population in a mix-zone, the statistical behavior of the population, and the geometry of a mix-zone. To mitigate such inferences, it is

proposed to dynamically adjust the geometry of a mix-zone based on multiple factors, e.g., the statistical behavior and the movement patterns of the users. But, an adversary could still perform semantic linking attacks when the traffic density is sparse [176]. Swing & Swap [177] and MixGroup [162] propose to construct a region in which vehicles exchange their pseudonyms (and the corresponding private keys). But, such schemes do not achieve liability attribution and non-repudiation, which are basic requirements for a secure VC system [6, 15, 25, 89].

2.4 Other VC-Related Works

Detection and eviction of a misbehaving vehicle from the VC systems are important for vehicular security and safety. Appropriate mechanisms should be put in place to monitor the behavior of nodes, report misbehaving actions, evict a wrongdoer, and distribute CRLs among the registered nodes, to ensure the efficiency, reliability and robustness of the VC system. Centralized detection and dissemination of CRLs is proposed [71, 72, 120, 121], leveraging fixed infrastructure or car-to-car epidemic distribution; on the contrary, [111, 140] propose decentralized detection and eviction protocols to protect the VC systems against misbehaving nodes until they are fully evicted from the system. The appropriate choice to identify the source of abuse, and accordingly report it, is orthogonal to our investigation and we assume that there is an event that triggers the revocation operations. Further discussion is outside the sphere of reference.

In the absence of a pervasive trusted infrastructure, as is the case in VC systems, an adversary could disrupt the operations of location-aware applications relying on the position of a node and its neighbors, e.g., disrupting vehicular traffic by relaying counterfeit positions for an accident [178]. The main challenge is to identify neighbors securely, i.e., discovery of devices located in ‘‘close’’ (physical) proximity in a way that they can directly communicate with each other. Even though cryptographic operations would ensure the authenticity of origin, there is no guarantee about the physical layer of communication [178, 179]. A fully distributed lightweight framework for discovery and verification of neighbor positions is proposed [180]: any node can anonymously identify and verify its neighbors without an omnipresent trusted infrastructure or a priori established trust. Further discussion is outside the extent of this thesis.

Routing in VC systems is based on geographical addressing (Geocast), i.e., the dissemination of beacons or event-driven messages in a certain geographical region [181]. Vehicles distribute data packets bidirectionally over a single hop or multiple wireless hops. Similar to any system based on routing, adversaries could deviate from system security policies, thus deteriorating routing performance. For example, an external adversary could replay valid packets or internal adversaries could falsely advertise their locations: these result in misleading other nodes into creating false location tables with the geographical positions of their neighbors. A detailed discussion on Geocast-specific attacks along with a framework for secure

Geocast routing in VC systems are available in [181]. Further discussion on such aspects, e.g., [182], is beyond the scope of this thesis.

The openness of VC systems renders them vulnerable to *pollution* attacks: malicious insiders, i.e., compromised, faulty, or *''naughty''* vehicles, could inject faked messages, e.g., safety warnings and traffic information updates, thus jeopardizing data correctness or consistency and degrading the reliability and robustness of the system. This mainly stems from the fact that vehicles would simply trust data according to traditional notion of trust, i.e., node-centric trust establishment. Instead of trusting to a node per se, which is necessary but insufficient, [183] proposes a framework for data-centric trust establishment in which the *''trustworthiness attributed to node-reported data''*. Thus, the trustworthiness of an event, e.g, a weather report, is measured by different techniques, e.g., voting. This, also investigated in the context of participatory sensing [184, 185, 186], is orthogonal to our investigation and further discussion is beyond the scope of this thesis.

Service-oriented vehicular networks aim at providing multi-service environment to bring forth a number of customer benefits closer to a market-centric VC deployment [67] to achieve better return on investment. By leveraging the concepts of *Car as a Platform* and *Mobility as a Service*, the envisioned vehicular ecosystem will facilitate a gamut of services ranging from Internet access and infotainment services [5] (e.g., finding a restaurant or available parking lot in Location Based Services (LBSs) [12, 40, 187, 188, 189, 190, 191]) to VSN [13, 192, 193] (e.g., photo, video and audio sharing), content distribution [194] (e.g., video streaming, downloading maps and multimedia files), and *''Vehicular-Application Store''* [195, 196] (e.g., E-hailing). In the context of this thesis, we primarily focus on the identity and credential management infrastructure, i.e., the VPKI, as the principal building block of ITSs. Further discussion on a specific application or a service is orthogonal to our investigation.

Chapter 3

Secure and Privacy-Preserving Vehicular Communication Systems: Requirements and Adversaries

The security and privacy requirements for the V2X communications have been extensively specified in the literature, e.g., as early as [25]; at the same time, the adversarial models have been described. In the context of this thesis, we only focus on the security and privacy requirements on vehicle-VPKI interactions, intra-VPKI actions, and the relevant requirements. In addition, we consider the VPKI entities to be not fully-trusted, in particular *honest-but-curious*.

3.1 Identity and Credential Management

Requirements

The security and privacy requirements for identity and credential management are as follows:

- *R1.1 Authentication and communication integrity, and confidentiality:* All vehicle-VPKI interactions should be authenticated, i.e., both interacting entities should corroborate the sender of a message and the liveness of the sender and the message (i.e., towards mitigating replay attacks). We further need to ensure communication integrity, i.e., that exchanged messages are protected from any alternation. To provide confidentiality, the content of sensitive information, e.g., exchanged messages between a vehicle and a VPKI entity to obtain pseudonyms, should be kept secret from other entities.

- *R1.2 Authorization and access control:* Only legitimate, i.e., registered, and authenticated vehicles should be serviced by the VPKI, notably obtain pseu-

donyms. Moreover, vehicles should interact with the VPKI entities according to the system protocols and policies, and domain regulations.

- *R1.3 Non-repudiation, accountability and eviction (revocation):* All relevant operation and interactions with the VPKI entities should be non-repudiable, i.e., no entity should be able to deny having sent a message. Moreover, all legitimate system entities, i.e., registered vehicles, as well as VPKI entities, should be accountable for their actions that could interrupt the operation of the VPKI or harm the vehicles. In case of any deviation from system policies, the misbehaving entities should be evicted from the system.

- *R1.4 Privacy (anonymity and unlinkability):* Vehicles should participate in the VC system *anonymously*, i.e., vehicles should communicate with others without revealing their long-term identifiers and credentials. Anonymity is conditional in the sense that the corresponding long-term identity can be retrieved by the VPKI entities, and accordingly revoked, if a vehicle deviates from system policies, e.g., submitting faulty information.

  In order to achieve *unlinkability*, the real identity of a vehicle should not be linked to its corresponding pseudonyms; in other words, the LTCA, should know neither the targeted PCA nor the actual pseudonym acquisition periods, nor the credentials themselves. Moreover, successive pseudonym requests should not be linked to the same requester and to each other. The PCA should not be able to retrieve the long-term identity of any requester, or link successive pseudonym requests (of the same requester). Furthermore, an external observer should not be able to link pseudonyms of a specific vehicle based on information they carry, notably their timing information[1]. In order to achieve *full unlinkability*, which results in perfect forward privacy, no single entity (even the PCA) should be able to link a set of pseudonyms issued for a vehicle as a response to a single request.

  The level of anonymity and unlinkability is highly dependent on the *anonymity set*, i.e., the number of active participants and the resultant number of requests to obtain pseudonyms, e.g., all vehicles serviced by one PCA; because pseudonyms carry the issuer information, the VPKI should enhance user privacy by rendering any inference (towards linking, thus tracking, vehicles) hard.

- *R1.5 Thwarting Sybil-based attacks:* At no point in time should any vehicle be able to obtain multiple simultaneously valid pseudonyms.

- *R1.6 Availability:* The VPKI should remain operational in the face of benign failures (system faults or crashes) and be resilient to resource depletion attacks, e.g., Distributed DoS (DDoS) attacks.

[1] This does not relate to location information that vehicular communication messages, time- and geo-stamped signed under specific pseudonyms, carry.

Adversarial Model

In the context of this thesis, we only consider adversaries for vehicle-VPKI interactions and intra-VPKI operations. In the VC systems, internal adversaries, i.e., registered-but-malicious (compromised or faulty) clients, raise two challenges: (i) they could obtain multiple simultaneously valid pseudonyms, thus misbehaving each as multiple registered legitimate-looking vehicles; (ii) they could degrade the operations of the system by mounting a clogging DoS attack against the VPKI servers. We assume that a (in principle small) fraction of the vehicles could be compromised and not yet evicted at any point in time. External adversaries can harm the system operations by launching a DoS (or a DDoS) attack to degrade the availability of the system. But they are unable to successfully forge messages or 'crack' the employed cryptosystems and cryptographic primitives.

Similar to any networked system, adversarial behavior is not limited to the clients; the back-end security infrastructure components, i.e., the VPKI entities, could misbehave too. We assume that the VPKI components are *honest-but-curious*: such entities are *honest*, i.e., thoroughly comply with the best practices, specified protocols, and system policies, but they are *curious*, i.e., they function towards collecting or inferring user sensitive information based on the execution of the protocols, thus harming user privacy[2]. Multiple VPKI entities could collude, i.e., share information that each of them individually obtains from the protocol execution with others, to harm user privacy.

3.2 Certificate Revocation List Distribution

Requirements

- *R2.1 Fine-grained authentication, integrity, and non-repudiation:* Each CRL (piece) should be authenticated and its integrity be protected, i.e., preventing alternation or replays. Moreover, each CRL (piece) should be non-repudiably connected to its originator (the VPKI entity).
- *R2.2 Unlinkability (perfect-forward-privacy):* CRLs should not enable any observer (even in collusion with a single VPKI entity) to link pseudonyms (and thus the corresponding signed messages) prior to their revocation. In fact, upon a revocation event, all non-revoked previously expired pseudonyms of an evicted vehicle should remain unlinkable.
- *R2.3 Availability:* The system should ensure any legitimate vehicle can obtain the latest CRL within a reasonable time interval despite of benign failures, e.g., system faults or crashes, or network outages, e.g., intermittent connectivity. Moreover, the system should be resilient to active disruptions, including resource depletion attacks.

[2]This model could be extended to the case that such inferences are combined with extra information derived from transcript of pseudonymously signed messages.

- *R2.4 Efficiency:* Generating, validating, and disseminating the CRL (pieces) and revocation event notification should be efficient and scalable even if the number of vehicles and credentials grow, i.e., incurring low computation and communication overhead. Moreover, a small fraction of bandwidth should be used for CRL distribution, in order not to interfere with transportation safety- and time-critical operations. However, allocation of a small amount of bandwidth in a timely fashion should be sufficient to distribute CRLs to all legitimate vehicles.

- *R2.5 Explicit and/or implicit notification on revocation events:* The system should notify, explicitly or implicitly, every legitimate vehicle within the system (domain) regarding revocation events and then CRL-updates (availability of new revocation information).

Adversarial Model

We extend the general adversary model in secure vehicular communications [25] to include VPKI entities that are *honest-but-curious*, i.e., entities complying with security protocols and policies, but motivated to profile users. In a VC environment, internal adversaries, i.e., malicious, compromised, or non-cooperative clients, and external adversaries, i.e., unauthorized entities, raise four challenges. More specifically in the context of this work, adversaries can try to (i) exclude revoked pseudonym serial numbers from a CRL, (ii) add valid pseudonyms by forging a fake CRL (piece), or (iii) prevent legitimate entities from obtaining genuine and the most up-to-date CRL (pieces), or delay the CRL distribution by replaying old, spreading fake CRL (pieces), or performing a DoS attack. This allows wrong-doers to remain operational in the VC system using their current revoked pseudonym sets. Moreover, they might be simply non-cooperative or malicious, tempted to prevent other vehicles from receiving a notification on a new CRL-update event, thus preventing them from requesting to download the CRLs. Lastly, (iv) VPKI entities (in collusion with vehicle communication observers) could potentially link messages signed under (non-revoked but expired) pseudonyms prior to the revocation events, e.g., inferring sensitive information from the CRLs towards linking pseudonyms, and thus tracking vehicles backwards. The PCAs operating in a domain (or across domains) could also collude, i.e., share information that each of them individually has, to harm user privacy.

3.3 Location Privacy Protection

Requirements

- *R3.1 Privacy (anonymity and unlinkability):* Vehicles should participate in the VC system *anonymously*, i.e., vehicles should communicate with others without revealing their long-term identifiers and credentials. Anonymity is conditional

in the sense that the corresponding long-term identity can be retrieved by the VPKI entities, and accordingly, the long-term credential revoked if vehicles deviate from system policies. In order to achieve *unlinkability*, we need to diminish the inference by an eavesdropper upon pseudonym change, i.e., mitigating syntactic and semantic linking attacks.

- *R3.2 Availability:* The system should ensure any legitimate vehicle is notified about CMIX parameters, e.g., the location, geometry, and the symmetric key corresponding to an approaching mix-zone, to facilitate their participate in the mix-zone. Moreover, a small fraction of bandwidth should be used for the distribution of mix-zone related material, to not interfere with the safety- and time-critical operations.

- *R3.3 Auditability and misbehavior detection:* In case of any deviation, the system should be able to initiate a (resolution) process to identify the misbehaving entity. This essentially allows an RSU to interact with the VPKI system towards detecting misbehavior. Depending on the situation, appropriate actions could be initiated, e.g., de-anonymizing the misbehaving entity, and/or revoking its cryptographic materials and evicting it from further accessing the system.

- *R3.4 Efficiency and scalability:* All mix-zone operations should be efficient and scale with the number of vehicles. The scalability results from fast generation and lightweight dissemination of the credentials, efficient operations, and fault-tolerant design to ensure that the system remains operational in the presence of benign failures or be resilient to resource depletion attacks.

Adversarial Model

We consider the general adversary model in [15, 25] for secure and privacy-preserving VC systems and more specifically the adversarial model assumptions of CMIX schemes [113, 131, 160, 161, 162] that consider external eavesdroppers, possibly with broad or global coverage range. Along these lines, we assume that RSUs and participating users/vehicles are honest. We consider external adversaries with wireless receivers placed near each mix-zone, to eavesdrop VC systems to infer user-sensitive information towards harming user privacy. They passively eavesdrop communication of vehicles entering and exiting the mix-zone, covering all entry and exit points of the mix-zones, towards linking pseudonyms before and after a mix-zone. This is based on information derived from CAMs, e.g., timing, velocity, and location. We do not constrain the choice and design of the inference algorithm, i.e., a tracking algorithm to link two pseudonyms of a vehicle, prior to and after pseudonym change in a mix-zone. Rather, in order to achieve tangible results, we devise a tracking algorithm (see Sec. 4.3), orthogonal to the defense mechanism.

In addition, we explore the consequences of strengthening the adversarial model. In particular, we consider (i) RSUs and VPKI entities that are *honest-but-curious*,

i.e., entities complying with security protocols and policies, but motivated to profile users by collecting or inferring user sensitive information based on the execution of the protocols. Moreover, (ii) the collaboration (collusion) of honest-but-curious entities that share information individually inferred by each. Finally, we consider (iii) a set of non-cooperative actions by registered vehicles that can affect the operation (or level) of protection of the scheme (and any CMIX scheme).

Extending the passive eavesdropper model: We focus on the effect and improvement of the CMIX approach. The investigation can be extended to the entire network, considering the optimal placement of eavesdroppers, increasing their coverage, and overall pseudonym usage. The adversarial model can be further strengthened if internal adversaries, including the non-cooperative vehicles joining the mix-zone, report the symmetric keys of the mix-zones and the observed communication to an external adversary (collection point). For example, an RSU could share a transcript of pseudonymously authenticated messages with an honest-but-curious VPKI entity to perform syntactic and semantic linking attacks. However, this adversarial model is beyond the scope of this investigation.

Chapter 4

Addressing Challenges

4.1 Identity and Credential Management Infrastructure for VANETs

We assume that a VPKI consists of a set of authorities with distinct roles: the RCA, the highest level authority, certifies other lower level authorities; the LTCA is the responsible entity for vehicle registration and LTC (X.509 certificate [197]) issuance; the PCA issues pseudonyms for the registered vehicles; and the RA is able to initiate a process to resolve a pseudonym, thus identifying the long-term identity of a vehicle used that pseudonym. We assume that each *domain* [46] is governed by only one LTCA, namely Home-LTCA (H-LTCA), while there are multiple PCAs operating in one or multiple domains. We further assume that each vehicle is only registered to its *H-LTCA* which is reachable by the registered vehicles in its domain and it can obtain pseudonyms from any PCA (as long as there is trust established between them). Trust between two domains can be established with the help of a higher-level authority, i.e., the RCA, or through cross certification between them. Each vehicle, depending on the policies and rules, can cross to other *foreign*[1] domains and communicate with the *Foreign-LTCA (F-LTCA)* in that foreign domain to obtain pseudonyms. The certificates of higher-level authorities are installed on the OBUs or the OBUs can obtain them in a secure manner; moreover, the OBUs are loosely synchronized with the VPKI servers. All vehicles registered in the system are provided with a HSM, providing a secure storage while ensuring proper operations of cryptographic algorithms. This ensures that private keys never leave the HSM and an adversary cannot inject fake future timestamps to mislead the recipients.

[1]The notion of ''foreign'' (pseudonym) was first introduced in [120] in the context of VC systems.

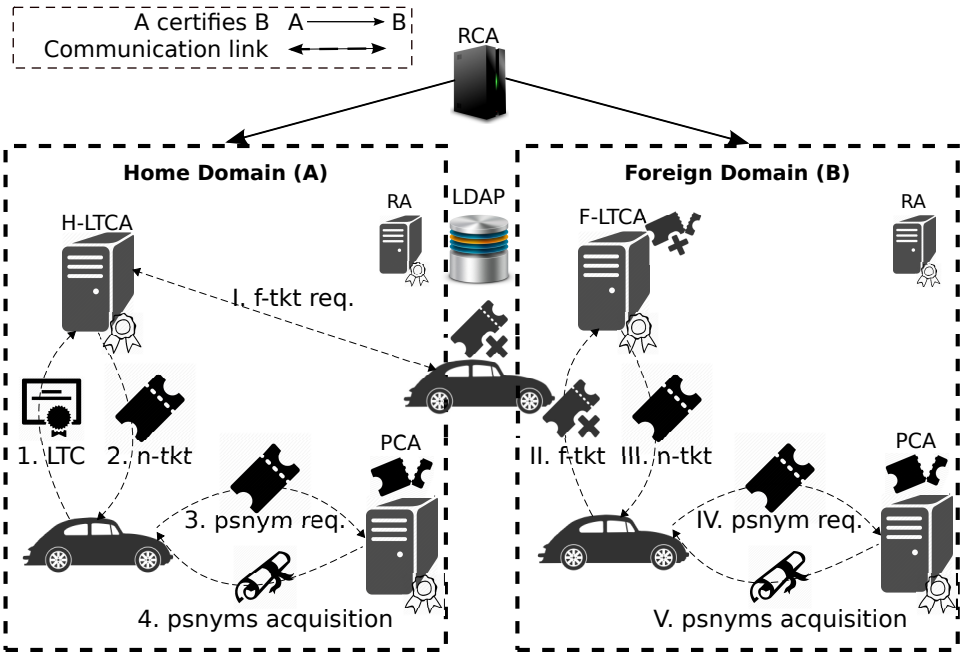


Figure 4.1: Pseudonym Acquisition Overview in the Home and Foreign Domains [taken from [35]].

System Overview

Fig. 4.1 illustrates pseudonym acquisition overview of our VPKI in a home domain (A) and a foreign domain (B). In the registration phase, each H-LTCA registers vehicles within its domain and maintains their long-term identities. At the bootstrapping phase, each vehicle needs to discover the VPKI-related information, e.g., the available PCAs in its home domain, or the desired F-LTCA and PCAs in a foreign domain, along with their corresponding certificates. To facilitate the overall intra-domain and multi-domain operations, a vehicle first finds such information from a Lightweight Directory Access Protocol (LDAP) [198] server. This is carried out without disclosing the real identity of the vehicle. The vehicle, i.e., the OBU, ‘‘decides’’ when to trigger the pseudonym acquisition process based on different parameters, e.g., the number of remaining valid pseudonyms, the residual trip duration, and the networking connectivity [58]. We presume connectivity to the VPKI (e.g., via RSUs); should the connectivity be intermittent, the OBU could initiate pseudonym provisioning proactively when there is connectivity.

The H-LTCA authenticates and authorizes vehicles, which authenticate the H-LTCA over a unidirectional (server-only) authenticated Transport Layer Security (TLS) [199] tunnel. This way the vehicle obtains a *native ticket* (*n-tkt*) from its H-LTCA while the targeted PCA or the actual pseudonym acquisition period is

Table 4.1: Notation used in the protocols.

$(P_v^i)_{PCA}$, P_v^i	current valid pseudonym signed by the PCA
(LK_v, Lk_v)	long-term public & private key pairs
(K_v^i, k_v^i)	pseudonymous public/private key pairs, corresponding to current valid pseudonym
Id_{req}, Id_{res}	request/response identifiers
Id_{CA}	Certification Authority unique identifier
$(msg)_{\sigma_v}$	a signed message with the vehicle's private key
N	nonce
t_{now}, t_s, t_e	fresh/current, starting, and ending timestamps
t_{date}	timestamps of a specific day
$n\text{-}tkt$, $(n\text{-}tkt)_{\text{LTCA}}$	native ticket
$f\text{-}tkt$, $(n\text{-}tkt)_{\text{LTCA}}$	foreign ticket
SN	serial number
Exp_{tkt}	ticket expiration time
$H()$	hash function
$Sign(Lk_{ca}, msg)$	signing a message with private key (Lk) of the CA
$Verify(LTC_{ca}, msg)$	verifying with the CA's public key
IK	identifiable key
V	vehicle
ζ, χ, ξ	temporary variables

hidden from the H-LTCA; the ticket is anonymized and it does not reveal its owner's identity (Protocol 1 in Sec. 4.1). The ticket is then presented to the intended PCA, over a unidirectional (server-only) authenticated TLS, for the vehicle to obtain pseudonyms (Protocol 2 in Sec. 4.1).

When the vehicle travels in a foreign domain, it should obtain new pseudonyms from a PCA operating in that domain; otherwise, the vehicle would stand out with pseudonyms issued by another PCA. The vehicle first requests a *foreign ticket* ($f\text{-}tkt$) from its H-LTCA (without revealing its targeted F-LTCA) so that the vehicle can be authenticated and authorized by the F-LTCA. In turn, the F-LTCA provides the vehicle with a new ticket ($n\text{-}tkt$), which is native within the domain of the F-LTCA to be used for pseudonym acquisition in that (foreign) domain. The vehicle then interacts with its desired PCA to obtain pseudonyms. Obtaining an $f\text{-}tkt$ is transparent to the H-LTCA: the H-LTCA cannot distinguish between native and foreign ticket requests. This way, the PCA in the foreign domain cannot distinguish native requesters from the foreign ones. For liability attribution, our scheme enables the RA, with the help of the PCA and the LTCA, to initiate a resolution process, i.e., to resolve a pseudonym to its long-term identity. Each vehicle can interact with any PCA, within its home or a foreign domain, to fetch the CRL [197] and perform OCSP [200] operations, authenticated with a current valid pseudonym. The notation used in the protocols is given in Table 4.1.

Protocol 1 Ticket Provisioning from the H-LTCA

$$V: \textbf{P1: } (t_s, t_e) \leftarrow (t_s, t_e) \tag{4.1}$$
$$\textbf{P2: } (t_s, t_e) \leftarrow (t_s, \Gamma_{P2}) \tag{4.2}$$
$$\textbf{P3: } (t_s, t_e) \leftarrow (t_{date} + \Gamma^{i}_{P3}, t_{date} + \Gamma^{i+1}_{P3}) \tag{4.3}$$
$$V: \zeta \leftarrow (Id_{req}, H(Id_{pca} \| Rnd_{n\text{-}tkt}), t_s, t_e) \tag{4.4}$$
$$V: (\zeta)_{\sigma_v} \leftarrow Sign(Lk_v, \zeta) \tag{4.5}$$
$$V \rightarrow H\text{-LTCA}: ((\zeta)_{\sigma_v}, \text{LTC}_v, N, t_{now}) \tag{4.6}$$
$$H\text{-LTCA}: \text{Verify}(\text{LTC}_v, (\zeta)_{\sigma_v}) \tag{4.7}$$
$$H\text{-LTCA}: IK_{n\text{-}tkt} \leftarrow H(\text{LTC}_v || t_s || t_e || Rnd_{IK_{n\text{-}tkt}}) \tag{4.8}$$
$$H\text{-LTCA}: \chi \leftarrow (H(Id_{pca} \| Rnd_{n\text{-}tkt}), IK_{n\text{-}tkt}, t_s, t_e) \tag{4.9}$$
$$H\text{-LTCA}: (n\text{-}tkt)_{\sigma_{h\text{-}ltca}} \leftarrow Sign(Lk_{h\text{-}ltca}, \chi) \tag{4.10}$$
$$V \leftarrow H\text{-LTCA}: (Id_{res}, (n\text{-}tkt)_{\sigma_{h\text{-}ltca}}, Rnd_{IK_{n\text{-}tkt}}, N{+}1, t_{now}) \tag{4.11}$$
$$V: \text{Verify}(LTC_{h\text{-}ltca}, (n\text{-}tkt)_{\sigma_{h\text{-}ltca}}) \tag{4.12}$$
$$V: H(\text{LTC}_v || t_s || t_e || Rnd_{IK_{n\text{-}tkt}}) \stackrel{?}{=} IK_{n\text{-}tkt} \tag{4.13}$$

VPKI Services and Security Protocols

In this section, we provide the detailed description of the protocols to obtain pseudonyms in a home domain. The detailed description of protocols to resolve and revoke a pseudonym can be found [35].

Ticket Acquisition in the Home Domain (Protocol 1): The vehicle prepares a request and calculates the hash value of the concatenation of its desired PCA identity and a random number, i.e., $H(Id_{PCA} \| Rnd_{n\text{-}tkt})$ (step 4.1). This conceals the targeted PCA and the actual pseudonym acquisition periods from the LTCA. In case of cross-domain operation, the vehicle interacts with the H-LTCA to obtain an *f-tkt* and it concatenates its targeted F-LTCA (instead of the desired PCA) and a random number. The vehicle then signs the request (step 4.2) and sends it to its H-LTCA to obtain an *n-tkt* (step 4.3). Upon a successful validation of the LTC and verification of the request (step 4.4), the H-LTCA generates the *''ticket identifiable key''* ($IK_{n\text{-}tkt}$) to bind the ticket to the LTC: $H(\text{LTC}_v || t_s || t_e || Rnd_{IK_{n\text{-}tkt}})$ (steps 4.5); this prevents the H-LTCA from mapping the ticket to a different LTC during resolution process. The H-LTCA then issues an anonymous ticket, $(n\text{-}tkt)_{\sigma_{h\text{-}ltca}}$ (step 4.6–4.7) and delivers it to the vehicle (step 4.8). Finally, the vehicle verifies the ticket and $IK_{n\text{-}tkt}$ (steps 4.9–4.10).

Pseudonym Acquisition (Protocol 2): With an *n-tkt* at hand, the vehicle interacts with the targeted PCA to obtain pseudonyms. The vehicle initiates a protocol to generate the required ECDSA public/private key pairs (which could be generated off-line) and sends a request to the PCA (steps 4.1–4.2). Upon reception and successful ticket verification (steps 4.3–4.4), the PCA verifies the targeted PCA (step 4.5), and whether or not the actual period of requested pseudonyms falls within the period specified in the ticket, i.e., $[t'_s,\ t'_e] \subseteq ([t_s, t_e])_{n\text{-}tkt}$ (step 4.6).

Protocol 2 Pseudonym Provisioning from the PCA

$$V : \zeta \leftarrow (Id_{req}, Rnd_{n\text{-}tkt}, t'_s, t'_e, (n\text{-}tkt)_{\sigma_{h\text{-}ltca}}, \{(K_v^1)_{\sigma_{k_v^1}}, \ldots, (K_v^n)_{\sigma_{k_v^n}}\}, N, t_{now}) \quad (4.1)$$

$$V \rightarrow \text{PCA} : (\zeta) \quad (4.2)$$

$$\text{PCA} : \text{Verify}(LTC_{ltca}, (n\text{-}tkt)_{\sigma_{ltca}}) \quad (4.3)$$

$$\text{PCA} : H(Id_{this\text{-}pca} \| Rnd_{n\text{-}tkt}) \stackrel{?}{=} H(Id_{pca} \| Rnd_{n\text{-}tkt}) \quad (4.4)$$

$$\text{PCA} : \textbf{P1 or P2: } [t'_s,\ t'_e] \stackrel{?}{\subseteq} ([t_s, t_e])_{n\text{-}tkt} \quad (4.5)$$

$$\textbf{P3: } [t'_s,\ t'_e] \stackrel{?}{=} ([t_s, t_e])_{n\text{-}tkt} \quad (4.6)$$

$$\text{PCA} : \textbf{for } \text{i} \leftarrow 1, n \textbf{ do} \quad (4.7)$$

$$\text{PCA} : \quad \text{Verify}(K_v^i, (K_v^i)_{\sigma_{k_v^i}}) \quad (4.8)$$

$$\text{PCA} : \quad IK_{P_v^i} \leftarrow H(IK_{n\text{-}tkt} || K_v^i || t_s^i || t_e^i || Rnd_{IK_{P_v^i}}) \quad (4.9)$$

$$\text{PCA} : \quad \xi \leftarrow (K_v^i, IK_{P_v^i}, t_s^i, t_e^i) \quad (4.10)$$

$$\text{PCA} : \quad (P_v^i)_{\sigma_{pca}} \leftarrow Sign(Lk_{pca}, \xi) \quad (4.11)$$

$$\text{PCA} : \textbf{end for} \quad (4.12)$$

$$V \leftarrow \text{PCA} : (Id_{res}, \{(P_v^1)_{\sigma_{pca}}, \ldots, (P_v^n)_{\sigma_{pca}}\}, \{Rnd_{IK_{P_v^1}}, \ldots, Rnd_{IK_{P_v^n}}\}, N{+}1, t_{now}) \quad (4.13)$$

$$V : \textbf{for } \text{i} \leftarrow 1, n \textbf{ do} \quad (4.14)$$

$$V : \quad \text{Verify}(LTC_{pca}, P_v^i) \quad (4.15)$$

$$V : \quad H(IK_{n\text{-}tkt} || K_v^i || t_s^i || t_e^i || Rnd_{IK_{P_v^i}}) \stackrel{?}{=} IK_{P_v^i} \quad (4.16)$$

$$V : \textbf{end for} \quad (4.17)$$

Then, the PCA initiates a proof-of-possession protocol to verify the ownership of the corresponding private keys, k_v^i. The PCA generates the *''pseudonym identifiable key''* ($IK_{P_v^i}$) to bind the pseudonyms to the ticket; this prevents the compromised (malicious) PCA from mapping the pseudonyms to a different ticket during the resolution process. It then issues the pseudonyms (steps 4.7–4.12), and delivers the response (step 4.13). Finally, the vehicle verifies the pseudonyms and $IK_{P_v^i}$ (steps 4.14–4.17).

Security and Privacy Analysis

We analyze the achieved security and privacy of our VPKI with respect to the requirements presented in Sec. 3.1. All the communication runs over secure channels, i.e., TLS with unidirectional authentication, thus we achieve *authentication, communication integrity* and *confidentiality* (R1.1 in Sec. 3.1). The H-LTCA authenticates and authorizes the vehicles based on the registration and their revocation status, and makes appropriate decisions. It grants a *service-granting ticket*, thus enabling the

vehicles to request pseudonyms from any PCA by presenting its anonymous ticket. The PCA then grants the service, based on prior established trust, by validating the ticket (R1.2 in Sec. 3.1). Given the ticket acquisition request is signed with the private key corresponding to the vehicle's LTC and pseudonym acquisition entails a valid ticket, the system provides *non-repudiation and accountability* (R1.3 in Sec. 3.1). Moreover, the LTCA and the PCA calculate ticket and pseudonym identifiable keys (IK_{tkt} and IK_P) to bind them to the corresponding LTC and ticket respectively (R1.3 in Sec. 3.1).

According to the protocol design, the vehicle conceals the identity of its targeted PCA with $H(Id_{PCA}||Rnd_{n\text{-}tkt})$, and the targeted F-LTCA when operating in a foreign domain. The vehicle hides the actual pseudonym acquisition periods, i.e. $[t'_s,\ t'_e]$, while only $[t_s,\ t_e]$ is revealed to the LTCA. We further propose a policy in [58] for the PCA to issue time-aligned pseudonyms for all vehicles so that timing information cannot be used to link two successive pseudonyms as they are time-aligned with those of all other active vehicles that obtain pseudonyms by the same PCA. Thus timing information does not degrade user privacy (R1.4 in Sec. 3.1). This is further discussed in [35, 58]. Moreover, the separation of duties between the LTCA and the PCA provides *conditional anonymity*, but revoked under special circumstances, e.g., misbehavior (R1.3 in Sec. 3.1).

The H-LTCA enforces a policy that each vehicle cannot obtain tickets with overlapping lifetime: upon receiving a request, the H-LTCA checks if a ticket was issued for the requester during that period. This ensures that no vehicle can obtain more than a single valid ticket to request multiple simultaneously valid pseudonyms. Moreover, a ticket is implicitly bound to a specific PCA; thus, it cannot be used more than once or be reused for other PCAs. The PCA also issues the pseudonyms with non-overlapping lifetimes; all in all, no vehicle can be provided with more than one valid pseudonym at any time; thus, Sybil-based misbehavior is thoroughly thwarted within a multi-domain VC environment (R1.5 in Sec. 3.1). We achieve availability in the face of a crash failure by mandating load-balancers and server redundancy [34]; in case of a DDoS attack, we use a puzzle technique [201] as a mitigation approach (R1.6 in Sec. 3.1), further discussed in [35]. For a detailed discussion on the security and privacy analysis, we refer readers to our publications [34, 35].

Performance Evaluation

We are primarily interested in evaluating the performance, i.e., scalability and efficiency, of the full-blown implementation of our VPKI. We allocate Virtual Machines (VMs) for distinct VPKI servers and clients (emulating OBUs). Our VPKI implementation is in C++ and we use OpenSSL for cryptographic protocols and primitives (ECDSA and TLS). We use ECDSA-256 public/private key pairs based on the standard [5, 6]. We run our experiments in a controlled environment which essentially eliminate the propagation delay on the vehicle-VPKI connectivity.

Table 4.2 details the specifications of the allocated VMs. Our setup considers two LTCAs, five PCAs and 25 VMs for the clients. 10K threads execute ticket

Table 4.2: Servers and Clients Specifications.

	LTCA	PCA	Clients
VM Number	2	5	25
Dual-core CPU (Ghz)	2.0	2.0	2.0
BogoMips	4000	4000	4000
Memory	2GB	2GB	1GB
Database	MySQL	MySQL	MySQL
Web Server	Apache	Apache	—
Load Balancer	Apache	Apache	—
Emulated Threads	—	—	400

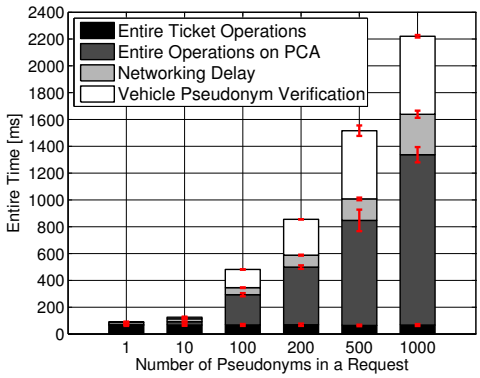


Figure 4.2: Client processing time [taken from [34]].

and pseudonym acquisitions (Protocol 1 and 2) on 25 VMs by sending requests to the VPKI entities frequently (every 10 minutes). We have to emphasize that the processing power of our emulating OBUs is comparable to the processing power of the Nexcom boxes (dual-core 1.66GHz, 2GB memory) in PRESERVE project [30] as we run 400 threads on each VM.

Fig. 4.2 depicts the latency for the pseudonym acquisition protocols (Protocol 1 and 2) for each individual component, i.e., ticket provisioning (end-to-end), pseudonym verification (by the client), pseudonym issuance (by the PCA), and network transmission latency. In our setup, we do not consider the processing time to generate the public/private key pairs on the client as they can be generated off-line. As the Fig. 4.2 shows, the end-to-end latency to obtain 100 pseudonyms is around 500 ms.

Fig. 4.3 shows the average response time for the LTCA to issue a ticket, approximately 5 ms, including request decapsulation, LTC verification, and response encapsulation. Fig. 4.4 shows the performance of the PCA issuing different numbers of pseudonyms for the requesters. For instance, the cumulative probability of latencies to issue 200 pseudonyms is: $F_x(t = 500) = 0.9$, or $Pr\{t \leq 500\} = 0.9$. The results confirm the scalability of our scheme as requesting more than 120 pseudonyms every 10 minutes is considered as an extreme case if we compare it with the C2C-CC proposal to use one pseudonym per day or per trip [16, 92]. It is

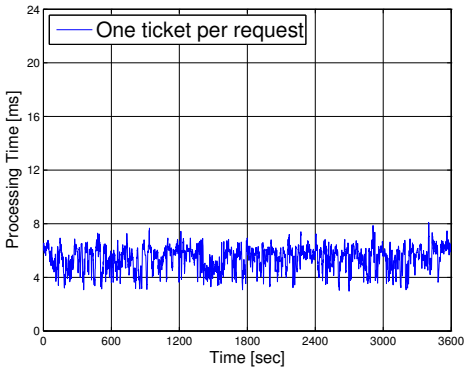


Figure 4.3: LTCA performance [taken from [34]].

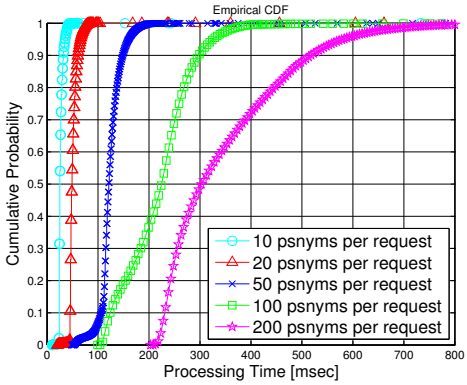


Figure 4.4: PCA performance [taken from [34]].

Table 4.3: Experiment Parameters.

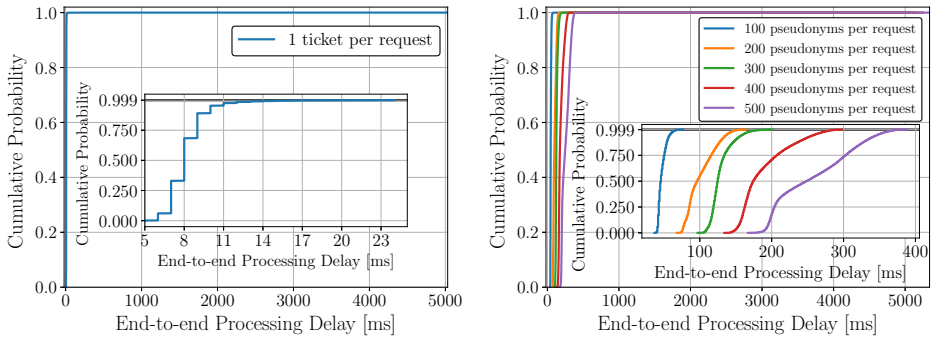
Parameters	Config-1	Config-2
total number of vehicles	1000	100, 50,000
hatch rate	1	1, 100
interval between requests	1000-5000 ms	1000-5000 ms
pseudonyms per request	100, 200, 300, 400, 500	100, 200, 500
LTCA memory request	128 MiB	128 MiB
LTCA memory limit	256 MiB	256 MiB
LTCA CPU request	500 m	500 m
LTCA CPU limit	1000 m	1000 m
LTCA HPA	1-40; CPU 60%	1-40; CPU 60%
PCA memory request	128 MiB	128 MiB
PCA memory limit	256 MiB	256 MiB
PCA CPU request	700 m	700 m
PCA CPU limit	1000 m	1000 m
PCA HPA	1-120; CPU 60%	1-120; CPU 60%

paramount to emphasize that by allocating modest VMs for the VPKI entities, we can provide very large number of clients with pseudonyms.

We provide an extensive evaluation of the overall system performance, i.e., efficiency, scalability, and robustness, of the full-blown implementation of our VPKI by leveraging two large-scale mobility traces [202, 203], and an evaluation of the resiliency of our scheme to DDoS attacks. Additional results are provided in [35, 58].

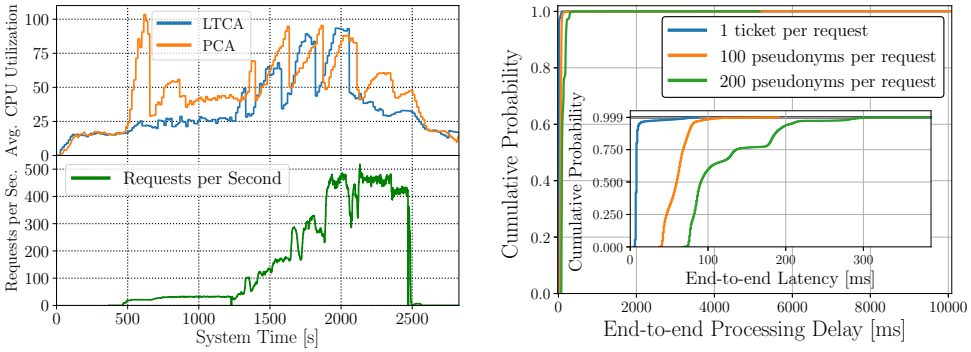
Large-scale Pseudonym Acquisition

Fig. 4.5.a illustrates the Cumulative Distribution Function (CDF) of the single ticket issuance processing delay (executed based on Config-1 in Table 4.3); as illustrated, 99.9% of ticket requests are served within 24 ms: $F_x(t = 24\,ms) = 0.999$, i.e.,



(a) Ticket Issuance (b) Pseudonyms Issuance

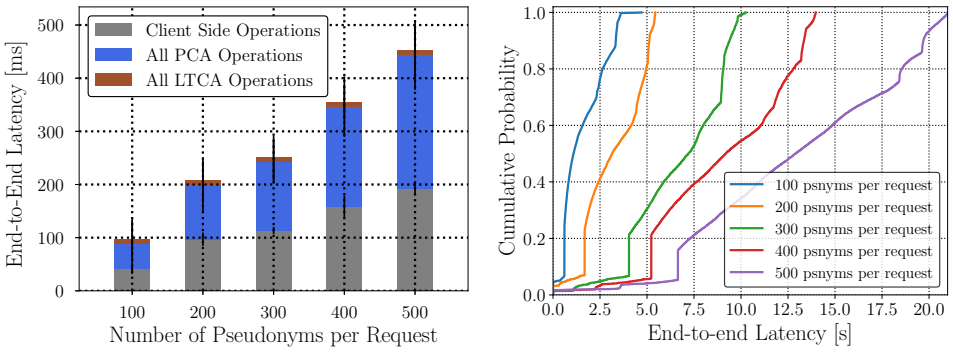
Figure 4.5: (a) CDF of end-to-end latency to issue a ticket. (b) CDF of end-to-end processing delay to issue pseudonyms. [taken from [87]].



(a) (b)

Figure 4.6: VPKIaaS system in a flash crowd load situation. (a) CPU utilization and the number of requests per second. (b) CDF of processing latency to issue tickets and pseudonyms. [taken from [87]].

$Pr\{t \leq 24\,ms\} = 0.999$. Fig. 4.5.b shows the CDF of processing latency for issuing pseudonyms with different batches of pseudonyms per request as a parameter. For example, with a batch of 100 pseudonyms per request, 99.9% of the vehicles are served within less than 77 ms ($F_x(t = 77\,ms) = 0.999$). Even with a batch of 500 pseudonyms per request, the VPKI as a Service (VPKIaaS) system can efficiently issue pseudonyms: $F_x(t = 388\,ms) = 0.999$. The results confirm that the VPKIaaS scheme is efficient and scalable: the pseudonym acquisition process incurs low latency and it efficiently issues pseudonyms for the requesters.



(a) (b)

Figure 4.7: VPKIaaS system with flash crowd load pattern. (a) Average end-to-end latency to obtain pseudonyms. (b) CDF of end-to-end latency, observed by clients. [taken from [87]].

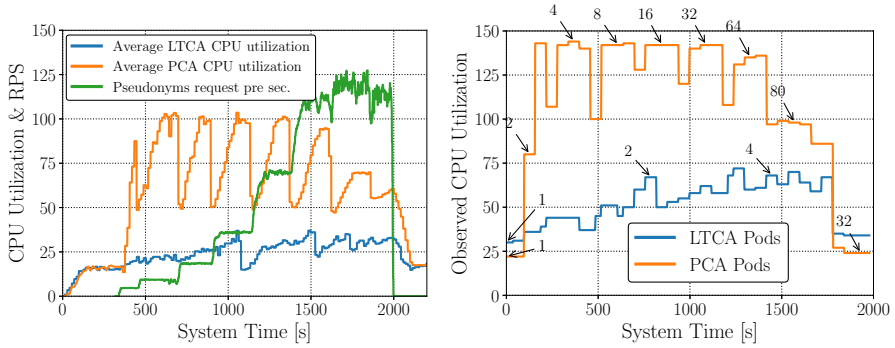
VPKIaaS with Flash Crowd Load Pattern

Fig. 4.6 shows the performance of the VPKIaaS when a surge in pseudonym acquisition requests happens to the VPKIaaS (executed based on Config-2 in Table 4.3, with 100 pseudonyms per request for Fig. 4.6.a). We assess CPU utilization of the LTCA and the PCA Pods (Fig. 4.6.a top) and the total number of pseudonyms requests per second (Fig. 4.6.a bottom). When the number of requests per second increases, the average CPU utilization would rise; however, when CPU utilization hits 60% threshold, defined in the Horizontal Pod Autoscalers (HPAs) [204], the LTCA and the PCA deployment would horizontally scale to handle demanding loads, thus the average CPU utilization drops upon scaling out.

Fig. 4.6.b shows the end-to-end processing latency to obtain tickets and a batch of 100 or 200 pseudonyms in a flash crowd situation. The processing latency to issue a single ticket is: $F_x(t = 87\,ms) = 0.999$; to issue a batch of 100 pseudonyms per request, the processing latency is: $F_x(t = 192\,ms) = 0.999$. In comparison with processing delay under 'normal' conditions (Fig. 4.5), the processing latency of issuing a single ticket increases from 24 ms to 87 ms; the processing latency to issue a batch of 100 pseudonyms increased from 77 ms to 192 ms. Thus, even under such a highly demanding request rate, the VPKIaaS system issues credentials efficiently.[2]

Fig. 4.7.a shows the latency for each system component to obtain different batches of pseudonyms per request (Config-2 in Table 4.3). Our VPKIaaS system

[2]The total number of vehicles requesting 100 pseudonyms (under Config-2 in Table 4.3) is 398,870 and the VPKIaaS system issued approximately 40 millions pseudonyms within 2,500 seconds; with such an arrival rate, the VPKIaaS system would issue 0.5×10^{12} pseudonyms per year. Obviously, this number is lower that the one mentioned in Sec. 1.2, i.e., 1.5×10^{12}. Note that this is a proof of concept of the implementation and evaluation of the VPKIaaS system; by allocating more resources and increasing the pseudonym request rates, the VPKIaaS system would issue even further pseudonyms.



(a) (b)

Figure 4.8: Each vehicle requests 500 pseudonyms (CPU utilization observed by HPA). (a) Number of active vehicles and CPU utilization. (b) Dynamic scalability of VPKIaaS system. [taken from [87]].

outperforms prior work [66]: the processing delay to issue 100 pseudonym for [66] is approx. 2000 ms, while it is approx. 56 ms in our system, i.e., achieving a 36-fold improvement over prior work [66]. Fig. 4.7.b illustrates the average end-to-end latency to obtain pseudonyms, observed by clients. As we can see, during a surge of requests, *all* vehicles obtained a batch of 100 pseudonyms within less than 4,900 ms (including the networking latency). Obviously, the shorter the pseudonym lifetime, the higher the workload on the VPKI, thus the higher the end-to-end latency. Note that serving requests under a flash crowd scenario at this rate (Config-2 in Table 4.3) implies that our VPKIaaS system would serve 720,000 vehicles joining the system within an hour. Thus, even under such flash crowd load pattern, our VPKIaaS system can comfortably handle such a high demand of requests.

Dynamic-scalability of the VPKIaaS

In this scenario, we demonstrate the performance of our VPKIaaS system, notably its reliability and dynamic scalability. To emulate a large volume of workload, we generated synthetic workload using 30 containers, each with 1 vCPU and 1GB of memory (executed based on Config-2 in Table 4.3). Fig. 4.8.a shows the average CPU utilizations of the LTCA and PCA Pods (observed by HPA) as well as the total number of requests per second. Fig. 4.8.b shows how our VPKIaaS system dynamically scales out or scales in according to the rate of pseudonyms requests. The numbers next to the arrows show the number of LTCA and PCA Pod replicas at any specific system time. As illustrated, the number of PCA Pods starts from 1 and it gradually increases; at system time 1500, there is a surge in pseudonym requests, thus the number of PCA Pods increased to 80. Note that issuing a ticket is more efficient than issuing pseudonyms; thus, the LTCA micro-service scaled out only up to 4 Pod replicas.

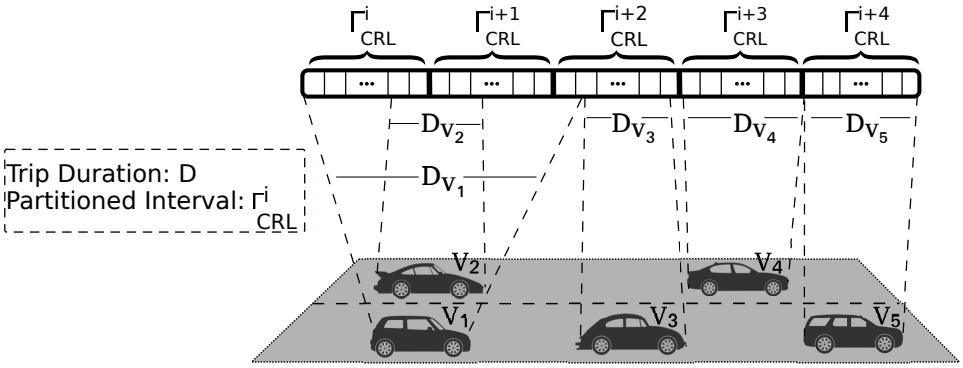


Figure 4.9: CRL as a Stream: V_1 subscribes to $\{\Gamma^{i}_{CRL}, \Gamma^{i+1}_{CRL}, \Gamma^{i+2}_{CRL}\}$; V_2 : $\{\Gamma^{i}_{CRL}, \Gamma^{i+1}_{CRL}\}$; $V_3 : \{\Gamma^{i+2}_{CRL}\}$; $V_4 : \{\Gamma^{i+3}_{CRL}\}$; and $V_5 : \{\Gamma^{i+4}_{CRL}\}$. [taken from [44]].

4.2 Certificate Revocation List Distribution in VANETs

High-level overview: The default policy is to distribute all revocation information to all vehicles. Nonetheless, this approach ignores the locality, the temporal nature of pseudonyms, and other constraints, e.g., the average daily commute time. Locality could be geographical, i.e., credentials relative to the corresponding region, and temporal, i.e., relevance to the lifetime of pseudonyms with respect to the trip duration of a vehicle. To efficiently, effectively, and timely distribute the CRLs across the V2X network, we propose making the CRL acquisition process *vehicle-centric*, i.e., through *a content-based and context-sensitive ''publish-subscribe''* scheme [205, 206].

Fig. 4.9 shows that by starting a new trip, each vehicle only subscribes to receive the pieces of CRLs, i.e., the content, corresponding to its actual trip duration and its targeted region, i.e., the context. To reap the benefits of the ephemeral nature pseudonyms and the timely-aligned pseudonym provisioning policy, towards an effective, efficient, and scalable CRL distribution, a fixed interval, Γ_{CRL}, is predetermined by the PCAs in the domain. They publicize revoked pseudonyms whose lifetimes fall within Γ_{CRL}, i.e., distributing only the serial number of these pseudonyms rather than publishing the entire CRL. Note that Γ, the universally fixed interval to obtain pseudonyms [35], and Γ_{CRL} are not necessarily aligned due to the unpredictable nature of revocation events.

When a vehicle reliably connects to the VPKI, it can obtain the *''necessary''* CRL pieces corresponding to its trip duration during the pseudonym acquisition phase. However, if reliable connectivity is not guaranteed, or if a vehicle obtained (possibly preloaded with enough) pseudonyms in advance, or a new revocation event happens, one can be notified about a new CRL-update (revocation) event: a signed fingerprint (a Bloom Filter (BF) [127, 128]) of CRL pieces is broadcasted by RSUs and it is integrated in a subset of recently issued pseudonyms, this way

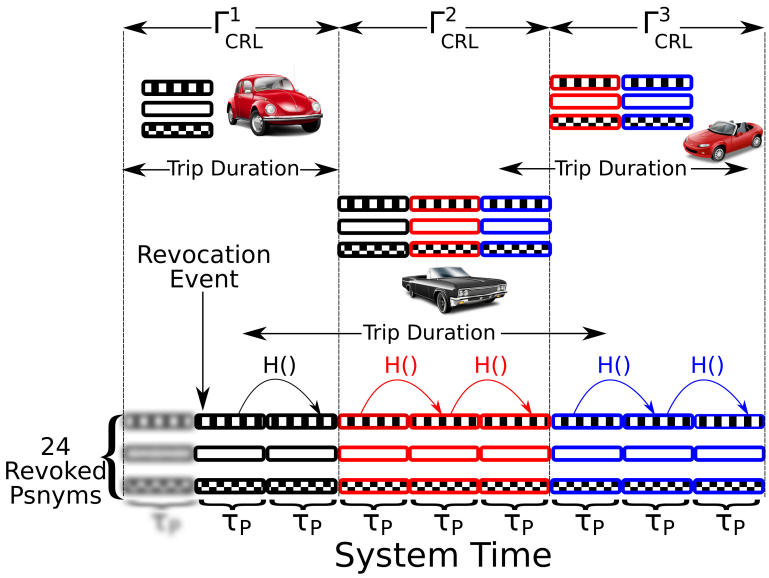


Figure 4.10: A vehicle-centric approach: each vehicle only subscribes for pieces of CRLs corresponding to its trip duration. [taken from [44, 45]].

readily broadcasted by vehicles (termed *fingerprint-carrier* nodes) along with their CAMs. This essentially piggybacks a notification about the latest CRL-update event and an authenticator for validating CRL pieces. This provides CRL validation for free: pseudonyms are readily validated by the receiving vehicles since each vehicle verifies the signature on a pseudonym before validating the content of a CAM, i.e., the verification of CRL pieces does not incur extra computation overhead. This eliminates the need for signature verification, but a BF membership test, for each CRL piece as the fingerprint is signed with the private key of the PCA.

Our scheme does not require prior knowledge on trip duration in order to obtain CRLs, i.e., a vehicle can be oblivious to the trip duration. In fact, such information would not be relevant to the CRL dissemination: due to the unpredictable nature of revocation events, the PCAs disseminate at each point revoked pseudonyms whose lifetimes fall within a Γ_{CRL} interval. As long as a vehicle moves inside a domain, it does not need to receive CRLs from other domains: all vehicles in the domain are issued pseudonyms by the PCAs in that domain. In other words, our scheme does not require any communication and cooperation between RSUs and PCAs from different domains on CRL construction and distribution tasks; only PCAs-RSUs collaboration within a domain. The PCAs operating in a domain construct the CRLs and push the CRL pieces to the RSUs so that the RSUs broadcast the CRL pieces for the current Γ_{CRL}.

Fig. 4.10 illustrates an example of 24 revoked pseudonyms to be distributed. A vehicle traveling within Γ^1_{CRL} would possibly only face revoked pseudonyms with a lifetime falling in that interval, 6 pseudonyms, shown in black, instead of all 24

entries (the blurred pseudonyms are expired, thus not included in the CRL). These 6 revoked pseudonyms within Γ^1_{CRL} can be implicitly bound without compromising their unlinkability prior to the revocation event, in a way that one can simply derive subsequent pseudonyms from an anchor (the blurred pseudonyms are non-revoked but expired and they cannot be linked to the revoked ones; this becomes clear later). Thus, in this example, distributing 3 entries for that vehicle is sufficient. Another vehicle, however, traveling for a longer duration, e.g., from the middle of Γ^1_{CRL} till the beginning of Γ^3_{CRL}, would need to be provided with all 24 revocation entries, i.e., requiring 9 entries to derive all 24 revoked pseudonyms.

In a more realistic example, assume there are 1 million vehicles in the system, each has 6 hours worth of pseudonyms (72 pseudonyms per day with $\Gamma = 30$ min and $\tau_P = 5$ min, i.e., 6 pseudonyms per Γ), all are issued timely aligned with the rest with non-overlapping intervals [35]. Suppose 1 percent of them are compromised or their sensors became faulty and thus evicted from the system. As a result, the revocation information to be disseminated for a day contains 720,000 entires, thus a CRL of around 22 MB (with 256-bit long serial numbers per pseudonym). By implicitly binding pseudonyms belonging to each OBU, one can distribute 1 entry for a batch of revoked pseudonyms per Γ (with some additional information), in total, 12 entries per revoked vehicle instead of 72 entries. Thus, the size of the CRL for that day becomes 7.3 MB, with 120,000 entries (with 256-bit serial numbers and 256-bit of complementary information for each entry). This already shows a significant reduction of the CRL size. However, distributing all that revocation information ignores the temporal nature of pseudonyms and the vehicle trip duration; it is more effective to distribute revocation information for a protocol-selectable period in the near future. Therefore, when a vehicle is to travel approximately within a Γ_{CRL} interval, assumed for example to be 30 min, it will only receive pieces of information for that Γ_{CRL}, i.e., around 10,000 entries and thus a CRL size of 625 KB instead of 22 MB, i.e., 3 orders of magnitude reduction of the CRL size distributed at any point in time.

Security and Privacy Analysis

The authenticity and integrity of each CRL piece is validated by testing each piece against the fingerprint, periodically broadcasted by RSUs and integrated in a subset of recently issued pseudonyms (R2.1 in Sec. 3.2). Moreover, no PCA can deny the inclusion of pseudonym serial number as the fingerprint of CRL pieces is signed with the PCA's private key (R2.1 in Sec. 3.2). Furthermore, each query to obtain CRL pieces is authenticated, in fact signed with the current valid pseudonym of the vehicle, thus preventing from abusing mechanism. If a *legitimate-looking* node aggressively requests CRL pieces, responding to such requests can be of the lowest priority and they are reported as potential misbehavior.

Upon a revocation event and CRL release, an external observer can try to link the revoked pseudonyms backwards (towards the beginning of the Γ interval). However, it is infeasible to link the previously non-revoked (but expired) pseudonyms

belonging to a misbehaving vehicle due to the utilization of a hash-chain during pseudonym issuance process, i.e., strong user privacy protection for a period, during which the vehicle was not compromised (R2.2 in Sec. 3.2).

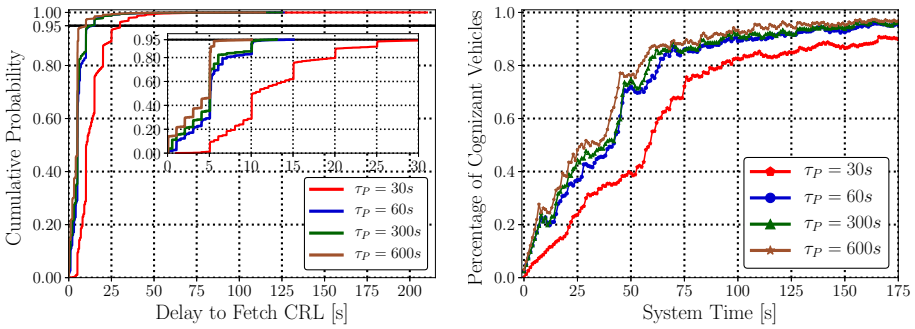
In collusion with V2X observers, honest-but-curious PCAs operating in a given domain might be tempted to infer sensitive information from the pseudonyms, e.g., timing information, or, in our context, the CRLs, towards linking pseudonym sets and tracking a vehicle. However, all the issued pseudonyms are aligned with global system time (PCA clock), thus, there is no distinction among pseudonyms based on pseudonym timing information. Moreover, the CRLs do not disclose extra information to harm user privacy[3]. Moreover, PCAs randomly select a subset of pseudonyms to be fingerprint-carries; thus, correlating any of these pseudonyms does not imply that they belong to the same vehicle (R2.2 in Sec. 3.2).

We leverage RSUs and car-to-car epidemic distribution to disseminate CRL pieces and signed fingerprints for increased availability or intermittent connectivity (R2.3 in Sec. 3.2). The resilience to pollution and DDoS attacks stems from three factors: (i) a huge reduction of the CRL size, notably because of distributing CRL information only for relevant periods of time, (ii) very efficient verification of CRL pieces, i.e., testing against a BF with hash and not signature validation, and (iii) integrating the fingerprint of CRL pieces in a subset of pseudonyms (R2.3 in Sec. 3.2).

The efficiency stems from the efficient construction of an authenticator for CRL pieces (minimal overhead on the PCA side), fast verification of each piece (minimal overhead on the vehicle side), and implicit binding of a batch of pseudonyms. Moreover, leveraging recurrent interactions with the VPKI, which issues time-aligned pseudonyms for all vehicles, and distributing CRLs with respect to locality, the ephemeral nature of credentials, and the average trip duration enhances efficiency (R2.4 in Sec. 3.2). We allocate a small fraction of bandwidth for CRL distribution and we apply a rate limiting mechanism to prevent abuse of the mechanism (R2.3 and R2.4 in Sec. 3.2). However, allocating a small amount of bandwidth is sufficient to timely distribute CRLs to practically all legitimate vehicles within the system (R2.4 in Sec. 3.2), as demonstrated in performance evaluation. Note that if pseudonyms were provided for a long period and vehicles had only unidirectional connectivity [47], then the VPKI cannot integrate new information into the pseudonyms for efficiency reasons. Thus, the signed fingerprint of CRL pieces would need to be disseminated through RSUs on a weekly basis.

Malicious entities might try to prevent other legitimate vehicles from receiving CRL-update notifications, thus preventing them from requesting the latest CRL, i.e., compromising availability and essentially harming the VC system security (as evicted nodes would remain undetected). RSUs periodically broadcast the signed fingerprint,

[3]Each PCA can trivially link the issued pseudonyms for the same vehicle as a response to a single request. However, one can configure the system to achieve *full unlinkability*, i.e., Γ is set equal to τ_P and force obtaining each single pseudonym with a different ticket. This implies that even honest-but-curious PCAs cannot link any two pseudonyms issued for a single vehicle, but it would be impractical in most setting.



(a) Vehicle-centric scheme ($\mathbb{B}$ =10 KB/s) (b) Vehicle-centric scheme ($\mathbb{B}$ =10 KB/s)

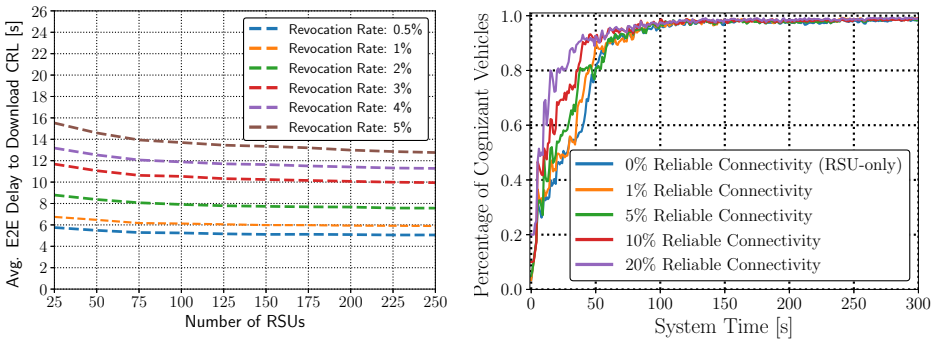
Figure 4.11: (a) End-to-end latency to fetch CRL pieces. (b) Percentage of cognizant vehicles over time. [taken from [44]].

corresponding to all CRL pieces of a given Γ_{CRL}, to ensure reception of the CRL validation authenticator in a region. Moreover, the PCAs randomly choose a subset of recently issued pseudonyms to piggyback the CRL-update notification. Vehicles beacon CAMs at a high rate, each signed with the private key of a pseudonym that possibly carries a notification about a CRL-update event and attach the pseudonym to a significant fraction of CAMs, in fact free notification about a revocation event at any point in time in the system (R5). Further evidence to the availability, the resiliency, and the efficiency, is provided through the detailed experimental evaluation in [44, 45].

Performance Evaluation for the Vehicle-Centric CRLs Distribution

Fig. 4.11.a shows the CDF of end-to-end latencies to obtain the needed CRL. For example, with $\tau_P = 60s$, 95% of the vehicles received the needed pieces in 15s. Fig. 4.11.b shows the percentage of cognizant vehicles over time, i.e., those that successfully obtained the CRL pieces. Obviously, the longer the pseudonym lifetime is, the shorter the CRL size is, thus the faster the convergence time becomes. For example, the percentage of cognizant nodes at system time 50 sec, with pseudonym lifetime 30s and 600s, is 39% and 76%, respectively.

Fig. 4.12.a shows the average end-to-end delay to download the CRL as a function of the number of RSUs for our scheme. The delays were averaged over vehicles operating during the rush hours. The total number of pseudonyms is 1.7M ($\tau_P = 60s$) and the maximum bandwidth to distribute CRL pieces is 25 KB/s. In general, a higher number of RSUs and a lower revocation rate result in a lower average delay to obtain the CRL. For example, the average latency, with $\mathbb{R}$ =1%, decreases from 6.91 to 6.23 as the number of RSUs increases from 25 to 100. As Fig. 4.12.a shows, leveraging the car-to-car epidemic CRL distribution makes the deployment of a large number of RSUs unnecessary. The optimal number of RSUs to be deployed for a given domain can be properly determined to achieve a certain level of quality of service. Further discussion is beyond the scope of our work.



(a) Vehicle-centric scheme ($\mathbb{B}$ =25 KB/s) (b) Vehicle-centric scheme (TX =5s)

Figure 4.12: (a) Average end-to-end delay to download CRLs. (b) Dissemination of CRL fingerprints. [taken from [44]].

Fig. 4.12.b shows how fast a CRL fingerprint is distributed: the signed fingerprint of CRL pieces is periodically broadcasted only by RSUs [126], or they are broadcasted by RSUs (approx. 365 bytes with $TX = 5s$) and, in addition, integrated into a subset of pseudonyms with 36 bytes of extra overhead ($p = 10^{-30}$, $\mathbb{R} = 0.5\%$). Obviously, the distribution of CRL fingerprints with our scheme is faster when there is a small fraction of vehicles with reliable connectivity. However, there is a time lag from the time a PCA releases CRL fingerprints until practically all vehicles are informed about a new CRL-update event. Depending on the percentage of vehicles with reliable connectivity and the frequency of revocation events, the PCA could *''predict''* a suitable time to reveal the CRL fingerprint to ensure that every legitimate vehicle operating within the system would receive the CRL fingerprint. For example, the PCA could integrate in a fraction of the recently issued pseudonyms the fingerprint of the current Γ_{CRL} and integrate in another fraction of newly issued pseudonyms the fingerprint of the subsequent Γ_{CRL}.

4.3 Location Privacy Protection for VANETs

CMIX with Decoy Traffic

The VPKI system chooses a subset of RSUs, located near intersections where vehicles physically mix [113], to establish a cryptographically protected area and construct a CMIX for private pseudonym changes. RSUs are responsible for the initiation of the pseudonym transition process and maintaining a symmetric key to establish the encrypted region. To mitigate syntactic and semantic linking attacks, we introduce broadcasting decoy traffic at each mix-zone. Such traffic emulates vehicles that do not exist in reality. The RSU at each mix-zone facilitates obtaining *Chaff Pseudonyms (CPs)* in order to generate *chaff CAMs* (or *chaff DENMs*). The purpose is to decrease the probability of linking two pseudonyms of a vehicle prior to and after pseudonym change. In case of sparse traffic (low vehicle density),

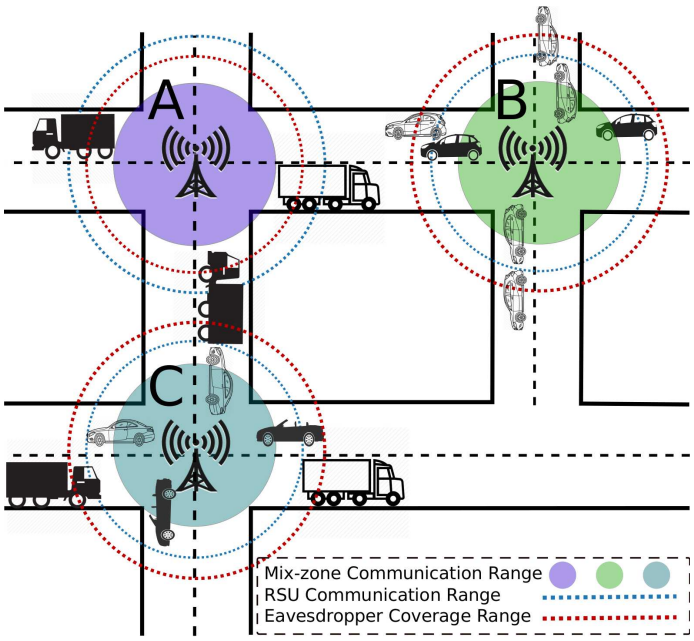


Figure 4.13: Mix-zones construction with decoy traffic. [taken from [86]].

RSUs could also emulate a chaff vehicle by periodically broadcasting chaff CAMs. Our system can be configured so that for each vehicle, multiple *seemingly identical* chaff vehicles could (potentially) appear as if they uniformly exit from different exit points of a mix-zone. As a result, it is hard for an eavesdropper to identify actual traces based on the CAMs attributes, e.g., velocity, acceleration, mix-zone geometry, and time spent in a mix-zone. Each vehicle could request multiple chaff pseudonyms (and the corresponding chaff private keys) from an RSU. For ease of exposition, we assume each vehicle requests one chaff pseudonym in each mix-zone. Extension to multiple chaff pseudonyms and multiple PCAs operating in a domain is straightforward.

Fig. 4.13 shows three mix-zones: the colored disks indicate the approximate encrypted range of a mix-zone; the blue dotted circles denote the transmission range of RSUs. The coverage range of eavesdroppers denoted by red dotted circles; for mix-zones B and C, the external adversaries eavesdrop all entry and exit points of the RSUs while for mix-zone A, the eavesdropper eavesdrops all entry and exit points of the mix-zone. The RSU coverage range can be either larger or smaller than the local eavesdropper; however, the operation of our scheme does not depend on these ranges. The RSU range needs to always exceed the mix-zone range, simply in order to allow vehicles to execute the CMIX participation protocol, notably obtaining the mix-zone symmetric key. Black vehicles are the real ones while the white ones represent non-exiting vehicles, i.e., the decoy traffic. Once a vehicle enters a mix-zone, it requests to obtain the mix-zone symmetric key. An RSU

leverages its knowledge about the road layout and vehicles to determine how many chaff vehicles are required. In the case of sparse traffic density, an RSU generates synthetic CAMs, resembling the traces towards an exit point of the mix-zone. The system can be configured to have RSUs provide and/or emulate one (see mix-zone C in Fig. 4.13) or multiple (see mix-zone B in Fig. 4.13) chaff vehicles. In our scheme, each vehicle only provides its length to the RSU; this information is used by an RSU to coordinate with another vehicle in the mix-zone towards disseminating decoy traffic, i.e., generating synthetic CAMs towards resembling a non-existing, *but seemingly identical*, vehicle, exiting from an opposite exit point of the mix-zone.

Each PCA pre-generates a distinct set of chaff public and private keys (chaff pseudonyms) and delivers them to an RSU, responsible for a mix-zone construction. Each vehicle could send a request to the RSU to obtain one chaff pseudonym. The RSU randomly assigns chaff pseudonyms to a subset of vehicles, termed *relaying vehicles*. The VPKI system cannot correlate a vehicle and a chaff pseudonym since the RSU randomly assigns a chaff pseudonym to a requesting vehicle. Note that accountability for chaff CAMs is not paramount as such (chaff) credentials are not valid and they cannot be used for any application. In case of deviation from system protocols, a misbehaving vehicle can still be identified.

In order to preserve the correct functionality of transportation safety applications, our scheme provides vehicles with information to identify chaff messages. Therefore, each PCA proactively constructs a Cuckoo Filter (CF) [207] by including chaff pseudonyms in a probabilistic data-structure and RSUs distribute these condensed fingerprints of chaff pseudonyms among legitimate vehicles across a region. This facilitates discarding chaff pseudonyms by legitimate vehicles, thus, ensuring the correct operation of safety applications. Similarly to BF [127, 128], CFs provide fast membership tests at the cost of a false positive rate (ρ), but in contrast support dynamic updates of the underlying set. This data structure includes the fingerprints of the chaff pseudonyms used to sign chaff CAMs and chaff DENMs. When receiving a CAM or a DENM, an OBU could efficiently validate the attached pseudonym against the corresponding CF; if the membership test is positive, the CAM or the DENM is discarded; otherwise, the signature will be verified.

Chaff CAMs are to be disseminated until a vehicle reaches another mix-zone or the end of the trip duration. When a relaying vehicle intends to stop disseminating chaff CAMs, e.g., entering another mix-zone, it queries the PCA, signed under the private key of the chaff pseudonym, to remove that chaff pseudonym from the corresponding CF. Further dissemination of chaff CAMs using such a chaff pseudonym is considered a misbehavior and it can be identified by a misbehavior detection system, e.g. [142], that triggers the revocation. The CFs are frequently updated by the PCAs and pushed to the corresponding RSUs.

An RSU operating a mix-zone cannot filter out chaff pseudonyms, originating from other mix-zones; the PCA prepares a distinct set of chaff pseudonyms for each RSU, operating a mix-zone. As a result, an RSU cannot distinguish between a real pseudonym and a chaff one of another RSU. However, a vehicle might encounter other relaying vehicles with chaff pseudonyms obtained from other mix-zones. For

example, when a vehicle is crossing mix-zone A and moving towards mix-zone B in Fig. 4.13, it might encounter chaff pseudonyms originated from mix-zone B. Thus, it needs to request and obtain the CF corresponding to mix-zone B. The vehicle could directly interact with the PCA and request to obtain the CFs, corresponding to the nearby mix-zones. The PCA needs to identify the physical location[4], e.g., [178, 209, 210], of requesting vehicles; in fact, requesting vehicles should be physically ''close'' to a mix-zone to obtain the corresponding CF for. Otherwise, an external adversary could request to obtain all CFs, thus filtering out all chaff pseudonyms exiting the mix-zones.

Security and Privacy Analysis

All the V2X communication in a mix-zone is encrypted and hidden from an external observer. Upon a pseudonym change in a mix-zone, an external adversary, observing the encrypted communication cannot distinguish among vehicles sets towards correlating their corresponding pseudonyms (R3.1 in Sec. 3.3). A single entity cannot fully de-anonymize a user, link two successive pseudonyms, or link a chaff pseudonym to a pseudonymous identifier of a given vehicle. An LTCA or a PCA can infer no information to harm user privacy during changing pseudonyms since all communication inside a mix-zone is encrypted. An external adversary observing the communication could distinguish among pseudonym and chaff pseudonym sets based on the timing information [35]. To eliminate any distinction, the PCA issues pseudonyms and chaff pseudonyms with fully overlapping lifetimes, thus, timing information cannot harm user privacy. Moreover, the VPKI system issues fully unlinkable pseudonyms for all vehicles, thus, even if two pseudonyms are obtained by the same requester, they cannot be linked since each is requested using a distinct ticket [34, 35, 58]. LTCA cannot differentiate between a chaff pseudonym and a real one. A PCA can only differentiate chaff pseudonyms that it issued; in other words, it cannot distinguish a chaff pseudonym, issued by another PCA, from a real one. Moreover, a PCA cannot infer any information towards correlating a chaff pseudonym and an actual pseudonym: the RSU randomly assigns one chaff pseudonym to a relaying vehicle.

An honest-but-curious RSU learns the length of a requesting vehicle during mix-zone symmetric key acquisition process. However, this does not reveal additional information since the length is already included in the CAMs, frequently disseminated by the vehicle; thus, unlike the chaff-based CMIX [131] that requires vehicles provide their intended trajectory path to the RSUs, our scheme does not provide additional information (in comparison with the CMIX scheme [113]) to the RSUs. An RSU operating a mix-zone cannot filter out chaff pseudonyms originated from other mix-zones; this diminishes the probability of linking two successive pseudonyms belonging to the same vehicle; however, an RSU can filter out chaff

[4]Physical identification of vehicles is also a key requirement in the original mix-zone scheme [113, 160, 208]; this prevents an adversary from remotely requesting the symmetric keys of the mix-zones.

pseudonyms that it provides and link successive pseudonyms upon pseudonym change in the mix-zone. We quantitatively evaluated the successful linkability in the presence of honest-but-curious RSUs in performance evaluation. Collusion by PCA_A and PCA_B results in filtering out chaff pseudonyms they issued; but, they cannot observe the encrypted communication. Collusion by RSU_H and PCA_H enable them to decrypt the encrypted communication and filter out all chaff pseudonyms. A collusion of the LTCA, PCA_H, and RSU_H enable them to link all pseudonyms issued in a given domain with their real identities. As a result, they can link any pseudonym to its prior or successive pseudonyms.

Issuing chaff pseudonyms, constructing and disseminating the CF data-structure, and validating chaff pseudonym requests are all efficient processes (see performance evaluation). Each RSU, responsible for constructing a mix-zone, disseminates required information to the vehicles approaching the mix-zone, e.g., symmetric session key, mix-zone geometries, and CFs. This information is (signed by the RSU and) encrypted using the public key of a vehicle, approaching the mix-zone. All vehicle-RSU interactions are mutually authenticated using the currently valid vehicle's pseudonym and we leverage RSUs and car-to-car epidemic distribution to disseminate the CFs (R3.2 in Sec. 3.3). Non-cooperative vehicles could ignore changing their pseudonyms in order to degrade the anonymity set size of the mix-zone. However, as it is shown in Sec. 4.3, such behavior does not degrade the user privacy protection. Vehicles could also repeatedly request to obtain multiple chaff pseudonyms from the RSUs, monopolizing a substantial portion of the chaff pseudonyms (constructed by the PCA and pushed to the RSUs); however, each vehicle is equipped with an HSM which guarantees all outgoing signatures are signed under the private key of a single valid pseudonym at any time. In case of deviating from the system security policy, suspicious activities or (high-rate) spurious requests are sent to the RA to initiate a process to (possibly) resolve a pseudonym, thus identifying the long-term identity of a misbehaving vehicle, i.e., the pseudonym owner, and thus, their credentials will be revoked (R3.3 in Sec. 3.3).

The efficiency of the system stems from efficient CF construction of chaff pseudonyms (minimal overhead on the PCA side) and very fast validation (membership check) of chaff pseudonyms from a CF (minimal overhead on the vehicle side) (R3.4 in Sec. 3.3). Our scheme does not introduce extra computation overhead on the RSU side (in comparison with the CMIX scheme [113]) during mix-zone advertisement and symmetric key distribution. We allocate a small fraction of bandwidth for CFs distribution, which is sufficient to timely distribute CFs to all legitimate vehicles approaching a mix-zone. Our scheme introduces communication overhead to disseminate decoy traffic to enhance user privacy. In order to balance communication overhead and user privacy protection, our scheme also provides fine-grained adaptive mechanism to adjust the amount of decoy traffic in various situations, i.e., less decoy traffic during the rush-hours or more decoy traffic in sparse traffic conditions. Given a data rate of several Mbit/sec for modern IEEE 802.11p interfaces [211], dissemination of decoy traffic does not pose a significant communication overhead. Disseminating decoy traffic for all vehicles introduces resealable computation and

Algorithm 3 Syntactic and Semantic Linking Attacks

```
1: procedure LinkingSuccessivePseudonymsAlgorithm( )
2:     Fetch eavesdropped beacon and road layout information
3:     Classify eavesdropped beacons based on vehicle length
4:     Create a list with the first & last seen beacons for each identifier
5:     Filter out trivially linked pseudonyms (not changing psnyms)
6:     MaxTravTime ← Maximum time to traverse a mix-zone
7:     MinTravTime ← Minimum time to traverse a mix-zone
8:     for Each B_i in BEACON_SET do
9:         B_i^f is the first seen message for beacon B_i
10:        B_i^l is the last seen message for beacon B_i
11:        for Each B_{i+1}^f in BEACON_SET do
12:            B_i^l and B_{i+1}^f are not correlated
13:            diff ← time difference between B_i^l and B_{i+1}^f
14:            if diff ≥ MinTravTime && diff ≤ MaxTravTime then
15:                if pseudo-id for B_i^l and B_{i+1}^f not seen together then
16:                    if exists a road path from B_i^l to B_{i+1}^f then
17:                        if B_{i+1}^f direction is from an exit point then
18:                            B_i^l and B_{i+1}^f are correlated
19:                            break
20:                        end if
21:                    end if
22:                end if
23:            end if
24:        end for
25:    end for
26: end procedure
```

communication overhead (see [86] for a detailed quantitative analysis of our scheme on computation and communication overhead).

Tracking Algorithm

Algorithm 3 shows our tracking algorithm in order to link two successive pseudonyms upon pseudonym change within a mix-zone. It first fetches eavesdropped beacon information and the road layout information (step 3.2, i.e., step 2 in Algorithm 3). It then classifies beacons based on the length of the vehicles (step 3.3). Next, it selects the first and the last observed beacons corresponding to each pseudonymous identifier (step 3.4). It then removes the beacons that enter and exit the mix-zone with the same pseudonymous identifiers, i.e., filtering out trivially linked pseudonyms (step 3.5). The minimum and maximum time to traverse a mix-zone is calculated based on the mix-zone geometry and vehicle speed limits (steps 3.6 –3.7). The algorithm aims at linking the last observed beacon, in fact, the one

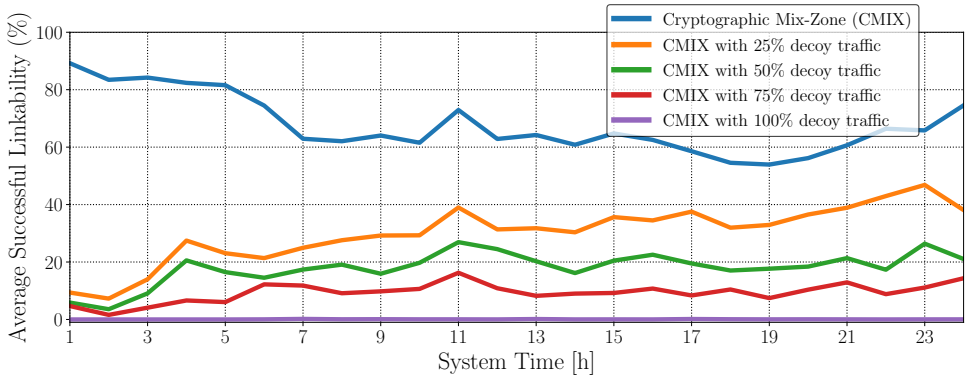


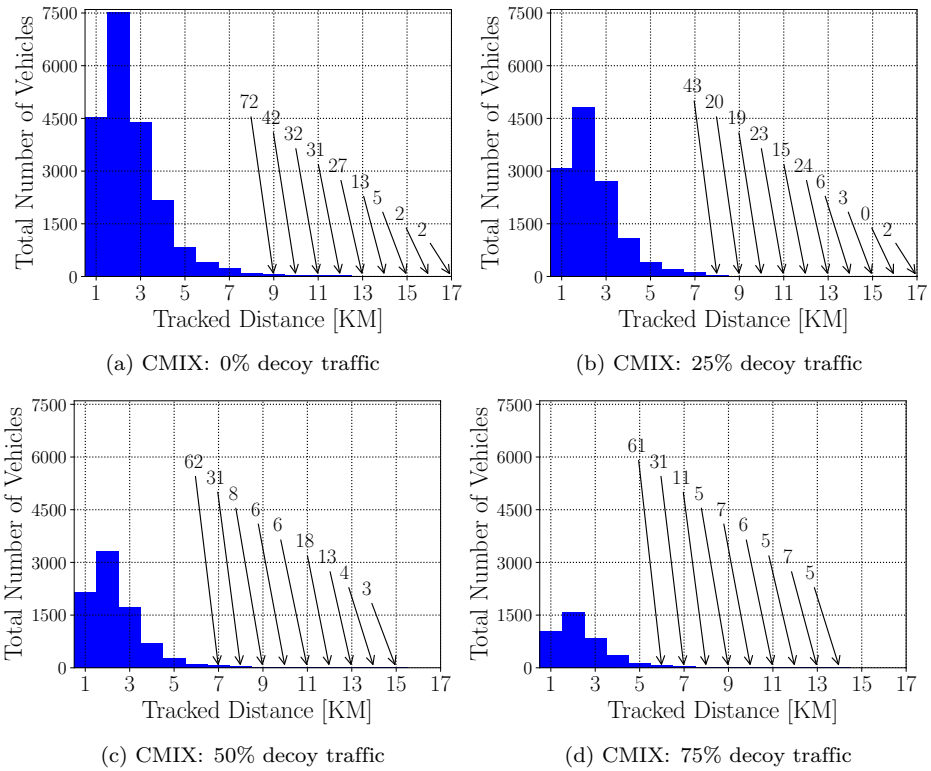
Figure 4.14: Average successful linkability comparison with the CMIX scheme [113] through conducting syntactic and semantic linking attacks. [taken from [86]].

seen before entering the mix-zone, to one of the messages exiting the mix-zone. Two pseudonyms are deemed correlated (i.e., belonging to the same vehicle) if (i) the time difference between the two observed beacons is within the minimum and maximum time to traverse the mix-zone, (ii) the two pseudonyms have not been seen together (i.e., syntactic linking [77]), (iii) there exists a road path from the last seen beacon (B_i^l) to the first seen beacon (B_{i+1}^f) [18], and (iv) the direction of the first seen beacon (B_{i+1}^f) is from one of the exit points of the mix-zone (steps 3.8 –3.25).

Performance Comparison

Based on the ground truth (included in the simulation results) and leveraging our novel tracking algorithm, we compute the *average successful linkability metric* towards linking pseudonyms before and after a cryptographically protected mix-zone. Fig. 4.14 shows the average pseudonym linkability by the eavesdroppers for a full-day realistic mobility pattern in the city of Luxembourg [203]. As we can see, the tracking algorithm could link pseudonyms for the CMIX scheme with high probability success rate during the non-rush hours period (until system time 6). The probability of linking two successive pseudonyms decreases when the traffic density increases; but still, it can successfully link the pseudonyms with ≈63% success rate at system time 7. By introducing decoy traffic for a fraction of vehicles, one can reduce the linkability: with 50% of vehicles to be the relaying vehicles, broadcasting decoy traffic, the probability of linking drops from ≈63% to ≈17% at system time 7. More so, one can eliminate (syntactic and semantic) pseudonym linking attacks by disseminating decoy traffic for all vehicles.

If the number of vehicles in a mix-zone is less than a predefined (system parameter) threshold, the RSU generates decoy traffic for all those vehicles. This stems from the results of tracking algorithm: if there are few vehicles inside a mix-zone, an adversary could easily track all those vehicles. In our simulation, we defined this



(a) CMIX: 0% decoy traffic

(b) CMIX: 25% decoy traffic

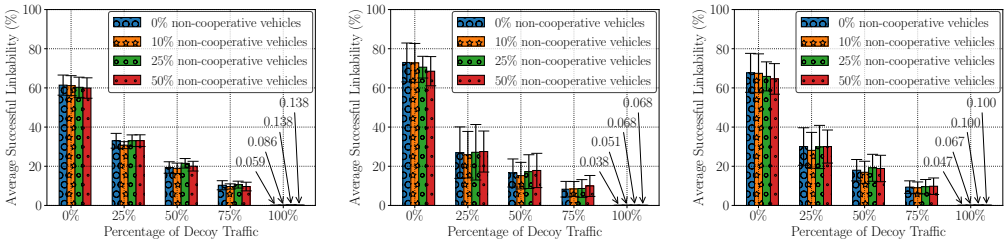
(c) CMIX: 50% decoy traffic

(d) CMIX: 75% decoy traffic

Figure 4.15: Histogram of tracked distances by eavesdroppers based on the linked pseudonyms sets for the baseline scheme (CMIX) and our scheme. [taken from [86]].

threshold to be two, i.e., if there are one or two vehicles in a mix-zone, the RSU disseminates decoy traffic for all vehicles. This is also visible in Fig. 4.14: during very sparse traffic conditions (at system time 1), the average successful tracking is ≈7%-9%. Intuitively, the rate of decoy traffic should be inversely proportional to the traffic density, i.e., the higher the number of vehicles inside a mix-zone, the lower the probability of linking becomes, thus the less the number of chaff vehicles needed. This trades off pseudonyms unlinkability for (communication and computation overhead) cost, which is important for balancing the effects of chaff messages on communication overhead in dense traffic scenarios.

Fig. 4.15 shows the histogram of the number of vehicles, tracked by the eavesdroppers, based on the linked pseudonyms sets. With the baseline scheme, the eavesdroppers could link 4,536 vehicles for 1 KM, 7,532 vehicles for 2 KMs, and 4,409 vehicles for 3 KMs. In contrast, by introducing decoy traffic for vehicles exiting the mix-zones, the total number of vehicles, tracked by the eavesdroppers, drastically decreases: with 75% of decoy traffic, the eavesdroppers could only link 1,044 vehicles for 1 KM, 1,576 vehicles for 2 KMs, and 837 vehicles for 3 KMs. Note that by disseminating 100% decoy traffic, the probability of linking two successive



(a) During Rush Hours (b) During Non-rush Hours (c) During 24 Hours

Figure 4.16: Average successful linkability in the presence of non-cooperative vehicles, not changing their pseudonyms while crossing the mix-zones. [taken from [86]].

pseudonyms by the eavesdroppers is very low, thus such tracking becomes ineffective (see Fig. 4.14 and Fig. 4.16).

Fig. 4.16 shows the average success rates in the presence of non-cooperative vehicles that try to diminish the anonymity set size of a mix-zone. Such vehicles exit the mix-zone without changing their pseudonyms; also, if chosen to be relaying vehicles, they do not disseminate decoy traffic. The tracking algorithm (step 4 in Algorithm 3) filters out these trivially linked pseudonyms, i.e., CAMs of vehicles that enter and exit the mix-zone with the same pseudonym. Fig. 4.16.a shows the average successful tracking during the rush hours. The average successful tracking in the presence of non-cooperative vehicles for the CMIX scheme slightly decreases: the eavesdroppers filter out transcript of pseudonymously authenticated messages with the same pseudonym. Thus, non-cooperative vehicles, not changing their pseudonyms, do not help eavesdroppers link successive pseudonyms with higher percentage of successful tracking. During the non-rush hour periods (Fig. 4.16.b), the average successful tracking for the CMIX scheme is higher than the one during the rush-hour periods: due to lower number of vehicles in a mix-zone, the probability of linking by an eavesdropper increases; still, non-cooperative vehicles that do not change their pseudonyms, when crossing a mix-zone, do not highly affect the anonymity set size. Fig. 4.16.c shows the average successful tracking for the entire intervals: eavesdroppers could successfully link 68% of successive pseudonyms before and after pseudonym changes in the mix-zones.

The average successful tracking for our scheme is not considerably affected in the presence of non-cooperative vehicles thanks to dissemination of decoy traffic. Note that selection of non-cooperative vehicles is independent of selection of relaying vehicles, i.e., in each scenario, different sets of vehicles are selected to be non-cooperative. Thus, a direct comparison of the scenarios with different percentage of non-cooperative vehicles is not straightforward. In order to mitigate the effect of non-cooperative vehicles, an RSU could monitor the behavior of vehicles when entering and exiting the mix-zone; if a substantial fraction of vehicles exit the mix-zone without changing their pseudonyms, the RSU can increase the percentage of decoy traffic.

Chapter 5

Summary of Original Work

In this chapter, the summary of the papers in the context of this thesis, along with the contribution of the author, are given.

5.1 Paper A: VeSPA: Vehicular Security and Privacy-preserving Architecture

Nikolaos Alexiou, Marcello Laganà, Stylianos Gisdakis, Mohammad Khodaei, and Panos Papadimitratos
In the Proceedings of the 2nd ACM workshop on Hot topics on wireless network security and privacy (ACM HotWiSec), pp. 19–24 Budapest, Hungary, April 2013.

Summary

Vehicular Communications (VCs) are reaching a near deployment phase and will play an important role in improving road safety, driving efficiency and comfort. The industry and the academia have reached a consensus for the need of a Public-Key Infrastructure (PKI), in order to achieve security, identity management, vehicle authentication, as well as preserve vehicle privacy. Moreover, a gamut of proprietary and safety applications, such as location-based services and pay-as-you-drive systems, are going to be offered to the vehicles. The emerging applications are posing new challenges for the existing Vehicular Public-Key Infrastructure (VPKI) architectures to support Authentication, Authorization and Accounting (AAA), without exposing vehicle privacy. In this work, we present an implementation of a VPKI that is compatible with the VC standards. We propose the use of tickets as cryptographic tokens to provide AAA and also preserve vehicle privacy against adversaries and the VPKI. Finally, we present the efficiency results of our implementation to prove its applicability.

Contribution

The work in this project was the continuation of the MSc thesis [212] of the author of this thesis. This work reflects his work as a research engineer within the Networked Systems Security (NSS) group. He significantly contributed to the design and carried out the implementation and the performance analysis of the system.

5.2 Paper B: Towards Deploying a Scalable and Robust Vehicular Identity and Credential Management Infrastructure

Mohammad Khodaei, Hongyu Jin, and Panos Papadimitratos
Presented at: Conference on Vehicular Networking Conference (IEEE VNC), Paderborn, Germany, December 2014.

Summary

Several years of academic and industrial research efforts have converged to a common understanding on fundamental security building blocks for the upcoming Vehicular Communication (VC) systems. There is a growing consensus towards deploying a Vehicular Public-Key Infrastructure (VPKI) enables pseudonymous authentication, with standardization efforts in that direction. However, there are still significant technical issues that remain unresolved. Existing proposals for instantiating the VPKI either need additional detailed specifications or enhanced security and privacy features. Equally important, there is limited experimental work that establishes the VPKI efficiency and scalability. In this paper, we are concerned with exactly these issues. We leverage the common VPKI approach and contribute an enhanced system with precisely defined, novel features that improve its resilience and the user privacy protection. In particular, we depart from the common assumption that the VPKI entities are fully trusted and we improve user privacy in the face of an *honest-but-curious* security infrastructure. Moreover, we fully implement our VPKI, in a standard-compliant manner, and we perform an extensive evaluation. Along with stronger protection and richer functionality, our system achieves very significant performance improvement over prior systems, contributing the most advanced VPKI towards deployment.

Contribution

The author of this thesis, with the help of the other authors, enhanced the system design and significantly improved the performance of the system. He also carried out the implementation and the performance analysis of the system. The article was written by all authors.

5.3 Paper C: The Key to Intelligent Transportation: Identity and Credential Management in Vehicular Communication Systems

Mohammad Khodaei and Panos Papadimitratos
In IEEE Vehicular Technology (VT) Magazine, vol.10, no. 4, pp. 63–69, December 2015.

Summary

Vehicular Communication (VC) systems will greatly enhance intelligent transportation systems. But their security and the protection of their users' privacy are a prerequisite for deployment. Efforts in industry and academia brought forth a multitude of diverse proposals. These have now converged to a common view, notably on the design of a security infrastructure, a Vehicular Public-Key Infrastructure (VPKI) that shall enable secure conditionally anonymous VC. Standardization efforts and industry readiness to adopt this approach hint to its maturity. However, there are several open questions remaining, and it is paramount to have conclusive answers before deployment. In this article, we distill and critically survey the state of the art for identity and credential management in VC systems, and we sketch a roadmap for addressing a set of critical remaining security and privacy challenges.

Contribution

The article was put together and written by both authors.

5.4 Paper D: Evaluating On-demand Pseudonym Acquisition Policies in Vehicular Communication Systems

Mohammad Khodaei and Panos Papadimitratos
Presented at: the First International Workshop on Internet of Vehicles and Vehicles of Internet (IoV-VoI), Paderborn, Germany, July 2016.

Summary

Standardization and harmonization efforts have reached a consensus towards using a special-purpose Vehicular Public-Key Infrastructure (VPKI) in upcoming Vehicular Communication (VC) systems. However, there are still several technical challenges with no conclusive answers; one such an important yet open challenge is the acquisition of short-term credentials, *pseudonym*: how should each vehicle interact

with the VPKI, e.g., how frequently and for how long? Should each vehicle itself determine the pseudonym lifetime? Answering these questions is far from trivial. Each choice can affect both the user privacy and the system performance and possibly, as a result, its security. In this paper, we make a novel systematic effort to address this multifaceted question. We craft three generally applicable policies and experimentally evaluate the VPKI system performance, leveraging two large-/scale mobility datasets. We consider the most promising, in terms of efficiency, pseudonym acquisition policies; we find that within this class of policies, the most promising in terms of privacy protection policy incurs only a mild increase in overhead. Moreover, in all cases, this work is the first to provide tangible evidence that the state-of-the-art VPKI can serve sizable areas or domain with modest computing resources.

Contribution

The author of this thesis contributed the implementation and performance analysis of the work. The paper was written by both authors.

5.5 Paper E: RHyTHM: A Randomized Hybrid Scheme To Hide in the Mobile Crowd

Mohammad Khodaei, Andreas Messing, and Panos Papadimitratos
Presented at: Conference on Vehicular Networking Conference (IEEE VNC), Torino, Italy, November 2017.

Summary

Any on-demand pseudonym acquisition strategy is problematic should the connectivity to the credential management infrastructure be intermittent. If a vehicle runs out of pseudonyms with no connectivity to refill its pseudonym pool, one solution is the *on-the-fly* generation of pseudonyms, e.g., leveraging anonymous authentication. However, such a vehicle would stand out in the crowd: one can simply distinguish pseudonyms, thus signed messages, based on the pseudonym issuer signature, link them and track the vehicle. To address this challenge, we propose a randomized hybrid scheme, RHyTHM, to enable vehicles to remain operational when disconnected without compromising privacy: vehicles with valid pseudonyms help others to enhance their privacy by randomly joining them in using *on-the-fly self-certified* pseudonyms along with aligned lifetimes. This way, the privacy of disconnected users is enhanced with a reasonable computational overhead.

Contribution

The main idea of this article was the result of fruitful discussions with the third author. The work in this project was conducted within the scope of the MSc thesis of the second author. The author of this thesis contributed to the design, implementation, and performance evaluation. The article was written by all authors.

5.6 Paper F: SECMACE: Scalable and Robust Identity and Credential Management Infrastructure in Vehicular Communication Systems

Mohammad Khodaei, Hongyu Jin, and Panos Papadimitratos
In IEEE Transaction on Intelligent Transportation Systems, vol. 19, no. 5, pp. 1430–1444, May 2018.

Summary

Several years of academic and industrial research efforts have converged to a common understanding on fundamental security building blocks for the upcoming Vehicular Communication (VC) systems. There is a growing consensus towards deploying a special-purpose identity and credential management infrastructure, i.e., a Vehicular Public-Key Infrastructure (VPKI), enabling pseudonymous authentication, with standardization efforts towards that direction. In spite of the progress made by standardization bodies (IEEE 1609.2 and ETSI) and harmonization efforts (Car2Car Communication Consortium (C2C-CC)), significant questions remain unanswered towards deploying a VPKI. The precise understanding of the VPKI, a central building block of secure and privacy-preserving VC systems, is still lacking. This paper contributes to the closing of this gap. We present SECMACE, a VPKI system, which is compatible with the IEEE 1609.2 and ETSI standards specifications. We provide a detailed description of our state-of-the-art VPKI that improves upon existing proposals in terms of security and privacy protection, and efficiency. SECMACE facilitates multi-domain operations in the VC systems and enhances user privacy, notably preventing linking *pseudonyms* based on timing information and offering increased protection even against *honest-but-curious* VPKI entities. We propose multiple policies for the vehicle-VPKI interactions based on which and two large mobility traces, we evaluate the full-blown implementation of SECMACE. With very little attention on the VPKI performance thus far, our results reveal that modest computing resources can support a large area of vehicles with very low delays and the most promising policy in terms of privacy protection can be supported with moderate overhead.

Contribution

This paper, based on prior works [34, 58, 213], consolidated the design, implementation, and evaluation. The author of this thesis contributed to all these aspects, together with the other authors. The article was written primarily by the author of this thesis and the last author of the paper.

5.7 Paper G: Efficient, Scalable, and Resilient Vehicle-Centric Certificate Revocation List Distribution in VANETs

Mohammad Khodaei and Panos Papadimitratos
Presented at: 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks (ACM WiSec), Stockholm, Sweden, June 2018.

Summary

In spite of progress in securing Vehicular Communication (VC) systems, there is no consensus on how to distribute Certificate Revocation Lists (CRLs). The main challenges lie exactly in (i) crafting an efficient and timely distribution of CRLs for numerous anonymous credentials, *pseudonyms*, (ii) maintaining strong privacy for vehicles prior to revocation events, even with *honest-but-curious* system entities, (iii) and catering to computation and communication constraints of on-board units with intermittent connectivity to the infrastructure. Relying on peers to distribute the CRLs is a double-edged sword: *abusive peers* could ''pollute'' the process, thus degrading the timely CRLs distribution. In this paper, we propose a *vehicle-centric* solution that addresses all these challenges and thus closes a gap in the literature. Our scheme radically reduces CRL distribution overhead: each vehicle receives CRLs corresponding only to its region of operation and its actual trip duration. Moreover, a ''fingerprint'' of CRL 'pieces' is attached to a subset of (verifiable) pseudonyms for fast CRL 'piece' validation (while mitigating resource depletion attacks abusing the CRL distribution). Our experimental evaluation shows that our scheme is efficient, scalable, dependable, and practical: with no more than 25 KB/s of traffic load, the latest CRL can be delivered to 95% of the vehicles in a region (15×15 KM) within 15s, i.e., more than 40 times faster than the state-of-the-art. Overall, our scheme is a comprehensive solution that complements standards and can catalyze the deployment of secure and privacy-protecting VC systems.

Contribution

The author of this thesis contributed to the design, implementation, and performance evaluation of the work. The paper was written by both authors.

5.8 Paper H: Scaling Pseudonymous Authentication for Large Mobile Systems

Mohammad Khodaei, Hamid Noroozi, and Panos Papadimitratos
In the Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks (ACM MobiHoc), pp. 174–184, Miami FL, USA, May 2019.

Summary

The central building block of secure and privacy-preserving Vehicular Communication (VC) systems is a Vehicular Public-Key Infrastructure (VPKI), which provides vehicles with multiple anonymized credentials, termed *pseudonyms*. These pseudonyms are used to ensure message authenticity and integrity while preserving vehicle (thus passenger) privacy. In the light of emerging large-scale multi-domain VC environments, the efficiency of the VPKI and, more broadly, its scalability are paramount. By the same token, preventing misuse of the credentials, in particular, Sybil-based misbehavior, and managing *''honest-but-curious''* insiders are other facets of a challenging problem. In this paper, we leverage the state-of-the-art VPKI system and *enhance* its functionality towards a highly-available, dynamically-scalable, and resilient design; this ensures that the system remains operational in the presence of benign failures or resource depletion attacks, and that it dynamically *scales out*, or possibly *scales in*, according to request arrival rates. Our full-blown implementation on the Google Cloud Platform shows that deploying large-scale and efficient VPKI can be cost-effective.

Contribution

This paper consolidates the design, implementation, and evaluation of the work in [35]. The author of this thesis contributed to all these aspects, together with the other authors; the article was written by all authors.

5.9 Paper I: Scalable & Resilient Vehicle-Centric Certificate Revocation List Distribution in Vehicular Communication Systems

Mohammad Khodaei and Panos Papadimitratos
In IEEE Transactions on Mobile Computing (TMC), to appear.

Summary

In spite of progress in securing Vehicular Communication (VC) systems, there is no consensus on how to distribute Certificate Revocation Lists (CRLs). The main

challenges lie exactly in (i) crafting an efficient and timely distribution of CRLs for numerous anonymous credentials, *pseudonyms*, (ii) maintaining strong privacy for vehicles prior to revocation events, even with *honest-but-curious* system entities, (iii) and catering to computation and communication constraints of on-board units with intermittent connectivity to the infrastructure. Relying on peers to distribute the CRLs is a double-edged sword: *abusive peers* could ''pollute'' the process, thus degrading the timely CRLs distribution. In this paper, we propose a *vehicle-centric* solution that addresses all these challenges and thus closes a gap in the literature. Our scheme radically reduces CRL distribution overhead: each vehicle receives CRLs corresponding only to its region of operation and its actual trip duration. Moreover, a ''fingerprint'' of CRL 'pieces' is attached to a subset of (verifiable) pseudonyms for fast CRL 'piece' validation (while mitigating resource depletion attacks abusing the CRL distribution). Our experimental evaluation shows that our scheme is efficient, scalable, dependable, and practical: with no more than 25 KB/s of traffic load, the latest CRL can be delivered to 95% of the vehicles in a region (15×15 KM) within 15s, i.e., more than 40 times faster than the state-of-the-art. Overall, our scheme is a comprehensive solution that complements standards and can catalyze the deployment of secure and privacy-protecting VC systems.

Contribution

This paper is the continuation of [44]. The author of this thesis contributed to all aspects of the paper including the design, implementation, and performance evaluation of the work. The paper was written by both authors.

5.10 Paper J: Cooperative Location Privacy in Vehicular Networks: Why Simple Mix-zones are not Enough

Mohammad Khodaei and Panos Papadimitratos
Submitted to the IEEE Internet Of Things Journal.

Summary

Vehicular communications disclose rich information about the vehicles and their whereabouts. Pseudonymous authentication secures communication while enhancing user privacy. To enhance location privacy, cryptographic mix-zones were proposed to facilitate vehicles covertly transition to new ephemeral credentials. The resilience to (*syntactic* and *semantic*) pseudonym linking (attacks) highly depends on the geometry of the mix-zones, mobility patterns, vehicle density, and arrival rates. Our experimental results show that an eavesdropper could successfully link ≈73% of pseudonyms (during non-rush hours) and ≈62% of pseudonyms (during rush hours) after vehicles change their pseudonyms in a mix-zone. To mitigate such

inference attacks, we present a novel *cooperative mix-zone* scheme that enhances user privacy regardless of the vehicle mobility patterns, vehicle density, and arrival rate to the mix-zone. A subset of vehicles, termed *relaying vehicles*, are selected to be responsible for emulating non-existing vehicles. Such vehicles cooperatively disseminate decoy traffic without affecting safety-critical operations: with 50% of vehicles as relaying vehicles, the probability of linking pseudonyms (for the entire interval) drops from ≈68% to ≈18%. On average, this imposes 28 ms extra computation overhead, per second, on the Roadside Units (RSUs) and 4.67 ms extra computation overhead, per second, on the (relaying) vehicle side; it also introduces 1.46 KB/sec extra communication overhead by (relaying) vehicles and 45 KB/sec by RSUs for the dissemination of decoy traffic. Thus, user privacy is enhanced at the cost of low computation and communication overhead.

Contribution

The author of this thesis contributed to the design, implementation, and evaluation. The article was written by both authors.

5.11 Publications not included in this thesis

Proceedings

- Christian Vaas, Mohammad Khodaei, Panos Papadimitratos, Ivan Martinovic, *''Nowhere to hide? Mix-Zones for Private Pseudonym Change using Chaff Vehicles''*, In IEEE Vehicular Networking Conference (VNC), December 2018, Taipei, Taiwan.

Book Chapter

- Hongyu Jin, Mohammad Khodaei, Panos Papadimitratos, *''Security and Privacy in Vehicular Social Networks''*, In Vehicular Social Networks, Taylor & Francis Group, March 2016.

Technical Report

- Mohammad Khodaei and Panos Papadimitratos, *''Security and Privacy Challenges for Deploying On-road Electric Vehicle Charging''*.

Posters & Demos

- M. Khodaei and P. Papadimitratos, *''A Cooperative Location Privacy Protection Scheme for Vehicular Ad-hoc Networks''*, Cybersecurity and Privacy (CySeP) Summer School jointly with IEEE EuroS&P, Stockholm, Sweden, June, 2019.

- H. Noroozi, M. Khodaei, and P. Papadimitratos, *''VPKIaaS: Towards Scaling Pseudonymous Authentication for Large Mobile Systems''*, Cybersecurity and Privacy (CySeP) Summer School jointly with IEEE EuroS&P, Stockholm, Sweden, June, 2019.
- H. Noroozi, M. Khodaei, and P. Papadimitratos, *''Poster: Mix-Zones Everywhere: A Dynamic Cooperative Location Privacy Protection Scheme''*, in Proceedings of the IEEE Vehicular Networking Conference (VNC), Taipei, Taiwan, Dec. 2018.
- H. Noroozi, M. Khodaei, and P. Papadimitratos, *''DEMO: VPKIaaS: A Highly-Available and Dynamically-Scalable Vehicular Public-Key Infrastructure''*, in Proceedings of the ACM Conference on Security and Privacy in Wireless & Mobile Networks (WiSec), Stockholm, Sweden, June 2018.
- M. Khodaei, H. Noroozi, and P. Papadimitratos, *''POSTER: Privacy Preservation through Uniformity''*, in Proceedings of the ACM Conference on Security and Privacy in Wireless & Mobile Networks (WiSec), Stockholm, Sweden, June 2018.
- H. Noroozi, M. Khodaei, and P. Papadimitratos. *''VPKIaaS: A Highly-Available and Dynamically-Scalable Vehicular Public-Key Infrastructure''*, Cybersecurity and Privacy (CySeP) Summer School, Stockholm, Sweden, June, 2018.
- M. Khodaei and P. Papadimitratos. *''Security & Privacy for Vehicular Communication Systems''*, Cybersecurity and Privacy (CySeP) Summer School, Stockholm, Sweden, June, 2018.
- H. Noroozi, M. Khodaei, and P. Papadimitratos, *''A Highly Available and Dynamically Scalable Vehicular Public-Key Infrastructure (VPKI): VPKI as a Service (VPKIaaS)''*, Cybersecurity and Privacy (CySeP) Summer School, Stockholm, Sweden, June, 2017.
- M. Khodaei and P. Papadimitratos, *''Security & Privacy for Vehicular Communication Systems: The Key to Intelligent Transportation''*, Cybersecurity and Privacy (CySeP) Summer School, Stockholm, Sweden, June, 2017.
- M. Khodaei and P. Papadimitratos, *''Secure and Privacy-Preserving Vehicular Communication Systems: Identity and Credential Management Infrastructure''*, ITRL Conference on Integrated Transport: Connected and Automated Transport Systems, KTH, Stockholm, Sweden, Nov. 2016.
- M. Khodaei, and P. Papadimitratos, *''The Key to Intelligent Transportation: Identity and Credential Management for Vehicular Communication Systems''*, 4$^{\text{th}}$ ACCESS Industrial Workshop, Stockholm, Sweden, May 2016.

- M. Khodaei, and P. Papadimitratos, *''The Key to Intelligent Transportation: Identity and Credential Management for Vehicular Communication Systems''*, Cybersecurity and Privacy (CySeP) Winter School, Stockholm, Sweden, Oct. 2015.
- M. Khodaei, H. Jin and P. Papadimitratos, *''Deploying a Vehicular Credential Management System: Challenges Ahead''*, Cybersecurity and Privacy (CySeP) Winter School, Stockholm, Sweden, Oct. 2014.
- H. Jin, M. Khodaei and P. Papadimitratos, *''Secure and Privacy-enhancing Location-based Services''*, Cybersecurity and Privacy (CySeP) Winter School, Stockholm, Sweden, Oct. 2014.
- H. Jin, M. Khodaei and P. Papadimitratos, *''Privacy-preserving PKI for Location-based Services''*, Trust in the Digital Life (TDL), Vienna, Austria, Apr. 2014.

Chapter 6

Conclusions and Future Work

6.1 Summary of Contributions

This thesis systematically surveyed the state-of-the-art for security and privacy in the Vehicular Communication (VC) systems. More specifically, in the context of this thesis, we focused on security, privacy, and efficiency of an identity and credential management infrastructure for the VC systems. We proposed a Vehicular Public-Key Infrastructure (VPKI) that facilitates multi-domain operations in the VC systems and enhances user privacy in the presence of honest-but-curious VPKI entities. We developed a standard-compliant full-fledged, refined, cross-platform VPKI and we extensively evaluated our implementation to illuminate its efficiency, scalability and reliability.

More so, we proposed a practical framework to effectively distribute Certificate Revocation Lists (CRLs): our vehicle-centric scheme distributes necessary CRL pieces corresponding to a vehicle's targeted region and actual trip duration, i.e., obtaining only region- and time-relevant revocation information. Through extensive experimental evaluation, we demonstrated that our scheme is highly efficient and scalable, and it is resilient against selfish nodes, as well as pollution and Denial of Service (DoS) attacks. This supports that our scheme is a viable solution towards catalyzing the deployment of the secure and privacy-protecting VC systems. Our evaluation shows that the deployment of VPKI facilities can be cost-effective.

In order to enhance location privacy protection, i.e., mitigating syntactic and semantic linking attacks, we proposed a novel scheme to introduce broadcasting decoy traffic at each mix-zone. This protects user privacy regardless of the geometry of the mix-zones, mobility patterns, vehicle density, and arrival rates. Our system enhances user privacy protection at the cost of low computation and communication overhead while it ensures that the operation of the safety applications remains unaffected by the dissemination of decoy traffic.

6.2 Future Research

Although communications inside the mix-zones are cryptographically protected, the physical properties of wireless radio signals, e.g., Received Signal Strength Indication (RSSI), time of arrival, Doppler shift, etc. could be used by an adversary to localize and identify propagation path from a transmitter, e.g., [214]. Leveraging Radio Frequency (RF)-based characteristics, e.g., angle-of-arrival [60, 61], physical layer device identification [214, 215, 216], and physical layer localization with additional equipments, e.g., [217, 218, 219, 220], can localize vehicles based on the physical layer attributes of transmitters or identify decoy traffic from the actual traffic. Tracking an object using such properties, e.g., [220], raises privacy concerns as such interfaces are uniquely associated with a single vehicle. Beyond that, by leveraging our scheme to disseminate decoy traffic, an adversary could filter out chaff Cooperative Awareness Messages (CAMs) from the actual ones since both are originating from the same transmitter, e.g., based on the Doppler shift and RSSI [221, 222], or alternatively, by identifying the source Network Interface Card (NIC) of an IEEE 802.11 frame [214]. Leveraging these techniques to identify vehicles based on the signal's device-of-origin and track them accordingly requires a stronger adversary with more sophisticated resources to conduct such attacks. Mitigating inference based on physical layer device identification is one of our future work.

A stronger adversarial model for location privacy protection in Cryptographic Mix-Zones (CMIXs) would be any of the internal adversaries, including the non-cooperative vehicles joining the mix-zone, report the symmetric keys of the mix-zones and the observed communication to an external adversary. For example, a fraction of malicious vehicles or compromised RSUs could covertly send the CMIX symmetric key or the Cuckoo Filters (CFs) to other (internal or external) adversaries, thus, increasing pseudonyms linkability towards harming user privacy. Introducing chaff CAMs does not fully diminish the pseudonyms linkability in the presence of malicious vehicles or compromised RSUs. That requires introducing chaff CAMs combined with other techniques, e.g., simultaneously changing pseudonyms by all the vehicles inside a mix-zone, to fully diminish the syntactic and semantic linking attacks. This requires further investigation and remains as our future work.

Bibliography

[1] ‘‘Car to car communications a step closer,’’ Dec. 2012. [Online]. Available: https://www.itsinternational.com/its10/feature/car-car-communications-step-closer

[2] ‘‘U.S. Department of Transportation Announces Decision to Move Forward with Vehicle-to-Vehicle Communication Technology for Light Vehicles,’’ Feb. 2014. [Online]. Available: https://mobility21.cmu.edu/u-s-department-of-transportation-announces-decision-to-move-forward-with-vehicle-to-vehicle-communication-technology-for-light-vehicles/

[3] ‘‘Google Self-Driving Car Project.’’ [Online]. Available: https://waymo.com/

[4] M. Khodaei, ‘‘Secure and Privacy Preserving Vehicular Communication Systems: Identity and Credential Management Infrastructure,’’ Licentiate Thesis, Royal Institute of Technology (KTH), Stockholm, Sweden, Nov. 2016. [Online]. Available: http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-193030

[5] ETSI-TR-102-638, ‘‘Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions,’’ ETSI, Tech. Rep., Jun. 2009. [Online]. Available: https://www.etsi.org/deliver/etsi_tr/102600_102699/102638/01.01.01_60/tr_102638v010101p.pdf

[6] ‘‘IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages,’’ *IEEE Std 1609.2-2016 (Revision of IEEE Std 1609.2-2013)*, Mar. 2016. [Online]. Available: https://ieeexplore.ieee.org/document/7426684

[7] 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, May 2013. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6515060

[8] ‘‘ETSI TS 102 637-2, Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification

of Co-operative Awareness Basic Service,'' Mar. 2011. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/102600_102699/10263702/01.02.01_60/ts_10263702v010201p.pdf

[9] P. Papadimitratos, A. La Fortelle, K. Evenssen, R. Brignolo, and S. Cosenza, ''Vehicular Communication Systems: Enabling Technologies, Applications, and Future Outlook on Intelligent Transportation,'' *IEEE Communications Magazine*, vol. 47, no. 11, pp. 84--95, Nov. 2009. [Online]. Available: https://ieeexplore.ieee.org/document/5307471

[10] H. Jin, M. Khodaei, and P. Papadimitratos, ''Privacy-preserving PKI for Location-based Services,'' in *TDL - Trust in the Digital Life*, Vienna Austria, Apr. 2014. [Online]. Available: https://people.kth.se/~khodaei/files/posters/TDL_ATTPS.pdf

[11] ------, ''Secure and Privacy-enhancing Location-based Services,'' in *Cybersecurity and Privacy (CySeP) Winter School*, Stockholm, Sweden, Oct. 2014. [Online]. Available: https://people.kth.se/~khodaei/files/posters/TDL_ATTPS.pdf

[12] H. Jin and P. Papadimitratos, ''Resilient Privacy Protection for Location-Based Services Through Decentralization,'' *ACM Transactions on Privacy and Security (ACM TOPS)*, vol. 22, no. 4, pp. 21:1--36, Sep. 2019. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/3319401

[13] H. Jin, M. Khodaei, and P. Papadimitratos, ''Security and Privacy in Vehicular Social Networks,'' in *Vehicular Social Networks*. Taylor & Francis Group, Mar. 2016. [Online]. Available: https://people.kth.se/~papadim/publications/fulltext/Security-and-Privacy-in-Vehicular-Social-Networks.pdf

[14] ''ETSI TS 102 637-3, v1. 1.1, Intelligent Transport Systems (ITS). Vehicular Communications; Basic Set of Applications; Part 3: Specification of Decentralized Environmental Notification Basic Service,'' Sep. 2010. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/102600_102699/10263703/01.01.01_60/ts_10263703v010101p.pdf

[15] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, ''Secure Vehicular Communication Systems: Design and Architecture,'' *IEEE Communications Magazine*, vol. 46, no. 11, pp. 100--109, Nov. 2008. [Online]. Available: https://ieeexplore.ieee.org/document/4689252

[16] Car-to-Car Communication Consortium (C2C-CC), Jun. 2013. [Online]. Available: http://www.car-2-car.org/

[17] E. Sampson, ''The future looks bright for ITS,'' Jun. 2015. [Online]. Available: https://www.itsinternational.com/its10/its8/feature/future-looks-bright-its/

[18] B. Wiedersheim, Z. Ma, F. Kargl, and P. Papadimitratos, ‘‘Privacy in Inter-Vehicular Networks: Why Simple Pseudonym Change is not Enough,’’ in *IEEE International Conference on Wireless On-demand Network Systems and Services*, Kranjska Gora, Slovenia, Feb. 2010. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/5437115

[19] J. Krumm, ‘‘Inference Attacks on Location Tracks,’’ in *International Conference on Pervasive Computing*, Toronto, Canada, May 2007, pp. 127--143. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-540-72037-9_8

[20] P. LeBeau, ‘‘Ford exec backpedals after saying it tracks drivers,’’ Jan. 2014. [Online]. Available: http://www.cnbc.com/2014/01/09/ford-exec-backpedals-after-saying-it-tracks-drivers.html

[21] M. van Rijmenam, ‘‘The Re-Identification of Anonymous People With Big Data.’’ [Online]. Available: https://datafloq.com/read/re-identifying-anonymous-people-with-big-data/228

[22] Y.-A. De Montjoye, C. A. Hidalgo, M. Verleysen, and V. D. Blondel, ‘‘Unique in the crowd: The privacy bounds of human mobility,’’ *Scientific reports*, vol. 3, Feb. 2013. [Online]. Available: https://www.nature.com/articles/srep01376.pdf

[23] G. Greenwald, ‘‘NSA Prism Program Taps in to User Data of Apple, Google and Others,’’ Jun. 2013. [Online]. Available: http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

[24] S. Era and B. Preneel, ‘‘Cryptography and Information Security in the Post-Snowden Era,’’ May 2015. [Online]. Available: https://pdfs.semanticscholar.org/03ee/f5e2bf41a9656697d26969f3920ea2795052.pdf

[25] P. Papadimitratos, V. Gligor, and J.-P. Hubaux, ‘‘Securing Vehicular Communications-Assumptions, Requirements, and Principles,’’ in *Workshop on Embedded Security in Cars (ESCAR)*, Berlin, Germany, Nov. 2006, pp. 5--14. [Online]. Available: https://people.kth.se/~papadim/publications/fulltext/secure-vehicular-communication-requirements-fundamentals.pdf

[26] J. Golson, ‘‘Tesla driver killed in crash with Autopilot active, NHTSA investigating.’’ [Online]. Available: http://www.theverge.com/2016/6/30/12072408/tesla-autopilot-car-crash-death-autonomous-model-s

[27] Car-to-Car Communication Consortium (C2C-CC), ‘‘PKI Memo,’’ http://www.car-2-car.org/, Feb. 2011.

[28] A. Kung, ‘‘Security Architecture and Mechanisms for V2V/V2I, SeVeCom - Deliverable 2.1,’’ Feb. 2008. [Online]. Available: https://sevecom.eu/Deliverables/Sevecom_Deliverable_D2.1_v3.0.pdf

[29] P. Papadimitratos, L. Buttyan, J.-P. Hubaux, F. Kargl, A. Kung, and M. Raya, ''Architecture for Secure and Private Vehicular Communications,'' in *IEEE International Conference on ITS Telecommunications (ITST)*, Sophia Antipolis, Jun. 2007, pp. 1--6. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/4295890

[30] PRESERVE Project, www.preserve-project.eu/, Jun. 2015.

[31] W. Whyte, A. Weimerskirch, V. Kumar, and T. Hehn, ''A Security Credential Management System for V2V Communications,'' in *IEEE Vehicular Networking Conference (VNC)*, Boston, MA, Dec. 2013, pp. 1--8. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6737583

[32] ''Vehicle Safety Communications Security Studies: Technical Design of the Security Credential Management System - Final Report,'' Jul. 2016. [Online]. Available: https://www.regulations.gov/document?D=NHTSA-2015-0060-0004

[33] M. Khodaei and P. Papadimitratos, ''Secure and Privacy Preserving Vehicular Communication Systems: Identity and Credential Management Infrastructure,'' in *ITRL Conference on Integrated Transport: Connected and Automated Transport Systems*, Stockholm, Sweden, Nov. 2016. [Online]. Available: https://people.kth.se/~khodaei/files/talks/ITRL16/itrl16.pdf

[34] M. Khodaei, H. Jin, and P. Papadimitratos, ''Towards Deploying a Scalable & Robust Vehicular Identity and Credential Management Infrastructure,'' in *IEEE Vehicular Networking Conference (VNC)*, Paderborn, Germany, Dec. 2014. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7013306

[35] ------, ''SECMACE: Scalable and Robust Identity and Credential Management Infrastructure in Vehicular Communication Systems,'' *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 5, pp. 1430--1444, May 2018. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8332521

[36] ''Let's Encrypt Stats,'' https://letsencrypt.org/stats/, Jun. 2017.

[37] ''Comodo Certification Authority,'' https://ssl.comodo.com/, Oct. 2018.

[38] ''Symantec SSL/TLS Certificates,'' https://www.websecurity.digicert.com/ssl-certificate, Oct. 2018.

[39] J. Harding, G. Powell, R. Yoon, J. Fikentscher, C. Doyle, D. Sade, M. Lukuc, J. Simons, and J. Wang, ''V2V Communications: Readiness of V2V Technology for Application,'' U.S. Department of Transportation - National Highway Traffic Safety Administration - DOT HS 812 014, Tech. Rep., Aug. 2014. [Online]. Available: http://www.nhtsa.gov/staticfiles/rulemaking/pdf/V2V/Readiness-of-V2V-Technology-for-Application-812014.pdf

[40] R. Shokri, G. Theodorakopoulos, P. Papadimitratos, E. Kazemi, and J.-P. Hubaux, ‘‘Hiding in the Mobile Crowd: Location Privacy through Collaboration,’’ *IEEE Transactions on Dependable and Secure Computing*, vol. 11, no. 3, pp. 266--279, May 2014. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6682907

[41] E. Topalovic, B. Saeta, L.-S. Huang, C. Jackson, and D. Boneh, ‘‘Towards Short-lived Certificates,’’ *Web 2.0 Security and Privacy*, 2012. [Online]. Available: http://www.ieee-security.org/TC/W2SP/2012/papers/w2sp12-final9.pdf

[42] P. McDaniel and A. Rubin, ‘‘A Response to ‘‘Can We Eliminate Certificate Revocation Lists?’’,’’ in *FC (Springer)*, Berlin, Heidelberg, Feb. 2000, pp. 245--258. [Online]. Available: https://link.springer.com/chapter/10.1007/3-540-45472-1_17

[43] J. Clark and P. C. Van Oorschot, ‘‘SoK: SSL and HTTPS: Revisiting Past Challenges and Evaluating Certificate Trust Model Enhancements,’’ in *IEEE SnP*, Berkeley, USA, May 2013. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6547130

[44] M. Khodaei and P. Papadimitratos, ‘‘Efficient, Scalable, and Resilient Vehicle-Centric Certificate Revocation List Distribution in VANETs,’’ in *Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks (ACM WiSec)*, Stockholm, Sweden, Jun. 2018. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/3212480.3212481

[45] ------, ‘‘Scalable & Resilient Vehicle-Centric Certificate Revocation List Distribution in Vehicular Communication Systems,’’ *IEEE Transactions on Mobile Computing (TMC)*, 2020. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9042314

[46] ------, ‘‘The Key to Intelligent Transportation: Identity and Credential Management in Vehicular Communication Systems,’’ *IEEE Vehicular Technology Magazine*, vol. 10, no. 4, pp. 63--69, Dec. 2015. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7317862

[47] V. Kumar, J. Petit, and W. Whyte, ‘‘Binary Hash Tree based Certificate Access Management for Connected Vehicles,’’ in *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks (ACM WiSec)*, Boston, USA, Jul. 2017. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/3098243.3098257

[48] M. A. Simplicio Jr, E. L. Cominetti, H. K. Patil, J. E. Ricardini, and M. V. M. Silva, ‘‘ACPC: Efficient Revocation of Pseudonym Certificates using Activation Codes,’’ *Elsevier Ad Hoc Networks*, Jul. 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1570870518304761

[49] J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. Soong, and J. C. Zhang, ''What Will 5G Be?'' *IEEE Journal on Selected Areas in Communications (JSAC)*, vol. 32, no. 6, pp. 1065--1082, Jun. 2014. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6824752

[50] M. Agiwal, A. Roy, and N. Saxena, ''Next Generation 5G Wireless Networks: A Comprehensive Survey,'' *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 1617--1655, Feb. 2016. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7414384

[51] 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 (TVT)*, vol. 65, no. 12, pp. 9457--9470, Jul. 2016. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7513432

[52] I. Ari, B. Hong, E. L. Miller, S. A. Brandt, and D. D. Long, ''Managing Flash Crowds on the Internet,'' in *IEEE/ACM MASCOTS*, Orlando, FL, USA, Oct. 2003, pp. 246--249. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/1240667

[53] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, ''Efficient and Robust Pseudonymous Authentication in VANET,'' in *ACM VANET*, NY, USA, Sep. 2007, pp. 19--28. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/1287748.1287752

[54] P. Papadimitratos, G. Calandriello, J.-P. Hubaux, and A. Lioy, ''Impact of Vehicular Communications Security on Transportation Safety,'' in *IEEE INFOCOM Mobile Networking for Vehicular Environments (MOVE) Workshop (IEEE MOVE)*, Phoenix, AZ, USA, Apr. 2008, pp. 1--6. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/4544663

[55] 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 (TDSC)*, vol. 8, no. 6, pp. 898--912, Nov. 2011. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/5611547

[56] M. Khodaei, A. Messing, and P. Papadimitratos, ''RHyTHM: A Randomized Hybrid Scheme To Hide in the Mobile Crowd,'' in *IEEE Vehicular Networking Conference (VNC)*, Torino, Italy, Nov. 2017. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8275642

[57] Z. Ma, F. Kargl, and M. Weber, ''Pseudonym-on-demand: A New Pseudonym Refill Strategy for Vehicular Communications,'' in *IEEE Vehicular Technology Conference (VTC)*, Calgary, BC, Sep. 2008. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/4657287

[58] M. Khodaei and P. Papadimitratos, ‘‘Evaluating On-demand Pseudonym Acquisition Policies in Vehicular Communication Systems,’’ in *Proceedings of the First International Workshop on Internet of Vehicles and Vehicles of Internet (IoV/VoI)*, Paderborn, Germany, Jul. 2016. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/2938681.2938684

[59] J. R. Douceur, ‘‘The Sybil Attack,’’ in *ACM Peer-to-peer Systems*, London, UK, Mar. 2002. [Online]. Available: https://link.springer.com/chapter/10.1007/3-540-45748-8_24

[60] B. Xiao, B. Yu, and C. Gao, ‘‘Detection and Localization of Sybil Nodes in VANETs,’’ in *Proceedings of the 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks*, Los Angeles, CA, USA, Sep. 2006, pp. 1--8. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/1160972.1160974

[61] P. Golle, D. Greene, and J. Staddon, ‘‘Detecting and Correcting Malicious Data in VANETs,’’ in *Proceedings of the 1st ACM international workshop on Vehicular Ad Hoc Networks*, Philadelphia, Pennsylvania, USA, Oct. 2004, pp. 29--37. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/1023875.1023881

[62] H. Noroozi, M. Khodaei, and P. Papadimitratos, ‘‘A Highly Available and Dynamically Scalable Vehicular Public-Key Infrastructure (VPKI): VPKI as a Service (VPKIaaS),’’ in *Cybersecurity and Privacy (CySeP) Summer School*, Stockholm, Sweden, Jun. 2017. [Online]. Available: https://people.kth.se/~khodaei/files/posters/cysep17-vpkiaas.pdf

[63] ------, ‘‘DEMO: VPKIaaS: A Highly-Available and Dynamically-Scalable Vehicular Public-Key Infrastructure,’’ in *Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks (ACM WiSec)*, Stockholm, Sweden, Jun. 2018. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/3212480.3226100

[64] ------, ‘‘VPKIaaS: A Highly-Available and Dynamically-Scalable Vehicular Public-Key Infrastructure,’’ in *Cybersecurity and Privacy (CySeP) Summer School*, Stockholm, Sweden, Jun. 2018. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/3212480.3226100

[65] ------, ‘‘VPKIaaS: Towards Scaling Pseudonymous Authentication for Large Mobile Systems,’’ in *Cybersecurity and Privacy (CySeP) Summer School jointly with IEEE EuroS&P*, Stockholm, Sweden, Jun. 2019. [Online]. Available: https://people.kth.se/~khodaei/files/posters/cysep19-vpkiaas-poster.pdf

[66] P. Cincilla, O. Hicham, and B. Charles, ‘‘Vehicular PKI Scalability-Consistency Trade-Offs in Large Scale Distributed Scenarios,’’ in *IEEE*

Vehicular Networking Conference (VNC), Columbus, Ohio, USA, Dec. 2016. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7835970

[67] P. Papadimitratos, ‘‘"On the road" - Reflections on the Security of Vehicular Communication Systems,’’ in *IEEE Conference on Vehicular Electronics and Safety (ICVES)*, Columbus, OH, USA, Sep. 2008, pp. 359--363. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/4640913

[68] M. Raya, D. Jungels, P. Papadimitratos, I. Aad, and J.-P. Hubaux, ‘‘Certificate Revocation in Vehicular Networks,’’ EPFL, Switzerland, Tech. Rep., Jan. 2006. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.92.2291&rep=rep1&type=pdf

[69] L. Fischer, A. Aijaz, C. Eckert, and D. Vogt, ‘‘Secure revocable anonymous authenticated inter-vehicle communication (SRAAC),’’ in *4th Conference on Embedded Security in Cars (ESCAR)*. Berlin, Germany: Citeseer, Nov. 2006. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.71.1642&rep=rep1&type=pdf

[70] F. Stumpf, L. Fischer, and C. Eckert, ‘‘Trust, Security and Privacy in VANETs - a Multilayered Security Architecture for C2C-Communication,’’ in *VDI/VW-Gemeinschaftstagung: Automotive Security*, Wolfsburg, Germany, Nov. 2007, pp. 55--70. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.157.3809

[71] K. P. Laberteaux, J. J. Haas, and Y.-C. Hu, ‘‘Security Certificate Revocation List Distribution for VANET,’’ in *Proceedings of the fifth ACM international workshop on VehiculAr Inter-NETworking*, New York, NY, USA, Sep. 2008. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/1410043.1410063

[72] J. J. Haas, Y.-C. Hu, and K. P. Laberteaux, ‘‘Design and Analysis of a Lightweight Certificate Revocation Mechanism for VANET,’’ in *Proceedings of the sixth ACM international workshop on VehiculAr InterNETworking*, New York, NY, USA, Sep. 2009. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/1614269.1614285

[73] F. Schaub, Z. Ma, and F. Kargl, ‘‘Privacy Requirements in Vehicular Communication Systems,’’ in *IEEE International Conference on Computational Science and Engineering (CSE).*, vol. 3, Vancouver, BC, Canada, Aug. 2009, pp. 139--145. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/5283398

[74] J. J. Haas, Y.-C. Hu, and K. P. Laberteaux, ‘‘Efficient Certificate Revocation List Organization and Distribution,’’ *IEEE Journal on Selected Areas in Communications (JSAC)*, vol. 29, no. 3, pp. 595--604, Feb. 2011. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/5719271

[75] M. Gerlach and F. Guttler, ‘‘Privacy in VANETs using Changing Pseudonyms - Ideal and Real,’’ in *IEEE Vehicular Technology Conference (VTC)*, Dublin, Ireland, Apr. 2007. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/4212947

[76] L. Buttyán, T. Holczer, A. Weimerskirch, and W. Whyte, ‘‘SLOW: A Practical Pseudonym Changing Scheme for Location Privacy in VANETs,’’ in *IEEE Vehicular Networking Conference (VNC)*, Tokyo, Japan, Oct. 2009, pp. 1--8. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/5416380

[77] M. Khodaei, H. Noroozi, and P. Papadimitratos, ‘‘POSTER: Privacy Preservation through Uniformity,’’ in *Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks (ACM WiSec)*, Stockholm, Sweden, Jun. 2018, pp. 279--280. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/3212480.3226101

[78] ETSI-EN-302-637-2-V1.3.2, ‘‘Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service,’’ ETSI EN 302 637-2 V1.3.2, Nov. 2014. [Online]. Available: https://www.etsi.org/deliver/etsi_en/302600_302699/30263702/01.03.02_60/en_30263702v010302p.pdf

[79] M. Ullmann, T. Strubbe, and C. Wieschebrink, ‘‘Technical Limitations, and Privacy Shortcomings of the Vehicle-to-Vehicle Communication,’’ in *Proceedings of the IARIA VEHICULAR Conference*, Barcelona, Spain, Nov. 2016. [Online]. Available: https://smartmobilitycommunity.eu/sites/default/files/images/vehicular_2016_2_20_30014.pdf

[80] S. Bai, ‘‘US-EU V2V V2I Message Set Standards Collaboration,’’ https://docbox.etsi.org/workshop/2014/201402_ITSWORKSHOP/S02_ITS_SomeBitsFromtheWorld/HONDA_BAI.pdf, Feb. 2013.

[81] K. Emara, W. Woerndl, and J. Schlichter, ‘‘Vehicle Tracking using Vehicular Network Beacons,’’ in *IEEE International Symposium on ‘‘A World of Wireless, Mobile and Multimedia Networks’’ (WoWMoM)*, Madrid, Spain, Jun. 2013. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6583473

[82] K. Emara, ‘‘Poster: PREXT: Privacy Extension for Veins VANET Simulator,’’ in *IEEE Vehicular Networking Conference (VNC)*, Columbus, OH, USA, Dec. 2016. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7835979

[83] M. Gruteser and X. Liu, ‘‘Protecting Privacy in Continuous Location-Tracking Applications,’’ *IEEE Security & Privacy*, no. 2, pp. 28--34, Mar. 2004. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/1281242

[84] P. Golle and K. Partridge, ''On the Anonymity of Home/Work Location Pairs,'' in *Pervasive computing*. Nara, Japan: Springer, Berlin, Heidelberg, May 2009, vol. 5538, pp. 390--397. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-642-01516-8_26

[85] C. Y. Ma, D. K. Yau, N. K. Yip, and N. S. Rao, ''Privacy Vulnerability of Published Anonymous Mobility Traces,'' *IEEE/ACM transactions on networking (TON)*, vol. 21, no. 3, pp. 720--733, Jun. 2013. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/1859995.1860017

[86] M. Khodaei and P. Papadimitratos, ''Cooperative Location Privacy in Vehicular Networks: Why Simple Mix-zones are not Enough,'' *Submitted to IEEE Internet Of Things Journal*. [Online]. Available: http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-273027

[87] M. Khodaei, H. Noroozi, and P. Papadimitratos, ''Scaling Pseudonymous Authentication for Large Mobile Systems,'' in *Proceedings of the 12th ACM Conference on Security & Privacy in Wireless and Mobile Networks (ACM WiSec)*, Miami, FL, USA, May 2019. [Online]. Available: https://dl.acm.org/doi/10.1145/3317549.3323410

[88] ETSI, ''ETSI TS 103 097 v1.2.1-Intelligent Transport Systems (ITS); Security; Security Header and Certificate Formats,'' ETSI TS 103 097, Jun. 2015. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/103000_103099/103097/01.02.01_60/ts_103097v010201p.pdf

[89] ETSI TR 102 731, ''Intelligent Transport Systems (ITS); Security; Security Services and Architecture,'' Sep. 2009. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/102700_102799/102731/01.01.01_60/ts_102731v010101p.pdf

[90] ETSI TR 102 941, ''Intelligent Transport Systems (ITS); Security; Trust and Privacy Management,'' Jun. 2012. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/102900_102999/102941/01.01.01_60/ts_102941v010101p.pdf

[91] M. Gerlach, F. Friederici, P. Ardelean, and P. Papadimitratos, ''Security Demonstration,'' in *Car-to-Car Communication Consortium (C2C-CC) Forum and Demonstration*, Dudenhofen, Germany, Oct. 2008. [Online]. Available: http://www.broadbit.net/portal/?tag=c2c-cc

[92] N. Bißmeyer, H. Stubing, E. Schoch, S. Gotz, J. P. Stotz, and B. Lonc, ''A Generic Public Key Infrastructure for Securing Car-to-X Communication,'' in *ITS World Congress*, Orlando, Florida, USA, Oct. 2011. [Online]. Available: https://www.researchgate.net/profile/Brigitte_Lonc/publication/268100474_A_Generic_Public_Key_Infrastructure_for_Securing_Car-to-X_Communication/links/55954faa08ae793d137affc8.pdf

[93] F. Kargl, P. Papadimitratos, L. Buttyan, M. Muter, E. Schoch, B. Wiedersheim, T.-V. Thong, G. Calandriello, A. Held, and A. Kung, ''Secure Vehicular Communication Systems: Implementation, Performance, and Research Challenges,'' *IEEE Communications Magazine*, vol. 46, no. 11, pp. 110--118, Nov. 2008. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/4689253

[94] F. Kargl, P. Papadimitratos, T. Holczer, S. Cosenza, A. Held, M. Mütter, N. Asaj, P. Ardelean, D. de Cock, M. Sall, and B. Wiedersheim, ''Secure Vehicle Communication (demo),'' in *ACM International Conference on Mobile Systems, Applications and Services (ACM MobiSys)*, Jul. 2009. [Online]. Available: https://www.sigmobile.org/mobisys/2009/wip.html

[95] J. P. Stotz, N. Bißmeyer, F. Kargl, S. Dietzel, P. Papadimitratos, and C. Schleiffer, ''Security Requirements of Vehicle Security Architecture, PRESERVE - Deliverable 1.1,'' www.preserve-project.eu/, Jun. 2011.

[96] M. Laganà, M. Feiri, M. Sall, A. Lange, A. Tomatis, and P. Papadimitratos, ''Secure Communication in Vehicular Networks: PRESERVE VSS Kit 1 Demo,'' in *IEEE International Symposium on Wireless Vehicular Communications (IEEE WiVec)*, Dresden, Germany, Jun. 2013. [Online]. Available: https://people.kth.se/~papadim/publications/fulltext/VNC-2012-PRESERVE-demo_camera-ready.pdf

[97] M. Khodaei, H. Jin, and P. Papadimitratos, ''Deploying a Vehicular Credential Management System: Challenges Ahead,'' in *Cybersecurity and Privacy (CySeP) Winter School*, Stockholm, Sweden, Oct. 2014. [Online]. Available: https://people.kth.se/~khodaei/files/posters/cysep14.pdf

[98] S. Giannetsos, S. Gisdakis, H. Jin, M. Khodaei, and P. Papadimitratos, ''Secure Communication in Vehicular Network, Demo and Static Testbed,'' in *Cyber-Security and Privacy Winter School (CySeP)*, Stockholm, Sweden, Oct. 2015.

[99] M. Khodaei and P. Papadimitratos, ''The Key to Intelligent Transportation: Identity and Credential Management for Vehicular Communication Systems,'' in *Cybersecurity and Privacy (CySeP) Winter School*, Stockholm, Sweden, Oct. 2015. [Online]. Available: https://people.kth.se/~khodaei/files/posters/cysep15.pdf

[100] ------, ''The Key to Intelligent Transportation: Identity and Credential Management for Vehicular Communication Systems,'' in 4^{th} *ACCESS Industrial Workshop*, Stockholm, Sweden, May 2016. [Online]. Available: https://people.kth.se/~khodaei/files/posters/access16.pdf

[101] S. Gisdakis, M. Laganà, T. Giannetsos, and P. Papadimitratos, ''SEROSA: SERvice Oriented Security Architecture for Vehicular Communications,'' in

IEEE Vehicular Networking Conference (VNC), Boston, MA, USA, Dec. 2013. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6737597

[102] 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*, Nov. 2007. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/4357367

[103] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, ''ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications,'' in *IEEE Conference on Computer Communications (INFOCOM)*, Phoenix, AZ, USA, Apr. 2008. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/4509774

[104] D. Boneh and H. Shacham, ''Group Signatures with Verifier-Local Revocation,'' in *Proceedings of the 11th ACM conference on Computer and communications security*, NY, USA, Oct. 2004. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/1030083.1030106

[105] D. Förster, H. Löhr, and F. Kargl, ''PUCA: A Pseudonym Scheme with User-Controlled Anonymity for Vehicular Ad-Hoc Networks (VANET),'' in *IEEE Vehicular Networking Conference (VNC)*, Paderborn, Germany, Dec. 2014. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7013305

[106] N. Ristanovic, P. Papadimitratos, G. Theodorakopoulos, J.-P. Hubaux, and J.-Y. Le Boudec, ''Adaptive Message Authentication for Multi-hop Networks,'' in *IEEE International Conference on Wireless On-Demand Network Systems and Services*, Bardonecchia, Italy, Jan. 2011, pp. 96--103. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/5720206

[107] H. Jin and P. Papadimitratos, ''Scaling VANET Security through Cooperative Message Verification,'' in *IEEE Vehicular Networking Conference (VNC)*, Kyoto, Japan, Dec. 2015, pp. 275--278. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7385588

[108] ------, ''DoS-resilient Cooperative Beacon Verification for Vehicular Communication Systems,'' *Ad Hoc Networks*, vol. 90, p. 101775, Jul. 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1570870518307108

[109] N. Bißmeyer, J. Petit, and K. M. Bayarou, ''CoPRA: Conditional Pseudonym Resolution Algorithm in VANETs,'' in *IEEE Conference on Wireless On-demand Network Systems and Services (WONS)*, Banff, Canada, Mar. 2013, pp. 9--16. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6578314

[110] F. Schaub, F. Kargl, Z. Ma, and M. Weber, ''V-tokens for Conditional Pseudonymity in VANETs,'' in *IEEE Wireless Communication and Networking Conference (WCNC)*, Sydney, Australia, Apr. 2010, pp. 1--6. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/5506126

[111] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux, ''Eviction of Misbehaving and Faulty Nodes in Vehicular Networks,'' *IEEE Journal on Selected Areas in Communications (JSAC)*, pp. 1557--1568, Oct. 2007. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/4346443

[112] J. Camenisch, S. Hohenberger, M. Kohlweiss, A. Lysyanskaya, and M. Meyerovich, ''How to Win the Clonewars: Efficient Periodic n-Times Anonymous Authentication,'' in *ACM Conference on Computer and Communications Security (CCS)*, Oct. 2006, pp. 201--210. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/1180405.1180431

[113] J. Freudiger, M. Raya, M. Félegyházi, P. Papadimitratos, and J.-P. Hubaux, ''Mix-zones for Location Privacy in Vehicular Networks,'' in *Win-ITS*, Vancouver, BC, Canada, Aug. 2007. [Online]. Available: https://people.kth.se/~papadim/publications/fulltext/location-privacy-mix-zones-vanet.pdf

[114] R. Lu, X. Li, T. H. Luan, X. Liang, and X. Shen, ''Pseudonym Changing at Social Spot: An Effective Strategy for Location Privacy in VANETs,'' *IEEE Transactions on Vehicular Technology (TVT)*, vol. 61, no. 1, pp. 86--96, Jan. 2012. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/5960806

[115] S. Eichler, ''Strategies for Pseudonym Changes in Vehicular Ad Hoc Networks Depending on Node Mobility,'' in *IEEE Intelligent Vehicles Symposium*, Istanbul, Turkey, Jun. 2007, pp. 541--546. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/4290171

[116] P. Papadimitratos, A. Kung, J.-P. Hubaux, and F. Kargl, ''Privacy and Identity Management for Vehicular Communication Systems: a Position Paper,'' in *Workshop on standards for privacy in user-centric identity management*, Zurich, Switzerland, Jul. 2006. [Online]. Available: https://infoscience.epfl.ch/record/94374

[117] M. Gerlach, ''Assessing and Improving Privacy in VANETs,'' in *Workshop on Embedded Security in Cars (ESCAR)*, Berlin, Germany, Nov. 2006. [Online]. Available: https://www.semanticscholar.org/paper/Full-Paper-%3A-Assessing-and-Improving-Privacy-in-Gerlach/32c807631d9bb4c16c5ccd0eebc81e97e3a8be58

[118] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki, ''CARAVAN: Providing Location Privacy for VANET,'' in

Workshop on Embedded Security in Cars (ESCAR), Cologne, Germany, Nov. 2005. [Online]. Available: https://apps.dtic.mil/docs/citations/ADA459198

[119] M. Gerlach, A. Festag, T. Leinmüller, G. Goldacker, and C. Harsch, ''Security Architecture for Vehicular Communication,'' in *Workshop on Intelligent Transportation*, Hamburg, Germany, Mar. 2007. [Online]. Available: http://www.leinmueller.de/lib/exe/fetch.php/publications/wit07secarch.pdf

[120] P. Papadimitratos, G. Mezzour, and J.-P. Hubaux, ''Certificate Revocation List Distribution in Vehicular Communication Systems,'' in *ACM VANET*, San Francisco, CA, Sep. 2008, pp. 86--87. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/1410043.1410062

[121] M. E. Nowatkowski and H. L. Owen, ''Certificate Revocation List Distribution in VANETs Using Most Pieces Broadcast,'' in *Proceedings of the IEEE SoutheastCon*, Concord, NC, USA, Mar. 2010. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/5453881

[122] M. Nowatkowski, C. McManus, J. Wolfgang, and H. Owen III, ''Cooperative Certificate Revocation List Distribution Methods in VANETs,'' in *Ad Hoc Networks*. Springer, Sep. 2009, pp. 652--665. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-642-11723-7_44

[123] E. N. Michael and L. O. Henry, ''Scalable Certificate Revocation List Distribution in Vehicular Ad Hoc Networks,'' in *IEEE GLOBECOM Workshops*, Miami, FL, USA, Dec. 2010, pp. 54--58. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/5700380

[124] P. Ardelean and P. Papadimitratos, ''Implementation and Evaluation of Certificate Revocation List Distribution for Vehicular Ad-hoc Networks,'' http://secowinetcourse.epfl.ch/previous/08/Ardelean.Petra/Final_Report.pdf, EPFL, Tech. Rep., Jan. 2009.

[125] H.-C. Hsiao, A. Studer, C. Chen, A. Perrig, F. Bai, B. Bellur, and A. Iyer, ''Flooding-Resilient Broadcast Authentication for VANETs,'' in *ACM Mobile Computing and Networking*, Las Vegas, Nevada, USA, Sep. 2011. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/2030613.2030635

[126] V. T. Nguyen, J. Jose, X. Wu, and T. Richardson, ''Secure Content Distribution in Vehicular Networks,'' *arXiv e-prints*, p. arXiv:1601.06181, Jan. 2016. [Online]. Available: https://arxiv.org/abs/1601.06181

[127] B. H. Bloom, ''Space/Time Trade-offs in Hash Coding with Allowable Errors,'' *Communications of the ACM*, vol. 13, no. 7, pp. 422--426, Jul. 1970. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/362686.362692

[128] M. Mitzenmacher, ‘‘Compressed Bloom Filters,’’ *IEEE transactions on networking*, vol. 10, no. 5, pp. 604--612, Dec. 2002. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/1041067

[129] K. Rabieh, M. Pan, Z. Han, and V. Ford, ‘‘SRPV: A Scalable Revocation Scheme for Pseudonyms-Based Vehicular Ad Hoc Networks,’’ in *IEEE International Conference on Communications (ICC)*, Kansas City, MO, USA, May 2018, pp. 1--6. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8422736

[130] M. Khodaei and P. Papadimitratos, ‘‘A Cooperative Location Privacy Protection Scheme for Vehicular Ad-hoc Networks,’’ in *Cybersecurity and Privacy (CySeP) Summer School jointly with IEEE EuroS&P*, Stockholm, Sweden, Jun. 2019. [Online]. Available: https://people.kth.se/~khodaei/files/posters/cysep19-cmix-poster.pdf

[131] C. Vaas, M. Khodaei, P. Papadimitratos, and I. Martinovic, ‘‘Nowhere to hide? Mix-Zones for Private Pseudonym Change using Chaff Vehicles,’’ in *IEEE Vehicular Networking Conference (VNC)*, Taipei, Taiwan, Dec. 2018. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8628449

[132] M. Khodaei and P. Papadimitratos, ‘‘Poster: Mix-Zones Everywhere: A Dynamic Cooperative Location Privacy Protection Scheme,’’ in *IEEE Vehicular Networking Conference (VNC)*, Taipei, Taiwan, Dec. 2018. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8628340

[133] G. Rigazzi, A. Tassi, R. J. Piechocki, T. Tryfonas, and A. Nix, ‘‘Optimized Certificate Revocation List Distribution for Secure V2X Communications,’’ in *IEEE Vehicular Technology Conference (VTC)*, Toronto, ON, Canada, Sep. 2017. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8288287

[134] M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams, ‘‘X. 509 Internet Public Key Infrastructure Online Certificate Status Protocol-OCSP,’’ RFC 2560, Tech. Rep., Jun. 1999. [Online]. Available: https://dl.acm.org/doi/pdf/10.17487/RFC2560

[135] G. Marias, K. Papapanagiotou, and P. Georgiadis, ‘‘ADOPT: A Distributed OCSP for Trust Establishment in MANETs,’’ in *European Wireless Conference*, Nicosia, Cyprus, Apr. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/5755348

[136] J. Forné, J. L. Muñoz, O. Esparza, and F. Hinarejos, ‘‘Certificate Status Validation in Mobile Ad Hoc Networks,’’ *IEEE Wireless Communications*, vol. 16, no. 1, Mar. 2009. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/4804369

[137] C. Gañán, J. L. Muñoz, O. Esparza, J. Mata-Díaz, and J. Alins, ''Toward Revocation Data Handling Efficiency in VANETs,'' in *Springer Nets4Cars/Nets4Trains*, Vilnius, Lithuania, Apr. 2012. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-642-29667-3_7

[138] C. Gañán, J. L. Muñoz, O. Esparza, J. Mata-Díaz, J. Hernández-Serrano, and J. Alins, ''COACH: Collaborative Certificate Status Checking Mechanism for VANETs,'' *Network and Computer Applications*, vol. 36, no. 5, Sep. 2013. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804512000616

[139] C. Gañán, J. L. Muñoz, O. Esparza, J. Loo, J. Mata-Díaz, and J. Alins, ''BECSI: Bandwidth Efficient Certificate Status Information Distribution Mechanism for VANETs,'' *Hindawi-MIS*, vol. 9, no. 4, pp. 347--370, Mar. 2013. [Online]. Available: https://core.ac.uk/download/pdf/83951457.pdf

[140] T. Moore, M. Raya, J. Clulow, P. Papadimitratos, R. Anderson, and J.-P. Hubaux, ''Fast Exclusion of Errant Devices from Vehicular Networks,'' in *IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*, San Francisco, CA, Jun. 2008, pp. 135--143. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/4557749

[141] A. Wasef and X. Shen, ''EDR: Efficient Decentralized Revocation Protocol for Vehicular Ad hoc Networks,'' *IEEE Transactions on Vehicular Technology (TVT)*, vol. 58, no. 9, pp. 5214--5224, May 2009. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/4967903

[142] N. Bißmeyer, ''Misbehavior Detection and Attacker Identification in Vehicular Ad Hoc Networks,'' Ph.D. dissertation, Darmstadt University of Technology, Germany, Dec. 2014. [Online]. Available: http://tuprints.ulb.tu-darmstadt.de/4257/

[143] D. Förster, H. Löhr, J. Zibuschka, and F. Kargl, ''REWIRE–Revocation Without Resolution: A Privacy-Friendly Revocation Mechanism for Vehicular Ad-Hoc Networks,'' in *Trust and Trustworthy Computing*, Heraklion, Greece, Aug. 2015. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-319-22846-4_12

[144] S. Micali, ''Scalable Certificate Validation and Simplified PKI Management,'' in *1st Annual PKI research workshop*, vol. 15, 2002. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.128.1775&rep=rep1&type=pdf

[145] J. A. Solworth, ''Instant Revocation,'' in *European PKI*, Trondheim, Norway, Jun. 2008. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-540-69485-4_3

[146] J. Iliadis, S. Gritzalis, D. Spinellis, D. De Cock, B. Preneel, and D. Gritzalis, ''Towards a Framework for Evaluating Certificate Status Information Mechanisms,'' *Elsevier ComCom*, vol. 26, no. 16, pp. 1839--1850, Jan. 2003. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0140366403000793

[147] D. Cooper, ''A More Efficient Use of Delta-CRLs,'' in *IEEE S&P*, CA, USA, May 2000. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/848456

[148] S. Micali, ''Efficient Certificate Revocation,'' Mar. 1996. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.17.1875

[149] A.-A. Chariton and e al, ''CCSP: a Compressed Certificate Status Protocol,'' in *IEEE Conference on Computer Communications (INFOCOM)*, Atlanta, GA, USA, May 2017. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8057065/

[150] J. Larisch, D. Choffnes, D. Levin, B. M. Maggs, A. Mislove, and C. Wilson, ''CRLite: A Scalable System for Pushing All TLS Revocations to All Browsers,'' in *IEEE Symposium on SnP*, San Jose, CA, USA, May 2017. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7958597

[151] M. A. S. Junior, E. L. Cominetti, H. K. Patil, J. Ricardini, L. Ferraz, and M. V. Silva, ''Privacy-preserving Method for Temporarily Linking/Revoking Pseudonym Certificates in VANETs,'' in *IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, New York, NY, USA, Aug. 2018, pp. 1322--1329. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8456051

[152] M. A. Simplicio Jr, E. L. Cominetti, and H. K. Patil, ''Privacy-preserving Linkage/Revocation of VANET Certificates without LAs,'' in *IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, Aug. 2018. [Online]. Available: https://eprint.iacr.org/2018/788.pdf

[153] ETSI, ''Intelligent Transport Systems (ITS); Security; ITS Communications Security Architecture and Security Management,'' ETSI TS 102-940, Nov. 2016. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/102900_102999/102940/01.02.01_60/ts_102940v010201p.pdf

[154] ------, ''Intelligent Transport Systems (ITS); Security; Security Header and Certificate Formats,'' ETSI TS 103-097, Jun. 2015. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/103000_103099/103097/01.02.01_60/ts_103097v010201p.pdf

[155] ------, ''Intelligent Transport Systems (ITS); Security; Stage 3 Mapping for IEEE 1609.2,'' ETSI TS 102-867, Jun. 2012. [Online]. Available: https://archive.org/details/etsi_ts_102_867_v01.01.01/page/n9/mode/2up

[156] J. Bellatti, A. Brunner, J. Lewis, P. Annadata, W. Eltarjaman, R. Dewri, and R. Thurimella, ''Driving Habits Data: Location Privacy Implications and Solutions,'' in *IEEE Security & Privacy*, vol. 38, no. 1, Jan. 2017, pp. 12--20. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7854104

[157] S. Narain, T. D. Vo-Huu, K. Block, and G. Noubir, ''Inferring User Routes and Locations Using Zero-Permission Mobile Sensors,'' in *IEEE S&P*, San Jose, CA, USA, May 2016, pp. 397--413. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7546514

[158] X. Gao, B. Firner, S. Sugrim, V. Kaiser-Pendergrast, Y. Yang, and J. Lindqvist, ''Elastic Pathing: Your Speed is Enough to Track You,'' in *Proceedings of the ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp)*, Seattle, Washington, Sep. 2014, pp. 975--986. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/2632048.2632077

[159] Q. Technologies, ''Leading the World to 5G: Cellular Vehicle-to-Everything (C-V2X) Technologies,'' https://www.qualcomm.com/media/documents/files/cellular-vehicle-to-everything-c-v2x-technologies.pdf, Jun. 2016.

[160] A. R. Beresford and F. Stajano, ''Mix zones: User Privacy in Location-Aware Services,'' in *IEEE Annual Conference on Pervasive Computing and Communications Workshops*, Orlando, FL, USA, Mar. 2004, pp. 127--131. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/1276918

[161] C. Cornelius, A. Kapadia, D. Kotz, D. Peebles, M. Shin, and N. Triandopoulos, ''Anonysense: Privacy-Aware People-Centric Sensing,'' in *Proceedings of the 6th international conference on Mobile systems, applications, and services.* ACM, Jun. 2008, pp. 211--224. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/1378600.1378624

[162] R. Yu, J. Kang, X. Huang, S. Xie, Y. Zhang, and S. Gjessing, ''MixGroup: Accumulative Pseudonym Exchanging for Location Privacy Enhancement in Vehicular Social Networks,'' *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 1, pp. 93--105, Jan. 2016. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7042791

[163] M. Gruteser and D. Grunwald, ''Anonymous Usage of Location-based Services Through Spatial and Temporal Cloaking,'' in *ACM MobiSys*, San Francisco, USA, May 2003, pp. 31--42. [Online]. Available: https://dl.acm.org/doi/pdf/10.1145/1066116.1189037

[164] ''ETSI TS 102 637-2, Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Co-operative Awareness Basic Service,'' Mar. 2011. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/102600_102699/10263702/01.02.01_60/ts_10263702v010201p.pdf

[165] D. Boneh, X. Boyen, and H. Shacham, ''Short Group Signatures,'' in *Advances in Cryptology CRYPTO*. Springer, 2004. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-540-28628-8_3

[166] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki, ''Enhancing Wireless Location Privacy using Silent Period,'' in *IEEE Wireless Communication and Networking Conference (WCNC)*, New Orleans, LA, USA, Mar. 2005. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/1424677

[167] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, ''AMOEBA: Robust Location Privacy Scheme for VANET,'' *IEEE Journal on Selected Areas in Communications (JSAC)*, vol. 25, no. 8, pp. 1569--1589, Oct. 2007. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/4346444

[168] G. P. Corser, A. Arenas, and H. Fu, ''Effect on Vehicle Safety of Nonexistent or Silenced Basic Safety Messages,'' in *ICNC*, Kauai, HI, USA, Feb. 2016, pp. 1--5. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7440550

[169] 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 WiSec)*, New York, NY, USA, Jun. 2015. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/2766498.2766500

[170] D. Förster, H. Löhr, A. Grätz, J. Petit, and F. Kargl, ''An Evaluation of Pseudonym Changes for Vehicular Networks in Large-Scale, Realistic Traffic Scenarios,'' *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 10, pp. 3400--3405, Dec. 2017. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8214224

[171] A. Tomandl, F. Scheuer, and H. Federrath, ''Simulation-based Evaluation of Techniques for Privacy Protection in VANETs,'' in *IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, Barcelona, Spain, Oct. 2012. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6379070

[172] A. Wasef and X. Shen, ''REP: Location Privacy for VANETs Using Random Encryption Periods,'' *Mobile Networks and Applications*, vol. 15, no. 1, pp. 172--185, Feb. 2010. [Online]. Available: https://link.springer.com/article/10.1007/s11036-009-0175-4

[173] N. Ravi, C. M. Krishna, and I. Koren, ''Enhancing Vehicular Anonymity in ITS: A New Scheme for Mix Zones and Their Placement,'' *IEEE Transactions on Vehicular Technology (TVT)*, Aug. 2019. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8809087/

[174] B. Palanisamy and L. Liu, ''Attack-Resilient Mix-zones over Road Networks: Architecture and Algorithms,'' *IEEE Transactions on Mobile Computing (TMC)*, vol. 14, no. 3, pp. 495--508, Mar. 2015. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6815691

[175] ------, ''Mobimix: Protecting Location Privacy with Mix-zones Over Road Networks,'' in *IEEE 27th International Conference on Data Engineering*, Hannover, Germany, Apr. 2011, pp. 494--505. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/5767898

[176] N. Guo, L. Ma, and T. Gao, ''Independent Mix Zone for Location Privacy in Vehicular Networks,'' *IEEE Access*, vol. 6, pp. 16 842--16 850, Apr. 2018. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8278175

[177] M. Li, K. Sampigethaya, L. Huang, and R. Poovendran, ''Swing & Swap: User-centric Approaches Towards Maximizing Location Privacy,'' in *ACM WPES*, Alexandria, Virginia, USA, Oct. 2006, pp. 19--28. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/1179601.1179605

[178] P. Papadimitratos, M. Poturalski, P. Schaller, P. Lafourcade, D. Basin, S. Capkun, and J.-P. Hubaux, ''Secure Neighborhood Discovery: A Fundamental Element for Mobile Ad Hoc Networking,'' *IEEE Communications Magazine*, vol. 46, no. 2, pp. 132--139, Feb. 2008. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/4473095

[179] M. Poturalski, P. Papadimitratos, and J. P. Hubaux, ''Formal Analysis of Secure Neighbor Discovery in Wireless Networks,'' *IEEE Transactions on Dependable and Secure Computing (IEEE TDSC)*, vol. 10, no. 6, pp. 355--367, November 2013. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6522408

[180] M. Fiore, C. Casetti, C. Chiasserini, and P. Papadimitratos, ''Discovery and Verification of Neighbor Positions in Mobile Ad Hoc Networks,'' *IEEE Transactions on Mobile Computing*, vol. 12, no. 2, pp. 289--303, Feb. 2013. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6104050

[181] A. Festag, P. Papadimitratos, and T. Tielert, ''Design and Performance of Secure Geocast for Vehicular Communication,'' *IEEE Transactions on Vehicular Technology (TVT)*, vol. 59, no. 5, pp. 2456--2471, Jun. 2010. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/5431029

[182] E. Schoch, F. Kargl, T. Leinmüller, S. Schlott, and P. Papadimitratos, ''Impact of Pseudonym Changes on Geographic Routing in VANETs,'' *European Workshop on Security and Privacy in Ad hoc and Sensor Networks (ESAS)*, pp. 43--57, Sep. 2006. [Online]. Available: https://link.springer.com/chapter/10.1007/11964254_6

[183] M. Raya, P. Papadimitratos, V. D. Gligor, and J.-P. Hubaux, ''On Data-Centric Trust Establishment in Ephemeral Ad Hoc Networks,'' in *IEEE Conference on Computer Communications (INFOCOM)*, Phoenix, AZ, Apr. 2008. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/4509775

[184] S. Gisdakis, T. Giannetsos, and P. Papadimitratos, ''SPPEAR: Security and Privacy-preserving Architecture for Participatory-sensing Applications,'' in *ACM Conference on Security & Privacy in Wireless and Mobile Networks (ACM WiSec)*, Oxford, United Kingdom, Jul. 2014, pp. 39--50. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/2627393.2627402

[185] ------, ''SHIELD: A Data Verification Framework for Participatory Sensing Systems,'' in *ACM Conference on Security & Privacy in Wireless and Mobile Networks (ACM WiSec)*, New York, NY, USA, Jun. 2015, pp. 16:1--16:12. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/2766498.2766503

[186] ------, ''Security, Privacy, and Incentive Provision for Mobile Crowd Sensing Systems,'' *IEEE Internet of Things Journal*, vol. 3, no. 5, pp. 839--853, Oct. 2016. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7463023

[187] R. Shokri, P. Papadimitratos, and J.-P. Hubaux, ''MobiCrowd: A Collaborative Location-Privacy Preserving Mobile Proxy,'' in *ACM MobiSys*, no. EPFL-POSTER-187771, Jun. 2010. [Online]. Available: https://infoscience.epfl.ch/record/187771

[188] R. Shokri, P. Papadimitratos, G. Theodorakopoulos, and J.-P. Hubaux, ''Collaborative Location Privacy,'' in *IEEE International Conference on Mobile Ad-hoc and Sensor Systems (IEEE MASS)*, Los Alamitos, CA, USA, Oct. 2011, pp. 500--509. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6076648

[189] V. Manolopoulos, P. Papadimitratos, S. Tao, and A. Rusu, ''Securing Smartphone based ITS,'' in *IEEE International Conference on ITS Telecommunications (IEEE ITST)*, St. Petersburg, Russia, Aug. 2011, pp. 201--206. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6060053

[190] V. Manolopoulos, S. Tao, A. Rusu, and P. Papadimitratos, ''HotMobile 2012 Demo: Smartphone-based Traffic Information System for Sustainable

Cities,'' in *ACM International Workshop on Mobile Computing Systems and Applications (ACM HotMobile)*, San Diego, CA, USA, Feb. 2012. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/2436196.2436213

[191] S. Gisdakis, V. Manolopoulos, S. Tao, A. Rusu, and P. Papadimitratos, ''Secure and Privacy-Preserving Smartphone-Based Traffic Information Systems,'' *IEEE Transactions on Intelligent Transportation Systems (IEEE ITS)*, vol. 16, no. 3, pp. 1428--1438, Jun. 2015. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6991589

[192] M. Khodaei and P. Papadimitratos, ''Security & Privacy for Vehicular Communication Systems,'' in *Cybersecurity and Privacy (CySeP) Summer School*, Stockholm, Sweden, Jun. 2018. [Online]. Available: https://people.kth.se/~khodaei/files/posters/cysep18.pdf

[193] ------, ''Security & Privacy for Vehicular Communication Systems: The Key to Intelligent Transportation,'' in *Cybersecurity and Privacy (CySeP) Summer School*, Stockholm, Sweden, Jun. 2017. [Online]. Available: https://people.kth.se/~khodaei/files/posters/cysep17.pdf

[194] H. Zhu, R. Lu, X. Shen, and X. Lin, ''Security in Service-Oriented Vehicular Networks,'' *IEEE Wireless Communications*, vol. 16, no. 4, pp. 16--22, Aug. 2009. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/5281251

[195] A. Goodwin, ''Ford unveils open-source Sync developer platform,'' Oct. 2009. [Online]. Available: https://www.cnet.com/roadshow/news/ford-unveils-open-source-sync-developer-platform/

[196] S. Mollman, ''From cars to TVs, apps are spreading to the real world,'' Oct. 2009. [Online]. Available: http://edition.cnn.com/2009/TECH/10/08/apps.realworld/

[197] D. Cooper, ''Internet X. 509 Public Key Infrastructure Certificate and Certificate Revocation List Profile,'' Tech. Rep., May 2008. [Online]. Available: https://www.hjp.at/doc/rfc/rfc5280.html

[198] J. Sermersheim, ''Lightweight Directory Access Protocol (LDAP): The Protocol,'' Jun. 2006. [Online]. Available: https://www.hjp.at/doc/rfc/rfc4511.html

[199] T. Dierks, ''The Transport Layer Security (TLS) Protocol Version 1.2,'' Aug. 2008. [Online]. Available: https://www.hjp.at/doc/rfc/rfc5246.html

[200] S. Santesson, M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams, ''X. 509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP,'' Tech. Rep., Jun. 2013. [Online]. Available: https://www.hjp.at/doc/rfc/rfc6960.html

[201] M. Abliz and T. Znati, ‘‘A Guided Tour Puzzle for Denial of Service Prevention,’’ in *IEEE Computer Security Applications Conference (ACSAC)*, Honolulu, HI, Dec. 2009, pp. 279--288. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/5380686

[202] S. Uppoor, O. Trullols-Cruces, M. Fiore, and J. M. Barcelo-Ordinas, ‘‘Generation and Analysis of a Large-scale Urban Vehicular Mobility Dataset,’’ *IEEE Transactions on Mobile Computing*, vol. 13, no. 5, pp. 1061--1075, May 2014. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6468040

[203] L. Codeca, R. Frank, and T. Engel, ‘‘Luxembourg Sumo Traffic (LuST) Scenario: 24 Hours of Mobility for Vehicular Networking Research,’’ in *IEEE Vehicular Networking Conference (VNC)*, Kyoto, Japan, Dec. 2015, pp. 1--8. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7385539

[204] ‘‘Horizontal Pod Autoscaler,’’ https://kubernetes.io/docs/tasks/run-application/horizontal-pod-autoscale/, Jan. 2019.

[205] P. T. Eugster, P. A. Felber, R. Guerraoui, and A.-M. Kermarrec, ‘‘The Many Faces of Publish/Subscribe,’’ *ACM computing surveys (CSUR)*, vol. 35, no. 2, pp. 114--131, Jun. 2003. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/857076.857078

[206] Y. Huang and H. Garcia-Molina, ‘‘Publish/Subscribe in a Mobile Environment,’’ *Wireless Networks*, vol. 10, no. 6, pp. 643--652, Nov. 2004. [Online]. Available: https://link.springer.com/article/10.1023/B:WINE.0000044025.64654.65

[207] B. Fan, D. G. Andersen, M. Kaminsky, and M. D. Mitzenmacher, ‘‘Cuckoo Filter: Practically Better Than Bloom,’’ in *ACM CoNEXT*, Sydney, Australia, Dec. 2014, pp. 75--88. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/2674005.2674994

[208] A. R. Beresford and F. Stajano, ‘‘Location Privacy in Pervasive Computing,’’ *IEEE Pervasive computing*, vol. 2, no. 1, pp. 46--55, Jan. 2003. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/1186725

[209] S. Brands and D. Chaum, ‘‘Distance-Bounding Protocols,’’ in *Workshop on the Theory and Application of Cryptographic Techniques*, Berlin, Heidelberg, May 1993, pp. 344--359. [Online]. Available: https://link.springer.com/chapter/10.1007/3-540-48285-7_30

[210] P. Papadimitratos and A. Jovanovic, ‘‘Protection and Fundamental Vulnerability of GNSS,’’ in *IEEE IWSSC*, Toulouse, France, Oct. 2008, pp. 167--171. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/4656777

[211] ''IEEE Standard for Wireless Access in Vehicular Environments (WAVE) –Networking Services,'' *IEEE Vehicular Technology Society*, Jan. 2016. [Online]. Available: https://ieeexplore.ieee.org/document/7458115

[212] M. Khodaei, ''Secure Vehicular Communication Systems: Design and Implementation of a Vehicular PKI (VPKI),'' Master's thesis, Division of Network and Systems Engineering, Royal Institute of Technology (KTH), Stockholm, Sweden, Oct. 2012. [Online]. Available: http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-119820

[213] N. Alexiou, M. Laganà, S. Gisdakis, M. Khodaei, and P. Papadimitratos, ''VeSPA: Vehicular Security and Privacy-preserving Architecture,'' in *Proceedings of the 2nd ACM workshop on Hot topics on wireless network security and privacy (ACM HotWiSec)*, Budapest, Hungary, Apr. 2013. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/2463183.2463189

[214] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, ''Wireless Device Identification with Radiometric Signatures,'' in *Proceedings of the 14th ACM international conference on Mobile computing and networking*, San Francisco, California, USA, Sep. 2008, pp. 116--127. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/1409944.1409959

[215] K. B. Rasmussen and S. Capkun, ''Implications of Radio Fingerprinting on the Security of Sensor Networks,'' in *IEEE International Conference on Security and Privacy in Communications Networks and the Workshops-SecureComm*, Nice, France, Jun. 2007, pp. 331--340. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/4550352

[216] B. Danev, D. Zanetti, and S. Capkun, ''On Physical-Layer Identification of Wireless Devices,'' *ACM Computing Surveys (CSUR)*, vol. 45, no. 1, p. 6, Nov. 2012. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/2379776.2379782

[217] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, ''Fingerprints in the Ether: Using the Physical Layer for Wireless Authentication,'' in *IEEE International Conference on Communications*, Glasgow, UK, Aug. 2007, pp. 4646--4651. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/4289438

[218] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, ''Using the Physical Layer for Wireless Authentication in Time-variant Channels,'' *IEEE Transactions on Wireless Communications*, vol. 7, no. 7, pp. 2571--2579, Jul. 2008. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/4570223

[219] A. Al-Momani, R. W. van der Heijden, F. Kargl, and C. Waldschmidt, ''Exploiting Propagation Effects for Authentication and Misbehavior

Detection in VANETs,'' in *IEEE Vehicular Networking Conference (VNC)*, Columbus, OH, USA, Dec. 2016, pp. 1--4. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7835973

[220] C. Vaas, M. Roeschlin, P. Papadimitratos, and I. Martinovic, ''Poster: Tracking Vehicles Through Encrypted Mix-Zones Using Physical Layer Properties,'' in *IEEE Vehicular Networking Conference (VNC)*, Taipei, Taiwan, Dec. 2018. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8628387

[221] Y. Yao, B. Xiao, G. Wu, X. Liu, Z. Yu, K. Zhang, and X. Zhou, ''Voiceprint: A Novel Sybil Attack Detection Method Based on RSSI for VANETs,'' in *IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, Denver, CO, USA, Jun. 2017, pp. 591--602. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8023157

[222] S. So, J. Petit, and D. Starobinski, ''Physical Layer Plausibility Checks for Misbehavior Detection in V2X Networks,'' in *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, Miami, Florida, USA, May 2019, pp. 84--93. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/3317549.3323406