
KTH Electrical Engineering

# Secure and Privacy Preserving Vehicular Communication Systems: Identity and Credential Management Infrastructure

MOHAMMAD KHODAEI

Licentiate Thesis
Stockholm, Sweden 2016

KTH Royal Institute of Technology
School of Electrical Engineering
SE-100 44 Stockholm
SWEDEN

TRITA-EE 2016:159
ISSN 1653-5146
ISBN 978-91-7729-134-3

Akademisk avhandling som med tillstånd av Kungliga Tekniska högskolan framlägges till offentlig granskning för avläggande av teknologie licentiatesexamen i elektro och systemteknik november 2016 i Q2, Kungliga Tekniska högskolan, Osquldas Väg 10, Stockholm.



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 the 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. 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 openness of the wireless communication, an observer can eavesdrop the vehicular communication to infer users' sensitive information, thus profiling 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 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.

# 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 collaborators: my especial regards go to my friend, *Hongyu Jin*, for all of his time, efforts and fruitful discussions we had. I would also like to thank the rest of the group members of NSS for all the pleasant times and interesting discussions, specially *Kewei Zhang*, *Syed Muhammad Zubair*, and *Moritz Wiese*. I would like also to thank *Marcello Laganà* for his help during my early days at NSS.

I would like to thank all of my colleagues, administrators and faculty at Laboratory of Communication Networks (LCN) for all the useful interactions, help, and friendly environment. I feel happy to be a member of such an academic environment.

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, August 2016

# Contents

# 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, 4]. These set the ground for the emergence of innovative applications to improve road safety, transportation efficiency, and driving experience.

In Vehicular Communication (VC) systems, vehicles are to be provided with special-purpose sensors and equipments to monitor their operation and surrounding. Fig. 1.1 illustrates a smart vehicle, 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). They broadcast their movement behaviors to nearby vehicles, e.g., beaconing their position as well as lane changing and emergency braking notifications, or communicate with the back-end infrastructure. Vehicles periodically disseminate messages about their actions and whereabouts containing location, velocity, and acceleration. As a result, neighboring vehicles will be informed about possible unexpected incidents or objects beyond their sight. 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] and Vehicular Social Networks (VSNs) [11] 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)*.

Fig. 1.2 illustrates a vehicular communication network: vehicles can directly

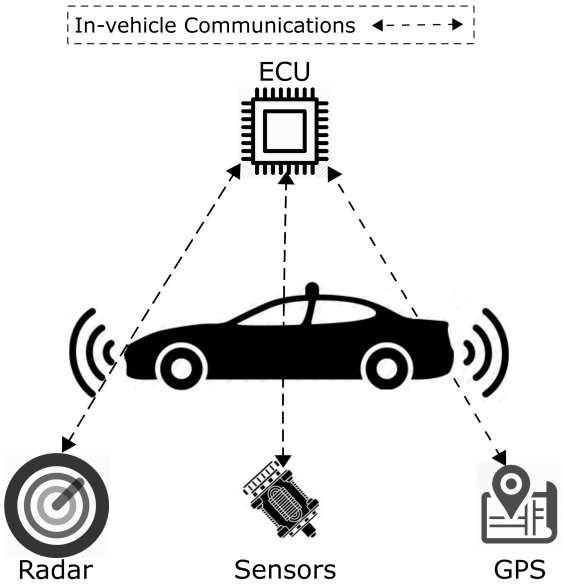


Figure 1.1: A Smart Vehicle Equipped with ECU, Sensors, Radar, and GPS

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) [12] frequently [5]; these messages disseminate valuable information on potentially dangerous vehicle movement, environmental hazards, or even assist regulating traffic [9, 13]. More precisely, CAMs provide road safety by means of periodic beaconing of vehicle trajectory information to neighboring vehicles. Such beaconing messages entail 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 [12]. DENMs can be triggered in environmental hazard events, e.g., *''precipitation''*, *''road adhesion''*, *''visibility''*, and *''wind''* [12], or in traffic events [14], e.g., *''road-work warning''*, *''traffic condition warning''*, and *''stationary vehicle''* [12].

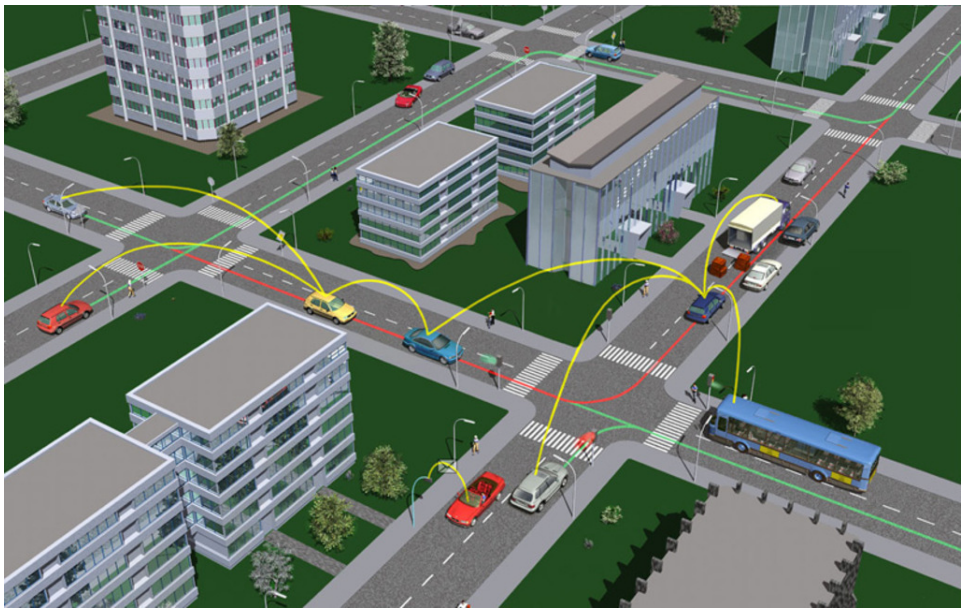

Figure 1.2: A Vehicular Communication Network [Source: C2C-CC [15]]

## 1.2 Challenges and Problem Statement

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 identify users and track vehicles, thus harming user privacy: by cross-referencing the time, location, and other external information, e.g., local hospital admissions and driving patterns [16, 17, 18], it would be feasible to track and identify a vehicle. The experience from mobile applications and LBSs [19, 20, 21] hints that this is a realistic threat to user privacy, aggravated, of course, by the recent stream of disclosures on mass surveillance [22, 23]. 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 [24]. The importance of secure communication in the VC systems is due to the physical damages and injuries to the human safety: a fatal crash could threaten human safety [25] as vehicles could be compromised or their sensors become faulty. Anonymity may be abused by ‘‘malicious’’ (compromised or malfunctioning) vehicles to corrupt system operations to 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 [24]; 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.*

Last but not least, in the light of the VC large-scale environment, the efficiency, scalability and robustness of any scheme that we design are paramount. We need to extensively evaluate its viability in terms of performance and cost for a large-scale deployment as VC becomes ubiquitous. We further need to enable interoperability of vehicles from different Original Equipment Manufacturers (OEMs) while facilitating their operation in a multi-domain VC system.

**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.

## 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 (whose text partially relies on [26]). We then describe the security and privacy requirements and the adversaries in Chapter 3 (whose text relies on [26]). In Chapter 4, we present our contributions (whose text relies on [26]), 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 a compendium including four published papers and one in submission in chronological order, all involving the author of this thesis.

# 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) [27, 28, 29]) and harmonization efforts (C2C-CC [15, 30]) have reached a consensus towards deploying a Vehicular Public-Key Infrastructure (VPKI) in order to protect V2V and/or V2I (V2X) communication with the help of public key cryptography. These efforts unfolded in parallel by academic works that developed the same concepts, e.g., [14, 31, 32]. A set of Certification Authorities (CAs), constituting the VPKI, provide credentials to registered (thus legitimate) vehicles. Each legitimate vehicle is equipped with a Long Term Certificate (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 [14, 33] as well as in subsequent projects, e.g., Crash Avoidance Metrics Partnership Vehicle Safety Consortium (CAMP VSC3) [34, 35] and Preparing Secure Vehicle-to-X Communication Systems (PRESERVE) [36, 37].

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 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

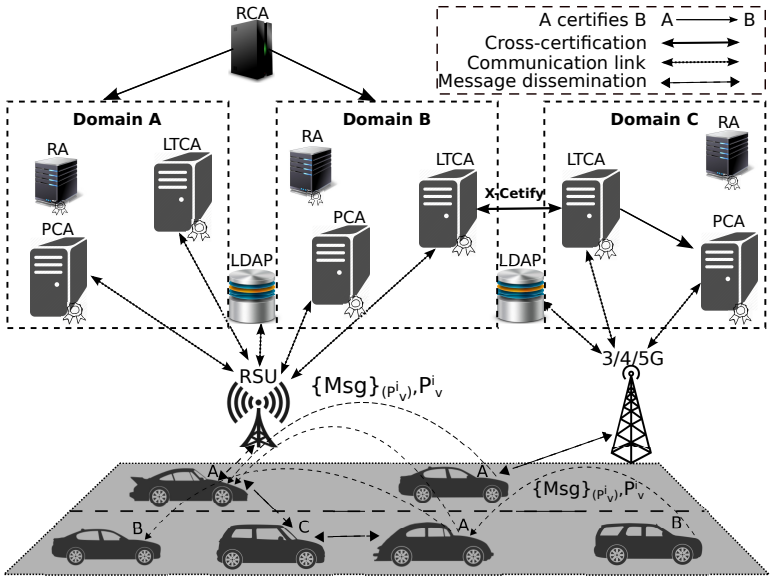


Figure 2.1: VPKI Overview

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 [24, 38]. 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 [39].

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 [15, 30]), e.g., PRESERVE [37, 40], 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 [41]: 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 [42, 43, 44, 45, 46] 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 [42]. For example, the signing delay with Group Signatures with Verifier Local Revocation (GS-VLR) [47] (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) [42]. [48] 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.

[42, 43, 44] 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 [42]). 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. However, this trades off linkability: one could trivially link messages if signed under the same pseudonym.

Sybil-based [49] 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 [30, 34, 40, 41, 50]. 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 [30, 34, 40, 50] or the security infrastructure does not prevent a vehicle from obtaining simultaneously valid pseudonyms via multiple pseudonym requests [41]. 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 [51]. [42, 48] prevent Sybil-based misbehavior by leveraging ''periodic n-show credentials'' [52], 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 [17]. There are different strategies for pseudonyms transition, i.e., changing the currently used (or expired) pseudonym to a new one. Some proposals [53, 54] 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, [55] suggests that each vehicle should be silent, i.e., not beaconing, for a *quiet-time* interval, or if the speed is below a threshold [56]. However, vehicle transceivers cannot be simply switched off [57] as they could cause fatal accidents, thus seriously jeopardizing human safety. [58, 59] 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 [41, 48]. 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.

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 Certificate Revocation Lists (CRLs) among the registered nodes, to ensure the efficiency, reliability and robustness of the VC system. [60, 61, 62, 63] propose centralized detection and dissemination of CRLs, leveraging on fixed infrastructure or car-to-car epidemic; on the contrary, [51, 64] 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 [65]. 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 [65]. A fully distributed lightweight framework for discovery and verification of neighbor positions is proposed [66]: 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 [67]. 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 [67]. Further discussion on such attacks is beyond the reference 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, [68] 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 is orthogonal to our investigation and further discussion is beyond the extent 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 [39] to achieve better return on investment. By leveraging the concepts of *''Car as a Platform'' (CaaP)* and *''Mobility as a Service'' (MaaS)*, 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) [69, 70, 71, 10]) to VSN [11] (e.g., photo, video and audio sharing), content distribution [72] (e.g., video streaming, downloading maps and multimedia files), and *''Vehicular-Application Store''* [73, 74] (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

# Requirements and Adversaries for Identity and Credential Management

The security and privacy requirements for the V2X communications have been extensively specified in the literature, e.g., as early as [24]; 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 Security and Privacy Requirements

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

- *R1. 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. We further need to ensure the communication integrity, i.e., exchanged messages should be 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.

- *R2. Authorization and access control:* Only legitimate, i.e., registered, and authenticated vehicles should be able to be serviced by the VPKI, notably obtain pseudonyms. Moreover, vehicles should interact with the VPKI entities according to the system protocols and policies, and domain regulations.

- *R3. 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.

- *R4. 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.

- *R5. Thwarting Sybil-based attacks:* At no point in time should any vehicle be able to obtain multiple simultaneously valid pseudonyms.

- *R6. 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 Denial of Service (DDoS) attacks.

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

## 3.2 Adversaries

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 can degrade the operations of the system by mounting a clogging Denial of Service (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. In this work, 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.

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

# Chapter 4

# Identity and Credential Management Infrastructure

## 4.1 System Model and Assumptions

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 [75]) 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* [38] is govern 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 Hardware Security Module (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 [61] in the context of VC systems.

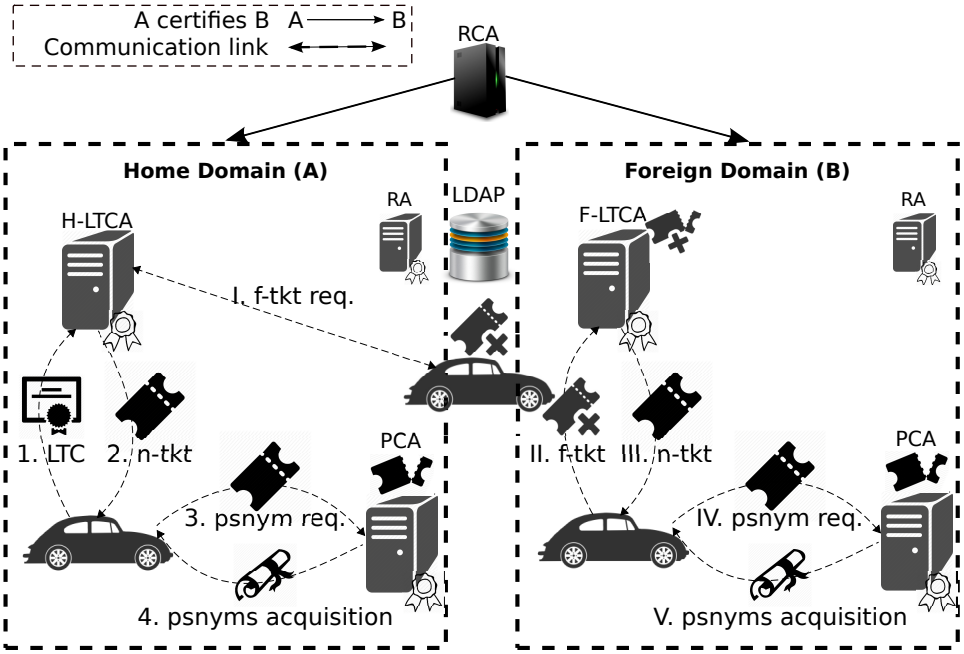


Figure 4.1: Pseudonym Acquisition Overview in the Home and Foreign Domains

## 4.2 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) [76] 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 [77]. 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 mutually authenticated Transport Layer Security (TLS) [78] 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 hidden from the H-LTCA; the ticket is anonymized and it does not reveal its owner's identity (Protocol 1

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 |
| $n\text{-}tkt$, $(n\text{-}tkt)_{LTCA}$ | native ticket |
| $f\text{-}tkt$, $(n\text{-}tkt)_{LTCA}$ | 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 |
| $\zeta, \chi, \xi$ | temporary variables |

in Sec. 4.3). 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. 4.3).

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 [75] and perform Online Certificate Status Protocol (OCSP) [79] operations, authenticated with a current valid pseudonym. The notation used in the protocols is given in Table 4.1.

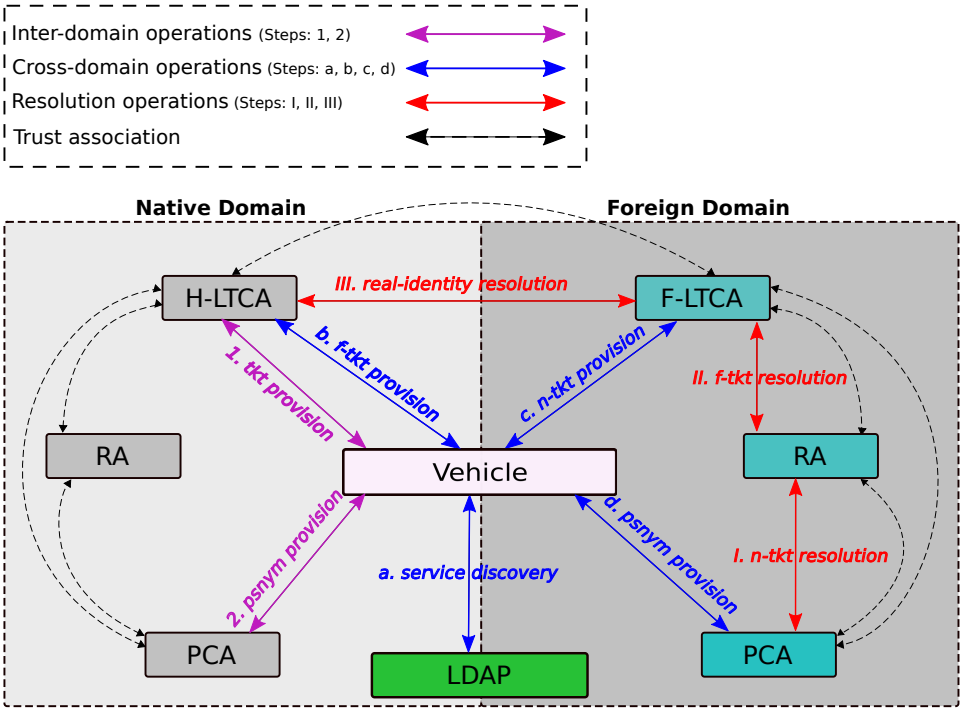


Figure 4.2: VPKI Security Protocols Overview: Pseudonym Provision and Resolution

## 4.3 VPKI Services and Security Protocols

An overview of the security protocols to obtain pseudonyms in a native and a foreign domain, and the operations to resolve (and possibly revoke) a pseudonym are illustrated in Fig. 4.2. 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 [26].

**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: $H(LTC_v||t_s||t_e||Rnd_{IK_{n\text{-}tkt}})$ (steps 4.5); this prevents the H-LTCA from mapping

**Protocol 1** Ticket Provisioning from the H-LTCA

$$V : \zeta \leftarrow (Id_{req}, H(Id_{PCA} \| Rnd_{n\text{-}tkt}), t_s, t_e) \quad (4.1)$$

$$V : (\zeta)_{\sigma_v} \leftarrow Sign(Lk_v, \zeta) \quad (4.2)$$

$$V \rightarrow H\text{-}LTCA : ((\zeta)_{\sigma_v}, LTC_v, N, t_{now}) \quad (4.3)$$

$$H\text{-}LTCA : \text{Verify}(LTC_v, (\zeta)_{\sigma_v}) \quad (4.4)$$

$$H\text{-}LTCA : IK_{n\text{-}tkt} \leftarrow H(LTC_v || t_s || t_e || Rnd_{IK_{n\text{-}tkt}}) \quad (4.5)$$

$$H\text{-}LTCA : \chi \leftarrow (SN, H(Id_{PCA} \| Rnd_{n\text{-}tkt}), IK_{n\text{-}tkt}, Rnd_{IK_{n\text{-}tkt}}, t_s, t_e, Exp_{n\text{-}tkt}) \quad (4.6)$$

$$H\text{-}LTCA : (n\text{-}tkt)_{\sigma_{h\text{-}ltca}} \leftarrow Sign(Lk_{ltca}, \chi) \quad (4.7)$$

$$V \leftarrow H\text{-}LTCA : (Id_{res}, (n\text{-}tkt)_{\sigma_{h\text{-}ltca}}, N{+}1, t_{now}) \quad (4.8)$$

$$V : \text{Verify}(LTC_{h\text{-}ltca}, (n\text{-}tkt)_{\sigma_{h\text{-}ltca}}) \quad (4.9)$$

$$V : H(LTC_v || t_s || t_e || Rnd_{IK_{n\text{-}tkt}}) \stackrel{?}{=} IK_{n\text{-}tkt} \quad (4.10)$$

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). 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).

## 4.4 Security and Privacy Analysis

We analyze the achieved security and privacy of our VPKI with respect to the requirements presented in Chapter 3. All the communication runs over secure channels, i.e., TLS with uni- or bidirectional authentication, thus we achieve *authentication, communication integrity* and *confidentiality* (R1). 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 (R2). Given the ticket acquisition request is signed with the private key corresponding to the vehicle's LTC and pseudonym acquisition entails a valid ticket,

**Protocol 2** Pseudonym Provisioning from the PCA

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

$$V \rightarrow PCA : (\zeta) \quad (4.2)$$

$$PCA : ReceiveReq(\zeta) \quad (4.3)$$

$$PCA : \text{Verify}(LTC_{ltca}, (n\text{-}tkt)_{\sigma_{ltca}}) \quad (4.4)$$

$$PCA : H(Id_{this\text{-}PCA} \| Rnd_{n\text{-}tkt}) \stackrel{?}{=} H(Id_{PCA} \| Rnd_{n\text{-}tkt}) \quad (4.5)$$

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

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

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

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

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

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

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

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

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

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

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

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

the system provides *non-repudiation and accountability* (R3). 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 (R3).

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 [77] 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 (R4). This is further discussed in [26, 77]. Moreover, the separation of duties between the LTCA and the PCA provides *conditional anonymity*, but revoked under special circumstances, e.g., misbehavior (R3).

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

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 |

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 (R5). We achieve availability in the face of a crash failure by mandating load-balancers and server redundancy [80]; in case of a DDoS attack, we use a puzzle technique [81] as a mitigation approach (R6), further discussed in [26]. For a detailed discussion on the security and privacy analysis, we refer readers to our publications [26, 80].

## 4.5 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 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 [36] as we run 400 threads on each VM.

Fig. 4.3 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. 4.3 shows, the end-to-end latency to obtain 100 pseudonyms is around 500 ms.

Fig. 4.4 shows the average response time for the LTCA to issue a ticket, approximately 5 ms, including request decapsulation, LTC verification, and response

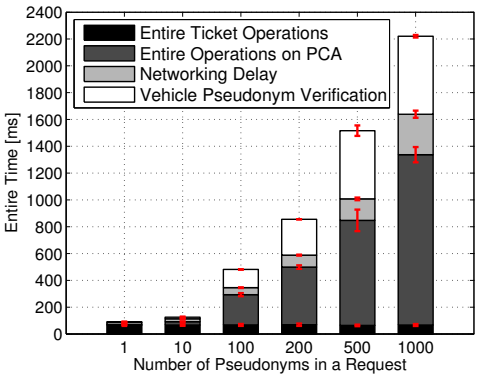


Figure 4.3: Client processing time [taken from [80]]

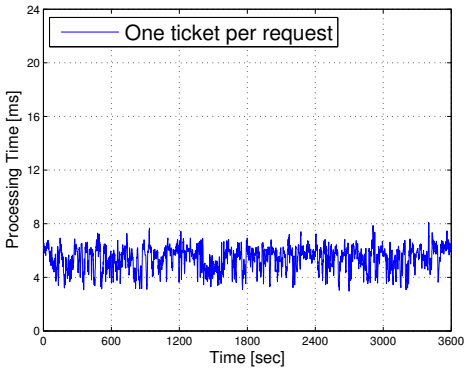


Figure 4.4: LTCA performance [taken from [80]]

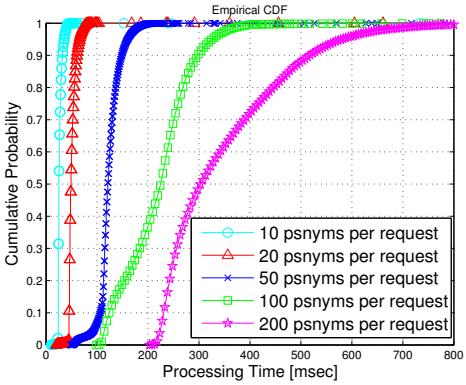


Figure 4.5: PCA performance [taken from [80]]

encapsulation. Fig. 4.5 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 [15, 30]. It is 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 [82, 83], and an evaluation of the resiliency of our scheme to DDoS attacks. Additional results are provided in [26, 77].

# 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.

**Paper A: VeSPA: Vehicular Security and Privacy-preserving Architecture**
*Nikolaos Alexiou, Marcello Laganà, Stylianos Gisdakis, Mohammad Khodaei, Panos Papadimitratos*
*In ACM HotWiSec, Budapest, Hungary, April 2013*

**Abstract:** Vehicular Communication (VC) 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 [84] of the author of this licentiate thesis. This work reflects his work as a research engineer within the Networked Systems Security (NSS) group. He has significantly contributed to the design and carried out the implementation and the performance analysis of the system.

**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*

**Abstract:** 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 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.

**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*

**Abstract:** 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 idea of this article was the result of fruitful discussions with the second author. The paper was written by both authors.

**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*

**Abstract:** 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.

**Paper E: SECMACE: Scalable and Robust Identity and Credential Management Infrastructure in Vehicular Communication Systems**
*Mohammad Khodaei, Hongyu Jin, and Panos Papadimitratos*
*Submitted to: IEEE Transaction on Intelligent Transportation Systems*

**Abstract** 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 is mainly based on prior works [77, 85, 80] consolidating the design, implementation, and evaluation of the work with the help of other authors. The author of this thesis contributed to all these aspects and the article was written by all authors.

### Publications not included in this thesis

#### Book Chapter

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

#### Posters & Demos

- 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 Next Steps

## 6.1 Summary of Contributions

This thesis critically surveys the state-of-the-art for identity and credential management in the VC systems. It addresses several technical challenges with no conclusive answers or even contradicting views within standardization bodies and harmonization efforts. The precise understanding of the VPKI, a central building block of secure and privacy-preserving VC systems, is still lacking. In the context of this thesis, we contribute to the closing of this gap. We focus on security, privacy, and efficiency of an identity and credential management infrastructure for the VC systems. We propose a VPKI that facilitates multi-domain operations in the VC systems and enhances user privacy in the presence of honest-but-curious VPKI entities. We develop a standard-compliant full-fledged, refined, cross-platform VPKI and we extensively evaluate our implementation to illuminate its efficiency, scalability and reliability.

## 6.2 Ongoing and Future Research

There is still a plethora of research challenges for identity and credential management in the VC systems. In what follows, we address our future research direction.

**VPKI enhancements:** In VC systems, having a reliable network connectivity and coverage is highly desirable; so far, we have not dwelt on the problem of a reliable Vehicle-VPKI connectivity for obtaining pseudonyms. This problem, as the optimal placement of RSUs and their configuration (their transmission power level, antenna type, etc.) to have a reliable network coverage, has been orthogonal to our investigations. But, in order to have a realistic view of the exact end-to-end latency to obtain pseudonyms, we need to consider the actual networking latency, e.g., through RSUs or alternatively over cellular networks. Towards that, we will model networking latency in simulation by considering the road topology, traffic density, and surrounding environment.

Pseudonymous authentication was elaborated by several projects [14, 33, 86] and proposals [26, 41, 48, 77, 80, 85] for secure and privacy-preserving VC systems (but also in other domains, e.g., LBS [10]): mobile nodes, e.g., vehicles and smart-phones, query the CA servers to obtain pseudonyms, using which they could disseminate information about their surroundings in a secure and privacy-preserving manner. Foregoing schemes propose to issue pseudonyms with non-overlapping lifetimes (validity intervals) to thwart Sybil attack. By eavesdropping the traffic in an area, an attacker could link pseudonymously authenticated messages through cross-referencing the user location and the timing information of the credentials, i.e., pseudonym lifetime and issuance time. More precisely, without examining the content of the message, an adversary could link the pseudonyms, thus pseudonymously authenticated messages, by inspecting successive pseudonym lifetimes. This could result in reconstructing users whereabouts, thus harming their privacy. Of course, this highly depends on the anonymity set, i.e., the active participants in the system, the strategy to issue pseudonyms (overlapping vs. non-overlapping validity intervals), and pseudonym changing strategies, i.e., when to switch to another pseudonym. Further investigation to evaluate the level of unlinkability achieved under various circumstances is indeed required.

In order to ensure the correctness of the employed security and privacy protocols, we plan to rigorously analyze the achieved security and privacy properties. Towards that, we intend to employ an automated protocol verifier, e.g., ProVerif [87], to model and formally assess our security and privacy protocols and evaluate the achieved user privacy (secrecy, strong secrecy and unlinkability) in the presence of honest-but-curious VPKI entities.

**Efficient distribution of revocation information:** Standardization bodies and harmonization efforts have consensus on utilizing public key cryptography to secure the VC communications and a number of projects developed security and privacy-preserving architectures for the VC systems. Despite their advanced status on many aspects, there is no consensus on the need and the method for revocation of short-lived certificates, i.e. pseudonyms. It is generally accepted that compromised, faulty, or illegitimate nodes should be evicted from the VC system. But the main challenge is: *how to disseminate pseudonyms validity information without interfering vehicles operations.* In other words, *is it viable to timely disseminate pseudonyms revocation information among all registered entities with limited bandwidth capacity, intermittent connectivity and rapidly changing of network topology?* Of course there is a trade off between vulnerability and cost [38]: more frequent vehicle interaction with the VPKI narrows down the vulnerability window, but it incurs extra overhead to the VPKI under some circumstances, e.g., during harsh traffic conditions. This needs to be explored further to identify a practical and feasible mechanism to efficiently disseminate the pseudonyms revocation information among all registered entities.

**A Secure and Privacy-preserving Architecture for Platooning:** Autonomous vehicles are the upcoming evolution in ITSs and they will improve transportation safety, efficiency, and driving assistance. Such automated vehicles

are provided with special-purpose sensors, e.g., camera and Light Detection And Ranging (LIDAR), to detect objects and recognize traffic signs. A use case scenario for such autonomous automated vehicles is a platoon of vehicles, i.e., the ability of vehicles to efficiently, effectively and in a secure, privacy-preserving and ad hoc manner, craft a group of vehicles. In such a highly dynamic network of vehicles, a new vehicle could join the platoon or those in the platoon could leave it. There are many challenges from an identity and credential management perspective: *how to establish a secure and privacy-preserving platoon?* And, *how to detect a malicious (compromised or faulty) vehicle and possibly evict it from the platoon?*

# Bibliography


[1] ‘‘Car to car communications a step closer,’’ Dec. 2012. [Online]. Available: http://www.itsinternational.com/categories/location-based-systems/features/car-to-car-communications-a-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: http://www.nhtsa.gov/About+NHTSA/Press+Releases/2014/USDOT+to+Move+Forward+with+Vehicle-to-Vehicle+Communication+Technology+for+Light+Vehicles

[3] M. Strohm, ‘‘6 firms that are testing driverless cars.’’ [Online]. Available: http://www.bankrate.com/finance/auto/companies-testing-driverless-cars-1.aspx

[4] ‘‘Google Self-Driving Car Project.’’ [Online]. Available: https://www.google.com/selfdrivingcar/

[5] European Telecommunications Standards Institute, ‘‘Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions,’’ ETSI Tech. TR-102-638, June 2009.

[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.

[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.

[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,’’ March 2011.

[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.

[10] H. Jin and P. Papadimitratos, ‘‘Resilient Collaborative Privacy for Location-Based Services,’’ in *Secure IT Systems*. Stockholm, Sweden: Springer International Publishing, pp. 47–63, Sep. 2015.

[11] H. Jin, M. Khodaei, and P. Papadimitratos, ‘‘Security and Privacy in Vehicular Social Networks,’’ in *Vehicular Social Networks*. Taylor & Francis Group, 2016.

[12] ‘‘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.

[13] 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*, vol. 16, no. 3, pp. 1428–1438, June 2015.

[14] 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.

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

[16] E. Sampson, ‘‘The future looks bright for ITS,’’ June 2015. [Online]. Available: http://www.itsinternational.com/sections/comment-interview/interviews/the-future-looks-bright-for-its/

[17] 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.

[18] J. Krumm, ‘‘Inference Attacks on Location Tracks,’’ in *International Conference on Pervasive Computing*, Toronto, Canada, pp. 127–143, May 2007.

[19] 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

[20] 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

[21] 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.

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

[23] S. Era and B. Preneel, ''Cryptography and Information Security in the Post-Snowden era,'' May 2015.

[24] P. Papadimitratos, V. Gligor, and J.-P. Hubaux, ''Securing Vehicular Communications-Assumptions, Requirements, and Principles,'' in *ESCAR*, Berlin, Germany, pp. 5–14, Nov. 2006.

[25] 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

[26] M. Khodaei, H. Jin, and P. Papadimitratos, ''SECMACE: Scalable and Robust Identity and Credential Management Infrastructure in Vehicular Communication Systems,'' *Submitted to the IEEE Transactions on Intelligent Transportation Systems*.

[27] T. ETSI, ''ETSI TS 103 097 v1. 1.1-Intelligent Transport Systems (ITS); Security; Security Header and Certificate Formats, Standard, TC ITS,'' Apr. 2013.

[28] ETSI TR 102 731, ''Intelligent Transport Systems (ITS); Security; Security Services and Architecture,'' Sep. 2009.

[29] ETSI TR 102 941, ''Intelligent Transport Systems (ITS); Security; Trust and Privacy Management,'' June 2012.

[30] 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, pp. 12, Oct. 2011.

[31] P. Papadimitratos, L. Buttyan, J.-P. Hubaux, F. Kargl, A. Kung, and M. Raya, ''Architecture for Secure and Private Vehicular Communications,'' in *IEEE ITST*, Sophia Antipolis, pp. 1–6, June 2007.

[32] 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.

[33] A. Kung, ''Security Architecture and Mechanisms for V2V/V2I, SeVeCom - Deliverable 2.1,'' Feb. 2008.

[34] W. Whyte, A. Weimerskirch, V. Kumar, and T. Hehn, ''A Security Credential Management System for V2V Communications,'' in *IEEE VNC*, Boston, MA, pp. 1–8, Dec. 2013.

[35] ‘‘Vehicle Safety Communications Security Studies: Technical Design of the Security Credential Management System,’’ July 2016. [Online]. Available: https://www.regulations.gov/document?D=NHTSA-2015-0060-0004

[36] ‘‘Preparing Secure Vehicle-to-X Communication Systems - PRESERVE.’’ [Online]. Available: http://www.preserve-project.eu/

[37] J. P. Stotz, N. Bißmeyer, F. Kargl, S. Dietzel, P. Papadimitratos, and C. Schleiffer, ‘‘Security Requirements of Vehicle Security Architecture, PRESERVE - Deliverable 1.1,’’ June 2011. [Online]. Available: http://www.preserve-project.eu/

[38] M. Khodaei and P. Papadimitratos, ‘‘The Key to Intelligent Transportation: Identity and Credential Management in Vehicular Communication Systems,’’ *IEEE VT Magazine*, vol. 10, no. 4, pp. 63–69, Dec. 2015.

[39] P. Papadimitratos, ‘‘"On the road" - Reflections on the Security of Vehicular Communication Systems,’’ in *IEEE ICVES*, Columbus, OH, USA, pp. 359–363, Sep. 2008.

[40] N. Bißmeyer, J. Petit, and K. M. Bayarou, ‘‘CoPRA: Conditional Pseudonym Resolution Algorithm in VANETs,’’ in *IEEE WONS*, Banff, Canada, pp. 9–16, Mar. 2013.

[41] S. Gisdakis, M. Laganà, T. Giannetsos, and P. Papadimitratos, ‘‘SEROSA: SERvice Oriented Security Architecture for Vehicular Communications,’’ in *IEEE VNC*, Boston, MA, USA, Dec. 2013.

[42] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, ‘‘On the Performance of Secure Vehicular Communication Systems,’’ *IEEE TDSC*, vol. 8, no. 6, pp. 898–912, Nov. 2011.

[43] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, ‘‘Efficient and Robust Pseudonymous Authentication in VANET,’’ in *ACM VANET*, NY, USA, pp. 19–28, Sep. 2007.

[44] P. Papadimitratos, G. Calandriello, J.-P. Hubaux, and A. Lioy, ‘‘Impact of Vehicular Communications Security on Transportation Safety,’’ in *IEEE INFOCOM Workshops*, Phoenix, AZ, pp. 1–6, Apr. 2008.

[45] 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.

[46] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, ‘‘ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications,’’ in *IEEE INFOCOM*, Phoenix, AZ, USA, April 2008.

[47] 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.

[48] D. Förster, H. Löhr, and F. Kargl, ''PUCA: A Pseudonym Scheme with User-Controlled Anonymity for Vehicular Ad-Hoc Networks (VANET),'' in *IEEE VNC*, Paderborn, Germany, Dec. 2014.

[49] J. R. Douceur, ''The Sybil Attack,'' in *ACM Peer-to-peer Systems*, London, UK, Mar. 2002.

[50] F. Schaub, F. Kargl, Z. Ma, and M. Weber, ''V-tokens for Conditional Pseudonymity in VANETs,'' in *IEEE WCNC*, NJ, USA, Apr. 2010.

[51] 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*, pp. 1557–1568, Oct. 2007.

[52] J. Camenisch, S. Hohenberger, M. Kohlweiss, A. Lysyanskaya, and M. Meyerovich, ''How to Win the Clonewars: Efficient Periodic n-Times Anonymous Authentication,'' in *ACM CCS*, NY, USA, pp. 201–210, Oct. 2006.

[53] 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.

[54] R. Lu, X. Li, T. H. Luan, X. Liang, and X. Shen, ''Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in VANETs,'' *IEEE Transactions on Vehicular Technology*, vol. 61, no. 1, pp. 86–96, July 2011.

[55] S. Eichler, ''Strategies for Pseudonym Changes in Vehicular Ad Hoc Networks Depending on Node Mobility,'' in *IEEE Intelligent Vehicles Symposium*, Istanbul, Turkey, pp. 541–546, June 2007.

[56] 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, pp. 1–8, Oct. 2009.

[57] 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, July 2006.

[58] M. Gerlach, ''Assessing and Improving Privacy in VANETs,'' in *ESCAR, Embedded Security in Cars*, Berlin, Germany, Nov. 2006.

[59] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki, ''CARAVAN: Providing Location Privacy for VANET,'' in *ESCAR, Embedded Security in Cars*, Cologne, Germany, Nov. 2005.

[60] 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.

[61] P. Papadimitratos, G. Mezzour, and J.-P. Hubaux, ''Certificate Revocation List Distribution in Vehicular Communication Systems,'' in *ACM VANET*, San Francisco, CA, pp. 86–87, Sep. 2008.

[62] 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.

[63] 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.

[64] T. Moore, M. Raya, J. Clulow, P. Papadimitratos, R. Anderson, and J.-P. Hubaux, ''Fast Exclusion of Errant Devices from Vehicular Networks,'' in *IEEE SECON*, San Francisco, CA, pp. 135–143, June 2008.

[65] 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.

[66] 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.

[67] 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, June 2010.

[68] M. Raya, P. Papadimitratos, V. D. Gligor, and J.-P. Hubaux, ''On Data-Centric Trust Establishment in Ephemeral Ad Hoc Networks,'' in *IEEE INFOCOM*, Phoenix, AZ, Apr. 2008.

[69] R. Shokri, P. Papadimitratos, and J.-P. Hubaux, ''MobiCrowd: A Collaborative Location-Privacy Preserving Mobile Proxy,'' in *ACM MobiSys*, no. EPFL-POSTER-187771, June 2010.

[70] 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, pp. 500–509, Oct. 2011.

[71] 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.

[72] 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.

[73] 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/

[74] 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/

[75] D. Cooper, ''Internet X. 509 Public Key Infrastructure Certificate and Certificate Revocation List Profile,'' May 2008.

[76] J. Sermersheim, ''Lightweight Directory Access Protocol (LDAP): The Protocol,'' June 2006.

[77] 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*, Paderborn, Germany, pp. 7–12, July 2016.

[78] T. Dierks, ''The transport layer security (tls) protocol version 1.2,'' Aug. 2008.

[79] 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., June 2013.

[80] 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, pp. 33–40, Dec. 2014.

[81] M. Abliz and T. Znati, ''A Guided Tour Puzzle for Denial of Service Prevention,'' in *IEEE Computer Security Applications Conference, ACSAC'09.*, Honolulu, HI, pp. 279–288, Dec. 2009.

[82] 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.

[83] L. Codeca, R. Frank, and T. Engel, ''Luxembourg Sumo Traffic (LuST) Scenario: 24 Hours of Mobility for Vehicular Networking Research,'' in *IEEE VNC*, Kyoto, Japan, pp. 1–8, Dec. 2015.

[84] M. Khodaei, ''Secure Vehicular Communication Systems: Design and Implementation of a Vehicular PKI (VPKI),'' Master's thesis, Lab of Communication Networks (LCN), KTH University, Oct. 2012.

[85] 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*, Budapest, Hungary, pp. 19–24, Apr. 2013.

[86] ''U.S. Department of Transportation (DoT). Safety Pilot Model Deployment.'' [Online]. Available: http://safetypilot.umtri.umich.edu/

[87] B. Blanchet, ''Automatic Proof of Strong Secrecy for Security Protocols,'' in *IEEE Symposium on Security and Privacy*, California, USA, May 2004.