Security and Privacy in Vehicular Social Networks

Hongyu Jin, Mohammad Khodaei and Panos Papadimitratos
Networked Systems Security Group, KTH Royal Institute of Technology, Sweden
{*hongyuj, khodaei, papadim*}@kth.se
www.ee.kth.se/nss

I. Introduction

During the past decade, the trend is to enable vehicle communication, by equipping them with On-Board Units (OBUs). Vehicular Communication (VC) systems facilitate Intelligent Transport Systems (ITSs), enabling various applications on top of Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication. Vehicles can also access various Service Providers (SPs) through Base Stations (BSs), Access Points (APs) and Road-Side Units (RSUs). Basically, original VC applications aim at providing awareness to avoid vehicle collisions and helping drivers choose better routes based on traffic density [44]. This is achieved by vehicles' active periodical beaconing of the current status and sensed context information (e.g., obstacles or accidents). These transmissions leverage OBUs pre-installed in the vehicles and do not assume any relationships with neighbors before the transmissions and receptions.

At the same time, interconnected vehicles facilitate message exchange beyond transportation safety and efficiency. This enables socializing with the drivers and passengers of nearby vehicles. Unlike Online Social Networks (OSNs) and most Mobile Social Networks (MSNs), the users/devices (nodes) in Vehicular Social Networks (VSNs) mostly interact when they are within communication range (i.e., physically close to each other, as determined by their trips). Due to the mobility of vehicles, they have ephemeral encounters and interactions. However, vehicle interactions could exploit such characteristics and even promote content dissemination in VSNs thanks to broad network of vehicle contacts during the trips. Moreover, vehicle connectivity to the Internet (leveraging BSs or APs) can enable interactions among VSNs, OSNs and MSNs.

Traditional social networks leverage long-term user identities (i.e., an identity is created based on, e.g., an e-mail address or a username, and cannot be changed during its lifespan), and all user activities are carried out under these identities. The users also interact based on established relationships (e.g., within friends or group members), which are linked to their identities. However, these identities do not necessarily indicate the true identities of the users (i.e., user profiles can be faked); thus, no strong authentication is required: the users are not kept accountable for their actions. On the contrary, in VC systems, there is consensus in academia and industry that vehicles do not expose long-term identities due to privacy concerns, rather, short-term and unlinkable identities should be used to preserve user privacy. While privacy is important in VC systems, strong identification of drivers and vehicles is needed considering the high stakes in traffic systems (notably, driver and passenger safety): the messages in VC systems need to be properly protected by proving that the messages are originated from legitimate users in the system, in order to guarantee the secure and privacy preserving operations in the system. Both of the requirements can be achieved leveraging pseudonymous authentication [45], [35], [10], [30], [44], [26], [33]. In fact, security and privacy in VC systems have been extensively studied and significant effort has already been made towards the deployment of secure VC systems, which are the basis for secure ITSs.

VSNs consider the VC network as the underlying networking facility, along with its location and context-specific services and features. While we embrace emerging VSN applications, it is important that VC system security and privacy are not compromised by the VSN functionality. VSNs could and in fact should build upon the security infrastructures designed and deployed for VC systems and seek to address VSN-specific requirements based on extensions or tailoring of those security infrastructures. Moreover, security solutions proposed for the relevant areas (e.g., Location-based Service (LBS) and participatory sensing) could evolve and be integrated into VSNs. This could largely promote the popularity and deployment of VSNs rather than building the whole infrastructure from scratch; this is what we advocate in this chapter. We outline the VSN architecture and content dissemination in different architectures. We continue with the investigation of security and privacy requirements in the VC landscape. This is important so that VSN can be deployed, possibly promising the adoption of VC technology itself, while ensuring the strong security and privacy protection for the overall system. Moreover, we survey the existing security and privacy solutions for emerging applications (which are potential applications for VSNs) and show that they could be integrated to the VSNs eliminating the need to introduce redundant components to the system. We close this chapter with a discussion of open challenges for the security and privacy, and a brief conclusion.

II. Vehicular Social Networks

OSNs with rich features have been integrated into people's daily lives. They have satisfied users' demand on socializing with friends or making new friends among people with common interests. Nowadays, OSNs are easily accessible from mobile devices (e.g., smartphones) and many of them exploit user mobility, thus, they are location-aware. Users can look for nearby users or tag posts with their current locations; this way they can be discovered by other users with location-based searching.

OSNs maintain steady user relationships: users with common interests have direct or indirect relationships. Leveraging the Internet, user interactions are not time-/space-restricted. Although there exist decentralized social networks (e.g., Synereo[1]), the dominant OSNs (e.g., facebook[2] and twitter [3]) are centralized, with their servers storing information related to the users or the data generated and disseminated by the users. Most OSNs follow a publisher/subscriber model: users publish the content to the central server and the central server disseminates the data to the users who have subscribed to the content (e.g., followers or friends). The content dissemination in OSNs is not necessarily a real-time process: the users can see the content at any time they wish as long as they have access to the Internet.

Social networks can also be decentralized. Decentralized social networks highlight users' control over their own data. The data are stored locally and shared with other users who they trust or closely relate to. Leveraging decentralization of social networks, user mobility could be exploited in MSNs to promote information sharing and region-specific interactions. Decentralized social networks emerged mainly due to privacy concerns in centralized OSNs [52], [13], [41]. Centralized servers could breach user privacy simply because all user-related sensitive data are stored in those central servers: data are exposed once the server is compromised or even the central server itself could be interested in the data. This coincides with privacy concerns in the context of VSNs, as it will become clear in the discussion below.

Essentially, user socialization could appear in any network where communication (thus user interactions) is convenient. As described earlier, vehicles are communication-enabled thanks to the OBUs pre-installed in the vehicles. Thus, interconnected vehicles enable drivers and passengers to socialize with other nearby users, forming VSNs. VSNs inherit characteristics of traditional social networks but they also have their own properties. In principle, VSNs are social networks built on top of Vehicular Ad-hoc Networks (VANETs) and considered as an extension of user-centric social networks. Applications in the VSNs could be based on the purpose of VC systems, e.g., safety applications, while entertainment applications could also be involved. We discuss different characteristics of VSNs illustrated in Fig. 1 in the rest of this section.

A. Networking Architecture

An OBU could integrate, an IEEE 802.11p interface as well as cellular and Wi-Fi interfaces. Through the IEEE 802.11p interface, vehicles communicate with other vehicles (V2V) or with RSUs (V2I). Cellular and Wi-Fi interfaces enable connection to the Internet via BSs and APs, and access to various SPs.

VSNs can be either centralized, decentralized or in a hybrid form. Similar to OSNs, a centralized VSN involves a central server, and users can interact via the central server. Decentralized VSNs could leverage VANETs to form groups on-the-fly and enable communication among the group members. In addition, information obtained from the central servers could be shared with other nodes in an ad hoc manner.

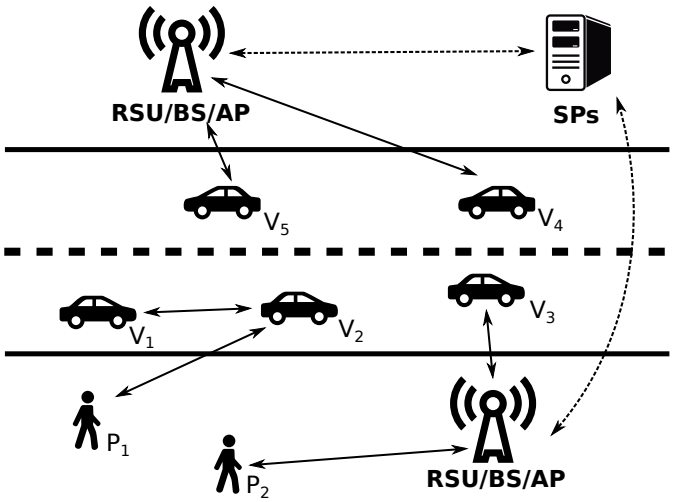

Fig. 1. Illustration of VSNs: (1) Vehicles (with OBUs, e.g., V_3, V_4 and V_5) and users (with smartphones, e.g., P_2) can access various Service Providers (SPs) via Road-Side Units (RSUs), Base Stations (BSs) or Access Points (APs); (2) Vehicles (e.g., V_1 and V_2) or users (e.g., P_1) can interact with each other in an ad-hoc network (e.g., share information obtained from SPs). (Icons made by Freepik from www.flaticon.com)

B. Participation and Social Relations

The participants in the VSNs are not limited to vehicles equipped with OBUs, but they can also be passengers and pedestrians using smartphones. The VSNs leverage VC systems while highlighting the social connections between the participants. Smartphone users could bring OSNs and VSNs closer. In fact, it becomes more common that data are shared among applications. VSN users could share data they obtained from the VSN or even the VC system within other OSNs they join. Such interactions among the OSNs and VSNs could promote the popularization of the VSN applications. Moreover, smartphone-based ITSs [40], [54], [17], [27] leverage smartphones and have been proposed as an alternative approach before OBU-equipped vehicles become universal.

VSN applications could exploit different kinds of user relations. Interest-based applications could maintain long-term relations among users. VSN users could be friends in OSN applications and at the same time interact with VC-related and ITS-related information within the VSN context, e.g., wish to share traffic-related information. In this case, OSN application only provide a way to establish relation in VSN applications. VSN interactions could also strictly specific to geographic regions while these interactions are short-term and do not assume any relationships a priori. For example, passengers with same destination in public transportation can share Point of Interest (POI) information around the destination.

[1] www.synereo.com
[2] www.facebook.com
[3] www.twitter.com

C. Applications

Any transportation-related information could be facilitated by VSN applications. Users can obtain traffic information from central providers and share these information with nearby users, or they can sense surrounding traffic condition and construct a global view based on contributed sensing data from multiple nearby users. This can be seen as an extension of VC applications. LBS is another type of important application in VSN. Traditional LBSs (e.g., querying POIs from LBS servers) could still exist in VSNs. However, as socialization is highlighted in VSNs, users could largely exploit their mobility and even generate customized location-dependent information (e.g., travel guide of a certain place) based on their interests, which can be later shared with other users who have similar interests. This is more dynamic and more user-centric compared to information that could be obtained from traditional LBSs. In general, users can in fact share any information they are interested in within VSNs, as long as the senders and the receivers are allowed to do so (e.g., not a copyrighted music).

III. Security and Privacy Considerations in VSNs

Security and privacy are key factors for designing and deploying a large scale trustworthy VSN. As described earlier, VSNs are built on top of VC systems and VSN applications should not deteriorate achieved VC system security and privacy. Security and privacy requirements could vary depending on VSN applications. For example, for a safety application (e.g., hazard warning), integrity, non-repudiation and accountability are of paramount importance (unlike confidentiality) while for a traffic management application, not only the integrity but also the verifiability of the content is crucial to prevent users being misled. On the contrary, for entertainment applications, the availability of the service is important. Next, we list and explain the basic security and privacy requirements for VSNs based on those for VC systems [45]; while in the following subsections, we further explain security and privacy concerns for the VSN applications.

A. Basic Security and Privacy Requirements

Authentication and Integrity: A node should authenticate the source of a message so that only the information from trusted, i.e., legitimate, source should be accepted. Moreover, messages should not be tampered: unauthorized entities should not be able to alter the content of the messages.

Confidentiality: Information exchanged by the users could be done in confidential manner: information is accessible only by authorized recipients, e.g., vehicles in a platoon, or vehicles from the same manufacturer. Information could be simply broadcasted, which does not need to be confidential (e.g., traffic conditions disseminated to a specific region).

Accountability and Non-repudiation: Entities in the system, including vehicles (i.e., OBUs), smartphones and infrastructures, should be accountable for the actions they perform in the system, and should not be able to deny the actions they have performed in the system.

Unlinkability and Anonymity: User identities should not be exposed, i.e., users should be anonymous and their (authenticated) messages should not be linkable. However, for practicality and efficiency, we inherit conditional anonymity (i.e., pseudonymity) from the VC domain: user messages are only linkable over a system defined period τ, and users are pseudonymous as long as they do not misbehave in the system. Moreover, users should be able to gain and accumulate reputation or credits for their contribution to the system while using pseudonyms as their legitimate identities in the system.

Access Control: Only legitimate entities, registered within the system, should be able to operate and contribute to the system. The system should prevent any illegitimate entity from participating in system operations, e.g., content delivery or crowdsourcing. In VSNs, user interactions could also be restricted by relationships: unlink message broadcast and sender authentication in VC systems, user interactions could be allowed strictly based on relationships (e.g., among friends).

Availability: The system should remain operational even in case of a fault. Especially, the functionality of underlying network architecture (i.e., user safety and traffic efficiency) should not be affected due to the system failure.

B. Adversarial Model

Honest-but-Curious Entities: Recent experience from mobile applications (e.g., LBSs) [29] shows that service providers are aggressively collecting user information in order to profile users. For example, an LBS server could collect user queries (including user locations and interests) in order to offer customized services or push advertisements to the users. This led to the concerns from the users on their private information. In a general sense, this applies to every entity within the system, e.g., passive observers, service providers and security infrastructure entities, which can infer information in order to infringe user privacy. Many works try to solve this problem by transferring the trust to an introduced Trusted Third Party (TTP) [22], [42]: a proxy is introduced between the users and the honest-but-curious server, so that all user requests are anonymized by the proxy before forwarding to the servers. However, the same concern should be applied to any entity that is introduced to solve this problem, for which those works assumed to be fully trustworthy. Essentially, if the same information is available to the servers and the introduced TTPs, then there is no difference between what the servers and those entities could do (i.e., the information they can infer).

This is why we need to extend our adversarial model from *fully-trustworthy* to *honest-but-curious* servers. Honest-but-curious entities never deviate from system security policies or protocols, but they are tempted to infer and exploit user sensitive information, e.g., profile users and push advertisements to users based on their interests.

Malicious Participants: Due to the dynamic nature (intensified in a decentralized architecture) of VSNs, registered vehicles and users (legitimate insiders) are able to disseminate faulty information to affect a process, e.g, temperature measurement. In addition, internal adversaries might try to pollute the content achieved from the content provider before they

share with other users. This is due to the openness of sharing data in VSNs which leads to additional vulnerabilities than in traditional social networks. Polluted data reported from faulty insiders should be filtered out and malicious users should be evicted from the system. This requires that the accountability of user actions in the network be preserved. The situation is even worse if a malicious user is able to equip with multiple valid (yet fake) identities and affect the system with those identities. For example, an adversary could clone an identity (which he/she should not own) to mislead other users by disseminating aggressively the false information. This type of attack is well known as Sybil-based misbehavior [15] in which an attacker is able to clone an identity, thus creating socialbots. They can perform various kinds of attacks, e.g., injecting bogus messages to control the outcome of a specific protocol, or disseminating spams to other users.

On the contrary, external adversaries have limited capabilities to destroy the system; however, they can try to harm user privacy by eavesdropping the communication, or they could simply launch jamming and Distributed Denial of Service (DDoS) attacks on a specific target or area to breach the system availability.

Selfish Participants: Crowdsourcing based mobile applications [19], [49], [20], [39] have been widely used for enhancing transportation efficiency and safety. These applications rely on users' participation and contribution to measure specific phenomena (e.g., temperature and traffic status). However, such applications would not work without active participation of users. In a VSN, selfish users could try to achieve higher and optimal awards by sacrificing the minimum resources. These misbehaving internal adversaries utilize the resource of other nodes to achieve a better service without participating in the tasks [32]. The success of these applications depends on the participation of the majority of users and their collaboration to achieve desired goals. Unless the mechanisms that motivates the user participation are in place, selfish users would not be willing to consume resources for other users or the system. Appropriate mechanisms should be provided to monitor user activities or incentivize users for their contribution to the system; the system should be able to identify selfish users or free riders, thus eradicate them from the system or degrade and limit their access to (the services in) the system.

IV. Existing Security and Privacy Solutions

A lot of research effort on security and privacy have been carried out in the relevant areas, e.g., VC, MSN and crowdsourcing. Security and privacy solutions in those areas could be evolved and integrated to VSNs in order to address similar problems that exist in the VSNs. In this section, we introduce existing solutions from other domains that could facilitate secure and privacy preserving VSNs.

A. Decentralization

Decentralization of a system could be due to various reasons, among which privacy is one of the main concerns that motivates the decentralization. It has been considered in many works that the central servers in OSNs or LBSs are tend to collect sensitive information of users and even inferring extra information from the collected data [48], [24], [31]. Such central servers fall into honest-but-curious model. Location privacy is a main concern in VSNs, since the interactions among the entities in VSNs are location-dependent: information obtained from the servers are customized based on the geographical information of the vehicles (e.g., LBSs). The geographical information could be used to track the users and even the interests of a specific user can be inferred from the information being requested. *k-anonymity* [23], [22] has been widely used for protecting location information of users in both centralized or decentralized manners. Anonymizer-based approaches leverage an anonymizer introduced between the users and the servers [22], [42]. However, it has been considered in many works that such anonymizer could also be a threat for user privacy, i.e., they can also be honest-but-curious [48], [31]. Decentralized approaches have been proposed to eliminate such concerns. Users could leverage peers around them to form a region that involves $k-1$ other users and use this obfuscated region instead of an accurate location [23], [28]. Such approaches trade off high burden on the users' mobile devices for searching nearby peers. Moreover, it is also an issue that have been pointed out in many research, the strategy of peer selections determines the efficiency and effectiveness of the schemes [23], [28]. Especially, when node mobilities are not predictable, this would be even harder.

Such collaboration in VSNs could be made easier by forming groups in VANET leveraging similar mobilities of vehicles. In [46], nearby vehicles form groups and maintain the groups as long as the vehicles are within each other's communication range. Each group has a leader which acts as a temporary anonymizer for the group. The group leader is rotated over time within the group in order to share the burden among the group members and limit the information that could be learned by the group leader. Such temporary centralization leverages the characteristics of VANET and decrease the effort for searching for the most suitable peers. However, these approaches would not help if the honest-but-curious server is only interested in the symbolic locations (e.g., church, shopping mall and railway station) of the users, since all the k members are likely to fall in a same symbolic location.

Content-sharing can further protect privacy of users, since the users do not need to query the content-provider for every request, from which the content-provider could learn sensitive data of the users. For example, information sharing in LBS [48] help users to protect their privacy in a collaborative way. In [48], users share LBS-obtained information with their neighbors so that the users who need the same information does not need to query the LBS server again. This decreases the user exposure to the LBS server. However, it can also allow internal attackers to provide faulty information to benign users, while the receivers do not have clue if the information is valid or not, as long as they do not query the LBS server directly. As a common issue in an open decentralized network architectures, it is vulnerable to active malicious nodes within the network. Thus, the user authentication is needed to eliminate illegitimate users from the network.

B. Pseudonymous Authentication

To address the concern brought by the openness of decentralized systems, transmissions in VSNs should be verifiable in terms of trust, especially for the safety-related applications. In most of the VSN applications, users are strangers to each other and had no social interaction before. Vehicles have limited time to share information with each other due to the mobility of vehicles, i.e., the V2V communications are highly dynamic and unreliable. This implies that the users cannot leverage accumulated reputation for trust establishment among the users. Public-Key Infrastructure (PKI)-based solutions could be used to ensure authenticity and integrity of the transmitted messages, in which trust among the vehicles are established leveraging a TTP (i.e., a Certification Authority (CA)). However, with traditional certificate-based authentication, one can easily trace the messages related to a specific vehicle based on its identity (in the certificate), thus profile its behavior/action, especially considering the openness of wireless networks. Encryption of messages would help so that only the targeted recipients could decrypt the messages. However, as described earlier, vehicles have ephemeral encounter events so that it is unrealistic to negotiate (multiple pairs of) security associations within short period with (multiple) recipient(s) and encrypt all the transmissions. Moreover, it is hard to decide in advance the interested recipients in case the transmission are region-based/targeted, i.e., the messages should be authenticated and broadcasted to all the neighboring nodes. Thus, the approaches relying on long-term identity cannot be used since all the user actions could be linkable. This motivated many works with their solutions leveraging anonymous credentials to satisfy both the security and privacy requirements in VC domain.

Generally, there are two categories of Vehicular Public-Key Infrastructure (VPKI) schemes proposed for the VC systems: public key based and group signature based schemes. The public key based schemes [1], [26], [51], [47], [3], [33] equip users with a set of short-term (pseudonymous) credentials (i.e., pseudonyms), switching from one pseudonym to another over time. A pseudonym is a public key authenticated by the Pseudonymous Certification Authority (PCA). The pseudonyms are essentially unlinkable, i.e., one cannot link two pseudonyms since they are anonymized (i.e., do not include any information that could be linkable). Each user signs an outgoing content with time- and geo-stamped using the private key corresponding to the current valid pseudonym. The content is attached with the pseudonym (and possibly the chain of trust) to facilitate the verification by the recipient. Having received a content, depending on the spatial, temporal, and interest scope of the receivers, they verify the attached pseudonyms first and then validate the signature on the content using the public key of the attached pseudonym.[4] Using the anonymous pseudonyms, one can achieve integrity, non-repudiation, accountability and conditional anonymity. Pseudonymous can be integrated with different services (and their SPs) to provide secure and privacy preserving VSNs. For example, in [31], a secure and privacy-enhancing LBS is proposed leveraging information sharing and the pseudonymous authentication. Users authenticate their queries and responses under the pseudonyms obtained from the PCA. In this way, illegitimate users are prevented from providing false information to the benign users, while internal adversaries are kept accountable for their actions. Fig. 2 shows the secure and privacy preserving VSNs architecture leveraging pseudonymous authentication.

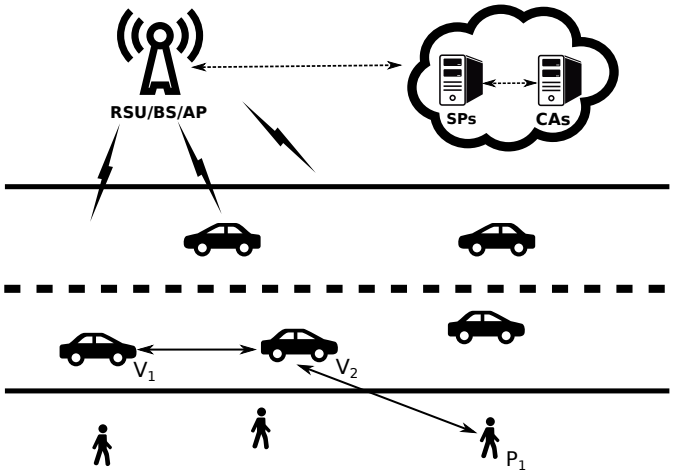

Fig. 2. Vehicles and users can obtain pseudonyms from the Certification Authorities (CAs). The communication in the VSNs is protected with pseudonymous authentication including P2P communication (e.g., V_1-V_2 and V_2-P_1) in the ad-hoc network and vehicle/user-SP communication. (Icons made by Freepik from www.flaticon.com)

The other schemes propose the use of group based signature schemes [9], [51], [37], [38] for identity and credential management in VC systems. These approaches leverage group signatures [11], [6], [4] in which the receiver can verify that a legitimate group member has signed a message without knowing who the signer is. In case of a misbehavior, the group manager is able to *open* a signature, thus disclosing and revoking the signer's identity.

While group signatures can be used to protect the transmitted messages, such schemes exhibit high computational overhead for signature generation and verification [8]. The integration of group signatures and pseudonyms could decrease the computational overhead for resource-constrained devices. [8] proposes a hybrid approach in which the vehicles generate public/private key pairs and sign the public keys with their own group signing keys. In this way, a pseudonym needs to be verified only once for the first time it is received and cached locally during its lifetime. For the following messages signed under the cached pseudonyms, only the signatures on the messages need to be verified with the public key of the pseudonym, which are much cheaper than group signature verifications.

C. Sybil Resilience

Using such pseudonymous authentication approaches, it is possible that a compromised vehicle equipping itself with multiple simultaneously valid pseudonyms (e.g., by requesting pseudonyms for the same period multiple times). This set the

[4]We assume that the sender and receiver trust the pseudonym issuer, the PCA.

ground for Sybil-based misbehavior [15]. The early proposal [44] propose to equip each vehicle with a tamper-proof Hardware Security Module (HSM), which prevents adversaries from manipulating pseudonym acquisition and usage. However, in a heterogeneous system like VSN, where various kinds of mobile devices are involved, such assumption would not stand.

It would be straightforward if the pseudonym provider simply issues pseudonyms with non-overlapping lifetimes and keeps a record of pseudonym issuance for each vehicle. Then, the pseudonym provider would know until when the issued pseudonyms are valid for a vehicle and only issue pseudonyms for the period after that. However, this would not work if there exist multiple pseudonym providers (so that a vehicle can request pseudonyms from the closest one) and a vehicle can request pseudonyms from different pseudonym providers. This is due to the separation of duties among authorities is enforced in VC domain so that the pseudonym providers are not allowed to share their records (otherwise the authorities could collude and infer extra information) [33], [24]. [33] proposes a ticket-based scheme: an anonymized ticket is obtained from identity provider, then the ticket is used to obtain pseudonyms from a pseudonym provider. Each ticket is bound to a specific pseudonym provider without disclosing the targeted pseudonym provider to the identity provider, so that each ticket can be used only once while not revealing location of the vehicle to the identity provider. Moreover, the identity provider (only) learns for which period a vehicle has requested pseudonyms for, so no ticket will be issued again for the same period.

D. Data Verification

Entity authentication would help to eliminate illegitimate users and enhance the trustworthiness of the content being transmitted among the users. Leveraging post-misbehavior approaches (e.g., pseudonym resolution [33]), the entities that provided faulty information could be punished (e.g., revoked from the system). However, accepting false information (e.g., related to safety applications) from internal adversaries would be fatal and the problem would not be solved although the entities could be revoked from the system, if such misbehaviors have already led to accidents. This requires the received data to be verified and validated before it is accepted, i.e., the trustworthiness of the received data need to be verified even after the source and the integrity of the data is verified with signature verification.

[14], [25] propose internal attacker detection approaches for sensing data aggregation based on redundancy of data received from multiple sensing entities, assuming the majority of the internal nodes are honest. In both works, the authors leverage entity authentication. In [14], each vehicle aggregates the received data which correspond to the same event and merge the data with its own sensing data and forward to neighboring vehicles. Each received message contains a path list and the redundancy is determined based on the nodes included in the path lists so that malicious nodes could not increase the redundancy of false information by affecting the aggregated data from multiple paths. In [25], the sensing data from users' mobile devices are sent to and aggregated by the central server. The aggregated data then can be queried by the users. The server detects the outliers purely based on the sensing data (e.g., temperature measurement) submitted from users' mobile devices. The server is trained with initial submissions and is updated with the successive submissions, then the outliers are detected based the training results.

E. Fairness and Incentives

Collaboration among the nodes is the basis of security and privacy solutions in various domains (e.g., privacy-enhancing LBS [48] and Participatory Sensing (PS) networks [7], [21]). Such solutions rely on participation and contribution from single entities to share workload of tasks or form groups to provide shelters for the nodes who wish to perform privacy-sensitive activities. In [48], LBS-obtained information is shared with other peers so that the peers who is looking for the same information does not need to expose their location (and activities) to the possibly honest-but-curious LBS servers. Crowdsourcing applications leverage contribution from the users in the system to infer context-dependent data (e.g., temperatures and humidity) when central providers do not exist. In principle, user experience would be improved with more user participation. However, without any guarantee for users' participation, selfish users could choose to benefit from the system while not contributing to the system (e.g., requesting information from neighbors while not sharing information with others). A motivation is needed for the user participation to keep the whole system operational.

Users' contribution can be monitored by the central infrastructures. [36] proposes cooperative verification of safety beacons in VANET, in which vehicles share the verification results with other vehicles so that each and every vehicle does not need to verify the signatures on all the received beacons. The whole process is monitored by the RSUs leveraging ID-based signcryption scheme [5], [2]. The RSUs provide each vehicle with a token for each time slot. A token is used by a vehicle to sign and encrypt its own verification effort (an integrated signature on multiple beacons), and decrypt and verify the verification efforts from other vehicles within the time slot. The vehicles have to prove to the RSUs that reasonable amount of effort have been made to obtain a new token for the next time slot, otherwise would not be able to decrypt the integrated signatures and benefit from other vehicles during the next time slot.

Incentivized scheme can be used to ensure the users' contribution, in which users are awarded virtual credits for their contribution. [55], [12] propose incentive mechanism for data forwarding in Delay Tolerant Network (DTN), in which a central server stores the credits of different users. After each successful transmission, the credit is charged from the source node and distributed to intermediate nodes which relayed the packets. If a node does not actively participate in the transmissions, it would not have enough credits to send its own packets.

V. Open Challenges

Based on and beyond the existing solutions for security and privacy preserving VSNs, there still exist a number of significant security and privacy challenges towards deploying such VSNs. Next, we explain these challenges with the current (yet not complete) efforts towards them.

A. Resilience Considerations

Sybil resilience in VSNs remains an open challenge in the absence of consensus because the standardization bodies [16], [30] and harmonization efforts do not have conclusive views on that front. For example, Car2Car Communication Consortium (C2C-CC) [10] proposes to issue pseudonyms with overlapping lifetimes in order to keep the safety applications operational at any given point in time [34], while [44], [33] (works in the context of SeVeCom [35] and PRESERVE EU project [50] respectively) proposes to issue pseudonyms with non-overlapping lifetimes in order to eliminate the possibility of equipping a vehicle with multiple simultaneously valid short-term identities. However, beyond enforcing this constraint within a domain, malicious users could exploit the existence of multiple domains [1], [26], [18] to obtain simultaneously valid pseudonyms from different domains, depending on the pseudonym usage policies.

[26], [43] propose to use an HSM module for pseudonym management and cryptographic operations in order to prevent malicious users from deviating system policies for the pseudonym usage. However, in a VSN, a heterogeneous networks with various kinds of mobile devices involved, it is not realistic to assume that all the devices (e.g., smartphones) would be integrated with HSMs. Therefore, it is interesting to raise a question: *how to prevent users, with no HSM equipment, from obtaining pseudonyms from different PCAs in a multi-domain environment?* To the best of our knowledge, [33] is the only scheme that prevents Sybil-based misbehavior at the security infrastructure without relying on HSM.

However, another issue still remains: *how to prevent users from sharing pseudonyms with each other?* Users can still transfer the private keys and pseudonyms to other devices if a pseudonym is not explicitly bound to an entity. Even though the ownership of the pseudonym is maintained by the security infrastructure and the real identity of the owner of a pseudonym could be resolved in case of misbehavior, such an on-demand process does not support real-time detection and prevent the users from sharing/transferring their credentials in the presence of malicious users (e.g., two malicious nodes can share their pseudonyms and act as Sybil nodes in two different areas).

B. Inference Attacks

Open wireless networks inevitably face security and privacy issues because anyone can eavesdrop the messages and manipulate them. Messages eavesdropped in the VSN can be used to infer user activities, profile users or track a specific user. An observer could leverage different techniques, e.g., data mining, with the publicly available information to link user messages and track them based on the geographical information included in the messages. In principle, inference attacks are feasible due to openness of the transmitted messages (i.e., user information is anonymized but message content is kept open). Keeping message content confidential would prevent external eavesdroppers, however, this would introduce extra processing delay and affect real-time operations in the system.

Due to the disclosed location information and the structure of the roads (i.e., mobility restrictions), it is not difficult to link users according to the available information. For example, an attacker who is able to eavesdrop all beacons within the VANET is able to track the vehicles with almost 100% accuracy [53]. Meta-data in the disseminated data can be used as extra information to link users. For example, an adversary can link beacons based on, e.g., speed and direction, or even link pseudonyms based on their lifetimes [33]. As the VSN applications become popular, more and more data will be exchanged among the vehicles; thus, the privacy of users is at stake.

C. Operational Challenges in Identity Management

Facilitating cross domain operations is one of the main operational challenges in VC systems [34]. Similar to VC systems, trust establishment has to be taken into consideration before deploying a secure and privacy-preserving multi-domain VSN. Trust establishment among the vehicles within the same domain, e.g., Volvo cars (assuming cars from the same manufacturer fall in a same domain), should be easy; however, in this case, it is not clear how a user with Volvo car should establish trust with a Toyota car. The key operational questions are: *who will be operating the identity and credential provision?* More importantly, *how the trust among the vehicles are established?* [34].

On the other hand, pseudonymous authentication provides adequate level of security and privacy; however, revocation of the pseudonyms has not been fully addressed by academia and the industry. There are several challenges in pseudonym acquisition and revocation, e.g., connectivity to the CA for fetching Certificate Revocation List (CRL), acquisition of a large number of pseudonyms in an unstable network condition and the necessity to integrate a misbehavior detection mechanism to identify misbehaving entities and revocation of them.

As described in IV-E, there are the cases when user contribution needs to be recorded and incentivized: any contribution made under pseudonyms should be dedicated to corresponding long-term identities, otherwise the record would be lost once a new pseudonym is used. This could be achieved with the help of a central server keeping the credits of each user. However, such approach conflicts with the motivation behind pseudonymous authentication: any two pseudonyms of a same user should not be linkable, as it requires the central server to identify which pseudonyms corresponds to which long-term identities. This leaves a challenge of accumulating credits for user contribution while preserving user privacy.

VI. Conclusions

In this chapter, we surveyed and presented the state-of-the-art VC systems, security and privacy architectures and

technologies, emphasizing on security and privacy challenges and their solutions for P2P interactions in VSNs towards standardization and deployment. We note that beyond safety applications that have drawn a lot of attention in VC systems, there is significant and rising interest in vehicle-to-vehicle interaction for a range of transportation efficiency and infotainment applications, notably LBS as well as a gamut of services by mobile providers. While this enriches the VC systems and the user experience, security and privacy concerns are also intensified. This is especially so, considering (i) the privacy risk from the exposure of the users to the service providers, and (ii) the security risk from the interaction with malicious or selfish and thus misbehaving users or infrastructure. We showed existing solutions can in fact evolve and address the VSN-specific challenges, and improve or even accelerate the adoption of VSN applications.

REFERENCES

[1] Nikolaos Alexiou, Marcello Laganà, Stylianos Gisdakis, Mohammad Khodaei, and Panos Papadimitratos. Vespa: Vehicular security and privacy-preserving architecture. In *ACM HotWiSec*, Budapest, Hungary, April 2013.

[2] Paulo S. L. M. Barreto, Benoît Libert, Noel McCullagh, and Jean-Jacques Quisquater. Efficient and provably-secure identity-based signatures and signcryption from bilinear maps. In *Advances in Cryptology-ASIACRYPT*. Chennai, India, December 2005.

[3] Norbert Bißmeyer, Jonathan Petit, and Kpatcha M Bayarou. Copra: Conditional pseudonym resolution algorithm in vanets. In *IEEE WONS*, Banff, Canada, March 2013.

[4] Dan Boneh, Xavier Boyen, and Hovav Shacham. Short group signatures. In *Advances in Cryptology–CRYPTO*, Santa Barbara, CA, August 2004.

[5] Dan Boneh and Matt Franklin. Identity-based encryption from the weil pairing. In *Advances in Cryptology-CRYPTO*, Santa Barbara, CA, August 2001.

[6] Dan Boneh and Hovav Shacham. Group signatures with verifier-local revocation. In *ACM CCS*, Washington, DC, October 2004.

[7] Jeffrey A. Burke, Deborah Estrin, Mark Hansen, Andrew Parker, Nithya Ramanathan, Sasank Reddy, and Mani B. Srivastava. Participatory sensing. *Center for Embedded Network Sensing*, 2006.

[8] Giorgio Calandriello, Panos Papadimitratos, J-P Hubaux, and Antonio Lioy. On the performance of secure vehicular communication systems. *IEEE TDSC*, 8(6):898–912, 2011.

[9] Giorgio Calandriello, Panos Papadimitratos, Jean-Pierre Hubaux, and Antonio Lioy. Efficient and robust pseudonymous authentication in vanet. In *ACM VANET*, Montral, Canada, September 2007.

[10] Car-to-Car Communication Consortium (C2C-CC). http://www.car-2-car.org/.

[11] David Chaum and Eugène Van Heyst. Group signatures. In *Advances in Cryptology-EUROCRYPT*, Brighton, UK, April 1991.

[12] Bin Chen and Mun Choon Chan. Mobicent: a credit-based incentive system for disruption tolerant network. In *IEEE INFOCOM*, San Diego, CA, March 2010.

[13] Leucio Antonio Cutillo, Refik Molva, and Thorsten Strufe. Safebook: Feasibility of transitive cooperation for privacy on a decentralized social network. In *IEEE WoWMoM*, Kos, Greece, June 2009.

[14] Stefan Dietzel, Julian Gurtler, Rens van der Heijden, and Frank Kargl. Redundancy-based statistical analysis for insider attack detection in vanet aggregation schemes. In *IEEE VNC*, Paderborn, Germany, December 2014.

[15] John R Douceur. The sybil attack. In *ACM Peer-to-peer Systems*. London, UK, March 2002.

[16] TCITS ETSI. Etsi ts 103 097 v1. 1.1-intelligent transport systems (ITS); security; security header and certificate formats, standard, tc its, 2013.

[17] Mohamed Fazeen, Brandon Gozick, Ram Dantu, Moiz Bhukhiya, and Marta C González. Safe driving using mobile phones. *IEEE Transactions on Intelligent Transportation Systems*, 13(3), 2012.

[18] David Förster, Hans Löhr, and Frank Kargl. PUCA: A Pseudonym Scheme with User-Controlled Anonymity for Vehicular Ad-Hoc Networks (VANET). In *IEEE VNC*, Paderborn, Germany, December 2014.

[19] Jon Froehlich, Tawanna Dillahunt, Predrag Klasnja, Jennifer Mankoff, Sunny Consolvo, Beverly Harrison, and James A. Landay. Ubigreen: investigating a mobile tool for tracking and supporting green transportation habits. In *International Conference on Human Factors in Computing Systems*, April 2009.

[20] Raghu K Ganti, Nam Pham, Hossein Ahmadi, Saurabh Nangia, and Tarek F Abdelzaher. GreenGPS: a participatory sensing fuel-efficient maps application. In *ACM MobiSys*, San Francisco, CA, June 2010.

[21] Raghu K. Ganti, Fan Ye, and Hui Lei. Mobile crowdsensing: current state and future challenges. *IEEE Communications Magazine*, 49(11):32–39, 2011.

[22] Bugra Gedik and Ling Liu. Protecting location privacy with personalized k-anonymity: Architecture and algorithms. *IEEE Transactions on Mobile Computing*, 7(1):1–18, 2008.

[23] Gabriel Ghinita, Panos Kalnis, and Spiros Skiadopoulos. Mobihide: a mobilea peer-to-peer system for anonymous location-based queries. In *Advances in Spatial and Temporal Databases*. Boston, MA, July 2007.

[24] Stylianos Gisdakis, Thanassis Giannetsos, and Panos Papadimitratos. Sppear: security & privacy-preserving architecture for participatory-sensing applications. In *Proceedings of the 2014 ACM conference on Security and privacy in wireless & mobile networks*, pages 39–50, 2014.

[25] Stylianos Gisdakis, Thanassis Giannetsos, and Panos Papadimitratos. Shield: A data verification framework for participatory sensing systems. In *ACM WiSec*, New York, NY, June 2015.

[26] Stylianos Gisdakis, Marcello Laganà, Thanassis Giannetsos, and Panos Papadimitratos. SEROSA: Service oriented security architecture for vehicular communications. In *IEEE VNC*, Boston, MA, December 2013.

[27] Stylianos Gisdakis, Vasileios Manolopoulos, Sha Tao, Ana Rusu, and Panos Papadimitratos. Secure and privacy-preserving smartphone-based traffic information systems. *IEEE Transactions on Intelligent Transportation Systems*, 16(3):1428–1438, 2015.

[28] Aris Gkoulalas-Divanis, Panos Kalnis, and Vassilios S Verykios. Providing k-anonymity in location based services. *ACM SIGKDD Explorations Newsletter*, 12(1):3–10, 2010.

[29] Glenn Greenwald. NSA prism program taps in to user data of apple, google and others, June 2013.

[30] IEEE P1609.2/D12. Draft Standard for Wireless Access in Vehicular Environments, Jan. 2012.

[31] Hongyu Jin and Panos Papadimitratos. Resilient collaborative privacy for location-based services. In *Nordic Conference on Secure IT Systems*. Stockholm, Sweden, October 2015.

[32] Apu Kapadia, David Kotz, and Nikos Triandopoulos. Opportunistic sensing: Security challenges for the new paradigm. In *COMSNETS*, Bangalore, India, January 2009.

[33] M. Khodaei, Hongyu Jin, and P. Papadimitratos. Towards deploying a scalable & robust vehicular identity and credential management infrastructure. In *IEEE VNC*, Paderborn, Germany, December 2014.

[34] Mohammad Khodaei and Panos Papadimitratos. The key to intelligent transportation: Identity and credential management in vehicular communication systems. *IEEE Vehicular Technology Magazine*, 10(4):63–69, 2015.

[35] Tim Leinmüller, Levente Buttyan, Jean-Pierre Hubaux, Frank Kargl, Rainer Kroh, Panos Papadimitratos, Maxim Raya, and Elmar Schoch. Sevecom-secure vehicle communication. In *IST Mobile and Wireless Communication Summit*, Mykonos, Greece, June 2006.

[36] Xiaodong Lin and Xu Li. Achieving efficient cooperative message authentication in vehicular ad hoc networks. *IEEE Transactions on Vehicular Technology*, 62(7):3339–3348, 2013.

[37] Xiaodong Lin, Xiaoting Sun, Pin han Ho, and Xuemin Shen. GSIS: A secure and privacy-preserving protocol for vehicular communications. *IEEE Transactions on Vehicular Technology*, 56(6):3442–3456, 2007.

[38] Rongxing Lu, Xiaodong Lin, Haojin Zhu, Pin-Han Ho, and Xuemin Shen. ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications. In *IEEE INFOCOM*, Phoenix, AZ, Apr. 2008.

[39] Guilherme Maia, Andre LL Aquino, Aline Viana, Azzedine Boukerche, and Antonio AF Loureiro. HyDi: a hybrid data dissemination protocol for highway scenarios in vehicular ad hoc networks. In *ACM DIVANet*, Paphos, Cyprus Island, October 2012.

[40] Vasileios Manolopoulos, Panos Papadimitratos, Sha Tao, and Ana Rusu. Securing smartphone based its. In *ITS Telecommunications*, St. Petersburg, Russia, August 2011.

[41] Ghita Mezzour, Adrian Perrig, Virgil Gligor, and Panos Papadimitratos. Privacy-preserving relationship path discovery in social networks. In *International Conference on Cryptology and Network Security*. Kanazawa, Japan, December 2009.

[42] Mohamed F Mokbel, Chi-Yin Chow, and Walid G Aref. The new casper: query processing for location services without compromising privacy. In *Proceedings of the 32nd international conference on Very large data bases*, Seoul, Korea, September 2006.

[43] Panos Papadimitratos, Levente Buttyan, Tamas Holczer, Elmar Schoch, Julien Freudiger, Maxim Raya, Zhendong Ma, Frank Kargl, Antonio Kung, and J-P Hubaux. Secure vehicular communication systems: Design and architecture. *IEEE Communications Magazine*, 46(11):100–109, 2008.

[44] Panos Papadimitratos, Levente Buttyan, J-P Hubaux, Frank Kargl, Antonio Kung, and Maxim Raya. Architecture for secure and private vehicular communications. In *ITST*, Sophia Antipolis, France, June 2007.

[45] Panos Papadimitratos, Virgil Gligor, and Jean-Pierre Hubaux. Securing vehicular communications-assumptions, requirements, and principles. In *ESCAR*, Berlin, Germany, November 2006.

[46] Krishna Sampigethaya, Mingyan Li, Leping Huang, and Radha Poovendran. AMOEBA: Robust location privacy scheme for vanet. *IEEE Journal on Selected Areas in Communications*, 25(8):1569–1589, 2007.

[47] Florian Schaub, Frank Kargl, Zhendong Ma, and Michael Weber. V-tokens for conditional pseudonymity in vanets. In *IEEE WCNC*, NJ, USA, April 2010.

[48] 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*, 11(3):266–279, 2014.

[49] Stephen Smaldone, Chetan Tonde, Vancheswaran K. Ananthanarayanan, Ahmed Elgammal, and Liviu Iftode. The cyber-physical bike: A step towards safer green transportation. In *HotMobile*, Phoenix, AZ, March 2011.

[50] Jan Peter Stotz, Norbert Bißmeyer, Frank Kargl, Stefan Dietzel, Panos Papadimitratos, and Christian Schleiffer. Security requirements of vehicle security architecture, PRESERVE - Deliverable 1.1, June 2011.

[51] Ahren Studer, Elaine Shi, Fan Bai, and Adrian Perrig. Tacking together efficient authentication, revocation, and privacy in vanets. In *IEEE SECON*, Rome, Italy, June 2009.

[52] Akriti Verma, Deepak Kshirsagar, and Sana Khan. Privacy and security: Online social networking. *International Journal of Advanced Computer Research*, 3(8):310–315, 2013.

[53] Björn Wiedersheim, Zhendong Ma, Frank Kargl, and Panos Papadimitratos. Privacy in inter-vehicular networks: Why simple pseudonym change is not enough. In *IEEE WONS*, Kranjska Gora, Slovenia, February 2010.

[54] Jorge Zaldivar, Carlos T Calafate, Juan Carlos Cano, and Pietro Manzoni. Providing accident detection in vehicular networks through obd-ii devices and android-based smartphones. In *IEEE Conference on Local Computer Networks*, Bonn, Germany, October 2011.

[55] Jun Zhou, Xiaolei Dong, Zhen-Fu Cao, and Athanasios Vasilakos. Secure and privacy preserving protocol for cloud-based vehicular dtns. *Information Forensics and Security, IEEE Transactions on*, 10(6):1299–1314, 2015.