Journal of
Sensor and Actuator Networks

MDPI

Review

Social Internet of Vehicles for Smart Cities

Leandros A. Maglaras *, Ali H. Al-Bayatti, Ying He, Isabel Wagner and Helge Janicke

School of Computer Science and Informatics, De Montfort University, The Gateway, Leicester LE1 9BH, UK; alihmohd@dmu.ac.uk (A.H.A.-B.); ying.he@dmu.ac.uk (Y.H.); isabel.wagner@dmu.ac.uk (I.W.); heljanic@dmu.ac.uk (H.J.)

* Correspondence: leandros.maglaras@dmu.ac.uk; Tel.: +44-116-207-8483

Academic Editor: Ioannis Chatzigiannakis
Received: 1 December 2015; Accepted: 3 February 2016; Published: 6 February 2016

Abstract: Digital devices are becoming increasingly ubiquitous and interconnected. Their evolution to intelligent parts of a digital ecosystem creates novel applications with so far unresolved security issues. A particular example is a vehicle. As vehicles evolve from simple means of transportation to smart entities with new sensing and communication capabilities, they become active members of a smart city. The Internet of Vehicles (IoV) consists of vehicles that communicate with each other and with public networks through V2V (vehicle-to-vehicle), V2I (vehicle-to-infrastructure) and V2P (vehicle-to-pedestrian) interactions, which enables both the collection and the real-time sharing of critical information about the condition on the road network. The Social Internet of Things (SIoT) introduces social relationships among objects, creating a social network where the participants are not humans, but intelligent objects. In this article, we explore the concept of the Social Internet of Vehicles (SIoV), a network that enables social interactions both among vehicles and among drivers. We discuss technologies and components of the SIoV, possible applications and issues of security, privacy and trust that are likely to arise.

Keywords: Social Internet of Things; Internet of Vehicles; security; privacy; trust

1. Introduction

Smart cities are areas where innovation is supported through digital networks and applications [1]. Smart cities are often called sustainable, digital or connected cities [2]. The goal of converting a city into a smart environment is to alleviate the problems resulting from urbanization and increased urban population. A smart city is an urban area that provides the conditions for sustainable economic growth and quality of life. Smart solutions, like traffic congestion avoidance [3], green buildings [4] and modern industrial control systems (ICS) [5], are some of the technologies that can make today's urbanization sustainable. A smart city involves the intelligent use of technology to improve how people live, work, commute and share information [6]. A key aspect of a smart city is next generation vehicles that incorporate new sensing, communication and social capabilities as part of the wider Internet of Things concept. By providing mobile wireless sensing and communications, vehicles can facilitate data access, which is fundamental to make smart cities a reality.

Wireless networks can be divided into three main categories. First, infrastructure wireless networks rely on a central station that coordinates all communications [7]. Second, non-structured networks or *ad hoc* networks give equal roles to all stations in the network [8,9]. Third, hybrid networks combine the first two categories [10]. An example of hybrid networks is hybrid vehicular *ad hoc* networks (hybrid-VANETs) [11], which use *ad hoc* networks for communication between vehicles and infrastructure networks, such as wireless local area networks (WLANs) and cellular systems for communication with a core network [12,13]. Smart vehicles, through their advanced communication capabilities, will be able to interact not only with navigation and broadcast satellites,

but also with passenger smart phones, roadside units and other smart vehicles, making them an important component of IoT and the development of smart cities [14]. VANETs combine these with new applications and methods to enable the intelligent communication between vehicles and the connection to the Internet. VANETs rely on roadside units (RSU) and on-board units (OBU) to facilitate the connectivity and the intelligence of the smart vehicle. RSUs are communication infrastructure units that are positioned next to roads to connect vehicles to a larger infrastructure or to a core network, such as a metropolitan traffic management system. The OBU is a network device integrated into smart vehicles that supports different wireless networks, such as dedicated short-range communication (DSRC) and WLAN. A VANET has a diverse range of applications, from road safety, through the detection and avoidance of traffic accidents [15], traffic control, through reduction of traffic congestion [16], as well as infotainment, through the improvement of driving comfort [17]. Recently, three of the biggest companies that provide digital content and operating systems for mobile devices, Google, Apple and Microsoft, have announced their actions toward taking over the in-car infotainment system with their operating systems dedicated to vehicles and mobile devices (CarPlay, Android Auto and Windows Mobile) [18].

The Social Internet of Things (SIoT) [19] is a network of intelligent objects that have social interactions. The Social Internet of Vehicles (SIoV) [20,21] is an example of a SIoT where the objects are smart vehicles. The authors in [21] designed analytical models of the subsystems involved in the SIoV interaction process and proposed models that could be useful in order to deploy Social Internet of Vehicles (SIoV)-based safety, efficiency or comfort applications. Although the basic rules are the same for both social networks of humans and social networks of vehicles, there are significant differences in terms of the dynamic nature of the entities, their social interactions, the topology of the network, privacy concerns and security issues that arise. In this article, we will present a comprehensive review of the research and analysis of such systems.

Social Internet of Vehicles (SIoV) describes both the social interactions among vehicles [22] and among drivers [23]. As described in [23], a vehicular social network is created when a driver enters an area where other people with common interests or relevant content exist. Contrary to this, Nitti *et al*. [22] describe a vehicular social network as social interactions among cars, which communicate autonomously to look for services (automaker patches or updates) and exchange information relevant to traffic. Given that vehicles are becoming more and more autonomous [24] and that applications supporting social interactions among drivers and passengers are already being developed [25,26] we strongly believe that SIoV will eventually be a network of both drivers, passengers and cars. This new interconnection among entities on different levels (vehicles, drivers, passengers) creates new capabilities, poses new challenges and exposes the network to new threats.

New applications that are based on the social concept of vehicular networking were recently developed. For example, RoadSpeak [27] is a voice chatting system that allow commuters to dynamically enter vehicular social networks on the fly and exchange messages. NaviTweet [26] incorporates the driver's preferences into the navigator's route calculation using traffic voice tweets. Caravan Track [25] is a similar application that allows drivers to share mobility data among a cluster of cars. This application, supported by Ford, can be used to filter incoming information to suit the needs and desires of the driver. Porsche also unveiled its new concept electric car that has the ability to post updates to social media [28]. As we move to the era of the next generation of vehicles, smart vehicles with sensing, communication and sociability capabilities, more applications and technologies are going to be developed that will materialize the idea of SIoV.

This article provides an comprehensive survey of the Social Internet of Vehicles. We first review components and technologies of the SIoV in Section 2. We then discuss context awareness in Section 3. In Section 4, we present how social network analysis methods can be applied in SIoVs. Next, in Section 5, we review security and trust issues related to SIoVs. Finally, we discuss current challenges and open issues regarding driver privacy in Section 6.

2. SIoV Technologies and Components: Next Generation of Vehicles

The design, development and deployment of vehicular networks is boosted by recent advances in context-aware technology and wireless vehicular communication techniques, such as dedicated short-range communications (DSRC), Long-Term Evolution (LTE), IEEE 802.11p and Worldwide Interoperability for Microwave Access (WiMax) [29]. An increasing number of social network applications is being proposed for vehicular networks, which leads to a shift from traditional vehicular networks toward SIoV. In this section, we briefly introduce the key aspects that enable SIoV in current vehicular networks. Similar to [30], we focus on three main components: (1) next-generation vehicles; (2) vehicle context-awareness; and (3) SIoV context-aware applications.

Vehicular *ad hoc* networks (VANETs) are a kind of mobile *ad hoc* network that has been proposed to enhance traffic safety and provide comfort applications to drivers. The unique features of VANETs include fast-moving vehicles that follow pre-determined paths (*i.e.*, roads) and messages with different priority levels. For example, messages for comfort and infotainment applications have low priority, while messages for traffic safety applications require timely and reliable message delivery [31]. Using the on-board unit, vehicles can communicate among themselves (vehicle-to-vehicle, V2V) and with roadside units (vehicle-to-infrastructure, V2I). This enables several other forms of communication, such as vehicle-to-broadband cloud (V2B), where the vehicle communicates with a monitoring data centre, vehicle-to-human (V2H) to communicate with vulnerable road users, for example pedestrians or bicycles, or vehicle-to-sensor (V2S), where the vehicles communicate with sensors embedded in the environment [31].

Vegni *et al*. [32] introduced next generation vehicles as smart vehicles that represent the convergence of communications, infrastructure, computers and autonomy, resulting in new capabilities, such as sensing, navigation, sociability, context-awareness and communication. Based on these aspects, smart vehicles exhibit five features: self-driving, safety driving, social driving, electric vehicles and mobile applications.

2.1. Self-Driving

The aim of autonomous cars is to drive independently without human interaction and to navigate the roads safely to reduce traffic accidents. According to a report by KPMG [33], the use of autonomous vehicles could eliminate 90% of all vehicle accidents. The industry [34] defined six accreditation levels of autonomous driving: At Level 0 (no automation), the driver has control of all aspects of the driving, even if he or she is assisted by various intervention or warning systems. At Level 1 (driver assistance), the vehicle will be fully controlled by the driver. This might include specific warning applications, such as blind spot detection. Level 2 (partial automation) has a low level of automation, including lane detection and an assisted braking system. Level 3 (conditional automation) combines two functions for congested traffic, namely driving in a straight line and automatic speed reduction. Level 4 (high automation) allows limited self-driving, which requires the driver to maintain consistent observation of the roadway in selected environments, to cede control when required. At Level 5 (full automation), the vehicle is capable of reaching the navigated destination without human interaction.

Current mass-market technology offers features on accreditation Level 2 (partial automation). For example, the 2014 Mercedes S-Class comes with options for auto-parking, clever steering, lane keeping, automated acceleration/braking and fatigue monitoring [35]. In traffic jams, the 2014 BMW i3 can accelerate autonomously and brake up to 30 miles per hour [36]. The 2015 Audi A7 provides autonomous braking in traffic jams [37].

In the future, most technology companies and automobile manufacturers predict to offer features on higher accreditation levels. For example, Tesla expects to build a vehicle that can drive 90% of distances in fully-automated mode in 2016. In 2018, Google expects to provide fully-autonomous vehicles on the market. In 2020, Mercedes-Benz, GM, Nissan, Volvo, BMW and Audi all expect to sell fully-automated/self-driving vehicles.

2.2. Safety Driving

The aim of the safety driving feature is to reduce casualties, injures and create vision zero [38], *i.e.*, to reach the ambition of zero traffic accidents. To help achieve this goal, vehicular networks enable applications that provide a wide range of information to drivers and travellers. An example application is described in [39], where the authors propose the use of V2I communications in order to reduce the emergency services' arrival time.

2.3. Social Driving

In social driving, vehicles gather *on-the-fly*to be part of a social network that consists of neighbouring vehicles. These vehicles can share the same interests, locations, move towards the same direction/destination or be part of existing relationships. There exist smart tools that use real-time traffic information, collected by a participatory sensing approach in order to help drivers choose the best route, e.g., Waze [40], Google Live Traffic to Google Maps [41], *etc*. Uber and Lyft, two applications that were recently launched, although having raised many legal issues, also give the users the opportunity to share their cars with people that have similar destinations [42] and can be considered as different expressions of the social driving concept.

2.4. Electric Vehicles

There is high customer growth and interest in fully-electric, hybrid (gas-electric) and zero-emission vehicles. Especially in highly populated areas and low speed zones, these vehicles can contribute to the protection of the environment. Novel methods that deal with the optimal charging of electric vehicles, in static or dynamic mode, have recently been introduced. These vary from stationary stations that are scattered across the road network in central positions [43–45], dynamic wireless charging methods that take advantage of the mobility of nodes [46,47] and eco-routing algorithms that run in isolation in every vehicle or in a central way for a fleet of vehicles [48,49]. The authors in [50] present a method for dynamic wireless charging of vehicles based on the concept that vehicles meet at rendezvous points, giving a social aspect to the power transfer procedure.

2.5. Mobile Applications

The integration of network adapters, on-board units, different types of sensors and Global Positioning system (GPS) receivers enables vehicles to gather and analyse information about themselves and the surrounding environment and disseminate this information to nearby vehicles [31].

Depending on their primary purpose, VANET applications are classified into comfort applications and safety applications. Comfort or entertainment applications provide ease, high levels of comfort and tranquillity to all passengers, including the driver. This can include information of current restaurant menus, prices and discounts on highway services, nearby gas stations, shop discounts and current prices for nearby hotels. For passengers, this can also include online gaming, Internet access and social instant messaging [51]. Safety applications use dedicated short-range communications (DSRC) to improve road safety and avoid accidents or reduce their severity.

These five features will expose SIoV to a plethora of sensor data that need to be analysed, to enable vehicles to become context-aware.

In their seminal work, Alam *et al*. [20] envisioned the concept of a social network among cars as a cyber-physical layer on top of the physical vehicular network. Based on this concept, the authors proposed application scenarios that target both drivers, authorities and cars and discussed privacy issues that arise from such a system. Using this work as a basis, we elaborate in the following sections on how next generation vehicles can achieve higher levels of vehicle context-awareness. This is followed by a discussion as to how approaches to social network analysis can be applied within an SIoVs and what new security and privacy challenges arise.

3. Vehicle Context-Awareness

A key aspect in IoV is to enable vehicles to be context-aware, *i.e.*, to be aware of the circumstances that exist around the vehicle, especially those that are particularly relevant to it [52]. Context-aware systems are those that have the capability to adapt their behaviour to their current contextual environment. Context-awareness in vehicles can be provided by three main subsystems: sensing, reasoning and acting [53,54].

The sensing subsystem gathers contextual information from different sensors integrated with the vehicle's OBU. The type of these sensors differs according to the vehicle's requirements, for example location, infrared or ultrasound. In other terms, this phase represents the way context data are collected.

The reasoning subsystem processes raw data to extract high-level contextual information, such as the driver's situation. Contextual information can be either extracted from a single sensor, defining certain contextual information, or extracted from multiple sensors, defining uncertain contextual information. Detecting driver's fatigue levels is considered uncertain (high-level) contextual information.

The acting subsystem represents the application enforcer, which provides services to users or other drivers. Disseminating warning messages, in-vehicle alerts and smart assisted parking are examples of high-level applications deployed to prevent accidents and reduce road congestion.

Several context-aware systems and frameworks for the SIoV have been proposed in the literature. Hu *et al*. [55] presented s-frame, a framework for social vehicular networks formed by in-vehicle or mobile equipment used by passengers, vulnerable road users and drivers that supports high-level context-aware applications.

Alhammad *et al*. [54] designed a VANET on-street context-aware smart parking assisting system, deploying the concept of the centralized InfoStation to locate and reserve a parking slot. This reservation process is dictated by the driver's preferences. All parking zones have a dedicated InfoStation that acts as a terminal, providing wireless coverage over DSRC, as shown in Figure 1.

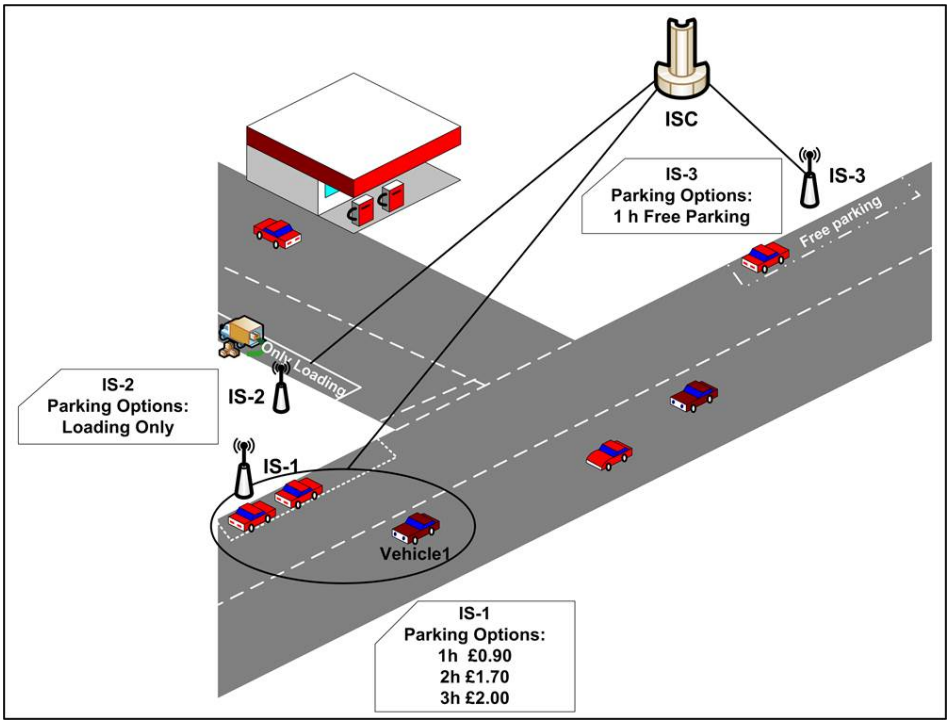

Figure 1. On-street parking system scenario.

Wan *et al*. [29] presented a cloud-based context-aware dynamic parking service that provides planning services for traffic authorities, a parking reservation service and context-aware optimization. Their framework allows drivers to park their vehicle alongside the road for short periods, provided this does not impede the traffic flow. To provide this service, the framework considers contextual information, such as time (e.g., rush hours) and road conditions (e.g., the width of a road). Traffic authorities can manage this service dynamically and effectively reduce parking problems in a smart city.

Shu *et al*. [56] designed SocialDrive to allow drivers to disseminate real-time travel information on social networks and to help them understand their own driving behaviour. SocialDrive provides contextual data to drivers to reflect the ultimate driving style, which can reduce fuel consumption by eliminating unwanted habits.

4. Social Network Analysis in SIoVs

Social network analysis (SNA) can be used to discover important players in a network and refers to the use of network theory to analyse social networks. Individual actors within the network, which can either be vehicles, drivers or even passengers, are represented by nodes, and the interactions or relationships among them are represented by edges [57]. Based on the interaction among entities of the network, which can be either static or dynamic, metrics, like centrality, cohesion, degree and clustering coefficient, can reveal relations among nodes, as well as groups of entities that share common habits.

Cunha *et al*. [58] showed that vehicles tend to show a similar behaviour and routines in terms of mobility. The mobility of vehicles can be mapped as a social network, following the same basic laws of degree distribution and distance among nodes. Applying SNA on vehicular networks can therefore improve the performance of communication protocols and services. Traditional concepts from graph theory, like centrality and clustering, can be applied in vehicular networks, as long as they incorporate their specific features, such as mobility of nodes, channel conditions and drivers' behaviour.

The centrality of nodes plays a crucial role in information spreading in a network [59,60]. In a similar way, central nodes can serve as good spreaders of infections [61] or as good points for building defence mechanisms [62]. Furthermore, central nodes can be elected as the clusterhead of groups that are created on the fly. A clusterhead may act as a relay node for traffic coming or destined to different clusters or as a relay node for intra-cluster communication [63].

4.1. Centrality of Nodes in an SIoV

Centrality metrics have been developed and used in the SNA to characterize and measure the importance of individual entities in a social network. The objective of these metrics is to find nodes that are central in a graph and can thus serve as relay nodes in terms of efficient information dissemination. Generally, a node with high centrality is more central compared to its neighbours, although it is highly affected by the network topology and the application that is used.

Betweenness centrality is a good metric for identifying nodes that can participate in the forwarding procedure of data [64], especially when used in static networks. According to betweenness centrality, a node is central to the degree that it stands between others. For example, in Figure 2, nodes A and B are the most central nodes, because they participate in the majority of shortest paths between the rest of the nodes. Betweenness centrality has been adapted for different types of networks, e.g., sensor networks, where the remaining energy of nodes influences the selection of the next hop in a forwarding chain [65], and delay-tolerant networks, where the delay that every message faces is affected by the popularity of nodes [66].

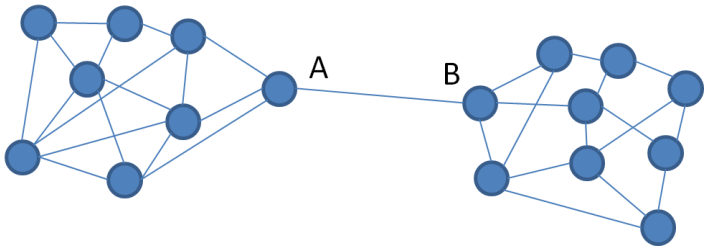

Figure 2. Betweenness centrality.

In mobile *ad hoc* networks, centrality metrics represent the significance of nodes at any time instance. Daly *et al*. [67] show an effective use of social network and centrality analysis in mobile networking. They derive a social routing algorithm from a combination of similarity and betweenness centrality. When the exact location of the destination node is unknown, the algorithm forwards messages to the nearest central node, thereby increasing the potential of selecting a suitable carrier of the information towards the destination.

Aside from betweenness centrality, there are similar metrics that combine graph theory with social characteristics. In degree centrality, central actors are the ones that have the most ties in the network graph. Closeness centrality focuses on how close one actor is to the other. The idea is that an actor is central if it can quickly interact with all others, and it is based on the geodesic distances among nodes. Smart vehicles that are equipped with GPS and communication capabilities can make use of closeness centrality to dynamically identify the central nodes that can be good candidates for forwarding important messages [68].

Maglaras *et al.* [69] proposed to rank vehicles based on the road segments that they are going to follow. They start by ranking each road segment according to how many vehicles that enter the network are going to traverse it, based on their historic data. For vehicles with no previous historic data, the shortest path in terms of distance is assumed as the preferred path. Then, each vehicle is assigned a unique ranking based on the accumulated ranking of the roads that it is going to traverse. This metric represents the significance of the node in terms of dissemination capabilities, and it ranks the importance of a node based on dynamic features, e.g., the traffic of road segments and the route of the vehicle. Following a similar approach, Bradai and Ahmed [70] rank vehicles based on the relative location to their neighbours and their potential of reaching other vehicles. Based on these characteristics and inspired by SNA, they propose a new centrality metric, called dissemination capacity. The proposed ReViVprotocol adds a rebroadcaster selection module to the existing IEEE DSRC and thereby reduces the reported delay, so that real-time streaming applications become feasible.

The role of central nodes can be played by roadside units (RSUs), which are computing devices located on the roadside that provide connectivity support to passing vehicles. RSUs can be of different kinds, for example cellular base stations or wireless access points, and can provide various kinds of communication capabilities to approaching vehicles. The optimal placement of RSUs is similar to determining the central nodes in a VANET, and it has been widely investigated both for urban [71] and highway [72] environments. Rongxing *et al*. [73] propose a novel Social-based PRivacy-preserving packet forwardING(SPRING) protocol for vehicular networks. In SPRING, the optimal locations where the RSUs must be deployed are intersections where many social interactions happen. The RSUs are used as relay nodes to assist cars in packet forwarding. Similar to this work, Huang *et al*. [74] investigate the RSU optimal placement problem, taking into account location privacy parameters. The authors in [75] present a density-based approach for roadside unit deployment in urban scenarios, where RSUs are placed according to the inverse proportion of vehicles densities, in order to reassure seamless connectivity to the Internet.

4.2. Social Clustering of Vehicles

Clustering is a method widely used in all kinds of networks, ranging from mobile *ad hoc* networks [76] to sensor networks [77]. Clustering exists in different forms and can be performed using a wide range of network characteristics, bringing significant benefits to a network. For example, clustering can alleviate the problem of an overwhelming number of broadcasts in dense networks (broadcast storm) [78], increasing the system throughput and improving the bit error rate. It can significantly decrease packet delays and provide better spectrum utilization in time and space. Clusters that partition the network cleverly can also allow data aggregation and increase network longevity. By creating small groups of nodes that share common characteristics, the network appears to be smaller and more stable. To form clusters, vehicles can combine LTE and DSRC communication capabilities, as shown in Figure 3. Cluster heads can perform special operations inside a cluster, such as regulation of channel use, aggregation of data, scheduling and packet routing.

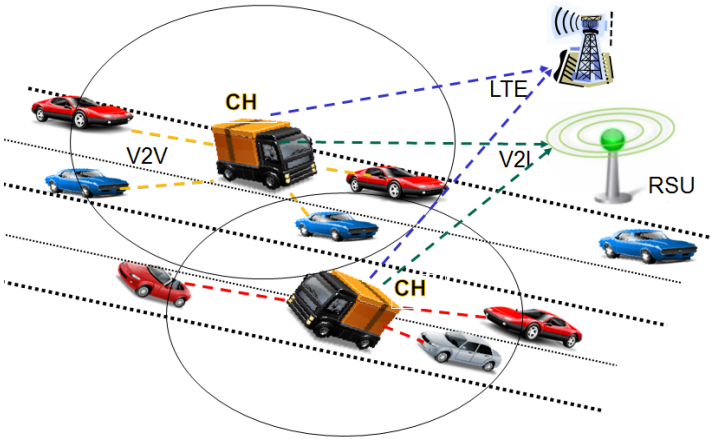

Figure 3. Clustering of vehicles.

A special characteristic of a VANET environment is diversity in the mobility patterns that vehicles follow, which is based on the road network's local condition, for example reacting to traffic congestion or accidents. This characteristic makes a VANET a very dynamic network where the vehicle density exhibits large variations. Another problem that the communication between moving vehicles has arises when the receiver and the source are moving towards different directions. The problem that is called Doppler shift has attracted much attention, and many solutions have been proposed [79]. The authors in [80] identified the key factors that affect the delivery of warning messages between vehicles, which are the radio propagation model, the density of vehicles and the roadmap. This work showcased how dynamic a VANET environment can be and how small variations in only one feature can heavily affect the performance of the network.

Having this dynamic characteristic of a VANET in mind, a good clustering method that can reassure good stability and high cluster lifetime must incorporate many different factors during both the cluster formation and cluster maintenance processes [63,81]. In addition, an effective clustering method has to take into account signal fading and channel interference. Hassanabadi *et al*. [82] presented APROVE, a protocol for distributed election of cluster heads using affinity propagation from a communications perspective. Maglaras *et al*. [81] proposed a distributed clustering algorithm, which applies virtual forces among the nodes to form stable clusters. The applied force is relative to the current and predicted future distance among each pair of vehicles and to their relative velocities. The method assigns positive virtual forces among vehicles that move towards each other and negative forces to vehicles that follow different directions. Nodes decide whether to become cluster heads, join a nearby cluster or leave their cluster depending on their current state and the relation of the total virtual forces applied to it from its neighbours. Vegni *et al*. [83] introduced a new cluster-based routing

protocol that reduces network overload, message duplication and packet collisions by allowing vehicles to selectively transmit messages.

When moving on the social aspect of vehicular communications, new parameters, like the frequency of interactions between entities, historical data of driver behaviour and driver habits, must be taken into account. As drivers tend to follow similar routes when moving in a city or on a highway, past mobility information can be used to build distinct social profiles of the drivers. These social profiles can become a basic characteristic to create social groups of vehicles and drivers. In [84], the nodes are divided into different groups based on the regularity of contact between vehicles with fixed routes. Using the social behaviour of vehicles as a basic parameter in the clustering formation procedure, the method presented in [85] manages to increase cluster stability. The social behaviour of drivers is derived from historical data that are collected from RSUs, which are deployed at critical points of the road network. To implement the proposed clustering method, the path that vehicles are likely to follow is added to every beacon message. Both methods use the routes that the vehicles follow or tend to follow as an additional parameter to form stable clusters.

A special category of clusters is platoons. Platooning describes the automated coupling of vehicles by electronic means, with the first vehicle taking control [86]. The lead vehicle decides the speed with which the platoon will move, while the remaining vehicles regulate their speed to follow automatically. The advantages of this scheme are higher security and improved use of resources. Large transport vehicles naturally have a high air resistance, which can be reduced through slipstream effects within a platoon. This saves fuel and helps to make better use of road space [87]. A platoon can consist of an arbitrary number of vehicles, and as vehicles become members of the platoon, they can also form a social network on the fly [88]. After the creation of the platoon, the leading vehicles can serve as the clusterhead and take over most of the communications between the platoon and the outer network (see Figure 4).

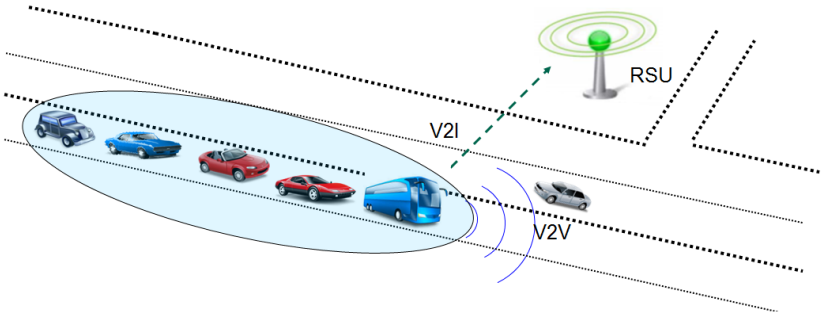

Figure 4. A platoon of vehicles.

5. SIoV Security Issues

The security of a vehicular network is a vital aspect of an SIoV, as the compromise of a vehicle can lead to life-threatening situations, as well as a general degradation of other components that use the SIoV as part of a wider smart city infrastructure. Different from a standard computer network, a vehicular network provides a large number of distributed and heterogeneous resources and computational functionalities. The connectivity between vehicles in various geographic locations makes security a more complicated issue to solve, as is the heterogeneous nature in terms of ownership, manufacturer and, indeed, users. Social vehicular network security considers social characteristics and human behaviour [30] alike. This section reviews issues of security, trust and reputation in vehicular networks with a particular focus on the social aspects.

5.1. SIoV Threats

Existing research of vehicular security threats considers them as a whole and has not highlighted the social aspects that have a direct impact on the security of the overall infrastructure. Raya reviewed the threats to vehicular networks and classified them into insider/outsider, malicious/rationale and active/passive [89]. Zeadally [90] classified them into threats to availability, threats to authenticity and threats to confidentiality. In the following, we describe the main security threats and highlight some solutions for SIoV security.

5.1.1. Denial of Service Attack

Denial of service (DoS) attacks aim to prevent legitimate users from accessing data or services in computer networks. In vehicular networks, this attack floods and jams the traffic with large volumes of irrelevant messages that negatively impact the communication between the network's nodes, on-board units and roadside units. Because the vehicle under attack is part of the wider infrastructure of the SIoV embedded in a smart city environment, there is a large number of high-powered computing facilities in close proximity to the target. An attacker can potentially use these for jamming attacks against the target's on-board sensory equipment to counter the target vehicle's ability to identify rogue messages through corroboration with its local information sources.

The problem of DoS attacks can be addressed by using a voting scheme [91]. However, voting schemes may fail if the attacker can produce false identities to disguise himself [92].

5.1.2. False Message Injection

An insider attacker can sign a false message and broadcast it to the network. The attacker can thus manipulate the traffic flow and affect the decisions of other drivers, causing damage through traffic jams or accidents.

In vehicular networks, the notion of proof-of-relevance (PoR) has been proposed to address this issue by filtering false data via authentic consensus. PoR is based on the idea that witness vehicles provide authenticated endorsements to information about an event. The event reporter can thus prove that he/she is authentically relevant to the event [93].

5.1.3. Malware

Malware, such as viruses or worms, is usually introduced through outside unit software and firmware updates. Malware can infect vehicles and even allow remote adversaries to take control of individual vehicles. Remote access Trojans, paired with the advanced communication facilities that VANETs bring to the SIoV, can gain control of the internal CAN bus and disrupt essential services. Remote attacks of this form have been widely demonstrated and have shown in dummy tests to risk the safety of drivers and passengers [94]. Other research on malware targeting vehicles has shown that the spread of malware can be achieved through vulnerabilities in the computers used to maintain and diagnose vehicles during servicing. This has wider implications than just the infection of a single vehicle, because the spread of malicious software is taking place through a trusted service platform, potentially affecting an entire product line. As this is already possible with today's technologies, the potential for malware to spread through the SIoV is even higher, for example when a vehicle's social component receives software or firmware updates from another unknown vehicle.

Existing work proposed the person authentication system [95] to ensure only the authorized user can use the vehicle. Zhang proposed a cloud-assisted vehicle malware defence framework to address the malware challenges [96]. A key challenge is the maintenance of up-to-date patches and signature files. While cloud-assisted frameworks can centralize some of these efforts and make the problem more manageable, the roll-out of automated patch management in a large-scale SIoV is a formidable challenge, given the heterogeneous nature of current vehicles. Other considerations are that the sophistication of advanced persistent threats (APT) is beyond what manufacturers and

infrastructure providers are prepared to or can afford to defend against. This means that the defence of individual vehicles will be left to individuals, which based on experience with currently-available ICT infrastructures, is open to a wide array of threats, including masquerading and social engineering attacks on the members of the SIoV.

5.1.4. Masquerading and Sybil

In a masquerading attack, a vehicle fakes its identity and pretends to be legitimate in the vehicle network. Outsiders can conduct attacks, such as injecting false messages. In a Sybil attack, the attacker generates multiple identities and pretends to be multiple legitimate vehicles concurrently. They can artificially disrupt a roadway and affect the decision making of the other drivers through smart routing systems [16]. In this attack mode, a vehicle can claim multiple locations at the same time, which can cause traffic chaos.

Sybil attacks can be detected using resource testing [97], which assumes that vehicles have limited resources. This problem can also be address by using public key cryptography [98], where vehicles are authenticated using public keys. However, these approaches are based on assumptions and have limitations in addressing Sybil attacks. Sybil attacks can be launched on the basis of a large compromised SIoV, because a bot-net that is deployed on an SIoV is difficult to defend against, as the nodes are in a constant flux of reconfiguration. Together with randomized attack patterns, this can lead to denial of service attacks against the wider smart city infrastructure through jamming of low-power sensory infrastructures or the degradation of essential monitoring services.

5.1.5. Impersonation Attack

In an impersonation attack, the attacker steals the identity of a legitimate vehicle and can then broadcast security messages on that vehicle's behalf. These messages can impact other drivers' decision making and create traffic problems.

Chhatwal has proposed an approach called building up secure connection along with key factors (BUCK) to detect and isolate the impersonation attack [99].

5.1.6. Solutions and Future Directions

Tremendous research has been done in protecting vehicular networks from being attacked. These include public key infrastructure [100], trusted architectures, such as the IEEE 1609.2 Security Framework [101], and key management and authentication schemes [102]. However, less research has been conducted in the area of social vehicular network security. With the increasing integration of smart devices and vehicles, human beings will play an important role in V2V (vehicle-to-vehicle), V2R (vehicle-to-road), V2H (vehicle-to-human) and V2S (vehicle-to-sensor) interactions. This calls for new research in two directions. First, research needs to address security issues from a social perspective, such as policy making, law enforcement or security awareness training. Second, research needs to study the interaction between human agents and technical security solutions. Experience can be borrowed from social network security [100], where social aspects are well researched.

5.2. SIoV Trust Issues

Trust has been well studied in social networks. Golbeck introduced the concept of social trust based on sociological foundations, defining trust as "a commitment to an action based on a belief that the future actions of that person will lead to a good outcome" [103]. Golbeck sees social networks as platforms to build mutual trust between entities [104]. However, trust in a social network consisting of vehicles and drivers has not been well studied. This section reviews the trust issues in the SIoV.

5.2.1. Trust Characteristics of SIoV

Trust in the SIoV exhibits five characteristics that are different from trust in traditional social settings.

Uncertainty

Trust in the SIoV is uncertain and dynamic. Because the SIoV is inherently dynamic, information can change rapidly, and trust may only be valid for a short period of time. When establishing trust, the SIoV needs to take into account three uncertainties caused by the SIoV's dynamic nature: the uncertainty of an entity's identity, the uncertainty of an interaction entity's behaviour (intentional or unintentional) and the uncertainty in observations. Existing work in social networks addressed this issue by expressing trust using a continuous variable instead of a discrete-valued variable, as the former can better capture the dynamic feature of the context [105].

Subjectivity

Trust in the SIoV is subjective. Our level of trust depends on how our own actions are affected by the context [106]. Trust decision-making thus exhibits a level of subjective probability that is difficult to predict and monitor. We face an inherent risk in vehicular networks when we make trust decisions within the SIoV. Existing work in social trust addressed this issue by proposing recommendation systems. For example, Yang proposed a recommendation system for online social networks based on Bayesian inference [107]. Users can share content ratings with their friends, allowing them to make informed decisions. This provides an opportunity to choose the option with the smallest level of perceived risk.

Intransitivity

Trust in the SIoV is not always transitive. Trust is transitive when it can be extended outside the scope of the two entities who established it [108]. However, this is not always the case. If A trusts B and B trusts C, this does not necessarily mean that A trusts C. Trust transitivity depends on the extent to which you trust the trustee and the trustee's recommendations. As with subjectivity, research in social networks has developed recommendation systems to make trust-based recommendations by allowing users to share trust ratings with peers.

Context Dependence

Trust in the SIoV is context-dependent. For example, A may trust B as a physician to perform medical checks (in the context of a medical situation), while A would not trust B to perform surgery (in the context of an accident). Similarly, different types of trust need to be established in an SIoV, depending on the given context. In social networks, Jøsang's subjective logic [109] has been widely used to model trust networks. Cerutti uses subjective logic in a decision-making approach that considers the notion of confidence. The approach determines weights associated with trust ratings and outputs a trust degree that depends on the current interaction context [110].

Non-Cooperativeness

Trust in the SIoV is not always cooperative. Trust decisions are usually made cooperatively between different entities. However, not all entities in an SIoV are cooperative. Entities may refuse to cooperate for selfish or malicious reasons. Existing work in social networks aims to separate selfish entities once they are detected and encourages altruistic behaviours with incentive mechanisms. Cho [111] researched the trade-off between selfish and altruistic behaviours in terms of a node's individual welfare, for example saving energy, and global welfare, for example achieving a goal with adequate service availability.

5.2.2. Trust and Reputation

Reputation management is part of trust management. Although the concepts of trust and reputation are often used interchangeably, they are subtly different. Trust is active and indicates whether an entity believes in the trust quality of a peer. Reputation is passive and indicates an opinion about an entity. A reputation system is further classified as positive reputation and negative reputation. Positive entity behaviour is recorded in positive reputation systems, and negative entity behaviour is recorded in negative reputation systems [105]. The authors in [112] present a cooperative neighbour position verification mechanism based on V2V communications among vehicles; it can mitigate the impact of adversary users by excluding malicious nodes from the packet routing mechanism. The aim of the reputation system in the SIoV is to establish trust values for each entity in the SIoV, providing information for other entities to make trust-based decisions. It provides information on whether a peer is trustworthy or not, encourages peers to participate in a trustworthy way and isolates untrustworthy peers from acting in the process. Experience can be borrowed from reputation and trust management in social networks to support trust-based decision-making in the SIoV [113].

Another aspect of the use of trust and reputation within a SIoV is related to the length of interactions between peers in the network. Most work on trust assumes that peers build and establish trust through a number of interactions and that trust can be verified eventually to influence future interactions or recommendations for that peer. While these assumptions hold in the context of electronic transactions and service provisions, they are more difficult to assess in the highly dynamic, reactive environment of the SIoV. In addition, many reputation-based systems rely on the predictability, rationality and repetition of behaviours. In a targeted cyber-attack scenario, these assumptions do not necessarily hold, especially if a malware's spread affects a large number of vehicles in a platoon.

In sum, trust is a multidimensional concept. Trust-based management and decision making in SIoV faces big challenges. Trust establishment needs to address the trust characteristics of the SIoV. Future work should also focus on how to adapt the trust decision frameworks, models and systems in social networks to address similar issues in the SIoV.

6. SIoV Privacy Issues

The SIoV enables social interactions among vehicles and drivers and thus incorporates features of both vehicular networks and social networks. Both types of networks raise important privacy issues that need to be considered in the context of the SIoV. In this section, we review these privacy issues, discuss privacy-enhancing technologies for the SIoV and highlight research questions that need to be addressed to make SIoVs viable.

6.1. Privacy in Vehicular Networks

The main privacy issue in vehicular networks is location privacy [114]. Vehicles in a vehicular network broadcast unencrypted messages that contain a vehicle identifier along with the vehicle's location, speed and heading. In many cases, these data can be linked to the driver's identity. Using these data, a system that is ultimately designed to offer safety and comfort applications to drivers can be abused by third parties, such as employers, insurance companies or criminal organizations to track individuals [115]. This tracking can reveal sensitive locations, such as home or work locations, along with the time and duration of each visit [116], effectively allowing one to infer the detailed behavioural profiles of drivers.

It is important to note that the location privacy requirements of participants in vehicular networks can conflict with authentication requirements. Because messages in vehicular networks can contain information about safety-critical events, recipients of messages need to make sure that messages have been sent by a trustworthy source before acting on them [117]. If this is realized

by strong authentication of message senders, the vehicular network cannot provide privacy at the same time.

Therefore, privacy-preserving solutions for vehicular networks often rely on pseudonyms. A pseudonym takes the place of a vehicle identifier, and it should not be possible to link pseudonyms to the real identifier. Because it can be desirable to allow authorities to find the real origin of a message, for example when misbehaviour has been detected, cryptographic schemes have been designed to provide privacy against ordinary participants, but allow authorities to revoke privacy [118]. To protect against tracking attacks, pseudonyms need to be exchanged frequently, and it is important to ensure that successive pseudonyms cannot be linked to each other [119]. Methods to achieve this unlinkability of pseudonyms include mix zones [120] and silent periods [121]. Recently, a new method that guarantees anonymity while at the same time spotting and revoking malicious users of a VANET is introduced [122].

6.2. Privacy in Social Networks

Privacy issues in social networks include identity theft, stalking, the possibility to create digital dossiers about participants and inadvertent publication of information that was intended to remain private [123]. This is exacerbated by the fact that many social networks have overly complex privacy policies and do not promote available privacy controls to users [124]. In addition, even when users choose to keep most of their information private, several attacks have shown that it is possible to infer sensitive attributes despite restrictive privacy settings [125,126]. This is made worse by the fact that information about a user is often revealed by the user's friends and family, resulting in a situation of interdependent privacy, *i.e.*, where a user's privacy depends on other people [127].

Privacy towards the provider of a social network can be achieved by encrypting all information that a user posts to the social network. Several approaches have been proposed that add encryption to existing social networks without requiring the consent or participation of the provider and without affecting the usability of the social network [128–130].

Another privacy concern in social networks is link privacy, *i.e.*, the privacy of relationships between users. Link privacy aims to hide the type and existence of social relationships. This is important because it is possible to re-identify anonymous users in a social network graph [131] and to infer global relationship information by subverting a limited number of user accounts [132]. Mitigation strategies against attacks on link privacy aim to make attacks more expensive and rely on the network provider to implement them [133].

6.3. Privacy-Enhancing Technologies for the SIoV

Combining privacy issues from social networks and vehicular networks, it is easy to see some of the privacy issues that will affect the SIoV. In particular, we envision three risks. First, the privacy threats against social and vehicular networks will become accessible to a wider range of adversaries. For example, it will be possible to eavesdrop on information about social networks via wireless vehicular transmissions, and it will be possible to find location information via online social networks. Second, the information available today will be augmented in two directions: social network profiles will be combined with ubiquitous geo-tagging, and vehicular network messages will be combined with information about a driver's preferences and behaviour. This will allow the inference of much more detailed driver profiles, which can be exploited for marketing or surveillance. Third, it is unclear how privacy policies can be effectively conveyed to a driver in a vehicle and how privacy controls may be offered to drivers. This may lead to even more inaccessible privacy policies and less accessible privacy controls than with today's social networks [124].

To counter these risks, privacy-enhancing technologies for the SIoV are needed. To date, there are very few approaches in the literature that specifically target SIoVs. Most notably, the proposed SIoV architecture in [20] attempts to address privacy issues. However, their approach has three weaknesses. First, their approach relies on cloud storage, which means that the privacy

issues associated with cloud computing apply, for example data privacy both towards the cloud provider and the provider's other customers [134]. Second, the privacy protection proposed in their architecture consists of tagging all messages with a privacy value (public, private and protected). This policy-based protection depends on whether the recipient of a message honours the transmitted privacy value and is ineffective against most adversaries. Third and most importantly, it does not include technical privacy protections, such as cryptographic means.

Future privacy-enhancing technologies for SIoVs should be based on proven privacy-enhancing technologies for social networks and vehicular networks. New privacy-enhancing technologies and those resulting from combinations of existing technologies need to be evaluated thoroughly to make sure that they provide an adequate amount of privacy. Because the SIoV is a combination of social and vehicular networks, evaluations need to use a selection of privacy metrics from both domains [135,136].

7. Conclusions

In this article, we surveyed the key concepts of the Social Internet of Vehicles (SIoV), a new type of network that enables social interactions between vehicles, drivers and passengers in the Internet of Vehicles. More specifically, we reviewed enabling technologies and key components of the SIoV and presented context-aware SIoV applications that can be deployed in a smart city. Three main components were introduced that include next-generation vehicles, vehicle context-awareness and SIoV context-awareness applications. Context-aware systems allow vehicles to adapt their behaviour as per the contextual information gathered from different subsystems, such as sensing, reasoning and acting. Several context-aware frameworks are available that support high-level context-aware applications design. Future work should enhance the context-aware systems by adapting existing frameworks and incorporating context-aware applications from different vendors.

We also identified the types of interactions that can happen between vehicles, drivers and passengers and discussed how social network analysis methods can be used to improve the operation of an SIoV. Using historical data of drivers, vehicles that are moving in a road network can be ranked in terms of their social behaviour. Ranking of vehicles can be used in order to perform efficient message dissemination by selecting the nodes that follow populated roads, so as to alleviate the broadcast storm problem. In order to cope with the interference caused by flooding of messages, clustering of vehicles can also be used, where the social characteristics of the drivers can help in the creation of more stable and robust clustering formations. Combined communication capabilities along with social behaviour of the vehicles can facilitate eco-routing and dynamic charging of electric vehicles. Established social metrics, like degree or betweenness centrality, finally, can be modified in order to cope with the dynamic environment of a vehicular network and provide efficient tools for facilitating the communication among the nodes. Future work should focus on the development of new social metrics that can be dynamic and also able to rank in an efficient manner different entities that co-exist in an SIoV; smart vehicles, passengers, road users and drivers.

Finally, we discussed the issues of security, trust and privacy that SIoVs faces and highlighted how existing security solutions can be applied to these highly dynamic networks. Current security solutions place an imbalanced focus on technical aspects over social aspects. However, with the integration of smart devices and vehicles, the human aspect has become vital. Future research should address the social perspective of security and the interaction between human agents and technical solutions. Trust has been well studied in social networks, but less work can be found in the SIoV. Trust in the SIoV has demonstrated five different characteristics, which are uncertainty, subjectivity, intransitivity, context dependency and non-cooperativeness. Future work should focus on the adaption of the trust decision frameworks, models and systems in social networks, addressing the trust characteristics of the SIoV. Future privacy-enhancing technology in SIoV should be based on existing work for both social networks and vehicular networks. Privacy metrics from both domains need to be considered in order to thoroughly evaluate the upcoming SIoV privacy technologies.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Caragliu, A.; Del Bo, C.; Nijkamp, P. Smart cities in Europe. *J. Urban Technol.* **2011**, *18*, 65–82.
2. Ishida, T.; Isbister, K. *Digital Cities: Technologies, Experiences, and Future Perspectives*; Number 1765; Springer Science & Business Media: Berlin, Germany, 2000.
3. Xiong, Z.; Sheng, H.; Rong, W.; Cooper, D.E. Intelligent transportation systems for smart cities: A progress review. *Sci. China Inf. Sci.* **2012**, *55*, 2908–2914.
4. Bowerman, B.; Braverman, J.; Taylor, J.; Todosow, H.; von Wimmersperg, U. The vision of a smart city. In Proceedings of the 2nd International Life Extension Technology Workshop, Paris, France, 28 September 2000; Volume 28.
5. Su, K.; Li, J.; Fu, H. Smart city and the applications. In Proceedings of the 2011 International Conference on Electronics, Communications and Control (ICECC), Zhejiang, China, 9–11 September 2011; pp. 1028–1031.
6. Hollands, R.G. Will the real smart city please stand up? Intelligent, progressive or entrepreneurial? *City* **2008**, *12*, 303–320.
7. El-Hoiydi, A.; Decotignie, J.D. WiseMAC: An ultra low power MAC protocol for the downlink of infrastructure wireless sensor networks. In Proceedings of the Ninth International Symposium on Computers and Communications (ISCC 2004), Alexandria, Egypt, 28 June–1 July 2004; Volume 1, pp. 244–251.
8. Perkins, C.E. *Ad Hoc Networking*; Addison-Wesley Professional; Addison-Wesley: Boston, MA, USA, 2008.
9. Caballero-Gil, P.; Caballero-Gil, C.; Molina-Gil, J. How to build vehicular ad-hoc networks on smartphones. *J. Syst. Architect.* **2013**, *59*, 996–1004.
10. Liu, B.; Liu, Z.; Towsley, D. On the capacity of hybrid wireless networks. In Proceedings of the Twenty-Second Annual Joint Conference of the IEEE Computer and Communications on IEEE Societies (INFOCOM 2003), San Francisco, CA, USA, 30 March–3 April 2003; Volume 2, pp. 1543–1552.
11. Wang, M.; Shan, H.; Lu, R.; Zhang, R.; Shen, X.; Bai, F. Real-time path planning based on hybrid-VANET-enhanced transportation system. *IEEE Trans. Veh. Technol.* **2014**, *64*, 1664–1678.
12. Tornell, S.M.; Patra, S.; Calafate, C.T.; Cano, J.C.; Manzoni, P. GRCBox: Extending smartphone connectivity in vehicular networks. *Int. J. Distrib. Sens. Netw.* **2015**, *2015*, 478064.
13. Marquez-Barja, J.M.; Ahmadi, H.; Tornell, S.M.; Calafate, C.; Cano, J.; Manzoni, P.; Da Silva, L. Breaking the vehicular wireless communications barriers: Vertical handover techniques for heterogeneous networks. *IEEE Trans. Veh. Technol.* **2014**, *64*, 5878–5890.
14. Gubbi, J.; Buyya, R.; Marusic, S.; Palaniswami, M. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Gener. Comput. Syst.* **2013**, *29*, 1645–1660.
15. Joerer, S.; Bloessl, B.; Huber, M.; Jamalipour, A.; Dressler, F. Demo: Simulating the impact of communication performance on road traffic safety at intersections. In Proceedings of the 20th Annual International Conference on Mobile Computing and Networking, Maui, HI, USA, 7–11 September 2014; pp. 287–290.
16. Maglaras, L.A.; Basaras, P.; Katsaros, D. Exploiting vehicular communications for reducing CO_2 emissions in urban environments. In Proceedings of the 2013 International Conference on Connected Vehicles and Expo (ICCVE), Las Vegas, NV, USA, 2–6 December 2013; pp. 32–37.
17. Cheng, H.T.; Shan, H.; Zhuang, W. Infotainment and road safety service support in vehicular networking: From a communication perspective. *Mech. Syst. Signal Process.* **2011**, *25*, 2020–2038.
18. Gruyer, D.; Belaroussi, R.; Revilloud, M. Accurate lateral positioning from map data and road marking detection. *Expert Syst. Appl.* **2016**, *43*, 1–8.
19. Atzori, L.; Iera, A.; Morabito, G.; Nitti, M. The Social Internet of Things (SIoT)—When social networks meet the internet of things: Concept, architecture and network characterization. *Comput. Netw.* **2012**, *56*, 3594–3608.
20. Alam, K.; Saini, M.; El Saddik, A. Toward social internet of vehicles: Concept, architecture, and applications. *IEEE Access* **2015**, *3*, 343–357.
21. Alam, K.M.; Saini, M.; Saddik, A.E. Workload model based dynamic adaptation of social internet of vehicles. *Sensors* **2015**, *15*, 23262–23285.

22. Nitti, M.; Girau, R.; Floris, A.; Atzori, L. On adding the social dimension to the internet of vehicles: Friendship and middleware. In Proceedings of the 2014 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), Odessa, Ukraine, 27–30 May 2014; pp. 134–138.
23. Luan, T.; Lu, R.; Shen, X.; Bai, F. Social on the road: Enabling secure and efficient social networking on highways. *IEEE Wirel. Commun.* **2015**, *22*, 44–51.
24. Schwarz, C.; Thomas, G.; Nelson, K.; McCrary, M.; Sclarmann, N.; Powell, M. *Towards Autonomous Vehicles*; Technical Report 25-1121-0003-117; Mid-America Transportation Center, Lincoln, NE, USA, 2013.
25. Squatriglia, C. Ford's Tweeting Car Embarks on American Journey 2.0. Wired. 2010. Available online: http://www.wired.com/2010/05/ford-american-journey/ (accessed on 15 January 2016).
26. Sha, W.; Kwak, D.; Nath, B.; Iftode, L. Social vehicle navigation: Integrating shared driving experience into vehicle navigation. In Proceedings of the 14th Workshop on Mobile Computing Systems and Applications, Jekyll Island, GA, USA, 26–27 February 2013.
27. Smaldone, S.; Han, L.; Shankar, P.; Iftode, L. RoadSpeak: Enabling voice chat on roadways using vehicular social networks. In Proceedings of the 1st Workshop on Social Network Systems, Glasgow, UK, 1 April 2008; pp. 43–48.
28. Leggett, T. Porsche Concept Challenges Tesla and Posts to Social Media. Available online: http://www.bbc.co.uk/news/technology-34263592 (accessed on 15 January 2016).
29. Wan, J.; Zhang, D.; Zhao, S.; Yang, L.; Lloret, J. Context-aware vehicular cyber-physical systems with cloud support: Architecture, challenges, and solutions. *IEEE Commun. Mag.* **2014**, *52*, 106–113.
30. Vegni, A.; Loscri, V. A Survey on Vehicular Social Networks. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 2397–2419.
31. Al-Sultan, S.; Al-Doori, M.M.; Al-Bayatti, A.H.; Zedan, H. A comprehensive survey on vehicular ad hoc network. *J. Netw. Comput. Appl.* **2014**, *37*, 380–392.
32. Vegni, A.M.; Biagi, M.; Cusani, R. *Smart Vehicles, Technologies and Main Applications in Vehicular Ad Hoc Networks*; INTECH Open Access Publisher: Rijeka, Croatia, 2013.
33. Silberg, G.; Wallace, R. *Self-Driving Cars: The Next Revolution*; Technical Report; KPMG: Amstelveen, The Netherlands, 2012.
34. SAE On-Road Automated Vehicle Standards Committee. *Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems*; Technical Report J3016_201401; SAE: Hong Kong, China, 2014.
35. Mercedes-Benz UK Ltd. Saloon—Specs, Prices & Offers. Available online: http://www2.mercedes-benz.co.uk/content/unitedkingdom/mpc/mpc_unitedkingdom_website/en/home _mpc/passengercars /home/new_cars/models/s-class/_w222.flash.html (accessed on 15 January 2016).
36. BMW of North America. BMW I Overview—BMW North America. Available online: http://www.bmwusa.com/bmw/BMWi (accessed on 15 January 2016).
37. Audi of America. Audi Innovation: Performance for the Driver. Available online: http://www.audiusa.com/technology (accessed on 15 January 2016).
38. Ding, Z. The enlightenment of vision zero to China's road safety management. In Proceedings of the 2010 WASE International Conference on Information Engineering (ICIE), Beidaihe, China, 14–15 August 2010; Volume 3, pp. 352–355.
39. Barrachina, J.; Garrido, P.; Fogue, M.; Martinez, F.J.; Cano, J.C.; Calafate, C.T.; Manzoni, P. Reducing emergency services arrival time by using vehicular communications and Evolution Strategies. *Expert Syst. Appl.* **2014**, *41*, 1206–1217.
40. Waze. Real-time maps and traffic information based on the wisdom of the crowd. Available online: http://solsie.com/2009/09/real-time-maps-and-traffic-information-based-on-the-wisdom-of-the-crowd/ (accessed on 15 January 2016).
41. Arrington, M. *Google Redefines GPS Navigation Landscape: Google Maps Navigation for Android 2.0*; TechCrunch: San Francisco, CA, USA, 2009.
42. Portland makes Uber and Lyft legal—For now. Available online: http://www.oregonherald.com/oregon/localnews.cfm?id=8910 (accessed on 15 January 2016).
43. Machiels, N.; Leemput, N.; Geth, F.; van Roy, J.; Buscher, J.; Driesen, J. Design criteria for electric vehicle fast charge infrastructure based on flemish mobility behaviour. *IEEE Trans. Smart Grid* **2014**, *5*, 320–327.

44. Putrus, G.; Suwanapingkarl, P.; Johnston, D.; Bentley, E.; Narayana, M. Impact of electric vehicles on power distribution networks. In Proceedings of the IEEE Vehicle Power and Propulsion Conference (VPPC '09), Dearborn, MI, USA, 7–10 September 2009; pp. 827–831.
45. Ruiz, M.A.; Abdallah, F.A.; Gagnaire, M.; Lascaux, Y. Telewatt: An innovative electric vehicle charging infrastructure over public lighting systems. In Proceedings of the 2013 International Conference on Connected Vehicles and Expo (ICCVE), Las Vegas, NV, USA, 2–6 December 2013; pp. 741–746.
46. Jung, G.; Song, B.; Shin, S.; Lee, S.; Shin, J.; Kim, Y.; Lee, C.; Jung, S. Wireless charging system for On-Line Electric Bus (OLEB) with series-connected road-embedded segment. In Proceedings of the 2013 12th International Conference on Environment and Electrical Engineering (EEEIC), Wroclaw, Poland, 5–8 May 2013; pp. 485–488.
47. Maglaras, L.; Topalis, F.V.; Maglaras, A.L. Cooperative approaches for dymanic wireless charging of Electric Vehicles in a smart city. In Proceedings of the 2014 IEEE International Energy Conference (ENERGYCON), Cavtat, Croatia, 13–16 May 2014; pp. 1365–1369.
48. Boriboonsomsin, K.; Barth, M.J.; Zhu, W.; Vu, A. Eco-routing navigation system based on multisource historical and real-time traffic information. *IEEE Trans. Intell. Transp. Syst.* **2012**, *13*, 1694–1704.
49. Liu, Z.; Zhang, W.; Ji, X.; Li, K. Optimal planning of charging station for electric vehicle based on particle swarm optimization. In Proceedings of the 2012 IEEE Innovative Smart Grid Technologies—Asia (ISGT Asia), Tianjin, China, 21–24 May 2012; pp. 1–5.
50. Dutta, P. Coordinating rendezvous points for inductive power transfer between electric vehicles to increase effective driving distance. In Proceedings of the 2013 International Conference on Connected Vehicles and Expo (ICCVE), Las Vegas, NV, USA, 2–6 December 2013; pp. 649–653.
51. Jakubiak, J.; Koucheryavy, Y. State of the art and research challenges for VANETs. In Proceedings of the 2008 5th IEEE Consumer Communications and Networking Conference; Las Vegas, NV, USA, 10–12 January 2008.
52. Eskandarian, A. *Handbook of Intelligent Vehicles*; Springer: London, UK, 2012.
53. Wang, Z.; Lu, J. The design and implementation of client about vehicle context-aware system based on Ubiquitous Network. In Proceedings of the 2013 IEEE 4th International Conference on Electronics Information and Emergency Communication (ICEIEC), Beijing, China, 15–17 November 2013; pp. 325–328.
54. Alhammad, A.; Siewe, F.; Al-Bayatti, A. An InfoStation-based context-aware on-street parking system. In Proceedings of the 2012 International Conference on Computer Systems and Industrial Informatics (ICCSII), Sharjah, UAE, 18–20 December 2012; pp. 1–6.
55. Hu, X.; Zhao, J.; Seet, B.C.; Leung, V.; Chu, T.; Chan, H. S-Aframe: Agent-Based Multilayer Framework With Context-Aware Semantic Service for Vehicular Social Networks. *IEEE Trans. Emerg. Top. Comput.* **2015**, *3*, 44–63.
56. Shu, W.; Zhang, G.; Wu, M.Y.; Lu, J.L. A social-network-enabled green transportation system. In Proceedings of the 2013 International Conference on Connected Vehicles and Expo (ICCVE), Las Vegas, NV, USA, 2–6 December 2013; pp. 425–430.
57. Scott, J. *Social Network Analysis*; Sage Publications Ltd: Thousand Oaks, CA, USA, 2012.
58. Cunha, F.; Carneiro Vianna, A.; Mini, R.; Loureiro, A. How effective is to look at a vehicular network under a social perception? In Proceedings of the 2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Lyon, France, 7–9 October 2013; pp. 154–159.
59. Basaras, P.; Katsaros, D.; Tassiulas, L. Detecting influential spreaders in complex, dynamic networks. *Computer* **2013**, *46*, 24–29.
60. Borge-Holthoefer, J.; Rivero, A.; Moreno, Y. Locating privileged spreaders on an online social network. *Phys. Rev. E* **2011**, *85*, doi:10.1103/PhysRevE.85.066123.
61. Canright, G.S.; Engø-Monsen, K. Spreading on networks: A topographic view. *Complexus* **2006**, *3*, 131–146.
62. Noel, S.; Jajodia, S. Optimal IDS sensor placement and alert prioritization using attack graphs. *J. Netw. Syst. Manag.* **2008**, *16*, 259–275.
63. Souza, E.; Nikolaidis, I.; Gburzynski, P. A new aggregate local mobility (ALM) clustering algorithm for VANETs. In Proceedings of the 2010 IEEE International Conference on Communications (ICC), Cape Town, South Africa, 23–27 May 2010; pp. 1–5.
64. Bavelas, A. A mathematical model for group structures. *Hum. Organ.* **1948**, *7*, 16–30.

65. Cuzzocrea, A.; Papadimitriou, A.; Katsaros, D.; Manolopoulos, Y. Edge betweenness centrality: A novel algorithm for QoS-based topology control over wireless sensor networks. *J. Netw. Comput. Appl.* **2012**, *35*, 1210–1217.
66. Bali, R.S.; Kumar, N.; Rodrigues, J.J. Clustering in vehicular ad hoc networks: Taxonomy, challenges and solutions. *Veh. Commun.* **2014**, *1*, 134–152.
67. Daly, E.M.; Haahr, M. Social network analysis for routing in disconnected delay-tolerant manets. In Proceedings of the 8th ACM International Symposium on Mobile ad Hoc Networking and Computing, Montreal, QC, Canada, 9–14 September 2007; pp. 32–40.
68. Loulloudes, N.; Pallis, G.; Dikaiakos, M.D. *The Dynamics of Vehicular Networks in Urban Environments*; arXiv preprint arXiv:1007.4106; Cornell University: Ithaca, NY, USA, 2010.
69. Maglaras, L.A.; Stathakidis, E.; Jiang, J. Social aspect of vehicular communications. *EAI Trans. Cloud Syst.* **2015**, *1*, 1–10.
70. Bradai, A.; Ahmed, T. ReViV: Selective rebroadcast mechanism for video streaming over VANET. In Proceedings of the 2014 IEEE 79th Vehicular Technology Conference (VTC Spring), Seoul, Korea, 18–21 May 2014; pp. 1–6.
71. Aslam, B.; Amjad, F.; Zou, C.C. Optimal roadside units placement in urban areas for vehicular networks. In Proceedings of the 2012 IEEE Symposium on Computers and Communications (ISCC), Cappadocia, Turkey, 1–4 July 2012; pp. 000423–000429.
72. Rashidi, M.; Batros, I.; Madsen, T.K.; Riaz, M.T.; Paulin, T. Placement of Road Side Units for floating car data collection in highway scenario. In Proceedings of the 2012 4th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), St. Petersburg, Russia, 3–5 October 2012; pp. 114–118.
73. Lu, R.; Lin, X.; Shen, X. SPRING: A social-based privacy-preserving packet forwarding protocol for vehicular delay tolerant networks. In Proceedings of the 2010 IEEE INFOCOM, San Diego, CA, USA, 14–19 March 2010; pp. 1–9.
74. Huang, X.; Kang, J.; Yu, R. Optimal roadside unit placement with location privacy enhancement in vehicular social network. In Proceedings of the 2015 5th International Conference on Information Science and Technology (ICIST), Changsha, China, 24–26 April 2015; pp. 254–259.
75. Barrachina, J.; Garrido, P.; Fogue, M.; Martinez, F.J.; Cano, J.C.; Calafate, C.T.; Manzoni, P. D-RSU: A density-based approach for road side unit deployment in urban scenarios. In Proceedings of the 2012 IEEE Intelligent Vehicles Symposium, Madrid, Spain, 3–7 June 2012; pp. 1–6.
76. Yu, J.Y.; Chong, P.H.J. A survey of clustering schemes for mobile ad hoc networks. *IEEE Commun. Surv. Tutor.* **2005**, *7*, 32–48.
77. Younis, O.; Krunz, M.; Ramasubramanian, S. Node clustering in wireless sensor networks: Recent developments and deployment challenges. *IEEE Netw.* **2006**, *20*, 20–25.
78. Tseng, Y.C.; Ni, S.Y.; Chen, Y.S.; Sheu, J.P. The broadcast storm problem in a mobile ad hoc network. *Wirel. Netw.* **2002**, *8*, 153–167.
79. Nyongesa, F.; Djouani, K.; Olwal, T.; Hamam, Y. Doppler Shift Compensation Schemes in VANETs. *Mob. Inf. Syst.* **2015**, *2015*, 438159.
80. Fogue, M.; Garrido, P.; Martinez, F.J.; Cano, J.C.; Calafate, C.T.; Manzoni, P. Identifying the key factors affecting warning message dissemination in VANET real urban scenarios. *Sensors* **2013**, *13*, 5220–5250.
81. Maglaras, L.; Katsaros, D. Distributed clustering in vehicular networks. In Proceedings of the 2012 IEEE 8th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Barcelona, Spain, 8–10 October 2012; pp. 593–599.
82. Hassanabadi, B.; Shea, C.; Zhang, L.; Valaee, S. Clustering in vehicular ad hoc networks using affinity propagation. *Ad Hoc Netw.* **2014**, *13*, 535–548.
83. Vegni, A.M.; Stramacci, A.; Natalizio, E. Opportunistic clusters selection in a reliable enhanced broadcast protocol for vehicular ad hoc networks. In Proceedings of the 2013 10th Annual Conference on Wireless On-demand Network Systems and Services (WONS), Banff, AB, Canada, 18–20 March 2013; pp. 95–97.
84. Shi, J.; Wang, X.; Huang, M. Social-Based Routing for Vehicular Ad Hoc Networks in Fixed-Route Transportation Scenarios. In *Wireless Communications, Networking and Applications*; Springer: Berlin, Germany, 2016; pp. 681–691.

85. Maglaras, L.; Katsaros, D. Social clustering of vehicles based on semi-Markov processes. *IEEE Trans. Veh. Technol.* **2015**, *65*, 318–332.
86. Jia, D.; Lu, K.; Wang, J.; Zhang, X.; Shen, X. A Survey on platoon-based vehicular cyber-physical systems. *IEEE Commun. Surv. Tutor.* **2015**, *18*, doi:10.1109/COMST.2015.2410831.
87. Van Arem, B.; van Driel, C.J.; Visser, R. The impact of cooperative adaptive cruise control on traffic-flow characteristics. *IEEE Trans. Intell. Transp. Syst.* **2006**, *7*, 429–436.
88. Mohaien, A.; Kune, D.F.; Vasserman, E.Y.; Kim, M.; Kim, Y. Secure encounter-based mobile social networks: Requirements, designs, and tradeoffs. *IEEE Trans. Dependable Secur. Comput.* **2013**, *10*, 380–393.
89. Raya, M.; Hubaux, J.P. The security of vehicular ad hoc networks. In Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks, Alexandria, VA, USA, 7 November 2005; pp. 11–21.
90. Zeadally, S.; Hunt, R.; Chen, Y.S.; Irwin, A.; Hassan, A. Vehicular ad hoc networks (VANETS): Status, results, and challenges. *Telecommun. Syst.* **2012**, *50*, 217–241.
91. Malla, A.M.; Sahu, R.K. Security attacks with an effective solution for DOS attacks in VANET. *Int. J. Comput. Appl.* **2013**, *66*, 45–49.
92. Lesser, V.; Ortiz, C.L., Jr.; Tambe, M. *Distributed Sensor Networks: A Multiagent Perspective*; Springer Science & Business Media: Berlin, Germany, 2012; Volume 9.
93. Cao, Z.; Kong, J.; Gerla, M.; Chen, Z.; Hu, J. Filtering false data via authentic consensus in vehicle ad hoc networks. *Int. J. Auton. Adapt. Commun. Syst.* **2010**, *3*, 217–235.
94. Koscher, K.; Czeskis, A.; Roesner, F.; Patel, S.; Kohno, T.; Checkoway, S.; McCoy, D.; Kantor, B.; Anderson, D.; Shacham, H.; *et al.* Experimental security analysis of a modern automobile. In Proceedings of the 2010 IEEE Symposium on Security and Privacy (SP), Oakland, CA, USA, 16–19 May 2010; pp. 447–462.
95. Krishna, A.S.; Hussain, S.A. Smart vehicle security and defending against collaborative attacks by malware. *Int. J. Embed. Softw. Comput.* **2015**, doi:10.4010/2015.444.
96. Zhang, T.; Antunes, H.; Aggarwal, S. Defending connected vehicles against malware: Challenges and a solution framework. *IEEE Internet Things J.* **2014**, *1*, 10–21.
97. Newsome, J.; Shi, E.; Song, D.; Perrig, A. The sybil attack in sensor networks: Analysis & defences. In Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks, Berkeley, CA, USA, 26–27 April 2004; pp. 259–268.
98. Raya, M.; Papadimitratos, P.; Hubaux, J.P. Securing vehicular communications. *IEEE Wirel. Commun.* **2006**, *13*, 8–15.
99. Chhatwal, S.S.; Sharma, M. Detection of impersonation attack in VANETs using BUCK Filter and VANET Content Fragile Watermarking (VCFW). In Proceedings of the 2015 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 8–10 January 2015; pp. 1–5.
100. Kumar, N.; Iqbal, R.; Misra, S.; Rodrigues, J.J. An intelligent approach for building a secure decentralized public key infrastructure in VANET. *J. Comput. Syst. Sci.* **2015**, *81*, 1042–1058.
101. Schweppe, H.; Weyl, B.; Roudier, Y.; Idrees, M.S.; Gendrullis, T.; Wolf, M.; Serme, G.; de Oliveira, S.A.; Grall, H.; Sudholt, M.; *et al*. Securing car2X applications with effective hardware software codesign for vehicular on-board networks. In Proceedings of the 27th Joint VDI/VW Automotive Security Conference, Berlin, Germany, 11–12 October 2011.
102. Lu, R.; Lin, X.; Liang, X.; Shen, X. A dynamic privacy-preserving key management scheme for location-based services in vanets. *IEEE Trans. Intell. Transp. Syst.* **2012**, *13*, 127–139.
103. Golbeck, J. Computing with trust: Definition, properties, and algorithms. In Proceedings of the 2006 Securecomm and Workshops, Baltimore, MD, USA, 28 August–1 September 2006; pp. 1–7.
104. Golbeck, J. *Computing with Social Trust*; Springer Science & Business Media: Berlin, Germany, 2008.
105. Adams, W.J.; Hadjichristofi, G.C.; Davis, N.J., IV. Calculating a node's reputation in a mobile ad hoc network. In Proceedings of the 24th IEEE International Performance, Computing, and Communications Conference, Phoenix, AZ, USA, 7–9 April 2005; pp. 303–307.
106. Gupta, S. A General Context-dependent Trust Model for Controlling Access to Resources. Ph.D. Thesis, Jadavpur University, Kolkata, India, 2012.
107. Yang, X.; Guo, Y.; Liu, Y. Bayesian-inference-based recommendation in online social networks. *IEEE Trans. Parallel Distrib. Syst.* **2013**, *24*, 642–651.

108. Sherchan, W.; Nepal, S.; Paris, C. A survey of trust in social networks. *ACM Comput. Surv.* **2013**, *45*, doi:10.1145/2501654.2501661.
109. Jøsang, A.; Hayward, R.; Pope, S. Trust Network Analysis with Subjective Logic. In Proceedings of the 29th Australasian Computer Science Conference, Hobart, Australia, 16–19 January 2006; Volume 48, pp. 85–94.
110. Cerutti, F.; Toniolo, A.; Oren, N.; Norman, T.J. *Context-Dependent Trust Decisions with Subjective Logic*; arXiv preprint arXiv:1309.4994; Cornell University: Ithaca, NY, USA, 2013.
111. Cho, J.H.; Chen, R. On the tradeoff between altruism and selfishness in MANET trust management. *Ad Hoc Netw.* **2013**, *11*, 2217–2234.
112. Fogue, M.; Martinez, F.; Garrido, P.; Fiore, M.; Chiasserini, C.F.; Casetti, C.; Cano, J.; Calafate, C.; Manzoni, P. Securing warning message dissemination in vanets using cooperative neighbour position verification. *IEEE Trans. Veh. Technol.* **2014**, *64*, 2538–2550.
113. Cho, J.H.; Swami, A.; Chen, I.R. A survey on trust management for mobile ad hoc networks. *IEEE Commun. Surv. Tutor.* **2011**, *13*, 562–583.
114. Eckhoff, D.; Sommer, C. Driving for Big Data? Privacy Concerns in Vehicular Networking. *IEEE Secur. Priv.* **2014**, *12*, 77–79.
115. Dötzer, F. Privacy Issues in Vehicular Ad Hoc Networks. In *Privacy Enhancing Technologies*; Danezis, G., Martin, D., Eds.; Number 3856 in Lecture Notes in Computer Science; Springer: Berlin, Heidelberg, Germany, 2006; pp. 197–209.
116. Wiedersheim, B.; Ma, Z.; Kargl, F.; Papadimitratos, P. Privacy in inter-vehicular networks: Why simple pseudonym change is not enough. In Proceedings of the 7th International Conference on Wireless On-Demand Network Systems and Services, Kranjska Gora, Slovenia, 3–5 February 2010; pp. 176–183.
117. Hartenstein, H.; Laberteaux, K.P. A tutorial survey on vehicular ad hoc networks. *IEEE Commun. Mag.* **2008**, *46*, 164–171.
118. Lin, X.; Sun, X.; Ho, P.H.; Shen, X. GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications. *IEEE Trans. Veh. Technol.* **2007**, *56*, 3442–3456.
119. Buttyán, L.; Holczer, T.; Vajda, I. On the effectiveness of changing pseudonyms to provide location privacy in VANETs. In *Security and Privacy in Ad-Hoc and Sensor Networks*; Stajano, F., Meadows, C., Capkun, S., Moore, T., Eds.; Number 4572 in Lecture Notes in Computer Science; Springer: Berlin, Heidelberg, Germany, 2007; pp. 129–141.
120. Freudiger, J.; Raya, M.; Félegyházi, M.; Papadimitratos, P. Mix-zones for location privacy in vehicular networks. In Proceedings of the First International Workshop on Wireless Networking for Intelligent Transportation Systems (Win-ITS), Vancouver, BC, Canada, 14–17 August 2007.
121. Huang, L.; Matsuura, K.; Yamane, H.; Sezaki, K. Enhancing wireless location privacy using silent period. In Proceedings of the 2005 IEEE Wireless Communications and Networking Conference, New Orleans, LA, USA, 13–17 March 2005; Volume 2, pp. 1187–1192.
122. Caballero-Gil, C.; Molina-Gil, J.; Hernández-Serrano, J.; León, O.; Soriano-Ibañez, M. Providing k-anonymity and revocation in ubiquitous VANETs. *Ad Hoc Netw.* **2016**, *36*, 482–494.
123. Gross, R.; Acquisti, A. Information Revelation and Privacy in Online Social Networks. In Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society, Alexandria, VA, USA, 7 November 2005; pp. 71–80.
124. Bonneau, J.; Preibusch, S. The Privacy Jungle: On the Market for Data Protection in Social Networks. In *Economics of Information Security and Privacy*; Moore, T., Pym, D., Ioannidis, C., Eds.; Springer: New York, NY, USA, 2010; pp. 121–167.
125. Zheleva, E.; Getoor, L. To join or not to join: The illusion of privacy in social networks with mixed public and private user profiles. In Proceedings of the 18th International Conference on World Wide Web, Madrid, Spain, 20–24 April 2009; pp. 531–540.
126. Mislove, A.; Viswanath, B.; Gummadi, K.P.; Druschel, P. You are who you know: Inferring user profiles in online social networks. In Proceedings of the third ACM International Conference on Web Search and Data Mining, New York, NY, USA, 4–6 February 2010; pp. 251–260.
127. Thomas, K.; Grier, C.; Nicol, D.M. unFriendly: Multi-party Privacy Risks in Social Networks. In *Privacy Enhancing Technologies*; Atallah, M.J., Hopper, N.J., Eds.; Number 6205 in Lecture Notes in Computer Science; Springer: Berlin, Heidelberg, Germany, 2010; pp. 236–252.

128. Lucas, M.M.; Borisov, N. FlyByNight: Mitigating the Privacy Risks of Social Networking. In Proceedings of the 7th ACM Workshop on Privacy in the Electronic Society, Sydney, Australia, 19–22 May 2008; pp. 1–8.
129. Beato, F.; Kohlweiss, M.; Wouters, K. Scramble! Your social network data. In *Privacy Enhancing Technologies*; Fischer-Hübner, S., Hopper, N., Eds.; Number 6794 in Lecture Notes in Computer Science; Springer: Berlin, Heidelberg, Germany, 2011; pp. 211–225.
130. Guha, S.; Tang, K.; Francis, P. NOYB: Privacy in online social networks. In Proceedings of the First Workshop on Online Social Networks, Reno, NV, USA, 23–24 February 2008; pp. 49–54.
131. Narayanan, A.; Shmatikov, V. De-anonymizing social networks. In Proceedings of the 30th IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 17–20 May 2009; pp. 173–187.
132. Korolova, A.; Motwani, R.; Nabar, S.U.; Xu, Y. Link privacy in social networks. In Proceedings of the 17th ACM Conference on Information and Knowledge Management, Napa Valley, CA, USA, 26–30 October 2008; pp. 289–298.
133. Effendy, S.; Yap, R.H.; Halim, F. Revisiting link privacy in social networks. In Proceedings of the Second ACM Conference on Data and Application Security and Privacy, San Antonio, TX, USA, 7–9 February 2012; pp. 61–70.
134. Takabi, H.; Joshi, J.; Ahn, G.J. Security and privacy challenges in cloud computing environments. *IEEE Secur. Priv.* **2010**, *8*, 24–31.
135. Wagner, I.; Eckhoff, D. Privacy assessment in vehicular networks using simulation. In Proceedings of the 2014 Winter Simulation Conference (WSC), Savanah, GA, USA, 7–10 December 2014; pp. 3155–3166.
136. Wagner, I.; Eckhoff, D. Technical Privacy Metrics: A Systematic Survey. *arXiv:1512.00327*, 2015. http://arxiv.org/abs/1512.00327 (accessed 5 February 2016).