Future Internet **2015**, *7*, 257-275; doi:10.3390/fi7030257

OPEN ACCESS

future internet

ISSN 1999-5903

www.mdpi.com/journal/futureinternet

Article

Vehicular Internet: Security & Privacy Challenges and Opportunities

Kamran Zaidi * and Muttukrishnan Rajarajan *

School of Mathematics, Computer Science and Engineering, City University London, EC1V 0HB London, UK

* Authors to whom correspondence should be addressed; E-Mails: kamran.zaidi.1@city.ac.uk (K.Z.); r.muttukrishnan@city.ac.uk (M.R.); Tel.: +44-207-7040-3888 (K.Z.); +44-207-7040-4073 (M.R.).

Academic Editors: Steven Furnell and Andrew Hudson-Smith

Received: 28 April 2015 / Accepted: 9 July 2015 / Published: 24 July 2015

Abstract: The vehicular internet will drive the future of vehicular technology and intelligent transportation systems (ITS). Whether it is road safety, infotainment, or driver-less cars, the vehicular internet will lay the foundation for the future of road travel. Governments and companies are pursuing driver-less vehicles as they are considered to be more reliable than humans and, therefore, safer. The vehicles today are not just a means of transportation but are also equipped with a wide range of sensors that provide valuable data. If vehicles are enabled to share data that they collect with other vehicles or authorities for decision-making and safer driving, they thereby form a vehicular network. However, there is a lot at stake in vehicular networks if they are compromised. With the stakes so high, it is imperative that the vehicular networks are secured and made resilient to any attack or attempt that may have serious consequences. The vehicular internet can also be the target of a cyber attack, which can be devastating. In this paper, the opportunities that the vehicular internet offers are presented and then various security and privacy aspects are discussed and some solutions are presented.

Keywords: vehicular internet; VANETs; networks; security; privacy; ad hoc networks

1. Introduction

The developments in the automotive industry in the last few decades have been impressive. Cars today are much more fuel-efficient than ever before. However, the advancements in automotive technology did

not have the same impact on the safety of the roads. Vehicles today are still as vulnerable to accidents due to fog, ice, and other hazards on the road, but above all, they are vulnerable to human error. However, this is all set to change: the automotive industry has been working actively for years to put different sensors in cars and connect them to an on-board computer. With advancement in telecommunications, it is now possible to connect vehicles to each other through wireless technologies to enable them to communicate and cooperate. Now, not only is the automotive industry pursuing autonomous vehicles—they are being encouraged by the governments as well. The UK government announced in March 2015 that a £100 m funding for research into driver-less cars will bring in companies from not only the automotive industry but also from Information Technology (IT), telecommunications, and infrastructure [1]. In the US, car manufacturers like General Motors (GM) are already selling 4G Long Term Evolution (LTE)-connected cars in their 2015 fleet and they predict having fully autonomous cars by the end of this decade [2]. Moreover, IEEE believes that the need to get a driver's license might be eliminated by 2040 as autonomous cars would be ubiquitous [3].

Car manufacturers such as GM and Ford have opened up application development for their platforms by making their Application Program Interface (API) available to developers [4,5]. They plan to follow the conventional business model, *i.e.*, the developers submit their apps which are tested and approved before making them available for download. This LTE connectivity alone will serve to improve the in-vehicle infotainment services by providing access to high-speed internet, streaming movies, navigation, music, and live television, *etc.* The other aspect is commercial, *i.e.*, offering location-based services and ads to the vehicle passengers. The LTE connectivity will not only bring internet to the vehicle but also make the vehicle a part of the internet, easing the way for the Vehicular *Ad Hoc* Networks (VANETs).

The true potential of the connected vehicle will be realized only when vehicles are interconnected to each other. This network, formed by the interconnection of vehicles, is referred to as VANET. This paradigm shift in vehicular technology will usher in a new era of innovation and will open a huge range of application areas that can help in improving road safety and reducing accidents on roads.

VANETs are considered important due to their huge potential and numerous applications. VANETs not only offer immense safety enhancements but also many commercial opportunities. Wireless access in the vehicular environment (WAVE) is based on IEEE 802.11p standard and provides the basic radio standard for Dedicated Short Range Communication (DSRC) in VANETs. DSRC has been allocated 75 MHz in the 5.9 GHz band by the FCC (Federal Communications Commission) in the US, and a similar band has been allocated in Europe as well. Vehicles use DSRC radios to communicate with each other, *i.e.*, vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication. The communication range of DSRC is between 300 and 1000 m.

With the addition of 4G/LTE connectivity in vehicles, it is obvious that connected vehicles would be able to share data through the cloud. The advantages of using cloud are huge as the opportunities for applications are virtually limitless. The communication environment with both LTE and DSRC is shown in Figure 1.

DSRC specifies one main type of beacon message, *i.e.*, Basic Safety Message (BSM), that a vehicle transmits every 100 milli secs. In BSM, vehicles broadcast their location, speed, acceleration, and other useful parameters, which help other vehicles avoid collisions and generate warnings for improved safety. These messages also help the vehicles maintain the list of their neighbours. The congestion information

is already available through navigation systems (Sat Nav) but exact real-time position information of other vehicles is not. This is the future that can enable the driver to drive safely even if there is zero visibility or when the driver is unable to drive, *etc.* Therefore, the vision is to create a mutual awareness among all vehicles on the road that leads to driver-less cars.

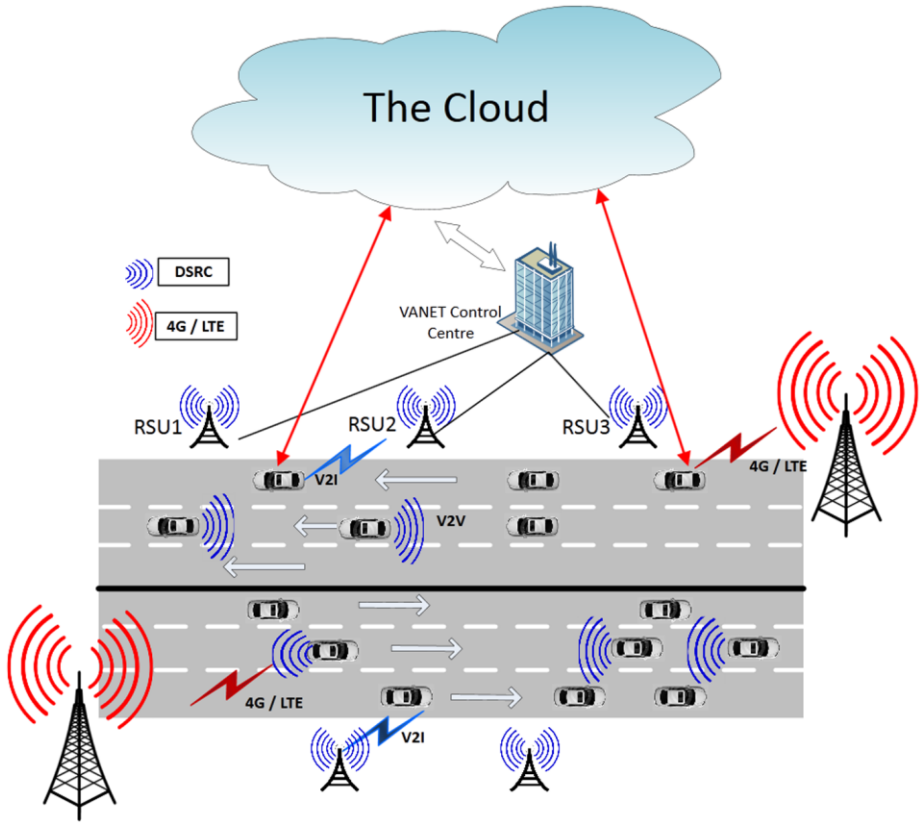

Figure 1. Vehicular Internet environment.

All vehicles can be programmed to transmit their location information whenever they make a sudden change in speed or position. However, the bandwidth in DSRC is quite limited, so we just cannot have vehicles transmitting their position and speed information all the time or we will have a jammed channel. The DSRC band consists of seven bands of 10 MHz each with a 5 MHz guard band in the beginning. One band out of these is reserved for BSM, but even this dedicated channel can be congested very quickly if the traffic is heavy and many vehicles are broadcasting BSMs.

The DSRC and 4G/LTE connectivity in vehicles can supplement each other and solve the bandwidth problem to give high quality, reliable, and secure information to VANET users. This combination will make it possible for a wide variety of applications and opportunities that will be discussed in the next section.

2. Applications for VANETs

Many different convenience and commercial applications have been proposed for VANETs by researchers in [6–8] and safety applications have been proposed by the US Department of Transportation in [9]. With so many vehicles on the roads/highways having so much computing power and sensors, it is obvious and logical to utilize all this data to form an array of scattered sensor networks or highly mobile *ad hoc* networks. Some of the applications that have been recommended for VANETs include:

i. **Safety applications:** Notifications for crashes, hazards on the roads (slippery or wet road conditions), traffic violation warnings, curve speed warnings, emergency electronics brake light, pre-crash sensing, co-operative forward collision warnings, *etc.* This could also include generating warning messages that inform drivers of approaching emergency vehicles.
ii. **Convenience applications:** Navigation, personal routing *etc*., Congestion advice, toll collection, parking availability information, *etc.* Also, in disaster situations, the critical things are power failure and network breakdown. The connected vehicles can play a very significant role in such situations as they have on-board batteries and many sensors including cameras, *etc.*, thus providing valuable images and SOS calls. The vehicular network can become the emergency communication mechanism. Similarly, road and weather conditions can be monitored by sharing the data from on-board vehicle sensors [9].
iii. **Commercial applications:** Vehicle diagnostics exchanges for avoiding possible car problems, location-based services such as advertisements and entertainment, *i.e.*, data/video relay, social networking updates, *etc.*

In the applications discussed above, the vehicles are sharing information in V2V and V2I communications that includes their position information and also information of road conditions. Furthermore, the driver may need to make life-saving decisions based on the information received (e.g., emergency brake light, forward collision warning). It is therefore necessary that the privacy, reliability, and integrity of the messages are ensured so that actions can be taken in a split second after the information is received due to the speeds involved in the case of vehicles.

3. VANET and the Cloud

The large amount of unused storage space and computing power coupled with on-board sensors provide a unique opportunity to utilize vehicles as a wireless sensor network. The vehicles will be equipped with not only sensors to measure temperature, humidity, wind, *etc*., but also with cameras. This together with high speed (4G/LTE) connectivity can be a great advantage for a variety of applications. VANETs can be a part of the cloud in the following three possible ways (Figure 2).

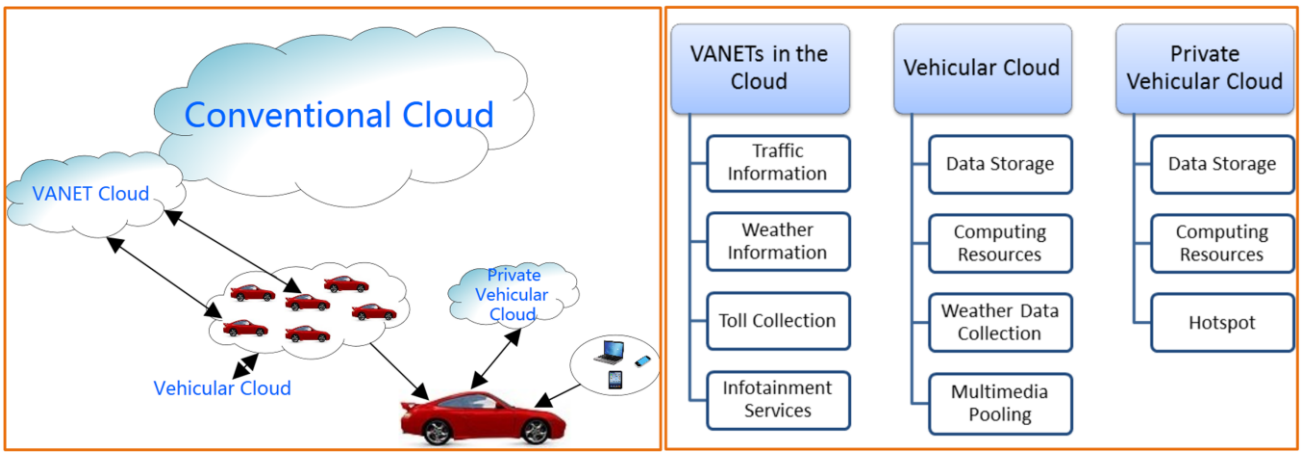

Figure 2. VANETs and cloud (left), cloud applications (right).

3.1. VANETs in the Cloud

The connected vehicles can connect to the cloud and upload their data, including sensor readings, traffic information, *etc.*, for downloading by other vehicles that are following behind. This allows the users to share data anonymously and preserve their security and privacy. The application servers in the cloud can aggregate the information coming in from vehicles and then compile the data to make announcements for traffic, road conditions, accidents, and weather conditions based on vehicle sensor data [9]. This improves the reliability of the information by filtering out biased or false information based on the number of users reporting such information.

3.2. Vehicular Cloud

The vehicles can connect together forming a vehicular cloud that will offer storage space, computing resources, sensor readings, *etc*. as an on-demand service to clients. The clients could be individuals, corporations, or government departments such as the meteorology department, police, or highway authorities. Moreover, with cameras onboard vehicles and high-speed connectivity, the police or emergency services can even request images from vehicles for an area that they want to monitor such as the site of an accident. Ericsson has already developed its own Connected Vehicle Cloud (CVC) for vehicle telematics and is behind Volvo Cars Sensus, which is an infotainment system for Volvo vehicles [10]. The CVC is designed to open new business opportunities by providing the vehicle data to companies, allowing developers to develop new applications by giving them an open platform, and facilitating the drivers by connecting them to the manufacturers and other service providers.

3.3. Private Vehicular Cloud

The storage, connectivity, and computing resources of the vehicle can be utilized by the owner as a private cloud, *i.e.*, the user connects to the internet and uploads their data to their "private cloud". This not only makes their data available to them whenever they want, but it also gives them physical ownership of their data.

4. Autonomous Vehicle

The autonomous vehicle is a reality today (Google Car) and it is only logical to say that the technology will improve further and reduce in cost to become a feature in the near future. However, it will take some time for it to become a driver-less feature on a big scale. Also, it is possible that much like cruise control, this could become a feature that could be activated on the motorway/highway.

Autonomous vehicles would need almost no input from the driver. This would be possible with a lot of hardware like cameras, radars, and Laser Illuminated Detection and Ranging (Lidars) to sense oncoming obstacles. Image processing techniques are applied to images from the cameras to recognize and identify shapes and features. This enables the vehicle to sense the approaching obstacle and automatically apply breaks or reduce speed much more quickly than the driver would ever be able to. The use of these and other technologies therefore ensures that human errors can be reduced to a large extent and, as a result, roads can be made much safer. This would enable the driver to be more productive by doing something like reading, browsing on the internet or making a phone call. In terms

of safety, autonomous vehicles are not only a possibility but a necessity for safe motoring. The next step in autonomous vehicles is vehicle swarm.

5. Vehicle Platoon/Swarm

Travelling at high speeds brings more problems into the picture and makes things a lot more complicated when the vehicle is on a motorway/highway. However, these problems can be reduced if the vehicles form a group and then travel in a formation on highways and motorways. This will have two benefits: first, vehicles are synchronized (*i.e.*, vehicles travel in a straight line and maintain a fixed distance from each other and the vehicle in front informs the cars behind if they should reduce speed or change lanes in advance, and then all of them can do it in tandem) and second, the randomness in the immediate vicinity of the vehicles is reduced, which makes things much simpler and safer. Safe Road Trains for the Environment (SARTRE) is an EU-financed 6.4-million-dollar project that has proven this concept in collaboration with Volvo and UK-based company Ricardo, among others [11]. The aim of the SARTRE project was to develop a road train or platoon concept in vehicular traffic where a lead vehicle driven by a professional driver takes control of a platoon of vehicles that go in a semi-autonomous state [11]. The SARTRE project demonstrated successfully that vehicle platoons are not only safe but can be very efficient in reducing congestion and improving safety.

The vehicle swarm (shown in Figure 3) can be imagined by thinking of the motorway/highway as a conveyor belt, but where a conveyor belt moves with a constant steady speed, a group of vehicles on the motorway can move with any set constant speed. This can be possible by allowing like-minded vehicles, *i.e.*, vehicles that intend to travel at roughly the same speed, to team up and form groups or a "vehicle swarm". Ricardo, a British engineering firm involved in the SARTRE project, believes that vehicle platooning is possible with fully autonomous vehicles [12].

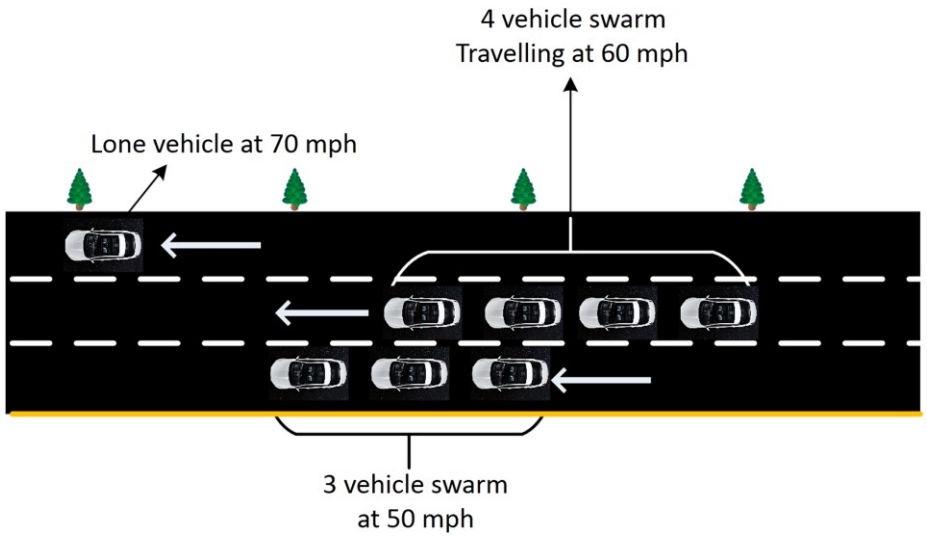

Figure 3. Vehicle swarm concept.

6. Security and Privacy Issues

Security and privacy of users in VANETs are very important but, at the same time, an objective and realistic definition of security and privacy is also needed. This means that the level of security and

privacy assured in a VANET can be no more than it is in the real world [13]. In the real world, a vehicle can be identified by its registration plate and then tracked by authorities via video cameras as is the practice nowadays. Similarly, there are cases (e.g., stolen car, accident, or misbehaving vehicle) when the whereabouts of a vehicle in a VANET have to be determined by the authorities, e.g., in case of accidents, which implies traceability. The US Department of Transportation (DOT) has identified many safety applications which require each vehicle to periodically transmit its current location to its one-hop neighbours at a rate of up to 10 Hz [14]. These messages, called Cooperative Awareness Messages (CAMs), are susceptible to an eavesdropper who can then get the location of that vehicle. Therefore, it is necessary that the messages are secured from giving away the user's location. The security and privacy goals and how they are achieved in VANETs are shown in Figure 4 and are discussed below in detail.

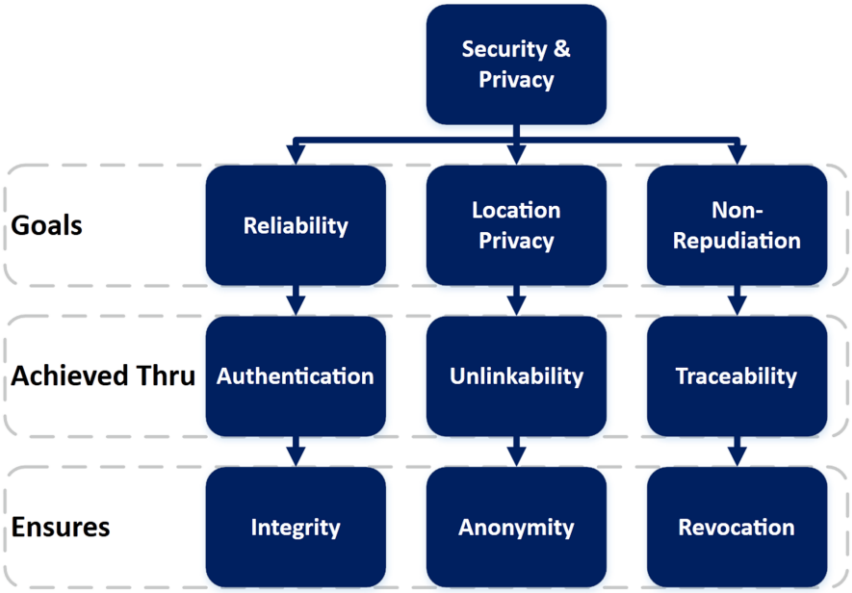

Figure 4. Security and privacy goals in VANETs and how they are achieved.

It is essential for VANET security that the location of a vehicle is transmitted while preserving the location privacy of the user. This location information can be used by adversaries in tracking vehicles or routes. As discussed previously, location privacy requires unlinkability, which ensures anonymity. As the information in VANETs is very critical for safety, it is imperative that it should be reliable. Reliability is achieved through authentication, which ensures the integrity of the messages, *i.e.*, they have not been tampered with. Another requirement for VANETs is non-repudiation, which means that users should not be able to deny sending a message so that they can be tracked and penalized in case of a false message. This is achieved by making the messages traceable but only by the authorities so that they can be revoked. It has been proposed [15] that the tracing should be done by multiple authorities in order to provide extra security and privacy. Different security schemes have been used to protect privacy or achieve anonymity and, based on the underlying security mechanisms they use, these schemes can be classified as:

- Pseudonyms coupled with public key infrastructure (PKI)
- Trust-based schemes
- Group signatures

- k-anonymity schemes
- Identity-based signature schemes

There are various issues associated with each of these schemes which are discussed in the next section.

7. Review of Security and Privacy-Preserving Schemes in VANETs

7.1. Pseudonyms Coupled with PKI-Based Schemes

As the vehicles are transmitting their location information, e.g., to warn other users of accidents, researchers [16,17] have discussed using pseudonyms to preserve the privacy of users. The use of Pseudonyms (PNs) hides the real identity of the user and prevents the linking of the real identity of the user with the pseudonym, thereby providing unlinkability. However, the Regional Trusted Authority (RTA) that issues pseudonyms can reveal the real identity of the user if the user commits an illegal act, hence providing traceability.

In all cases, the On Board Unit (OBU) is assumed to be a tamper-proof device which contains the unique Vehicle Identification Number or VIN. This VIN is tied to an identity certificate at the time of registration. From here on, the Trusted Authority (TA) (e.g., transport authority) is tasked with issuing new blocks of pseudonyms/certificates to the vehicles, to be used while communicating with the Road Side Units (RSUs). These certificates have a validity period and the vehicle switches its pseudonyms to ensure privacy. The authors in [18] suggest that short-term linkability should be allowed so that the receiver is able to verify that two or more messages in a short time frame have come from the same sender, as this might be required by applications. The recommended time after which the pseudonyms are switched also varies, e.g., every minute or every few minutes, with every message or every second [19]. However, the frequency of PN changes is directly proportional to the computation overhead at the RSU, which can slow down packet delivery. Also, the OBU is also supposed to store the public keys of all CA (Certificate Authority) / TA. Furthermore, different PKI-based techniques that use a CA/TA connected with the RSU have been suggested.

The downside of the pseudonym scheme is that the user (OBU) has to have hundreds or thousands of these pseudonyms stored on board and they need to be refreshed after some time (e.g., once a year). Different papers have explored this and proposed different methods of refreshing these, e.g., downloading new pseudonyms when the vehicles go in for service (once a year). It is also suggested that the pseudonyms are refilled at social spots [20]. In [13], a PN distribution scheme is proposed which incorporates control channels and service channel intervals in communication between vehicle and RSU for PN refill. It is important to note that pseudonym schemes alone do not support authentication, integrity, and non-repudiation. Signing protocols have been proposed that provide integrity and authentication. In this, a large number of certified public-private key pairs are stored in the OBU. Each key pair will be used for a short period of time and then discarded. Using PKI involves downloading and maintaining public key certificates, which results in heavy computational overhead that is not desirable in VANETs as the computing power of OBU is limited.

Anonymous certificates in PKI-based schemes can guarantee identity privacy but cannot guarantee location privacy. This is because an attacker can monitor the certificate change by a vehicle between two observation points while moving in the same lane with the same speed. Also, the TA/CA has the

ability/capability to identify the real identity of a vehicle based on its anonymous certificate. In [15], a method has been proposed so that multiple authorities are required to de-anonymize a user to increase the security. In [17], authors propose that the users change their PNs only at predetermined locations (mix zones) where the density of vehicles is high and the speed and direction of vehicles changes often. However, the authors conclude that such a technique provides limited privacy due to the inherent lack of randomness in vehicle mobility.

A major drawback of using PN is maintaining the Certificate Revocation List (CRL), which keeps track of revoked certificates of misbehaving vehicles. This list then has to be checked to ensure whether a vehicle is revoked or not, which is both time- and resource-consuming. Authors in [19] propose a reduction in CRL size by limiting the list to regions, *i.e.*, each RTA will maintain its own CRL, thereby reducing the size of each CRL.

7.2. Trust-Based Schemes

VANETs share many characteristics with Mobile *Ad Hoc* Networks (MANETs). Trust-based routing schemes have been proposed for MANETs and the same idea of trust has also been applied to VANETs in [16,21,22]. However, apart from a lot of similarities between them, e.g., decentralized system, mobility, and openness, VANETs are different as they consist of a much larger number of nodes and their topology changes quickly as vehicles move fast [23]. Therefore, forming a network based on the trustworthiness of vehicles is quite challenging. In MANETs, the focus is on reliable packet delivery, whereas in VANETs the aim is to increase road safety and, therefore, the decision-making process has to be very fast due to the high speeds and limited time involved.

In [24], authors propose trust establishment through infrastructure or in a self-organizing manner. The former means to use a central authority or security infrastructure and the latter involves developing a trust score dynamically. In infrastructure-based trust establishment, there has to be a centralized authority, but it is very difficult to do that quickly in VANETs due to the size and time restrictions. In self-organizing trust establishment, the trust is based on the direct (self-interaction), indirect (receiving interaction information from other nodes), and hybrid approaches (combination of the two) as shown in Figure 5.

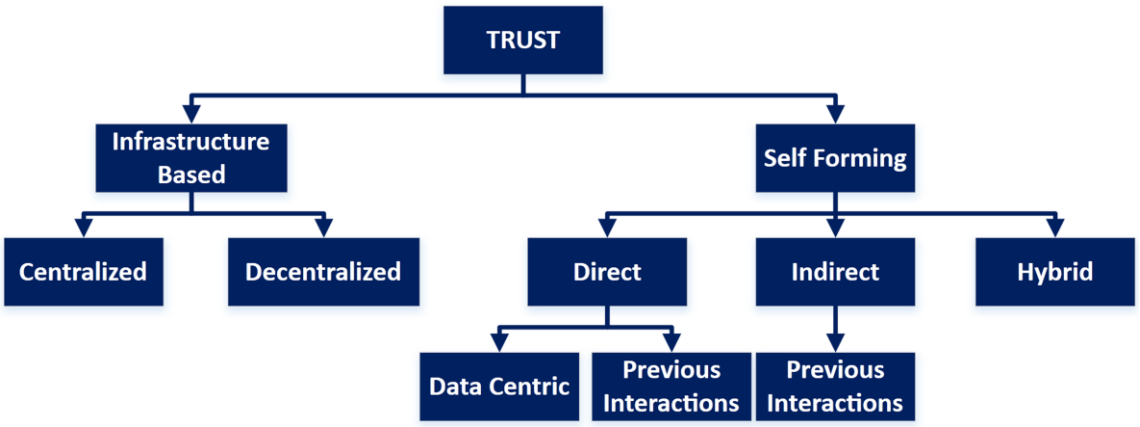

Figure 5. Classification of trust establishment approaches.

As the vehicle's trust score has to be updated and linked with some identification (Pseudonym/Certificate, *etc.*), it again raises the problems of privacy. Moreover, in VANETs, the trust information might not be available in the beginning, or a default trust score has to be assigned. Also, once a group of vehicles form a network, it is then difficult to protect oneself from an insider. To account for this, data-centric trust schemes have been suggested in [25], where a malicious node can be identified based on the data/information being exchanged. In [26], a data-centric mechanism is proposed that enables users to aggregate the data and then determine if a rogue is sending false data. The rogue node can then be reported and its data is ignored.

7.3. Group Signatures

For VANETs, authors in [27] proposed the grouping of vehicles travelling at the same speed and in the same direction. This allows group members to anonymously issue messages and sign them with the group signature on behalf of the group. This also allows extended silent periods for vehicles as only one vehicle in the network transmits at a time. By combining the vehicles into groups, the authors proposed that a vehicle can reduce its V2I transmission, which enhances the anonymity of vehicles. Group signatures allow the distribution of a group public key associated with multiple group private keys. Therefore, an attacker will be able to detect that a message has been sent by a particular group but it will not be able to identify which vehicle sent the message [24].

In [18], a scheme based on group signatures and short-lived keys, called Temporary Anonymous Certified Keys (TACS), is presented as an efficient way to fulfill the privacy and safety requirements. The scheme suggests a long-term group key stored in the OBU provided by a managing authority which the OBU uses anonymously to prove to the RA that it is a valid OBU and to get a short-term certified key that is only valid in that RA's region. As soon as the OBU moves into a new region, it has to update its TACS by getting a new short-lived certified key from the new RA. This ensures that OBUs update their keys after entering a new region. This ensures short-term linkability and traceability in the long run as the managing authority can be queried by the RA for the real identity of the vehicle.

Group signatures provide a high level of privacy but revocation becomes a serious problem when the size of the group increases, thereby raising scalability issues. Furthermore, they can be computationally more expensive [28].

7.4. Identity-Based Encryption Schemes with Pseudonyms

Identity-based encryption (IBE) was first proposed in [29]. Identity-based cryptography allows the public key of an entity to be derived from its public identity information such as name, email address, or VIN, *etc*. Anybody who wants to send a message to a user can use the recipient's identity to get their public key and encrypt the message using this key, which can only be decrypted by the private key of the intended recipient. A private key generator (PKG) is used to generate and distribute private keys for users (through a secure channel) and also to distribute the public key. IBE is highly suited to a dynamic *ad hoc* network like VANETs, as it allows nodes that have not met before to start communicating with each other quickly and safely.

The authors in [15,30,31] have used the idea of IBE in VANETs. The proposed architecture in [31] consists of four entities, two TAs which are trace authority (TRA), a PKG, an RSU at the roadside, and

mobile OBUs on vehicles. Privacy in IBE schemes is achieved by using pseudonyms that the user can request from the TRA. The TRA is responsible for registration of RSUs and OBUs, and can reveal the actual identity of the signing OBU. The PKG is responsible for generating and assigning private keys for OBUs and RSUs. Self-generating pseudonyms (PNs) are suggested for privacy preservation. For authentication, a pool of PNs is preloaded into a vehicle for different regional trusted authorities (RTAs). Users from different regions can authenticate each other via RTAs. RTAs are responsible for generating cryptographic key materials for the RSUs and the vehicles in the region and deliver them over secure channels. The users use their self-generated pseudonyms as identifiers instead of real-world identities. Similarly, the idea of IBE is used in [30] to improve the performance and reduce the processing time of RSU when it is verifying signatures for a large number of users.

Identity-based cryptography seems to be a good candidate for security and privacy in VANETs but has its own limitation and challenges, especially with revocation, which is still a major problem and is open for research. Secure channels for secret key distribution and heavy computation costs are other factors to consider.

7.5. k-Anonymity Schemes

Researchers have proposed k-anonymity schemes for VANETs. In [32], a k-anonymity scheme has been proposed where k vehicles in a region are assigned the same PN for communicating with the RSU. This ensures that an attacker cannot associate a message with a specific vehicle. An attacker can only detect that a group of nodes are receiving the messages but cannot determine which one in particular. The source and destination anonymity cannot be guaranteed as VANETs are inherently changing all the time, therefore, it is difficult to identify the source and destination. In k-anonymity schemes, when a message has to be delivered to a vehicle, the region is flooded with the message to ensure that it reaches the destination vehicle. However, in such a multi-hop scheme there is a clear problem of the scarce bandwidth resource utilization. The network might be flooded by the same message, causing congestion which is highly undesirable in VANETs.

8. Performance Comparison

In order to compare the performance of different schemes discussed in this paper, it is necessary to have complete details of the algorithms proposed for all the schemes. One parameter that can be used to judge the performance of networks is control overhead, but in order to calculate this, it is necessary to know the exact type and size of data that the OBU will be handling. This can only be obtained after finalizing the type of applications that will be deployed in VANETs. Similarly, bandwidth utilization is another important parameter that has to be taken into account, but it is difficult to calculate it as the type of data and applications in VANETs have not been finalized. Therefore, we have compared the major performance characteristics of the discussed schemes by defining or modifying some parameters in Table 1 and we have discussed the major features and disadvantages of each scheme in Table 2. For comparison of the schemes discussed, we have used the rating system of HIGH, MED, and LOW in Table 1. The performance metrics used in Table 1 are described below:

- **Scalability:** Scalability is a well-defined performance metric for network protocols and architectures and it means how well a system can cope with the expansion of the network while maintaining the performance standards. A LOW in this category means that the scheme is not suitable for a network in which the number of nodes can grow beyond a small number. A MED in this category means that the scheme can work well for a limited number of nodes but it should not exceed that limit. A HIGH means that the scheme is highly scalable and can work well for a very large number of nodes.
- **Computing cost:** The computing cost has been chosen as a metric because it is always in demand and usually it is always less than what is desired. Furthermore, experience has shown that the appetite of programs and data eats up the computing power available very quickly. We have considered the computing cost at both the RSU and OBU. This metric is especially important at the OBU end where we can have reasonable, but never excessive, computing power. A LOW here means that the computing resources required are much less than available. HIGH means that computing resources available might fall short of what is required. MED means that the computation resources are sufficient.
- **Privacy:** This is the fundamental requirement of all schemes studied and has been rated according to the merits and demerits of each when viewed in its entirety, e.g., in the case of pseudonym *cum* PKI schemes, the privacy has been rated as MED as the PNs changing and their maintenance poses a serious challenge for the successful deployment in VANETs. HIGH means strong, MED means acceptable but risky, and LOW means unacceptable or no level of privacy.
- **Latency:** This is another well-known parameter for networks that means delays which are experienced in a network due to any reason. A network with LOW latency is considered to be fast and vice versa.
- **Cost of deployment:** This parameter indicates whether the infrastructure requirements make it easy to deploy in the practical world or not. A scheme with HIGH cost of deployment is obviously high-cost and difficult to deploy, *i.e.*, with many additions/changes to the existing network making it impractical. A scheme which gets a LOW in this metric will be low-cost to deploy and will require a few changes to the existing network to make it feasible.

Table 1. Performance metrics for security schemes in VANETs.

S/No	Scheme	Scalability	Computing cost		Privacy	Latency	Deployment cost
			RSU	OBU			
1	Pseudonym *cum* PKI	HIGH	HIGH	HIGH	MED	MED	HIGH
2	Group Signatures	LOW	MED	HIGH	HIGH	HIGH	HIGH
3	Trust-Based Schemes	LOW	HIGH	HIGH	LOW	HIGH	HIGH
4	K-anonymity	LOW	MED	HIGH	HIGH	HIGH	MED
5	Identity-Based Encryption (IBE) with Pseudonyms	HIGH	MED	HIGH	HIGH	HIGH	HIGH

Table 2. Qualitative Comparison of Security Schemes in VANETs.

S/No	Schemes	Features	Disadvantages
1	Pseudonym *cum* PKI	*(a)* User privacy is achieved by using pseudonym coupled with PKI; (*b*) Certificates (public, private key pairs) are downloaded from trusted authority; (*c*) Pseudonyms are changed continuously for preserving privacy.	*(a)* Thousands of certificates to be downloaded to OBU; (*b*) Certificates need to be replenished periodically; *(c)* CRL has to be maintained and it keeps on changing and is time- and resource-hungry; (*d*) The CA can link pseudonyms with vehicles, and therefore have to be secure.
2	Group Signatures	*(a)* Privacy achieved by forming groups; (*b*) Reduced transmission by ways of periodic broadcasts by a single member of group.	*(a)* TA can reveal the real identity of user (*b*) CRL has to be maintained and checked and it increases with the size of the group.
3	Trust-Based Schemes	Information accepted based on trust. Trust established based on previous record in a centralized authority or based on current and previous interactions with the user in the same session.	*(a)* No initial trust information available as centralized system would be too slow/too huge; (*b*) Protection against inside attackers is difficult; (*c*) Trust score has to be maintained and checked.
4	K-anonymity	*(a)* Messages are disseminated by ways of flooding it to neighbours; (*b*) Ensures privacy as long as size of group is adequate.	Flooding is used to disseminate messages which if not effective, can overwhelm the network and eat up bandwidth for the same message. Efficient and practical algorithm missing.
5	Identity-Based Encryption (IBE) With Pseudonyms	*(a)* User's public key is derived from his public identification such as VIN, *etc*., which eliminates the need for public key distribution (*b*) No need for certificate downloads and storage in OBUs (*c*) Additional information such as a time stamp can also be added.	*(a)* Secure channel needed for private key distribution; (*b*) PKG has to be highly secure; (*c*) TRA can reveal the real identity of the user, therefore must be secure; (*d*) Revocation is still an open problem.

9. Challenges

9.1. Security

Securing the vehicle from external attacks so that vehicle is not hijacked remotely is a very real threat and will be the most important challenge to address. This will be especially challenging in autonomous or driver-less vehicles, as by design the vehicle is required to navigate on its own by controlling the steering and control system of the vehicle. The brains of the vehicle or the OBU will control the movement of the vehicle and the OBU will be connected to the internet and the vehicular cloud. Therefore, securing the control systems of the vehicle will be the first thing that has to be done and is only possible with very strong security systems in place to secure the vehicles from a cyber attack.

9.2. Privacy

The information that is collected from the car's sensors has to be protected and should only be used after anonymizing it. The concern is that your car should warn you if you are over the speed limit

but should not turn against you, *i.e.*, reporting to the authorities that you went over the speed limit. However, there are many instances when sharing location information with some service providers might actually be beneficial for the user, e.g., insurance companies might offer to reduce the insurance premiums if such details are shared. There can be similar incentives from other service providers to use vehicle sensor data in return for some reward that can actually encourage participation from the users.

9.3. Cost

Another important factor is undoubtedly the cost. When there are so many features and hardware available for the vehicles, it all comes down to how affordable all this can be made. A logical solution could be offering all the available features to the buyer as a customizable solution at the time of buying the vehicle or as later add-ons, which will keep the cost of the vehicle in check.

10. Possible Solutions to Security Issues

We have proposed some solutions in [15,26] to the issues mentioned above. The issues of identity, PN generation, security, and privacy preservation have been addressed in [15]. We propose a digital identity scheme for VANETs (DIVA) by considering that it is the driver who is to be held liable for the vehicle and not *vice versa*. Therefore, we use the identification of the vehicle (VID) and the driver (DrL) to form a new digital identity. The two identities are merged into one after authentication from two authorities, *i.e.*, the vehicle registration authority and the driver license authority. Each of the two authorities issues the user a token and secret keys which are then used by the user to generate their pseudonym. Therefore, even if the master key is compromised, the tokens can only be traced by the two authorities and no individual authority can reveal the true identity of the user. Moreover, in DIVA, the PNs are being generated at the OBU, which reduces the latency at the RSU. The performance of the scheme is compared with two other schemes efficient conditional privacy preservation (ECPP) [33] and pseudonymous authentication-based conditional privacy (PACP) [34] as shown in Figure 6.

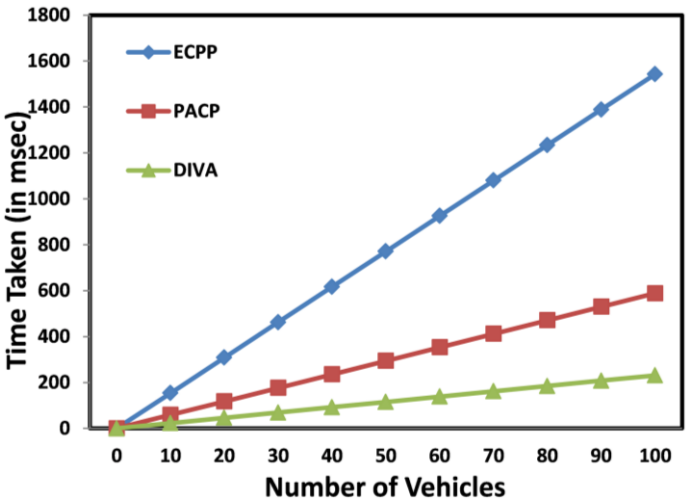

Figure 6. Comparison of protocol latency at RSU [15].

To compute latency at the RSU, the same parameters are used as in [34], *i.e.*, key size of 160 bits and times required for a pairing operation and point multiplication to be 7.3 ms and 8.5 ms, respectively.

The major operations in our scheme for RSU to perform decryption and signature verification involve two pairing operations (PO) and one point multiplication (MP), whereas ECPP requires 13 MPs and six POs and PACP requires two POs and one MP for verification at RSU. However, in both PACP and ECPP, the RSU generates and verifies the PN tokens and short-lived key pairs, respectively, for the vehicles, which causes more delay as shown in Figure 6. The graph shows the latency when only one token is being generated for each vehicle as the number of vehicles increases from one to 100. In DIVA, the PNs are being generated at the OBU and therefore, there is no extra delay at the RSU and the latency is reduced at the RSU, which is desirable.

The issues associated with trust and rogue nodes in VANETs are addressed in [26]. As discussed previously, trust is difficult to maintain in VANETs and honest nodes can turn rogue once they become part of the network. Therefore, a data-centric rogue node detection scheme (C-DAC) is presented in [26] to address the issues of trust and security in VANETs. A mechanism has been proposed where users can aggregate the data that they are receiving while sharing their own data with their neighbours. The scheme is not dependent on any past trust value and only relies on the data that is received from the node, which is highly desirable as trust is difficult to manage in VANETs. C-DAC allows the vehicles to get a very good picture of the *normal* conditions/data in their vicinity. Therefore, any abnormal or anomalous data received can be rejected and the user reported. In order to check the proposed model, it is simulated using OMNET++, SUMO [35], and VACaMobil [36]. OMNET is a modular C++ library and framework that is used for network simulations. Simulation of Urban Mobility (SUMO) is a software tool for vehicular traffic generation by specifying speed, vehicle behaviour, road type, and conditions. VACaMobil is a car mobility manager for OMNET that works with SUMO. Different scenarios with and without accidents are simulated with parameters given in Table 3. The results show that using this scheme, vehicles can effectively determine false data and the emergency message can successfully be conveyed to vehicles that are far off so that they can gradually slow down.

Table 3. Simulation parameters for C-DAC [26].

Parameter	Value
Simulation Time	500 s
Scenario	3 Lane Highway
Highway Length	5-Kms
Max Vehicle Speed	28 m/s or 100 Km/h
Mobility Tool	VACaMobil
Network Simulation Package	OMNET++
Vehicular Traffic Generation Tool	SUMO
Number of Vehicles	330
Vehicle Density	20–30 veh/Km
Wireless Protocol	802.11p
Transmission Range	500 m in each direction

The proposed C-DAC scheme also effectively solves the problem of broadcast storms, *i.e.*, when nodes try to send the same emergency message to alert other vehicles causing congestion and a choked network very quickly. C-DAC has the ability to convey the emergency information to other vehicles far behind successfully and efficiently without causing network congestion. This success, *i.e.*, how far

the information is successfully received on the road, is compared with another scheme, Adaptive and Mobility Based Algorithm (AMBA) [37], and is shown in Figure 7.

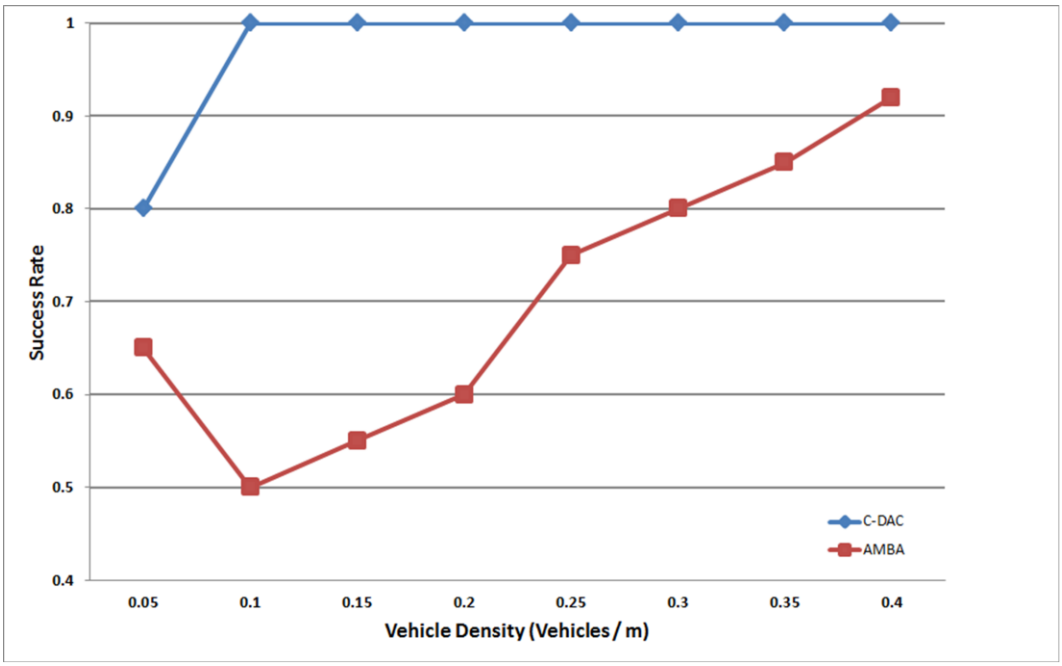

Figure 7. Percentage of vehicles within 3 km that received the emergency information successfully [26].

11. Conclusions

It is evident from the discussion above that the security and privacy challenges in vehicular internet are significant. The risks associated with the adoption of technologies associated with VANETs will be weighed against the benefits they provides. However, the benefits clearly outweigh the risks and this is what the users will consider when adopting these technologies. The privacy will be important to the user but probably not in every case and not for everyone. Also, the incentives will decide whether the users voluntarily share the data or share it after anonymizing it. The autonomous car is a reality today and there is no doubt that it will become commonplace in the years to come. The connected vehicle is imminent and it is important that steps are taken to minimize the security and privacy issues associated with it before its launch.

Author Contributions

Kamran Zaidi contributed to the design of the proposed schemes, implementation and simulation setup and writing of the initial draft paper. Muttukrishnan Rajarajan supervised the research work and provided guidance in terms of the structure, content and proofreading of the final paper.

Conflicts of Interest

The authors declare no conflict of interest.

References

1. The Telegraph. Available online: http://tinyurl.com/telegraph-co-uk-finance-budget (accessed on 10 June 2015).
2. General Motors. Available online: http://media.gm.com/media/us/en/gm/news.detail.html/content/Pages/news/us/en/2013/Feb/0225_4g-lte.html (accessed on 10 June 2015).
3. IEEE Intelligent Transportation System Society. Available online: http://its.ieee.org/2014/09/15/you-wont-need-a-drivers-license-by-2040/ (accessed on 07 June 2015).
4. Ford. Available online: https://developer.ford.com/ (accessed on 09 June 2015).
5. General Motors. Available online: https://developer.gm.com/ (accessed on 10 June 2015).
6. Hartenstein, H.; Laberteaux, K.P. A Tutorial Survey on Vehicular Adhoc Networks. *IEEE Commun. Mag.* **2008**, *46*, 164–171.
7. Faezipour, M.; Nourani, M.; Saeed, A.; Addepalli, S. Progress and Challenges in Intelligent Vehicle Area Networks. *Commun. ACM* **2012**, *55*, 90–100.
8. Haas, J.J.; Hu, Y.; Laberteaux, K.P. Real-World VANET Security Protocol Performance. In Proceedings of the IEEE GLOBECOM 2009, Global Telecommunications Conference, Honolulu, HI, USA, 30 November–4 December 2009.
9. United States Department of Transportation. Available online: http://www.its.dot.gov/connected_vehicle/connected_vehicle_apps.htm (accessed on 09 June 2015).
10. Ericsson. Available online: http://archive.ericsson.net/service/internet/picov/get?DocNo=28701-FGD101192&Lang=EN&HighestFree=Y (accessed on 08 June 2015).
11. The SARTRE Project. Available online: http://www.sartre-project.eu/en/Sidor/default.aspx (accessed on 09 June 2015).
12. New Scientist. Available online: http://tinyurl.com/newscientist-com-article (09 June 2015).
13. Benin, J.; Nowatkowski, M.; Owen, H. Unified pseudonym distribution in VANETs. In Proceedings of the 2010 IEEE 6th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Niagara Falls, ON, USA, 11–13 October 2010; pp. 529–533.
14. *Vehicle Safety Communications Project Final Report: Identify Intelligent Vehicle Safety Applications Enabled by DSRC*; DOT HS 809 859; U.S. Department of Transportation, National Highway Traffic Safety Administration: Washington, DC, USA, 2005.
15. Zaidi, K.; Rahulamathavan, Y.; Rajarajan, M. DIVA-Digital Identity in VANETs: A multi-authority framework for VANETs. In Proceedings of the 2013 19th IEEE International Conference on Networks (ICON), Singapore, Singapore, 11–13 December 2013; pp. 1–6.
16. Abumansoor, O.; Boukerche, A. Towards a Secure Trust Model for Vehicular Ad Hoc Networks Services. In Proceedings of the 2011 IEEE Global Telecommunications Conference (GLOBECOM 2011), Houston, TX, USA, 5–9 December 2011; pp. 1–5.
17. Liu, B.; Chiang, J.; Haas, J.; Hu, Y. Short paper: A practical view of "mixing" identities in vehicular networks. In *WiSec'11, Proceedings of the Fourth ACM Conference on Wireless Network Security*; ACM: New York, NY, USA, 2011; pp. 157–162.

18. Studer, A.; Shi, E.; Bai, F.; Perrig, A. TACKing Together Efficient Authentication, Revocation, and Privacy in VANETs. In Proceedings of the 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON'09), Rome, Italy, 22–26 June 2009; pp. 1–9.
19. Benin, J.; Nowatkowski, M.; Owen, H. Framework to Support Per Second Shifts of Pseudonyms in Regional VANETs. In Proceedings of the 2010 IEEE 72nd Vehicular Technology Conference, Fall (VTC 2010-Fall), Ottawa, ON, USA, 6–9 September 2010; pp. 1–5.
20. Lu, R.; Lin, X.; Luan, T.H.; Liang, X.; Shen, X. Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in VANETs. *IEEE Trans. Veh. Technol.* **2012**, *61*, 86–96.
21. Haas, J.J.; Hu, Y.-C.; Laberteaux, K.P. Design and analysis of a lightweight certificate revocation mechanism for VANET. In *Proceedings of VANET*; ACM: New York, NY, USA, 2009; pp. 89–98.
22. Raya, M.; Papadimitratos, P.; Aad, I.; Jungels, D.; Hubaux, J.-P. Eviction of misbehaving and faulty nodes in vehicular networks. *IEEE J. Sel. Areas Commun.* **2007**, *25*, 1557–1568.
23. Zhang, J. A Survey on Trust Management for VANETs. In Proceedings of the 2011 IEEE International Conference on Advanced Information Networking and Applications (AINA), Biopolis, Singapore, 22–25 March 2011; pp. 105–112, doi:10.1109/AINA.2011.86.
24. Wex, P.; Breuer, J.; Held, A.; Leinmuller, T.; Delgrossi, L. Trust Issues for Vehicular Ad Hoc Networks. In Proceedings of the Vehicular Technology Conference, 2008, Singapore, Singapore, 11–14 May 2008; pp. 2800–2804, doi:10.1109/VETECS.2008.611.
25. Kargl, F.; Papadimitratos, P.; Buttyan, L.; Muter, M.; Schoch, E.; Wiedersheim, B.; Thong, T.-V.; Calandriello, G.; Held, A.; Kung, A.; *et al*. Secure vehicular communication systems: Implementation, performance, and research challenges. *IEEE Commun. Mag.* **2008**, *46*, 110–118.
26. Zaidi, K.; Milojevic, M.; Rakocevic, V.; Rajarajan, M. Data-centric Rogue Node Detection in VANETs. In Proceedings of the 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Beijing, China, 24–26 September 2014; pp. 398–405.
27. Sampigethaya, K.; Huang, L.; Li, M.; Poovendran, R.; Matsuura, K.; Sezaki, K. CARAVAN: Providing location privacy for vanet. In Proceedings of the Workshop on Embedded Security in Cars (ESCAR), Cologne, Germany, 29–30 November 2005.
28. Ma, D.; Tsudik, G. Security and privacy in emerging wireless networks [Invited Paper]. *IEEE Wirel. Commun.* **2010**, *17*, 12–21.
29. Shamir, A. Identity-based cryptosystems and signature schemes. In *Advances in Crypto'84*; Lecture Notes in Computer Science; Springer-Verlag: Berlin, Germany; Heidelberg, Germany, 1984; Volume 196, pp. 47–53.
30. Shim, K. CPAS: An Efficient Conditional Privacy-Preserving Authentication Scheme for Vehicular Sensor Networks. *IEEE Trans. Veh. Technol.* **2012**, *61*, 1874–1883.
31. Lu, H.; Li, J.; Guizani, M. A Novel ID-based Authentication Framework with Adaptive Privacy Preservation for VANETs. In Proceedings of the Computing, Communications and Applications Conference (ComComAp), Hong Kong, China, 11–13 January 2012.
32. Zhang, C.; Lin, X.; Lu, R.; Ho, P. RAISE: An efficient RSU-aided message authentication scheme in vehicular communication networks. In Proceedings of the IEEE International Conference on Communications (ICC'08), Beijing, China, 19–23 May 2008; pp. 1451–1457.

33. Lu, R.; Lin, X.; Zhu, H.; Ho, P.H.; Shen, X. ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications. In Proceedings of the IEEE 27th Conference on Computer Communications, Phoenix, AZ, USA, 13–18 April 2008; pp. 1229–1237.
34. Dijiang, H.; Misra, S.; Verma, M.; Xue, G. PACP: An Efficient Pseudonymous Authentication-Based Conditional Privacy Protocol for VANETs. *IEEE Trans. Intell. Transp. Syst.* **2011**, *12*, 736–746.
35. Behrisch, M.; Bieker, L.; Erdmann, J.; Krajzewicz, D. Sumo-Simulation of Urban Mobility: An overview. In Proceedings of the SIMUL 2011, the 3rd International Conference on Advances in System Simulation, Barcelona, Spain, 23–29 October 2011; pp. 63–68.
36. Baguena, M.; Tornell, S.; Torres, A.; Calafate, C.; Cano, J.-C.; Manzoni, P. Vacamobil: Vanet car mobility manager for omnet++. In Proceedings of the 2013 IEEE International Conference on Communications Workshops (ICC), Budapest, Hungary, 9–13 June 2013; pp. 1057–1061.
37. Hafeez, K.A.; Zhao, L.; Ma, B.; Mark, J.W. Performance Analysis and Enhancement of the DSRC for VANET's Safety Applications. *IEEE Trans. Veh. Technol*. **2013**, *62*, 3069–3083.