sensors

MDPI

Article

Positioning Information Privacy in Intelligent Transportation Systems: An Overview and Future Perspective †

Aleksandr Ometov [1,*], Sergey Bezzateev [2], Vadim Davydov [3], Anna Shchesniak [3], Pavel Masek [4], Elena Simona Lohan [1] and Yevgeni Koucheryavy [1]

[1] Tampere University, 33720 Tampere, Finland; elena-simona.lohan@tuni.fi (E.S.L.); yk@cs.tut.fi (Y.K.)
[2] Saint-Petersburg State University of Aerospace Instrumentation (SUAI), St. Petersburg 190000, Russia; bsv@aanet.ru
[3] ITMO University, St. Petersburg 191002, Russia; vadim.davydov@niuitmo.ru (V.D.); anna.schesnyak@scaegroup.com (A.S.)
[4] Brno University of Technology, 60190 Brno, Czech Republic; masekpavel@vutbr.cz
* Correspondence: aleksandr.ometov@tuni.fi

† This paper is an expanded version of the conference paper: Davydov, V; Bezzateev, S. Secure Information Exchange in Defining the Location of the Vehicle. In Proceedings of the 41st IEEE International Conference on Telecommunications and Signal Processing (TSP), Athens, Greece, 4–6 July 2018.

Received: 25 February 2019; Accepted: 26 March 2019; Published: 3 April 2019

check for updates

Abstract: Today, the Intelligent Transportation Systems (ITS) are already in deep integration phase all over the world. One of the most significant enablers for ITS are vehicle positioning and tracking techniques. Worldwide integration of ITS employing Dedicated Short Range Communications (DSRC) and European standard for vehicular communication, known as ETSI ITS-G5, brings a variety of options to improve the positioning in areas where GPS connectivity is lacking precision. Utilization of the ready infrastructure, next-generation cellular 5G networks, and surrounding electronic devices together with conventional positioning techniques could become the solution to improve the overall ITS operation in vehicle-to-everything (V2X) communication scenario. Nonetheless, effective and secure communication protocols between the vehicle and roadside units should be both analyzed and improved in terms of potential attacks on the transmitted positioning-related data. In particular, said information might be misused or stolen at the infrastructure side conventionally assumed to be trusted. In this paper, we first survey different methods of vehicle positioning, which is followed by an overview of potential attacks on ITS systems. Next, we propose potential improvements allowing mutual authentication between the vehicle and infrastructure aiming at improving positioning data privacy. Finally, we propose a vision on the development and standardization aspects of such systems.

Keywords: Intelligent Transportation Systems; positioning; data privacy; authentication; GDPR

1. Introduction

Today, the technology is penetrating most of the modern digital systems [1]. Billions of interconnected devices are already deployed, and many would join them soon in the race towards smart interconnected world [2]. One of the promising paradigms is the utilization of Intelligent Transportation Systems (ITS), which is driven by one of the biggest markets being automotive [3]. The technologies covered by ITS are usually split into two major groups: vehicle-to-vehicle (V2V) [4,5] and vehicle-to-infrastructure (V2I) [6,7]. In an attempt to cover the challenges from both groups, a new trend called vehicle-to-everything (V2X) [8,9] has recently emerged, focusing on interconnecting cars with other surrounding objects.

Different standardization communities are already working hard to standardize the technological requirements, thus aiming for the same goal: to develop a unified ecosystem that would allow reliable, fast and secure communications between vehicles and roadside infrastructure. Such technologies as Dedicated Short Range Communications (DSRC) in the USA [10,11] and ETSI ITS-G5 in Europe [12,13] are actively developing aiming at being deployed in the oncoming decade. Moreover, DSRC has recently been selected as a V2X communications technology in the USA which means that all the newly produced cars would be equipped with a wireless IEEE 802.11p module [14] that could also be used for positioning tasks [15]. Japan is also actively involved in equipping the vehicles with DSRC aiming to have more than 100,000 operational by 2025 [16].

Previously, V2X development was not so widespread as smart cars were limited in numbers, highly priced and thus inaccessible to the majority of the world's population. In this paper, we will focus only on the vehicular positioning privacy in an urban scenario where a conventional Global Navigation Satellite System (GNSS) can be affected negatively by propagation in complex environments issues [17]. Nowadays, this problem becomes exceptionally significant due to the fast development of vehicle use delegation [18] in the car-sharing business [19,20].

Indeed, GNSSs proved themselves to be inefficient in urban-canyon operation scenario [21] also known as multipath interference phenomenon, caused by tall buildings blocking lines of sight (LOS) from the receiver to the navigation satellites. Some works have proven that no-line-of-sight (NLOS) signals could still be used for positioning if longer integration times and data wipe-off are present [22,23].

Many solutions were proposed to mitigate the challenges of efficient vehicle location determination. Simultaneously, operation in the city allows broad communication possibilities due to high coverage of various wireless technologies including conventional cellular and other heterogeneous techniques [24,25].

Overall, several radio-ranging-based cooperative positioning (CP) techniques were already proposed to enable vehicular localization in urban environment [26]. Nonetheless, the localization problem in conventional Mobile ad hoc networks (MANETs) with range measurements is often tackled by trilateration and multilateration to some fixed or mobile anchor nodes [27].

The internode distance is commonly measured using radio-ranging or range-rating techniques such as the time of arrival (TOA), time difference of arrival (TDOA), received signal strength (RSS), and other techniques [28]. The infrastructure in ITS provides the nodes not only with precise positions on the trusted infrastructure units but could also deliver regularly updated maps of the RSS based on the devices involved. Despite common V2I infrastructure nodes, the development of cellular networks beyond 5G would allow more precise positioning by utilizing specific synchronization signals with 5G New Radio (5G NR) even under high mobility constrains [29].

Since vehicular positioning mostly relies on the data provided by the Location Solution Provider (LSP), many concerns arise in regard to controlling personal information of the user [30]. Potential misuse of such sensitive data by LSP while user blindly agrees to the terms of use or even unauthorized tracking of the vehicle may occur when relying on the ITS positioning techniques. Note, that such situations appear even today and many security-related questions of said networks are still open [31]. For example, U.S.-based LocationSmart company was leaking the sensitive information about the positions of the smartphones operating under various cellular operators [32]. A similar case was reported earlier the same month by The New York Times, the service initially used to monitor calls from inmates and allowing to find almost any cell phone in the U.S. in seconds was misused [33]. Note, it is possible to uniquely identify the node based on just four hours of the monitoring while having access to the position-related data provider in 95% cases [34] based on said digital activity 'footprints' [35].

From the V2X positioning perspective, researchers have proposed a considerable number of privacy-preserving protocols for data exchange between the vehicle and the surrounding nodes [36]. Most of these protocols imply authentication of the vehicle to the trusted anchor nodes [37]. However, protocols without mutual authentication may be vulnerable to a wide range of attacks that should be carefully taken into consideration during the system development phase. The main contributions of this paper can be listed as:

1. an overview of existing privacy-related V2X solutions for infrastructure-based ITS systems;
2. a modified solution for data privacy enhancement based on well-known protocol;
3. a discussion of possible cybersecurity attacks on mentioned systems;
4. an overview of present standardization and General Data Protection Regulation (GDPR) related activities.

The rest of the paper is organized as follows. First, we survey the existing solutions for vehicular localization in Section 2. Next, we provide an overview of the protocols that utilize additional data from the environment/user to assist in locating the vehicle in Section 3. Further, we propose a simple extension to said protocols in Sections 3 and 4. Next, we elaborate on potential attacks on proposed architecture in Section 5. The last section provides future perspectives concerning standardization aspects and concludes the paper.

2. Solutions for Spotting of Vehicles on the Road

In this section, we consider several approaches for the localization techniques and the corresponding benefits and drawbacks. First, we list various potential ways to determine vehicle location with a simplified representation given in Figure 1.

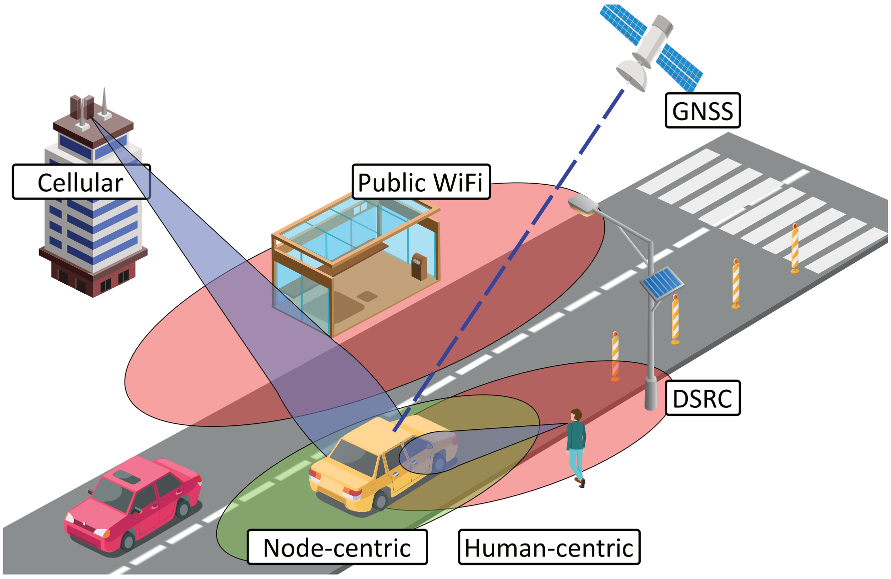

Figure 1. General example of vehicular positioning techniques.

2.1. Global Navigation Satellite Systems

One of the GNSSs is the Global Positioning System (GPS) which is a technology, network, and service owned and maintained by the USA [38]. The GPS service provides end-users with an opportunity to estimate their position and to retrieve globally synchronized time. Entire GPS architecture consists of space, control, and user segments [39]. The space segment is comprised of a constellation of 31 satellites (as of March, 2019), not including the decommissioned, on-orbit spares. GPS satellites operate in medium Earth orbit (MEO) at an altitude of approximately 20,200 km (11,550 miles) [40]. The GPS control segment is comprised of a global network of ground stations designed for tracking the constellation of satellites in MEO and also monitoring their transmissions, communicating and analyzing the data. The user segment consists of end users (civilian and military).

The second GNSS giant is the Russian Global Navigation Satellite System (GLONASS) which serves the same role despite some minor differences [41]. GLONASS satellite orbits are arrayed in three planes, separated from one another in right ascension of ascending node by 120 degrees, with eight satellites in each plane. The number of spacecraft is 26 including 24 actively operational ones (as of March, 2019), and the altitude is 19,100 km (11,868 miles) [42].

Finally, GNSS positioning technology widely used in the European Union is GALILEO starting 2005 [43]. GALILEO system currently has 26 operational satellites on the orbit placed in 3 orbital planes, at 29,600 km (18,400 miles) altitude [44]. Worth to note, the GNSS system specifically utilized in China–BeiDou Navigation Satellite System (BDS). BDS constellation currently has 17 operational satellites, and the number is expected to reach 35 by 2020 [45]. Nonetheless, most of the mass-produced vehicles are already equipped with both GPS and GLONASS systems [46].

The fundamental principle of using the GNSS system is to determine the location by measuring the timing of the reception of a synchronized signal from the navigation satellites [47,48]. Despite almost-the-entire-globe coverage, GNSS has a number of challenges that could not be neglected.

To start with, the material penetration characteristics limit the use of GNSS in hard-reach places such as underground parking, tunnels, etc. Next, because of the near-spherical shape of the Earth calculating an accurate distance between two points requires the use of spherical geometry and trigonometric math functions. However, many applications calculate an approximate distance using simplified ones. Thus, the GNSS-based calculation of the distance between two objects can lead to errors of 10 percent or more [49]. The most significant issue of the GNSS is its propagation in urban environments where multipath fading has a tremendously adverse effect on the position estimation.

2.2. Infrastructure-Based Methods

Some vehicles are already equipped with conventional IEEE 802.11 wireless modules commonly referred to as Wi-Fi. By using previously estimated maps together with sensed Received Signal Strength Indicator (RSSI) along with the Base Station (or access point) Identificator (BSID), the vehicle can approximate its location in the complex metropolitan environment, which is generally a challenging task for GNSS [50]. This methodology would be widely used in DSRC since all of the infrastructure nodes positions would be known forming a full map of BSIDs [51].

The main drawback of the technique is the need for continually updating the RSSI maps since the changes in the environment (such as new roads, new trees, new buildings, etc.) affect the RSSI, and Wi-Fi is operating in unlicensed spectrum affected by many interference sources. Therefore, the Wi-Fi network faces changes over time, and these changes need to be monitored continuously in order to rely on Wi-Fi positioning. Nonetheless, another drawback of using Wi-Fi for vehicular positioning is the lack of centralized infrastructures and the difficulty to achieve a high quality of positioning system, due to significant fluctuations in RSS of Wi-Fi APs. The advantage of using a Wi-Fi network is the possibility to serve in the metropolitan scenario with complex GNSS propagation characteristics, where GNSS is likely to fail. Similar issues could be encountered while utilizing any short-range wireless technology, such as Bluetooth Low Energy (BLE) [52] or Zigbee [53].

The other technique that could be utilized by smart cars is so-called cellular-positioning that has been used for localization of phones over the decades. Already in 2G, the Cell-ID-based positioning with accuracies on the order of a few hundred meters was feasible [54]. The efficiency was improved to tens of meters in 3G using TDOA measurements. Current cellular based-solutions also make use of Angle of Arrival (AOA) or combined AOA-TOA techniques [55].

2.3. 5G Communications as an Improvement for Positioning

The evolution of wireless communications brought us to the next frontier of positioning as well [30]. Moving towards higher millimeter wave (mmWave) frequencies (>6 GHz) as part of 5G NR systems networks pushes towards the utilization of highly directional antennas on both transmitter and receiver sides [56]. In mmWave frequencies higher than 30 GHz, the lower signal wavelength would allow for packing hundreds of antenna elements in a small area, enabling the implementation of highly directional beamforming capabilities, thus providing better spatial reuse and, consequently, better positioning [57]. In particular, it is achieved by utilizing massive Multiple Input Multiple Output (MIMO) technique [58]. 5G positioning for vehicular networks represents its separate niche or interest [59]. 5G NR is generally expected to provide an accurate positioning from a single reference base station (BS) also form multipath components of up to 0.5 m [60], which is especially beneficial for V2I scenarios.

2.4. Node-Centric Localization

This method enables non-instrumented vehicles to determine their locations by collecting data from neighboring vehicles through V2V direct communications, Light Detection and Ranging (LIDAR) techniques, radars, etc. The node-centric approach specifies the routing path as a sequence of connected nodes. Every vehicle has an opportunity to communicate and sense some or all of its neighbors as depicted in a Fog Internet of Vehicles paradigm [61].

As an example, to localize a vehicle among its neighbors, the authors in [62] propose a distributed algorithm that uses inter-vehicle distance estimates obtained via a radio-based ranging technology. There are two kinds of nodes involved, namely common nodes and beacon nodes; beacon nodes can determine their location, whereas common nodes are not location-aware. The localization process is based on the estimation of common nodes locations. This method is beneficial for hard-to-reach places, e.g., tunnels, underground parking. In [63,64], and in [65] the technologies of cooperative driving with automated vehicles and intervehicle communications are shown along with the corresponding benefits.

Despite actual communication devices utilizing mmWave band, radars open another prospect for vehicle localization, especially significant for autonomous driving since most of the vehicles of this type are already equipped with some LIDARs and radars. Trailblazing work [66] shows the benefits of utilizing a combination of mmWave radar together with static beacons as an indistinguishable replacement of the GNSS system. Authors in [67] proposed and proved that utilizing omnidirectional mmWave radar allows to reach 25 cm-level accuracy even under the effects of snowfall.

2.5. Human-Centric Localization

Human-centric localization is targeted at people carrying gadgets [68,69]. As soon as a person starts to approach the vehicle, a gadget (smartphone, smartwatch, or augmented reality glasses) is changing the state to pre-authentication phase [70]. From telecommunications perspective, the enablers for such authentication are already present in current 3GPP LTE deployments [71] and ProSe service responsible for handling those as part of Device-to-Device (D2D) communications [72]. Therefore, the preliminary connection establishment could be automatically detected by the vehicle, and the last known location of the hand-held device could be utilized to improve the positioning of the vehicle.

There have been numerous studies focusing on human-vehicle interaction ways of driver identification using sitting postures were investigated in [73], the interaction between a human and a vehicle is described in [74], and authors provide an overview of the importance of human-vehicle interaction in autonomous vehicles in [75].

As positive aspects, we can distinguish the high accuracy in location determination owing to the availability of base station cell IDs and, consequently, the availability of data for calculation of the approximate vehicle location [76]. On the other hand, this method is highly dependent on the actual availability of devices, e.g., device utilization might become impossible due to insufficient battery power.

2.6. Verifiable Multilateration

Generally, verifiable multilateration is a technique based on the measurement of the difference in distance between two or more stations at known locations by broadcast signals at known times. Recently, researchers have proposed a number of positioning and distance estimation techniques in [63,77]. This method requires to install a set of base stations controlled by a central authority, for example, a cellular or Low-Power Wide-Area Wireless Technology (LPWA) operator. If the base stations can uniquely compute the vehicle location using these distance bounds, and if this location falls into the triangular pyramid formed between the verifiers, then they conclude that the vehicle location is correct. Equivalently, only three verifiers are needed to define the vehicle location in two dimensions; the verifiers still consider the location correct if it can be uniquely computed and if it falls in the triangle formed between them [63].

This approach poses a number of problems, namely:

- Simultaneous reception: In this method, the vehicle communicates with at least three base stations in order to obtain its current coordinates. Certainly, in the real world, it is impossible to get three signals perfectly synchronized.
- Security: In the communication process, it is vital not to allow the attacker to receive the transmitted data. In [78,79] the potential cyber-attacks specific to automated vehicles are investigated. Therefore, it is necessary to provide a secure transfer of information between the station and the vehicle.
- Confidence or trustability of the access nodes: Before transmitting the information, it is required to ensure that the base station is trustworthy valid by employing mutual authentication. Some of the approaches to mutual authentication were described in [80,81]. This problem could also be addressed with conventional role-based models [82].
- Anonymity: In some situations, the base station is not supposed to obtain any information about the vehicle, neither the identification nor the location. In this paper, we show several protocols fulfilling mobile node anonymity requirement.

3. Vehicle Location Protocols Using Additional Information

Previously listed methods allow for the design of an effective hybrid system meeting the necessary security requirements and being both accurate and fast in determining the location [83]. A number of experiments have already been carried out, proving the benefits of such utilization [84,85].

The grouping could be done as following. As for the first strategy, we assume having 'beacon' and 'common' nodes in the system. The modification is such that the beacon node is a node where a passenger with a smartphone is present. Furthermore, the smartphone can identify the location more accurately due to cellular signal presence. Common nodes are the nodes where the smartphone does not transmit any information about the location. In this case, the beacon nodes are polled to receive it. At the same time, all vehicles monitor their surroundings for infrastructure units and corresponding RSSI values. The protocol execution example is shown in Figure 2 for a beacon node and a common node.

A beacon vehicle has a GNSS receiver and a list of available infrastructure access points (APs). At this moment, a common node is location-unaware. Hence it requests the beacon node for a list of available infrastructure APs. In the reply, the beacon node also transmits an approximate location in addition to requested data.

Indeed, the positioning techniques as we know them today are relying on their own collected location data. The systems of tomorrow would also rely on neighbors and infrastructure thus moving the information security aspects to an entirely new level.

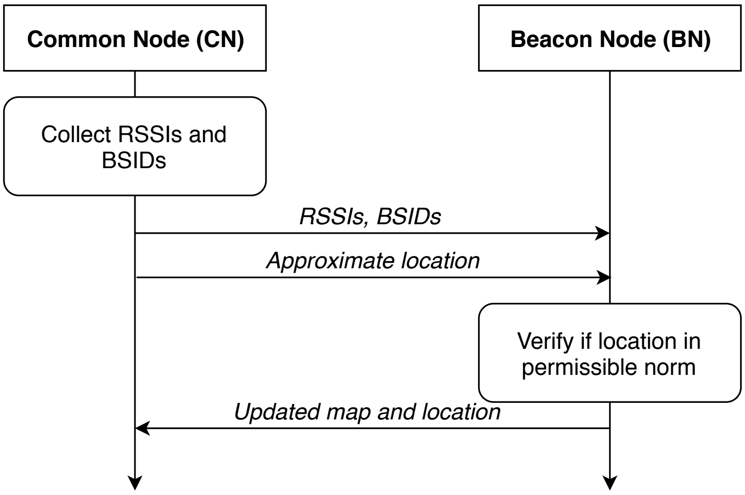

Figure 2. An illustration of communication between common and beacon nodes.

In this section, we consider possible protocols for data exchange between a vehicle not possessing reliable location information and its surrounding roadside elements and other traffic participants carrying location data. The crucial feature of these protocols is the presence or absence of anonymity of the vehicle requesting location information. The anonymity of the request for location is an essential property of the protocol, and its availability requires significant complication of the protocol. The anonymity in this work is considered as the process of 'hiding' the actual vehicle location. Generally, the localization process could be viewed as follows.

- First, the 'indirect' distance to the static trusted nodes obtained from the known units (cellular or infrastructure units) is estimated. Mutual authentication also takes place during this phase.
- Next, the distances are utilized to estimate the location of the node through classical geometry by, for example, triangulation.

We further list the potential options for securely executing the first phase.

Distance Determination without Anonymity

In 2004, authors proposed a distance-bounding protocol in [86], we further refer to it as protocol P-04. The action here is performed between V—the vehicle, and S—the base station. Key constructs utilized by this work are given in Table 1. The protocol is shown in Figure 3.

Table 1. Key constructs utilized in this work.

Construct	Description
V	Target vehicle
S	Target base station
N_V, N'_V, N_S	Random nonces
$h(x)$	Hashing function
id_x	Unique identification number
K_{VS}	Pairwise symmetric key
$sig_{K_{VS}}(x)$	Signature by K_{VS}
d_{VS}	Distance between nodes
t_{VS}	Time between message exchange
σ	Delay in response to the base station
$\overline{t_{VS}}$	Miscalculated time of passing the signal
$F(x)$	Homomorphic transformation

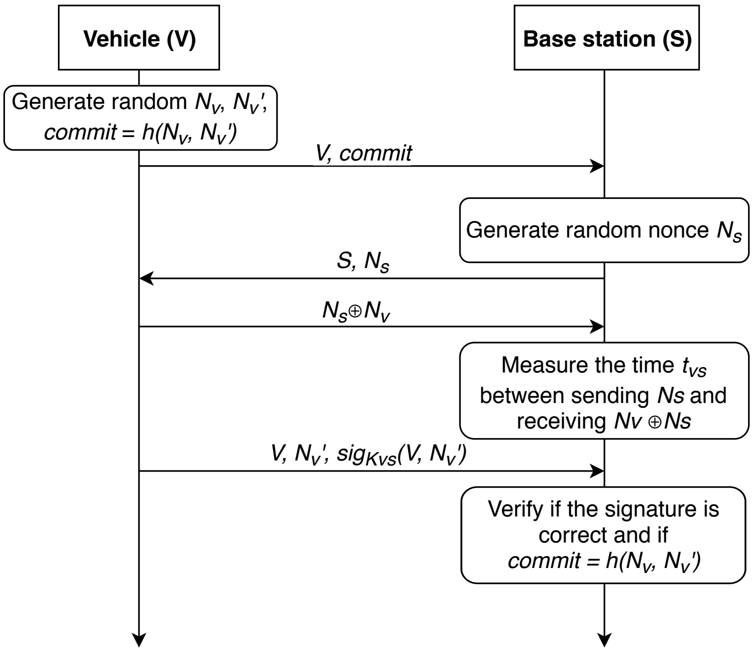
Vehicle (V)
Base station (S)
Generate random N_V, N_V', $commit = h(N_V, N_V')$
V, commit
Generate random nonce N_S
S, N_S
$N_S \oplus N_V$
Measure the time t_{VS} between sending Ns and receiving $Nv \oplus Ns$
V, N_V', $sig_{Kvs}(V, N_V')$
Verify if the signature is correct and if $commit = h(N_V, N_V')$

Figure 3. The distance-bounding protocol P-04 [86].

First, a shared symmetric key must be generated between the vehicle and the infrastructure node for secure exchange of information. Key generation algorithm depends on the computing power modules installed in the vehicle and base station. Now, it is presumed that such a link has already been established and the data exchange between the station and the vehicle takes place via the secure medium. It is also presumed that a shared symmetric key was delivered after the devices have established a secure link employing, for example, the well-known Diffie-Hellmann protocol. Thus, common pairwise key K_{VS} could be utilized for the message authentication for both vehicle and BS. Basically, we state that correct deciphering of $e = E_{K_{VS}}(m)$ and obtaining m is only feasible for the vehicle and the BS.

The first step of the protocol for determining the distance between the base station and the vehicle is the generation of two random nonces (N_V, N_V'). Next, it in necessary to calculate their hash function h (*commit*) on the vehicle side and to send the result to the infrastructure. In turn, the BS generates one nonce (N_S) and sends it to V. The vehicle must calculate $N_S \oplus N_V$ and return it.

The key point of the protocol is that S measures the time between sending N_S and receiving $N_S \oplus N_V$. Using this time, the infrastructure can estimate the distance d_{VS} to the vehicle. After that, V communicates with the base station, sending the identification number *id*, N_V' and the signature of *id* and N_V', using their pairwise symmetric key K_{VS}. Base station S verifies if the signature and $commit = h(N_V, N_V')$ are correct. If all checks are correct, the base station considers the distance d_{VS} computed at the previous step to be reliable. Further, the received value d_{VS} can either be sent to the vehicle or used on a dedicated server to calculate the vehicle's location.

In 2006, this protocol was improved in [63], further referred as P-06 protocol. The modified strategy is shown in Figure 4. In this improved version of the protocol, only the last two steps were modified. V sends encrypted information, its *id* number, N_S and N_V' with the symmetric key K_{VS}. S decrypts the message and verifies if $commit = h(N_V, N_V')$.

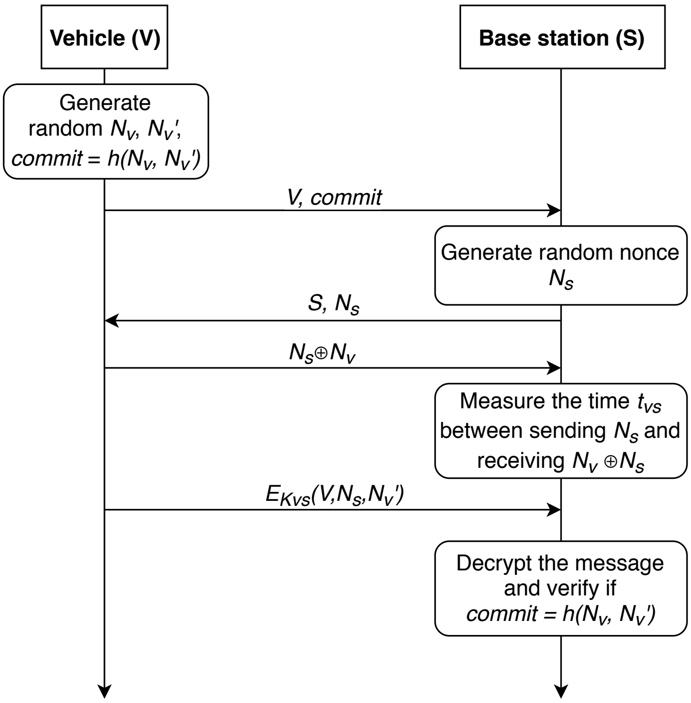
Vehicle (V)
Base station (S)
Generate random N_V, N_V', *commit* = $h(N_V, N_V')$
V, commit
Generate random nonce N_S
S, N_S
$N_S \oplus N_V$
Measure the time t_{VS} between sending N_S and receiving $N_V \oplus N_S$
$E_{Kvs}(V, N_S, N_V')$
Decrypt the message and verify if *commit* = $h(N_V, N_V')$

Figure 4. An improved distance-bounding P-06-M protocol.

Carrying out a XOR operation imposes extra computational cost; to address this problem, we propose to modify the protocol slightly. Proposed modification is shown in Figure 5 and detailed in [87].

This modification eliminates the necessity for XOR calculation. Should both the vehicle and the infrastructure node require to determine vehicle location, an extra step can be added to the protocol, namely, as $S \rightarrow V : E_{K_{VS}}(t_{VS}, N_V)$.

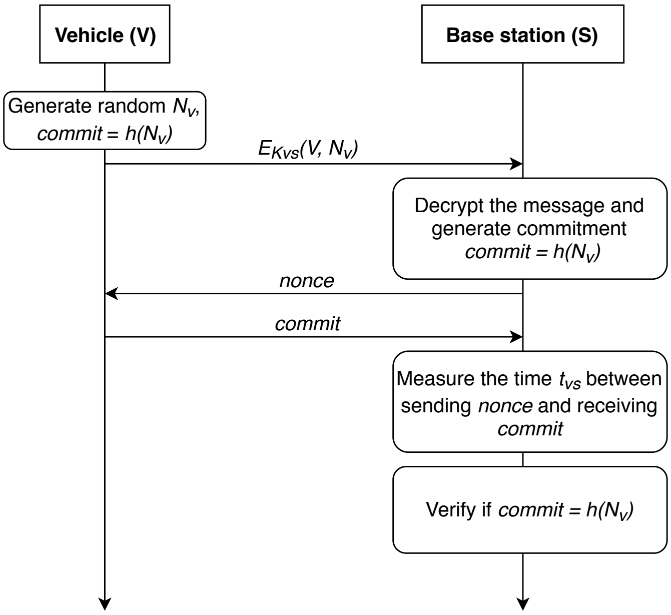
Vehicle (V)
Base station (S)
Generate random N_V, *commit* = $h(N_V)$
$E_{Kvs}(V, N_V)$
Decrypt the message and generate commitment *commit* = $h(N_V)$
nonce
commit
Measure the time t_{VS} between sending *nonce* and receiving *commit*
Verify if *commit* = $h(N_V)$

Figure 5. Potential improvement of distance-bounding protocol.

The above-listed protocols assume that the vehicle is a location-unaware data transmission initiator. We note that discussed protocols suggest vehicle authentication via Public Key Infrastructure, while mutual authentication is not present. The protocols should be improved to allow mutual authentication since a malicious BS attack could be executed, thus compromising the localization process. We propose our improvement in the next section.

4. Location Determination with Mutual Base Station Authentication

Next, we consider the modification of the described protocol that allows for ensuring the anonymity of the vehicle while determining the distance to the base station, further referred as P-AF-BS protocol and shown in Figure 6.

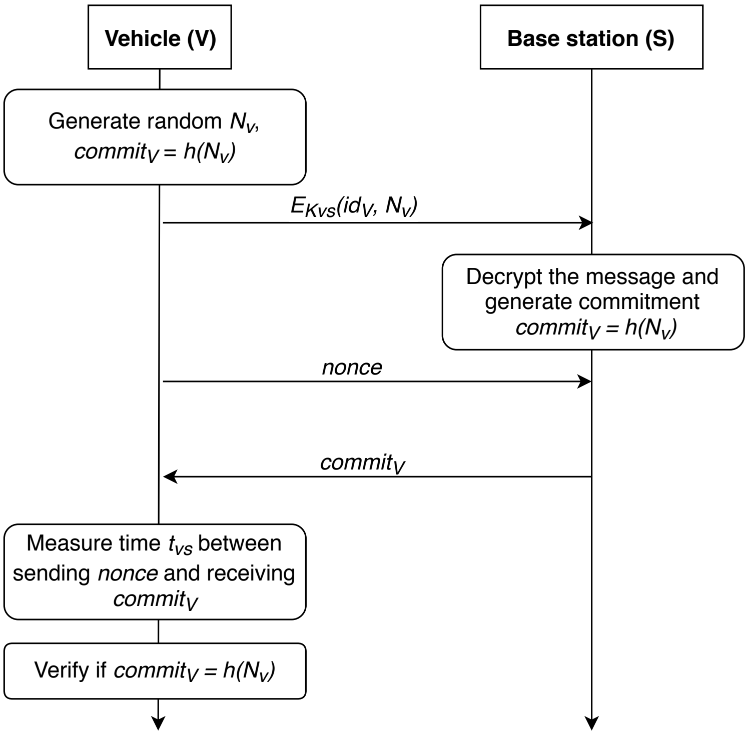
Vehicle (V)
Base station (S)
Generate random N_V, $commit_V = h(N_V)$
$E_{Kvs}(id_V, N_V)$
Decrypt the message and generate commitment $commit_V = h(N_V)$
nonce
$commit_V$
Measure time t_{VS} between sending *nonce* and receiving $commit_V$
Verify if $commit_V = h(N_V)$

Figure 6. Distance-bounding protocol with base station authentication.

In the previous section, we discussed the protocols for vehicle-to-base station communication by transferring the corresponding vehicle *id* and location, yet this approach is vulnerable to a number of security issues. An attacker controlling a malicious BS could gain access to the localization of any vehicle, control its movement, or deceive the vehicle by transmitting the wrong distance, which might lead to unpleasant consequences. Security of such a protocol might be significantly improved by not allowing the base station access to precise vehicle location. There are two possible ways of delivering this improvement:

- The distance is calculated on the side of the vehicle, all the operations are performed in a special secure computing module;
- The distance is calculated on the side of the base station, while the vehicle actions are limited to sending requests and receiving answers.

4.1. Vehicle-Centered Approach

First, we consider the case where the calculation is carried out on the vehicle side. In this case, the vehicle needs to contact at least three BSs, calculate the time of the signal traveling to the base station, and then, using verifiable multilateration method [63], calculate its coordinates. The P-AF-V protocol for exchanging information with the base station is shown in Figure 7.

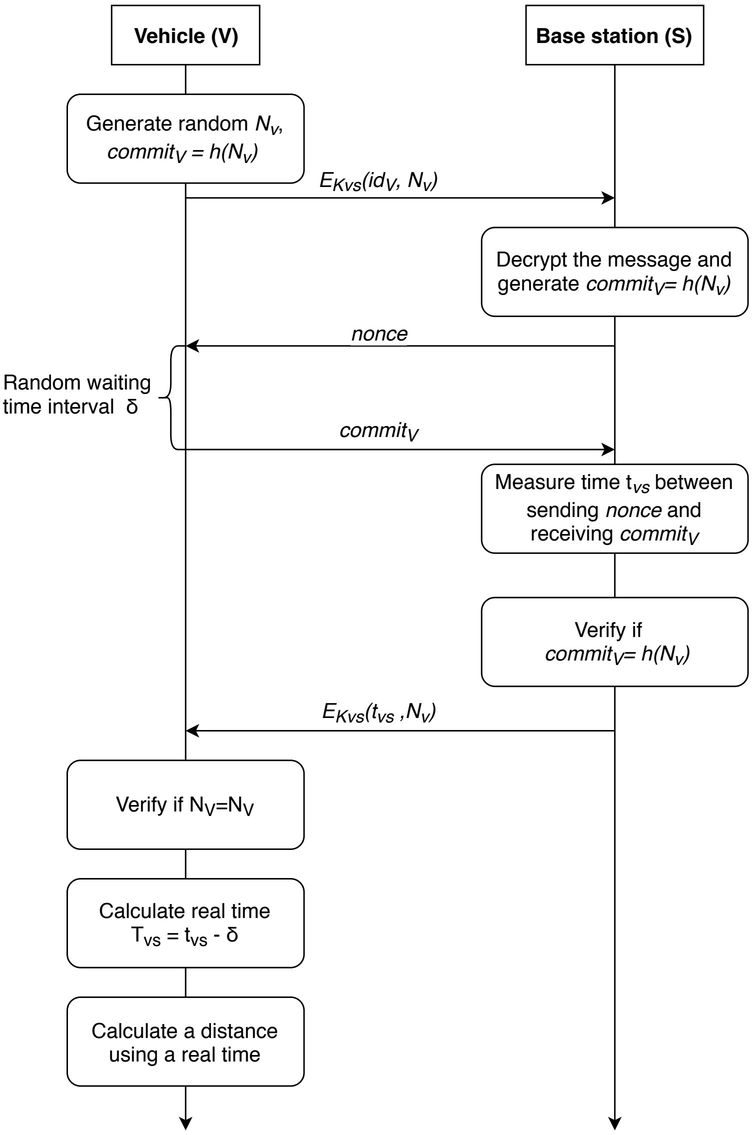
Vehicle (V)
Base station (S)
Generate random N_v, $commit_V = h(N_v)$
$E_{Kvs}(id_V, N_v)$
Decrypt the message and generate $commit_V = h(N_v)$
nonce
Random waiting time interval δ
$commit_V$
Measure time t_{VS} between sending nonce and receiving $commit_V$
Verify if $commit_V = h(N_v)$
$E_{Kvs}(t_{vs}, N_v)$
Verify if $N_V = N_V$
Calculate real time $T_{vs} = t_{vs} - \delta$
Calculate a distance using a real time

Figure 7. A distance-bounding P-AF-V protocol with the property of anonymity (calculations are made on the vehicle side).

After receiving the message *nonce* from the base station, the vehicle chooses a random number δ, which determines the delay in response to the base station, waits for this time interval and sends a *commitment* message to the base station afterwards. Thus, the base station does not know the random delay time chosen by the vehicle and, therefore, does not have an ability to determine the real time t_{VS} of the signal passing to the vehicle and back.

Accordingly, the station transmits its miscalculated time of passing the signal $\overline{t_{VS}} = t_{VS} + \delta$ to the vehicle, which can, in turn, calculate the real time of the signal passing through it $t_{VS} = \overline{t_{VS}} - \delta$. It is worth noting that the vehicle must quickly obtain information from at least three different stations, calculate the distance to a particular station, and then calculate the coordinates.

4.2. Protocols of the Distance Determination Which Have the Property of Anonymity

Now, we will consider the protocol where the calculation is carried out at the station side. The corresponding protocol is shown in Figure 8.

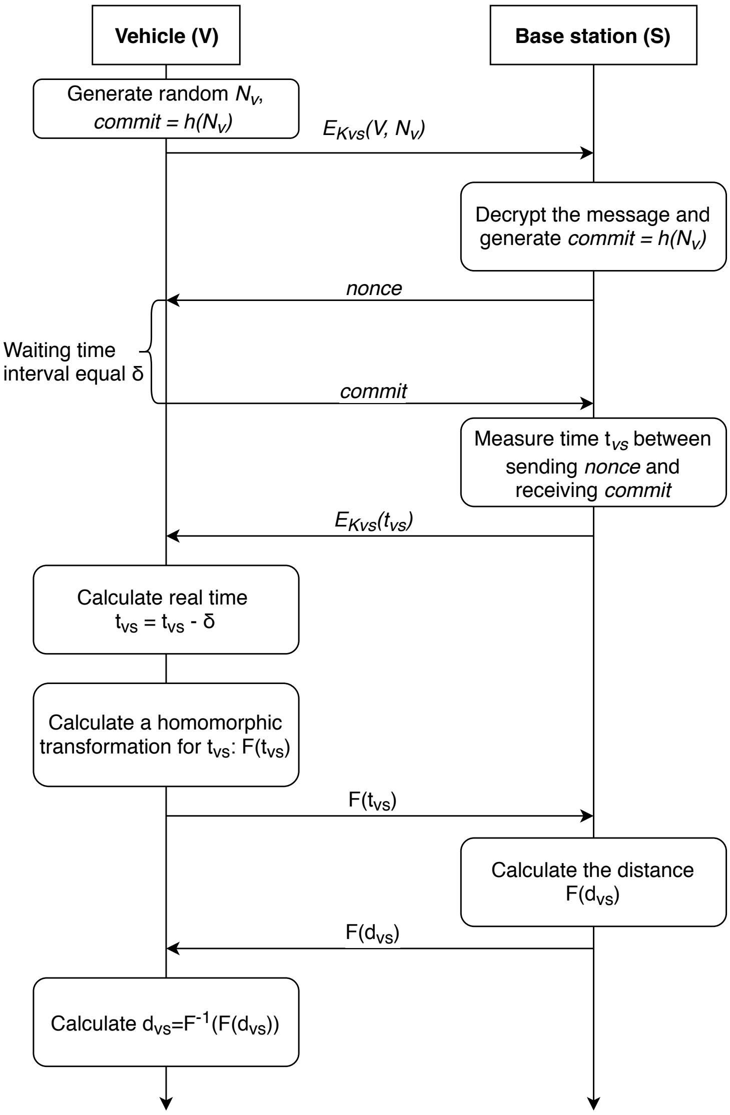
Vehicle (V)
Base station (S)
Generate random N_v, *commit* = $h(N_v)$
$E_{Kvs}(V, N_v)$
Decrypt the message and generate *commit* = $h(N_v)$
nonce
Waiting time interval equal δ
commit
Measure time t_{vs} between sending *nonce* and receiving *commit*
$E_{Kvs}(t_{vs})$
Calculate real time $t_{vs} = t_{vs} - δ$
Calculate a homomorphic transformation for t_{vs}: $F(t_{vs})$
$F(t_{vs})$
Calculate the distance $F(d_{vs})$
$F(d_{vs})$
Calculate $d_{vs}=F^{-1}(F(d_{vs}))$

Figure 8. A distance-bounding P-AF-BS protocol with the property of anonymity (calculations are made on the base station side).

In this protocol, we use a fully homomorphic encryption (FHE) [88]. This technique is detailed in [89,90]. We repeat all the steps (excluding the last one) from the protocol of vehicle-side distance calculation, shifting this calculation to the side of the base station. Further, sending the result of the homomorphic transformation $F(t_{VS})$ to the base station, where the distance to the vehicle is calculated, or using the information received from other stations, its location is determined, the value $F(d_{VS})$ or the result of a homomorphic transformation of the coordinates of the car. After this, the received information is delivered to the vehicle. The use of a homomorphic transformation obfuscates the true values of t_{VS} from the base station, and the vehicle determines the true value of the distance to a particular station or its location in this case. This allows for avoiding complex calculations at the vehicle side, shifting the calculation workload to the BS side.

Here, we compare the discussed protocols and also elaborate on the improved one. Further on, n—is a message length; λ—the system security parameter. Let's consider our protocols and estimate three factors: number of operations, the storage space, and the complexity of the calculations as: Random number generation—$O(1)$; Transmission—$O(1)$; Hashing, Encryption

(MD5)—$O(n)$ [91]; Signature—$O(n)$ [91]; Verification—$O(n)$ [91]; Measurement—$O(n)$ [92]; Calculation (subtraction)—$O(log(n))$ [92]; XOR—$O(n)$ [93]; and Homomorphic encryption—$O(\lambda^{3.5})$ [94].

From the Table 2 it can be seen that the less computationally expensive protocol is the improved distance-bounding one because there are less operations, as it is shown in Figure 9, and only one random nonce is stored. Of course, the last proposed protocol is the most difficult one which is mainly due to the introduced anonymity improvement.

Table 2. The complexity evaluation.

Protocol	Storage Space	Complexity
Protocol-2004 (P-04)	2 random nonces; Hash value	$5O(n) + 8O(1)$
Protocol-2006 (P-06)	2 random nonces; Hash value; Symmetric keys	$5O(n) + 8O(1)$
Modified Protocol-2006 (P-06-M)	Random nonce; Hash value; Symmetric keys	$5O(n) + 5O(1)$
BS-based anonymity-focused protocol (P-AF-BS)	Random nonce; Hash value; Symmetric keys; Interval sigma	$9O(n) + 7O(1)$
Vehicle-based anonymity-focused protocol (P-AF-V)	Random nonce; Hash value; Symmetric keys; Interval sigma	$2O(\lambda^{3.5}) + 10O(n) + 9O(1)$

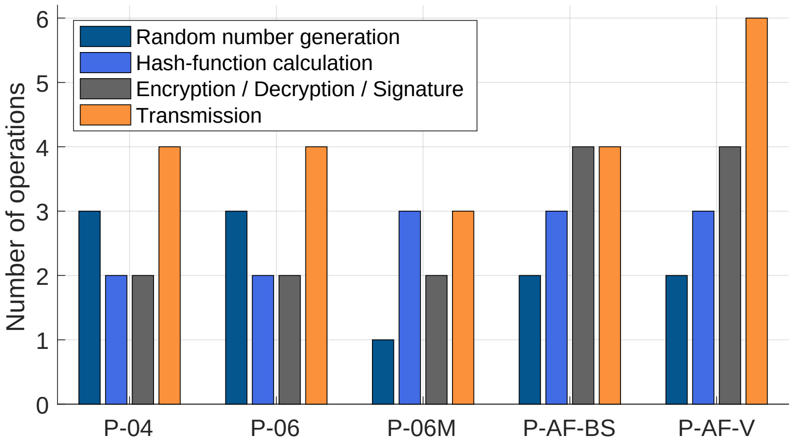

Figure 9. Number of different operations required per protocol.

5. Related Security and Privacy Threats

In this section, we list the attacks explicitly dangerous for location data exchange with another nodes. Note, we further elaborate not only on the attacks explicitly related to the exchange of the data between the vehicle and infrastructure node.

Attackers are mainly focusing on two main sides while penetrating ITS systems. First, to get unauthorized access based on weaknesses in social engineering and/or physical protection of infrastructure elements and onboard controllers. Second, to exploit the design of the security protocols and communications mainly in terms of message modification or replaying previously received messages [95]. Most of the attacks today are solved with Trusted Platform Module (TPM)-based protection, identity-based cryptography, and short-lived key certificates.

5.1. Security Threats

Conventional and Infrastructure-Related Attacks

Man-in-the-middle attack (MITM): (today also referred to as person-in-the-middle attack) is an active attack where an eavesdropper can intercept and modify fully or partly the positioning signaling between two vehicles or between a vehicle and the terrestrial infrastructure used for positioning, such as cellular signaling [96]. Increasing the security and authentication of the data signaling protocols is one solution to mitigate this attack type.

Replay attack: This attack is similar to the previous one. Here, the attacker can replay the messages traveling between vehicles or vehicles and infrastructure thus affecting the correctness of the positioning itself instead [97].

Sybil Node (Rogue AP): This attack and hardware/software unauthorized modifications are another active attacks, where BS or AP would transmit intentionally erroneous positioning-related data [98]. To cope with this attack type, outlier detection mechanisms need to be used [99].

Jamming attack: The attacker can be either a stationary or a moving jammer. Given the nature of the mobility of the vehicular networks, it is rational to have a moving jammer that tracks the desired node and causes regular interference. Utilizing spread spectrum techniques could assist in addressing this attack. As one of the options, the Frequency Hopping Spread Spectrum (FHSS) makes the incoherent signal period impulse-noise to the eavesdroppers. On the other hand, Direct Sequence Spread Spectrum (DSSS) symbolizes each data bit in the original signal by multiple bits in the transmitted signal [100] which is also a recommended technique to resist jamming.

Passive Eavesdropping attack: In this type of passive attack, an attacker can listen to the positioning signaling between two vehicles or between a vehicle and the infrastructure [101]. If the positioning signaling channel is strongly encrypted – this type of attack may be mitigated.

Message modification attack: This attack is targeted at altering the message during or after transmission (active attack) [102]. The adversary may wish to change the source or content of the message in terms of the position or time information that had been sent and saved in its device, in order to escape the consequences of a criminal/car accident event.

Key and/or Certificate Replication: This attack involves the system endorsement with a node of similar identity. The execution of the attack relies on the key management or certificates replacement, in order to forbid the identification and abuse the authorities [103].

While most of the security threats could be mitigated by employing the integration of stronger information security systems, privacy-related attacks could not be overcome by mere modifying the hardware/software side of the system.

Attacks Related to Distributed Operation

Congestion attacks: Generally, urban traffic congestion is considered as one of the major problems from the vehicular systems' operation perspective. Modern cars are already available to report the congestion-related data either with integrated wireless modules or via hand-held user devices. Focusing on the first case, Vehicular Ad-Hoc Networks (VANETs) can provide timely information to the surrounding nodes which result in more effective route selection (around a sudden traffic jam) using the information obtained from other cars. From the information security perspective, the V2V radio connectivity of autonomous vehicles will offer attackers opportunities to combine multiple compromised vehicles into botnets of cars, which will lead to other serious security consequences [104].

From the infrastructure perspective, such attacks may potentially lead to incorrect traffic light signaling. As a result, the optimization algorithm running in the ITS cloud may operate based on the incorrect data, leading to congestion [95].

Repudiation attacks: This attack is an example of adequately tracking and recording the user actions, which can maliciously manipulate or fake the identification of new nodes [105]. This attack is used to modify the user's information about the actions performed by the malicious and to register false data in log files. It can also be used to manipulate the master data in a similar pattern involving the messages. If this attack takes place, the data stored in the log files may be considered invalid or misleading.

Routing Loop Attack: In this type of attack, an internal attacker receives a message, updates it and sends it back to one of the previous forwarders (or the source) even if there is a better node in its routing table that is available to be the next forwarder according to the routing strategy. This attack aims to delay or prevent the delivery of a message [106]. The primary countermeasure against routing-related attacks is by utilizing Intruder Detection techniques and excluding the node from the network [107].

Sinkhole Attack: In this type of routing attack, the attacker (already being in the system, i.e., an internal one) attempts to announce the nodes in the network with a different location in its beacon messages followed by drops of any other packets [108]. It results in the poisoning of the routing tables and packet loss. The attacker may also be intellectual and analyze the captured packets while conventional one just affects the overall system operation in a harmful way.

Wormhole Attack: This type of routing attack corresponds to cases of two terminals having a link in between and they resend messages received by one of them to another [109]. Therefore, they can dominate on the routing path by replaying the valid beacons from other nodes. Attackers tend to dominate the connection so they can eavesdrop or share the network.

5.2. Privacy Threats

Unauthorized use of location data and location-based services: This threat could be considered as unauthorized use of tolled highways pretending to have a position of a neighbor vehicle which is not situated on a highway or unauthorized access in a car park [110].

Disclosure of unwanted information: As an example, consider a case such as if a person leaving the house empty for a long trip by car or by boat (which may enable house burglaries); how often an employee, supposed to be at the office, is visiting places by car (which may lead to loss of social reputation); how often a spouse is visiting places that he/she has never mentioned to his/her relatives (which may cause family crises), etc.

Tracking malware applications: A vehicle-installed software could contain malware to "steal" the tracking patterns of the users inside the vehicle, i.e., the user positions and speeds in time; such information, if sold to car dealers, could adversely affect the price of a vehicle, e.g., in function of the types of roads where vehicle and how often it was driven, etc.

Scrambler attack: An additional measure to achieve a higher level of anonymity in vehicular systems is the utilization of dynamically changing identifiers (from MAC to application layer), so-called pseudonyms [111]. The effectiveness of this approach, however, is clearly reduced if specific characteristics of the physical layer (e.g., in the transmitted signal) reveal the link between two messages with different pseudonyms. In contrast to other physical layer fingerprinting methods, it does not rely on potentially fragile features of the channel or the hardware but exploits the transmitted scrambler state that each receiver has to derive in order to decode a packet, making this attack extremely robust. The most straightforward solution is to employ a cryptographic pseudo-random number generator, possibly seeded by a large number of entropy sources in a vehicle (e.g., engine start time, sensors data, SNR, vehicles nearby, etc.). Another solution is the deployment of constant network-wide scrambler values.

As compared to security threats, privacy issues always had more involvement by the actual humans. One option to improve privacy in ITS systems is to utilize the solutions with strong anonymity properties [112,113] or frequently changing pseudonyms [114]. Some researchers foresee that Software-defined networking (SDN) will become an ultimate enabler for overcoming previously listed security and privacy problems of ITS [115,116] supporting both V2V and V2I scenarios.

6. Discussion and Future Perspectives

This section provides an overview of the future development of privacy strategies in positioning from EU regulations perspective in addition to conclusions of this work.

Recently introduced General Data Protection Regulation (GDPR) policy broadly states that *profiling* and processing the location information of an individual could be done concerning personal aspects which are naturally related to person's movement and location data. According to [117], it could be done only when EU law regulations or the Member States demands or allows it, or "with the explicit consent of the data subject." Thus, tracking and monitoring the data of the user's vehicle also falls within this regulation. However, the definition of *personal location* data should be treated more carefully especially for cases when the *identifiability* of the said individual could be established. This way, the GDPR aspects related to the protection of personal data also should be taken into consideration while operating with personal location data.

In the ITS case and focusing on conventional GNSS systems, all the supported systems are controlled by the authorities, namely military for GPS and GLONASS and, in contrast, civilian Galileo in EU, which makes the implementation of GDPR more complicated. In order to overcome this issue, European Telecommunications Institute (ETSI) is actively developing a standard EN 303 413 [118] aiming to overcome the interoperability of those systems. However, the corresponding questions remain unclear from the telecommunications side especially while speaking about 5G [119]. Moreover, location-related data may be stored in the environments potentially not controlled by the operators themselves [120].

Industrial giants, such as Huawei, already rise the question on how to address the challenges of private positioning in future networks [121]. One of the fundamental principles to be followed is by following the GDPR Article 25, i.e., to implement a privacy-by-design approach to achieve privacy from the commencement of the system perspective.

Aiming to achieve the above-mentioned, we have shown different location estimation techniques for ITS scenario in this paper. We analyzed the existing protocols for the information exchange between the vehicle and the base station during the localization process. Subsequently, we presented an improved protocol for the data exchange, where much attention was paid to the security of signaling information transmission. Using the modified protocol, the vehicle can also rely on the location data without disclosing the identity, and thus the privacy could be generally improved.

In real life, the selection of the protocol highly depends on the application needs. If the system architect wants to have maximum anonymity, it is recommended to utilize the modified protocol, but it is the most difficult one for implementation. The optimal option is to use a protocol with a property of anonymity but BS-based. The complexity is not much higher compared to others, and there are no complex operations.

Author Contributions: Conceptualization, S.B., V.D., P.M. and A.S.; methodology, S.B. and V.D.; software, V.D.; validation, A.O., P.M. and A.S.; formal analysis, E.S.L.; investigation, A.S.; resources, A.O.; writing—original draft preparation, S.B. and V.D.; writing—review and editing, A.O., A.S., P.M. and E.S.L.; visualization, A.O.; supervision, S.B., E.S.L. and Y.K.; project administration, S.B. and A.O.; funding acquisition, S.B., E.S.L. and Y.K.

Funding: This work was supported by the Academy of Finland (project #313039—PRISMA) and the work of the second author is supported by the Academy of Finland under a personal grant. The described research was also supported by the National Sustainability Program under grant LO1401. The described research was partially financed by the Ministry of Industry and Trade of Czech Republic project No. FV20487.

Acknowledgments: For the research, the infrastructure of the SIX Center was used.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

Abbreviations

The following abbreviations are used in this manuscript:

5G	5th generation cellular networks
AOA	Angle of Arrival
AP	Access Point
BDS	BeiDou Navigation Satellite System
BLE	Bluetooth Low Energy
BSID	Base station identificator
CP	Cooperative positioning
DSRC	Dedicated Short Range Communications
DOS	Denial of Service Attack
D2D	Device-to-Device communications
EN	European Union
ETSI	European Telecommunications Institute
FHE	Fully homomorphic encryption
GNSS	Global Navigation Satellite System
GDPR	General Data Protection Regulation
GPS	Global Positioning System
ITS	Intelligent Transportation Systems
ITS-G5	Intelligent Transport Systems operating in the 5 GHz frequency band
LoS	Lines of sight
LPWA	Low-Power Wide-Area Wireless Technology
LSP	Location Solution Provider
LIDAR	Light Detection and Ranging
MANET	Mobile ad hoc network
MEO	Medium Earth orbit
MITM	Man-in-the-middle attack
MIMO	Multiple Input Multiple Output
NR	New radio
RSS	Received signal strength
RSSI	Received signal strength indicator
TDOA	Time difference of arrival
TPM	Trusted Platform Module
TOA	Time of arrival
VANET	Vehicular Ad-Hoc Network
V2I	Vehicle-to-infrastructure paradigm
V2V	Vehicle-to-vehicle paradigm
V2X	Vehicle-to-everything paradigm
XOR	Exclusive OR operation

References

1. Aijaz, A.; Dohler, M.; Aghvami, A.H.; Friderikos, V.; Frodigh, M. Realizing the Tactile Internet: Haptic Communications over Next Generation 5G Cellular Networks. *IEEE Wirel. Commun.* **2017**, *24*, 82–89. [CrossRef]
2. Cisco. Visual Networking Index: Global Mobile Data Traffic Forecast Update 2017–2022. 2019. Available online: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-738429.html (accessed on 1 April 2019).
3. Menouar, H.; Guvenc, I.; Akkaya, K.; Uluagac, A.S.; Kadri, A.; Tuncer, A. UAV-enabled Intelligent Transportation Systems for the Smart City: Applications and Challenges. *IEEE Commun. Mag.* **2017**, *55*, 22–28. [CrossRef]

4. Lin, D.; Kang, J.; Squicciarini, A.; Wu, Y.; Gurung, S.; Tonguz, O. MoZo: A Moving Zone Based Routing Protocol Using Pure V2V Communication in VANETs. *IEEE Trans. Mob. Comput.* **2017**, *16*, 1357–1370. [CrossRef]
5. Vinel, A.; Lyamin, N.; Isachenkov, P. Modeling of V2V Communications for C-ITS Safety Applications: A CPS Perspective. *IEEE Commun. Lett.* **2018**, *22*, 1600–1603. [CrossRef]
6. Zhang, F.; Xi, J.; Langari, R. Real-time Energy Management Strategy Based on Velocity Forecasts Using V2V and V2I Communications. *IEEE Trans. Intell. Transp. Syst.* **2017**, *18*, 416–430. [CrossRef]
7. Dey, K.C.; Rayamajhi, A.; Chowdhury, M.; Bhavsar, P.; Martin, J. Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) Communication in a Heterogeneous Wireless Network–Performance Evaluation. *Transp. Res. Part C Emerg. Technol.* **2016**, *68*, 168–184. [CrossRef]
8. Lee, K.; Kim, J.; Park, Y.; Wang, H.; Hong, D. Latency of Cellular-based V2X: Perspectives on TTI-Proportional Latency and TTI-Independent Latency. *IEEE Access* **2017**, *5*, 15800–15809. [CrossRef]
9. Seo, H.; Lee, K.D.; Yasukawa, S.; Peng, Y.; Sartori, P. LTE Evolution for Vehicle-to-Everything Services. *IEEE Commun. Mag.* **2016**, *54*, 22–28. [CrossRef]
10. Wang, Y.; Duan, X.; Tian, D.; Chen, M.; Zhang, X. A DSRC-Based Vehicular Positioning Enhancement Using a Distributed Multiple-Model Kalman Filter. *IEEE Access* **2016**, *4*, 8338–8350. [CrossRef]
11. Abboud, K.; Omar, H.A.; Zhuang, W. Interworking of DSRC and Cellular Network Technologies for V2X Communications: A Survey. *IEEE Trans. Veh. Technol.* **2016**, *65*, 9457–9470. [CrossRef]
12. ETSI. *Intelligent Transport Systems (ITS); Access Layer Specification for Intelligent Transport Systems Operating in the 5 GHz Frequency Band*; Draft ETSI EN 302 663 V1.2.0; ETSI: Valbonne, France, 2012.
13. Deinlein, T.; German, R.; Djanatliev, A. Evaluation of Single-Hop Beaconing with Congestion Control in IEEE WAVE and ETSI ITS-G5. In Proceedings of the International Conference on Measurement, Modelling and Evaluation of Computing Systems, Erlangen, Germany, 26–28 February 2018; pp. 273–282.
14. FierceWireless. DSRC Mandate Moving off the Table for Automakers. 2017. Available online: https://www.fiercewireless.com/wireless/report-dsrc-mandate-moving-off-table-for-auto-makers (accessed on 1 April 2019).
15. Li, J.; Cui, X.; Li, Z.; Liu, J. Method to Improve the Positioning Accuracy of Vehicular Nodes Using IEEE 802.11p Protocol. *IEEE Access* **2018**, *6*, 2834–2843. [CrossRef]
16. Engadget. Most of Toyota's Cars Will Talk to Each Other by 2025. 2017. Available online: https://www.engadget.com/2018/04/16/toyota-vehicle-to-vehicle-communications/ (accessed on 1 April 2019).
17. Wang, L.; Groves, P.D.; Ziebart, M.K. Multi-Constellation GNSS Performance Evaluation for Urban Canyons Using Large Virtual Reality City Models. *J. Navig.* **2012**, *65*, 459–476. [CrossRef]
18. Ometov, A.; Bezzateev, S.; Kannisto, J.; Harju, J.; Andreev, S.; Koucheryavy, Y. Facilitating the Delegation of Use for Private Devices in the Era of the Internet of Wearable Things. *IEEE Internet Things J.* **2017**, *4*, 843–854. [CrossRef]
19. Bardhi, F.; Eckhardt, G.M. Access-based Consumption: The Case of Car Sharing. *J. Consum. Res.* **2012**, *39*, 881–898. [CrossRef]
20. Dmitrienko, A.; Plappert, C. Secure Free-floating Car Sharing for Offline Cars. In Proceedings of the 7th ACM on Conference on Data and Application Security and Privacy, Scottsdale, AZ, USA, 22–24 March 2017; pp. 349–360.
21. Cui, Y.; Ge, S.S. Autonomous Vehicle Positioning with GPS in Urban Canyon Environments. *IEEE Trans. Robot. Autom.* **2003**, *19*, 15–25.
22. Wang, L.; Groves, P.D.; Ziebart, M.K. Shadow Matching: Improving Smartphone GNSS Positioning in Urban Environments. In *China Satellite Navigation Conference (CSNC)*; Springer: Berlin/Heidelberg, Germany, 2013; pp. 613–621.
23. Douglas, I.J. Improving GPS Global Navigation Accuracy for Connected Vehicles in an Urban Canyon. Ph.D. Thesis, University of Windsor, Windsor, ON, Canada, 2016.
24. del Peral-Rosado, J.; Saloranta, J.; Destino, G.; López-Salcedo, J.; Seco-Granados, G. Methodology for Simulating 5G and GNSS High-Accuracy Positioning. *Sensors* **2018**, *18*, 3220. [CrossRef] [PubMed]
25. Kumar, D.; Saloranta, J.; Kaleva, J.; Destino, G.; Tölli, A. Reliable Positioning and mmWave Communication via Multi-Point Connectivity. *Sensors* **2018**, *18*, 4001. [CrossRef]
26. Soatti, G.; Nicoli, M.; Garcia, N.; Denis, B.; Raulefs, R.; Wymeersch, H. Implicit Cooperative Positioning in Vehicular Networks. *arXiv* **2017**, arXiv:1709.01282.

27. Han, G.; Jiang, J.; Zhang, C.; Duong, T.Q.; Guizani, M.; Karagiannidis, G.K. A Survey on Mobile Anchor Node Assisted Localization in Wireless Sensor Networks. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 2220–2243. [CrossRef]
28. Mahmoud, A.; Noureldin, A.; Hassanein, H.S. VANETs Positioning in Urban Environments: A Novel Cooperative Approach. In Proceedings of the 82nd Vehicular Technology Conference (VTC Fall), Boston, MA, USA, 6–9 September 2015; pp. 1–7.
29. Talvitie, J.; Levanen, T.; Koivisto, M.; Pajukoski, K.; Renfors, M.; Valkama, M. Positioning of High-speed Trains Using 5G New Radio Synchronization Signals. *arXiv* **2018**, arXiv:1805.01830.
30. Lohan, E.S.; Alén-Savikko, A.; Chen, L.; Järvinen, K.; Leppäkoski, H.; Kuusniemi, H.; Korpisaari, P. 5G Positioning: Security and Privacy Aspects. In *A Comprehensive Guide to 5G Security*; John Wiley & Sons Ltd.: Hoboken, NJ, USA, 2018; p. 281.
31. Kalinin, M.; Krundyshev, V.; Zegzhda, P.; Belenko, V. Network Security Architectures for VANET. In Proceedings of the 10th International Conference on Security of Information and Networks, Jaipur, India, 13–15 October 2017; pp. 73–79.
32. WIRED Media Group. Website Leaked Real-time Location of Most US Cell Phones to Almost Anyone. 2018. Available online: https://arstechnica.com/information-technology/2018/05/service-leaked-locations-of-us-cell-phones-for-free-no-password-required/ (accessed on 1 April 2019).
33. The New York Times. Service Meant to Monitor Inmates' Calls Could Track You, Too. 2018. Available online: https://www.nytimes.com/2018/05/10/technology/cellphone-tracking-law-enforcement.html (accessed on 1 April 2019).
34. De Montjoye, Y.A.; Hidalgo, C.A.; Verleysen, M.; Blondel, V.D. Unique in the Crowd: The Privacy Bounds of Human Mobility. *Sci. Rep.* **2013**, *3*, 1376. [CrossRef] [PubMed]
35. NBCUniversal Media. Your Phone May Be Tracking Your Every Move. 2017. Available online: https://www.nbclosangeles.com/news/local/Smartphone-Location-Tracking-423054644.html (accessed on 1 April 2019).
36. Sui, P.; Li, X.; Bai, Y. A Study of Enhancing Privacy for Intelligent Transportation Systems: *k*-Correlation Privacy Model Against Moving Preference Attacks for Location Trajectory Data. *IEEE Access* **2017**, *5*, 24555–24567. [CrossRef]
37. Chen, C.L.; Chiang, M.L.; Peng, C.C.; Chang, C.H.; Sui, Q.R. A Secure Mutual Authentication Scheme with Non-Repudiation for Vehicular Ad Hoc Networks. *Int. J. Commun. Syst.* **2017**, *30*, e3081. [CrossRef]
38. Liu, K.; Lim, H.B.; Frazzoli, E.; Ji, H.; Lee, V.C. Improving positioning accuracy using GPS pseudorange measurements for cooperative vehicular localization. *IEEE Trans. Veh. Technol.* **2014**, *63*, 2544–2556. [CrossRef]
39. Hegarty, C.J. The Global Positioning System (GPS). In *Springer Handbook of Global Navigation Satellite Systems*; Springer: Cham, Switzerland, 2017; pp. 197–218.
40. U.S. Coast Guard Navigation Center. GPS Contallation Status. 2019. Available online: https://www.navcen.uscg.gov/?Do=constellationStatus (accessed on 1 April 2019).
41. Li, X.; Ge, M.; Dai, X.; Ren, X.; Fritsche, M.; Wickert, J.; Schuh, H. Accuracy and Reliability of Multi-GNSS Real-time Precise Positioning: GPS, GLONASS, BeiDou, and Galileo. *J. Geod.* **2015**, *89*, 607–635. [CrossRef]
42. Information and Analysis Center for Positioning, Navigation and Timing. GLONASS contallation Status. 2019. Available online: https://www.glonass-iac.ru/en/GLONASS/ (accessed on 1 April 2019).
43. Nurmi, J.; Lohan, E.S.; Sand, S.; Hurskainen, H. *GALILEO Positioning Technology*; Springer: Dordrecht, The Netherlands, 2015; Volume 176.
44. European GNSS Service Center. GALILEO Contallation Status. 2019. Available online: https://www.gsc-europa.eu/system-status/orbital-and-technical-parameters (accessed on 1 April 2019).
45. Sun, F.; Liu, S.; Zhu, X.; Men, B. Research and Progress of Beidou Satellite Navigation System. *Sci. China Inf. Sci.* **2012**, *55*, 2899–2907. [CrossRef]
46. Angrisano, A.; Gaglione, S.; Gioia, C. Performance Assessment of GPS/GLONASS Single Point Positioning in an Urban Environment. *Acta Geod. Geophys.* **2013**, *48*, 149–161. [CrossRef]
47. Renfro, B.A.; Terry, A.; Boeker, N. *An Analysis of Global Positioning System (GPS) Standard Positioning System (SPS) Performance for 2015*; Technical Report; Space and Geophysics Laboratory, Applied Research Laboratories, The University of Texas at Austin: Austin, TX, USA, 2017.
48. Specht, C.; Mania, M.; Skóra, M.; Specht, M. Accuracy of the GPS Positioning System in the Context of Increasing the Number of Satellites in the Constellation. *Polish Marit. Res.* **2015**, *22*, 9–14. [CrossRef]

49. Meridian World Data, Inc. Distance Calculation. 2018. Available online: http://www.meridianworlddata.com/distance-calculation/ (accessed on 1 April 2019).
50. Laitinen, E.; Lohan, E.S.; Talvitie, J.; Shrestha, S. Access Point Significance Measures in WLAN-based Location. In Proceedings of the 9th Workshop on Positioning Navigation and Communication (WPNC), Dresden, Germany, 15–16 March 2012; pp. 24–29.
51. Ma, S.; Lee, H.; Cheng, H. A Positioning Accuracy Enhancement Method Based on Inter-Vehicular Communication and Self-Organizing Map. In Proceedings of the International Conference on Information and Communication Technology Convergence (ICTC), Jeju, Korea, 17–19 October 2018; pp. 748–753.
52. Llorca, D.F.; Quintero, R.; Parra, I.; Sotelo, M. Recognizing Individuals in Groups in Outdoor Environments Combining Stereo Vision, RFID and BLE. *Clust. Comput.* **2017**, *20*, 769–779. [CrossRef]
53. Lei, Y.; Wang, T.; Wu, J. Vehicles Relative Positioning Based on ZigBee and GPS Technology. In Proceedings of the 6th International Conference on Electronics Information and Emergency Communication (ICEIEC), Beijing, China, 17–19 June 2016; pp. 59–62.
54. Sivers, M.; Fokin, G. LTE Positioning Accuracy Performance Evaluation. In Proceedings of the Conference on Smart Spaces, St. Petersburg, Russia, 26–28 August 2015; pp. 393–406.
55. Koivisto, M.; Costa, M.; Hakkarainen, A.; Leppanen, K.; Valkama, M. Joint 3D Positioning and Network Synchronization in 5G Ultra-Dense Networks Using UKF and EKF. In Proceedings of the Globecom Workshops (GC Wkshps), Washington, DC, USA, 4–8 December 2016; pp. 1–7.
56. Halvarsson, B.; Simonsson, A.; Elgcrona, A.; Chana, R.; Machado, P.; Asplund, H. 5G NR Testbed 3.5 GHz Coverage Results. In Proceedings of the 87th Vehicular Technology Conference (VTC Spring), Porto, Portugal, 3–6 June 2018; pp. 1–5.
57. Rastorgueva-Foi, E.; Costa, M.; Koivisto, M.; Leppänen, K.; Valkama, M. User Positioning in mmW 5G Networks using Beam-RSRP Measurements and Kalman Filtering. *arXiv* **2018**, arXiv:1803.09478.
58. Liu, Y.; Shi, X.; He, S.; Shi, Z. Prospective Positioning Architecture and Technologies in 5G Networks. *IEEE Netw.* **2017**, *31*, 115–121. [CrossRef]
59. Wymeersch, H.; Seco-Granados, G.; Destino, G.; Dardari, D.; Tufvesson, F. 5G mmWave Positioning for Vehicular Networks. *IEEE Wirel. Commun.* **2017**, *24*, 80–86. [CrossRef]
60. Wymeersch, H.; Garcia, N.; Kim, H.; Seco-Granados, G.; Kim, S.; Went, F.; Fröhle, M. 5G mm Wave Downlink Vehicular Positioning. In Proceedings of the Global Communications Conference (GLOBECOM), Abu Dhabi, United Arab Emirates, 9–13 December 2018, pp. 206–212.
61. Kang, J.; Yu, R.; Huang, X.; Zhang, Y. Privacy-Preserved Pseudonym Scheme for Fog Computing Supported Internet of Vehicles. *IEEE Trans. Intell. Transp. Syst.* **2018**, *19*, 2627–2637. [CrossRef]
62. Parker, R.; Valaee, S. Vehicle Localization in Vehicular Networks. In Proceedings of the 64th Vehicular Technology Conference (VTC), Montreal, QC, Canada, 25–28 September 2006; pp. 1–5.
63. Capkun, S.; Hubaux, J.P. Secure Positioning of Wireless Devices with Application to Sensor Networks. In Proceedings of the 24th Annual Joint Conference of the IEEE Computer and Communications Societies, Miami, FL, USA, 13–17 March 2005; Volume 3, pp. 1917–1928.
64. Johnson, D.B.; Maltz, D.A. Dynamic Source Routing in Ad Hoc Wireless Networks. In *Mobile Computing*; Springer: Boston, MA, USA, 1996; pp. 153–181.
65. Kato, S.; Tsugawa, S.; Tokuda, K.; Matsui, T.; Fujii, H. Vehicle Control Algorithms for Cooperative Driving with Automated Vehicles and Intervehicle Communications. *IEEE Trans. Intell. Transp. Syst.* **2002**, *3*, 155–161. [CrossRef]
66. Clark, S.; Durrant-Whyte, H. Autonomous Land Vehicle Navigation Using Millimeter Wave Radar. In Proceedings of the International Conference on Robotics and Automation, Leuven, Belgium, 16–20 May 1998; Volume 4, pp. 3697–3702.
67. Yoneda, K.; Hashimoto, N.; Yanase, R.; Aldibaja, M.; Suganuma, N. Vehicle Localization Using 76GHz Omnidirectional Millimeter-Wave Radar for Winter Automated Driving. In Proceedings of the Intelligent Vehicles Symposium (IV), Changshu, China, 26–30 June 2018; pp. 971–977.
68. Sánchez-Carmona, A.; Robles, S.; Borrego, C. PrivHab+: A Secure Geographic Routing Protocol for DTN. *Comput. Commun.* **2016**, *78*, 56–73. [CrossRef]
69. Bou Abdo, J.; Bourgeau, T.; Demerjian, J.; Chaouchi, H. Extended Privacy in Crowdsourced Location-based Services Using Mobile Cloud Computing. *Mob. Inf. Syst.* **2016**, *2016*, 7867206. [CrossRef]

70. Ometov, A.; Petrov, V.; Bezzateev, S.; Andreev, S.; Koucheryavy, Y.; Gerla, M. Challenges of Multi-Factor Authentication for Securing Advanced IoT (A-IoT) Applications. *arXiv* **2019**, arXiv:1901.06977.
71. Cui, X.; Gulliver, T.A.; Song, H.; Li, J. Real-time Positioning Based on Millimeter Wave Device to Device Communications. *IEEE Access* **2016**, *4*, 5520–5530. [CrossRef]
72. Lin, X.; Andrews, J.G.; Ghosh, A.; Ratasuk, R. An Overview of 3GPP Device-to-Device Proximity Services. *IEEE Commun. Mag.* **2014**, *52*, 40–48. [CrossRef]
73. Riener, A.; Ferscha, A. Supporting Implicit Human-to-Vehicle Interaction: Driver Identification from Sitting Postures. In Proceedings of the 1st Annual International Symposium on Vehicular Computing Systems (ISVCS), Dublin, Ireland, 22–24 July 2008; p. 10.
74. Lu, Z.; de Winter, J.C. A Review and Framework of Control Authority Transitions in Automated Driving. *Procedia Manuf.* **2015**, *3*, 2510–2517. [CrossRef]
75. Dunbar, J.; Gilbert, J.E. The Human Element in Autonomous Vehicles. In Proceedings of the International Conference on Engineering Psychology and Cognitive Ergonomics, Vancouver, BC, Canada, 9–14 July 2017; pp. 339–362.
76. Campos, R.S. Evolution of Positioning Techniques in Cellular Networks, from 2G to 4G. *Wirel. Commun. Mob. Comput.* **2017**, *2017*, 2315036. [CrossRef]
77. Esteves, J.S.; Carvalho, A.; Couto, C. Generalized Geometric Triangulation Algorithm for Mobile Robot Absolute Self-localization. In Proceedings of the IEEE International Symposium on Industrial Electronics, Rio de Janeiro, Brazil, 9–11 June 2003; Volume 1, pp. 346–351.
78. Larson, U.E.; Nilsson, D.K. Securing Vehicles Against Cyber Attacks. In Proceedings of the 4th Annual Workshop on Cyber Security and Information Intelligence Research: Developing Strategies to Meet the Cyber Security and Information Intelligence Challenges Ahead, Oak Ridge, TN, USA, 12–14 May 2008; p. 30.
79. Petit, J.; Shladover, S.E. Potential Cyberattacks on Automated Vehicles. *IEEE Trans. Intell. Transp. Syst.* **2015**, *16*, 546–556. [CrossRef]
80. Dolev, S.; Krzywiecki, Ł.; Panwar, N.; Segal, M. Vehicle Authentication via Monolithically Certified Public Key and Attributes. *Wirel. Netw.* **2016**, *22*, 879–896. [CrossRef]
81. Zhang, C.; Lin, X.; Lu, R.; Ho, P.H. RAISE: An Efficient RSU-aided Message Authentication Scheme in Vehicular Communication Networks. In Proceedings of the International Conference on Communications, Beijing, China, 19–23 May 2008; pp. 1451–1457.
82. Kalinin, M.; Krundyshev, V.; Rezedinova, E.; Zegzhda, P. Role-based Access Control for Vehicular adhoc Networks. In Proceedings of the International Black Sea Conference on Communications and Networking (BlackSeaCom), Batumi, Georgia, 4–7 June 2018; pp. 1–5.
83. del Peral-Rosado, J.A.; Raulefs, R.; López-Salcedo, J.A.; Seco-Granados, G. Survey of Cellular Mobile Radio Localization Methods: From 1G to 5G. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 1124–1148. [CrossRef]
84. Qian, C.; Xu, H.; Li, P.; Wang, Y. Design and Implementation of Urban Vehicle Positioning System Based on RFID, GPS and LBS. In Proceedings of the Conference on Complex, Intelligent, and Software Intensive Systems, Turin, Italy, 10–13 July 2017; pp. 599–608.
85. Rohani, M.; Gingras, D.; Gruyer, D. A Novel Approach for Improved Vehicular Positioning Using Cooperative Map Matching and Dynamic Base Station DGPS Concept. *IEEE Trans. Intell. Transp. Syst.* **2016**, *17*, 230–239. [CrossRef]
86. Hubaux, J.P.; Capkun, S.; Luo, J. The Security and Privacy of Smart Vehicles. *IEEE Secur. Priv.* **2004**, *2*, 49–55. [CrossRef]
87. Davydov, V.; Bezzateev, S. Secure Information Exchange in Defining the Location of the Vehicle. In Proceedings of the 41st International Conference on Telecommunications and Signal Processing (TSP), Athens, Greece, 4–6 July 2018; pp. 1–5.
88. Brakerski, Z.; Vaikuntanathan, V. Efficient Fully Homomorphic Encryption from (Standard) LWE. *SIAM J. Comput.* **2014**, *43*, 831–871. [CrossRef]
89. Rohilla, A.; Khurana, M.; Singh, L. Location Privacy using Homomorphic Encryption over Cloud. *Int. J. Comput. Netw. Inf. Secur.* **2017**, *9*, 32. [CrossRef]
90. Alanwar, A.; Shoukry, Y.; Chakraborty, S.; Martin, P.; Tabuada, P.; Srivastava, M. PrOLoc: Resilient Localization with Private Observers Using Partial Homomorphic Encryption. In Proceedings of the 16th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN), Pittsburgh, PA, USA, 18–21 April 2017; pp. 41–52.

91. Rachmawati, D.; Tarigan, J.; Ginting, A. A Comparative Study of Message Digest 5 (MD5) and SHA256 Algorithm. *J. Phys. Conf. Ser.* **2018**, *978*, 012116. [CrossRef]
92. Guerzhoy, M. Complexity of Aarithmetic Operations. 2018. Available online: https://www.cs.toronto.edu/~guerzhoy/180/lectures/W11/lec1/ComplArithm.html (accessed on 1 April 2019).
93. Montanaro, A.; Osborne, T. On the Communication Complexity of XOR Functions. *arXiv* **2009**, arXiv:0909.3392.
94. Armknecht, F.; Boyd, C.; Carr, C.; Gjøsteen, K.; Jäschke, A.; Reuter, C.A.; Strand, M. A Guide to Fully Homomorphic Encryption. *IACR Cryptol. ePrint Arch.* **2015**, *2015*, 1192.
95. Ta, V.T.; Dvir, A.; Arie, Y. Securing Road Traffic Congestion Detection by Incorporating V2I Communications. In Proceedings of the 19th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM), Chania, Greece, 12–15 June 2018; pp. 1–6.
96. Al-Kahtani, M.S. Survey on Security Attacks in Vehicular Ad hoc Networks (VANETs). In Proceedings of the 6th International Conference on Signal Processing and Communication Systems (ICSPCS), Gold Coast, QLD, Australia, 12–14 December 2012; pp. 1–9.
97. Capkun, S.; Hubaux, J.P. Secure Positioning in Wireless Networks. *IEEE J. Sel. Areas Commun.* **2006**, *24*, 221–232. [CrossRef]
98. Yu, B.; Xu, C.Z.; Xiao, B. Detecting Sybil Attacks in VANETs. *J. Parallel Distrib. Comput.* **2013**, *73*, 746–756. [CrossRef]
99. Li, X.; Li, Z.; Han, J.; Lee, J.G. Temporal Outlier Detection in Vehicle Traffic Data. In Proceedings of the 25th International Conference on Data Engineering, Shanghai, China, 29 March–2 April 2009; pp. 1319–1322.
100. Mokhtar, B.; Azab, M. Survey on Security Issues in Vehicular Ad Hoc Networks. *Alex. Eng. J.* **2015**, *54*, 1115–1126. [CrossRef]
101. Mahajan, S.; Jindal, A. Security and Privacy in VANET to Reduce Authentication Overhead for Rapid Roaming Networks. *Int. J. Comput. Appl.* **2010**, *1*, 21–25. [CrossRef]
102. 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.
103. 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. [CrossRef]
104. Garip, M.T.; Gursoy, M.E.; Reiher, P.; Gerla, M. Congestion Attacks to Autonomous Cars Using Vehicular Botnets. In Proceedings of the NDSS Workshop on Security of Emerging Networking Technologies (SENT), San Diego, CA, USA, 8 February 2015.
105. Smitha, A.; Pai, M.M.; Ajam, N.; Mouzna, J. An Optimized Adaptive Algorithm for Authentication of Safety Critical Messages in VANET. In Proceedings of the 8th International Conference on Communications and Networking in China (CHINACOM), Guilin, China, 14–16 August 2013; pp. 149–154.
106. Alsharif, N.; Wasef, A.; Shen, X. Mitigating the Effects of Position-based Routing Attacks in Vehicular Ad Hoc Networks. In Proceedings of the International Conference on Communications (ICC), Kyoto, Japan, 5–9 June 2011; pp. 1–5.
107. Erritali, M.; El Ouahidi, B. A Review and Classification of Various VANET Intrusion Detection Systems. In Proceedings of the National Security Days (JNS3), Rabat, Morocco, 26–27 April 2013; pp. 1–6.
108. Sirola, P.; Joshi, A.; Purohit, K.C. An Analytical Study of Routing Attacks in Vehicular Ad-Hoc Networks (VANETs). *Int. J. Comput. Sci. Eng.* **2014**, *3*, 210–218.
109. Hasrouny, H.; Samhat, A.E.; Bassil, C.; Laouiti, A. VANET Security Challenges and Solutions: A Survey. *Veh. Commun.* **2017**, *7*, 7–20. [CrossRef]
110. Simic, M.N. Vehicular Ad Hoc Networks. In Proceedings of the 11th International Conference on Telecommunication in Modern Satellite, Cable and Broadcasting Services (TELSIKS), Nis, Serbia, 16–19 October 2013; Volume 2, pp. 613–618.
111. Bloessl, B.; Sommer, C.; Dressier, F.; Eckhoff, D. The Scrambler Attack: A Robust Physical Layer Attack on Location Privacy in Vehicular Networks. In Proceedings of the International Conference on Computing, Networking and Communications (ICNC), Garden Grove, CA, USA, 16–19 February 2015; pp. 395–400.
112. Gedik, B.; Liu, L. Protecting Location Privacy with Personalized k-anonymity: Architecture and Algorithms. *IEEE Trans. Mob. Comput.* **2008**, *7*, 1–18. [CrossRef]
113. Artail, H.; Abbani, N. A Pseudonym Management System to Achieve Anonymity in Vehicular Ad Hoc Networks. *IEEE Trans. Dependable Secure Comput.* **2016**, *13*, 106–119. [CrossRef]

114. Gerlach, M.; Guttler, F. Privacy in VANETs Using Changing Pseudonyms-Ideal and Real. In Proceedings of the 65th Vehicular Technology Conference, Dublin, Ireland, 22–25 April 2007; pp. 2521–2525.
115. Kalinin, M.; Zegzhda, P.; Zegzhda, D.; Vasiliev, Y.; Belenko, V. Software Defined Security for Vehicular ad hoc Networks. In Proceedings of the International Conference on Information and Communication Technology Convergence (ICTC), Jeju, Korea, 19–21 Octber 2016; pp. 533–537.
116. Di Maio, A.; Palattella, M.; Soua, R.; Lamorte, L.; Vilajosana, X.; Alonso-Zarate, J.; Engel, T. Enabling SDN in VANETs: What is the Impact on Security? *Sensors* **2016**, *16*, 2077. [CrossRef] [PubMed]
117. European Parliament and Council of the European Union. *General Data Protection Regulation (EU) 2016/679 ("GDPR")*; EU Regulation; European Parliament and Council of the European Union: Brussels, Belgium, 2018.
118. ETSI. *Satellite Earth Stations and Systems (SES); Global Navigation Satellite System (GNSS) Receivers; Radio Equipment Operating in the 1 164 MHz to 1 300 MHz and 1 559 MHz to 1 610 MHz Frequency Bands; Harmonised Standard Covering the Essential Requirements of Article 3.2 of Directive 2014/53/EU*; Draft ETSI EN 303 413 V1.1.0; ETSI: Valbonne, France, 2017.
119. Di Taranto, R.; Muppirisetty, L.S.; Raulefs, R.; Slock, D.; Svensson, T.; Wymeersch, H. Location-aware Communications for 5G Networks. *IEEE Signal Process. Mag.* **2014**, *31*, 102–112. [CrossRef]
120. Ahmad, I.; Kumar, T.; Liyanage, M.; Okwuibe, J.; Ylianttila, M.; Gurtov, A. 5G Security: Analysis of Threats and Solutions. In Proceedings of the Conference on Standards for Communications and Networking (CSCN), Helsinki, Finland, 18–20 September 2017; pp. 193–199.
121. Huawei. 5G Security: Forward Thinking. 2015. Available online: https://www.huawei.com/minisite/5g/img/5G_Security_Whitepaper_en.pdf (accessed on 1 April 2019).