applied sciences

MDPI

Review

Issues, Challenges, and Research Opportunities in Intelligent Transport System for Security and Privacy

Qazi Ejaz Ali *, Naveed Ahmad, Abdul Haseeb Malik, Gauhar Ali and Waheed ur Rehman

Department of Computer Science, University of Peshawar, Pakistan; n.ahmad@uop.edu.pk (N.A.); haseeb@uop.edu.pk (A.H.M.); gauharstd@uop.edu.pk (G.A.); wahrehman@uop.edu.pk (W.u.R.)

* Correspondence: qaziejazali@uop.edu.pk; Tel.: +92-91-921-6732

Received: 18 September 2018; Accepted: 4 October 2018; Published: 17 October 2018

Abstract: Intelligent transport system (ITS), owing to their potential to enhance road safety and improve traffic management, have attracted attention from automotive industries and academia in recent years. The underlying technology—i.e., vehicular ad-hoc networks (VANETs)—provide a means for vehicles to intelligently exchange messages regarding road and traffic conditions to enhance safety. The open nature of ITS as wireless communication technology leads to many security and privacy challenges. These challenges pertain to confidentiality, authentication, integrity, non-repudiation, location privacy, identity privacy, anonymity, certificate revocation, and certificate resolution. This article aims to propose a novel taxonomy of security and privacy issues and solutions in ITS. Furthermore, categorization of security and privacy schemes in ITS and their limitations are discussed with various parameters—scalability, privacy, computational cost, communication overhead, latency—and various types of security attacks has been analyzed. This article leverages new researchers for challenges and opportunities related to security and privacy in ITS.

Keywords: intelligent transport system; security; anonymity; privacy; authentication

1. Introduction

Intelligent transport system (ITS) is an emerging type of information and communication technology (ICT) application, which is based on inter-vehicular communication (IVC). IVC enabled vehicles provide updated information regarding traffic conditions. ITS can be used to minimize road accidents, congestion, and improve traffic efficiency. ITS plays an important role in the economy of a country by reducing fuel consumption and efficient time management of individuals [1,2]. Intelligent transport system stations (ITS-Ss) with the arrangement of wireless communication is a new growing area of research to reduce road accidents, congestion, and improve traffic efficiency [3].

Vehicular ad hoc network (VANET) is an important component of ITS. VANET uses ITS mechanisms to provide reliable information about vehicle's location, speed, heading, and road conditions. Increase in population and lack of seriousness in driving results in traffic congestions, road accidents and unnecessary delays in traveling [4]. Figure 1 shows one of the scenarios of un-seriousness in driving. For the betterment of society, there should be a positive use of technology in transport systems to reduce congestion, accidents, and unnecessary delays in traveling. In order to provide the best services to humanity, ITS is introduced to avoid congestion, traffic jams, and accidents, and to improve traffic efficiency [5].

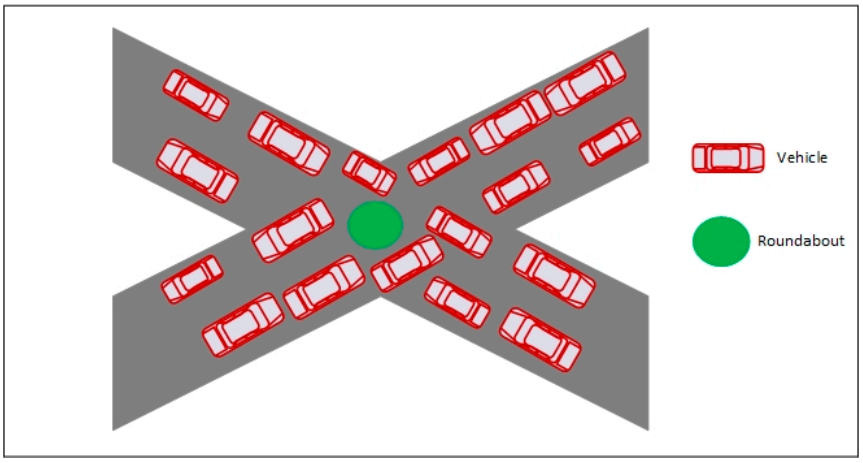

Figure 1. Scenario without intelligent transport system.

ITS has a wide range of applications [6]. However, generally, ITS applications are classified into advanced driver assistance systems (ADAS), advanced traveler information systems (ATIS), and advanced traffic management systems (ATMS) [7]. ADAS, ATIS, and ATMS help ITS-Ss to communicate with each other, in order to provide road safety, traffic efficiency, and comfort as shown in Figure 2. ADAS applications include cooperative collision warning, slow vehicle indications, lane change messages, speed control, reverse parking assistance, and intersection collision warnings. Similarly, ATIS applications include public transport information, trip reservation, route planning, internet booking, local electronic commerce, and trip matching services. While ATMS applications include dynamic route information, dynamic lane assignment, hazardous location, deterioration detection, and incident detection.

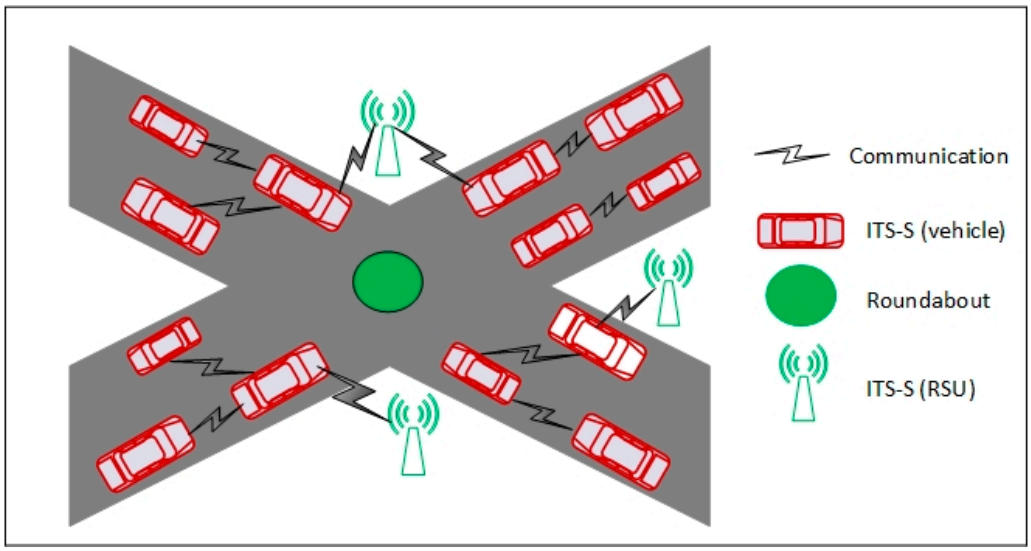

Figure 2. Intelligent transport system scenario.

The most important component of ITS dissemination formation is ITS-S, as depicted in Figure 3. ITS-S consists of vehicles, road side units (RSUs) and servers. There is an on-board unit (OBU) in each ITS-S (vehicle). The OBU enables an ITS-S (vehicle) to communicate with other ITS-Ss (vehicles or RSUs). According to the European Telecommunication Standards Institute (ETSI) [8] ITS-S architecture as shown in Figure 4, consists of facilities layer, networking and transport layer and the access layer. ITS-S facilities layer resemble application, presentation, and session layers of the OSI model. Similarly, ITS-S networking and transport layers show a resemblance of transport and network layers of the OSI

model. ITS-S access layer provides the capabilities of data link and physical layers of the OSI model with improvement to ITS.

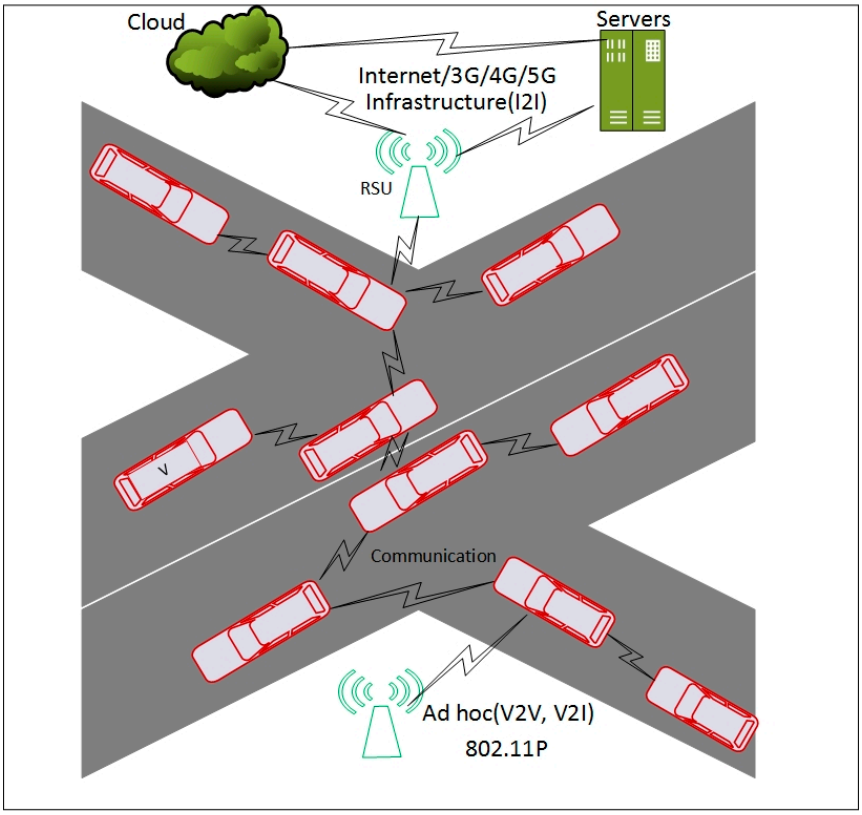

Figure 3. Intelligent transport system dissemination formation.

To enable vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) wireless communication (known as 'V2X'), dedicated short range communication (DSRC) is used [9]. DSRC provides communication range from 100 to 1000 m, with the data communication rate of around 27 Mbps [10]. DSRC is known as wireless access in vehicular environment (WAVE), also called IEEE 802.11P standard [11–13]. DSRC requires low latency and high data rate to support short distance communication [14]. In ITS, DSRC is based on the access layer as discussed in IEEE 802.11P standard. Spectrum allocation for DSRC is from 5.85 GHz to 5.925 GHz as specified by United States (US) Federal Communication Commission (FCC) and European Electronic Communications Committee (ECC). Institute of Electrical and Electronics Engineers (IEEE) and ETSI segmented DSRC band into seven different channels each of 10 MHz. Among the seven channels, there is one control channel and six are service channels. The service channels are used for data transmission while the control channel is used for setting the services and applications strived on service channels.

In order to provide the services for resource management, security, networking, multichannel operations and single channel operations, IEEE has advised the standards for WAVE. WAVE IEEE standard adds the functionalities of IEEE 802.11P and IEEE 1609.x protocol stack [15–19].

As shown in Figure 4, in order to use the wireless medium in ITS, IEEE advised, IEEE WAVE also called IEEE 1609.x protocol stack [19]. IEEE 1609.1, IEEE 1609.2, IEEE 1609.3, and IEEE 1609.4 (1609.x) define the architecture, transmission framework, management, security and access in ITS. In Europe, IEEE WAVE is called ITS-G5. IEEE 1609.1 defines beacon format and storage of beacons by facilities layer. IEEE 1609.2 standard defines secure beacons format for DSRC. IEEE 1609.2 determines techniques to secure messages. It specifies the processes of how ITS-Ss (vehicles) performed security assistance, such as confidentiality, authentication, integrity, access control, and non-repudiation. IEEE 1609.3

specifies WAVE Short Message (WSM) and its related protocol WAVE Short Message Protocol (WSMP) to ensure the services of the networking and transport layer related to safety applications. It also specifies WAVE Service Advertisement (WSA) message. WSA message is used in a given area to advertise the accessibility of DSRC services like a WSA can be broadcasted by an ITS-S (RSU) to advertise the presence of media downloading service. IEEE 1609.4 standard discusses the management and usage of DSRC channels.

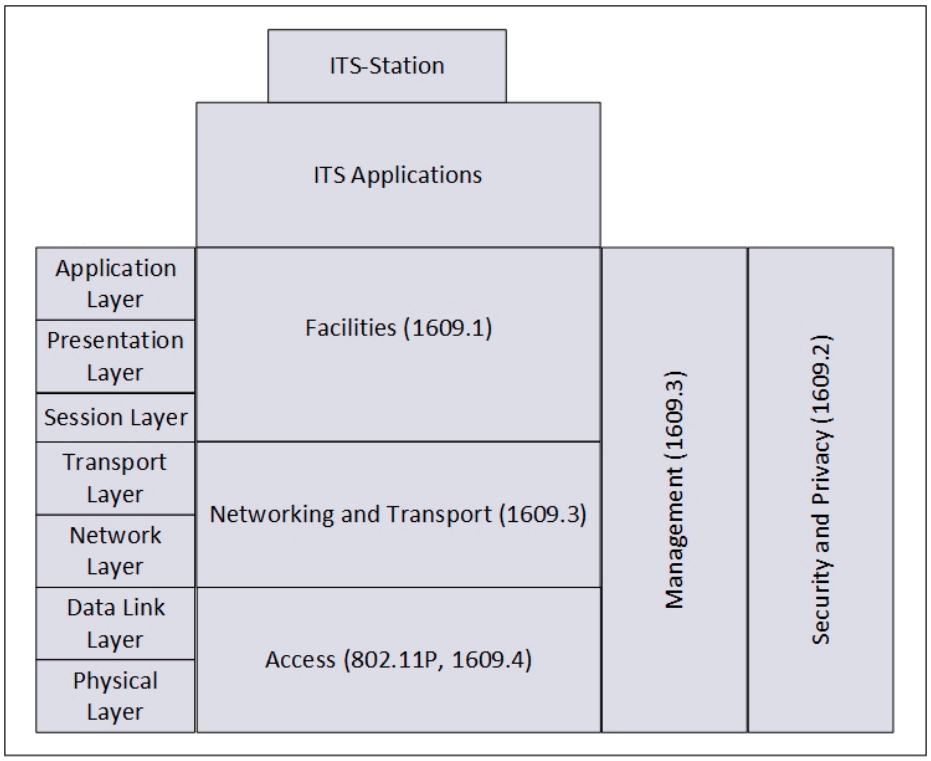

Figure 4. ITS-S architecture with 802.11P/WAVE and IEEE 1609.x.

ITS can be differentiated from mobile ad hoc network (MANET) [20] in terms of its unique characteristics. The unique characteristics are: (a) dynamic topology, (b) high speed, (c) vehicles mobility is restricted to fixed roads/maps, (d) sparse and dense scenarios, (e) vehicle privacy, and (f) unlimited storage and power.

In ITS, every vehicle generates beacons regarding its current position, heading, speed, and road condition. However, there are also malicious vehicles and their aim is to damage the network. Malicious vehicles can misguide the honest vehicles. Checking the reliability of beacons is a challenge in ITS. There should be trustworthy techniques to verify the originality of beacons. Reliable security frameworks should be designed and developed to achieve the ITS objectives. If there is no proper security and privacy approaches, attackers may misguide or track vehicles to get malicious benefits. In order to provide a safe and efficient environment for ITS, first, the security and privacy challenges must be addressed.

In ITS, the main issues are due to the following reasons:

- Dynamic speed and topology: As the nature of ITS is ad hoc. There is no fixed topology. The speed of vehicles is changing, with respect to time. The beacon generation and verification should be done in minimum time, otherwise, there may be congestion and accidents [21].
- Sparse and dense scenarios: In the sparse scenario, inter-vehicle distance is large. While in the dense scenario, the numbers of vehicles are more with reduced distances. Thus, verification of more beacons in the dense scenario is difficult as compared to the sparse scenario. There

should be smart security and privacy approaches that work efficiently in both sparse and dense scenarios [22].

- Bandwidth limitation: The problem of bandwidth limitation arises if there are more vehicles (dense scenarios) [23]. This problem may cause communication interference, delay, and affects the delivery ratio. Well-established security approaches need to be developed in order to address this issue.
- Decentralization: Due to the ad hoc nature of ITS, there is no fixed central system that ensures trustworthy communication of vehicles. As different vehicles are joining and leaving the VANET [5]. There is a need to focus on the designing of trustworthy security approaches to work reliably under decentralized scenario.
- Malicious attackers: Due to the wireless and ad hoc nature of ITS, attackers try to inject bogus beacons or alter the attacked beacons [24]. The attacker tries to misguide honest vehicles for their personal interest.

In ITS, a lot of research work is done to consider security and privacy issues. Andrea et al. [25] discussed the security susceptibility and threats in ITS. There are security and privacy-related challenges from the perspective of applications, network and technologies. Niu et al. [26] discussed only the issues of integrity and access control but did not elaborate the various security and privacy mechanisms. Qu et al. [27] present a survey on the security and privacy issues of ITS, but it lacks proper analysis of the security and privacy approaches. Similarly, Lin et al. [24] present a survey and discuss security and privacy approaches but it lacks proper analysis for different types of attacks on ITS communication layers, scalability, and computational cost. Engoulou et al. [28] specified security and privacy requirements in ITS but do not properly analyze the security and privacy techniques for ITS suitability.

Petit et al. [29] provide an excellent survey on pseudonyms schemes in ITS but consider only limited types of attacks. There is a lack of the individual technique proper analysis in each group. Similarly, a survey presented in [30] is an excellent survey on pseudonym changing mechanisms to protect location privacy but lacks analysis of each technique in every privacy category of ITS with respect to latency, computational cost, communication overhead, and different types of attacks as discussed in Section 2 of this paper. A number of surveys have been conducted for the security and privacy challenges in ITS. However, still there is a need to present an extensive survey of ITS security and privacy to assist researchers in the emerging area of ITS. This paper discusses the security and privacy challenges in ITS and provides analysis of security and privacy approaches in terms of different types of attacks on ITS communication layers, scalability, computational cost, communication overhead, and latency. The contributions of this paper are:

- The ITS security and privacy challenges are reviewed and presented.
- Different types of security and privacy attacks in ITS are analyzed and discussed.
- Privacy schemes in ITS are examined and categorized based on scalability, latency, computational cost, communication overhead, security, and privacy attacks.
- New research challenges in ITS security and privacy are presented.
- A discussion towards the integration of ITS in the cloud is presented.

The rest of this paper is organized as follows: Section 2 consists of ITS security and privacy challenges. Section 3 consists of the categorization of privacy mechanisms in ITS. Section 4 presents the group/ring signature-based schemes. Section 5 consists of the pseudonym-based approaches. Section 6 presents hybrid schemes. Section 7 discusses the integration of ITS in the cloud. While Section 8 presents a conclusion and future direction.

2. ITS Security and Privacy Challenges

In ITS, security and privacy are the most ambitious problems and privacy should be examined along with security [27]. Every member of ITS should be authenticated. Similarly, every beacon should

be verified to reduce the risk of security and privacy attacks in ITS. ITS-S (vehicle) privacy ensures the protection of the ITS user location and real identity. Security and privacy needs are satisfied through fictitious identities [29]. The nature of ITS is that it is wireless, with high speed mobility, dynamic topology, sparse and dense scenarios and is susceptible to attacks when segregating with other ICT based networks. In ITS, vehicles broadcast messages to inform other vehicles about the traffic situations, however, malicious vehicles might broadcast bogus messages or alter the original messages of a legitimate ITS user. The aim of ITS cannot be achieved and honest ITS users can be misguided. An adversary can misguide or eavesdrop honest ITS user's data for his/her personal interest. Therefore, there should be proper mechanisms to ensure the authenticity and integrity of messages [31]. If an ITS-S (vehicle) is found guilty, it should be revoked from ITS. There should be proper security and privacy approaches for registration and revocation of vehicles. Blossl et al. [32], discussed the issue of scrambler attacks on location privacy of vehicles/drivers. Usage of predictable scramblers cannot protect location privacy of vehicles. The scrambler (change signals) component of all IEEE 802.11p and Wi-Fi radio transceivers cannot guarantee the performance at the lower physical layer and needs to improve the performance of wireless communication. There is also a need to incorporate strong cryptographic techniques.

Eckhoff et al. [33] proposed a scheme to protect user privacy in which a user, as well as authority, cannot track a vehicle. However, the mechanism is not at par with ITS system because there is no consideration for revocation and accountability of malicious vehicles. Security and privacy issues are mainly categorized as features, attacks, and challenges as shown in Figure 5. These issues are given in detail as follows:

- Confidentiality: This feature ensures that only authorized ITS users have access to data. The data cannot be snooped or hindered by unauthorized users. Confidentiality is an important service in ITS, during the pseudonym registration and obtaining phases. Thus, it is important to ensure confidentiality of ITS. Therefore, advanced cryptographic techniques should be considered [34].
- Integrity: Integrity can assure the exact delivery of messages. In ITS integrity is important, because wrong or tampered messages can misguide honest ITS users. Integrity avoids expected or unexpected intervention during the communication. In order to achieve fair integrity in ITS, strong security mechanisms should be designed [35].
- Availability: This feature in ITS guarantees that the servers and data are always available to authorize ITS users. In ITS, services are needed in real time. Therefore, the availability feature should be considered. Maheswariet al. [36] discussed that denial of service attack is the most dangerous threat for the availability of services in ITS. In order to ensure availability, enhanced security approaches should be considered in ITS.
- Identification: This feature can ensure that unauthorized ITS-S (vehicles) cannot be linked in ITS. Identification of each ITS-S is difficult. Therefore, there is a need to design and develop effective mechanisms for the identification of vehicles [37].
- Authentication: Authentication can ensure that the messages received are legitimate. However, authentication can be carried out in ITS without revealing the real identity of the vehicle. Efficient approaches are needed to deal with this feature [37].
- Non-Repudiation: This feature ensures that the communicating entities cannot deny the previous communication. In order to avoid malicious threats in ITS, a non-repudiation feature must be considered.
- Privacy: A privacy feature in ITS can guarantee that only the authorized servers can control the anonymity. Confidentiality aims to encrypt the data, while privacy ensures that the real identity of information cannot be revealed from messages/data [38–41]. In ITS, privacy of a legitimate vehicle is the most important attribute. In order to avoid tractability of an honest ITS user, there is a great need for the design and development of security and privacy mechanisms.

- Trust: Trust can guarantee the preceding security and anonymous communication features to be accomplished during the give and take phases among distinct entities. In ITS, the feature of trust can be divided between applications and entities [25]. In order to achieve trust in ITS, there is a need to develop trustworthy approaches.

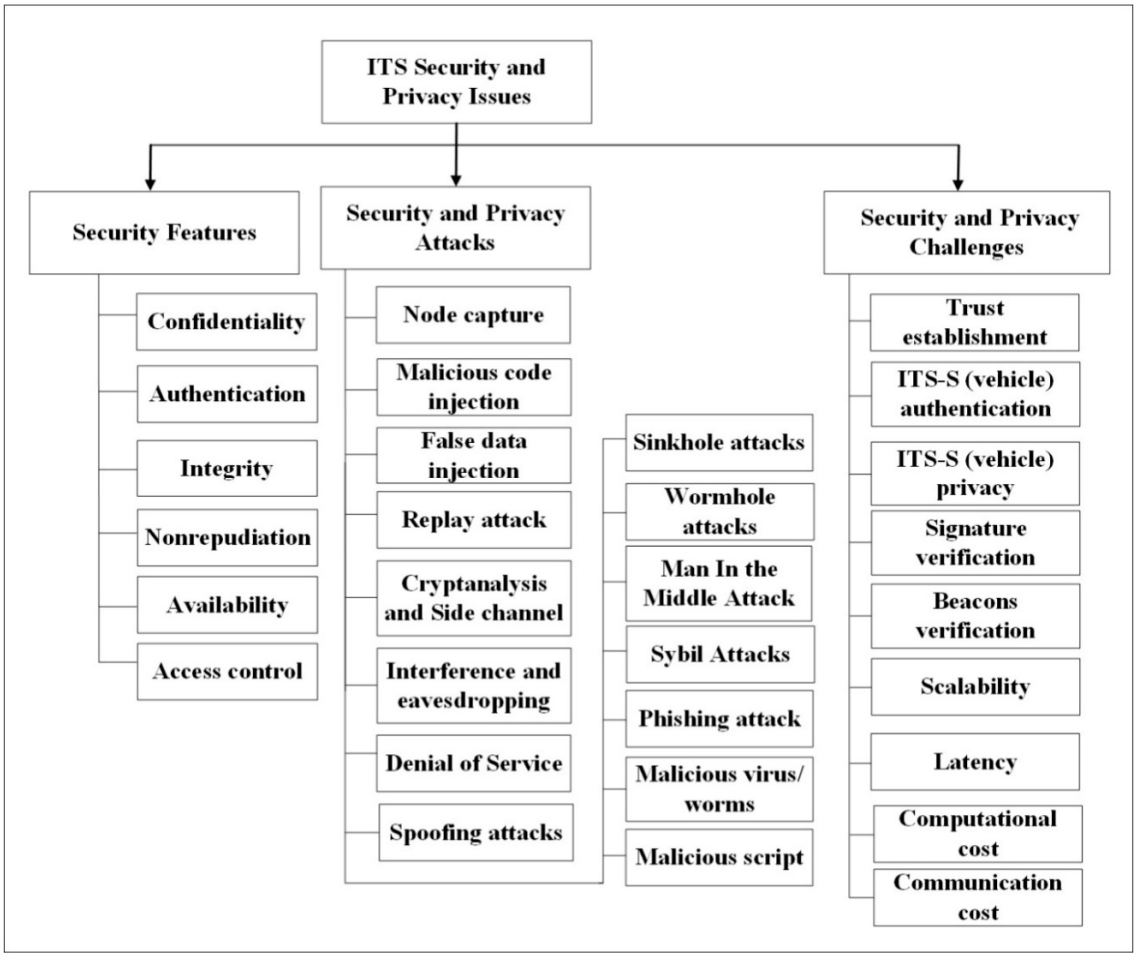

Figure 5. ITS security and privacy issues.

According to the ETSI, the communication architecture of an ITS-S consists of an access layer, networking and transport layer, and facilities layer [8]. In ITS, the facilities layer is constituted via obtaining the performance of data usages in the network and transport layer. In the facilities layer, security provocation can be judged by the provocation in the access and networking and transport layers.

(1) Access layer: The main objective of an access layer in ITS is to transmit and receive messages. The security challenges in this layer are:

(i) Node capture attack: In this type of attack, an opponent can get and hold the node i.e., ITS-S (vehicle or RSU) in ITS via meddling with the OBU of the vehicle [42]. If an ITS-S (vehicle or RSU) is paced by the node capture attack, the key information can be exhibited to the opponent. The attacker can easily copy the key information of the attacked node/ITS-S. In this way, the malicious vehicle can easily become an authorized vehicle to connect into the ITS. The node capture attack is considered as the node replication attack. In order to prevent the node capture attack, capable security and privacy approaches are needed [43].

(ii) Malicious code injection attacks: The malicious code injection attacks [44], can easily grant permission of an opponent into ITS. In order to preserve from malicious code injection attacks, the designing of capable code authentication approaches is required [44,45].

(iii) False data injection attacks: Yang et al. [35], discussed that with node captured attack, the opponent can easily insert the wrong information. In this way, the receiving vehicles are misguided, which affects the ITS. In order to identify false data, proper security schemes need to be designed [46].

(iv) Replay attacks: Replay attacks are also called freshness attacks [47,48], in this type of attack, an opponent can use an attached ITS-S to send messages with legal evidence. Authentication processes are commonly affected through replay attacks. To overcome the replay attack effect, proper time stamp approaches must be developed in ITS [49].

(v) Cryptanalysis and side-channel attacks: In this type of attack, an eavesdropper tries to get key information from the obtained cipher text [50]. However, if strong security and privacy techniques are used, the chances of cryptanalysis attack are less. Similarly, the opponent can launch aside-channel attack, the opponent can use some mechanisms on the devices (e.g., RSUs) in ITS and try to get the cipher key information. In order to relieve the side-channel attacks, effective security and key management approaches are required in ITS [34].

(vi) Interference and eavesdropping: As the nature of ITS is wireless, if there are no security measures the communication can be monitored easily by unauthorized parties [42,51]. To relieve ITS from eavesdropping, proper security approaches are needed. Noise data can be sent by the adversary to impede with the distributed information in wireless communication. In order to guarantee the timely and accurate delivery of information in ITS, effective security and privacy approaches are needed to avoid the interference by unauthorized users [52].

(2) Networking and Transport Layer: The primary function of the networking and transport layer in ITS, is to transmit data between ITS-Ss. In the network and transport layer security threats target on the smashup of the accessibility of the network stocks. Due to the wireless nature of ITS, security threats in this layer are crucial. Network and transport layer attacks in ITS are as follows:

(i) Denial of service (DoS) attacks: Due to DoS attacks [53], all the resources of ITS are exhausted with desperate flux. As a result, honest ITS-S cannot receive the service. In order to relieve from DoS attacks, effective ITS schemes should be designed to address DoS attacks [36].

(ii) Spoofing attacks: The main objective of spoofing attack [25,54] is to gain complete access to ITS. After keeping the full access to the ITS, adversary sends bogus beacons. To defend against spoofing attacks, effective security techniques are needed to focus on proper authentication [37,55].

(iii) Sinkhole attacks: In sinkhole attacks [56], the attacked ITS-S, arrogates prodigious capabilities of key generation and communication. This will attract other vehicles to communicate through the particular ITS-S (RSU), thus disrupting the ITS. To relieve the ITS from sinkhole attacks [57], proper security routing approaches are needed.

(iv) Wormhole attacks: Wormhole attacks [58] are launched by two petty ITS-Ss, in ITS to transfer beacons with secure links in order to claim a fake single node communication interpolate them [58]. Due to wormhole attacks, forwarding nodes (ITS-Ss) are decreased. Now maximum messages are delivering through malicious ITS-Ss. As a result, honest vehicles can be misguided. To defend the ITS against wormhole attacks, proper authentication approaches are needed.

(v) Man in the middle attack (MIMA): In MIMA [59], a malicious ITS-S (vehicle) is controlled by an opponent is placed virtually among other ITS-Ss (vehicles and RSUs). Malicious

ITS-S is a middle node between honest ITS-Ss, can record all the communication of the honest vehicles. This type of attack breaks the privacy, confidentiality, and integrity of vehicles by eavesdropping, modification, and full access to the communication between honest ITS-Ss. Secure and reliable communication approaches which can guarantee the authentication of uncompromised ITS-Ss can be an effective mechanism to MIMA [34,36].

(vi) Sybil Attacks: In Sybil attacks [25,60], a malicious vehicle can arrogate many real identities and imitate them in the ITS. Due to these attacks, a malicious vehicle can have many real identities. An honest ITS user cannot distinguish fake messages transmitted by the malicious vehicle. As a result, honest vehicles are misguided. In order to protect an ITS from Sybil attacks, proper authentication and identification secure approaches are needed to be developed [37].

(3) Facilities layer: User-requested services are provided by the facilities layer. Thus, security threats at the facilities layer are a center on services attacks. Here in ITS, many applicants inquiring in the facilities layer are discussed as follows:

(i) Phishing attack: In phishing attacks [25,61], an opponent can get ITS user private data such as identities through spoofing. In ITS robust secure mechanisms for pseudonym generation, acquiring and communication can relieve from phishing attacks.

(ii) Malicious virus/worms: Another threat to ITS, is malicious worms or virus [25,55,62]. An opponent can send virus along with beacons to infect the ITS with malicious self-spreading interventions. As a result, an adversary can get or modify private data of honest ITS user. For proper authentication, integrity check approaches are needed to relieve this type of attack [63].

(iii) Malicious script: Malicious script [25] in ITS, is inserted into application/software's to damage the system. As some ITS applications, like infotainment, point of interest notification, insurance etc. are linked with the internet. By executing the script, malicious scripts like the active-x script, java applets etc. the opponent can quickly victimize an honest ITS-S. Malicious scripts obtained through internet service, can stiff the outflow of private information or flush the ITS. To provide reliable protection for vehicles, proper mechanisms are required to validate the services through the internet.

Like security, one of the key human rights is privacy that needs to be preserved. United Nations (UN) human rights universal statement, introduced in 1948 article 12, says that: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks" [64].

Privacy of a user in ITS is a crucial issue [38]. The privacy issue in ITS can implicate vehicle loss, life threat and other damages, like stealing at home or office. In ITS, communication authenticity is achieved through identity. However, if real identities are used, the adversary can track the user path (e.g., start and end location of driving). Thus, an adversary can collect the daily routine information of a user. If the opponent gets ITS user confidential information, he/she can derive the schedule of the user. For example, at which time the user will be at home or their office or anywhere. By keeping this information, an opponent can charge fraud/theft or even endanger a user's life. Therefore, privacy preserving techniques are needed to develop, in order to ensure that private information of ITS user cannot be a leak to an adversary. In order to provide privacy for ITS-S, privacy related techniques are divided into: privacy preservation based on anonymity [65], privacy preservation based on encryption [66], and privacy preservation based on perturbation [67–69].

Qiu et al. [70] discussed that there are many techniques to preserve privacy-based anonymity—like T-closeness, L-diversity, and K-anonymity etc.—to preserve the real identities. However, anonymous communication can be affected through traffic analysis [71–73]. Privacy preservation based on

encryption using encryption techniques (e.g., zero-knowledge proof, secret sharing, homomorphism encryption etc.) can be used to guarantee that actual information related to the vehicle cannot be leaked by eavesdroppers [66]. However, encryption-based approaches only ensure confidentiality of data, not the privacy of the vehicles.

Similarly, privacy preservation based on perturbation approaches—like information sharing, information customization, etc.—changes the order of information being sent to achieve privacy preservation [67]. However, by using perturbation techniques, revocation in ITS cannot be achieved efficiently with respect to time. Therefore, the application of privacy preservation based on perturbation cannot be considered in ITS. Thus privacy preservation techniques along with confidentiality in ITS are still a great challenge.

3. Categorization of Security and Privacy Mechanisms in ITS

In ITS, privacy mechanisms involve proper verification, registration, and communication. In order to provide a trustworthy system, there must be effective authentication of vehicles and messages. With effective security and privacy schemes, an adversary can easily be identified. Once an adversary (malicious vehicle) is identified, it must be revoked and proper accountability can be performed. The effective revocation and accountability approaches can save the ITS from maximum damages and gain trust in return from ITS users. In order to establish a complete trustworthy system for transportation, confidentiality, integrity, authentication, and non-repudiation properties must be considered. In view of the aforementioned features, several researchers have made their best efforts to design security schemes for ITS. In this survey paper, security and privacy schemes in ITS as shown in Figure 6 are mainly categorized into (i) group/ring signature-based (GSB or RSB) schemes, (ii) pseudonym-based (PB) schemes, and (iii) hybrid schemes.

In order to critically analyze the security and privacy schemes in ITS, the following parameters are considered: (i) scalability, (ii) security/privacy, (iii) computational cost, (iv) latency, and (v) communication overhead. The parameters are obtained from the literature as discussed in the next sections of this paper.

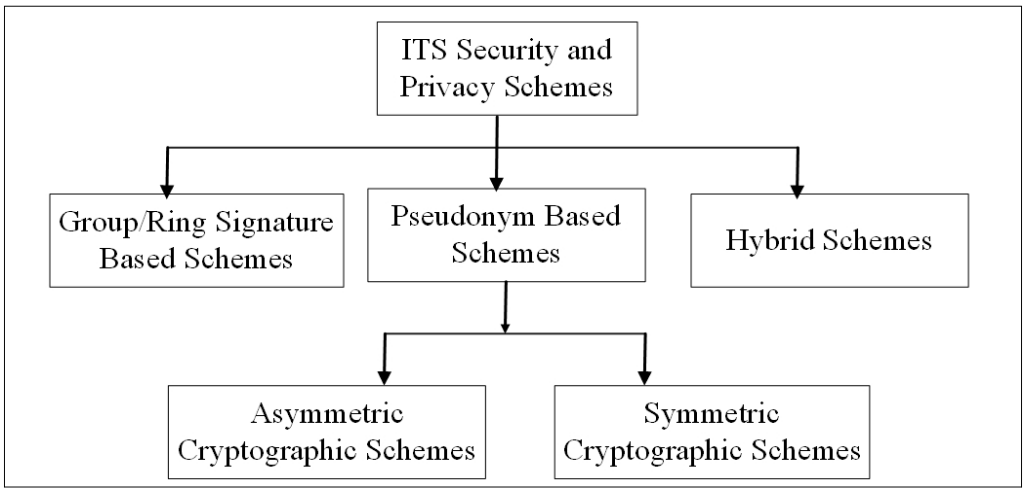

Figure 6. ITS security and privacy schemes categorization.

4. Group/Ring Signature Based Privacy Schemes

In order to provide anonymity and secure communication between V2X, as debated in the previous sections of this paper, there is a need to develop effective security and privacy mechanisms that address the issues of security and privacy efficiently. In ITS, a GSB approach is proposed by Guo et al. [74] that suggests the use of group signature to provide unlinkability of messages generated by the same user. Only the group manager can reveal the privacy because the group manager has all the ITS

users information and thus a single point of security risk. Zhu el al. [75] proposed that the privacy of an ITS user can be achieved through group signature. The asymmetric cryptography can be used in group signature. The group members have their private keys and the group asymmetric key. The private key is used to produce signatures and send messages. To verify the signatures with messages at the receiving vehicle, the group asymmetric key is used. The real identity of an ITS user can be exposed only to the group manager. A modified form of short group signature that uses batch verification proposed in [76]. However, the approach produces high computational and communication overheads. A decentralized approach of group signature is proposed by Zhang et al. [77], in which RSU acts as a manager of the small group. However, it is prone to side-channel attack.

Lin et al. [78] discussed a technique based on the group signature and identity-based signature. The technique combined short group signature and identity-based signature to provide anonymity. The main disadvantage of this technique is RSU participation in signature generation and verification, as there are side-channel attacks.

Huang et al. [79], discussed a technique of group verification by using elliptic curve cryptography (ECC) to minimize signature verification and communication overheads. However, the technique is prone to DoS attack. In order to minimize the computational time in verification of group signatures through RSUs, Zhang et al. [80] presented a technique which uses pseudonyms to achieve anonymity of ITS user. However, RSUs are located in open infrastructure and can easily be targeted by the adversaries. Similarly, the scheme suggested by Zhang et al. [80] is prone to DoS attacks, because bogus messages can easily be injected. Similarly, the mechanism presented in [81], improve the shortcomings of anonymity through pseudonyms. However, the mechanism is prone to Sybil and replay attacks.

Hao et al. [82] suggested Cooperative Message Authentication Protocol (CMAP) by using a short group signature approach. CMAP reduced computational and transmission costs, but the property of non-repudiation is not achieved. Furthermore, a group of vehicles can only verify the authenticity of the messages, while other vehicles just accept the messages on behalf of the verifier group. However, if any member of the verifier group is impersonated, the overall security of ITS is put at risk. To reduce the computational and communication overheads in GSB schemes, Lin et al. [83] presented an approach based on group authentication. The technique presented in [83], reduced computational and transmission costs, but is prone to DoS attacks and is also not scalable.

In summary, some group signature schemes incur high computational overhead and medium security, while in some schemes computational overhead is low but security is also low. The performance, security, and privacy analysis of GSB/RSB approaches are shown in Tables 1–3, respectively.

Table 1. GSB/RSB schemes performance.

Research Papers	Scalability	Security/Privacy	Computational Cost	Communication Overhead	Latency
[74]	Low	Low	High	High	High
[75]	Low	Low	Medium	Medium	Medium
[76]	Low	Medium	High	High	Medium
[77]	Low	Medium	Medium	Medium	Medium
[78]	Low	Low	Medium	Medium	Low
[79]	Medium	Low	Medium	Medium	Medium
[80]	Low	Low	Low	Low	Low
[81]	Low	Low	Low	Medium	Medium
[82]	Medium	Low	Medium	Low	Medium
[83]	Low	Low	Low	Low	Medium

Table 2. Attacks on GSB/RSB schemes.

Research Papers	Node Capture	Malicious Code Injection	False Data Injection	Replay	Side-Channel	Eavesdropping
[74]	No	No	Yes	Yes	No	Yes
[75]	No	No	Yes	No	No	Yes
[76]	No	Yes	Yes	Yes	No	Yes
[77]	No	Yes	Yes	Yes	Yes	Yes
[78]	No	No	Yes	No	Yes	Yes
[79]	No	No	Yes	Yes	No	Yes
[80]	No	Yes	Yes	No	Yes	Yes
[81]	No	Yes	Yes	Yes	No	Yes
[82]	No	Yes	Yes	Yes	No	Yes
[83]	No	No	No	No	No	No

Table 3. Attacks on GSB/RSB schemes.

Research Papers	DoS	Spoofing	Sinkhole	Wormhole	MIMA	Sybil	Phishing	Malicious Virus	Malicious Script
[74]	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
[75]	No	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
[76]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
[77]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
[78]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
[79]	Yes	Yes	No	No	Yes	Yes	Yes	Yes	Yes
[80]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
[81]	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
[82]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
[83]	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes

5. Pseudonym-Based Privacy Schemes

In pseudonym-based approaches, fictitious names are assigned to provide anonymity of ITS-Ss (vehicles). Pseudonym-based schemes are further categorized into asymmetric cryptographic based schemes and symmetric cryptographic-based schemes. To provide a trustworthy and reliable relationship between the vehicles and ITS servers, there should be proper verification and integrity checks for ITS communication. There are various cryptographic protocols that can be used in ITS to achieve reliable verification and integrity of ITS communication. In summary, asymmetric/public key cryptographic techniques and symmetric/secret key cryptographic techniques can be used;

(1) Public key cryptographic techniques: In public key cryptographic techniques [84] as shown in Figure 7, two keys are used namely public key and private key. Public key is used for encryption. It is publicly known in the system. While private key is used for decryption, it is only known to the receiver/authorized party of the messages. A certificate authority (CA) generates the key pairs in ITS. CA provides the public key certificates to ITS-Ss (vehicles) for reliable communication. CA can generate certificate revocation list (CRL) if any vehicle is violating the rules of CA (e.g., certificate expires, the participation of vehicle in malicious activities, keys compromised etc.). The CRL contains information of revoked certificates [80,85]. However, standalone usages of public key techniques produce substantial overheads in terms of a large number of certificates and CRLs.

(2) Secret key cryptographic techniques: Secret key cryptography uses a single key for both encryption and decryption [4], as shown in Figure 8. The key is shared between the two communicating nodes (ITS-Ss). However, secret key techniques alone can provide confidentiality of data. There are no proper guidelines for privacy and revocation of malicious users in ITS.

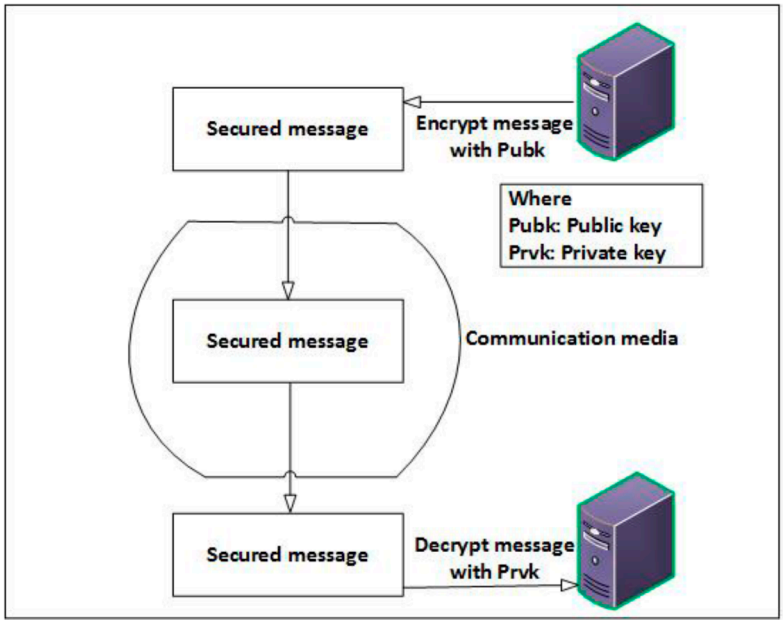

Figure 7. Asymmetric cryptographic approach.

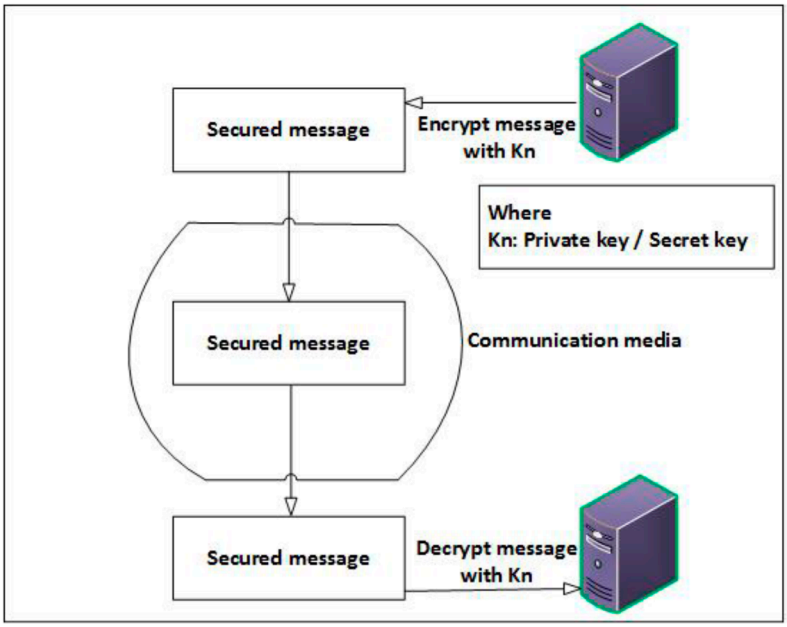

Figure 8. Symmetric cryptographic approach.

5.1. Public Key/Asymmetric-Based Pseudonym Schemes

In asymmetric based schemes, public key infrastructure (PKI) is used. A public key-based pseudonym scheme proposed by Raya et al. [86], in which several unidentified asymmetric keys are utilized so that the safety messages sending vehicle cannot be tracked. However, the limitations of this approach are, large storage is required to store enormous asymmetric keys and computational cost in terms of CRL entries checking. A technique called Expedite Message Authentication Protocol (EMAP) [87] uses hash function along with PKI to reduce the time checking process in CRL. However, the communication overhead is high, as hash codes are also exchanged along with CRLs. Also, large storage is required to store hash codes of CRLs. The schemes presented in [88,89] use ECC, to reduce communication and computational overheads. However, the privacy of source (sending

safety messages vehicle) is low. ECC [90] is based on the algorithmic artifact of oval arcs closed specific plots. ECC is basically a type of asymmetric encryption. However, only the signature with the messages cannot ensure the authenticity of messages. The messages are appended with digital certificates. ECC computational and transmission costs are affected by a number of vehicles. Similarly, speed affects delay in ECC [90]. Computational cost, transmission cost, and packet delivery ratio in dense and sparse scenarios are affected in ECC [90]. ECC schemes work well in sparse scenarios [91], but in dense scenarios, the efficiency of ECC is affected. ECC based schemes [91] alone do not provide the feature of non-repudiation and is prone to DoS attack. Authentication is the most important service in ITS and guarantee security. However, in order to achieve efficiency, an augmented authentication mechanism is still a big challenge [92].

Smith et al. [92], proposed a security scheme based on PKI. The scheme uses Merkle tree (MT) and elliptic curve digital signature algorithm (ECDSA) but incurs high computational delay. Construction of MT is a time-consuming activity. The scheme [92] considered no privacy for vehicles. There is a transmission overhead by sending the Merkle verification direction. However, only ECDSA-based authentication schemes are open to DoS attack.

In summary the performance, security, and privacy analysis of asymmetric encryption based pseudonym approaches are shown in Tables 4–6, respectively.

Table 4. Asymmetric based encryption schemes performance.

Research Papers	Scalability	Security/Privacy	Computational Cost	Communication Overhead	Latency
[86]	High	Low	High	High	High
[87]	High	Low	Low	High	High
[88]	High	Low	Medium	Medium	Medium
[89]	High	Low	Medium	Medium	Medium
[90]	High	Medium	High	High	High
[91]	High	Medium	High	High	High
[92]	High	Medium	High	High	High

Table 5. Attacks on asymmetric based encryption schemes.

Research Papers	Node Capture	Malicious Code Injection	False Data Injection	Replay	Side-channel	Eavesdropping
[86]	No	No	Yes	Yes	Yes	Yes
[87]	No	No	Yes	Yes	Yes	Yes
[88]	No	No	Yes	Yes	Yes	Yes
[89]	No	No	Yes	Yes	Yes	Yes
[90]	No	No	No	No	Yes	Yes
[91]	No	No	No	No	Yes	Yes
[92]	No	No	No	Yes	Yes	No

Table 6. Attacks on asymmetric based encryption schemes.

Research Papers	DoS	Spoofing	Sinkhole	Wormhole	MIMA	Sybil	Phishing	Malicious Virus	Malicious Script
[86]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
[87]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
[88]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
[89]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
[90]	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
[91]	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
[92]	Yes	No	Yes	Yes	Yes	No	Yes	Yes	Yes

5.2. Symmetric Cryptographic-Based Pseudonym Schemes/Symmetric Encryption

Symmetric encryption is more efficient than asymmetric encryption in terms of computation. However, symmetric cryptographic based schemes alone do not provide non-repudiation property. Schaub et al. [93] presented a symmetric cryptographic based scheme that does not depend on identity mapping to be performed by any party and the identity mapping information is directly incorporated in pseudonyms. The pseudonyms can be resolved only when multiple parties cooperate. This scheme suggests that fictitious perseverance is performed by decrypting the V-token. In this scheme, the CA and pseudonym provider (PP) can encrypt pseudonym linking information. However, the incorporation of pseudonyms resolution information directly in pseudonyms certificates can jeopardize the privacy of vehicles. In addition, there exists replay, Sybil and side-channel attacks.

The scheme proposed in [94] uses secret key cryptography. The scheme computes hashes (message digest) and sends along with safety messages for integrity. At the receiving end hashes are calculated and then compare with the received hashes to ensure integrity. However, the approach is prone to DoS, Sybil, and side-channel attacks. Carianha et al. [95] discussed the strategy to improve the privacy of vehicle location in mix-zones called anonymizing area using cryptographic mix-zone (CMAX) protocol. The assigned private key by RSU is used to encode the status information (heading, position, and velocity). As per CMAX protocol, the RSU assigns private key only to authorize vehicle that enters the mix-zone. The private key is then used to encrypt the messages/beacons. The sender private key will be used in a mix-zone to encrypt the status information. The RSU decrypts the messages using the private key of the receiving vehicle and forwards them to the receiving vehicles that are within the source vehicle proximity also called neighbor vehicle. However, the approach is prone to replay and side-channel attacks. The approach presented in [96] minimizes computational cost in signature verification but does not properly address the revocation process of malicious vehicles.

In [97], the researchers tried to protect the privacy of vehicles by using three entities in the model i.e., Key Management Center (KMC), RSU, and vehicle. The KMC is responsible for the registration of vehicles, road side units, and traceability of vehicles. KMC knows all the information of vehicles i.e., vehicle owner, date of registration, engine number. RSU will be responsible for the forwarding of messages and key updating distribution within the transmission range of 1 to 3 km. While the vehicle is incorporated with an OBU and tamper-proof device (TPD). TPD is designed to keep cryptographic stuff and to process the operations related to cryptography. While the OBU is used for communication of messages. For preserving the privacy and incidental derivative, self-generated pseudonyms are used. However, KMC is a single threat model, having all the information. The scheme is prone to false data injection, malicious code injection, side-channel, and Sybil attacks.

The secret key pseudonym-based scheme presented by Chim et al. [98] uses RSU for integrity check, but is prone to side-channel attacks. Similarly, the approaches presented in [99,100] employed symmetric encryption along with message digest to address the DoS attacks, but in these approaches the computational overhead is high and they are prone to impersonation and Sybil attacks. Jahanian et al. [101] presented a time efficient stream authentication (TESLA) based scheme. TESLA is a secret key cryptographic based approach in which a message authentication code is calculated through the secret shared key. The message authentication code is then affixed with the safety message. The message authentication code is verified through the secret shared key and is prone to replay and side-channel attacks.

An advanced version of TESLA, to avoid the problem of storage stationed DoS attack, TESLA++ is presented by Studer et al. [102]. TESLA++ is a symmetric cryptographic based scheme, in which the source reveals the secret key subsequently after some wait. However, TESLA++ does not furnish the property of non-repudiation.

TESLA++ is the combination of TESLA and elliptical curve digital signature algorithm (ECDSA) [92]. TESLA++ is an advanced variant of TESLA, but TESLA++ incurs substantial computational overheads by calculating message authentication codes (MACs) of messages in addition to performing the activities of TESLA and ECDSA. In ITS, a vehicle has to generate and verify a

large number of messages within a second to properly achieve the benefits of ITS. However, by using TESLA++ the generation and verification of beacons status at a vehicle are affected.

Another TESLA based approach presented in [103] for security checks in ad hoc networks. However, TESLA is prone to DoS attack [103]. In TESLA, the delay keys concept provides an opportunity for the adversary to attack. TESLA is also prone to pollution attack [104,105]. In pollution attack, the attackers can deluge the receiving node storage with enormous bogus messages with wrong keys and strip to a pollution attack state. However, TESLA is also prone to storage stationed DoS attack [106].

In summary the performance, security and privacy analysis of symmetric encryption-based pseudonym approaches are shown in Tables 7–9, respectively.

Table 7. Symmetric based encryption schemes performance.

Research Papers	Scalability	Security/Privacy	Computational Cost	Communication Overhead	Latency
[93]	High	Low	Medium	Medium	Medium
[94]	High	Low	Medium	Medium	Medium
[95]	High	Low	Low	Medium	Medium
[96]	High	Low	Low	Medium	Medium
[97]	High	Low	Low	Low	Medium
[98]	High	Low	Low	Low	Low
[99]	High	Low	High	Medium	High
[100]	High	Low	High	Medium	High
[101]	High	Low	High	High	High
[102]	High	Low	Low	High	High

Table 8. Attacks on symmetric based encryption schemes.

Research Papers	Node Capture	Malicious Code Injection	False Data Injection	Replay	Side-channel	Eavesdropping
[93]	No	No	Yes	Yes	Yes	No
[94]	No	Yes	Yes	Yes	Yes	Yes
[95]	No	No	No	Yes	Yes	No
[96]	No	No	Yes	Yes	Yes	No
[97]	No	Yes	Yes	Yes	Yes	Yes
[98]	No	No	Yes	Yes	Yes	No
[99]	No	Yes	Yes	No	Yes	Yes
[100]	No	Yes	Yes	Yes	Yes	Yes
[101]	No	No	Yes	Yes	Yes	No
[102]	No	No	Yes	Yes	No	No

Table 9. Attacks on symmetric based encryption schemes.

Research Papers	DoS	Spoofing	Sinkhole	Wormhole	MIMA	Sybil	Phishing	Malicious Virus	Malicious Script
[93]	Yes	No	Yes	Yes	No	Yes	Yes	No	No
[94]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
[95]	Yes	No	No	No	Yes	Yes	No	No	No
[96]	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
[97]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
[98]	Yes	No	No	Yes	Yes	No	Yes	Yes	Yes
[99]	Yes	Yes	Yes	Yes	Yes	No	No	Yes	Yes
[100]	No	Yes	Yes	Yes	Yes	No	No	No	No
[101]	Yes	Yes	No	No	Yes	No	No	Yes	Yes
[102]	Yes	Yes	No	No	Yes	No	No	No	No

6. Hybrid Privacy Schemes

Hybrid privacy schemes are the combination of the GSB and pseudonym-based schemes to provide a reliable framework for ITS. Calandriello et al. [107], presented a hybrid security

technique by combining standard pseudonym and group signature-based approach to induce self pseudonyms. The technique presented in [107], minimizes the computational overhead but introduces the problem of maintaining a large CRL and timely sharing of CRL to vehicles. Furthermore, self-generated pseudonyms introduce the problem of Sybil attacks. Another hybrid security approach is authentication with multiple levels of anonymity (AMLA) discussed by Bharadiya et al. [108]. The AMLA reduces computational and transmission costs but is prone to identity leaks, replay, and DoS attacks. Hence the security of AMLA is low and does not provide strong anonymity.

Wagan et al. [109] presented a hybrid approach, in which a group captain is selected on the basis of the same direction traveling. However, how a group captain is selected has not been properly addressed. Similarly, there are chances of malicious activities as no proper revocation mechanism for malicious vehicles are discussed. The approach [109] is time consuming because of the processes of computing keys, random numbers, and hashes are performed at the same time besides verification of hashes. The scheme is not scalable and provides low security.

Khodaei et al. [110] presented a hybrid scheme called RHyTHM. The scheme [110] suggested that the group manager allows a vehicle to sign a safety beacon in lieu of the class. If a vehicle runs out of pseudonyms, the vehicle executes a RHyTHM protocol, in which RHyTHM flag is sent in the message to the class. The outdated vehicle then uses self-generated pseudonyms for communication. However, there is the possibility of malicious attacks, in the case of self-generated pseudonyms. The approach has a high computational overhead in case of ITS. Similarly, the average latency and communication overhead is also high. In order to ensure that only trustworthy vehicles are tabbed for the relay is still a great challenge. Hu et al. [111] proposed a hybrid approach called privacy preserving trust basedrelay scheme (PTRS). The scheme suggested that there should be a trust/reputation value that ensures the trustworthiness of a relayed node. Trust authority (TA) is the sole entity of all information on vehicles and is a single point of attack. TA decides the trust level. However, the scheme is prone to replay attack. Furthermore, the computational and communication overheads are high. The vehicle can choose another vehicle for a relay that is to transmit messages. However, due to misreporting/obfuscation, a malicious vehicle can be selected as a relay.

In order to sum up the hybrid privacy approaches performance, Tables 10–12 show the performance, security, and privacy analysis, respectively.

Table 10. Hybrid security and privacy schemes performance.

Research Papers	Scalability	Security/Privacy	Computational Cost	Communication Overhead	Latency
[107]	Medium	Low	Medium	High	High
[108]	Medium	Low	Medium	Medium	Medium
[109]	Low	Low	High	High	High
[110]	Low	Low	High	High	High
[111]	Low	Low	High	High	High

Table 11. Attacks on hybrid security and privacy schemes.

Research Papers	Node Capture	Malicious Code Injection	False Data Injection	Replay	Side-Channel	Eavesdropping
[107]	No	No	No	Yes	Yes	Yes
[108]	Yes	Yes	Yes	Yes	No	Yes
[109]	No	No	Yes	Yes	No	Yes
[110]	Yes	Yes	Yes	Yes	No	No
[111]	Yes	No	Yes	Yes	No	Yes

Table 12. Attacks On hybrid security and privacy schemes.

Research Papers	DoS	Spoofing	Sinkhole	Wormhole	MIMA	Sybil	Phishing	Malicious Virus	Malicious Script
[107]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
[108]	Yes	Yes	No	No	Yes	No	Yes	Yes	Yes
[109]	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
[110]	Yes	No	No	No	No	Yes	Yes	Yes	Yes
[111]	No	Yes	No	No	No	Yes	Yes	No	No

7. Integration of ITS in Cloud

ITS can be integrated with the cloud to form the Internet of ITS-Ss [112]. Using the Internet of Things (IoT) technology in ITS forms Internet of ITS-Ss (IoITS-Ss) to achieve the applications of IoT in ITS. ITS is different from early networks as it has the characteristics of high speed, sparse and dense scenarios, point of interest spots, dynamic topology, security, location and identity privacy. As ITS-Ss (vehicles) on the internet of ITS-Ss are vulnerable to different types of security and privacy attacks from the perspective of global, local, passive, active attacks in the access layer, networking, and transport layer and facilities layer as discussed in Section 2 of this paper. The aim of IoITS-Ss is to gain infotainment services or other services through the Internet. Infotainment services include media downloading, electronic commerce, insurance, real time traffic analysis, parking guidance, and other point of interest services. As shown in Figure 3, the dissemination architecture of ITS, the internet/cloud services are accessed through 3G/4G/5G technology.

The main aim of IoITS-Ss is to provide convenience for ITS users. After connection of ITS with cloud provides more enhanced features like online traffic guidance [113]. ITS can be seen as a type of IoT. IoITS-Ss work well if the distances between ITS-Ss (vehicles) are large. DSRC provides communication range up to 1000 m. In scenarios where the number of vehicles are less, providing internet services is a great challenge for ITS. This will affect the typical applications of ITS, which are road safety, traffic efficiency, and comfort. In IoITS-Ss security and privacy is a great challenge, because of transportation crashes by untrue contents from IoITS-Ss heads straight to accidents, kidnapping, and cost of family living. Also, people want to keep their driving private. However, IoITS-Ss cloud takes ITS-Ss information and thus vehicles privacy can be leaked. If vehicles use the cloud more and more, the security and privacy are at great risk. In IoITS-Ss a part of information can be live and a part of information can be private to protect the privacy of vehicles. Cloud security and privacy in IoITS-Ss ensure vehicles security and privacy. According to [114–117], the following types of security and privacy attacks in IoITS-Ss—i.e., snooping, status spoofing, information altering, DoS, repudiation, obstruct, intervention, etc.—as discussed in Section 2 of this paper demise the performance, strength, vigor, privacy, and security. Scalable and trustworthy security and privacy techniques should be designed to address the issues of different types of attacks as discussed in Section 2 of this paper.

8. Conclusions

In this paper, we have discussed security and privacy issues in VANETs based ITS. Due to regular sensitive updates as beacons sent by vehicular nodes, security and privacy become key to its successful adoption. Although the subjects of security and privacy complement each other, our structured approach to the discussion ensured that we addressed both as separate but very key entities in the subject of ITS. ITS privacy as a subject has always been jumbled up with security discussions and addressed as a minor part of a whole, but here, we made it a focal point. To make ITS safe from security and privacy attacks, security and privacy techniques must be imposed. The perfect security and privacy techniques for ITS are still a big challenge for researchers. In this paper, we have discussed different types of security and privacy attacks and possible solutions to efficiently address the security and privacy issues in ITS. We also categorized and compared different ITS security and privacy schemes with respect to scalability, security and privacy, computational cost, communication overhead, and latency. Some schemes provide good security and privacy but are not scalable and

incur high computational and communication costs. While other approaches have low computational and communication costs but provide low security and privacy. This paper motivates researchers in the field of security and privacy for robust and panoramic solutions to the aforementioned issues described in the various sections.

Author Contributions: The main idea of the paper is proposed by Q.E.A. Q.E.A., N.A. and A.H.M. have systematically reviewed the literature and collected relevant data for analysis and comparisons. W.u.R. and G.A. finalized the structure of the paper. All the authors approved and read the final draft of the manuscript.

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

References

1. Dixit, M.; Kumar, R.; Sagar, A.K. Vanet: Architectures, research issues, routing protocols, and its applications. In Proceedings of the IEEE 2016 International Conference on Computing, Communication and Automation (ICCCA), Noida, India, 29–30 April 2016; pp. 555–561.
2. Browand, F.; McArthur, J.; Radovich, C. *Fuel Saving Achieved in the Field Test of Two Tandem Trucks*; PATH Technical Report for Task Order-4214; California PATH Program: Richmond, CA, USA, April 2004.
3. Vaibhav, A.; Shukla, D.; Das, S.; Sahana, S.; Johri, P. Security challenges, authentication, application and trust models for vehicular ad hoc network—A survey. *Int. J. Wirel. Microw. Technol.* **2017**, *3*, 36–48. [CrossRef]
4. Mejri, M.N.; Ben-Othman, J.; Hamdi, M. Survey on vanet security challenges and possible cryptographic solutions. *Veh. Commun.* **2014**, *1*, 53–66. [CrossRef]
5. Tangade, S.S.; Manvi, S.S. A survey on attacks, security and trust management solutions in vanets. In Proceedings of the IEEE 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), Tiruchengode, India, 4–6 July 2013; pp. 1–6.
6. Van der Heijden, R.; Argiolu, R.; Marchau, V. *Urban Land Use Changes and ICT-Based Innovation of Public Transport*; WIT Press: Billerica, MA, USA, 2004.
7. Baiocchi, A.; Cuomo, F.; de Felice, M.; Fusco, G. Vehicular ad-hoc networks sampling protocols for traffic monitoring and incident detection in intelligent transportation systems. *Transp. Res. Part C Emerg. Technol.* **2015**, *56*, 177–194. [CrossRef]
8. European Telecommunications Standards Institute. *102 940: Intelligent Transport Systems (Its); Security; Its Communications Security Architecture and Security Management*; Technical Specification; European Telecommunications Standards Institute: Nice, France, 2012.
9. Al-Sultan, S.; Al-Doori, M.M.; Al-Bayatti, A.H.; Zedan, H. A comprehensive survey on vehicular ad hoc network. *J. Netw. Comput. Appl.* **2014**, *37*, 380–392. [CrossRef]
10. Toor, Y.; Muhlethaler, P.; Laouiti, A. Vehicle ad hoc networks: Applications and related technical issues. *IEEE Commun. Surv. Tutor.* **2008**, *10*, 74–88. [CrossRef]
11. IEEE. *IEEE 802.11p Task Group*; IEEE: Washington, DC, USA, 19 November 2017.
12. DOT. *ASTM e2213-03 Standard Specification for Telecommunications and Information Exchange between Roadside and Vehicle Systems—5 ghz Band Dedicated Short Range Communications (DSRC) Medium access control (MAC) and Physical Layer (PHY) Specifications*; U.S. Department of Transportation: Washington, DC, USA, January 2010.
13. Bhoi, S.K.; Khilar, P.M. Vehicular communication: A survey. *IET Netw.* **2013**, *3*, 204–217. [CrossRef]
14. Lu, N.; Cheng, N.; Zhang, N.; Shen, X.; Mark, J.W. Connected vehicles: Solutions and challenges. *IEEE Internet Things J.* **2014**, *1*, 289–299. [CrossRef]
15. Karagiannis, G.; Altintas, O.; Ekici, E.; Heijenk, G.; Jarupan, B.; Lin, K.; Weil, T. Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions. *IEEE Commun. Surv. Tutor.* **2011**, *13*, 584–616. [CrossRef]
16. IEEE. *IEEE 1609 WG-DSRC Working Group*; IEEE: Washington, DC, USA, 2015.
17. Cailean, A.-M.; Cagneau, B.; Chassagne, L.; Popa, V.; Dimian, M. A survey on the usage of DSRC and VLC in communication-based vehicle safety applications. In Proceedings of the 2014 IEEE 21st Symposium on Communications and Vehicular Technology in the Benelux (SCVT), Delft, The Netherlands, 10 November 2014; pp. 69–74.
18. Yao, Y.; Rao, L.; Liu, X. Performance and reliability analysis of IEEE 802.11p safety communication in a highway environment. *IEEE Trans. Veh. Technol.* **2013**, *62*, 4198–4212. [CrossRef]

19. Uzc'ategui, R.A.; de Sucre, A.J.; Acosta-Marum, G. Wave: A tutorial. *IEEE Commun. Mag.* **2009**, *47*, 126–133. [CrossRef]
20. Manvi, S.; Kakkasageri, M. Issues in mobile ad hoc networks for vehicular communication. *IETE Tech. Rev.* **2008**, *25*, 59–72.
21. Zhang, J. A survey on trust management for vanets. In Proceedings of the 2011 IEEE International Conference on Advanced Information Networking and Applications (AINA), Singapore, 22–25 March 2011; pp. 105–112.
22. Shen, X.; Cheng, X.; Yang, L.; Zhang, R.; Jiao, B. Data dissemination in vanets: A scheduling approach. *IEEE Trans. Intell. Transp. Syst.* **2014**, *15*, 2213–2223. [CrossRef]
23. Bouassida, M.S. Authentication vs. privacy within vehicular ad hoc networks. *Int. J. Netw. Secur.* **2011**, *13*, 121–134.
24. Lin, J.; Yu, W.; Zhang, N.; Yang, X.; Zhang, H.; Zhao, W. A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. *IEEE Internet Things J.* **2017**, *4*, 1125–1142. [CrossRef]
25. Andrea, I.; Chrysostomou, C.; Hadjichristofi, G. Internet of things: Security vulnerabilities and challenges. In Proceedings of the 2015 IEEE Symposium on Computers and Communication (ISCC), Larnaca, Cyprus, 6–9 July 2015; pp. 180–187.
26. Niu, J.; Jin, Y.; Lee, A.J.; Sandhu, R.; Xu, W.; Zhang, X. Panel security and privacy in the age of internet of things: Opportunities and challenges. In Proceedings of the 21st ACM on Symposium on Access Control Models and Technologies, Shanghai, China, 6–8 June 2016; pp. 49–50.
27. Qu, F.; Wu, Z.; Wang, F.-Y.; Cho, W. A security and privacy review of vanets. *IEEE Trans. Intell. Transp. Syst.* **2015**, *16*, 2985–2996. [CrossRef]
28. Engoulou, R.G.; Bellaïche, M.; Pierre, S.; Quintero, A. Vanet security surveys. *Comput. Commun.* **2014**, *44*, 1–13. [CrossRef]
29. Petit, J.; Schaub, F.; Feiri, M.; Kargl, F. Pseudonym schemes in vehicular networks: A survey. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 228–255. [CrossRef]
30. Boualouache, A.; Senouci, S.-M.; Moussaoui, S. A survey on pseudonym changing strategies for vehicular ad-hoc networks. *IEEE Commun. Surv. Tutor.* **2017**, *20*, 770–790. [CrossRef]
31. Lin, X.; Lu, R.; Zhang, C.; Zhu, H.; Ho, P.-H.; Shen, X. Security in vehicular ad hoc networks. *IEEE Commun. Mag.* **2008**, *46*, 88–95.
32. 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 IEEE 2015 International Conference on Computing, Networking and Communications (ICNC), Garden Grove, CA, USA, 16–19 February 2015; pp. 395–400.
33. Eckhoff, D.; Sommer, C.; Gansen, T.; German, R.; Dressler, F. Strong and affordable location privacy in vanets: Identity diffusion using time-slots and swapping. In Proceedings of the 2010 IEEE Vehicular Networking Conference (VNC), Jersey City, NJ, USA, 13–15 December 2010; pp. 174–181.
34. Capkun, S.; Buttyan, L.; Hubaux, J.-P. Self-organized public-key management for mobile ad hoc networks. *IEEE Trans. Mob. Comput.* **2003**, *2*, 52–64. [CrossRef]
35. Yang, X.; Lin, J.; Yu, W.; Moulema, P.-M.; Fu, X.; Zhao, W. A novel en-route filtering scheme against false data injection attacks in cyber-physical networked systems. *IEEE Trans. Comput.* **2015**, *64*, 4–18. [CrossRef]
36. Maheswari, S.U.; Usha, N.; Anita, E.M.; Devi, K.R. A novel robust routing protocol RAEED to avoid DoS attacks in WSN. In Proceedings of the IEEE 2016 International Conference on Information Communication and Embedded Systems (ICICES), Chennai, India, 25–26 February 2016; pp. 1–5.
37. Chuang, M.-C.; Lee, J.-F. Team: Trust-extended authentication mechanism for vehicular ad hoc networks. *IEEE Syst. J.* **2014**, *8*, 749–758. [CrossRef]
38. Yang, X.; Ren, X.; Lin, J.; Yu, W. On binary decomposition based privacy-preserving aggregation schemes in real-time monitoring systems. *IEEE Trans. Parallel Distrib. Syst.* **2016**, *27*, 2967–2983. [CrossRef]
39. Zhang, L.; Cai, Z.; Wang, X. Fakemask: A novel privacy preserving approach for smartphones. *IEEE Trans. Netw. Serv. Manag.* **2016**, *13*, 335–348. [CrossRef]
40. Ren, X.; Yang, X.; Lin, J.; Yang, Q.; Yu, W. On scaling perturbation based privacy-preserving schemes in smart metering systems. In Proceedings of the IEEE 2013 22nd International Conference on Computer Communications and Networks (ICCCN), Nassau, Bahamas, 30 July–2 August 2013; pp. 1–7.
41. Cai, Z.; He, Z.; Guan, X.; Li, Y. Collective data-sanitization for preventing sensitive information inference attacks in social networks. *IEEE Trans. Dependable Secure Comput.* **2018**, *15*, 577–590. [CrossRef]

42. Zhao, N.; Yu, F.R.; Li, M.; Leung, V.C. Anti-eavesdropping schemes for interference alignment (IA)-based wireless networks. *IEEE Trans. Wirel. Commun.* **2016**, *15*, 5719–5732. [CrossRef]
43. Bharathi, M.V.; Tanguturi, R.C.; Jayakumar, C.; Selvamani, K. Node capture attack in wireless sensor network: A survey. In Proceedings of the 2012 IEEE International Conference on Computational Intelligence & Computing Research (ICCIC), Coimbatore, India, 18–20 December 2012; pp. 1–3.
44. Yang, X.; He, X.; Yu, W.; Lin, J.; Li, R.; Yang, Q.; Song, H. Towards a low-cost remote memory attestation for the smart grid. *Sensors* **2015**, *15*, 20799–20824. [CrossRef] [PubMed]
45. Seshadri, A.; Perrig, A.; van Doorn, L.; Khosla, P. Swatt: Software-based attestation for embedded devices. In Proceedings of the 2004 IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 9–12 May 2004; pp. 272–282.
46. Lin, J.; Yu, W.; Yang, X. Towards multistep electricity prices in smart grid electricity markets. *IEEE Trans. Parallel Distrib. Syst.* **2016**, *27*, 286–302. [CrossRef]
47. Mo, Y.; Sinopoli, B. Secure control against replay attacks. In Proceedings of the IEEE 2009 47th Annual Allerton Conference on Communication, Control, and Computing, Monticello, IL, USA, 30 September–2 October 2009; pp. 911–918.
48. Zhao, K.; Ge, L. A survey on the internet of things security. In Proceedings of the IEEE 2013 9th International Conference on Computational Intelligence and Security (CIS), Emeishan, China, 14–15 December 2013; pp. 663–667.
49. Cho, C.-H.; Do, K.-H.; Kim, J.-W.; Jun, M.-S. Design of RFID mutual authentication protocol using time stamp. In Proceedings of the IEEE Fourth International Conference on Computer Sciences and Convergence Information Technology (ICCIT'09), Seoul, Korea, 24–26 November 2009; pp. 1047–1051.
50. Zhang, J.; Gu, D.; Guo, Z.; Zhang, L. Differential power cryptanalysis attacks against present implementation. In Proceedings of the IEEE 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), Chengdu, China, 20–22 August 2010; Volume 6, pp. V6–V61.
51. Gomez, G.; Lopez-Martinez, F.J.; Morales-Jimenez, D.; McKay, M.R. On the equivalence between interference and eavesdropping in wireless communications. *IEEE Trans. Veh. Technol.* **2015**, *64*, 5935–5940. [CrossRef]
52. Mohammed, J.R. A new simple adaptive noise cancellation scheme based on ale and NLMS filter. In Proceedings of the IEEE 2007 Fifth Annual Conference on Communication Networks and Services Research (CNSR'07), Fredericton, NB, Canada, 14–17 May 2007; pp. 245–254.
53. Mahmoud, R.; Yousuf, T.; Aloul, F.; Zualkernan, I. Internet of things (IOT) security: Current status, challenges and prospective measures. In Proceedings of the IEEE 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), London, UK, 14–16 December 2015; pp. 336–341.
54. Mukaddam, A.; Elhajj, I.; Kayssi, A.; Chehab, A. Ip spoofing detection using modified hop count. In Proceedings of the 2014 IEEE 28th International Conference on Advanced Information Networking and Applications (AINA), Victoria, BC, Canada, 13–16 May 2014; pp. 512–516.
55. Wang, X.; Yu, W.; Champion, A.; Fu, X.; Xuan, D. Detecting worms via mining dynamic program execution. In Proceedings of the IEEE Third International Conference on Security and Privacy in Communications Networks and the Workshops (SecureComm 2007), Nice, France, 17–21 September 2007; pp. 412–421.
56. Ibrahim, A.; Rahman, M.M.; Roy, M.C. Detecting sinkhole attacks in wireless sensor network using hop count. *Int. J. Comput. Netw. Inf. Secur.* **2015**, *7*, 50.
57. Kalnoor, G.; Agarkhed, J. Qos based multipath routing for intrusion detection of sinkhole attack in wireless sensor networks. In Proceedings of the IEEE 2016 International Conference on Circuit, Power and Computing Technologies (ICCPCT), Nagercoil, India, 18–19 March 2016; pp. 1–6.
58. Lee, P.; Clark, A.; Bushnell, L.; Poovendran, R. A passivity framework for modeling and mitigating wormhole attacks on networked control systems. *IEEE Trans. Autom. Control* **2014**, *59*, 3224–3237. [CrossRef]
59. Padhy, R.P.; Patra, M.R.; Satapathy, S.C. Cloud computing: Security issues and research challenges. *Int. J. Comput. Netw. Inf. Secur.* **2011**, *1*, 136–146.
60. Newsome, J.; Shi, E.; Song, D.; Perrig, A. The sybil attack in sensor networks: Analysis & defenses. In Proceedings of the 3rd ACM International Symposium on Information Processing in Sensor Networks, Berkeley, CA, USA, 26–27 April 2004; pp. 259–268.
61. Jagatic, T.N.; Johnson, N.A.; Jakobsson, M.; Menczer, F. Social phishing. *Commun. ACM* **2007**, *50*, 94–100. [CrossRef]

62. Yu, W.; Zhang, N.; Fu, X.; Zhao, W. Self-disciplinary worms and countermeasures: Modeling and analysis. *IEEE Trans. Parallel Distrib. Syst.* **2010**, *21*, 1501–1514. [CrossRef]
63. Sahoo, A.K.; Das, A.; Tiwary, M. Firewall engine based on graphics processing unit. In Proceedings of the IEEE 2014 International Conference on Advanced Communication Control and Computing Technologies (ICACCCT), Ramanathapuram, India, 8–10 May 2014; pp. 758–763.
64. Assembly, U.G. *Universal Declaration of Human Rights*; UN General Assembly: New York, NY, USA, 10 December 1948.
65. Puttaswamy, K.P.; Bhagwan, R.; Padmanabhan, V.N. Anonygator: Privacy and integrity preserving data aggregation. In Proceedings of the ACM/IFIP/USENIX 11th International Conference on Middleware; Springer-Verlag: Berlin, Germany, 29 November 2010; pp. 85–106.
66. Girao, J.; Westhoff, D.; Schneider, M. Cda: Concealed data aggregation for reverse multicast traffic in wireless sensor networks. In Proceedings of the 2005 IEEE International Conference on Communications (ICC 2005), Seoul, Korea, 16–20 May 2005; Volume 5, pp. 3044–3049.
67. He, W.; Liu, X.; Nguyen, H.; Nahrstedt, K.; Abdelzaher, T. Pda: Privacy-preserving data aggregation in wireless sensor networks. In Proceedings of the 26th IEEE International Conference on Computer Communications (INFOCOM 2007), Barcelona, Spain, 6–12 May 2007; pp. 2045–2053.
68. Pingley, A.; Yu, W.; Zhang, N.; Fu, X.; Zhao, W. Cap: A context-aware privacy protection system for location-based services. In Proceedings of the 29th IEEE International Conference on Distributed Computing Systems (ICDCS'09), Montreal, QC, Canada, 22–26 June 2009; pp. 49–57.
69. Pingley, A.; Yu, W.; Zhang, N.; Fu, X.; Zhao, W. A context-aware scheme for privacy-preserving location-based services. *Comput. Netw.* **2012**, *56*, 2551–2568. [CrossRef]
70. Qiu, F.; Wu, F.; Chen, G. Privacy and quality preserving multimedia data aggregation for participatory sensing systems. *IEEE Trans. Mob. Comput.* **2015**, *14*, 1287–1300. [CrossRef]
71. Zhang, L.; Luo, J.; Yang, M. An improved DSSS-based flow marking technique for anonymous communication traceback. In Proceedings of the IEEE 2009 Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing (UIC-ATC'09), Brisbane, QLD, Australia, 7–9 July 2009; pp. 563–567.
72. Ling, Z.; Luo, J.; Yu, W.; Fu, X.; Xuan, D.; Jia, W. A new cell counter based attack against tor. In Proceedings of the 16th ACM Conference on Computer and Communications Security, Chicago, IL, USA, 9–13 November 2009; pp. 578–589.
73. Ling, Z.; Luo, J.; Yu, W.; Fu, X.; Xuan, D.; Jia, W. A new cell-counting-based attack against tor. *IEEE/ACM Trans. Netw.* **2012**, *20*, 1245–1261. [CrossRef]
74. Guo, J.; Baugh, J.P.; Wang, S. A group signature based secure and privacy-preserving vehicular communication framework. In Proceedings of the IEEE 2007 Mobile Networking for Vehicular Environments, Anchorage, AK, USA, 11 May 2007; pp. 103–108.
75. Zhu, X.; Jiang, S.; Wang, L.; Li, H. Efficient privacy-preserving authentication for vehicular ad hoc networks. *IEEE Trans. Veh. Technol.* **2014**, *63*, 907–919. [CrossRef]
76. Wasef, A.; Shen, X. Efficient group signature scheme supporting batch verification for securing vehicular networks. In Proceedings of the 2010 IEEE International Conference on Communications (ICC), Cape Town, South Africa, 23–27 May 2010; pp. 1–5.
77. Zhang, L.; Wu, Q.; Solanas, A.; Domingo-Ferrer, J. A scalable robust authentication protocol for secure vehicular communications. *IEEE Trans. Veh. Technol.* **2010**, *59*, 1606–1617. [CrossRef]
78. 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.
79. Huang, J.-L.; Yeh, L.-Y.; Chien, H.-Y. Abaka: An anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks. *IEEE Trans. Veh. Technol.* **2011**, *60*, 248–262. [CrossRef]
80. Zhang, C.; Lin, X.; Lu, R.; Ho, P.-H.; Shen, X. An efficient message authentication scheme for vehicular communications. *IEEE Trans. Veh. Technol.* **2008**, *57*, 3357–3368. [CrossRef]
81. Horng, S.-J.; Tzeng, S.-F.; Pan, Y.; Fan, P.; Wang, X.; Li, T.; Khan, M.K. b-specs+: Batch verification for secure pseudonymous authentication in vanet. *IEEE Trans. Inf. Forensics Secur.* **2013**, *8*, 1860–1875. [CrossRef]
82. Hao, Y.; Cheng, Y.; Zhou, C.; Song, W. A distributed key management framework with cooperative message authentication in vanets. *IEEE J. Sel. Areas Commun.* **2011**, *29*, 616–629. [CrossRef]
83. Lin, X.; Li, X. Achieving efficient cooperative message authentication in vehicular ad hoc networks. *IEEE Trans. Veh. Technol.* **2013**, *62*, 3339–3348.

84. Kumar, N.; Iqbal, R.; Misra, S.; Rodrigues, J.J. An intelligent approach for building a secure decentralized public key infrastructure in vanet. *J. Comput. Syst. Sci.* **2015**, *81*, 1042–1058. [CrossRef]
85. Al-Kahtani, M.S. Survey on security attacks in vehicular ad hoc networks (vanets). In Proceedings of the IEEE 2012 6th International Conference on Signal Processing and Communication Systems (ICSPCS), Gold Coast, QLD, Australia, 12–14 December 2012; pp. 1–9.
86. Raya, M.; Hubaux, J.-P. Securing vehicular ad hoc networks. *J. Comput. Secur.* **2007**, *15*, 39–68. [CrossRef]
87. Wasef, A.; Shen, X. Emap: Expedite message authentication protocol for vehicular ad hoc networks. *IEEE Trans. Mob. Comput.* **2013**, *12*, 78–89. [CrossRef]
88. Woodbury, A.D.; Bailey, D.V.; Paar, C. Elliptic curve cryptography on smart cards without coprocessors. In *Smart Card Research and Advanced Applications*; Springer: Boston, MA, USA, 2000; pp. 71–92.
89. Manvi, S.; Kakkasageri, M.; Adiga, D. Message authentication in vehicular ad hoc networks: ECDSA based approach. In Proceedings of the 2009 IEEE International Conference on Future Computer and Communication (ICFCC 2009), Kuala Lumpur, Malaysia, 3–5 April 2009; pp. 16–20.
90. Petit, J. Analysis of ecdsa authentication processing in vanets. In Proceedings of the IEEE 2009 3rd International Conference on New Technologies, Mobility and Security (NTMS), Cairo, Egypt, 20–23 December 2009; pp. 1–5.
91. Haas, J.J.; Hu, Y.-C.; Laberteaux, K.P. Real-world vanet security protocol performance. In Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM 2009), Honolulu, HI, USA, 30 November–4 December 2009; pp. 1–7.
92. 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 IEEE 2013 8th International ICST Conference on Communications and Networking in China (CHINACOM), Guilin, China, 14–16 August 2013; pp. 149–154.
93. Schaub, F.; Kargl, F.; Ma, Z.; Weber, M. V-tokens for conditional pseudonymity in vanets. In Proceedings of the 2010 IEEE Wireless Communications and Networking Conference (WCNC), Sydney, Australia, 18–21 April 2010; pp. 1–6.
94. Rhim, W. A Study on Mac-Based Efficient Message Authentication Scheme for VANET. Master's Thesis, Hanyang University, Seoul, Korea, 2012.
95. Carianha, A.M.; Barreto, L.P.; Lima, G. Improving location privacy in mix-zones for vanets. In Proceedings of the 2011 IEEE 30th International Performance Computing and Communications Conference (IPCCC), Orlando, FL, USA, 17–19 November 2011; pp. 1–6.
96. Sun, Y.; Lu, R.; Lin, X.; Shen, X.; Su, J. An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications. *IEEE Trans. Veh. Technol.* **2010**, *59*, 3589–3603. [CrossRef]
97. Wang, M.; Liu, D.; Zhu, L.; Xu, Y.; Wang, F. Lespp: Lightweight and efficient strong privacy preserving authentication scheme for secure vanet communication. *Computing* **2016**, *98*, 685–708. [CrossRef]
98. Chim, T.W.; Yiu, S.; Hui, L.C.; Li, V.O. Security and privacy issues for inter-vehicle communications in vanets. In Proceedings of the 6th Annual IEEE Communications Society Conference on Sensor, Mesh and ad hoc Communications and Networks Workshops (SECON Workshops' 09), Rome, Italy, 22–26 June 2009; pp. 1–3.
99. Vighnesh, N.; Kavita, N.; Urs, S.R.; Sampalli, S. A novel sender authentication scheme based on hash chain for vehicular ad-hoc networks. In Proceedings of the 2011 IEEE Symposium on Wireless Technology and Applications (ISWTA), Langkawi, Malaysia, 25–28 September 2011; pp. 96–101.
100. He, L.; Zhu, W.T. Mitigating dos attacks against signature-based authentication in vanets. In Proceedings of the 2012 IEEE International Conference on Computer Science and Automation Engineering (CSAE), Zhangjiajie, China, 25–27 May 2012; Volume 3, pp. 261–265.
101. Jahanian, M.H.; Amin, F.; Jahangir, A.H. Analysis of tesla protocol in vehicular ad hoc networks using timed colored petri nets. In Proceedings of the IEEE 2015 6th International Conference on Information and Communication Systems (ICICS), Amman, Jordan, 7–9 April 2015; pp. 222–227.
102. Studer, A.; Bai, F.; Bellur, B.; Perrig, A. Flexible, extensible, and efficient vanet authentication. *J. Commun. Netw.* **2009**, *11*, 574–588. [CrossRef]
103. Teichel, K.; Sibold, D.; Milius, S. An attack possibility on time synchronization protocols secured with tesla-like mechanisms. In *Information Systems Security*; Springer: Cham, Switzerland, 16 December 2016; pp. 3–22.
104. Wang, F.; Xu, Y.; Zhang, H.; Zhang, Y.; Zhu, L. 2flip: A two-factor lightweight privacy-preserving authentication scheme for vanet. *IEEE Trans. Veh. Technol.* **2016**, *65*, 896–911. [CrossRef]

105. Liu, Y.; Wang, L.; Chen, H.-H. Message authentication using proxy vehicles in vehicular ad hoc networks. *IEEE Trans. Veh. Technol.* **2015**, *64*, 3697–3710. [CrossRef]
106. Perrig, A.; Canetti, R.; Tygar, J.D.; Song, D. Efficient authentication and signing of multicast streams over lossy channels. In Proceedings of the 2000 IEEE Symposium on Security and Privacy (S&P 2000), Berkeley, CA, USA, 14–17 May 2000; pp. 56–73.
107. Calandriello, G.; Papadimitratos, P.; Hubaux, J.-P.; Lioy, A. Efficient and robust pseudonymous authentication in vanet. In Proceedings of the Fourth ACM International Workshop on Vehicular ad hoc Networks, Montreal, QC, Canada, 10 September 2007; pp. 19–28.
108. Bhavesh, N.B.; Maity, S.; Hansdah, R.C. A protocol for authentication with multiple levels of anonymity (amla) in vanets. In Proceedings of the IEEE 2013 27th International Conference on Advanced Information Networking and Applications Workshops (WAINA), Barcelona, Spain, 25–28 March 2013; pp. 462–469.
109. Wagan, A.A.; Mughal, B.M.; Hasbullah, H. Vanet security framework for trusted grouping using TPM hardware. In Proceedings of the IEEE Second International Conference on Communication Software and Networks (ICCSN'10), Singapore, 26–28 February 2010; pp. 309–312.
110. Khodaei, M.; Messing, A.; Papadimitratos, P. Rhythm: A randomized hybrid scheme to hide in the mobile crowd. *arXiv*, 2017; arXiv:1712.03405.
111. Hu, H.; Lu, R.; Huang, C.; Zhang, Z. Ptrs: A privacy-preserving trust-based relay selection scheme in vanets. *Peer-to-Peer Netw. Appl.* **2017**, *10*, 1204–1218. [CrossRef]
112. Sun, Y.; Wu, L.; Wu, S.; Li, S.; Zhang, T.; Zhang, L.; Xu, J.; Xiong, Y.; Cui, X. Attacks and countermeasures in the internet of vehicles. *Ann. Telecommun.* **2017**, *72*, 283–295. [CrossRef]
113. Ahmed, S.H.; Bouk, S.H.; Yaqub, M.A.; Kim, D.; Song, H.; Lloret, J. Codie: Controlled data and interest evaluation in vehicular named data networks. *IEEE Trans. Veh. Technol.* **2016**, *65*, 3954–3963. [CrossRef]
114. Lazarevic, A.; Srivastava, J.; Kumar, V. Cyber threat analysis–a key enabling technology for the objective force (a case study in network intrusion detection). In Proceedings of the 23rd Army Science Conference IT/C4ISR, Orlando, FL, USA, 2–5 December 2002.
115. Yu, L.; Deng, J.; Brooks, R.R.; Yun, S.B. Automobile ecu design to avoid data tampering. In Proceedings of the ACM 10th Annual Cyber and Information Security Research Conference, Oak Ridge, TN, USA, 7–9 April 2015; p. 10.
116. Sicari, S.; Rizzardi, A.; Grieco, L.A.; Coen-Porisini, A. Security, privacy and trust in internet of things: The road ahead. *Comput. Netw.* **2015**, *76*, 146–164. [CrossRef]
117. Singh, R.; Singh, P.; Duhan, M. An effective implementation of security based algorithmic approach in mobile ad hoc networks. *Hum. Cent. Comput. Inf. Sci.* **2014**, *4*, 7. [CrossRef]