VANET SECURITY AND PRIVACY – AN OVERVIEW

Marvy B. Mansour[1], Cherif Salama[2], Hoda K. Mohamed[3] and Sherif A. Hammad[4]

[1]British University in Egypt, Cairo, Egypt
[2,3]Computer and Systems Engineering Department, Ain Shams University, Cairo, Egypt
[4]Avelabs, Cairo, Egypt – Munich, Germany

ABSTRACT

Even though vehicular ad-hoc networks (VANETs) bring tremendous benefits to society, yet they raise many challenges where the security and privacy concerns are the most critical ones. In this paper, we provide a detailed overview of the state-of-the-art security and privacy requirements in VANET. Also, a brief of the approachesthat are proposed in the literature to fulfil these requirements is given in this paper. Besides that, a classification of the various VANET attacks based on the communication system layersisprovided in this paper. In addition, the different types of VANET adversaries and attackers arepresented here.In general, this paper aims to provide a good piece of information about VANET security and privacy, in order to be used as a tool to help researchers in this field in developing secure privacy-preserving approaches for VANET.

KEYWORDS

Security and Privacy Requirements in VANET, VANET Adversaries and Attackers, VANET Attacks, VANET Security and Privacy Approaches

1. INTRODUCTION

Nowadays, vehicles are equipped with high-technology devices, such as: GPS navigators, radars, and on-board units (OBUs). These wireless-enabled devices make vehicles intelligent and able to communicate with each other, and thereby form a self-organized vehicular ad-hoc network (VANET)[1]. Most proposed system architectures for VANET need to equip vehicles with a box thatcontains a radio interface to enable wireless communication between vehicles.The rapid mobility and dynamically changing topology of VANET cannot use the current IEEE wireless protocols 802.11 in its present state, so a modified version named 802.11p was developed by IEEE for vehicular networks. The modifications were mostly done in the MAC layer. Many wireless technologies like: a) IEEE 802.11p that is a standard for Dedicated Short Range Communication, DSRC, a Wifi typecalled Wireless Access in Vehicular Environment, WAVE, b) General Packet Radio Service (GPRS), c) IEEE 802.16 that is a standard for WiMAX, and d) 4G-Long Term Evolution (LTE) have been proposed for reliable vehicular communications.

Besides that, VANETs are always looked upon as systems that would open innovative and path breaking applications. Also, before the real technology hits the road, a series of detailed research is carried out around the world to make the system reliable and robust. In addition, VANETs are a promising area for the creation of Intelligent Transportation Systems (ITS)that provide assistance to drivers to increase their safety and comfort by offering useful services to them.Moreover, VANETis a kind of network that has two main types of communication: V2V and V2I, which are vehicle–to–vehicle and vehicle–to–infrastructure respectively. The set of applications that offer

DOI: 10.5121/ijnsa.2018.10202

comfort and convenience-based services are referred to as non-safety applications, while the safety applications are more concerned with life-saving services[1]. With the assistance of V2V and V2I communications, potentially fatal road accidents can be avoided; dangerous driving behaviors can be alerted; city traffic flows can be optimized; and traffic jams can be alleviated. However, sincevehicular communication systems (VCS) aim to serve people, any small error as unauthorized modification of data or system malfunction can be fatal.

Furthermore,VANETs command a unique grade of requirements to maintain liability and accountability of drivers involved in accidents, traffic violations, emission norms and irregularities in order to take punitive actions if adriver commits any crime. Besides that, location and context-aware services require pin-point user location and preferences to provide the most specific, exact and comprehensive list of personalized information.Despite that, communication of such information raises significant privacy issues that cannot be neglected. Also, privacy concerns in vehicular communications are necessary to provide protection for the user data from profiling and tracking. For example, location-based service applications have a high probability of privacy breaching and jeopardizing security-related issues [2], [3], [4], which decrease the widespread of VANET. Moreover, quality and privacy are two divergent tendencies that exist with VANET applications and have undeniable importance to the user[5].Thus, both industry and academia have paid extensive attentions to address the various VANET security- and privacy-related issues [6], [7]. On the account of improving and providing reliable services, many researchers have identified various privacy issues and came up with different techniques and approaches to maintainthe user's privacy, like the use of pseudonyms[8], mix-zones[9], [10], and group signatures [11]. However, some applications, such as safety critical ones,are time sensitive and prevent the use of security protocols with high computational overhead and cost [12]. Thus, security and privacy requirements in VANET should be taken into consideration when designing a robust system, otherwise, malicious attacks may ruin the original intention of VANET. In this context, prior to putting VANET into practice, it is important tohave an efficient secure privacy-preserving mechanism on board, which provides the needed security and privacy services while mitigates the well-known attacks in VANET.

The rest of this paper is organized as follows. In Section two, we briefly describe the essential security and privacy requirements in VANET. Then, in Section three, we provide anoverview of the security and privacy requirements versus the state-of-the-art approaches proposed for VANET security and privacy. While, in Section four, the main types of existing VANET adversaries, well-known attacks and attackers are discussed in details. Finally, in Section five, we conclude the paper.

2. Security and Privacy Requirements

In VANETs, malicious vehicles may disrupt the network performance, for example, via modifying or inserting fake information in the network,which could incur life-endangering accidents. There are three basic requirements that should be met in VANETs to deal with any threat, which are: authentication, integrity, and conditional privacy. These requirements are fundamental so that every VANET system should follow. However, there are other security and privacy requirements discussed in the literature[13]. Despite that, VANET brings in new challenges and conflicts between these security and privacy requirements in the system [14].

2.1 Security Requirements

There are several security requirements that should be taken into consideration when developing a secure architecture for VANET [15], [16], which are explainedin this section as follows:

- ***Authentication:***The basic and foremost requirement for vehicular network security is authentication. Authentication is essential for verifying a claim of authenticity. Particularly in VANET, authentication means verifying the identity of a vehicle and distinguishing legitimate vehicles from unauthorized vehicles. It is important to make sure that the transmitted messages originate from actual vehicles and not from non-existent nodes because transmission of malicious messages can lead to serious consequences like human injuries, traffic disruptions and in extreme cases may even lead to death. Also, an adversary may unnecessarily divert the traffic leading to chaos. Hence, message authentication is important in VANET. Besides that, authentication generally includes message integrity and sender verification.Moreover, for safety applications in V2V communication, the authentication requirement can deal with a masquerade attack. While, for commercial applications in V2I communication, authentication ensures that each user is authorized to access the needed service. Thereby, authentication is a fundamental access control mechanism in VANET.
- ***Integrity:*** A wireless channel is vulnerable to active attacks, e.g., data modification. Integrity is to assure that messages do not suffer from these attacks, and that all sent messages are not modified. Therefore, integrity protection is an essential requirement in vehicular communications.
- ***Accountability:***In accountability, a node sending a message is obligated for its actions. A law enforcing agency should be able to identify malicious drivers and accounts them for their actions. Also, accountability is regarded as a crucial requirement due to the safety-critical runtime environment of vehicular networks. Moreover, accountability by its nature imposes another potential security requirement known as non-repudiation.
- ***Non-repudiation:*** It is avoiding denying that the contents of a certain message have been sent by a certain entity. Hence, non-repudiation is a critical requirement for the reliable use ofVCS.
- ***Restricted Credential Usage:*** In order to achieve both authentication and accountability, a cryptographic token is used, which is called a credential. Restriction of parallel usage of authentication credentials at a particular time is a vital security requirement. It is quite necessary to protect the system from Sybil attacks, where in a fraudulent system an adversary may obtain an anonymous set of credentials to be used for impersonation of other vehicles in order to create network disturbances.
- ***Credential Revocation:*** Since VCSattaches an element of trust to a node's credential, there should be a methodology to invalidate a credential. In caseof misbehaved or faulty nodes, isolation of these nodes fromthe network is a must that is performed through revoking their credentials.
- ***Data Consistency:*** It generally encapsulates accuracy, usability, authenticity and integrity of data in vehicular networks. It also warrants that all drivers in the system perceive a consistent view of the data. Besides that, it ensures that the data sent by a certain vehicle and its nearby vehicles are consistent.

2.2 PRIVACY REQUIREMENTS

The need for privacy is addressed differently by various countries. Some countries enforce drivers' identification mechanism for crime prevention. While, some other countries may impose a mandatory privacy policy in the system. Moreover, the requirement for privacy is one of the vital reasons for public acceptance of VANETdeployment. Communication in the network should be anonymous where a message should not reveal any information about its sender.Also,the message sent should be protected in the presence of an unauthorised observer. Furthermore, the activities of a sender should be unlinkable to its source. In some schemes, a higher level of privacy is proposed where the identity of vehicles broadcasting announcements are protected even from the authorities[17]. However, full anonymity may allow for misbehaviour occurrence as attackers would act maliciously without the fear of being caught. Whereas, some other schemes allow authorities to reveal the identity of vehicles in case of misbehaviour detection so as to achieve conditional anonymity, that is, the identity of users remain anonymous unless they misbehave.

In this context, there are several privacy requirements that should be considered when designing a privacy-preserving architecture for VANET [18], which are describedin this section as follows:

- ***Anonymity:*** A message's sender should be indistinguishable or anonymous among a group of senders. In order to preserve privacy of senders, VANET needs to provide anonymity to senders/drivers. Thus in theory, it should not be possible to link a message content to the person who sent the message. However, this imposes a conflict between accountability and anonymity. Therefore, the provision of conditional anonymity is needed in order to achieve both security and privacy requirements.
- ***Conditional Privacy:***Undoubtedly, a driver benefits from the traffic-related messages that are automatically sent by other neighboring vehicles. However, these messages include a sender's private information, such as the vehicle's identity (plate license number), location, and direction. Clearly, people are not interested to expose these private information to third parties. Hence, a secure mechanism should prevent an unauthorized party from knowing the combination of the real identity and other private information. On the other hand, a trust authority (e.g., police officers) has the authority to reveal a vehicle's identity in case of criminal action occurrence. Thereby, conditional privacy preservation is essential in VANET.
- ***Confidentiality:*** This security service prevents the disclosure of message contents to unauthorized entities in order to maintain the user's privacy.
- ***Unlinkability:***An adversary cannot sufficiently distinguish whether the Items of Interest (IOI) (messages, actions, and / or subjects) used in vehicular networks are related or not. It is worth to note that unlinkability of sender to a certain message can be termed as anonymity, as this may breach the sender's anonymity.
- ***Minimum Disclosure:*** A user should reveal the minimum amount of information during communication. The user's data that is disclosed during a transaction should be minimum, in short no extra information than what is required for the job. The information collected should be adapted to the concerned specific requirement.
- ***Distributed Resolution:*** Distributing among authorities the process of identity resolution is an important privacy requirement, where authorities need to cooperate in order to link a credential to a specific entity. This property is crucial for maintaining conditional anonymity while still preserving the user's privacy.

- ***Perfect Forward Secrecy:*** Resolving a user's identity or credentials should not disclose anyinformation that allows the linkability of future messages to that user.

2.3 OTHER SYSTEM REQUIREMENTS

There are other system requirements that should be thought of when developing a robust architecture for VANET [13], [17], which are given in this section as follows:

- ***Scalability:***It may not be considered when designing a secure protocol for a traditional MANET because the number of users in MANET is not large and so failing to consider scalability would not lead to vital attacks. However, in VANET, scalability is an extremely vital factor. The incoming messages should be authenticated by a vehicle in a timely manner even in a high density area. Otherwise, some messages will be dropped before being verified if the security scheme is not efficient in high density areas. Moreover, a scheme that is not scalable is vulnerable to denial-of-service (DoS) attacks.
- ***Storage Requirements:*** Cryptographic authentication techniques have been widely exploited to secure VCS. Cryptographic credentials should be securely stored and constantly updated due to various reasons. One of these reasons is to achieve privacy. Two techniques commonly used to satisfy the property of privacy, which are pseudonyms and group signatures. In pseudonymous authentication, vehicles store a large number of public/private key pairs, and their corresponding certificates. The changing of pseudonyms is required to make tracking of vehicles by an adversarydifficult. Therefore, the size of an anonymous key should be kept as minimum as possible in order to minimize the storage space needed by a vehicle. While in group signature schemes, pre-storing a large amount of certificates is needed. However, the issue associated with group signatures is that the size of a signature is quite big.
- ***Availability:*** Some applications require high availability of a communication network, such as emergency services that are time sensitive. For example, in case of an emergency, the failure of instant reception of sent messages renders the application useless.
- ***Real-time Requirements:*** VANET applications, such as: safety-related applications, require updated or real-time information to be frequently broadcasted to vehicles via RSU or neighbouring vehicles.
- ***Robustness:***System robustness implies that the communication channel is secure and privacy-preserving, e.g. authentic and integrity-protected even in presence of malicious or faulty nodes.

3. SECURITY AND PRIVACY REQUIREMENTS VERSUS SECURITY APPROACHES

In this section, we briefly discuss different VANET approaches presented in the literature [19], which are proposed in order to fulfil various security and privacy requirements in VANET [20], [21], [22], [23]. Table 1 provides a summary of these approaches that are discussed below in details.

3.1 AUTHENTICATION AND PRIVACY

In recent days, two methods are used for providing anonymous services, which are Group Signature and Pseudonymous Authentication schemes. Both of them address the problem of authentication and privacy [24]. In group signature schemes, a vehicle is issued a group private key with which it signs a message; while in pseudonymous authentication schemes, each vehicle stores a set of identities. In addition, there are hybrid approaches that combine both group signature and pseudonymous authentication schemes, where a vehicle can maintain a pseudonyms set and a secret group signing key, and also can issue itself a certificate using the group key.

3.1.1 GROUP SIGNATURE SCHEME

There are some approaches in VANET that use group signature scheme in order to maintain the signer's anonymity. This scheme allows every group entity to generate a signature without revealing its exact identity, while other group members could verify the message authenticity. This signature scheme has two components: a group manager and group members. A group manager is responsible for the key distribution, adding a group member, detecting and revoking a misbehaved group member. Each group member signs a message by a group user key issued by the manager, while other members would not be able to identify the exact identity of sender. At first, the manager of group issues different group user keys for every group member, then issues group public key to all group members. A group member uses the group user key for signing messages, while uses the group public key for verifying the message authenticity. Only the group manager knows each member's real identity, thus it could detect and revoke the group members. Despite that this scheme

Table 1. Summary of VANET Security and PrivacyApproaches.

Security and Privacy Requirements	Security and Privacy Methods	Security and Privacy Approaches
Authentication, Privacy	Credential Usage, Digital Signature, Encryption, Anonymizer Proxy	**Group Signature Approaches:** TACK [25], BGLS [26], Signcryption [27], Trusted Platform Module (TPM) [28], [29], Batch Verification [30], Re-encryption [31]
		Pseudonymous Authentication Approaches: PASS [32], DCS [33], Mix-zone [34], Fixed Mix-zone [10], RLC [8]
Authentication, Data Integrity	Credential Usage, Digital Signature, Encryption, Message Authentication Code (MAC)	**Multiple Approaches:** Decision Packet [37], Security Mechanisms [38], Multi Operating Channels Model [39], Public Key Infrastructure (PKI) [40]
		Identity-based Approaches: Identity-based Batch Verification (IBV) [36], Identity-based Aggregate Signature[41]
Anonymity, Unlinkability	Pseudonym Usage, Silent Period, Mix-zone	**Pseudonym Approaches:** Pseudonymous Technique [42], Variable Pseudonyms [35], Silent Period [34]
		Mix-zone Approaches: Independent Mix-zone [9], Multiple Mix-zones [43]
		Other Approaches: VANET-based Clouds [44]
Traceability, Accountability,	Credential Usage, Digital Signature,	**Traceability:** Challenge-response Protocol [11]

Non-Repudiation	Misbehaviour Authority, Event Data Recorder (EDR)	**Accountability,Non-Repudiation:** Trusted Party [42], Identity-based Signature [45], Mobile Agent Protocol [46]
Misbehaviour Detection, Revocation	Intrusion Detection System (IDS), Certificate Revocation List (CRL), Reputation-based Methods	**Revocation Approaches:** CRL [32], Local and Global Revocation [48], Reputation-based Scheme [49], Certificate Revocation Scheme [50], Credential-based Protocol [51]
		Misbehaviour Detection Approaches: IDS [52], APDA [55], RRDA [56], Stable Community Detection [57], EAPDA [60], Verification Technique [61]

provides some security services, yet it incurs a large revocation cost. Also, vehicles can join andleave groups very rapidly; therefore this scheme is not practical to be used in real-life scenarios.

For example, a scheme based on group signature was presented by Studer *et al.* in [25], where a VANET key management approach using Temporary Anonymous Certificate Keys, TACKs, wasexamined. In [25], authors gave some valid assumptions and discussed the efficiency of their scheme. However, some issues in VANET still remain in their TACKs; such as: the detection andrevocation of temporary keysis restricted by the expiration scheme. Also, the correlation attack could happen in the following situation: when only one OBU is changing its keys at a certain time, the new key could be associated with the old key of this OBU by an adversary, so the adversary can compute the exact identity of the OBU. Also, Qin *et al.* in[26] proposed the use of Boneh, Gentry, Lynn and Shacham (BGLS) aggregate signature, which allows a receiver to verify a group of signatures in one operation. The authors also proposed a method to compress data and signatures to minimize the storage overhead of an OBU.

Besides that, Zhang *et al.* In[[27] used two mechanisms on top of a PKI system to achieve authentication, privacy, integrity, linkability, efficiency, and scalability. These mechanisms are known as Signcryption and group signature. The system depends heavily on distributed RSUs to run an on-the-fly group. Signcryption is a technique used to sign and encrypt a message at the same time. Also, it is used to enable a vehicle to ask for a secrete member key in order to join a group run by a RSU. Then, a RSU would check the validity of vehicle data and issues a key if the vehicle is legitimate. A RSUwould use a group signature where every vehicle in the group is capable of communicating with other group members and RSU without revealing its identity. This is made possible using anonymous group certificate. The authors also proposed that a vehicle can check if the sender is revoked through the RSU instead of maintaining a CRL. Besides that, batch verification is used to reduce the computation time needed. In addition, Wagan *et al.* in[28], [29] proposed an efficient group formation technique, where asymmetric cryptography is adopted for normal message communication and symmetric cryptography for event-driven messages. Vehicles form a trusted group using Trusted Platform Module (TPM) to improve security and privacy. While, in order to maintain conditional privacy for V2V communication in VANET, Kim and Lee in[30] presented a batch verification method to prohibit unnecessary group subscriptionsvia group signature method. This approach provides a variety of security requirements utilizing the group signature method. Whereas,Kanchan and Chaudhari in [31] provided a group signature method integrated with a re-encryption technique, where a third party can re-encrypt a message that can be decrypted by other authorized users. This approachallows the message broadcasted in a group to be read by any member of the group or other authorized groups using the re-encryption mechanism.

3.1.2 Pseudonymous Authentication Scheme

The idea behind Pseudonymous Authentication scheme is that each vehicle stores many pseudonymous certificates at first, and then randomly chooses one of these certificates to act as its identity at a certain time. Also, since a Trusted Authority (TA) has sufficient storage and could not be compromised; so, it is safe and feasible for a TA to store these pseudonymous certificates. When a vehicle first registers, the TA sends enough pseudonymous certificates to it, and a unique permanent identity.For privacy considerations, vehicles do not use the permanent identity to sign messages; they rather randomly choose one of the pseudonymous certificates that the TA has issued for digital signature. By this way, the temporary identity of each vehicle changes over time, and a malicious attacker can hardly trace a specific vehicle. This is because after altering the certificate,an attacker would not be able to link the new certificate with the old certificate, which means that the attacker has lost the target. However, this method still has some problems, such as high revocation cost. For example, when a vehicle is revoked, the number of pseudonymous certificates that needs to be added to the Certificate Revocation List (CRL) could be too large[32], where the size of CRL increases rapidly when the size of network increases.

In the context, many works on location privacy address the issue of pseudonyms' provisioning and update, i.e. how signatures using pseudonyms are assigned, and when pseudonyms are changed, as shown in Figure 1. For example, Sun *et al.* in [32] proposed a Pseudonymous Authentication and Strong privacy-preserving Scheme (PASS), where a vehicle can update its set certificates via the neighbouring RSU. Compared with the previous pseudonymous schemes, PASS has a lower revocation overhead and lower certificate update overhead too. Also, in [33], a Distributed Certificate Service approach, DCS, was presented by Wasef *et al.* in order to ensure that an OBU can update its certificate via a RSU; regardless whether this OBU currently exists in the same RSU domain where it has been registered or not. The DCS approach could rapidly certify many certificates and signatures. In addition, some schemes imply that the pseudonyms need to be changed every certain time in a mix-zone to preserve the user's location privacy, since a mix-zone creates a *k-anonymous* region where a silent period should be preserved between each pseudonym update [34]. For example, Amro in [10] presented a method for pseudonym update that exhibits the same level of privacy for all trafficscenarios. This method depends on fixing the mix-zone that thwarts an adversary from linking a particular pseudonym with the real identity of

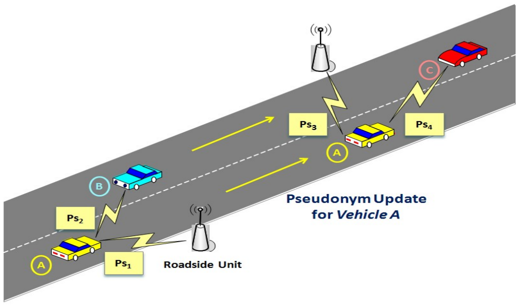

Figure1.Vehicle *A* updates its pseudonym (*Ps*) for each new message sent

a specific vehicle. Whereas, Wang and Yao in [8] proposed a pseudonym-enabled approach for maintaining privacy in VANET. In this approach, a RSU is used to assign a Reputation Label Certificate (RLC) for vehicles in its range in order to overcome the conflict between privacy-preservation and reputation determination of a certain vehicle.

3.2 Authentication and Data Integrity

One of cryptographic mechanisms used to achieve message authenticity and data integrity is the usage of symmetric primitives. This includes Message Authentication Code (MAC) appended with a message that is computed using shared symmetric secret key. In order to validate a MAC, a third entity needs to see the secret key, but would not know which of the two parties computed the MAC. While symmetric-based techniques are computationally efficient, they do not provide the property of non-repudiation.So, a digital signature is used to solve this problem, since signing a message using valid credentials issued from a Trusted Party (TP) would satisfy both authentication and data integrity. Digital signature schemes used in the literature include: Group Signatures (GS)[[11], traditional Public Key Cryptography (PKC)[35], identity-based signature & batch verification[[36].

For example, Kaur*et al.* in[37] presented an approach that utilizes a Decision Packet. In this approach, a node creates a route from departure node todestination node and performs the necessary verificationusing the Decision Packet's hash value,which thwart an attacker from changingthe hop count. Besides that, Ram*et al.* in [38]highlighted different security mechanisms in order to provide securityfor the routing protocol and to protect the user's information from modification. While, Multi Operating Channels Model was proposed by Nitish*et al.* in [39]to provide network protection against attacks that threatenthe network functioning and data confidentiality in VANET, such as: DoS andmodificationattacks. In addition, Nazmul in [40] adopted a Public Key Infrastructure (PKI) in order to fulfil the major security requirementsin VANET, such as: authentication, integrity, and non-repudiation. Also, an update certificate method is used in [40] when a vehicle enters a new region. In this approach, the computation time needed for message authentication is decreased in order to minimize the message loss rate due to message check delay. Moreover, Mahapatra and Naveena in [36] used an Identity-based Batch Verification (IBV) scheme, where they proposed to randomly update the anonymous identity and location after a certain time. While, Zhang *et al.* in[41]presented an approach that utilizes multiple TAs and a one-time identity-based aggregate signature. In this approach, vehicles are able to verify multiple messages simultaneously, where signatures are compressed into a single signature in order to minimize the storage space needed by a vehicle.

3.3 Anonymity and Unlinkability

A common approach to achieve anonymity is by using pseudonyms. For example, Kamat *et al.*in [[42]used a pseudonym as a public key in place of an identity in the ID-based announcement scheme. Each key could beeither used once for each message or used to sign multiple messages over its short lifetime, where the key update frequency is varieddepending on some factors, such as vehicle's speed. The pseudonyms are updated in order to prevent linking of differentvehicle's activities. However, drawbacks of the pseudonymous technique include: secure key distribution and management, and storage complexity. Also, randomly chosen and changing pseudonyms are used by Kounga *et al.* in [35] in order to prevent linking to the user's real identity. While, a silent period was proposed by Buttyan *et al.*in [34] in order to achieve unlinkability. The level of unlinkability depends on the number of vehicles present during the time the change of pseudonyms takes place. Also, the high velocity of vehicles present at the time of pseudonym update decreases the ability of an adversary to probabilistically determine and link pseudonyms and vice versa. During silent period, transmission of messages is temporarily disabled for a period of time, and a vehicle does not receive any incoming messages. The drawback of this technique is that it restricts a vehicle from generating or receiving a messagefor a certain period of time, which defeats the purpose of VANET deployment.

Besides that, Guo *et al.*in [9] presented an independent mix-zone mechanism to solve the problem of the pseudonym update in low density areas.This mechanism involves provisioning of certificates and pseudonyms, where a vehicle establishes a mix-zone through itsperiodically broadcasted messages. While other vehicles may produce random versions of a pseudonym respectively, which generatea*k*-anonymous mix-zone. In addition, Memon *et al.*in[[43]proposed a pseudonym update method with multiple mix-zones. Also, a cheating detection technique was presented in [[43]that enables a vehicle to check if the pseudonym update process was successful or not. Whereas, Hussain and Oh in[44] presented an approach that offers the following services:1) Maintains the user's privacy using multiple anonymity.2) Trackstheuser's route by saving beacon messages in Cloud. 3) Provides conditional privacy via anonymity withdrawal application. This approach incurs less overhead as compared to other approaches proposed in the literature.

3.4 TRACEABILITY, ACCOUNTABILITY AND NON-REPUDIATION

In a pervasive VANET environment, misbehaviour may take place as a result of hardware malfunctioning or may be intentional. For instance, the safety-related messages may contain fake information, or may have been modified, discarded or delayed intentionally. In such situations, it is desirable to achieve accountability. Also, the source of misbehaviour should be traceable for liability purposes. Traceability is desirable when a dispute arises, however, it is difficult to achievetraceability due to the need of privacy requirement. So, different methods are studied to solve this problem. For instance, in schemes that use pseudonyms, the pseudonyms could be linked with a specific identity that possesses the unique Electronic License Plate (ELP), in order to trace the misbehaved user by the authorities. Meanwhile, in schemes such as: group signatures, a tracing manager is adoptedto revoke the malicious vehicles by opening their signatures [11].

While, accountability is achieved if it satisfies traceability, non-repudiation and revocation requirements. The necessity for accountability in VANETs arises from the possibility of misbehaviour among users that may harm public road safety and jeopardize VANET future deployment. Misbehaviour in VANETs may occur due to malicious activities of users inside the system. Such activities may include: preventing message broadcasting to other vehicles; generating fake messages; injecting non-safety-related messages that may cause traffic jam in the network due to overload of the bandwidth; or escaping from an accident. While attacks performed by outsiders can be addressed by means of authentication, misbehaviour among legitimate senders is a more challenging problem to address. This is because legitimate senders possess valid credentials issued by an authority and could deceive other vehicles to trust them to perform malicious actions.

Another aspect of accountability is non-repudiation, where an entity is not able to deny the act of sending a message signed using a key that belongs exclusively to it, assuming forgery is not possible. A challenge-response protocol is another approach to achieve non-repudiation that was proposed by Chen *et al.*in [11], where: given a signature on a message, the challenge-response protocol determines whether a vehicle is the signer of the message. While in some other schemes, non-repudiation is assumed in the presence of a fully TP, such as Kamat *et al.* in[42]. In addition, Sun *et al.*in [45] presented a mutual authentication approach with DoS resilience. This approach adopts an identity-based signature scheme, and offers security services such as: unlinkability, conditional privacy, and non-repudiation. Besides that, Shehada *et al.*in [46]provided amobile agent protocol for VCS that providesa variety of security services including accountability and non-repudiation, as well as mitigates well-known attacks. Also, this protocol allows fast response for a vehicle's request, where the collected data is not lost even if the mobile agent is lost.

3.5 Misbehaviour Detection and Revocation

Detection of misbehaving vehicles is an important issue in VANET that has recently received a lot of attention. The authentication mechanism itself only guarantees the message integrity but cannot ensure that the content of message is correct. Therefore, when a vehicle misbehaves, such as: modifies a message, gives bogus information to others, attacks the network by pretending to be another one; the network should have the ability to detect these false messages and the malicious vehiclein order to revoke that vehicle through some schemes[[47].Some misbehaviour detection schemes (MDSs) are run by vehicles in order to detect any misbehaviour and then report the malicious vehicle to the Certificate Authority (CA). Meanwhile, the communication overhead is a big issue when distributing the CRL. Accordingly, some work have been done in order to decrease the size of CRL to reduce the network traffic during the distribution phase. For example, Sun *et al.* in[32] presented an authentication mechanism, where the size of CRL depends on the number of revoked vehicles and independent on the number of pseudonyms that the misbehaved vehicle owns. Despite that, the CRL distribution process to all remaining vehicles in the whole network takes large time. During this interval, the attacks could still jeopardize other drivers' safety.

In this context, the existing revocation schemes are mainly of two types, which are local revocation and global revocation that are described as follows[48]:

- In*Local Revocation*, a local voting mechanism is used to identify and revoke a malicious vehicle. Two requirements should hold that are: the majority is honest, and other vehicles are able to detect any misbehaviour. The viewpoint of Liu*et al.* in[48] is that these two requirements are demanding. Many legitimate nodes may be unable to vote as a result of the lack of detection ability, e.g. not within detection range. Also, there exists Sybil attacks that can affect the voting result.
- While, in*Global Revocation*,the CA identifies the accused vehicle, and determines whether to revoke it by the use of trust management. If one vehicle is judged as a misbehaving node, all its certificates are invalidated in the entire network. However, the main challenge in the global revocation scheme is that the CA is not always available and the latency may be unacceptablein real-life scenarios.

Moreover, in some revocation schemes, the CRL is no longer used. For example, in reputation-based schemes such as Malip *et al.* in[49], revocation is achieved by ceasing to provide misbehaved vehicles with their reputation credentials. A vehicle whose reputation score decreases to zero would not be able to continue its future participation in the network. On the other hand, Qu *et al.* in[50]providedan approach to maintain the security and privacy in VANET. This approachincurs a low computation time and enhances the certificate revocation process.Besides that, Singh and Fhom in [51] proposed an anonymous credential-based protocol that enables the revocation of a misbehaved vehicle. Also, this protocol provides the detection of fraudulent actions, where the revocation of subsequent credentials of a malicious entity is performed.

Furthermore, Erritali *et al.* in[52] presented anIntrusion Detection System (IDS) in VANET through classifying the detection system into signature-based, anomaly-based[53], and specifications-based systems[54]. Besides that, RoselinMary*et al.* in[55] adopted anAttacked Packet Detection Algorithm (APDA) to protect against some security attacks, such as: DoS attack. This algorithmreduces thetime delay to enhance VANET security. In addition, Gandhi and Keerthana in[56] presented a Request Response Detection Algorithm (RRDA) to determine DoS attack. This algorithm utilizes a hash table to minimizea DoS attack caused by a malicious vehicle, and sends messages to all vehicles from departure till destination as well as updates the hop count. Also, this algorithm minimizes the message delay as compared to other algorithms proposed in this context. While, Grzybek*et al.* in[57] proposed a stable community detection algorithm after considering the vehicle's dynamic motion, where authors evolved the Label Propagation Algorithm(LPA) community detection algorithm[58]with the Stability and Network Dynamics over a Sharper Heuristic for Assignment of Robust Communities (SandSHARC) [59]. Besides that, in [57], the authors evaluated their work by testing the stability of the detected community. Not only that, but alsoSingh and Sharma in[60] presented an Enhanced Attacked Packet Detection Algorithm (EAPDA) to mitigate various attacks, such as: DoS attack, which results in performance deterioration of VANET. This algorithm incurs less time delay as compared to other proposed algorithms. Whereas, Memon *et al.*in [61]presented a verification technique to verify the vehicle's activities in a private manner. In this technique, a RSU decides if a message is trusted or not, and then notifies the neighboring vehicles with the decision.

4. TYPES OF VANET ADVERSARIES, ATTACKS AND ATTACKERS

Vehicular networks are vulnerable to eavesdropping by adversaries in their wireless range as well as location samples can be collected for tracking purposes. Also, envisioned inter-vehicular communication protocols and applications provide information about different identifiers ranging from the vehicle IP address and destination IP address tothe protocol used. The interesting part is the association of these identifiers with location and time samples,i.e. identifier, location, and time. The identifier of a vehicle with its location and time-stamp are often referred to as the location sample. Many profiles of such location samples collected pose a serious threat to the privacy of the user. It is interesting to note that considering only location tracking of a caruser doesn't violate the user's privacy until the user is mapped to the vehicle, where breaching of privacy takes place.

When considering VANET security, a large number of threat models may be assumed. Athreat model includes an adversary that is a person or a group of people,which threatens the security and privacy of a given system. Moreover, in VANET, there are several possible attacks and attackers[15], [62], [47].In this section, we explain the different types of adversaries and attackers, and also classify the attackspresent in VCSbased on the communication system layers. Table 2shows the security and privacy requirements that are previously discussed in Section 2 against the various attacks present in VANET.

4.1 TYPES OF ADVERSARIES

VANET safety and non-safety applications may perform as expected or deviate from their expected operationsmainly due to adversarial activities. The adversarial incentives may be money, spying on the user, or some other personal benefits. Some of the previous works proposed in this context provide a survey of the adversaries relevant to the vehicular context [13], [5]. The different types of adversaries that are present in VANET are provided in this section as follows:

- ***External and Internal Adversaries:***Some adversaries could be internal entities while others could be external entities in/to the system.External adversaries are entities that are not equipped with credentials and keys to access the data-handling systems/servers or applications, where the processing of the user's location data, personal data and preferencesis performed. While entities having access to the previously mentioned systems and legitimate participants in the system can be termed as internal adversaries.
- ***Passive and Active Adversaries:*** A passive adversarycan only learn and listen, for instance an eavesdropper that intercepts messages between a user machine and an infrastructure.A passive adversary gathers information from the collected messages and vehicle movementsto draw inferences about a target user. Despite that a passive adversary learns about a specific user,it does not influence the user's behaviour.In contrast to apassive adversaryis an active adversarythat can affect the user's behaviour. For anadversary to be active, it vigorously participates in the network with intentions to cause disruption. This type of adversary may modify, replay or drop legitimate messages in order to present fake information to other vehicles. Other attacks that could be generated by this adversary type include generating and broadcasting bogus information to other vehicles.
- ***Local, Extended and GlobalAdversaries:***A local adversary has limited territorial effectand controlssome entities in network,such as: vehicles or RSUs. On the other side, for an adversary to be extended, it controls several nodes in the network. While, the strongest adversary has a global coverage of the network that is known as a global adversary. The distinction between these types of adversaries is important to preserve the user's privacy.
- ***Independent and Colluding Adversaries:*** Adversaries may perform independently, or may collude in order to exchange information and perform more effective attacks. For example, a group of vehicles may collude to perform a certain attack to achieve their mutual agenda or interest. Also, a group of colluder vehicles may clear the way for attackers by reporting falseinformation of traffic jam, which would convince other innocent vehicles by that wrong information since the report had come from more than one vehicle.

Table 2. Security and Privacy Requirements versus VANET Attacks.

	Security Requirements[15], [16]					**Attack Scope - CommunicationSystem Layers**
	Authentication	**Integrity**	**Accountability, Non-Repudiation, Credential Revocation**	**Restricted Credential Usage**	**Data Consistency**	
VANET Attacks [13]	Impersonation, Sybil Attack	🟩	Impersonation, Sybil Attack, Malicious Vehicle	Impersonation, Sybil Attack	🟩	Application and Transport Layers
	Bogus Information or Forgery, Jungle Communication, Tunnel Attack	Jungle Communication	Bogus Information or Forgery, Jungle Communication, Wormhole Attack	🟩	Bogus Information or Forgery, Wormhole Attack	Network Layer
	On-board Tampering orIllusion, Message Replay, Message Modification / Alteration, Denial-of-	On-board/Vehicle Information Tampering orIllusion, Message Modification	On-board/Vehicle Information Tampering orIllusion, Message Replay, Message Modification /	🟩	On-board Tampering orIllusion, Message Replay, Message Modification / Alteration	Physical Layer

	Service (DoS)	/ Alteration	Alteration	🟩		
	Privacy Requirements[17], [18]					**Attack Scope - Communication System Layers**
	Conditional Privacy	**Anonymity, Confidentiality, Unlinkability**	**Minimum Disclosure**	**Distributed Resolution**	**Perfect Forward Secrecy**	
VANET Attacks [13]	Movement Tracking	Movement Tracking	Movement Tracking	Movement Tracking – Internal Adversary [5]	Movement Tracking	Application and Transport Layers
	Location Disclosure, Trajectory Disclosure	Location Disclosure, Trajectory Disclosure	Location Disclosure, Trajectory Disclosure	🟩	🟩	Network Layer
	Eavesdropping, On-board Tampering orIllusion, Message Modification / Alteration	Eavesdropping	🟩	🟩	🟩	Physical Layer
	Other System Requirements[13], [14]					**Attack Scope - Communication System Layers**
	Scalability	**Storage Requirements**	**Availability**	**Real-time Requirements**	**Robustness**	
VANET Attacks [13]	🟩	Movement Tracking	Sybil Attack, Information Block	Sybil Attack, Information Block	All attacks in Application and Transport Layers	Application and Transport Layers
	Tunnel Attack, Wormhole Attack	🟩	Packet Dropping, Bogus Information or Forgery, Tunnel Attack, Wormhole Attack	Packet Dropping	All attacks in Network Layer	Network Layer
	DoS	🟩	On-boardTampering orIllusion, Message Replay, Message Modification / Alteration, Jamming, DoS, RSU Relocation	Message Replay, Jamming, DoS	All attacks in Physical Layer	Physical Layer

Moreover, there are other types of adversaries that are a mixture of the previous types, for example:

- ***Global Passive Adversary:*** A person or a group of people with enough privileges to eavesdrop on the whole network.
- ***Local Passive Adversary:***An entitythathas a restricted coverage range, e.g. through gaining accessto a RSU, and eavesdrops on the wireless communication.
- ***Local Active Adversary:***An entity thathas a restricted coverage range and performs malicious actions, such as compromising a neighbouring vehicle (target vehicle) or a RSU.

4.2 TYPES OF ATTACKS

In VANET, attacks may arise from faulty or hostile remote computing nodes. Also, the privacy attacksare of greater concern for a user than the security attacks[13]. In this part, the possible attacks that may occur in VANET are classified based on communication system layers as follows:

4.2.1 SECURITY ATTACKS ON APPLICATION AND TRANSPORT LAYERS

- ***Movement Tracking:***An attacker associates the identity of a vehicle to its messages then tracks the route of that vehicle.
- ***Impersonation Attack:***For malicious purposes, an attacker masquerades as another vehicle by using a false identity to attack and fool other vehicles. Furthermore, an attacker may pretend to be a RSU to send fake advertisements to vehicles in its coverage range.
- ***Sybil Attack:*** An attacker uses a faulty entityto create multiple fake identities and then acts as a few vehiclesto takeover part of the system. This allows an attacker to produce an illusion to other vehicles, for example, that there is a traffic congestiontoforceother vehicles to take an alternate routeto free the route for itself.
- ***Information Block:***Inthis attack, an attackermakes use of theVANET protocol. If a vehicle sends a message to its neighboring vehicles, the information is stopped while being transmitted causing confusion to other vehicles.
- ***Malicious Vehicle:*** When using pseudonyms, a malicious vehicle may change its identity and hence it may be hard to be tracked by authorities.

4.2.2 SECURITY ATTACKS ON NETWORK LAYER

- ***Location Disclosure:***A locationsample includes three components, which are: ID, location, and time. Any of these components could be modified and manipulated by attackers.Also, attackers may abstract the real identity of a target vehicle from its traffic-related messages, and further knows the vehicle's location sample.
- ***Trajectory Disclosure:***An attacker may globally observe the broadcasts of a target vehicle and uses this information to reveal the vehicle's identity.
- ***Packet Dropping:***In a multi‑hop communication, an attacker may automatically or selectively drop some or all packets received.
- ***Bogus Information or Forgery or Fabrication Attack:*** In this attack, an adversary broadcasts fake messages into the network. For instance, a malicious vehicle may send a fake congestion message or claim that it is an emergency car to make use of the lane alone. Moreover, this type of attack could lead to accidents. Therefore, verifying messages' freshness and validity in V2V communication is vital to make sure that the received messages are not forged.
- ***Jungle Communication:*** This attack is an evolution of the Bogus Information attack, wheredatais sent to other vehiclesthat continue to modify it in order to changeoriginal information.
- ***Tunnel Attack:***In this type of attack, false information is sent to a vehicle moving ina place with no GPS coverage, e.g. a tunnel, where the vehicle may update false information.
- ***Wormhole Attack:***In this attack,meaningless information is sent from authorized entitiesthat results in network disturbance.

4.2.3 SECURITY ATTACKS ON PHYSICAL LAYER

- ***Eavesdropping:***In VCS, overhearing of messages could allow an attacker to easily collect vehicle-specific information and infer the personal data of driver thus violates ones privacy.
- ***On-board / Vehicle Information Tampering or Illusion Attack:***It involvescheating with internal vehicle's information, such as: speed, position,via tampering hardware. The vehicle's information is provided incorrectly using sensors or internal devices, in order to trigger malfunction of a vehicle or to deceive other vehicles in the network. Also, sometimes an attacker may pretend to be another person by cloning the other's location.
- ***In-transit Traffic Tampering Attack:***A malicious entity mayintentionallycause delay, corruption, replay or modification of messages to damage the normal functioning of VANET communications. This attack includes:
  - ***Message Replay:*** An attacker records messages received from legitimate vehicles and then resends them back, for example, in order to disturb the traffic or cause some confusion. This attack can be done in two methods, which are: using one's OBU or using a special piece of hardware. The duplicated messages might make a vehicle fail to know its neighbour's correct driving status, e.g., direction, position, speed, etc.
  - ***Message Modification / Alteration:***An attacker modifies information of a vehicle included in a message(e.g. position) for ones benefit, which could be a potential threat to the safety of other vehicles in network.

- ***Jamming Attack:***An attacker deliberately generates too many messages to overcrowd the wireless channel in order to trigger malfunction of network.

- ***Denial-of-Service (DoS) Attack:***An attacker attempts to disrupt the normal service of VANET byprohibiting services to be provided normally. This behaviour would cause serious consequences if the service is safety-related application. For example, an attacker may continuously broadcast a lotof dummy messages to flood the network aiming to bring down the transmissionchannel so that vehicles cannot exchange safety messages. For a sophisticated attacker, it may send a large number of messages with invalid signatures. In this case, a legitimate vehicle would spend a lot time verifying invalid signatures that causes a delayin verifying a legitimate message.
- ***RSU Relocation:*** An attacker may relocate a RSU in order to mislead vehicles.

4.2.4 GROUP-RELATED SECURITY ATTACKS

Some attacks may be carried out ifthe system utilizes a group approach [63], such as:

- Disclosure of group secrets.
- Tracing based on group secrets, where a vehicle could be traced based on its group key.
- Collusion between new Group Leader (GL) and old GL, where random rotation of GLs would not prevent the attacks based on disclosure of group secrets.

4.3 TYPES OF ATTACKERS

An attacker is an entity that compromises the security and breaches the privacy of another entity. Different attackers have different impacts on VANET. Although some attackers look for amusement and fun, some others look for severe damage or privacy breach. The broad categories of attackers explained in this section are as follows[21]:

- ***Malicious Attacker:*** A dangerous person whose main goal is to cause a great damage in system. This kind of attacker brings jeopardy to legitimate drivers. For instance, a malicious attacker may deliberately tamper messages and give wrong information to mislead other network entities. Also,malicious attackers could slow down or stop vehicles on a highway to cause accidents.A malicious attackermay breakdown the network by compromising a RSU.

- ***Selfish or Greedy Driver:*** A driver who abuses the system to maximize ones benefit. Most drivers misbehave for selfish reasons, where they do not want to share lanes with other vehicles. For example,a vehicle may tell other vehicles behind it that “there is congestion ahead” by injecting false messages so that the road is cleared for it.
- ***Snooper or Eavesdropper:***This person tries to collect information about a target vehicle via its broadcasts in order to identify that vehicle and hence could easily track it.
- ***Prankster:*** A hacker who performs some malicious actions or a person looking for fame. For example,a malicious entity that sends fake messages in order toslow down the network.
- ***Industrial Attacker:***A person who belongs to the automotive manufacturer and could tamper the GPS system, vehicle’s sensors, or other sensitive devices. So, a tamper-proof device (TPD) is recommended to be used to thwart such type of attacker.

5. Conclusion

In conclusion, the specific nature of VCS brings up the need to address various security and privacy issues for VANET to be widelyadopted by the society. Accordingly, the research community and industry have focused on securing vehicular communications. Also, the open fields of secure inter-vehicular communicationswith 5G-enabled vehicles [64]and driverless vehicle security [65] promise interesting research areas in VANET.

In this paper, we presented the essential security and privacy requirements in VANET as well as demonstrated the state-of-the-art approaches that are developed to fulfil these requirements. Besides that, a detailed description of differentcategories of possible adversaries in VANEThas been providedin this paper. In addition, a brief explanation of the common attacks and attackers in VCS has been given here.Finally, from our work, it can be clearly deduced that developing a secure privacy-preserving architecture is a major requirementfor the promotion of VANET worldwide. In this context, we believe that this paper would give the reader a good piece of information about VANET security and privacy. Hence, this paper is considered as a valuable reference when developing a secure privacy-preserving protocol for VANET that provides the previously mentioned security and privacy services while protects against the presented attacks.

Acknowledgements

We would like to thank the anonymous reviewers for their dedication and valuable comments that helped in motivating this work.

References

[1] Rasheed, A., Gillani, S., Ajmal, S., and Qayyum, A., “Vehicular Ad Hoc Network (VANET): A Survey, Challenges, and Applications,” in *Vehicular Ad-Hoc Networks for Smart Cities*,pp. 39-51, Springer, Singapore, 2017.

[2] Mansour, M., Fahmy, A., and Hashem, M., “Maintaining location privacy and anonymity for vehicle’s drivers in VANET,” in *International Journal of Emerging Technology and Advanced Engineering*, vol. 2, issue 11, pp. 8-40, Nov. 2012.

[3] Mansour, M. B., Salama, C., Mohamed, H. K., and Hammad, S. A., "CARCLOUD: A Secure Architecture for Vehicular Cloud Computing," in *14th Embedded Security in Cars Europe Conference*, *ESCAR,* Germany, Nov. 2016.

[4] Asuquo, P., Cruickshank, H., Morley, J., Anyigor Ogah, C.P., Lei, A., Hathal, W., and Bao, S., "Security and Privacy in Location-Based Services for Vehicular and Mobile Communications: An Overview, Challenges and Countermeasures," in *IEEE Internet of Things*, 2018.

[5] Emara, K., "Safety-aware Location Privacy in VANET: Evaluation and Comparison," in*IEEE Transactions on Vehicular Technology*, vol. 66, issue 12, pp.10718-10731, 2017.

[6] Laganà, M., et al., "Secure Communication in Vehicular Networks – PRESERVE Demo," in *Proceedings of the 5th IEEE International Symposium on Wireless Vehicular Communications*, 2013.

[7] Feiri, M., Petit, J., and Kargl, F., "The Impact of Security on Cooperative Awareness in VANET," in *IEEEVehicular Networking Conference, VNC,* 2014.

[8] Wang, S., and Yao, N., "A RSU-aided distributed trust framework for pseudonym-enabled privacy preservation in VANETs," in *Wireless Networks*, pp.1-17, 2018.

[9] Guo, N., Ma, L., and Gao, T., "Independent Mix Zone for Location Privacy in Vehicular Networks," in *IEEE Access*, 2018.

[10] Amro, B., "Protecting Privacy in VANETs Using Mix Zones With Virtual Pseudonym Change,"*arXiv preprint arXiv:1801.10294*, 2018.

[11] Chen, L., Ng, S., and Wang, G., "Threshold Anonymous Announcement in VANETs," in *IEEE Journal on Selected Areas in Communications*, vol. 29, pp. 605-615, 2011.

[12] Chirayil, G.S., and Thomas, A., "A Study on Cost Effectiveness and Security of VANET Technologies for Future Enhancement," in*Procedia Technology*, vol. 25, pp. 356-363, 2016.

[13] Chaubey, N.K., "Security Analysis of Vehicular Ad hoc Networks (VANETs): AComprehensive Study," in*International Journal of Security and Its Applications*, vol. 10, issue 5, pp.261-274, 2016.

[14] Zhu, L., Zhang, Z., and Xu, C., "Security and Privacy Preservation in VANET,"in *Secure and Privacy-Preserving Data Communication in Internet of Things*, pp. 53-76, Springer, Singapore, 2017.

[15] Siddiqui, N., Husain, M.S., and Akbar, M., "Analysis of Security Challenges in Vehicular Adhoc Network,"in *Proceedings of International Conference on Advancement in Computer Engineering &Information Technology, IJCSIT,* pp. s87-s90, 2016.

[16] Samara, G., and Al-Raba'nah, Y., "Security Issues in Vehicular Ad Hoc Networks (VANET): a survey,"*arXiv preprint arXiv:1712.04263*, 2017.

[17] Pathan,A.S.K.,"*Security of self-organizing networks: MANET, WSN, WMN, VANET*,"CRC press2016.

[18] Vijayakumar, P., Chang, V., Deborah, L.J., Balusamy, B., and Shynu, P.G., "Computationally efficient privacy preserving anonymous mutual and batch authentication schemes for vehicular ad hoc networks," in *Future Generation Computer Systems*, vol. 78, pp.943-955, 2018.

[19] Park, J. O.,and Choi, D. H.,"A design of framework for secure communication in vehicular Cloud environment," in*Journal of the Korea Institute of Information and Communication Engineering*, vol. 19, issue 9, pp. 2114–2120, 2015.

[20] Vijayalakshmi, V., Saranya, S., Sathya, M., and Selvaroopini, C.,"Survey on various mechanisms for Secure and Efficient VANET communication,"in*IEEE International Conference on Information Communication and Embedded Systems, ICICES,* pp. 1-5, 2014.

[21] Singh, A., and Kad, S., "A review on the various security techniques for VANETs," in*Procedia Computer Science*, vol. 78, pp.284-290, 2016.

[22] Hasrouny, H., Samhat, A. E., Bassil, C., and Laouiti, A., "VANet Security Challenges and Solutions: A Survey," in *Vehicular Communications*, Jan. 2017.

[23] Kim, M., "A Survey of Vehicular Ad-Hoc Network Security," in *International Conference on Mobile and Wireless Technology*, pp. 315-326, Springer, Singapore, June 2017.

[24] Manvi, S.S., and Tangade, S., "A survey on authentication schemes in VANETs for secured communication," in *Vehicular Communications*, vol. 9, pp.19-30, 2017.

[25] Studer, A., Shi, E., Bai, F., and Perrig, A., "Efficient mechanisms to provide convoy tacking together efficient authentication revocation, and privacy in vanets," *6th Annual IEEE*

Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, SECON, pp. 1-9, 2009.

[26] Ding, Q., Li, X., Jiang, M., and Zhou, X., "Reputation management in vehicular Ad Hoc Networks," in *International Conference on Multimedia Technology, ICMT*, Ningbo, China, pp. 1‑5, Oct. 2010.

[27] Lei, Z., Qianhong, W., Solanas, A., and Domingo‑Ferrer, J., "A scalable robust authentication protocol for secure vehicular communications," in *IEEE Transactions on Vehicular Technology*, vol. 59, pp. 1606-1617, March 2010.

[28] Wagan, A.A., Mughal, B.M., and Hasbullah, H., "VANET security framework for trusted grouping using TPM Hardware," in *2ndInternational Conference on Communication Software and Networks, ICCSN,* Singapore, pp. 309‑312, Feb. 2010.

[29] Wagan, A.A., Mughal, B.M., and Hasbullah, H., "VANET security framework for trusted grouping using TPM hardware: Group formation and message dissemination," in *International Symposium in Information Technology, ITSim,* Kuala Lampur, Malaysia, pp. 607‑11, June 2010.

[30] Kim,S. H., Lee, I. Y.,"A study on message authentication scheme based on efficient group signature in VANET," in*Journal of the Korea Institute of Information Security and Cryptology*, vol. 22, issue 2, pp. 239–248, 2012.

[31] Kanchan, S., and Chaudhari, N.S., "Integrating group signature scheme with Non-transitive Proxy Re-encryption in VANET,"in *IEEE International Conference on Computing, Analytics and Security Trends, CAST,* pp. 227-231, December 2016.

[32] Sun, Y., et al., "An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications," in *IEEE Transactions on Vehicular Technology*, vol. 59, no. 7, pp. 3589-3603, 2010.

[33] Wasef, A., Jiang, Y., and Shen, X., "DCS: An efficient distributed certificate service scheme for vehicular networks," in *IEEE Transactions on Vehicular Technology*, vol.59, no. 2, pp. 533-549, 2010.

[34] Buttyan, L., Holczer, T., Weimerskirch, A., and Whyte, W., "SLOW: A Practical Pseudonym Changing Scheme for Location Privacy in VANETs," in *IEEE Vehicular Networking Conference, VNC*, 2009.

[35] Kounga, G., Walter, T., and Lachmund, S., "Proving Reliability of Anonymous Information in VANETs," in *IEEE Transactions on Vehicular Technology*, vol. 58, no. 6, pp. 2977-2989, 2009.

[36] Mahapatra, P., and Naveena, A., "Enhancing Identity Based Batch Verification Scheme for Security and Privacy in VANET," in *IEEE 7th InternationalAdvance Computing Conference, IACC,* pp. 391-396, January 2017.

[37] Kaur, H., Batish, S., and Kakaria, A., "An approach to detect the wormhole attack in vehicular adhoc networks," in *International Journal of Smart Sensors and Ad Hoc Networks, IJSSAN,* pp.86-89, 2012.

[38] Raw, R. S., Kumar, M., and Singh, N., "Security challenges, issues and their solutions for VANET," in *International Journal of Network Security & Its Applications*, vol. 5, issue 5, pp. 95–105, 2013.

[39] Shukla, N., Dinker, A. G., Srivastava, N., and Singh, A., "Security in vehicular ad hoc network by using multiple operating channels," in *IEEE 3rd International Conference on Computing for Sustainable Global Development, INDIACom,* pp. 3064-3068, March 2016.

[40] Islam, N., "Certificate revocation in vehicular Ad Hoc networks: a novel approach," in *IEEE International Conference on Networking Systems and Security, NSysS,* pp. 1-5, January 2016.

[41] Zhang, L., Wu, Q., Domingo-Ferrer, J., Qin, B., and Hu, C., "Distributed aggregate privacy-preserving authentication in VANETs," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 3, pp. 516-526, 2017.

[42] Kamat, P., Baliga, A., and Trappe, W., "Secure, Pseudonymous, and Auditable Communication in Vehicular Ad Hoc Networks," *Security and Communication Networks*, vol.1, no. 3, pp. 233-244, 2008.

[43] Memon, I., Chen, L., Arain, Q.A., Memon, H., and Chen, G., "Pseudonym changing strategy with multiple mix zones for trajectory privacy protection in road networks," in *International Journal of Communication Systems*, vol. 31, issue 1, 2018.

[44] Hussain, R., and Oh, H.,“A secure and privacy-aware route tracing and revocation mechanism in VANET-based clouds,” in*Journal of the Korea Institute of Information Security and Cryptology*,vol. 24, issue 5, pp. 795–807, 2014.

[45] Sun, C., Liu, J., Xu, X., and Ma, J., “A Privacy-Preserving Mutual Authentication Resisting DoS Attacks in VANETs,” in *IEEE Access*, vol. 5, pp.24012-24022, 2017.

[46] Shehada, D., Yeun, C.Y., Zemerly, M.J., Al-Qutayri, M., and Al Hammadi, Y., “Secure Mobile Agent Protocol for Vehicular Communication Systems in Smart Cities,” in *Information Innovation Technology in Smart Cities*, pp. 251-271, Springer, Singapore, 2018.

[47] Sakiz, F., and Sen, S., “A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV,” in *Ad Hoc Networks*, vol. 61, pp.33-50, 2017.

[48] Liu, B., Chiang, J. T., and Hu, Y.-C., “Limits on revocation in vanets,” in *8th International Conference on Applied Cryptography and Network Security*, pp. 38-52, 2010.

[49] Malip, A., Ng, S., and Li, Q., “A Certificateless Anonymous Authenticated Announcement Scheme in Vehicular Ad Hoc Networks,”*Security and Communication Networks*, vol.7, no. 3, pp.588-601, 2014.

[50] Qu, F., Wu, Z., Wang, F., and Cho, W.,“A security and privacy review of VANETs,” in*IEEE Transactions on Intelligent Transportation Systems*,vol. 16, issue 6, pp. 1–12, 2015.

[51] Singh, A., and Fhom, H.C.S., “Restricted usage of anonymous credentials in vehicular ad hoc networks for misbehavior detection,” in *International Journal of Information Security*, vol. 16, issue2, pp.195-211, 2017.

[52] Erritali, M., and El Ouahidi, B., “A review and classification of various VANET Intrusion Detection Systems,” in *IEEE National Security Days, JNS3,* pp. 1-6, April 2013.

[53] Raja, P. K., Suganthi, M., and Sunder, M. R.,“Wireless node behaviour based Intrusion detection using genetic algorithm,” in*Ubiquitous Computing and Communication*, vol. 7, pp. 143–148, 2006.

[54] Ping, Y., Xinghao, J., Yue, W., and Ning, L., “Distributed intrusion detection for mobile ad hoc networks,” in *Journal of systems engineering and electronics*, vol. 19, issue 4, pp. 851-859, 2008.

[55] RoselinMary, S., Maheshwari, M., and Thamaraiselvan, M., “Early detection of DOS attacks in VANET using Attacked Packet Detection Algorithm (APDA), in *IEEEInternational Conference on Information Communication and Embedded Systems, ICICES,* pp. 237-240, February 2013.

[56] Gandhi, U.D., and Keerthana, R.V.S.M., “Request response detection algorithm for detecting DoS attack in VANET,” in *IEEE International Conference on Optimization, Reliabilty, and Information Technology, ICROIT,* pp. 192-194, February 2014.

[57] Grzybek, A., Seredynski, M., Danoy, G., and Bouvry, P., “Detection of stable mobile communities in vehicular ad hoc networks,” in *IEEE 17th International Conference on Intelligent Transportation Systems, ITSC*, pp. 1172-1178, October 2014.

[58] Leung, I.X., Hui, P., Lio, P., and Crowcroft, J., “Towards real-time community detection in large networks,” in *Physical Review E*, vol. 79, issue 6, pp. 066107, 2009.

[59] Herbiet, G.J., Bouvry, P., and Guinand, F., “Social relevance of topological communities in ad hoc communication networks,” in *IEEE International Conference on Computational Aspects of Social Networks, CASoN*, pp. 19-24, October 2011.

[60] Singh, A., and Sharma, P., “A novel mechanism for detecting DOS attack in VANET using Enhanced Attacked Packet Detection Algorithm (EAPDA),”in *IEEE 2nd International Conference on Recent Advances in Engineering & Computational Sciences, RAECS,*pp. 1-5,December 2015.

[61] Memon, I., Arain, Q. A., Memon, H., and Mangi, F. A., “Efficient user based authentication protocol for location based services discovery over road networks,” in *Wireless Personal Communications*, vol. 95, no. 4, pp. 3713-3732, 2017.

[62] Sumra, I.A., Abdullah, A., Ahmad, I., and Alghamdi, A., “Towards Improving Security in VANET: Some New Possible Attacks and Their Possible Solutions,” in*Internet Technology*,vol. 17, issue 4, pp.821-829, 2016.

[63] Hasrouny, H., Bassil, C., Samhat, A.E., and Laouiti, A., “Security risk analysis of a trust model for secure group leader-based communication in VANET,” in *Vehicular Ad-Hoc Networks for Smart Cities*, pp. 71-83, Springer, Singapore, 2017.

[64] Liao, D., Li, H., Sun, G., Zhang, M., and Chang, V., “Location and trajectory privacy preservation in 5G-Enabled vehicle social network services,” in *Journal of Network and Computer Applications*, pp. 1-11, 2018.

[65] De La Torre, G., Rad, P., and Choo, K.K.R., “Driverless vehicle security: Challenges and future research opportunities,” in *Future Generation Computer Systems*, 2018.

AUTHORS

Marvy B. Mansour is currently working as Assistant Lecturer at the British University in Egypt, Cairo, Egypt. She is now pursuing her Ph.D. Degree at Computer and Systems Engineering Department, Faculty of Engineering, Ain Shams University, Cairo, Egypt. She received her M.Sc. Degree at 2013 and B.Sc. Degree at 2007, from Computer Engineering Department, Faculty of Engineering, Arab Academy for Science, Technology and Maritime Transport, Cairo, Egypt.Previous Publications include: M. B. Mansour, C. Salama, H.K. Mohamed, S.A. Hammad, “CARCLOUD: A Secure Architecture for Vehicular Cloud Computing,” 14thEmbedded Security in Cars (ESCAR) Europe Conference, Germany, 2016. Fields of interest include: Cloud Security, Privacy, Security, VANET.

Cherif Salama was born in Cairo, Egypt, in 1979. He received the M.Sc. and B.Sc. degrees in electrical engineering from Ain Shams University, Cairo, Egypt in 2001 and 2006 respectively. He received his Ph.D. degree in Computer Science from Rice University, Houston, Texas in 2010.From 2001 to 2006, he was a Teaching and Research Assistant at Ain Shams University and from 2006 to 2010, he held the same position in Rice University. Since 2010, he has been an Assistant Professor in the Computer and Systems Engineering Department of the Faculty of Engineering of Ain Shams University. He is also currently the Unit Head of the Computer Engineering and Software Systems program at Ain Shams University. His research interests and publications span a relatively wide spectrum that includes hardware description languages, programming languages, parallel computing, Cloud Computing, artificial intelligence, and more.Mr. Salama was awarded a full fellowship when he joined Rice University as a graduate student. In addition to his participation in various research projects, he was a key person in the design and development of Verilog Preprocessor funded by the Intel Corporation through the Semiconductor Research Corporation.

Hoda K. Mohamed is a Professor at Computer and Systems Engineering from 2009. The manager of Information System Center in Faculty of Engineering, Ain Shams University from 2011 to 2015. She got her Ph.D., M.Sc. and B.Sc. from Ain Shams University in 2001, 1983, 1978 respectively. Research activities include: Intelligent systems, E-learning systems, Data Mining, Database systems, Image Processing, Artificial Intelligent, Software Engineering, Cloud Computing. Previous publications include: 1- Classification of IDS Alerts with Data Mining Techniques, International Journal of Electronic Commerce Studies Vol.7, No.1, pp.1-11, 2012. 2- Database Intrusion Detection using sequential data mining approaches, in the 9th IEEE International Conference on Computer Engineering and Systems (ICCES 2014), Cairo, Egypt, December 2014. 3- Energy efficient resource management for cloud computing environment, the 2014 9thICCES, Cairo, Egypt, December, 2014.

Sherif A. Hammad graduated from AinShams University, Faculty of Engineering as computer and systems engineer at 1983. MSc and PhD from the same school. Researcher at Institute Nationale Polytechnique de Grenoble France. Professor of Robotics and Automotive Systems. Was senior engineering manager in Mentor Graphics Egypt;

multinational electronic design automation cooperate from 1998-2012. Co-Founder and VP of Avelabs; an SME working in software development for automotive industry, Egypt – Germany. Civil Servant as Minister of Scientific Research during 2014-2015. Main interest is teaching and research in autonomous vehicles and automotive cyber security.