Scientific Research Publishing

Journal of Computer and Communications, 2016, 4, 12-27
http://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

Toward Secure Vehicular Ad Hoc Networks an Overview and Comparative Study

Yousef Al-Raba'nah, Mohammed Al-Refai

Department of Computer Science, Faculty of Information Technology, Zarqa University, Zarqa, Jordan
Email: yrabanah@zu.edu.jo, refai@zu.edu.jo

How to cite this paper: Al-Raba'nah, Y. and Al-Refai, M. (2016) Toward Secure Vehicular Ad Hoc Networks an Overview and Comparative Study. *Journal of Computer and Communications*, **4**, 12-27.
http://dx.doi.org/10.4236/jcc.2016.416002

Received: November 3, 2016
Accepted: December 5, 2016
Published: December 9, 2016

Abstract

Significant increasing in the number of vehicle accidents around the world and the resulting losses in both aspects human and material necessitate us to find efficient, innovative solutions to this passive phenomenon. Vehicular Ad hoc NETwork (VANET) is an emerging technology that attracts many research interests in the field of wireless communications due to its benefits in providing more road safety and enhancing traffic management. Security is one of the most critical issues that face VANETs. VANETs are vulnerable to different types of attacks as long as they are still a fertile area for attackers to compromise the network with their malicious attacks. However, to build robustness networks, a vital issue that needs to be taken into consideration is to make the networks resistant to security attacks. This paper presents an introduction to VANETs and its structure and provides an overview of fundamental security challenges and requirements in VANETs. It also discusses and investigates major security attacks and its effects on the security requirements. Afterwards, it studies, compares and finally classifies a variety of possible countermeasures that have been proposed to cope with these attacks.

Keywords

VANETs, Security, Authentication, Privacy, Attacks

1. Introduction

Tremendous developments in wireless communications and networks provide a wide variety of possibilities to use these technologies in different areas and applications. Hence, as more manufacturers of vehicles are equipping their vehicles with wireless communication devices, it is clear that the number of smart vehicles will be increasing dramatically in the near future [1]. Therefore, the future vehicles will certainly be able to communicate among themselves, which engender a new type of networks called Ve-

hicular Ad hoc NETwork (VANET). The emergence of VANET will play a major role in the enhancement of traffic management and make roads more safe and efficient than before [2].

Road safety is considered the primary challenge facing traffic management, where roads accidents have a massive impact (directly or indirectly) on our life. The statistical figures show that more than 1.2 million persons are killed every year, in addition to more than 50 million are injured in the world; these numbers are likely to increase by about 60% in the future if no efficient procedures and actions are taken [3]. All of that in addition to time waste caused by traffic congestion and financial losses which exceed hundreds of millions [4].

Vehicular Ad hoc Network seems to be an ideal solution to avoid road problems and improve traffic environment. Vehicular Ad Hoc Network is a wireless network which connects vehicles to each other via equipping them with certain wireless and processing capabilities; it is a particular form of Mobile Ad Hoc Networks (MANETs) where nodes could be vehicles or Road Side Units (RSUs) [2]. Unlike other types of MANETs, Nodes movements in VANET are restricted by road topology and must obey road signs and traffic lights. VANETs enable exchanging and analyzing road and traffic information by sending and receiving it wirelessly among nodes. The main goals of VANET are to provide more road safety, improve traffic environment and enhance users' road experience [5] [6].

The advent of such smart vehicles opens up opportunities for many promising applications of VANETs; the applications can be classified into two primary groups: safety and non-safety applications [7] [8]. The safety applications attempt to improve road safety and avoid accidents as possible, examples of these applications are collision avoidance, traffic management, traffic signal violation warning, emergency vehicles warning, curve speed warning, post accident warning, work zone warning, and road condition warning applications. The prime purpose of safety application is to minimize road accidents as well as save humans' lives. As for non-safety applications, whose purpose is to enhance the road experience and make it more comfort and enjoyable for passengers, they will be used as infotainment applications, for examples, music and video sharing, games, internet services, emails, weather, payment services, nearest restaurants, hotels, petrol stations, parking applications, etc. [4] [7] [8]. In both groups, the applications require the exchange of messages among nodes, the correctness of the messages contents and authenticity of theirs' transmitters have a conceptual influence on the network proceedings [9].

The nature of VANET makes it a favourite target for several attacks, the successful of an attack can lead to serious results in human lives and financial losses. Therefore, the security is always a focal issue in VANET that must be regarded to deploy a reliable network [10]. In this paper, our main effort concentrated on presenting a fundamental document which can provide the interested readers and researchers with the background information related to VANET security. The paper addresses several topics such as network structure, challenges, security requirements and attacks.

The rest of this paper organized as follows: Section 2 describes the structure of VANET. In Section 3, we identify the main VANET challenges. Section 4 outlines the security requirements. Section 5 presents and investigates the major attacks against VANET. In section 6, we list and discuss the possible countermeasures for the VANET attacks that already mentioned, and we summarize, compare, and classify the countermeasures. Section 7 concludes the paper.

2. VANETs Structure

Vehicular networks are expected to utilize various wireless access technologies in its communications, such as Dedicated Short-Range Communications (DSRC, 5.9 GHz), which was developed in response to highly dynamic environments in order to grant transferring data at high rates, such signals can reach up to 1000 M [2] [11]. Some of other wireless technologies are Worldwide Interoperability for Mobile Access (WiMAX), cellular systems, Wireless Local Area Network (WLAN) and Wireless Fidelity (WiFi) [7]. The nodes are equipped with particular devices to enable the communications between each other in a wireless manner, any node in ad hoc networks can commonly act as either a host which inquiries data or a router which forwards data [12]. Correspondingly, there are two types of nodes in VANETs:

Vehicles: Which represents the mobile nodes, this type of nodes equipped with several devices such as: On Board Unit (OBU), an OBU composed of wireless transmitter and receiver units that mounted on a vehicle and responsible for the communications with other nodes in the network [13]. Other installed devices are Event Data Recorder (EDR) and Tamper Proof Device (TPD). The EDR stores critical data about vehicles such as speed, position, time, transmissions and receives messages, trip details, etc. The EDR acts as a black box in an aeroplane, the stored data is useful especially in post-accident analysis, since it provides data about the vehicle before, during and after the accident, which give an accurate and reliable picture of accidents reasons. Whereas the TPD holds secret information such as cryptographic material, driver identity, in addition to carrying out cryptographic operations by processing, signing and verifying the exchanged messages. The vehicles also supplied with different sensors to collect data to process/share it depending on its importance [4].

RSU: Which represents the fixed infrastructure nodes (base stations), it plays as a router or gateway among vehicles themselves and between vehicles and external networks like the internet. As the range of ad hoc network is relatively limited to short distance, the RSUs can extend the range by re-distributing the information to forward it to other OBUs. The RSUs are deployed along the roadsides and can be connected to backbone networks to furnish different network applications and services [7] [13].

Vehicular Ad Hoc Networks have mainly two types of communications: Vehicular to Vehicular communications (V2V), and Vehicular to Infrastructure communications (V2I - I2V), see **Figure 1**. In the first type, vehicles communicate directly with other vehicles by exchanging messages with each other. Whereas in the latter, the communications are done between vehicles and fixed infrastructures (*i.e.* RSUs). The communications could be either in a single hop or multi-hop manner, depending on the distance

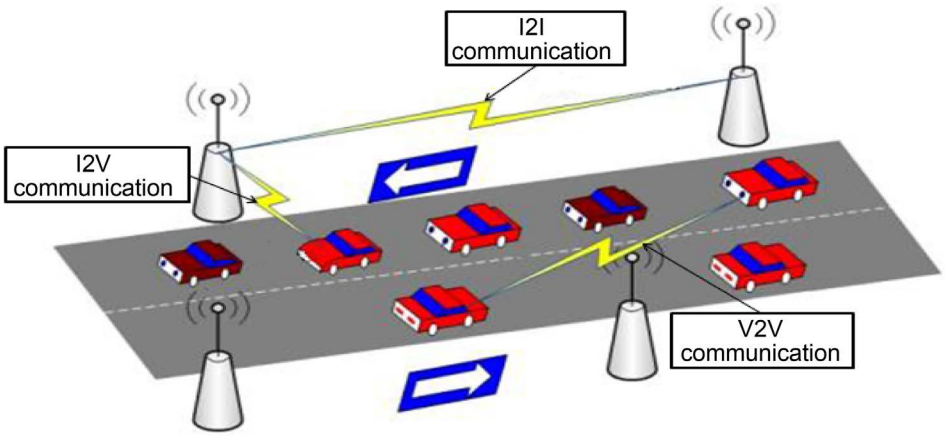

Figure 1. VANETs communications.

between the intended nodes. The RSUs also can communicate with each other to form Infrastructure to Infrastructure communications (I2I) [14] [15]. These communications can be utilized to build efficient applications that enable safe and comfort transportation for passengers.

3. VANETs Challenges

In regard to its nature, VANET is characterized by some particular features which make it quite different from other networks [16]. Therefore, VANET introduces several challenges which remain to be addressed in developing a usable and dependable network. In this section, we identify the main challenges in VANET as follows:

Volatility: In contrast with other networks, vehicles in VANET are characterized by their high speed. During navigations, vehicles can connect with other vehicles only for a short period as each vehicle moves in high mobility and may change its movement direction (consider two vehicles in contrary directions). Hence, the connectivity among vehicles can be extremely fleeting. However, securing vehicular communications by using password-based establishment will be difficult due to the lack of relatively long-lived context [4] [17]. Furthermore, any mechanism that requires multiple phases or robust collaboration such as voting may also be impractical [18].

Scalability: The size of the network is another challenge, with roughly more than one billion vehicles around the world [19], the system has to manage millions of nodes that connect to the network intermittently. Moreover, the lack of a universal authority to govern the network standards makes it finical to cope with different types of equipment and vehicles manufacturers, for example, the standards for DSRC in North America differ from that one in Europe [2]. All of that, in addition to the overwhelming majority of the currently used vehicles, haven't been supplied with the necessary equipments yet, which imposes a challenge per se. So in the development of VANETs applications, we must take into account that the communications will be limited to a few numbers of vehicles.

Liability: Vehicular communications provide a good chance to get critical data that

can assist legal investigations, particularly in the post-accident analysis, this indicates that detection of the messages sources should be possible, along with other data (driver identity, trip details, etc…) [18]. On the other hand, the anonymity of the message originator should be protected, and privacy must not be violated. The former prevents attackers who monitor vehicular communications from tracing vehicles, and of course, conceals the message originator information. However, the latter keeps drivers' personal information conserved from unauthorized access. Think of drivers' biometrics data which can be used to improve vehicle access and control; these data should be highly private and secret [4]. Hence, it is essential to find a compromise between liability versus anonymity and privacy.

Time Constraints: Some of VANETs messages such as emergency and safety messages are real-time sensitive, which means the messages should be delivered on time, any delay may cause catastrophic results. These types of messages should have high priorities over other messages and require rapid processing and low overhead to be transmitted with as little delay as possible [9]. Many of VANETs applications are rigorous with message delivery in terms of time, so to overcome this challenge, we should use efficient mechanisms such as fast cryptographic, fast message verification and authentication algorithms [20].

Mobility: As mentioned before, vehicles in VANETs move at high speeds and connect with nodes that may never be met before and possibly again, the connection lives for few seconds and afterwards broken due to the nature of the vehicles movements (directions and speeds), which in turn leads to highly dynamic network topology. Securing communications in such dynamic topologies may actually be difficult to achieve. Besides that, we need efficient algorithms that can optimize the use of the bandwidth in addition to the routes [2] [5]. Another issue raised by the mobility is the network density. The density varies from one location to another [21], for example, in a traffic jam or in metropolitan areas, where a number of vehicles are large, and the speed is limited up to 60 - 70 Kilometer per hour (Km/h), the density will be very high. On the other side, where the speed is relatively up to 180 - 220 Km/h such as in highway, the network density will be very low (maybe 1 - 2 vehicles in 1 Km).

4. Security Requirements

To deploy a secure and reliable network, a set of security requirements must be respected; failure to adhere to a requirement may lead to unreliable network and hence limits its deployment [9]. It is necessary to ensure that, the communications and messages exchanging through the network must be generated by legitimate nodes and can't be modified or suppressed by an attacker, essentially for safety message. The security also involves determining the responsibility of nodes while preserving theirs' privacy [20]. However, in the following, we address the main security requirements related to VANETs which are: authentication, availability, integrity, non-repudiation and privacy, these requirements can be thought as criteria to measure the network security.

Authentication: In order to provide trustworthy communications, messages in

VANETs must be generated by legitimate nodes. The authentication involves the process of verifying the message originator identity, to determine whether the originator has the rights to communicate among the network or not. Therefore, the authentication ensures that the message cannot be generated by virtual or malicious nodes [22]. It is noteworthy that the nodes identities are managed by a third party called certificate authority.

Availability: The network should always be available and keeps operating for its legitimate nodes even though in the presence of faults or attacks. The availability demands high connectivity and bandwidth to provide fast response time for real-time applications, where the message exchanging can't tolerate any delay. The delay even though in milliseconds makes some messages meaningless or may cause serious consequences [5] [9].

Integrity: The integrity ensures that the message received is the same as what has been generated. Integrity for a message implies that the message contents must be protected against alterations attacks during its transmission from the originator to the receiver [23]. At the originating side, the node must sign the message to be sent. Whereas at the receiving side, the node should be able to verify that the received message has been sent by another node without modification by anyone, to determine whether the message contents are correct or corrupted [12].

Non-Repudiation: Any node engaged in a message transmission must not have the ability to deny the transmission of that message. Further, the non-repudiation of message generator asserts that the message has been sent, whereas non-repudiation of receiver asserts that it was received [15]. Usually, the attackers hope to deny having sent or received messages to avoid the responsibility, non-repudiation helps in identifying the attackers and prevents them from disavowal their crimes, and hence detecting the malicious nodes [4] [5]. The non-repudiation is particularly useful in post-accidents investigations to trace paths and contents of the exchanged messages before the accidents [22].

Privacy: The private information of nodes must be maintained and kept away from unauthorized access, while authorities should have the ability to access these information. The privacy is an important issue, where the users want to guarantee that their sensitive information such as identity, speed, trip path, and position will be immunized [24] [25].

5. Attacks on VANETs

Referring to the fact that such networks have yet to be implemented, VANETs are expected to suffer from different types of attacks. The wireless access medium used in VANETs put them in the confrontation with the attackers who try to compromise the networks [9]. This section highlights and investigates the possible major attacks related to VANETs security, in addition to their imaginary scenarios, and lists the security requirements that involved in these attacks.

Denial of Service (DoS) Attacks: Denial of Service attack aims to prevent legitimate

nodes from partially or completely accessing the networks services and resources. Therefore, a part of or the whole network is no longer available for its legitimate nodes. The attack scenarios are several; an attacker can jam or flood the communication channel with dummy messages, and hence reduces the network performance and efficiency by consuming the network bandwidth [2]. The attack also occurs when an attacker takes control of a node's resources exclusively so that no one will be able to access these resources. Denial of Service attack is classified as one of the most serious attacks which can create catastrophic results since the nodes cannot be able to access the network and communicate with it [26]. Obviously, in this type of attack, the availability requirement would be affected. When the network is broken, its resources and services would not be available.

Sybil Attacks: In this type of attack, an attacker generates multiple messages to other nodes, where each message has a different identity. The attacker appears to others as multiple of nodes by creating several fake identities. The Sybil attack is very dangerous since a node can act to be in several positions at the same time and provide a chance to transmit false information, which results in a mess and severe risks in the network. For instance, when an attacker sends several messages to other nodes, the nodes feel these messages have come from different nodes, thereby there is congestion ahead, so they take an alternate route and leave the road to the attacker interests [15] [27]. The requirement involved in this attack is the authentication; an attacker can obtain several identities and communicate through the network, and this violates the authentication requirement. Availability is also the requirement relevant for this type of attack; Sybil nodes can generate multiple dummy messages and flood the communication channel and hence making it unavailable.

Information Disclosure Attacks: Attacks on privacy aim to get sensitive information regarding nodes illegally. Since there is a relation between a node and its owner, getting some information about the node could put the owner privacy at risk [28]. One of the most famous attacks in this category is the information disclosure attack. The information disclosure attack involves obtaining the target node identity to disclose sensitive information about that node. A scenario to execute this attack is by using a malicious code or a virus that infects the neighbours of the target node. Once attacked by the virus, they collect the required information such as the target identity and its position and report it back (some vehicle rental companies track their vehicles by using this approach) [20]. Information disclosure affects the privacy requirements as it would simplify obtaining sensitive information such as owner personal information and hence losing the node privacy.

Message Suppression/Alteration Attacks: The ultimate goal behind VANETs is to utilize the communications between vehicles for building applications that enable safe and efficient transportations. The correctness of the exchanged messages contents plays a major role in realizing that goal. However, as its name suggests, this type of attack affects a message by suppressing, modifying, corrupting or reusing its content for several purposes. An attacker can drop some packets and deny it from being transmitted to

other nodes, the attacker keeps the packets for later using. For instance, an attacker might suppress a congestion warning message which helps other nodes to take an alternative path to destinations and use it again in another situation to get the benefits. Consequently, other nodes will not receive the message and have to wait in the traffic. Moreover, this attack includes different forms such as delaying message transmission, replaying previously transmitted messages, or altering some contents of a message [2] [9] [15]. The requirements involved in such attacks are integrity and availability. In the first case, the content of the messages could be altered or modified, whereas in the second case, the message itself could be duplicated multiple times or even couldn't be transmitted.

Impersonation/Masquerading Attacks: In VANETs each node has a unique identity, the identity helps in distinguishing the nodes in the network, and it becomes extremely dangerous when nodes identities are fabricated or stolen. An attacker pretends to be another node by using a fabricated identity, or by stealing another legitimate node identity to spoil normal network proceedings or to get access to network resources that may not be available in normal situations. The attacker can generate messages on behalf of other nodes unobtrusively to gain its benefits. For instance, an attacker may impersonate as an ambulance to get the lane priority by calling other nodes to slow down and yield, or requesting nearby RSUs to turn traffic light to green. Furthermore, an attacker can masquerade and act as a message originator to transmit a modified version of the message and claims that the message is transmitted without any modification [12] [20] [28]. By the way, several requirements are relevant in these types of attacks, which are authentication, privacy, integrity and non-repudiation. Authentication requirement is affected since an attacker can get or hide in a valid identity and acts as a legitimate node in the network. A valid identity that an attacker obtained which corresponds to a legitimate node in the network can be used to get access to that victim's node information, therefore, violates privacy requirements. Malicious nodes can alter or corrupt the content of a received message and retransmit a modified version of the received message, thereby affects the integrity requirements. Finally, the non-repudiation requirement is significantly affected, if any identity is compromised then it would be impossible to detect the real perpetrator or malicious node.

6. Defensive Countermeasures: Discussion and Comparison

6.1. Defensive Countermeasures

In the last few years, many solutions have been proposed to mitigate the security attacks of VANETs. In the following, we discuss and review different countermeasures that have been recently proposed in the literature. For the sake of clarity, the discussion will concentrate on the countermeasures that related to the identified attacks in the previous section.

DoS Attacks Countermeasures: Authors in [29] proposed an approach to mitigate DoS attack which relied on the use of OBUs. The proposed technique provides four options to deter DoS attack based on the received malicious message. Once the OBU as-

sesses the message, it can decide to use one of the available switching options, and the chosen option will be passed to the next OBU in the network. The proposed switching options are channel switching, technology switching, frequency hopping spread spectrum, and multiple radio transceivers. Thereby, the proposed approach will improve the security by alleviating the DoS attacks through these options, since the chance of the network to still being available will be increased whenever an attack happens.

Roselin Mary *et al.* [26] also proposed an Attacked Packet Detection Algorithm (APDA) to detect DoS attacks. The proposed algorithm is integrated with every RSUs, any node can send a message to an RSU, the RSU detects the position of that node and tracks it if the message contains attacked packets, the APDA maintains a database for all validated nodes. Attacked packets are specified by the frequency which represents the number of sent packets per second, and the velocity which represents the rate of change in position (speed and direction). The APDA detects DoS attacks before the verification time, and it will reduce the overhead delay that occurs while processing void requests and packets, hence improves the security of VANETs.

Researchers in [30] proposed a new algorithm called Request Response Detection Algorithm (RRDA) which is based on APDA. The RRDA handles new requests that intend to join the network; it compares the new requests with a previously validated database that was maintained by APDA. The algorithm checks if the node has already existed in the database, if the node does not exist, it will discard the request. If the node exists, the algorithm verifies the request to determine whether allows the node to enter the network or not. The main advantage of the RRDA is that it will increase the response time in VANETs.

Another approach was proposed in [31] to detect DoS by checking the internet protocol (IP) addresses of the nodes depending on the bloom filter detection scheme. The bloom filter employs a combination of reactive and proactive approaches. The reactive approach is used to define all of the connected nodes IP addresses, and the proactive approach is used to keep the new nodes IP addresses. The authors utilized the bloom filter scheme to develop their bloom filter based IP-chock detection approach. The approach consists of three phases: the first phase gathers information required to be processed in next phases, such as IP addresses and traffic information. The second phase processes the information collected in the first phase if no malicious IP addresses are found the information will be stored in a database. In the third phase, Bloom filter with the hash function is used. If malicious IP addresses are detected in the second phase, an alarm message would be sent to all other connected nodes. According to the simulation results, this approach is efficient and effective regarding detection time, storage capacity and computational cost.

Sybil Attacks Countermeasures: Authors in [27] proposed an approach to detect Sybil attacks in VANETs that depends on the using of the received signal strength to verify the position of a node. In this approach, each node is suggested to periodically carry out the role of claimer, witness, or verifier under certain circumstances. The claimer node announces its position by broadcasting a message; the message contains

information such as node identity, node position, and node neighbours identities. The verifier employs the claimer's neighbours (or witness nodes) to collect the signal strength measurements which are used to estimate the claimer's position. Afterwards, the verifier node computes the difference between the estimated position and the announced position and compares the result with a threshold. If the threshold is exceeded, the claimer is treated as a suspicious node. The simulation results show that this approach is efficient in terms of detection time and economic cost, and has good performance in suppressing Sybil attacks. However, it violates the privacy requirements, since private information such as the node identity and position were disclosed.

Another detection approach called footprint was proposed by Chang *et al.* in [32]. When a node faces an RSU, it obtains an authorized message proves its presence within that RSU range at that particular time. Through its trip, the node gets series of authorized messages, by chaining these messages together, a trajectory of this node can be constituted. Referring to the fact that the trajectories constituted by an attacker are quite similar, it can be possible to detect and eliminate Sybil attack. The main assumption of this approach is that the chance for trajectories of two nodes to be the same is significantly rare. The footprint approach has the advantage of preserving the privacy of nodes in VANETs, but however, the authors suggest that all RSUs are trustworthy. If any RSU is compromised, it can be exploited by attackers to get fake legal trajectories.

Based on the theory that different nodes cannot have the same set of neighbouring nodes for a time longer than a certain time interval (threshold), Grover *et al.* in [33] proposed an approach to detect Sybil attacks using the resemblance of the neighbouring nodes information. All nodes broadcast beacon messages to announce their presences; each node in the sender communication range receives the message and creates a record of neighbouring nodes at specified time interval. Afterwards, the nodes exchange their records with other nodes in its communication range, if some nodes observe that they have the same neighbouring nodes for an interval greater than the threshold, they identify those nodes as Sybil nodes. The idea behind the approach is that all fake identities generated by an attacker their neighbours will share the same set of neighbouring nodes. The simulation results prove that this approach is efficient and effective in terms of computational cost and detection rate, and it is able to detect Sybil attack quickly as it does not require infrastructure support such as RSUs which cause communication overhead. However, the approach needs more investigations in high-density areas like a traffic jam.

Information Disclosure Attacks Countermeasures: Several researchers put forward many schemes to achieve information privacy in VANETs. Ying *et al.* in [34] proposed an approach called Protecting Location Privacy with Clustering Anonymization (PLPCA). The PLPCA approach used to protect nodes' locations against location-based services. The approach hides road and traffic information by transforming vehicular networks into an edge cluster graph. Afterwards, it employs a cloaking algorithm to further conceal the nodes locations. The cloaking algorithm used two privacy metrics: K-Anonymity, and l-diversity. Simulation results prove that the PLPCA has

good performance in hiding road and traffic information.

Authors in [35] proposed an efficient privacy-preserving scheme called Lightweight and Efficient Strong Privacy Preserving (LESPP). The proposed scheme secures vehicular communications in VANET and assures privacy preservation and conditional traceability by utilizing self-generated pseudo identity. The proposed scheme signs messages through using a lightweight symmetric encryption and message authentication code generation, and it uses a fast message authentication code re-generation for the verification process. The results show that the LESPP scheme is feasible and has good performance as it reduces the computation cost and decreases the communications overhead. The privacy in this scheme is preserved due to the fact that only the authority parties have the ability to expose the real node identity from its pseudo identity. Therefore, the attackers cannot trace or get information about any node.

Suppression/Alteration Attacks Countermeasures: Security approaches must ensure that messages are not compromised when they transmitted through the network. In order to achieve integrity requirement, several approaches were proposed. Authors in [4] proposed the use of digital signature to force integrity of messages and authenticate nodes. The proposed approach integrated the digital signature with the conventional Vehicular Public Key Infrastructure (VPKI) to encrypt/decrypt messages, where each node would be provided with a pair of public/private key. When a node sends a message, it signs the message with its own private key and attaches a digital certificate to the message, in addition to a timestamp which ensures the message freshness and certifies that an event happens at a given time, the timestamp helps in non-repudiation attacks. The digital certificate provided by a trusted certification authority, and it includes the public key that belongs to the private key the message sender uses to sign messages. On the other side, the message receiver node checks the certificate to extract the public key of the message sender node and verifies the sender signature by using the corresponding public key. The basic idea of the certificates is that a node is trusted by those nodes which are able to verify the node certificate. By this approach, all messages being transmitted would be verified to ensure its contents safety, and therefore the integrity is achieved. However, this approach has several limitations such as the computational overhead to check a digital signature for each received packet. However, the authors proposed the using elliptic curve cryptography to reduce the overhead.

Khan *et al.* in [36] proposed an approach called Detection of Malicious Node (DMN) to detect malicious node. The DMN suggests that a node is considered as a malicious node if it shows abnormal behaviour such as dropping or duplicating the packets it received. For any transmitted message, there is a source node which is the message generator, another node which is the message destination, and a set of intermediates nodes which are the relay nodes. When a node acts as a relay node, other trustier nodes are acting as verifiers for the relay node, the verifiers monitor the behaviour of the relay node by checking the number of packets received by the relay node, and the number of packets that the relay node drops or duplicates. If the number of dropping or duplicating packets by a relay node exceeds a threshold (distrust value), it will be considered as

a malicious node and its identity is broadcasted to all other nodes. The process of computing the number of dropping or duplicating packets by a node depends on the node speed within a particular time. Further, the verifier's nodes are selected based on several parameters such as its distrust value and distance. The simulation results show that the DMN improves the network utilization and performance, and has good throughput and packet delivery ratio, in addition to a low end to end delay.

However, it is a crucial issue to authenticate nodes and messages being transmitted through the network. Ensuring authentication will provide a great chance to avoid most of the security attacks. By the way, some of the proposed approaches mentioned above in this section such as digital signature [2], DMN [36], and IP-chock [31], can also be used against impersonation/masquerading attacks.

6.2. Summary and Comparison

In this subsection, we compare and summarize the proposed countermeasures in tabular forms. The countermeasures were discussed early in this section are addressed and extended to solve more than one attack. A comparison among the countermeasures also introduced by listing its advantages and—or—its limitations. Moreover, this subsection presents a classification for the countermeasures according to the identified attacks.

In Table 1, the countermeasures are listed and for each countermeasure we define the possible attacks that it could be used to solve. The last column presents a brief review for countermeasures.

Table 2 provides a classification for the countermeasures based on the attacks that they were proposed to solve. The table also defines the relevant security requirements.

7. Conclusions

Vehicular Ad Hoc Network is a promising research area that bodes for better transportation future; it has been found to provide several prospective objectives which could help in improving traffic efficiency and safety, as well as providing comfortable transportation for passengers. Despite its importance in saving humans' lives, VANETs are still in need for more investigations and countermeasures against different challenges and security attacks that constrain theirs' deployment. In this paper, we have looked at VANET and its structure. We have also provided an overview of main VANET challenges and security requirements. Different types of attacks have been investigated and highlighted, in addition to how these attacks affect on security requirements. Moreover, we have studied and surveyed a set of countermeasures that could be used against the identified attacks. Finally, we have made a comparative study among the countermeasures and classified them according to the attacks they could be used to solve. This research paper, however, is expected to be useful for interested researchers and readers as it provides an overview for security of VANETS and gives guidelines for designing secure and robust networks. Therefore, our research paper presents one step further toward the design of secure VANETs.

Table 1. Summary and comparison of countermeasures.

Countermeasures	Attacks	Review
Switching option	Dos	Ensures availability, effective in alleviating DoS attacks. However, it is difficult to be implemented as it requires additional hardware and efficient processing units.
APDA	Dos	Detects attacks before the verification time, hence reduces the overhead delay and improves the security.
RRDA	Dos Sybil	Increases the response time, but it used as an additional approach after implementing the APDA approach.
IP-chock	Dos Sybil Impersonation/Masquerading	Efficient and effective in terms of detection time, storage capacity and computational cost.
Received signal strength	Sybil	Efficient regarding detection time and economic cost, and has good performance. However, it violates the privacy requirement.
Footprint	Sybil	Preserves the privacy requirement. However, any compromised RSU can be exploited by attackers to get fake legal trajectories.
Resemblance of the neighboring nodes	Sybil Impersonation/Masquerading	Efficient and effective in terms of computational cost, detection rate, and communication overhead. But it needs more investigations in high-density areas like traffic jam
PLPCA	Information Disclosure	Effective and has good performance in hiding road and traffic information.
LESPP	Information Disclosure	Feasible and has good performance as it reduces the computation cost and decreases the communications overhead.
Digital Signature	Information Disclosure Suppression/Alteration Impersonation/Masquerading	Effective, simple and suitable approach to be implemented in securing vehicular networks. But it has high communications overhead.
DMN	DoS Sybil Suppression/Alteration Impersonation/Masquerading	Improves the network utilization and performance, and has good throughput and packet delivery ratio, in addition to low end to end delay.

By virtue of the security aspects that were discussed, it is obvious that VANETs require effective and efficient techniques to avoid security problems. Any design of

Table 2. Countermeasures classification.

Attacks	Security Requirements	Countermeasures
DoS	Availability	Switching Options, APDA, RRDA, IP-chock, and DMN
Sybil	Authentication Availability	RRDA, IP-chock, Received Signal Strength, Footprint, Resemblance of the neighboring nodes, and DMN
Information Disclosure	Privacy	PLPCA, LESPP, and Digital Signature
Suppression/Alteration	Availability Integrity	Digital Signature, and DMN
Impersonation/Masquerading	Authentication Privacy Integrity Non-Repudiation	Digital Signature, DMN, IP-chock, and Received Signal Strength

VANETs must satisfy all security requirements. Since different techniques are based on different assumptions and architectures, no specific technique can be used as a general countermeasure against attacks.

Acknowledgements

This research is funded by the Deanship of Research in Zarqa University/Jordan.

References

[1] Firooz, M.H. and Roy, S. (2012) Collaborative Downloading in VANET Using Network Coding. *Proceedings of IEEE International Conference on Communications* (*ICC*), Ottawa, 10-15 June 2012, 4584-4588.

[2] Samara, G., Al-Salihy, W. and Sures, R. (2010) Security Analysis of Vehicular Ad Hoc Nerworks (VANET). *Proceedings of Second International Conference on Network Applications Protocols and Services* (*NETAPPS*), IEEE, Kedah, 22-23 September 2010, 55-60. https://doi.org/10.1109/netapps.2010.17

[3] World Health Organization (WHO) http://apps.who.int/gho/data/node.main.A995

[4] Raya, M., Papadimitratos, P. and Hubaux, J.P. (2006) Securing Vehicular Communications. *IEEE Wireless Communications*, **13**, 8-15. https://doi.org/10.1109/WC-M.2006.250352

[5] Al-Raba'nah, Y. and Samara, G. (2015) Security Issues in Vehicular Ad Hoc Networks (VANET): A Survey. *International Journal of Sciences & Applied Research (IJSAR)*, **2**, 50-55.

[6] Singh, S., Kumari, P. and Agrawal, S. (2015) Comparative Analysis of Various Routing Protocols in VANET. *Proceedings of Fifth International Conference on Advanced Computing & Communication Technologies*, IEEE, Haryana, 21-22 February 2015, 315-319. https://doi.org/10.1109/acct.2015.113

[7] Al-Sultan, S., Al-Doori, M.M., Al-Bayatti, A.H. and Zedan, H. (2014) A Comprehensive Survey on Vehicular Ad Hoc Network. *Journal of Network and Computer Applications*, **37**, 380-392. https://doi.org/10.1016/j.jnca.2013.02.036

[8] Eze, E.C., Zhang, S.J., Liu, E.J. and Eze, J.C. (2016) Advances in Vehicular Ad-Hoc Net-

works (VANETs): Challenges and Road-Map for Future Development. *International Journal of Automation and Computing*, **13**, 1-18. https://doi.org/10.1007/s11633-015-0913-y

[9] Engoulou, R.G., Bellaïche, M., Pierre, S. and Quintero, A. (2014) VANET Security Surveys. *Computer Communications*, **44**, 1-13. https://doi.org/10.1016/j.comcom.2014.02.020

[10] Deshpande, S.G. (2013) Classification of Security attack in Vehicular Ad hoc network: A survey. *International Journal of Emerging Trends & Technology in Computer Science* (*IJETTCS*), **2**, 371-377.

[11] Zeadally, S., Hunt, R., Chen, Y.S., Irwin, A. and Hassan, A. (2012) Vehicular Ad Hoc Networks (VANETS): Status, Results, and Challenges. *Telecommunication Systems*, **50**, 217-241. https://doi.org/10.1007/s11235-010-9400-5

[12] La Vinh, H. and Cavalli, A.R. (2014) Security Attacks and Solutions in Vehicular Ad Hoc Networks: A Survey. *International Journal on Ad Hoc Networking Systems* (*IJANS*), **4**, 1-20. https://doi.org/10.5121/ijans.2014.4201

[13] CAR 2 CAR Communication Consortium Manifesto (C2C-CC). https://www.car-2-car.org/index.php?id=31

[14] Alam, M., Ferreira, J. and Fonseca, J. (2016) Introduction to Intelligent Transportation Systems. In: Alam, M., Ferreira, J. and Fonseca, J., Eds., *Intelligent Transportation Systems*, Springer International Publishing, Switzerland, 1-17. https://doi.org/10.1007/978-3-319-28183-4_1

[15] Mejri, M.N., Ben-Othman, J. and Hamdi, M. (2014) Survey on VANET Security Challenges and Possible Cryptographic Solutions. *Vehicular Communications*, **1**, 53-66. https://doi.org/10.1016/j.vehcom.2014.05.001

[16] Gillani, S., Shahzad, F., Qayyum, A. and Mehmood, R. (2013) A Survey on Security in Vehicular Ad Hoc Networks. In: Berbineau, M., Ed., *Communication Technologies for Vehicles*, Springer, Berlin Heidelberg, 59-74. https://doi.org/10.1007/978-3-642-37974-1_5

[17] Mokhtar, B. and Azab, M. (2015) Survey on Security Issues in Vehicular Ad Hoc Net-Works. *Alexandria Engineering Journal*, **54**, 1115-1126. https://doi.org/10.1016/j.aej.2015.07.011

[18] Qin, B., Wu, Q., Domingo-Ferrer, J. and Zhang, L. (2011) Preserving Security and Privacy in Large-Scale VANETs. In: Qing, S., Susilo, W., Wang, G. and Liu, D., Eds., *Information and Communications Security*, Springer, Berlin Heidelberg, 121-135. https://doi.org/10.1007/978-3-642-25243-3_10

[19] World Health Organization (WHO). http://www.who.int/features/2004/road_safety/en/

[20] Razzaque, M.A., Salehi, A. and Cheraghi, S.M. (2013) Security and Privacy in Vehicular Ad-Hoc Networks: Survey and the Road Ahead. In: Khan, S. and Khan Pathan, A.-S., Eds., *Wireless Networks and Security*, Springer, Berlin Heidelberg, 107-132. https://doi.org/10.1007/978-3-642-36169-2_4

[21] Toor, Y., Muhlethaler, P., Laouiti, A. and De La Fortelle, A. (2008) Vehicle ad Hoc Networks: Applications and Related Technical Issues. *IEEE Communications Surveys & Tutorials*, **10**, 74-88. https://doi.org/10.1109/COMST.2008.4625806

[22] Raya, M. and Hubaux, J.P. (2007) Securing Vehicular Ad Hoc Networks. *Journal of Computer Security*, **15**, 39-68. https://doi.org/10.3233/jcs-2007-15103

[23] Mejri, M.N. and Hamdi, M. (2015) Recent Advances in Cryptographic Solutions for Vehicular Networks. *IEEE Proceedings of International Symposium on Networks, Computers and Communications* (*ISNCC*), Hammamet, 13-15 May 2015, 1-7.

[24] Kaushik, S.S. (2013) Review of Different Approaches for Privacy Scheme in VANETs. *International Journal of Advances in Engineering & Technology* (*IJAET*), **5**, 356-363.

[25] Kim, Y. and Kim, I. (2013) Security Issues in Vehicular Networks. *IEEE Proceedings of the International Conference on Information Networking* (*ICOIN*), Bangkok, 28-30 January 2013, 468-472.

[26] Roselin, M.S., Maheshwari, M. and Thamaraiselvan, M. (2013) Early Detection of DOS Attacks in VANET Using Attacked Packet Detection Algorithm (APDA). *IEEE Proceedings of International Conference on Information Communication and Embedded Systems* (*ICICES*), Chennai, 21-22 February 2013, 237-240.

[27] Yu, B., Xu, C.Z. and Xiao, B. (2013) Detecting Sybil Attacks in VANETs. *Journal of Parallel and Distributed Computing*, **73**, 746-756. https://doi.org/10.1016/j.jpdc.2013.02.001

[28] Fuentes, J.M.D., González-Tablas, A.I. and Ribagorda, A. (2010) Overview of Security Issues in Vehicular Ad-Hoc Networks. In: Cruz-Cunha, M.M. and Moreira, F., Eds., *Handbook of Research on Mobility and Computing*, Hershey, New York.

[29] Hasbullah, H., Soomro, I.A. and Manan, J.A. (2010) Denial of Service (Dos) Attack and Its Possible Solutions in VANET. *International Journal of Electrical*, *Computer*, *Energetic*, *Electronic and Communication Engineering*, **4**, 813-817.

[30] Gandhi, U.D. and Keerthana, R.M. (2014) Request Response Detection Algorithm for Detecting DOS Attack in VANET. *IEEE Proceedings of International Conference on Optimization*, *Reliabilty*, *and In-Formation Technology* (*ICROIT*), Faridabad, 6-8 February 2014, 192-194.

[31] Verma, K. and Hasbullah, H. (2014) IP-CHOCK (Filter)-Based Detection Scheme for Denial of Service (DOS) Attacks in VANET. *IEEE Proceedings of International Conference on Computer and Information Sciences* (*ICCOINS*), Kuala Lumpur, 3-5 June 2014, 1-6. https://doi.org/10.1109/iccoins.2014.6868377

[32] Chang, S., Qi, Y., Zhu, H., Zhao, J. and Shen, X. (2012) Footprint: Detecting Sybil Attacks in Urban Vehicular Networks. *IEEE Transactions on Parallel and Distributed Systems*, **23**, 1103-1114. https://doi.org/10.1109/tpds.2011.263

[33] Grover, J., Laxmi, V. and Gaur, M.S. (2014) Sybil Attack Detection in VANET Using Neighbouring Vehicles. *International Journal of Security and Networks*, **9**, 222-233. https://doi.org/10.1504/IJSN.2014.066178

[34] Ying, B. and Makrakis, D. (2014) Protecting Location Privacy with Clustering Anonymization in Vehicular Networks. *Proceedings of IEEE Conference on Computer Communications Workshops* (*INFOCOM WKSHPS*), Toronto, 27 April-2 May 2014, 305-310.

[35] Wang, M., Liu, D., Zhu, L., Xu, Y. and Wang, F. (2016) LESPP: Lightweight and Efficient Strong Privacy Preserving Authentication Scheme for Secure VANET Communication. *Computing*, **98**, 685-708.

[36] Khan, U., Agrawal, S. and Silakari, S. (2014) Detection of Malicious Nodes (DMN) in Vehicular Ad-Hoc Networks. *Proceedings the International Conference on Information and Communication Technologies* (*ICICT*), Kochi, 3-5 December 2014, 965-972.