A Survey of Attacks and Detection Mechanisms on Intelligent Transportation Systems: VANETs and IoV

Article *in* Ad Hoc Networks · March 2017

DOI: 10.1016/j.adhoc.2017.03.006

Fatih Sakiz
Hacettepe University
4 PUBLICATIONS **148** CITATIONS
SEE PROFILE

Sevil Sen
Hacettepe University
43 PUBLICATIONS **704** CITATIONS
SEE PROFILE

A Survey of Attacks and Detection Mechanisms on Intelligent Transportation Systems: VANETs and IoV

Fatih Sakiz[*] and Sevil Sen
Department of Computer Engineering, Hacettepe University, Turkey

Abstract—**Vehicular ad hoc networks (VANETs) have become one of the most promising and fastest growing subsets of mobile ad hoc networks (MANETs). They are comprised of smart vehicles and roadside units (RSU) which communicate through unreliable wireless media. By their very nature, they are very susceptible to attacks which may result in life-endangering situations. Due to the potential for serious consequences, it is vital to develop security mechanisms in order to detect such attacks against VANETs. This paper aims to survey such possible attacks and the corresponding detection mechanisms that are proposed in the literature. The attacks are classified and explained along with their effects, and the solutions are presented together with their advantages and disadvantages. An evaluation and summary table which provides a holistic view of the solutions surveyed is also presented.**

Keywords— **Attacks, intrusion detection, misbehavior detection, IoV, VANET, security**

1. INTRODUCTION

Vehicular Ad Hoc Networks (VANETs) are a special type of mobile ad hoc network used for communication among and between vehicles and roadside units. VANETs are an emerging technology for many applications, including congestion monitoring and traffic management. For example, vehicles on a road where an accident has occurred can alert each other to take an alternative route in order to avoid the traffic jam that has built up following the accident. Beside safety-related applications, there are also other applications such as infotainment, payment services, insurance calculations based on usage, and other similar means. These are applications which require vehicles to communicate with infrastructure, people and the Internet, resulting in VANETs having evolved into the universal paradigm known as the Internet of Vehicles (IoV) [1].

The special characteristics of VANETs, such as high mobility, dynamic network topology, and

[*] Corresponding author. Tel.: +90-312-297-7500
E-mail addresses: fatihsakiz@hacettepe.edu.tr, ssen@cs.hacettepe.edu.tr.

predictable node movements, require new algorithms and protocols to be developed specific to this new environment. Security also poses a challenge, since it may affect life-or-death decisions. To date, studies have focused on VANET technologies with limited attention on security.

One of the first surveys on security attacks against VANETs found in the literature is proposed by Isaac et al. in [2]. The authors summarize the general approaches against attacks and report that for VANETs, many security challenges still remain unresolved. Since the survey's publication in 2010, studies on detection and prevention mechanisms have accelerated, with many approaches having been proposed. In this research, a detailed analysis of attacks against VANETs is presented, together with the detection systems proposed to date for each attack type. Furthermore, response mechanisms that are proposed for preventing or minimizing damage to the system are covered. Some solutions originally developed for MANETs are also included in the survey, since it is believed they could also be applicable to VANETs.

1.1. Security Challenges in VANETs

Mobile ad hoc networks introduce new security issues which should be taken into account: lack of central points, mobility, wireless links, cooperativeness, and lack of a clear line of defense [3]. The specific characteristics of VANETs make these issues more challenging besides, introducing the following new issues:

Privacy: It is difficult to provide user security while at the same time respecting privacy. Taking into consideration that authorities may need information from vehicle drivers in case of an event, and that drivers may want to keep their information (identity, location history, etc.) protected helps to understand the trade-off between user privacy and security [4]. In order to prevent the tracking of all vehicles ('big brother' scenario), a system should both provide users with anonymity, while also enabling the possible determination of a user's real identity upon legitimate requests from the appropriate authorities (police, manufacturers, courts, etc.) [5].

Scalability: The number of vehicles worldwide is estimated at over 1 billion; a number that continually increases [6]. In addition, the number of vehicles connected to VANETs is expected to exceed 250 million by 2020 [7]. Currently, there is no global authority providing security for such networks, largely because it is a challenging task to define standardized rules for VANETs since the aforementioned privacy-security trade-off differs from one country to the next [8]. In order to facilitate this, worldwide coordination between local authorities would be needed in order to provide standardized security.

Mobility: The topology of VANETs changes very rapidly due to one-time interactions between vehicles. While nodes can be observed moving at a maximum speed of 20 m/s in MANET simulations [9], the speeds of vehicles are in fact much faster than this limit. As a result, link breakages between vehicles are a common occurrence in vehicular networks. In particular, links between vehicles driving in opposite directions only last for a few seconds; hence the network can frequently become disconnected. Vehicles generally communicate with each other for just a short time, and then never see each other again, which hardens reputation-based systems. However, the topology changes in a more predictable way as opposed to MANETs simulations found in the literature.

Hard-delay constraints: Many applications, particularly safety-related applications in VANETs, require real-time responses. If these requirements are not met, the consequences could be catastrophic through incidents such as accidents or delayed rescue operations. Furthermore, these real-time requirements make applications vulnerable to Denial of Service (DoS) attacks. Some researchers state that many safety-related applications should focus primarily on the prevention of attacks, rather than detection and recovery because of real-time demands [10]. However real-time attack detection is also critical in such applications, especially when insiders bypass existing prevention mechanisms.

Cooperativeness: Many of VANETs algorithms and protocols assume that data will be disseminated by vehicles in communication. This feature makes vehicular networks vulnerable to attacks such as bogus information attacks. Many security mechanisms also rely on the cooperativeness of vehicles, since local data might not be sufficient for the prevention and detection of attacks.

Mobile ad hoc networks consist of various devices which have different computational and storage capacities from hand-held devices to powerful laptops. In addition, such devices usually run on battery power. Therefore *limited resources* are an issue faced by MANETs which should be considered while designing security solutions. However, the nodes in vehicular ad hoc networks are either vehicles or stable roadside units (RSUs) which have sufficient energy and computing power. Therefore VANET nodes will not be an easy target for energy depletion attacks such as Sleep Deprivation Torture [11] in MANETs. Moreover, we could introduce more security features for VANETs which might be impracticable for resource-constrained MANETs.

Another security challenge for MANETs which has less impact on VANETs is *lack of a clear line of defense*. Even though vehicular ad hoc networks do not have central points where security mechanism can be placed as in wired networks, roadside units could play a key role in security by carrying out resource-intensive jobs such as collecting alarms raised by vehicles and making decisions. Furthermore, these units and vehicles could be more protected and secure than hand-held devices in MANETs. RSU-based security solutions such as RSU-aided certificate revocation and RSU-based intrusion detection have already been proposed in the literature. On the other hand, largescale deployment of RSUs is a costly approach.

There have been many security solutions proposed for MANETs over the past decade. While some of these approaches are also adaptable to VANETs, most are deemed unsuitable for these highly dynamic systems due to the aforementioned reasons. Therefore, new approaches or adaptations of existing approaches to VANETs are needed. In this study, the focus is placed on attacks against vehicular communication systems, and the solutions proposed in the literature in order to detect such attacks and attackers. Even though there are existing prevention mechanisms, they may be susceptible to unknown attacks. Furthermore, those mechanisms cannot protect the network from insider attackers with authorized system access. In this study, the main focus is on detection mechanisms.

1.2. Evolution from VANETs to IoV

The Internet of Things (IoT) has been an emerging paradigm. IoT consists of different types of devices and technologies in order to provide a connection among things at any time, from any place, to any network. IoT has attractive areas of use such as smart home systems, assisted living, smart energy, e-health, and intelligent transportation systems. There has been a large increase in the number of things connected to the Internet. According to Gartner [12], Internet of Things will grow to 26 billion devices/units by 2020. It is expected that a considerable number of these devices will be vehicles, which form the Internet of Vehicles (IoV) or the Internet of Cars. IoV evolved from VANETs and is expected to eventually evolve to become the Internet of Autonomous Vehicles [13].

There are many open research areas on the Internet of Things, from identification and communication technologies to standardization [14]. Since many of the devices which constitute IoT are not designed with security in mind, security attacks and solutions are also some of the main research challenges. In this paper, attacks against IoV are classified in two groups, based on the target location of the attackers:

1. Inter-vehicle attacks: Vehicles could obtain valuable information from other vehicles or from the environment to provide functionalities such as traffic congestion detection or systems for deceleration warning. For instance, vehicles could exchange useful information such as accident notifications, traffic congestion, and road conditions in order to assist in traffic management. Therefore, misbehaving nodes and falsified data sent by these nodes in such critical applications could lead to such drastic results as a loss of life or loss of energy and money. VANETs are vulnerable to new forms of attack, from dropping attacks to bogus information attacks. Furthermore, since vehicles are connected through wireless communication links, they are also susceptible to eavesdropping and traffic analysis attacks. Even though VANETs share the vulnerabilities of wired networks and ad hoc networks such as spoofing and denial of service, they have additional security challenges due to their very nature, including dynamic but predictable topology changes and delay-tolerant data dissemination.

2. Intra-vehicle attacks: Intra-vehicle communication describes communications within a vehicle. Modern road vehicles have a swarm of sensors for checking the road condition, vehicle distance, obstacle detection, fire detection, vehicle speed/acceleration sensors, message display system, and an On-Board Unit (OBU) which consists of vehicle-to-vehicle and road-to-vehicle communication systems, among others. Intra-vehicle attacks such as deceiving a sensor/system could damage the vehicle and the environment. For example, an attack which spoofs GPS information or disables the steering or braking system in an autonomous vehicle could be extremely dangerous [13]. Furthermore, with the proliferation of the Internet of Things, vehicles will be more susceptible to attacks and malwares infected from the Internet, and a subsystem of a vehicle could be compromised and become remotely controllable. However, these types of attacks are out of scope for this study.

In this study, the primary focus is inter-vehicle attacks. Studies on such attacks and solutions have accelerated in recent years. In addition, inter-vehicle communications are considered more challenging than intra-vehicle communications, since vehicular communications are provided both when vehicles are stationary and mobile [15]. It is predicted that studies on intra-vehicle attacks will accelerate with the use of IoT and Internet of Autonomous Vehicles in the near future.

The remainder of the paper is organized as follows: attacks against VANETs are classified in Section 2, and proposed solutions for each attack type are given in Section 3. Section 4 presents the general evaluation of the proposed solutions, and conclusions are drawn in Section 5.

2. ATTACK TYPES

With the proliferation of VANETs, new security risks against these highly mobile, but predictable networks are highly likely to be exploited. In this section, existing attacks against VANETs are classified according to their goals and methods. Attacks that are very specific to some routing protocols are not studied in the literature, hence are not considered in this study. While some of the attacks are derivations of existing attacks against MANETs, some of them are specific to VANETs.

2.1. Sybil Attack

Sybil attack can be classified as one of the most dangerous attacks in VANETs. In a Sybil attack scenario, a node (vehicle) can pretend as if it has more than one identity. In other words, other nodes in the network are unable to distinguish if the information originates from one vehicle or from more than one vehicle. The main aim of the attacker is to shape the networks based on his/her goals. For example, an attacker could manipulate other vehicles’ behaviors such as making them take a different road from their scheduled route. Besides being one of the most dangerous forms of attack, Sybil attack is also among the most difficult to detect [16]. It becomes more risky on networks using geographical routing, since the attacker claims that the vehicle is in several positions by sending incorrect information about its position. Furthermore, it could show events occurring in positions other than their genuine positions.

One type of Sybil attack is called a *Node Impersonation Attack*. In VANETs, each vehicle in the network has a unique identity and vehicles use their identities while communicating with other vehicles in the network [16]. However, if a vehicle changes its identity without the knowledge of the RSU or the network, it could introduce itself as a different vehicle as in a Sybil attack. For example, a vehicle involved in a traffic accident could change its identity to appear as a moving vehicle in the network. Hence, other vehicles in the network see this vehicle as a different vehicle from those involved in the accident. Then, the malicious vehicle could send incorrect information about the road conditions to the surrounding RSUs.

2.2. Denial-of-Service Attack (DoS)

Denial-of-Service (DoS) attacks aim to make valid activities of a system unavailable. The attackers mainly send far more requests than the system can handle. In VANETs, an attacker could try to shut down the network established by RSUs, and stop communication between vehicles and/or RSUs [16]. As a result of a DoS attack, attackers cannot communicate with each other, and vehicles do not receive network information such as road status, resulting in severe consequences. In a Distributed Denial-of-Service (DDoS) attack, nodes could launch an attack from different locations, thereby making any detection harder. Nodes launching a DDoS attack could aim to harm not only the vehicles in the network, but also RSUs, which are an important aspect of the infrastructure in VANETs.

There are various types of DoS attacks in VANETs. JellyFish, intelligent cheater, and flooding attacks are some known examples to be found in the literature. Aad et al. [17] present *JellyFish attack*, which is a general class of protocol-compliant DoS attack against MANETs. It follows all routing protocol specifications, unlike many other types of routing attacks. An attacker could disorder, delay, or periodically drop packets it was supposed to forward. Eventually it exploits vulnerabilities of end-to-end congestion control protocols in order to drastically decrease network performance. JellyFish attack could easily be inherited by VANETs.

Similar to the JellyFish attack, *intelligent cheater attack* [18] also remains unsuspicious by following routing protocol specifications. The attacker appears to be operating normally for most of the time, but in fact just misbehaves in a discontinuous manner. Intelligent cheater attack and JellyFish attacks could easily bypass trust mechanisms. Because of their sneaky nature it is very difficult to detect such attacks, requiring end-to-end control mechanisms with long term monitoring for their detection [17]. However, long term monitoring could be impracticable for VANETs due to their highly mobile nature.

Flooding attacks generate traffic in order to exhaust network resources such as bandwidth, CPU, power, and other similar means. Flooding attacks can be divided into two groups: data flooding and routing control packets flooding. The consequences of each attack type are the same. Resources in the network become unavailable to legitimate users. In a *data flooding attack*, an attacker could create useless data packets and send them to all nodes through their neighbors. However, the attacker needs to first set the routes with all possible nodes in the network. In a *route request flooding attack*, the attacker broadcasts route request control packets to nodes which do not exist in the network.

Another type of DoS attack is the *jamming attack*, which refers to occupying the channel used in the network by transmitting radio frequency signals consisting of illegitimate traffic. The attack could be performed by an attacker who is not necessarily a member of the network. Since this paper’s focus is on insider attacks and jamming is a general problem for wireless networks, solutions against jamming are out of scope for this research.

Considering the fact that anyone with limited knowledge could perform DoS attacks, and could therefore prevent vehicles from getting real traffic events, the impact and the likelihood of the attack is considered very high. In addition, DoS attacks must be detected as quickly as possible and response mechanisms activated on time, since it is very difficult for the network to respond once an attack has been successfully performed. Besides detection and response mechanisms, mitigation techniques such as proposed by Biswas et al. [19] could be employed.

2.3. Blackhole Attack

Whereas DoS and DDoS aim to shut down the network, another attack that shapes the network is the Blackhole attack. It is known as a serious threat for MANETs and refers to an attacker that manipulates other nodes into sending their packets through itself as much as possible. In VANETs, an attacker vehicle could exploit routing protocols such as claiming that it has the best path for the destination vehicle/RSU or that it is in the best position to forward the packets. By broadcasting false routing information, it makes other vehicles prefer to send their packets via itself, assuming that it is on the true path. After misrouted victim vehicles send their packets to the attacker, it generally just discards all packets intentionally and as a result, packet losses occur in the network (Fig. 1).

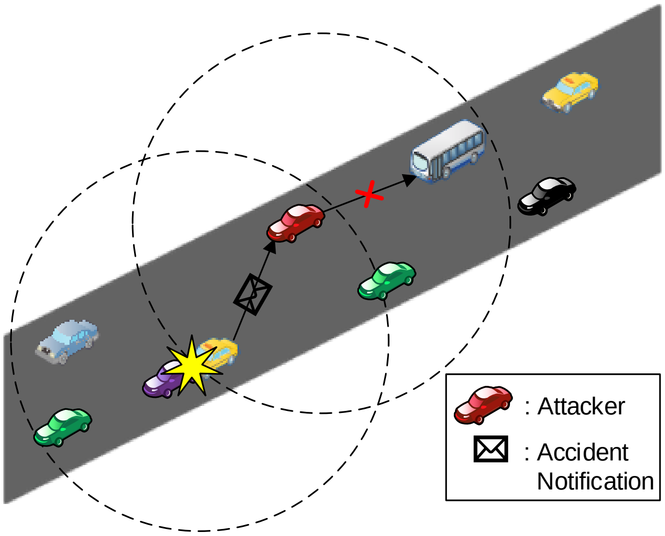

Fig. 1. Blackhole attack

Consequences of the attack for VANETs are more serious since packet losses in safety-related applications could cause life-endangering accidents. In [20], an analysis on the performance of Blackhole attacks in VANETs is given, and it is shown that the attack could affect the network in terms of end-to-end delay, throughput and network load, and that AODV is more vulnerable to the attack than OLSR. Besides simply dropping packets, attackers could also send packets between each other in such a way as to create their own network. For example, when a route request comes to a malicious vehicle, it could send the route request to another malicious vehicle. In that manner, information important to the network will not be forwarded by the attacker and may not be sent to the other vehicles as malicious vehicles only communicate between themselves, rather than the rest of the network. Therefore, vehicles other than the two malicious vehicles would not receive broadcasted safety messages.

2.4. Wormhole Attack

A wormhole attack [21], as already known from MANETs, is generally performed by two or more compromised nodes which involve themselves in as many routes as possible by advertising they know the shortest path to any destination. The goal of the attacker is to modify logical topology of the network in order to collect and/or manipulate large amounts of network traffic. In order to perform the attack in VANETs, after receiving a packet which should be forwarded, an attacker vehicle encapsulates the packet and sends it to another compromised vehicle (Fig. 2). The latter opens the encapsulated packet and spreads it. Since the original packet is encapsulated during the transmission, the hop count field cannot be increased, no matter how many hops are between them. Therefore, similar to the Blackhole attack, those two malicious vehicles make routing protocols prefer the link between them as the best route to any destination, instead of closer routes that already exist in the network. In addition, the attack could be performed even without compromising a node. The attacker could simply record the traffic at one point in the network and tunnel them through another via an out-of-band channel in order to replay or use it somewhere else. As a result, important information sent through the tunnel may not be broadcast/unicast [18], which can impose a considerable impact on communication. In another form of this attack, the vehicles could create their own private network.

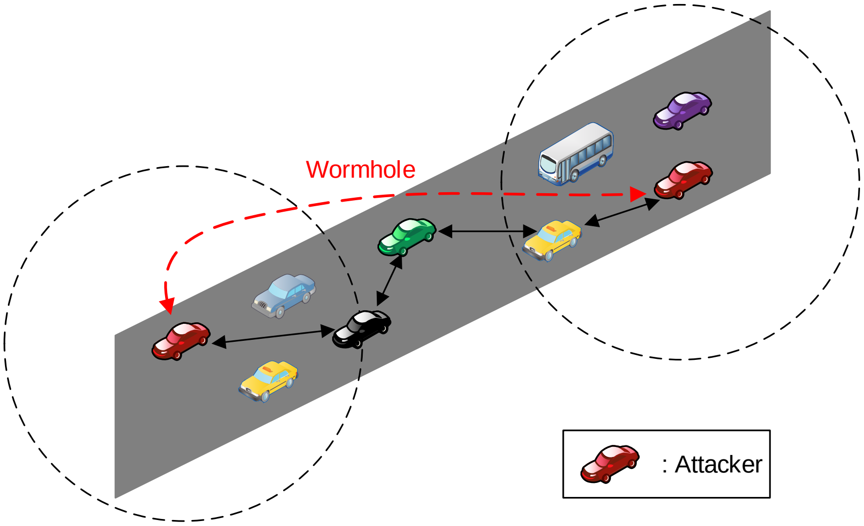

Fig. 2. Wormhole attack

2.5. Bogus Information Attack

In VANETs, vehicles use the information which is generated or forwarded by other vehicles or RSUs. However, received information may not always be true. A vehicle could generate false information on its own and then send it to the network [16]. The attacker generally aims to manipulate other vehicles with selfish and/or malicious intent. For example, a vehicle may generate information about a fake accident on the road and then send that information to other vehicles in order to make them take another road. This is more effective when there is no other vehicle to verify that information and the attack is very difficult to detect. Moreover, the consequences are more serious if there is an attacker moving around quickly – also called *motorway attacker* [22] – and broadcasts bogus information to groups it encounters. Since each group forms a separate network and does not know about the attacker's criminal records within other groups, the attacker could affect many vehicles without being detected. Even though a bogus information attack could cause very high impact by causing changes to drivers' behaviors, the attacker usually must have adequate knowledge of the network to avoid statistical detection mechanisms which limits the likelihood of the attack.

2.5.1 False Position Information

Disseminating false position information is a critical problem in VANETs, since safety-related applications are heavily dependent on reliable position information. In addition, analysis of the effects of false position information in VANETs shows that it could decrease the overall packet delivery ratio by up to approximately 90% [23]. As a result, disseminating false position information could cause performance, reliability, and security problems in VANETs.

2.5.2 Sensor Tampering

Since the OBU of a vehicle will probably be installed in a position with limited access, an attacker could try to deceive sensors by simulating false conditions in order to provide expected outputs. That technique is effective because such a deception will most likely remain unnoticed by an intra-vehicle detection system. For example, by braking within short periods, an attacker could manipulate safety-related applications in such a way as to make it appear that there is traffic on the road. Therefore, traffic jam messages will be broadcast over the network. Sensor tampering also covers illusion attack and GPS spoofing.

2.5.2.1 Illusion Attack

Illusion attack is peculiar to VANETs. The attacker mainly exploits the human psychological intuition. To do so, the attacker affects the behaviors of other drivers by disseminating false information in concert with a *scene* [24]. Firstly, the attacker needs to realize or create a suitable traffic situation in order to prepare the scene. Therefore, when other drivers receive corresponding false information messages, they are more likely to believe in them. For instance, if there are a lot of cars moving slowly at the front of the traffic they are in, drivers will probably believe that there is an accident ahead and consider alternative routes after receiving false warning messages (which indicate an accident). Secondly, the attacker needs to generate corresponding false message by deceiving its own sensor(s) in order to make them report valid but false message(s) instead of modifying their output(s) by itself [2]. The messages will remain intact and valid. As a result, false information could be distributed over the network. The attack is very difficult to detect, even within the vehicle itself.

2.5.2.2 GPS Spoofing

This attack is also known as a *tunnel attack* [25]. An attacker could inject false position information to another vehicle(s) by using GPS simulators. The victim could be waiting for a GPS signal after leaving a physical tunnel or a jammed-up area. The GPS simulator could generate signals which are stronger than original GPS signals. Therefore, even a vehicle which receives an original signal from the satellite will prefer to accept false position information sent by the attacker.

2.6. Replay Attack

In VANETs, messages could be stored for reuse later in order to deceive other entities in the network, as in MANETs. This is referred to as replay attack, and the aim is to exploit the conditions at the time when the original message is sent. After gathering information that moves around the network, the attacker could store that information and resend it to the network later on, even though it is no longer true or valid. In addition, the attack could be performed by the original sender. For example, an attacker could save a received message about an accident or traffic event which happened sometime in the past and then resend it later on (Fig. 3). Until the message becomes expired, the attacker could easily reuse it to deceive others. However, utilizing mechanisms which ensure the integrity of messages timestamps restricts its likelihood.

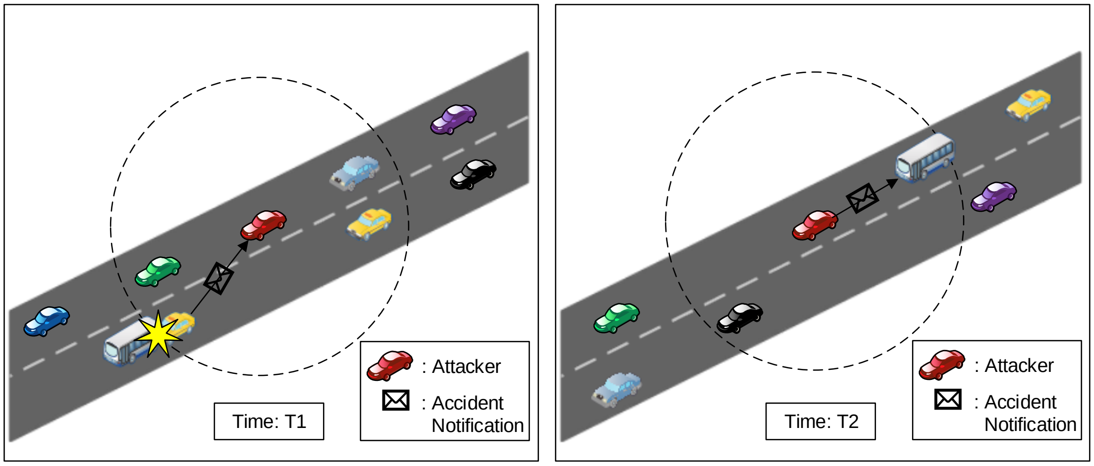

Fig. 3. Replay attack

2.7. Passive Eavesdropping Attack

Passive eavesdropping attack refers to monitoring the network to track vehicle movement or to listen in on their communication by utilizing wireless medium characteristics. Malicious vehicles could simply intercept and examine the messages which flow in the network. This passive attack is also known as traffic analysis attack or stealth attack [26]. The goal of the attacker is to gather information about the vehicles and communication patterns for further attacks. It is usually carried out before implementing other types of attacks such as blackhole and DoS attacks. The impact of passive eavesdropping attack could be very high, since it could be a part of an extremely sophisticated low-and-slow form of attack.

There are also other types of attacks such as route disruption attacks [27] in which attackers take advantage of the vulnerabilities and the cooperativeness of routing protocols. However, in the literature it was found that researchers mainly focus on routing protocol-independent attacks such as dropping, Sybil, and such like. Furthermore, some attacks reported in the literature are explored for an application scenario, especially for safety-related applications. While a few studies proposed especially for some routing protocols, which are explicitly specified in this survey, some of them aim at detecting application-specific attacks. At the top level, attacks can be classified according to network protocol stacks. All of the aforementioned attacks and the corresponding layers in which they could perform are presented in Fig. 4. Other classifications are also possible such as passive and active attacks, atomic and composite attacks, etc.

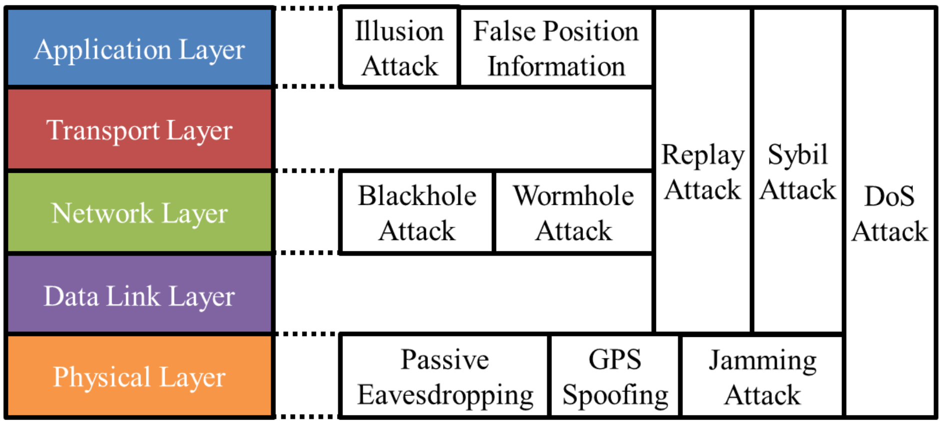

Fig. 4. Attacks with corresponding Internet Protocol Stack Layers

3. SECURITY SOLUTIONS

This section presents the security solutions proposed in the literature for each of the attack types mentioned in Section 2.

3.1. Sybil Attack

Sybil attack was introduced by Douceur in 2002 [28] and is one of the most dangerous and evasive attacks against VANETs since attackers could easily bypass security mechanisms based on honest majority assumption by using multiple identities. Sybil attacks employed with DoS attacks are claimed to be among the most dangerous forms of attack in VANETs [5]. Correspondingly, many researchers in the literature focused on detecting Sybil attacks.

In one of the earliest solutions for Sybil attacks, Golle et al. [29] devised a heuristic approach called adversarial parsimony in order to detect Sybil attacks in vehicular networks. Informally, it means finding the best explanation for corrupted data received. After improving the nodes' sensor capabilities such as using cameras and exchanging data via a light spectrum in order to verify that a claimed position is true, determining which nodes really exist is possible. Data collected from the sensors is used to reach information that enables distinguishing between nodes. After exchanging that information between vehicles, the heuristic mechanism detects inconsistencies in the case of a Sybil attack by comparing received data to a VANET model maintained by each vehicle and refers all of its knowledge about the VANET. However, detection mechanisms are neither supported with simulation nor explained in depth.

In another early study, Xiao et al. [30] presented a lightweight security scheme based on estimating the position of a node by analyzing its signal strength distribution. In this approach, three roles are assigned to vehicles. *Claimer* is the vehicle which periodically broadcasts beacon messages, including its identity and position. *Witness* is the vehicle residing in the claimer's signal range. Witness nodes measure signal strengths of the claimer and then save this information together with the corresponding claimer's identity information in their memory. Thus they keep a neighbor list which will be broadcast within the next beacon message. When a beacon message is received, *verifier* vehicles wait for a period of time in order to collect previous measurements of the claimer from witness nodes. Then, they can calculate an estimated position of the claimer. RSUs are used to certificate positions of vehicles around them in order to be sure about the direction of a vehicle. Hence, information received from Sybil nodes could be ignored. Also, all witnesses for a claimer should come from the opposite direction. Since vehicles from the same direction are potential Sybil nodes, it is ensured that all witnesses are physical vehicles. However, an attacker can change the strength of the signal to a value corresponding false position information and bypass the consistency check mechanism. A study on the effectiveness of using signal strength distribution to detect the attack is given in [31], and [32] shows that the type of antenna in use has a remarkable effect on detection.

Zhou et al. [33] propose a privacy-preserving detection scheme without forcing vehicles to disclose their identities in the network. The Department of Motor Vehicles (DMV) assigns a unique pool of pseudonyms instead of assigning exactly one ID for each vehicle and pseudonyms in the same pool are hashed to a common value. Thus, a vehicle can use any pseudonym in its pool and preserve its privacy. Since the hash is stored at the roadside units (RSU) and also at the DMV, a RSU could check whether received pseudonyms belong to the same pool or not. When a RSU becomes suspicious of a Sybil attack, it sends the pseudonyms and the hash values of the possible attacker to the DMV. After that, the DMV confirms whether or not the suspicious pseudonyms have been assigned to the same vehicle. The last step is necessary because the RSU could itself have been compromised by the attacker. In that case the RSU would need to be revoked. Although the solution can detect Sybil attacks while achieving privacy, it requires individual vehicles to be registered and administered by trusted authorities [34]. The authors have improved their scheme by making it adaptive based on traffic volumes in [35].

Similar to [33] in terms of preserving privacy, Yong Hao et al. [36] devise a protocol that enables vehicles to detect a Sybil attack in a cooperative manner. The protocol utilizes group signature to preserve privacy and correlation of mobility traces. It includes three phases: probing, confirmation and quarantine. In the *probing phase*, vehicles periodically broadcast their geographic information along with identifiers of the vehicles around them. The c*onfirmation phase* refers that in the case of an anomaly detection, vehicles around the possible attacker inform others by broadcasting warning messages with their partial signatures. If the number of vehicles which report anomalies reaches a threshold, it is possible to derive a complete signature and the attacker is identified. However, if no vehicle is able to derive a complete signature after the possible attacker is inspected by the first *n* consecutive vehicles which come from the opposite direction, the possible attacker is considered as benign. In the *quarantine phase*, the latest geographic information of the Sybil node will be notified by the vehicles around. The identified attacker could be isolated for a while or reported to legal authorities. According to simulations, the security protocol is efficient; however it is not evaluated in the existence of multi attackers.

Lee et al. [37] introduce a DTSA (Detection Technique against a Sybil Attack) protocol which uses Session Key based Certificate (SKC) and protects privacy of the vehicles. Firstly, each vehicle's unique ID should be registered to a global VANET server. Then, a vehicle V generates its anonymous ID and validates it by using a local VANET server. Next, they both generate a session key and use it in order to generate V's local certificate. After that, V could transmit messages using its local certificate. Any receiving vehicle could validate V's true identity by asking a local VANET server to send V's local certificate and compare it to the received message. If the result is not a match, the attack is detected. Even though simulation results show that detection time is low, using SKCs requires a large amount of overhead data.

Similar to DTSA [37] in terms of infrastructure, Rahbari et al. [38] present a cryptographic method which utilizes PKI infrastructure in order to detect a Sybil attack. The approach requires RSU support and includes four phases. In phase 1, each vehicle has to be registered and receive its group authentication key from RSU in order to start transmitting, receiving and authenticating messages within the group. In phase 2, when RSU receives a message from vehicle V, it forwards the message to the Local CA since the private key of a Local CA is necessary to decrypt the message. In phase 3, after decrypting the message, the Local CA needs the private key of V in order to check the identity of V. Therefore the Local CA sends a request to the Home CA. In phase 4, the Home CA replies with the private key of vehicle V and after that, the Local CA is able to detect a Sybil attack by comparing the reply message received from the RSU. Simulation results show that the proposed method has low delay and detect the attack efficiently. However, as the authors stated, vehicles moving to regions which belong to other CAs cause problems in the detection process.

Recently, Feng et al. [39] suggested a system called Event Based Reputation System (EBRS) in order to detect Sybil attacks. Each vehicle has a public key and pseudonyms which are valid for a limited time and validated by the Trusted Authority (TA) over RSUs, and a local certificate issued by an RSU. In addition, each RSU stores the pseudonyms, locally generated session key and local certificate of each vehicle in its area. When a vehicle V receives a warning message about an event E from a neighbor N, V will send N's pseudonym and N's local certificate that is encrypted with N's session key to local RSU. After that, the

RSU is able to find N’s session key corresponding to the received pseudonym and decrypt N’s local certificate by using the key. Then, if the decrypted certificate matches with N’s local (previously stored) certificate, N’s certificate is validated. Therefore, it is possible to detect forged, stolen, or expired pseudonyms. Furthermore, V will store or update the reputation and trusted values of event E in its event table. The system does not alert the driver of V unless both the reputation and trusted values of E reaches predetermined corresponding thresholds. If the warning message about E received from a Sybil attacker is false, the values would not increase since other vehicles have not reported the false event. According to simulations, EBRS could effectively detect Sybil attacks. However, the assumption that RSUs and OBUs could not be compromised may not always hold.

Another privacy-preserving solution called Footprint, which is based on similar motion trajectories of vehicles, is presented by Chang et al. in [40]. A dedicated RSU infrastructure is deployed and managed by a Trust Authority (TA) which is also responsible for trust relationship between entities in the network. An anonymous vehicle V communicates with encountered RSUs and demands authorized messages as a proof of presence located near to a specific RSU within a specific time. As V moves, consecutive authorized messages collected from encountered RSUs form a trajectory of the vehicle. When V starts communicating with a RSU and/or vehicle, it provides its trajectory (chain of authorized messages) to the other party to be verified. Since the authorized messages can be used to track the vehicle, they must be anonymously signed by RSUs. Therefore, instead of identifying the real trajectories of the vehicles, similarity between anonymous trajectories of a possible Sybil group is used in the detection process. In addition, two authorized messages issued by one RSU must be linkable only for a short period of time in order to prevent an attacker revealing the trajectory of V. Consequently, vehicle V could detect a Sybil “community” by comparing similarities between each pair of trajectories of vehicles. According to evaluation results, Footprint has high detection rate. However, it requires a dedicated infrastructure formed by RSUs and it makes an assumption that all RSUs are trustworthy.

Chen et al. [41] rely on the similarity of Sybil nodes’ motion trajectories, which are unrealistic and unacceptable in the real world, assuming Sybil nodes have the same location and motion trajectories all the time. The solution makes Sybil attack detection possible for each vehicle independently. It needs authorized infrastructures in order to provide tamper-free periodic digital signatures to nearby vehicular nodes. The authorized infrastructures could be RSUs and mobile units such as police vehicles and public transport vehicles. Vehicular nodes carry these signatures (infrastructure, time) and the signatures are exchanged between neighboring vehicles. With the limited assistance from the infrastructures, each node could detect the Sybil attack independently in four steps. After *gathering* signature vectors of all the neighboring nodes, it *calculates* the difference value of the gathered signature vectors. In *judging* step, a threshold is used to determine whether or not a Sybil attack exists. Finally, by *classifying*, Sybil attackers are detected and all Sybil nodes fabricated by the same malicious node are included into one Sybil set.

However, as shown in Grover et al. [42], if two or more vehicles driving in opposite directions receive the same signature at almost the same time from a RSU and this situation continues for a time exceeding a predefined threshold, those vehicles could be falsely identified as Sybil nodes (see Fig. 5 – Vehicle A and Vehicle B).

Park et al. [34] propose another approach based on timestamp series without using a vehicular public key infrastructure. Before one vehicle sends a message to another, it first sends a request to a nearby RSU in order to obtain a timestamp for the message. After that, the message is sent. The timestamps could be used to find each vehicle's recent trajectory and time. If vehicles receive similar timestamp series from the same RSUs for a certain amount of time (see attacker and Sybil vehicles in Fig. 5), they will be considered as Sybil nodes and treated as a single node. However, similarly to Chen et al. [41], two vehicles coming from opposite directions could be falsely accused as Sybil nodes because they will receive similar timestamps for a short while. Grover et al. [42] presented a similar system based on the theory that two nodes cannot have the same set of neighbors for a time longer than a threshold. The difference from the previous works in [34] and [41] is to be able to detect Sybil attacks by only using records collected from neighbor nodes. It does not ask for support from surrounding infrastructures such as RSUs. However, the false accusation problem still remains unresolved.

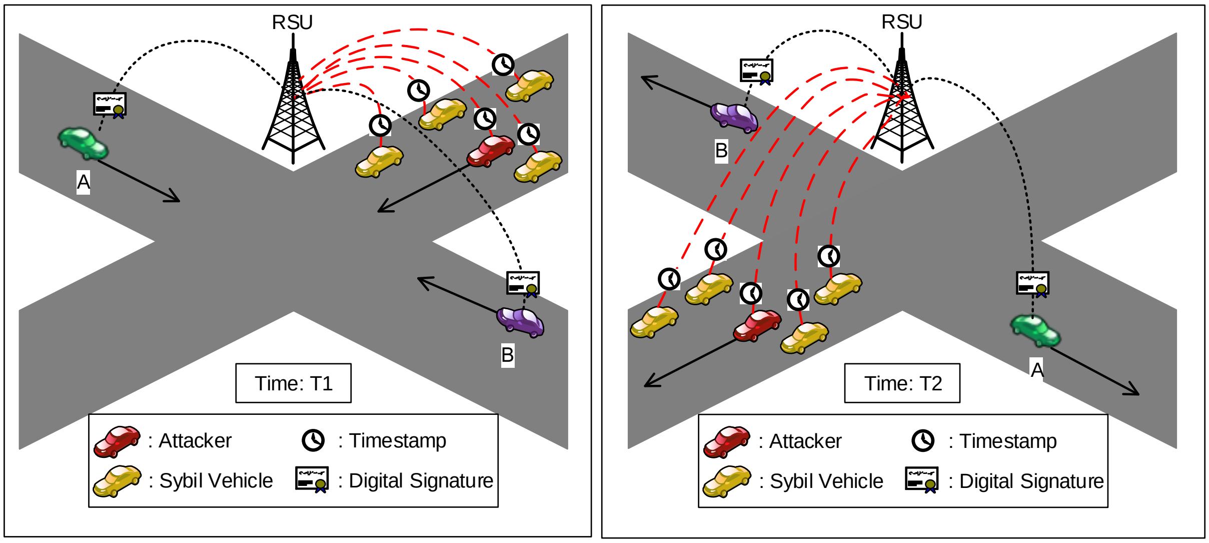

Fig. 5. Motion trajectories over time

To sum up, most of the promising detection techniques described focus on observing similarity of motion trajectories, which is the most significant characteristic of Sybil nodes in order to detect an attack. However, considering that many people follow the same route to their place of work at almost the same time, such as in the daily rush hour, false positive rates caused by false accusation of benign vehicles could increase. Moreover, vehicles in a network could follow the same routes in different modes such as platooning or as a motorcade during a ceremony; therefore, different models should be constructed for such cases.

3.2. Denial-of-Service Attack

The effects of a DoS attack in VANETs might be more severe than expected. For example, it could bring down the network and hence, cause traffic accidents. Some solutions, such as [17] that proposed detection of DoS attacks against MANETs, could also be employed in VANETs.

Soryal et al. [43] present a solution to detect DoS attacks in IEEE 802.11 DCF. They use a Markov chain model in order to generate an adaptive threshold, which is the maximum rate of messages any node can send over time with respect to the number of other nodes. If a node notices the number of CTS (Clear-to-Send) messages received per second for a destination address is above the threshold, the sender of the CTS messages is tagged as an attacker. The simulation results show that the threshold-based approach is able to detect the attacker(s) efficiently. However, the solution is not scalable because it is designed for nodes communicating with a single *hotspot* which acts the same as a RSU.

Verma et al. [44] devise a system to prevent DoS attacks by monitoring TCP packets. The mechanism, called *the request detector*, is deployed at the edge router of innocent hosts and can be considered as a RSU. The request detector keeps a table which records source and destination IP addresses by using *Bloom filter*, a space-efficient probabilistic data structure that guarantees no false negatives. The system continuously monitors SYN and corresponding SYN-ACK packets and maps them. If the number of outstanding SYN packets becomes more than the determined threshold within a certain amount of time or an unmapped ACK/SYN message is received, a suspicious alarm is sent to *The Response Detector* which is deployed at the protected master node. Therefore, the existence of DoS attacks can be known at a very early stage and according to simulation results, the approach uses memory efficiently. In [45], the same authors present another scheme based on Bloom filter and random deterministic message marking (IP-CHOCK) in order to detect DoS attacks. The mechanism should be deployed at edge routers in order to take place near the possible attacker. The packets are marked when they arrive at the edge router. The real source IP addresses of vehicles are included in the marking fields. Thus it is possible to reconstruct addresses at the destination. There are three phases in the detection process. IP addresses are collected during *detection engine phase 1* and checked as to whether or not they are malicious IPs during *detection engine phase 2*. In the *Bloom-filter phase*, if they are malicious, an alarm is raised and a reference link is sent to other vehicles. Evaluation results show that the proposed scheme effectively detects the attacks. However, both of the proposed schemes require a dedicated infrastructure.

Kerrache et al. [46] develop a framework called TFDD based on trust establishment between vehicles which is able to detect DoS and DDoS attacks in a distributed manner. Each vehicle V utilizes some parameters by using its various modules. The first parameter is honesty weight (H) which is initially assigned as 1 to each neighbor N. If V receives more packets from neighbor N than the thresholds which are predetermined, the *Intrusion Detection Module* punishes N by locally decreasing its H value. The second parameter is quality weight (Q) which refers to overall quality of packets received from N. These two parameters are periodically combined by the *Delayed Verification Module* in order to generate DoS weight (DW) which will be used as another parameter to globally decide whether or not a DoS attack exists. On the other hand, trust weight (TM) of every message M received from vehicle N is combined with the Q parameter by the same module. If the TM value is below a predefined threshold, the minimum of the two parameters is selected as the new TM value to impose a fine on N. After that, in the *Decision Module*, TM and DW parameters are combined in order to calculate the updated trust value between V and N (TN). If both TN and DW values are not between the two predefined thresholds, it is possible for vehicle V to include its neighbor N to its local blacklist. In that case, N could be included to the global blacklist and suspended from network operations by a trusted authority as proposed in [47]. Even though the scheme is able to detect the attack effectively according to simulation results, determining the thresholds in an adaptive manner could have increased detection rates.

DoS attacks can be implemented at different layers, hence different solutions are proposed for each layer. Since a DoS attack usually refers to exhausting available resources, determining threshold values is the most preferred method of the aforementioned solutions. Determining those thresholds dynamically is more suitable for VANETs due to its highly mobile and dynamic environment. In addition, almost all solutions presented have some kind of response mechanism to fight against an attack.

3.3. Blackhole Attack

Blackhole attacks result in packet losses in the network and it could affect life-or-death decisions where safety-related applications cannot send or receive critical data. For instance, a vehicle which is involved in a traffic accident should propagate warning messages, but an attacker could prevent others from receiving the warning by misrouting packets. Solutions which address such an attack are as follows:

Hortelano et al. [48] evaluate the protocol independent watchdog mechanism [9] in VANETs. In watchdog, if node A sends a packet to node B, node A can check whether or not node B forwards the packet by covertly listening to node B’s transmissions due to the nature of wireless medium. In the proposed solution, each vehicle uses a *neighbor trust level* for each neighboring vehicle. Neighbor trust level can be determined as the ratio of packets sent to the neighbor and the packets which are actually forwarded by the neighbor. However, packets may not be forwarded because of a collision, as well as due to an attack. Hence, a *tolerance threshold* is determined in order to prevent the false accusation of benign vehicles. Consequently, if a vehicle keeps on dropping packets until the tolerance threshold is exceeded, it will be considered as malicious and an alert message is generated. However, as the authors mentioned, a watchdog mechanism can be deceived when there are two consecutive attackers in the network.

Daeinabi et al. [49] propose an algorithm which utilizes vehicles monitoring each other in order to detect vehicles explicitly drop or duplicate packets. The vehicles are grouped into clusters and the Cluster Head (CH) is the most trustworthy vehicle in each cluster which can be selected dynamically. When a vehicle V joins the cluster, *verifiers* of V start monitoring the behavior of V. Verifier vehicles have to be more trustworthy than V and located in such a way that they are able to monitor V and report to the CH. If a verifier observes that V is dropping or duplicating packets, it reports V to the CH. After that, the CH increases the distrust value of V, and informs V's neighbors about the new distrust value. If that value becomes higher than a threshold, CH reports V to the Certificate Authority (CA). The CA adds V to the main blacklist and informs all vehicles. As a result, other vehicles isolate V from the network by not communicating with it. The simulation results show that the proposed algorithm could detect possible attackers at high speeds. However, it causes high end-to-end delay and jitter [50]. The algorithm is improved by including a prevention feature in [50] and by selecting verifiers more effectively in [51].

Wahab et al. [52] proposed a mechanism which also utilizes watchdog mechanism in order to detect selfish behaviors as well as Blackhole attacks against QoS-OLSR [53]. It is a five-phase detection technique based on Tit-for-Tat concept and Dempster-Shafer theory of evidence. In the *reputation calculation phase*, initial reputation values are assigned to vehicles and Multi-Point Relay (MPR) nodes are selected by elected cluster-heads in order to forward traffic to other clusters. In the *watchdogs monitoring phase*, MPR nodes are observed by cluster members, as the name implies. Then, the cluster-head utilizes a voting mechanism and aggregates observations to make a final decision for cooperation by using the Dempster-Shafer theory of evidence during the *votes aggregation phase*. After that, in *Tit-for-TaT cooperation regulation phase*, if the trustworthiness of a MPR is higher than a predetermined threshold, the decision will be made to cooperate with the MPR. Finally, during the *information dissemination phase*, cluster-heads broadcast the results to cluster members and other cluster-heads. As a result, the members isolate the vehicle(s) which are classified as malicious. Simulations show that the proposed cooperative mechanism performs better than techniques based on one-to-one watchdog decisions.

By using watchdog mechanism in a cooperative manner, Baiad et al. [54] proposed a solution based on monitoring in both network (VANET-OLSR protocol) and MAC layers in order to detect blackhole attack targeting the Multi Point Relays (MPRs). The solution utilizes the cooperative watchdog mechanism [55] which relies on routing level monitoring and could falsely accuse benign nodes in cases of packet loss due to legitimate collisions. In order to minimize the false positive rate, detections reported by the cooperative watchdog are filtered by using MAC layer monitoring. If the number of the sent RTS packets is different to the number of received CTS packets, the cause of the packet loss is a legitimate collision. The proposed cross-layer scheme correlates the results from both layers and, after eliminating watchdog detections caused by collisions, the attackers can be identified. Simulation results show that the scheme has a lower false positive rate and a higher detection percentage than the cooperative watchdog mechanism. However, randomly selected watchdog nodes, which are assumed as trusted, might be malicious and could affect the performance of the proposed solution. In [56], the authors enhanced their cross-layer solution by aggregating physical layer detection with MAC and network layer detection and improved the detection rate.

Unlike other solutions based on watchdog mechanism, Guo et al. [57] introduced a detection mechanism based on *encounter tickets (ER),* which is introduced in [58]. It is assumed that by using data about previous encounters of a vehicle, it is possible to evaluate its behavior. After two encountering entities such as vehicles and/or RSUs to successfully exchange data, they send a digitally signed ER which contains information about the encounter to each other. The ER includes timestamp, IDs of both vehicles, and the sequence numbers which are unique for each contact. Therefore, by exchanging ERs during an encounter, a vehicle could provide intact information to others about its behavior. It is also assumed that each vehicle has a *Trust Reputation (TR)* value which is decreased in case the vehicle V selectively drops packets. In addition, each vehicle has a blacklist and a meeting list which contains information about all previously encountered vehicles. Hence, if V has a TR value lower than a threshold or tries to forge or replay ERs, other nodes could detect and isolate vehicle V by adding it to their blacklists. The authors also introduced an adaptive threshold mechanism [59] and a more flexible approach for dense and sparse networks by using cluster analysis in [60]. However, the attacker could still drop packets after gaining reputation by tailgating [61].

Yao et al. [62], recently proposed an entity-centric trust model which could detect blackhole attacks. Each vehicle uses three trust parameters initialized with default values. Firstly, each vehicle A calculates its *direct trust value* to vehicle B based on B’s data forwarding rate and the forwarded data’s weight according to its data classes: traffic safety, traffic efficiency, and infotainment data. Secondly, the *recommendation value* of A to B is determined by utilizing A’s direct trust value to its neighbors and their comprehensive trust values to B. *Comprehensive trust*, the third parameter, refers to a dynamically varying combination of direct trust and recommendation parameters. If A’s calculated comprehensive trust value to B is lower than the predefined threshold, B could be detected as an attacker and isolated. Even though the proposed model could detect a blackhole attack while maintaining the routing performance at a reasonable level according to simulations, the rate of malicious vehicles in the network is not specified in the simulations.

To conclude, watchdog mechanism, which refers to checking the forwarding state of the forwarded packets by monitoring the next hop neighbor over wireless media, is the most chosen method to ensure that a neighbor is not a blackhole attacker. As shown in [55], utilizing watchdog mechanism in a cooperative manner could increase the detection rate.

3.4. Wormhole Attack

In a wormhole attack, the attackers use tunnel(s) which attract a large amount of network traffic. Therefore, collecting critical network data becomes possible for the attacker. Moreover, the attacker could manipulate traffic and/or perform more aggressive attacks by analyzing collected data. Attack detection is difficult since it does not generally affect normal network operations. Proposed works for detection are presented as follows.

Safi et al. [63] introduced a solution which relies on *leashes* for on-demand routing protocols. A leash is a mechanism that controls the packet's maximum and allowed transmission distance by using information in the packet. The authors prefer geographical leashes in order to guarantee that the distance between the sender and receiver of a packet is no larger than a certain value. It is assumed that all vehicles know their own location and that they have loosely synchronized clocks. When a vehicle wants to send a packet, the sending vehicle includes the time and its own location in the packet. The receiving vehicle then compares these values to its own parameters. By multiplying hop count value and predefined maximum transmission range value for a vehicle, it is possible to calculate the maximum travel distance (x) of a received packet. If x is smaller than the physical distance between the sender and receiver, or the packet has moved faster than a predefined maximum velocity threshold, the attack is detected. In addition, packets must be authenticated at each hop by using a HMAC-based algorithm in order to prevent modification and provide non-repudiation. In a similar manner, if vehicles' location parameters are involved in message authentication as in Biswas et al. [64], it is possible to detect the attack by identifying tunneled packets which have been transmitted over maximum allowed distances.

3.5. Bogus Information Attack

Disseminating bogus information could cause different results with respect to the intent. For example, a selfish attacker that manipulates other vehicles to take alternative roads is generally considered harmless. However, a malicious attacker could do the same in order to cause serious accidents. We researched and categorized previous works about disseminating false information and the results are presented as follows. The proposed solutions use a wide range of mechanisms such as verifiable multilateration and watchdog, since there are numerous kinds of false information which could be disseminated by the attacker.

Kim et al. [65] propose a message filtering model to effectively detect bogus information. The model includes a *threshold curve* and a *certainty of event (CoE)* curve. The CoE, which indicates the confidence level of a received message, is calculated by combining the data from various sources such as local sensors, RSUs and reputation mechanism. Priorities of the sources could be changed by the specific application for the event so as to minimize computation. For example, a warning message about the road condition that comes from a nearby trusted RSU could override other sources and make it unnecessary to check them. The more a vehicle approaches to a real event, the more it receives messages reporting the event which increases the CoE value. Since the solution relies on honest majority, an attacker which controls a small fraction of the network cannot deceive the vehicle. The threshold curve shows the insensitivity of the driver with respect to the distance to the event. Sensitivity and the distance to the event are inversely proportional. Therefore, while the threshold value is decreasing, the CoE value keeps increasing and, if it exceeds the threshold value which is assigned according to the application, the driver is warned with an alert message and the reputations of vehicles which reported the event will be increased. Otherwise, the alert is discarded; meaning it is considered bogus and the reputations of corresponding vehicles will be decreased and if they continue lying, their messages may be filtered. However, on the whole, it does not address bogus information attacks in various applications except the Electronic Emergency Brake Light (EEBL) application, which enables broadcasting self-generated emergency brake event information to nearby vehicles.

Another solution called *Misbehavior Detection System (MDS)* was devised by Raya et al. [66] to detect neighboring attackers disseminating bogus information. It is assumed that there is a Certificate Authority (CA) which provides one public/private key pair and a certificate for each vehicle. Also they use *entropy*, a typical measure of information, to make it possible for a vehicle to represent and compare normal and anomalous behaviors in order to detect the attacker. After that, the vehicle performs k-means clustering, partitioning observation space into k clusters in a way that the sum of distances of all points to the corresponding cluster centroids are minimized. Therefore, the vehicle could detect which neighbor(s) differentiates from other neighbors since it is the attacker. For instance, if high velocity information received from a neighboring attacker is contradictory to the state of the honest majority in a traffic jam, it will be detected. After detection, another proposed protocol, *Local Eviction of Attackers by Voting Evaluators (LEAVE)*, is activated to isolate the attacker by revoking its certificate. Although the system is effective and efficient, it requires an honest majority. If there are too many compromised neighbors, they could dominate what “normal” behavior looks like and the attacker could remain undetected.

Ghosh et al. [67] propose a scheme for post-crash notification (PCN) applications. It is assumed that the trajectories which a vehicle V follows in case of no alert and receiving a PCN alert conforms a free flow mobility model and a crash-modulated mobility model, respectively. Upon receiving a PCN alert, V analyzes its driver’s behaviors in response to the alert for a while and compares the actual trajectory and the expected trajectory based on the model. Based on the deviation, the alert is considered as valid or not. For example, if V comes across a crash site and the location of the site is different from the one reported by the PCN alert, V’s actual trajectories deviate from what was expected. Therefore, it is possible for each individual vehicle to identify the root-cause of misbehaviors by utilizing a cause-tree. After that, the scheme will be able to determine a response with respect to the identified root-cause. Even though the proposed scheme provides reasonable detection rates according to simulations, modeling expected trajectories for every possible alert situation in a sensitive manner is not a feasible solution [5].

3.5.1 False Position Information

In VANETs, false position information could cause a severe decrease in the overall packet delivery ratio which affects reliability. Since safety-related applications need reliable position information, serious safety issues could arise. Various approaches are proposed for detection.

Vora et al. [68] devise a solution for position verification in a region R. The solution includes two kinds of verifiers: *acceptors* and *rejecters*. While acceptors are distributed over the region R, rejecters are placed around the acceptors in a closed circular fashion. It is assumed that secure and reliable communication between verifiers is provided and verifiers are synchronized. When a node sends a signal, position verification is performed by the verifier which receives it first. If the signal is first received by an acceptor, it is verified that the node is located within region R. Despite the fact that the given approach is versatile, a node can spoof its location as soon as it resides within region R since it does not verify the exact location of the node. Although developed for mobile devices, it can also be implemented in vehicular networks. In VANETs, the approach can be implemented with multiple RSUs surrounding one RSU in order to check if a vehicle's claimed position is false or not.

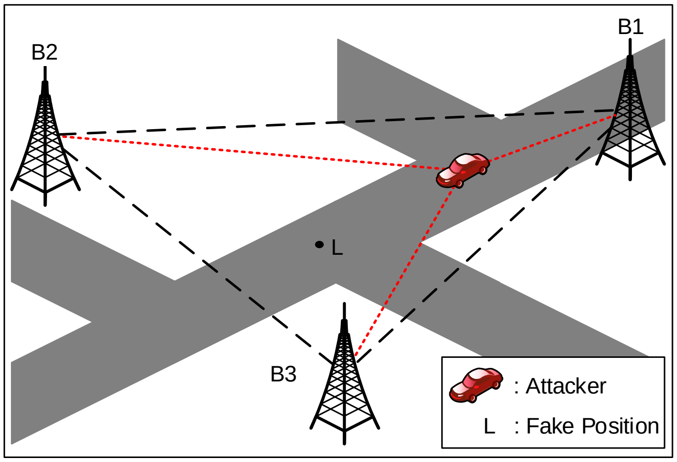

Fig. 6. Verifiable multilateration

By utilizing similar physical characteristics, Hubaux et al. [69] present *verifiable multilateration* which relies on *distance bounding* [70] for position verification in VANETs. Distance bounding is a technique to estimate physical distance. It is based on the fact that light travels at a finite speed. Therefore, by measuring the time between sending a message to vehicle A and receiving its corresponding message, it is possible to determine an upper bound on physical distance between RSU and vehicle A. An attacker vehicle could show itself further away by delaying messages, but will be detected if it tries showing itself closer to the RSU. Therefore, in a case there are two RSUs, vehicle A could not deceive both of them. If the same technique is employed by more than one station in different dimensions, it is called verifiable multilateration which enables estimating the exact location of vehicle A. In Fig. 6, the attacker vehicle can claim it is at location L by delaying messages coming from base station B1, however, it is impossible to reply to messages coming from B2 and B3 as if it is located at position L. The authors show that three stations positioned to form a triangle can verify vehicle A's location in two dimensions if it resides within the triangle and four verifiers forming a triangular pyramid can do the same operation in three dimensions. Although the verification process is fast, the solution requires a dedicated infrastructure and according to

[71], an attacker can send delayed responses to each station by using directed antennas to deceive the system.

Leinmüller et al. [71] propose another position verification approach based on a trust model. It is assumed that there are two groups of sensors which provide observations. The first group works autonomously and provides the necessary information in order to detect false (invalid or incorrect) position information. As an example of this*, the Acceptance Range Threshold (ART)* sensor discards packets which include position information that is further than the predefined maximum acceptance range threshold. Obtained information is weighted according to the reliability of the providing sensor and used to determine the overall trust ratings of neighbors. For example, information provided by an ART sensor is more reliable than the information provided by a *Map-Based Verification* mechanism which checks whether or not a vehicle is at an invalid location (*e.g.* off road). Because of weighting abnormal observations that are higher than normal, a vehicle's trust level is more affected by abnormal observations. Therefore, after sending one bogus information packet, the vehicle has to send a few correct information packets in order to regain its previous trust level. The second group works cooperatively with other vehicles. For instance, *Proactive Exchange of Neighbor Tables* mechanism lets the vehicles exchange and compare neighbor tables so as to believe the majority in case of false information. The approach needs no infrastructure and, according to the simulation, it detects vehicles which disseminate false positions with an accuracy of 95% in most scenarios. However, an attacker vehicle can still disseminate bogus information as long as it meets the criteria being enforced by the sensors. Moreover, it can deceive its own sensors, as described in the subsequent section.

Bissmeyer et al. [72] propose a signature-based scheme which relies on a plausibility model. Each vehicle is modeled as differently sized and nested rectangles, and intersecting rectangles that belong to different vehicles could indicate false position information. Due to inaccuracies of positioning systems such as GPS, the probability of a real intersection is associated with intrusion certainty and trust values by each individual vehicle. Intrusion certainty value is calculated based on the number of observed intersections, and the attack is not identified unless it is above a predetermined threshold. In addition, by utilizing the Minimum-Distance-Moved (MDM) concept proposed in [73], the trust values are also used for detection in such a way that when vehicle N remains as a neighbor of V for a distance which is larger than the transmission range, N becomes more trustworthy as a result. Therefore, from V's point of view, when N intersects with another neighbor and the difference between trust levels of both vehicles is higher than a threshold, the less trustworthy vehicle is identified as an attacker. According to the simulation results, the proposed plausibility model could detect false position information in spite of GPS error(s). However, an attacker whose transmission range is larger than other vehicles could bypass the trust mechanism.

Ruj et al. [74] devise a data-centric misbehavior detection system (MDS) which can be used to detect false location information. The idea of data-centric MDS concept is to classify data instead of classifying vehicles. Each vehicle can verify the location information independently by using the proposed technique. An attacker sends a beacon message which includes fake location information (L1) along with the timestamp it is sent (T1). After it is received by a vehicle V located at L2 at time T2, V can verify if L1 is correct or false by utilizing L1, L2, speed of light and the difference between T1 and T2. In that scenario, the attacker is not able to modify T1 in order to deceive V since it does not know the exact distance between itself and V. If the location is detected as false, V broadcasts a message to other vehicles and the CA through the nearest RSU. This leads to fines imposed on attackers instead of isolating them from the network. The authors compared the proposed scheme with existing MDSs in terms of communication overhead; however, it is not supported with simulations.

3.5.2 Sensor Tampering

Sensor tampering can be easily performed. All the attacker needs to do is to trick its own sensor(s) into reporting valid, but false messages. For example, the attacker can use some ice in order to deceive ice/temperature sensor(s) and generate messages indicating false road conditions. Therefore, it is possible to disseminate false information to the network even though message integrity remains protected.

3.5.2.1 Illusion Attack

In an illusion attack, the attacker needs a *scene* which enables the deceiving of other drivers easier, in addition to tricking sensors. Therefore, it is possible to influence other drivers' behaviors by disseminating bogus information which is supported by traffic situations.

Lo et al. [24] introduce the illusion attack and a plausibility mechanism called *Plausibility Validation Network (PVN),* which is capable of checking the output data of sensors and deciding whether or not the data is valid. The proposed solution includes a plausibility network (PN) checking module and a rule database. The system for any message which is received from other vehicles or generated from the sensors works as follows: Each message is evaluated with respect to its type (accident, general road condition, etc.). A corresponding predefined rule set is retrieved from the rule database for a PVN in order to check reasonability of the value of an element field (timestamp, velocity, etc.) of the given message. For example, similar to other fields, the plausibility of the timestamp field is checked by determining its minimum and maximum boundaries. The received timestamp value must be earlier than the receiver's current timestamp and later than the difference between the receiver's current timestamp and the validity period of the message. Lastly, the values are cross-verified with values of other relevant element fields. If the verification of all element fields in the message is completed successfully, the message will be considered as trustworthy. Otherwise, it will be discarded.

3.5.2.2 GPS Spoofing

Attackers could convince victim(s) to think that they are in a different location. To this end, they generally use GPS simulators which generate more powerful signals than the original GPS generates. Studer et al. [75] propose a simple mechanism to detect GPS spoofing by dead reckoning. Dead reckoning calculates one's current position by using a previously determined position and known or estimated speeds over elapsed time. Although it can detect and filter out spoofed GPS information, the calculated position is only approximate.

3.6. Replay Attack

In replay attack, legitimate data which is gathered or originated by the attacker is simply stored for use later. Therefore, as long as the data remains valid, the attacker can get the same results as recurring the original situation. A method which utilizes traditional timestamp mechanism for detecting the replay attack [76], could be employed for VANETs. A node that receives a message checks the timestamps. If the difference between current and received timestamps is larger than a predefined threshold, the message is rejected or dropped. The key point of detection of the attack is ensuring timestamp integrity.

3.7. Solutions for Multiple Misbehavior Detection

Yan et al. [77], devise a solution based on *"seeing is believing"* which enables fast detection of misbehaving vehicles. They assume that each vehicle has a front and a rear short-distance radar which are used as the *virtual "eye"* of the vehicle. By using radar detections, neighbors' data and incoming traffic data provided by vehicles which are further than one hop, it is possible for a vehicle to "see" whether received data are fake or not. After that, similarity of data provided by those sources is calculated. Different sources have different weights. While radar detections have the highest weight due to their high level reliability, incoming traffic data has the lowest weight. If the similarity among the data collected from three different sources is close to each other, the data will be accepted. Otherwise it will be discarded. The accepted data will be used to compute the average position and velocity. After that, *map history* including the vehicle's past observed movements will be built. By checking map history, it will be possible to determine whether the given position(s) are consistent or not. The solution requires line-of-sight (LOS) between vehicles. However, even when LOS is limited temporarily, it is still possible to detect an attacker by correlating information coming from "eyes" and received from other vehicles. According to the simulation results, the approach is efficient in detecting malicious vehicles. In [78], the authors extended their solution by applying a similarity model and adding more "eyes" such as infrared detectors and CCD (charge coupled device)-based sensors which can cooperate with each other. However, a Sybil attack could still be performed while LOS between vehicles is blocked.

Kumar and Chilamkurti [79] develop an adaptive scheme called T-CLAIDS, which is based on Learning Automata (LA) and watchdog mechanism. Each node runs a particular code called *automaton* which takes the density, mobility and direction of motion of the vehicles as inputs from the environment in order to perform actions such as data collection, detection and alert generation to produce outputs. The automaton also calculates a Collaborative Trust Index (CTI) and updates its value with respect to received rewards and penalties from the environment which monitors performed actions. If the CTI value is lower than a predefined threshold, a malicious activity is detected in that region and generated alarms are immediately transferred to other vehicles since automatons share information with each other. According to performance evaluation results, the solution is capable of detecting malicious activities and is scalable.

Another watchdog-based solution called AECFV, which is a framework based on clustering and utilizing RSUs, is proposed by Sedjelmaci and Senouci [80]. AECFV includes three systems. While *Local Intrusion Detection System (LIDS)* and *Global Intrusion Detection System (GIDS)* are for detection, *Global Decision System (GDS)* is used to make final decisions. LIDS runs at member vehicles within a cluster and makes monitoring their neighbors and the cluster-head behaviors possible in their transmission range. In order to reduce overhead, vehicles do not activate their LIDS until they reach an optimal state called *Nash equilibrium*, a game theory concept. GIDS runs at each cluster-head and allows it to evaluate trustworthiness of cluster member vehicles by monitoring them. GDS runs at each RSU and categorizes vehicles into lists such as blacklist or suspected list by calculating their trust level. The framework can be used to address blackhole, wormhole, selective forwarding and Sybil attacks by utilizing watchdog mechanism and calculating adaptive thresholds for send/dropped packet ratios and signal strength intensity with the help of learning algorithms based on Support Vector Machine (SVM). Simulation results show that AECFV effectively detects such attacks.

The watchdog mechanism was also used by Wahab et al. [81] to develop an intelligent detection model called CEAP which is based on SVM and Quality of Service Optimized Link State Routing protocol (VANET QoS-OLSR) in order to detect misbehaving MPRs. The model includes four phases: during the *data collection* phase, cluster head and other cluster members monitor the behaviors of MPR nodes in a continuous manner. After the *data exchange phase*, which includes sharing collected information with other members of the cluster, each monitoring vehicle utilizes SVM to classify MPRs as cooperative or malicious by using its own observations as test data and others' observations as training data in the *data analysis phase*. Finally, a *data propagation phase* is proposed to enable cluster heads to exchange classes of MPRs. Even though simulation results show that the model has higher packet delivery ratio and detection rate than existing detection systems, it assumed the cluster head is a trusted third party.

Grover et al. [82] also proposed a machine learning approach in order to detect misbehaviors in VANETs. Various forms of misbehaviors and legitimate instances are used to extract features. In order to identify different types of misbehaviors, different features are extracted by using three inputs, which are the proposed VANET model based on some assumptions such that RSUs are always honest, the attack model, and the VANET application affected by the attack. After conducting experiments with different combinations of attacks, the extracted features calculated by observer nodes are as follows: speed deviation, distance, received signal strength (RSS), and the number of generated/delivered/dropped/collided packets. In order to classify the behavior of a vehicle as honest or malicious, the authors used Naive Bayes, IBK, J-48, Random Forest (RF), and AdaBoost1 classifiers and compared their results. The comparison shows that RF and J-48 classifiers perform the best. However, as the authors stated, the proposed solution may not be suitable in detecting temporal attacks such as replay attacks in a realistic VANET scenario. In order to increase detection performance, the authors improved their scheme by combining the results of previously mentioned classifiers to reach a final decision using ensemble-based machine learning in [83].

Bouali et al. [84] developed Intrusion Prevention and Detection System (IPDS), a predictive approach which is able to detect multiple misbehaviors before they can take place by predicting vehicles' future behaviors. The vehicles are grouped into one-hop clusters and there are three roles within each cluster. Firstly, the most trustworthy vehicle in each cluster is elected as *CH*. Then, three recommenders are selected by the CH in such a way that the CH divides its communication range into three equal regions and the most trusted vehicle closest to each region center is selected as a *recommender*. After that, the rest of the vehicles become *member vehicles* which are monitored by the recommenders. The CH permanently monitors the member vehicles and updates their trust levels by using its own observations and the information received from the recommenders. In order to detect a future attack, the CH utilizes Kalman filtering, a method that is able to predict future trust levels by using current trust levels and the previously predicted information as inputs. In addition, according to prediction results, the CH classifies the vehicles into white (benign), black (malicious), and gray lists. The gray list includes vehicles which intermittently misbehave. Moreover, the CH is responsible for broadcasting the identities of the vehicles in black and gray lists. Therefore, vehicles in the blacklist could be isolated from the rest of the network and vehicles in the gray list could be used for routing purposes when there are no vehicles in the whitelist. Also they can be moved to whitelist or blacklist depending on their behaviors. According to simulation results, IPDS is able to detect various misbehaviors effectively and accurately. However, if multiple attackers behave normally until seizing the CH and recommenders roles, an attack may take place.

Kerrache et al. [85] developed a trust architecture called T-VNets which mainly evaluates two trust parameters in parallel: *inter-vehicles trust* and *RSUs-to-vehicles trust*. Inter-vehicles trust is built by combining data centric evaluation of messages received from each neighbor vehicle N with received reports about the neighbor. These reports are broadcast by the neighbors of N who detect a positive or negative change in the behavior of N by using a watchdog mechanism. RSUs-to-vehicles trust means that RSUs collect reports from vehicles, about their neighbors' behaviors which help them to have a quasi-global trust value of each vehicle historically and regionally, since RSUs are usually connected to each other. After that, inter-vehicles and RSUs-to-vehicles trust are combined to estimate a global trust value for each vehicle. The estimation could also be performed in a limited manner by each vehicle if there is no

RSU within its vicinity. Then, global trust values will be inserted to periodically exchanged Cooperative Awareness Messages (CAM) through the addition of new fields. CAM is an ETSI (European Telecommunications Standards Institute) ITS standard which enables the periodic exchange of information, dynamics and attributes between vehicles and infrastructure [86]. While CAMs are used to evaluate regional trust, another ETSI ITS standard called Decentralized Environmental Notification Messages (DENM) are used to dynamically calculate a specific event's trust since DENMs are triggered based on road hazards [87]. The global trust value of a vehicle V reporting the event and the data centric evaluation of DENM message are used to calculate the event's trust. Therefore, events which have a lower trust value than a predefined threshold will not be broadcast by an intermediary vehicles and the V's global trust level will be updated. As a whole, by determining threshold limits for calculated trust values, it is possible for a vehicle to effectively detect a malicious vehicle.

Last but not least, Zaidi et al. [88], developed a scheme which relies upon statistical techniques in order to detect multiple misbehaviors. It utilizes a model named *Greenshield's Model* to predict and explain the trends in real traffic flows. Each vehicle could estimate its own flow parameter (F) which should be very similar for vehicles located closely to each other by using a model that employs density referring to vehicles per kilometer and the average speed of other vehicles in its vicinity. After that, vehicles exchange their own F and density values along with their speed and location information; hence each vehicle could have information about surrounding vehicles. For each received message, vehicles compare the average of the received parameters to its own calculated parameters. If the difference is lower than a threshold, the message is accepted. Otherwise, the sender is monitored and the data is accepted until the number of collected messages is enough to perform a t-test. Results of the test determine whether or not the sender is malicious. Then, the malicious vehicle will be reported to other vehicles and isolated from the network by rejecting its data. According to simulations, the proposed scheme could detect malicious nodes even when 40% of the vehicles are malicious. However, an attack performed in a low and slow manner may remain undetected by the system since the attacker only manipulates values gradually.

The solutions presented here mainly rely on watchdog mechanism to detect multiple misbehaviors. The reason is that they are mostly developed to let vehicles perform intrusion detection independently. This feature makes them deployable more easily and more quickly than other solutions since there is no need for a dedicated infrastructure. Furthermore, it is shown that artificial intelligence-based approaches with watchdog mechanism proposed in recent years have a potential in detecting multiple misbehaviors.

4. DISCUSSION

VANETs are continuously developing and attracting increased attention. Consequently, new attacks are being discovered, with impacts ranging from misrouting vehicles to traffic accidents. Attacker motivation plays a critical role on the effect of an attack. For example, a driver could be deceived by an attacker to decelerate. This attacker could be a person who just wants to mess with other drivers for fun, or a terrorist who tries to create traffic congestion before a bombing attack. The attack surface even enlarges with the existence of IoV. In that case, an attacker could compromise some vehicles and turn them into zombie vehicles, awaiting orders from a command and control (C&C) server.

It is also significant to note that the number of road traffic deaths worldwide was 1.25 million in 2013 [89]. Safety related applications in VANETs such as post-crash notification and road hazard notification are expected to lower that number in the near future. However, they require real-time network operations which also demand message encryption at the same time. Therefore, for safety-related applications, intrusion prevention has higher priority than intrusion detection. Nevertheless, in the case of a highly motivated attacker who specifically targeted those applications and already bypassed the existing prevention systems, intrusion detection must also be performed in real-time. Otherwise, there could be catastrophic consequences such as traffic accidents and delayed rescue operations. In this section, first an outline is provided on the proposed approaches from the intrusion/misbehavior detection perspective, then other proactive and reactive solutions that could be employed as countermeasures to attacks are discussed. Finally, open issues are presented as directions to be considered for future research.

Table 1 – Outline of the Proposed Approaches

#	Study	Infrastructure	Proposed Method	Reputation Mechanism	Response Mechanism	Attack(s) Covered
1	Golle et al. [29]	OBU-based (standalone)	Comparing received data to the model	No	Correction	Sybil Attack
2	Xiao et al. [30]	Hybrid	Signal strength analysis	No	-	Sybil Attack
3	Zhou et al. [33]	RSU-based	Hashing pseudonyms to common values	No	Revocation	Sybil Attack
4	Rahbari et al. [38]	RSU-based	Public key Infrastructure	No	Revocation	Sybil Attack
5	Yong Hao et al. [36]	OBU-based (cooperative)	Watchdog mechanism	Yes	Isolation	Sybil Attack
6	Lee et al. [37]	RSU-based	Session-key-based certificate	No	-	Sybil Attack
7	Chen et al. [41]	Hybrid	Observing similarity of motion trajectories	No	-	Sybil Attack
8	Park et al. [34]	Hybrid	Observing similarity of motion trajectories	No	-	Sybil Attack
9	Feng et al. [39]	Hybrid	Public key Infrastructure	Yes	-	Sybil Attack
10	Grover et al. [42]	OBU-based (cooperative)	Observing similarity of motion trajectories	No	-	Sybil Attack
11	Chang et al. [40]	Hybrid	Observing similarity of motion trajectories	No	-	Sybil Attack
12	Soryal et al. [43]	RSU-based	Markov Chain model	No	Isolation	DoS Attack
13	Verma et al. [44]	RSU-based	Monitoring outstanding SYN packets	No	-	DoS / Flooding Attack
14	Verma et al. [45]	RSU-based	Packet marking	No	Alarm	DoS Attack
15	Kerrache et al. [46]	OBU-based (cooperative)	Trust model using transmission thresholds	Yes	Isolation	DoS Attack
16	Hortelano et al. [48]	OBU-based (standalone)	Watchdog mechanism	No	-	Blackhole Attack
17	Daeinabi et al. [49]	Hybrid	Watchdog mechanism	Yes	Isolation	Blackhole Attack
18	Guo et al. [57]	Hybrid	Encounter tickets	Yes	Isolation	Blackhole Attack
19	Wahab et al. [52]	OBU-based (hierarchical)	Watchdog mechanism	Yes	Isolation	Blackhole Attack
20	Baiad et al. [54]	OBU-based (hierarchical)	Watchdog mechanism	Yes	-	Blackhole Attack
21	Yao et al. [62]	OBU-based (cooperative)	Trust model based on weights	Yes	Isolation	Blackhole Attack
22	Safi et al. [63]	OBU-based (standalone)	Packet leashes	No	-	Wormhole Attack
23	Kim et al. [65]	Hybrid	Message filtering model	Yes	-	Bogus Information Attack
24	Raya et al. [66]	OBU-based (cooperative)	Entropy and k-means clustering	No	Revocation	Bogus Information Attack
25	Ghosh et al. [67]	OBU-based (standalone)	Observing deviation of motion trajectories	No	-	Bogus Information Attack
26	Vora et al. [68]	RSU-based	Time Difference	No	-	Bogus Information Attack
27	Hubaux et al. [69]	RSU-based	Verifiable multilateration	No	-	Bogus Information Attack
28	Leinmüller et al. [23]	OBU-based (cooperative)	Trust model using sensors	Yes	-	Bogus Information Attack
29	Bissmeyer et al. [72]	OBU-based (cooperative)	Plausibility model vehicle movements	Yes	-	Bogus Information Attack
30	Ruj et al. [74]	Hybrid	Watchdog mechanism	No	Fine Imposition	Bogus Information Attack
31	Lo et al. [24]	OBU-based (standalone)	Plausibility validation network model	No	-	Illusion Attack
32	Studer et al. [75]	OBU-based (standalone)	Dead reckoning	No	-	GPS Spoofing
33	Adjih et al. [76]	OBU-based (standalone)	Timestamps	No	Packet Dropping	Replay Attack
34	Yan et al. [77]	OBU-based (cooperative)	Computing similarity among collected data	Yes	Isolation	Multiple Misbehaviors
35	Grover et al. [82]	Hybrid	Machine Learning	Yes	-	Multiple Misbehaviors
36	Kumar et al. [79]	OBU-based (cooperative)	Watchdog mechanism	Yes	-	Multiple Misbehaviors
37	Sedjelmaci et al. [80]	Hybrid	Watchdog mechanism, Machine Learning	Yes	-	Multiple Misbehaviors
38	Wahab et al. [81]	OBU-based (hierarchical)	Watchdog mechanism, Machine Learning	No	Isolation	Multiple Misbehaviors
39	Bouali et al. [84]	OBU-based (hierarchical)	Watchdog mechanism	Yes	Isolation	Multiple Misbehaviors
40	Zaidi et al. [88]	OBU-based (cooperative)	Statistical data analysis	No	Isolation	Multiple Misbehaviors
41	Kerrache et al. [85]	OBU-based (cooperative)	Trust model using watchdog mechanism	Yes	Isolation	Multiple Misbehaviors

4.1. Outline of Proposed Approaches

In this work, a compilation has been created of the attacks and detection mechanisms proposed in the literature. Table 1 outlines the proposed solutions. Most of the solutions in Table 1 are OBU-based only which means they do not need a dedicated infrastructure. Vehicles performing situation evaluation by themselves without any infrastructure makes the detection process faster through lowering the detection time. Furthermore, due to highly mobile vehicles moving in very large areas, if central administration mechanisms were to be employed in intrusion detection by deploying RSUs that cover large areas, this could create high cost overheads, especially in rural areas. Therefore, if cost is a primary concern, OBU-based only approaches would be preferable to RSU-based only or even hybrid approaches. However, cost is not the only consideration if confidentiality and non-repudiation are required in order to detect attacks. OBU-based approaches are divided into three sub-architectures as standalone, cooperative, and hierarchical. Most of the OBU-based solutions are collaborative even though there are few standalone mechanisms such as [48][63] in which each node detects attacks on its own. Hierarchical architecture is also distributed and cooperative in nature, differently it divides network into groups such as clusters, and gives more responsibility to some nodes such as cluster heads. This architecture is generally preferred for vehicular ad hoc networks using clustered routing protocols such as QoS-OLSR [55][56].

Similar to some attacks which are inherited from MANETs to VANETs, some detection mechanisms such as [68] can be inherited in the same way. Therefore, we presented the mechanisms not only for VANETs but also some other mechanisms which originally developed for MANETs that could be applicable to VANETs. However, inheritance from MANET to VANET does not always work well because of VANETs' special characteristics such as high mobility. On the other hand, enhancing a vehicular ad hoc network with infrastructure could help vehicles in the detection of attacks as opposed to MANETs that are lack of central points, but it is a costly approach due to deploying RSUs on a large scale. Furthermore, many solutions proposed for MANETs are specific to the routing protocols used. However, mainly protocol-independent solutions are proposed for intrusion detection in VANETs. Only some approaches [52][81] use a particular architecture built as a result of routing protocol for detection. Since solutions are mainly proposed for specific protocols in MANETs, specification-based detection, where the violations of the set of constraints of a protocol defined is detected as attacks, is one of the most commonly proposed techniques. On the other hand, to our knowledge there is no solution based on specification-based detection for VANETs, anomaly-based intrusion detection, where intrusions are detected as deviations from the normal behaviors, is generally employed in the solutions. In order to define what "normal" is, the existence of honest majority in the environment is generally assumed in detection. However, that assumption could become a disadvantage especially in case of a Sybil attack because an attacker can affect decision processes by using the Sybil nodes to constitute a majority. There are also few signature-based approaches [46], or hybrid approaches [72].

In general, solutions to detect the attacks can be reviewed as follows. The approaches on Sybil attack are generally based on similar motion trajectories, identity registration, PKI, signal strength and/or sensors such as radars. For DoS attack detection, packet marking and thresholds which are determined statically or dynamically are utilized. Additionally, response mechanisms are developed due to the nature of the attack. In order to detect a blackhole attack, redundant paths or watchdog mechanisms are utilized, while assuming the existence of honest majority for both. Redundant paths are also used for wormhole attack detection. When it comes to bogus information attack, the solutions mostly rely on sensors and/or challenge-response procedures such as distance bounding to estimate distances. Moreover, location and digitally signed timestamp information are also utilized in order to determine location difference. For the rest, the solutions mainly based on machine learning and watchdog mechanisms are employed in order to detect multiple misbehaviors. Although computational intelligence has many promising applications to intrusion detection [90], there were only a few applications to VANETs [81][82] found in the literature.

While some approaches have response mechanism to detected attacks, they are mainly passive responses such as raising alarms, or active attacks that seek control over the attacked system [91] such as isolation of nodes and dropping malicious packets. Therefore, not only detecting attacks, but also identifying attackers is important in order to properly respond to attacks.

The proposed solutions address different types of attack since they utilize various methods specific to the attack(s). In the future, more protocol/application-specific attacks might need investigation. Please note that this paper's analysis is based on attacks taken into consideration for the purpose of detecting, as found in the literature. It is the authors' belief that each of the proposed solutions is a valuable contribution towards securing VANETs. They are useful in order to build one or more layers of strong, standard security architecture for VANETs, which could become the largest network in the future. It is hoped that this study will also help VANET researchers and designers to develop more secure architecture in order to provide a better transportation experience.

4.2. Other Countermeasures: Trust and Privacy

PKI, one of the most popular technologies to prevent intrusions in today's networks, is offered in some solutions such as [38] to provide encryption and authentication in VANETs. Digital signature is also used to ensure integrity of the messages and non-repudiation. Since most of the attacks are performed in the network layer, PKI and/or digital signatures are also used for routing operations. However, utilizing PKI requires revoking digital certificates and distributing large CRLs (Certificate Revocation List) which is a hot topic and suffers from real-time constraints. Moreover, using digital certificates cause concerns about users' privacy because users want to protect their private information like license plate and position. This is a challenging task especially in detection of a Sybil attack because trusted certification is required in order to guarantee that each entity has only a single identity. As a result, there is a trade-off between privacy and non-repudiation. Apart from some solutions such as [33], most of the Sybil attack detection mechanisms ignore privacy.

Trust is another key concept in vehicular networks as in human relationships. The concept brings predicting the future to mind and it is built by gaining reputation which refers to knowledge of the past. Reputation and cryptography are complementary mechanisms since the former could be used to detect insider threats which could not be detected by the latter. Some of the proposed detection systems employ reputation mechanisms in order to predict vehicles' future actions based on their past behaviors. Therefore, vehicles that deviate from a system's expectations could be detected and isolated. After that, the network could rely more on other (trustworthy) vehicles to perform network operations. This is especially the case for blackhole attacks. Since the attacker exploits the trust of others by dropping the packets which are expected to be forwarded, reputation mechanisms are mostly used to detect this type of attack. For further information on trust management, the readers could refer to the brief survey provided in [92].

4.3. Open Issues

Considering its huge benefits to attacker(s) such as exploiting honest majority assumption and possible serious consequences to others, it is not surprising that Sybil attack is the most preferred attack addressed by researchers, as can be seen from Table 1. Nevertheless, drawing the line between privacy and non-repudiation is still needed in detecting a Sybil attack. Furthermore, while there are numerous works on Sybil attack, some other attacks such as illusion attack, motorway attack that are peculiar to VANETs require further research. How to detect attacks and attackers, especially cooperative attack(er)s also needs to be investigated. Distributed and cooperation intrusion detection architectures are more suited to the problem. Even though using RSUs could be a costly approach, their future deployment could increase security.

Some of the proposed attacks are performed on the routing layer where the routing protocols run were originally developed without security in mind. On the other hand, the proposed secure routing protocols require a high level of overhead and fail to address the demand for real-time operations and privacy at the same time. As a result, implementation of a routing protocol which takes security into consideration and could make the detection process faster while preserving privacy is an unsolved problem that could be subjected to further study. Nevertheless, monitoring/securing one layer might not be enough for intrusion detection. Even though most of the presented solutions focus on detecting misbehaviors at a specific layer, the problem requires cooperation between different layers. There were only few cross-layer solutions

[54][56] found in the literature. Therefore, a study that implements an intrusion detection approach which incorporates the protocol stack and makes different communication types such as V2V and V2I possible at the same time is missing.

After resolving the abovementioned problems in detection, having response mechanisms still remains as an important necessity for the solutions. It is especially critical for detecting a DoS or DDoS attack since it is almost impossible to respond to the attack once it has been performed. The response mechanisms mostly aim to isolate the attacker from the network as soon as possible. The isolation could be performed by dropping/denying messages from the attacker, revoking the attacker's certificate and/or avoiding sending messages to the attacker. However, not all the proposed solutions have response mechanisms. It is considered that response mechanisms require more attention and that researchers should work on adaptive response mechanisms in order to discourage malicious and/or selfish activities in the future.

Another area that requires focus is the lack of reliable links. Many detection techniques collect data from nearby entities in order to detect misbehavior(s) and suffer from a lack of reliable links between entities due to their high level of mobility. In addition, high vehicle density could cause some problems such as broadcast storms and disrupt the links in the network [93]. Therefore, making links more reliable could make detection mechanisms more effective. Developing an intrusion detection architecture which provides better detection rates by utilizing complementary technologies such as wireless communication and VLC (Visible Light Communication) [94] at the same time remains as yet an unstudied area.

As previously stated, although computational intelligence has many promising applications to intrusion detection [90], there were only a few applications to VANETs found in the literature. It is also shown that machine learning-based approaches have the potential to discover complex properties of MANETs [95][96]. The suitability of these techniques to intrusion detection in VANETs could be explored in future studies. Moreover, they could be used to adaptively determine thresholds, which is necessary for such highly dynamic environments. Since most of the studies found in the literature determine thresholds experimentally and do not evaluate it in other scenarios, it is considered an open research area.

5. CONCLUSION

Conventional security approaches which are suitable for wired networks or even some MANETs cannot be directly applied to VANETs due to their very characteristics. In this paper, the aim was to provide a holistic view to previous works on intrusion/misbehavior detection in VANETs. Firstly, a survey has presented an overview of the attacks, together with their possible effects along with working principals. The techniques used in the attacks showed that the attackers generally exploit network and application layers operations. Then a survey was presented of solutions using different detection mechanisms proposed in the literature. Each was given along with the attack(s) they can address, along with the advantages and disadvantages. Lastly, a survey of solutions was presented in Table 1 with respect to the methods used, infrastructure, intrusion detection architecture, reputation, and response mechanisms. As can be observed from Table 1, most of the solutions prefer using only OBUs instead of requiring a dedicated RSU infrastructure, and employ the watchdog mechanism. Many do not provide a response mechanism, and only cover few attacks. All solutions are discussed, and open issues outlined for future research. In conclusion, attack/misbehavior detection in VANETs is a complex and challenging topic and, protocol stack-wide and adaptive detection techniques, computational intelligence-based approaches are promising areas that could be explored in future studies as a means to make VANETs more secure.

REFERENCES

[1] J. Wan, J. Liu, Z. Shao, A. Vasilakos, M. Imran, and K. Zhou, “Mobile Crowd Sensing for Traffic Prediction in Internet of Vehicles,” Sensors, vol. 16, no. 1, p. 88, Jan. 2016.

[2] J. T. Isaac, S. Zeadally, and J. S. Cámara, “Security attacks and solutions for vehicular ad hoc networks,” *IET Communications*, vol. 4, no. 7, p. 894, 2010.

[3] S. Şen and J. A. Clark, “Intrusion Detection in Mobile Ad Hoc Networks,” in *Guide to Wireless Ad Hoc Networks*, S. Misra, I. Woungang, and S. Chandra Misra, Eds. London: Springer London, 2009, pp. 427–454.

[4] A. Kapadia, N. Triandopoulos, C. Cornelius, D. Peebles, and D. Kotz, “AnonySense: Opportunistic and Privacy-Preserving Context Collection,” in *Pervasive Computing*, vol. 5013, J. Indulska, D. J. Patterson, T. Rodden, and M. Ott, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 280–297.

[5] D. Antolino Rivas, J. M. Barceló-Ordinas, M. Guerrero Zapata, and J. D. Morillo-Pozo, “Security on VANETs: Privacy, misbehaving nodes, false information and secure data aggregation,” *Journal of Network and Computer Applications*, vol. 34, no. 6, pp. 1942–1955, Nov. 2011.

[6] “World Vehicle Population Tops 1 Billion Units,” 2011. [Online]. Available: http://wardsauto.com/news-analysis/world-vehicle-population-tops-1-billion-units. [Accessed: 08-Jan-2017].

[7] “Gartner Says By 2020, a Quarter Billion Connected Vehicles Will Enable New In-Vehicle Services and Automated Driving Capabilities.” [Online]. Available: http://www.gartner.com/newsroom/id/2970017. [Accessed: 08-Jan-2017].

[8] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, “VANET security surveys,” *Computer Communications*, vol. 44, pp. 1–13, May 2014.

[9] S. Marti, T. J. Giuli, K. Lai, and M. Baker, “Mitigating routing misbehavior in mobile ad hoc networks,” in *Proceedings of the 6th annual international conference on Mobile computing and networking*, 2000, pp. 255–265.

[10] B. Parno and A. Perrig, “Challenges in securing vehicular networks,” in *Workshop on hot topics in networks (HotNets-IV)*, 2005, pp. 1–6.

[11] F. Stajano and R. Anderson, “The Resurrecting Duckling: security issues for ubiquitous computing,” *Computer*, vol. 35, no. 4, p. supl22-supl26, Apr. 2002.

[12] “Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020.” [Online]. Available: http://www.gartner.com/newsroom/id/2636073. [Accessed: 08-Jan-2017].

[13] M. Gerla, E.-K. Lee, G. Pau, and U. Lee, “Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds,” in *2014 IEEE World Forum on Internet of Things (WF-IoT)*, 2014, pp. 241–246.

[14] O. Vermesan *et al.*, “Internet of things strategic research roadmap,” *O. Vermesan, P. Friess, P. Guillemin, S. Gusmeroli, H. Sundmaeker, A. Bassi, et al., Internet of Things: Global Technological and Societal Trends*, vol. 1, pp. 9–52, 2011.

[15] A. M. Vegni, M. Biagi, and R. Cusani, “Smart Vehicles, Technologies and Main Applications in Vehicular Ad hoc Networks,” in *Vehicular Technologies - Deployment and Applications*, InTech, 2013.

[16] I. A. Sumra, I. Ahmad, H. Hasbullah, and others, “Classes of attacks in VANET,” in *Electronics, Communications and Photonics Conference (SIECPC), 2011 Saudi International*, 2011, pp. 1–5.

[17] I. Aad, J.-P. Hubaux, and E. W. Knightly, “Denial of service resilience in ad hoc networks,” in *Proceedings of the 10th annual international conference on Mobile computing and networking*, 2004, pp. 202–215.

[18] A.-S. K. Pathan, Ed., in *Security of self-organizing networks: MANET, WSN, WMN, VANET*, Boca Raton, Fla.: CRC Press, Auerbach, 2011, p. 200.

[19] S. Biswas, J. Misic, and V. Misic, “DDoS attack on WAVE-enabled VANET through synchronization,” in *Global Communications Conference (GLOBECOM)*, 2012, pp. 1079–1084.

[20] V. Bibhu, R. Kumar, B. S. Kumar, and D. K. Singh, “Performance Analysis of black hole attack in VANET,” *International Journal Of Computer Network and Information Security*, vol. 4, no. 11, p. 47, 2012.

[21] Y.-C. Hu, A. Perrig, and D. B. Johnson, “Packet leashes: a defense against wormhole attacks in wireless networks,” in *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, 2003, vol. 3, pp. 1976–1986.

[22] T. Moore, M. Raya, J. Clulow, P. Papadimitratos, R. Anderson, and J.-P. Hubaux, “Fast exclusion of errant devices from vehicular networks,” in *2008 5th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, 2008, pp. 135–143.

[23] T. Leinmüller and E. Schoch, “Greedy routing in highway scenarios: The impact of position faking nodes,” in *Proceedings of Workshop On Intelligent Transportation (WIT 2006)(Mar. 2006)*, 2006.

[24] N.-W. Lo and H.-C. Tsai, “Illusion attack on VANET applications-A message plausibility problem,” in *Globecom Workshops, 2007 IEEE*, 2007, pp. 1–8.

[25] M. Raya and J.-P. Hubaux, “Securing vehicular ad hoc networks,” *Journal of Computer Security*, vol. 15, no. 1, pp. 39–68, 2007.

[26] M. Jakobsson, S. Wetzel, and B. Yener, “Stealth attacks on ad-hoc wireless networks,” in *Vehicular Technology Conference, 2003. VTC 2003-Fall. 2003 IEEE 58th*, 2003, vol. 3, pp. 2103–2111.

[27] P. Ning and K. Sun, “How to misuse AODV: a case study of insider attacks against mobile ad-hoc routing protocols,” *Ad Hoc Networks*, vol. 3, no. 6, pp. 795–819, 2005.

[28] J. R. Douceur, “The sybil attack,” in *International Workshop on Peer-to-Peer Systems*, 2002, pp. 251–260.

[29] P. Golle, D. Greene, and J. Staddon, “Detecting and correcting malicious data in VANETs,” in *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*, 2004, p. 29.

[30] B. Xiao, B. Yu, and C. Gao, “Detection and localization of sybil nodes in VANETs,” in *Proceedings of the 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks*, 2006, p. 1.

[31] B. Yu, C.-Z. Xu, and B. Xiao, “Detecting Sybil attacks in VANETs,” *Journal of Parallel and Distributed Computing*, vol. 73, no. 6, pp. 746–756, Jun. 2013.

[32] G. Guette and B. Ducourthial, “On the Sybil attack detection in VANET,” in *Mobile Adhoc and Sensor Systems*, 2007, pp. 1–6.

[33] T. Zhou, R. R. Choudhury, P. Ning, and K. Chakrabarty, “Privacy-preserving detection of sybil attacks in vehicular ad hoc networks,” in *Fourth Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services*, 2007, pp. 1–8.

[34] S. Park, B. Aslam, D. Turgut, and C. C. Zou, “Defense against sybil attack in vehicular ad hoc network based on roadside unit support,” in *MILCOM 2009-2009 IEEE Military Communications Conference*, 2009, pp. 1–7.

[35] T. Zhou, R. R. Choudhury, P. Ning, and K. Chakrabarty, “P2DAP-Sybil Attacks Detection in Vehicular Ad Hoc Networks,” *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 3, pp. 582–594, Mar. 2011.

[36] Y. Hao, J. Tang, and Y. Cheng, “Cooperative sybil attack detection for position based applications in privacy preserved VANETs,” in *Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE*, 2011, pp. 1–5.

[37] B. Lee, E. Jeong, and I. Jung, “A DTSA (Detection Technique against a Sybil Attack) Protocol Using SKC (Session Key Based Certificate) on VANET,” *Int. J. Security its Appl*, vol. 7, no. 3, pp. 1–10, 2013.

[38] M. Rahbari and M. A. J. Jamali, “Efficient detection of sybil attack based on cryptography in VANET,” *International Journal of Network Security & Its Applications (IJNSA)*, vol. 3, no. 6, 2011.

[39] X. Feng, C. Li, D. Chen, and J. Tang, “A method for defensing against multi-source Sybil attacks in VANET,” *Peer-to-Peer Networking and Applications*, vol. 10, no. 2, pp. 305–314, 2017.

[40] S. Chang, Y. Qi, H. Zhu, J. Zhao, and X. Shen, “Footprint: detecting Sybil attacks in urban vehicular networks,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 6, pp. 1103–1114, 2012.

[41] C. Chen, X. Wang, W. Han, and B. Zang, “A robust detection of the sybil attack in urban vanets,” in *29th IEEE International Conference on Distributed Computing Systems Workshops*, 2009, pp. 270–276.

[42] J. Grover, M. S. Gaur, V. Laxmi, and N. K. Prajapati, “A sybil attack detection approach using neighboring vehicles in VANET,” in *Proceedings of the 4th international conference on Security of information and networks*, 2011, pp. 151–158.

[43] J. Soryal and T. Saadawi, “DoS attack detection in Internet-connected vehicles,” in *2013 International Conference on Connected Vehicles and Expo (ICCVE)*, 2013, pp. 7–13.

[44] K. Verma, H. Hasbullah, and A. Kumar, “Prevention of DoS attacks in VANET,” *Wireless personal communications*, vol. 73, no. 1, pp. 95–126, 2013.

[45] K. Verma and H. Hasbullah, “Bloom-filter based IP-CHOCK detection scheme for denial of service attacks in VANET,” *Security and Communication Networks*, vol. 8, no. 5, pp. 864–878, 2015.

[46] C. A. Kerrache, N. Lagraa, C. T. Calafate, and A. Lakas, “TFDD: A trust-based framework for reliable data delivery and DoS defense in VANETs,” *Vehicular Communications*, Dec. 2016.

[47] J. Zhang, P. Porras, and J. Ullrich, “Highly Predictive Blacklisting,” in *Proceedings of the 17th Conference on Security Symposium*, Berkeley, CA, USA, 2008, pp. 107–122.

[48] J. Hortelano, J. C. Ruiz, and P. Manzoni, “Evaluating the usefulness of watchdogs for intrusion detection in vanets,” in *2010 IEEE International Conference on Communications Workshops*, 2010, pp. 1–5.

[49] A. Daeinabi and A. G. Rahbar, “Detection of malicious vehicles (DMV) through monitoring in Vehicular Ad-Hoc Networks,” *Multimedia tools and applications*, vol. 66, no. 2, pp. 325–338, 2013.

[50] M. Kadam and S. Limkar, “Performance Investigation of DMV (Detecting Malicious Vehicle) and D&PMV (Detection and Prevention of Misbehave/Malicious Vehicles): Future Road Map,” in *Proceedings of the International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA)*, 2013, pp. 379–387.

[51] U. Khan, S. Agrawal, and S. Silakari, “Detection of malicious nodes (dmn) in vehicular ad-hoc networks,” *Procedia Computer Science*, vol. 46, pp. 965–972, 2015.

[52] O. A. Wahab, H. Otrok, and A. Mourad, “A Dempster–Shafer Based Tit-for-Tat Strategy to Regulate the Cooperation in VANET Using QoS-OLSR Protocol,” *Wireless Personal Communications*, vol. 75, no. 3, pp. 1635–1667, 2014.

[53] O. A. Wahab, H. Otrok, and A. Mourad, “VANET QoS-OLSR: QoS-based clustering protocol for Vehicular Ad hoc Networks,” *Computer Communications*, vol. 36, no. 13, pp. 1422–1435, Jul. 2013.

[54] R. Baiad, H. Otrok, S. Muhaidat, and J. Bentahar, “Cooperative cross layer detection for blackhole attack in VANET-OLSR,” in *2014 International Wireless Communications and Mobile Computing Conference (IWCMC)*, 2014, pp. 863–868.

[55] H. Sanadiki, H. Otrok, A. Mourad, and J.-M. Robert, “Detecting attacks in QoS-OLSR protocol,” in *2013 9th International Wireless Communications and Mobile Computing Conference (IWCMC)*, 2013, pp. 1126–1131.

[56] R. Baiad, O. Alhussein, H. Otrok, and S. Muhaidat, “Novel cross layer detection schemes to detect blackhole attack against QoS-OLSR protocol in VANET,” *Vehicular Communications*, vol. 5, pp. 9–17, Jul. 2016.

[57] Y. Guo, S. Schildt, J. Morgenroth, and L. C. Wolf, “A Misbehavior Detection System for Vehicular Delay Tolerant Networks.,” in *INFORMATIK*, 2012, pp. 1871–1877.

[58] F. Li, J. Wu, and A. Srinivasan, “Thwarting blackhole attacks in disruption-tolerant networks using encounter tickets,” in *The 28th Conference on Computer Communications*, 2009, pp. 2428–2436.

[59] Y. Guo, S. Schildt, and L. Wolf, “Detecting blackhole and greyhole attacks in vehicular delay tolerant networks,” in *2013 Fifth International Conference on Communication Systems and Networks (COMSNETS)*, 2013, pp. 1–7.

[60] Y. Guo, S. Schildt, and L. Wolf, “Using Cluster Analysis to Detect Attackers in Vehicular Delay Tolerant Networks,” in *International Conference on Ad Hoc Networks*, 2013, pp. 181–196.

[61] P. Nagrath, S. Aneja, N. Gupta, and S. Madria, “Protocols for mitigating blackhole attacks in delay tolerant networks,” *Wireless Networks*, vol. 22, no. 1, pp. 235–246, 2016.

[62] X. Yao, X. Zhang, H. Ning, and P. Li, “Using trust model to ensure reliable data acquisition in VANETs,” *Ad Hoc Networks*, vol. 55, pp. 107–118, Feb. 2017.

[63] S. M. Safi, A. Movaghar, and M. Mohammadizadeh, “A novel approach for avoiding wormhole attacks in VANET,” in *2009 First Asian Himalayas International Conference on Internet*, 2009, pp. 1–6.

[64] S. Biswas and J. Misic, “A Cross-Layer Approach to Privacy-Preserving Authentication in WAVE-Enabled VANETs,” *IEEE Transactions on Vehicular Technology*, vol. 62, no. 5, pp. 2182–2192, Jun. 2013.

[65] T. H.-J. Kim *et al.*, “Vanet alert endorsement using multi-source filters,” in *Proceedings of the seventh ACM international workshop on VehiculAr InterNETworking*, 2010, pp. 51–60.

[66] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux, “Eviction of misbehaving and faulty nodes in vehicular networks,” *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 8, pp. 1557–1568, 2007.

[67] M. Ghosh, A. Varghese, A. Gupta, A. A. Kherani, and S. N. Muthaiah, “Detecting misbehaviors in VANET with integrated root-cause analysis,” *Ad Hoc Networks*, vol. 8, no. 7, pp. 778–790, Sep. 2010.

[68] A. Vora and M. Nesterenko, “Secure location verification using radio broadcast,” *IEEE Transactions on Dependable and Secure Computing*, vol. 3, no. 4, pp. 377–385, 2006.

[69] J.-P. Hubaux, S. Capkun, and J. Luo, “The security and privacy of smart vehicles,” *IEEE Security & Privacy Magazine*, vol. 2, no. LCA-ARTICLE-2004-007, pp. 49–55, 2004.

[70] S. Brands and D. Chaum, “Distance-bounding protocols,” in *Workshop on the Theory and Application of Cryptographic Techniques*, 1993, pp. 344–359.

[71] T. Leinmuller, E. Schoch, and F. Kargl, “Position verification approaches for vehicular ad hoc networks,” *IEEE Wireless Communications*, vol. 13, no. 5, pp. 16–21, 2006.

[72] N. Bismeyer, C. Stresing, and K. M. Bayarou, “Intrusion detection in VANETs through verification of vehicle movement data,” in *Vehicular Networking Conference (VNC), 2010 IEEE*, 2010, pp. 166–173.

[73] R. K. Schmidt, T. Leinmüller, E. Schoch, A. Held, and G. Schäfer, “Vehicle behavior analysis to enhance security in vanets,” in *Proceedings of the 4th IEEE Vehicle-to-Vehicle Communications Workshop (V2VCOM2008)*, 2008.

[74] S. Ruj, M. A. Cavenaghi, Z. Huang, A. Nayak, and I. Stojmenovic, “On data-centric misbehavior detection in VANETs,” in *Vehicular technology conference (VTC Fall), 2011 IEEE*, 2011, pp. 1–5.

[75] A. Studer, M. Luk, and A. Perrig, “Efficient mechanisms to provide convoy member and vehicle sequence authentication in VANETs,” in *Third International Conference on Security and Privacy in Communications Networks and the Workshops*, 2007, pp. 422–432.

[76] C. Adjih, D. Raffo, and P. Mühlethaler, “Attacks against OLSR: Distributed key management for security,” in *2nd OLSR Interop/Workshop, Palaiseau, France*, 2005.

[77] G. Yan, S. Olariu, and M. C. Weigle, “Providing VANET security through active position detection,” *Computer Communications*, vol. 31, no. 12, pp. 2883–2897, 2008.

[78] G. Yan, B. B. Bista, D. B. Rawat, and E. F. Shaner, “General active position detectors protect VANET security,” in *2011 International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA)*, 2011, pp. 11–17.

[79] N. Kumar and N. Chilamkurti, “Collaborative trust aware intelligent intrusion detection in VANETs,” *Computers & Electrical Engineering*, vol. 40, no. 6, pp. 1981–1996, 2014.

[80] H. Sedjelmaci and S. M. Senouci, “An accurate and efficient collaborative intrusion detection framework to secure vehicular networks,” *Computers & Electrical Engineering*, vol. 43, pp. 33–47, 2015.

[81] O. A. Wahab, A. Mourad, H. Otrok, and J. Bentahar, “CEAP: SVM-based intelligent detection model for clustered vehicular ad hoc networks,” *Expert Systems with Applications*, vol. 50, pp. 40–54, 2016.

[82] J. Grover, N. K. Prajapati, V. Laxmi, and M. S. Gaur, “Machine learning approach for multiple misbehavior detection in VANET,” in *International Conference on Advances in Computing and Communications*, 2011, pp. 644–653.

[83] J. Grover, V. Laxmi, and M. S. Gaur, “Misbehavior Detection Based on Ensemble Learning in VANET,” in *Advanced Computing, Networking and Security*, vol. 7135, P. S. Thilagam, A. R. Pais, K. Chandrasekaran, and N. Balakrishnan, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 602–611.

[84] T. Bouali, S.-M. Senouci, and H. Sedjelmaci, “A distributed detection and prevention scheme from malicious nodes in vehicular networks,” *International Journal of Communication Systems*, vol. 29, no. 10, pp. 1683–1704, 2016.

[85] C. A. Kerrache, N. Lagraa, C. T. Calafate, J.-C. Cano, and P. Manzoni, “T-VNets: A novel trust architecture for vehicular networks using the standardized messaging services of ETSI ITS,” *Computer Communications*, vol. 93, pp. 68–83, Nov. 2016.

[86] E. ETSI, “302 637-2 V1.3.1-Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service,” *ETSI, Sept*, 2014.

[87] E. ETSI, “302 637-3 V1.2.2 (2014-11) Intelligent Transport Systems (ITS),” *Vehicular Communications*.

[88] K. Zaidi, M. B. Milojevic, V. Rakocevic, A. Nallanathan, and M. Rajarajan, “Host-Based Intrusion Detection for VANETs: A Statistical Approach to Rogue Node Detection,” *IEEE Transactions on Vehicular Technology*, vol. 65, no. 8, pp. 6703–6714, Aug. 2016.

[89] “WHO | Number of road traffic deaths,” *WHO*. [Online]. Available: http://www.who.int/gho/road_safety/mortality/traffic_deaths_number/en/. [Accessed: 18-Jan-2017].

[90] S. X. Wu and W. Banzhaf, “The use of computational intelligence in intrusion detection systems: A review,” *Applied Soft Computing*, vol. 10, no. 1, pp. 1–35, 2010.

[91] S. Axelsson, “Intrusion detection systems: A survey and taxonomy,” Technical report, 2000.

[92] J. Zhang, “A Survey on Trust Management for VANETs,” in *2011 IEEE international conference on Advanced information networking and applications (AINA)*, 2011, pp. 105–112.

[93] Y. Ji, P. Yue, and Z. Cui, “VANET 2.0: Integrating Visible Light with Radio Frequency Communications for Safety Applications,” in *Cloud Computing and Security*, vol. 10040, X. Sun, A. Liu, H.-C. Chao, and E. Bertino, Eds. Cham: Springer International Publishing, 2016, pp. 105–116.

[94] A.-M. Cailean, B. Cagneau, L. Chassagne, V. Popa, and M. Dimian, “A survey on the usage of DSRC and VLC in communication-based vehicle safety applications,” in *2014 IEEE 21st Symposium on Communications and Vehicular Technology in the Benelux (SCVT)*, 2014, pp. 69–74.

[95] S. Sen, “A survey of intrusion detection systems using evolutionary computation,” in *Bio-Inspired Computation in Telecommunications*, 2015, Chapter 4, pp. 73–94.

[96] S. Pastrana, A. Mitrokotsa, A. Orfila, and P. Peris-Lopez, “Evaluation of classification algorithms for intrusion detection in MANETs,” *Knowledge-Based Systems*, vol. 36, pp. 217–225, 2012.