SECURITY ATTACKS AND SOLUTIONS IN VEHICULAR AD HOC NETWORKS: A SURVEY

Vinh Hoa LA, Ana CAVALLI

Department of Software and Networks
Telecom SudParis, 9 rue Charles Fourier 91011 EVRY, France.

ABSTRACT

Vehicular Ad hoc Networks (VANETs) have emerged recently as one of the most attractive topics for researchers and automotive industries due to their tremendous potential to improve traffic safety, efficiency and other added services. However, VANETs are themselves vulnerable against attacks that can directly lead to the corruption of networks and then possibly provoke big losses of time, money, and even lives. This paper presents a survey of VANETs attacks and solutions in carefully considering other similar works as well as updating new attacks and categorizing them into different classes.

KEYWORDS

Vehicular Ad hoc Networks (VANETs), Security, Privacy, VANETs Attacks.

1. INTRODUCTION

In the last few years, accompanying the massive deployment of wireless technologies and the growing number of wireless products on motorized vehicles including remote keyless entry devices, personal digital assistants (PDAs), laptops, and mobile telephones, automotive industries have opened a wide variety of possibilities for both drivers and their passengers. Vehicular Ad hoc Networks (VANETs) have attracted a lot of attention in research community because of their varied value added services, namely vehicle safety, automated toll payment, traffic management, enhanced navigation, location-based service for finding the closest fuel station, travel lodge or restaurant and simply access to the Internet [1], [5].

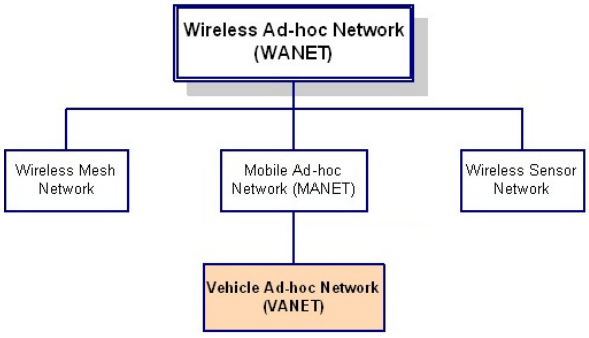

Fig. 1. Hierarchy of wireless ad hoc networks

However, many forms of attacks against VANETs have emerged recently and alarmed the unsettling situation of these networks' security. Being an implementation of Mobile Ad hoc

DOI : 10.5121/ijans.2014.4201

NETworks (MANETs) (Fig. 1), VANETs inherit all the discovered and undiscovered security and privacy vulnerabilities related to MANETs. Furthermore, VANETs have a number of distinctive properties [5] that could be also vulnerabilities for attackers to exploit. Those properties include the particular nature of communication in VANETs. Connections in a VANET in particular and in any Wireless Ad hoc Network in general are based on node-to-node communications: every node is able to act as either a host inquiring data or a router forwarding data. There are two types of nodes: (i) **RoadSide Units (RSUs)** standing for fixed nodes provisioned along the route and (ii) **OnBoard Unit (OBU)** referring to mobile nodes (i.e., vehicles) equipped with some sort of radio interface that enables connecting to other nodes in wireless manner**.** Fig. 2 depicts a general view of VANETs structure. It is worth mentioning that the speed of mobile nodes- vehicles in VANETs may be much higher than in MANETs. This reason makes VANETs very dynamic in nature. A number of nodes can communicate once as a group but can then rapidly change their own structure caused by leaving of a member or joining of another node. Therefore, it is expected that nodes are continuously "keeping in touch" with other nodes in the group to maintain the survival of the network. This aspect of VANETs seems to be very vulnerable and attacks can be unconsciously or intentionally performed to damage a part of or the total network. As mentioned above, VANETs provide many added applications that are safety, entertainment, or infotainment oriented. Attacks to VANETs may lead to catastrophic consequences such as the losses of lives in the case of traffic accident, losses of time (e.g., tampering traffic jam made by attacks) or financial losses (i.e., in payment services).

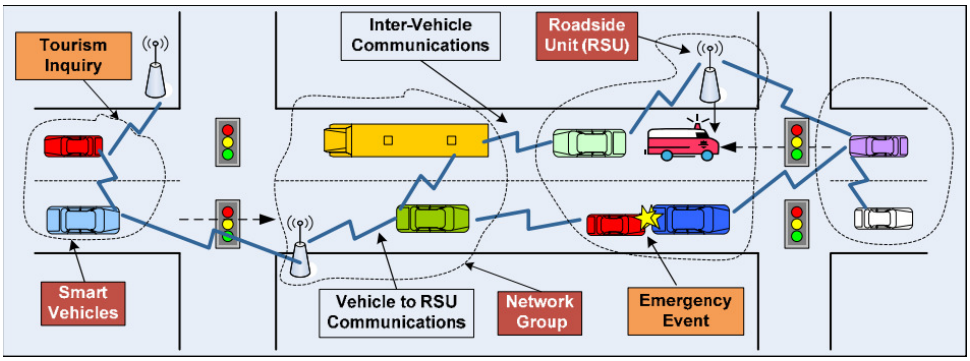

Fig. 2. A basic structure of VANETs [5]

The researches on VANETs security were triggered in the middle of 2000s and genuinely bloomed since 2007. In order to provide a thorough survey covering a big number of publications related to VANETs attacks, we searched for and collected papers approaching this topic from 2007 to 2013 that had made a significant contribution to the improvement of VANETs security. Fig. 3 indicated the numbers of publications each year that we found by searching on five main technical publishers, including IEEE explore, ACM Portal, Springer Online Library, Wiley Inter Science, and Elsevier Online Library, with either "VANETs security" "VANETs attacks" "VANETs vulnerabilities" keywords in title or abstract.

There has been many research works on the VANETs security in general and VANETs attacks in particular, especially the last three years from 2011 to 2013. However, there is a few survey works in the literature on VANETs attacks. In the existing surveys [2], [3], [6], some of attacks were not enough illustrated in detail and some were missed. Our paper aims to introduce more concisely the possible attacks, their mechanisms and influences as well as their corresponding solutions to thwart those attacks. We characterize the attacks (e.g., type of attacker, security aspects that are damaged) for a further classification. For each attack, we try to perform a concise scenario to better identify this attack. We equally point out the properties that can be collected to detect the attacks. These properties could be the input for an intrusion detector that

we consider as future work of our research. Our purpose in this study is to not only depict a detailed list containing up-to-date attacks but also a global view of security threats in VANETs, in order to provide a useful starting point for researchers interested in the subject and to help VANETs designers to develop and deploy secure VANETs infrastructures.

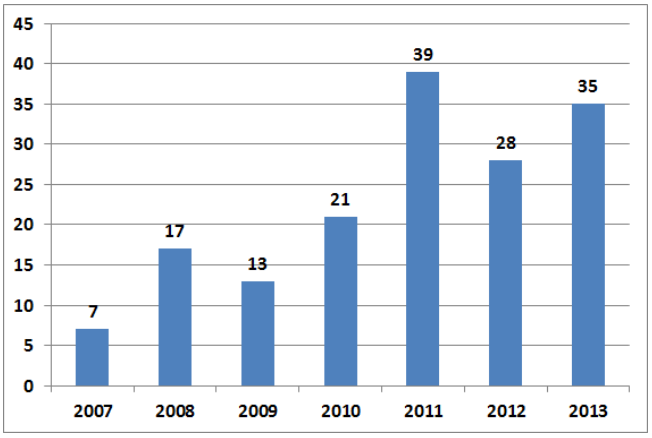

Fig. 3. VANETs security publications from 2007 to 2013

The rest of this paper is organized as follows: Section 2 presents some related works that are similar to our study. Section 3 is devoted to the VANETs security requirements. Section 4 contains the VANETs attacks and their corresponding solutions as well as examples. Section 5 summarizes the attacks that were mentioned in previous section, characterizes, and classifies them. Finally, we discuss about our study, conclude, and propose the future work in section 6.

2. RELATED WORK

In 2010, J.T. Isaac, S. Zeadally, and J.S. Camara published a paper on "Security attacks and solutions for vehicular ad hoc networks" [6]. They discussed some of the major security attacks that have been reported on VANETs before and in 2010. They presented also the corresponding security solutions that have been proposed to prevent those security attacks and vulnerabilities. The main security areas that they focused on include anonymity, key management, privacy, reputation, and location. *Anonymity* is a critical issue in VANETs concerning the physical identity of mobile nodes (i.e., vehicles) that should be kept secret in unauthorized components' point of view. *Key management* deals with problems on generating, distributing, and storing keys. For ad hoc networks, there are three main approaches for key management reported by literature, namely key exchange, key agreement, and key management infrastructure. *Privacy* refers to the ability of the drivers to protect sensitive information about them against unauthorized observers. *Reputation* of a member is usually evaluated by a particular one in answering the question "How much is this member trustable?" in a specific setting or domain of interest. Certainly, trustworthy behavior will be trusted and encouraged by reputation systems. In VANETs, the defense against compromised nodes, and malicious ones can be assured by applying such kinds of systems. *Location* refers to vehicle position in VANETs that can be considered as one of the most valuable pieces of information in geographic routing. It is often readily available through positioning services such as global positioning system (GPS).

In 2012, in the paper "Survey on Security Attacks in Vehicular Ad hoc Networks (VANETs)" [3], Mohammed Saeed Al-kahtani identified different security attacks, classified them, compared their defending mechanism in VANETs and suggested some future possibilities in this area. The author categorized three types of attacker as follows:

Insider vs. Outsider

If the attacker is a member node who can communicate with other members of the network, it will be known as an *Insider* and able to attack in various ways. Whereas, an o*utsider*, who is not authenticated to directly communicate with other members of the network, have a limited capacity to perform an attack (i.e., have less variety of attacks).

Malicious vs. Rational

A *malicious* attacker uses various methods to damage the member nodes and the network without looking for its personal benefit. On the contrary, a *rational* attacker expects its own benefit from the attacks. Thus, these attacks are more predictable and follow some patterns.

Active vs. Passive

An *active* attacker can generate new packets to damage the network whereas a *passive* attacker only eavesdrop the wireless channel but cannot generate new packets (i.e., less harmful).
In fact, there is another attribute to characterize an attacker, which is presented in [8]:

Local vs. Extended

An attacker is considered as local if it is limited in scope, even if it possesses several entities (e.g., vehicles or base stations). Otherwise, an extended attacker broadens its scope by controlling several entities that are scattered across the network. This distinction is especially important in wormhole attacks that we will describe later.

In 2013, Irshad Ahmed Sumra proposed five different classes of attacks [2] and every class is expected to provide better perspectives for the VANETs security (Table 1). This paper attempted to propose a classification and an identification of different attacks in VANETs.

Table 1: Proposed classification of attacks in [2]

Monitoring Attacks
Social Attacks
Timing Attacks
Application Attacks
Network Attacks

In first class- Network Attacks, attackers can directly affect other vehicles and infrastructure. These attacks are on the high level of danger because these affect the whole network. Whilst, in Application Attacks class, the objectives of attackers are applications that provide added service in VANETs. The attacker is mainly interested in changing contents used in applications and abusing it for their own benefits. The third class- Timing Attacks- is a type of attacks in which attackers' main objective is to add some time slot in original message, for example, to create delays in order to block this message come to the receiver before the expiration of its lifetime. All unmoral messages, which trigger bad emotions of other drivers, are classified into the class Social Attacks. Finally, attacks in which monitoring and tracking activities are performed are laying in the class Monitoring Attacks.

The related works above alert an alarming situation of VANETs security. In the next sections, we aim to emphasize security requirements in VANETs, then introduce more concisely the possible attacks, their corresponding countermeasures and propose another classification of these attacks.

3. VANETS SECURITY REQUIREMENTS

In this section, we present the main security requirements for VANETs [11], [12], [27], [37]. Three properties regarding security that cannot be ignored are confidentiality, integrity, and availability. In terms of VANETs security, these three properties stand for some more specific meaning.

Confidentiality

In VANETs, the definition of confidentiality refers to "**confidential communication**" [11]. In a group, none except group members are able to decrypt the messages that are broadcasted to every member of group; and none (even other members) except a dedicated receiver member is capable to decrypt the message devoted to it.

Integrity

It ensures that data or messages delivered among nodes are not altered by attackers. This concept in VANETs often combines with the concept "**authentication**" to guarantee that: A node should be able to verify that a message is indeed sent and signed by another node without being modified by anyone. In order to gain this property, Data Verification is also required: Once the sender vehicle is authenticated, the receiving vehicle performs data verifications to check whether the message contains the correct or corrupted data.

Availability

The network should be available even if it is under an attack without affecting its performance. This concept of VANETs is not different from itself in other kinds of networks but not easy to ensure because of the mobility in high speed of vehicles.

Besides three main security requirements above, the following security aspects should be also satisfied in VANETs:

Privacy

The profile or a driver's personal information must be maintained against unauthorized access. We consider the following two cases:

- Communications between vehicles and RSUs: Privacy means that an eavesdropper is impossible to decide whether two different messages come from the same vehicle.

- Communications between vehicles: Privacy means that determining whether two different valid messages coming from the same vehicle is intensely burdensome for everyone except a legitimate component (e.g., tracing manager [12]).

Identity privacy preserving is similar to the concept of **"Anonymity"**. That means identifying the physical identity of a message's originator should be computationally expensive.

Traceability and revocability

Although a vehicles real identity should be hidden from other vehicles, there should be still a component (e.g., Trace Manager) that has the ability to obtain vehicles' real identities and to revoke them from future usage.

Non-repudiation

Drivers must be reliably identified in case of accidents. A sender should have mandatory responsibility in transmitting the messages for the investigation that will determine the correct sequence and content of messages exchanged before the accident [8].

Real-time constraints

Since vehicles are able to randomly move in and quickly move out to a group of a VANET for a short duration, real-time constraints should be maintained.

Low Overhead

All messages in VANETs are time critical. Thus, “low overhead” is essential to retain the usefulness and validity of messages.

4. ATTACKS AND COUNTERMESURES IN VANETS

In this paper, only the attacks perpetrated against VANETs communication are taken into consideration. Physical problems (e.g., hardware tampering) are out of the scope of our research.

4.1. Sybil Attack

The Sybil attack is a well-known hurtful attack that was firstly described and formalized by Douceur [13] in the context of peer-to-peer networks. To perform this kind of attack, a vehicle declares to be several vehicles either at the same time or in succession. This attack is very dangerous since a vehicle can claim to be in different positions at the same time, thereby creating chaos and huge security risks in the network. The Sybil attack damages network topologies and connections as well as network bandwidth consumption. In Fig. 4, an attacker A transmits multiple messages with different identities to the other vehicles. Thus, other vehicles realize that there is currently a heavy traffic.

Fig. 4. Sybil attack

Traditionally in ad hoc networks, there are three types of defenses against Sybil attacks introduced, namely *registration, position verification,* and *radio resource testing* [16]. *Registration* itself is not enough to prevent Sybil attacks, because a malicious node has possibility to register with multiple identities by non-technical means such as stealing. Moreover, a strict registration may lead to serious privacy troubles. In *position verification* [26], the position of

nodes will be verified. The goal is to make certain that each physical node refers to one and only one identity. *Radio resource testing* [13], [14] is based on the assumption that all physical entities are limited in resources. The work done in [13] uses computational puzzles to test computational resources of each node. The general idea bases on the maximum capacity that an entity can solve multiple puzzles simultaneously. If an attacker impersonates different entities at the same time, it will have too many puzzles. It will be impossible to resolve and will be detected. However, this technique is not appropriate for VANETs since an attacker node can be equipped with more computational resources than an ordinary node. Thus, to eliminate this problem, the work done in [14] proposed another approach relying on the assumption that *"any physical device has only one radio"* and *"a radio is incapable of simultaneously sending or receiving on more than one channel"*. As a concrete example, in order to verify that none of the neighbors is Sybil identity, a node can assign each of its *n* neighbors a different channel on that it broadcasts some messages. Then it selects randomly a channel to listen. If its neighbor is legitimate, it will be able to get the response from the corresponding channel. Otherwise, that must be a Sybil node. The detection rate arises if this test is repeatedly processed.

However, the three aforementioned types of defenses are designed for indoor applications and they all rely on fixed base stations or specific hardware. They need an adaptation to be suitable for the highly mobile context of vehicular networks. The paper [16] proposed another solution rely on *detection and localization* of Sybil Nodes in VANETs. The motivation is to estimate a nodes position by analyzing its signal strength distribution between transmitted and received signals and then verify whether the estimated position is consistent with the claimed position. If they are too far from each other, this considered node is suspected as a Sybil attacker. The weakness of this approach is the fact that it is mostly based on several assumptions, which are not always realistic in practical VANETs.

In [36], the authors try to deal with the Sybil attack by *public key cryptography*. A Public Key Infrastructure for VANETs (VPKI) is proposed. The authors illustrate a complete solution to enhance communication security by addressing the key distribution and key revocation. The Sybil attack is always detected very early since each vehicle is authenticated correspondingly with its public key. Nonetheless, like any other cryptography-based approaches, the deployment of VPKI is a heavy and uncertain issue that must be tested to assess the possible utilization in reality.
Timestamp series [24] is another approach that relies on the prevention of Sybil attack and the protection of drivers' privacy. This approach works well for an initial development stage of VANETs with the availability of the RSU infrastructure. The main idea is the fact that two vehicles rarely pass through a few different RSUs far apart from each other at the same time. The RSU issues digital timestamps to each vehicle that passes through it. A traffic message sent out by any vehicle, thus, contains several timestamps corresponding to the previous passed RSUs. Therefore, if multiple traffic messages consist of very similar series of timestamps, they might be suspected as Sybil messages original from a single vehicle. This approach is economic since it does not use computational expensive public key infrastructure (PKI) or Internet accessible RSUs. Fig. 5 illustrates the working scenario of timestamp series approach.

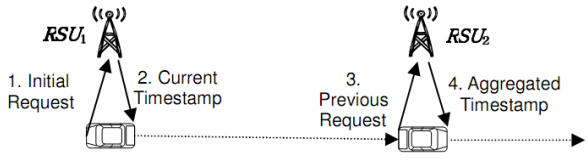

Fig. 5. Illustration of the timestamp series approach [24]

In [10], RobSAD (*Robust method of Sybil Attack Detection*) is proposed to detect Sybil attacks in the initial deployment stage of VANETs. The idea is based on the differences between the normal

and abnormal motion trajectories of legitimate vehicles and malicious vehicles respectively. Under normal conditions, people drive vehicles at their own chosen speed, selected path, and keep a reasonable safe distance from other vehicles. Therefore, physical nodes will have different motion trajectories and they can move separately. In contrast, Sybil nodes normally have the same motion trajectories all the time. The similarity of Sybil nodes motion trajectories is unrealistic and unacceptable in real world. RobSAD supposes that in VANETs, authorized infrastructures (i.e., RSUs) can provide vehicles digital signatures along with timestamp on-demand or periodically. Helped by RSUs, each node can record these signatures and use them to draw signature vectors of neighbors. Then it compares and measures the differences from the neighboring nodes signature vectors to detect Sybil nodes independently. Thus, this is a very effective, unique, and robust approach with higher detection rate and lower system requirements. This is because each node does not require collaborating with neighboring nodes but can detect attacks independently by comparing digital signatures. This approach uses infrastructure only to broadcast the digital signatures along with timestamp to other vehicular nodes.

The work done in [15] assesses the role of some assumptions on Sybil attack detection's success rate. In order to measure such a success rate, they evaluate the number of nodes that could be cheated from the sender's points of view and receiver's one. From the sender's point of view, they evaluate the impact of transmission power tuning. From the receiver's point of view, they characterize the impact of bi-directional antenna over omnidirectional antenna. To remain general, this assessment uniquely counts on reception signal strength and direction. Instead of using a propagation model to determine the precise location of a given node, they take into account a free space propagation model to compute the distance between transmitters and receivers. Their main purpose is to estimate the effects of assumptions and antennas in detecting Sybil attackers. Results demonstrate that Sybil attacks can be easily detected using bi-directional antennas in receiver's side. Thus, the usage of multiple antennas is significant in VANETs.

4.2. Bogus Information and Bush telegraph

The attacker performing Bogus Information attack can be outsider (intruder) or insider (legitimate user). The idea is to transmit incorrect or bogus information in the network for personal advantage. For instance, an attacker may transmit a message announcing "Heavy traffic conditions" to the others in order to make its movement easier on the road.

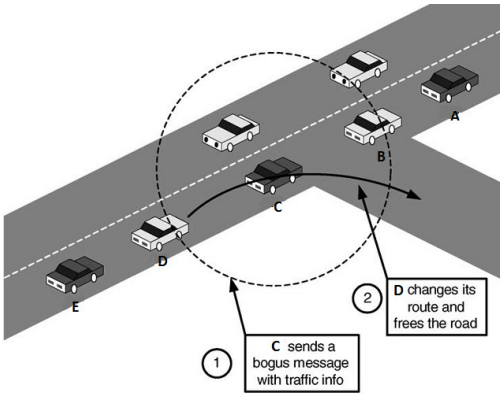

Fig. 6. Bogus information attack [8]

Fig. 6 demonstrates an example of bogus information attack, colluding attackers (A and C) disseminate false information to affect the decisions of other vehicles (D) and thus clear the way of attacker E.

Bush telegraph is a developed form of the bogus information attack. The difference in this case is that the attacker possesses multiple entities spread over several wireless hops. It is worth mentioning that after receiving a packet, a hop checks the error. If the error is small enough to be considered within tolerance margins, this error could be tolerated and ignored. Abusing this vulnerability, a bush telegraph attacker appends incremental errors to the data at each hop. At each hop, the error is probably small enough to be tolerated and hence accepted by the neighbor. After passing several hops, the overall accumulation of these errors eventually yields to bogus information.

ECDSA (Elliptic Curve Digital Signature Algorithm) [17] is named as one of the solutions for this kind of attacks. It is a message authentication scheme that uses hashing technique to keep messages more secured and provides strong authentication for the destination vehicles. Each vehicle consists of private key and public key. The public key is available to all vehicles in VANETs. Both the source and destination nodes are obligated to agree upon the elliptic curve domain parameters. ECDSA is actually a variant of DSA (Digital Signature Algorithm). The source vehicle hashes the message, encrypts it by using a secured hash algorithm and private key, and sends the message to the destination vehicle. At the destination, the message is decrypted using the public key, which is the hash of the message. This scheme is more secured on message authentications since hashing is a strong technique. Changes in messages will also change in the hash message, which makes it unique.

4.3. Impersonation Attack and Masquerade

In an ad hoc network, a node is free to move in and out. In VANETs, a host is uniquely identified by IP and MAC address. These measurements are not enough to authenticate senders. The attacker uses MAC and IP spoofing in order to get identity of other nodes and hide into the network. If there is no authentication process in order to make the network secure from malicious nodes, a malicious vehicle can send message on behalf of other vehicles to gain its own benefits or create chaos, traffic jam or accidents and hide itself [38]. It is achieved by using masquerade identity and messages fabrication, alteration and replay. For example, a malicious node may impersonate an ambulance to request others for priority lane or demand nearby RSUs to change traffic lights to green. Thus, the message from an OBU has to be integrity-checked and authenticated before it can be relied on. Furthermore, privacy is recently another important issue. A driver has the right to prevent the disclosure of its driving routes that someone can reach by tracing messages sent by its OBU. Therefore, an anonymous communications protocol is needed. While being anonymous, a vehicles real identity should be able to be revealed by a trusted party when necessary. For instance, the driver must be incapable to escape by using an anonymous identity after sending out fake messages and causing an accident. That is the reason why this kind of privacy is called conditional privacy. The work done in [19], [20] proposes a scheme, called SPECS (Secure and Privacy Enhancing Communications Schemes), to ensure the security and privacy issues of V2V (Vehicle-To-Vehicle) communications and detect the impersonation attacks. This approach is based on the idea of IBV (Identity-Based Batch Verification) Scheme [21], which suffers from impersonation attack and cannot fulfill privacy requirements. To protect the identity of each vehicle it uses pseudo-identity and a shared secret key m_i between a vehicle and RSU. The security scheme [3], [20] works as follows:

To authenticate a vehicle with a nearby RSU, the scheme uses Public Key Infrastructure (PKI) and assumes that there is a trusted authority (TA) constantly online and trusted. A secure fixed network is dedicated for communications between RSUs and TA. To avoid bottleneck, redundant TAs with identical functionalities and databases are installed. It is worth noting that TA is the only authorized component knowing the real identity of vehicles.

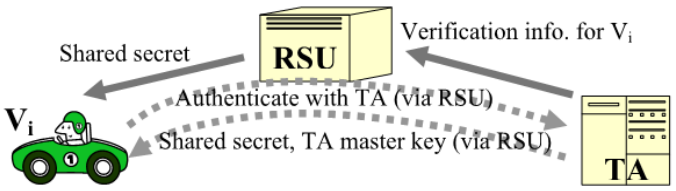

Fig. 7. Initial handshaking [20]

Fig. 7 illustrates an initial handshaking that is executed when a vehicle meets a new RSU. The vehicle authentication with the TA is performed via RSU. Then TA passes verification information to RSU. RSU then generates a shared secret key m_i with the vehicle. If this is the first time that the vehicle authenticates itself with the TA, TA will also pass its master key s and a shared secret m_i to the vehicle, via RSU of course. This only needs to be done once in the whole journey. For security reasons, s is not preloaded into any vehicle's hardware. Each time the vehicle passes a new RSU, a new shared-secret key is generated. To generate the signature, vehicle uses the shared secret key and hash function with the signing key. As m_i is only known by the vehicle, RSU and TA, attackers or other vehicles cannot generate the valid signing key to sign the message. RSU always verify the vehicle's signature even if the vehicle uses pseudo identity to sign the message. Invalid signatures can be detected using a batch verification process by RSU. In IBV (Identity-Based Batch Verification), if any invalid signature is found using the batch verification process the whole batch is dropped. However, SPECS does not drop the whole batch; it uses binary search, divides the batch in two halves, and checks the invalidity on each half. If an attacker is found, it notifies other vehicles and repeats the process until the search reaches a predefined level or all signatures are validated. After verifying the signature, the RSU broadcasts the message to all vehicles without the hash value, which is stored into positive and negative bloom filters. Any vehicle that wants to know the validity of a received message will create the hash value and compare with the bloom filters hash value. A message is valid if the hash value of this message is found in the positive bloom filter. Otherwise, the message is considered as invalid.

4.4. Timing Attack

Safety applications are one of the most important and promising advantages of VANETs. However, they are time critical applications and require data transmissions from one vehicle to another vehicle at the right time. In timing attacks [41], when malicious vehicles receive a message, they do not forward it as normal but add some timeslots to the original message to create delay. Thus, neighboring vehicles of the attackers receive the message after they actually require or after the moment when they should receive that message.

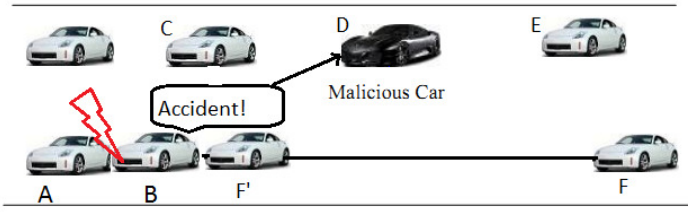

Fig. 8. Timing attack

In Fig. 8, there was an accident between two cars A and B. Malicious car D was announced about this accident but it delayed to transmit the message to the others by adding some timeslots to the

original message. F should receive this message soon to change the lane but because of the delay, it only received the message about accident when it has already reached the accident position (F'). There are also some other scenarios that are presented in [41] including both attacks to V2V communications and V2I communications.

In order to avoid timing attacks, data integrity verification is required to eliminate any timeslots that can be added to packets. TPM (*Trusted Platform Module*) [28] is one of the major security approaches to maintain the integrity of message by using the strong cryptographic functioning modules. Together with two protocols, namely Privacy Certification Authority (PCA) and Direct Anonymous Attestation (DAA), TPM has proved its two main advantages: (1) -Secure piece of hardware with cryptographic capabilities and (2) - Abilities to protect and store data in shielded location. TPM plays the role as a powerful solution for evenly other attacks that violate data integrity. However, like any other cryptographic solution, TPM can negatively affect to the performance of network.

4.5. Global Positioning System (GPS) Spoofing, Hidden vehicle and Tunnel Attack

In VANETs, a location table with the geographic locations and vehicles identities is a critical element that is maintained due to GPS satellite. Using the GPS satellite simulator to generate signals, that are stronger than those generated by the actual satellite system are, an attacker can produce false readings in the GPS to deceive vehicles to think that they are in a different location. **Hidden vehicle** is another concrete example of cheating with positioning information [8]. As Fig. 9 illustrates, the vehicle B deceives the vehicle A to believe that it is better placed (at B') for forwarding the warning message, but then keep silence about the accident.

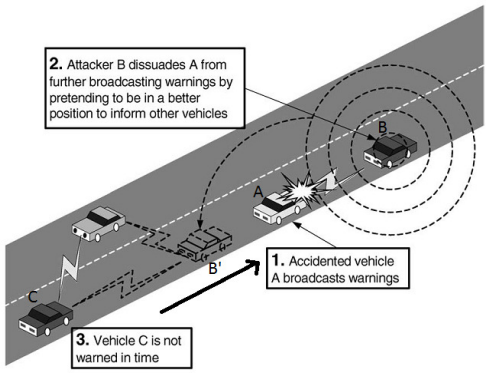

Fig. 9. Hidden vehicle attack [8]

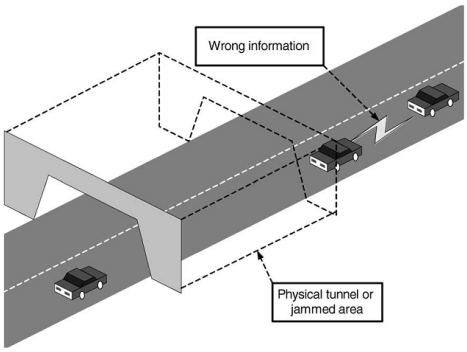

Fig. 10. Tunnel attack [8]

Another attack concerning position information is **Tunnel Attacks** [8]. Because of the temporary disappearance of GPS signals in tunnels, an attacker is possible to inject false positioning information once the vehicle leaves the tunnel and before it receives an authentic position update, as Fig. 10 illustrates. This phenomenon happens with either a physical tunnel or an area jammed by the attacker, that leads to the same effects.

In order to deal with problems from these kinds of attacks, one idea emerging is the work depicted in [16] that was earlier presented as a solution for Sybil attack. However, the ability of this approach's adaptation in VANETs is still a problematic issue.

4.6. Illusion Attack

In illusion attacks, the adversary deceives purposefully the sensors on his car to produce wrong sensor readings and thus incorrect traffic information. In consequence, the corresponding system reaction is invoked and then incorrect traffic warning messages are broadcasted to neighbors. Thus, illusion condition is successfully created. In general, drivers' behaviors will depend on the traffic warning messages they have received. Caused by illusions, vehicles received the wrong traffic information will most likely change their driving behaviors, correspondingly. Hence, the attacker can cause accident, traffic jam and decrease the performance by invisibly manipulating network topology of the network.

Traditional message authentication and message integrity verification cannot totally defend against illusion attacks because the adversary directly manipulates and confuses the sensors on a vehicle to report false information. *Plausibility Validation Network* (PVN) [23] is a security model to secure VANETs against illusion attacks. PVN processes by collecting raw sensors' data and verifying whether the collected data are plausible or not. Two types of inputs are taken into account: incoming data from antennas and data collected by sensors. An input data header will categorize the data. PVN has a rule database and data-checking module, which helps to check the validity of input data and take necessary action accordingly. A message is considered trustworthy if it passes all verifications. Otherwise, it is declared as an invalid message and dropped automatically. PVN has possibility of cooperation with various types of cryptography methods and defend against further attacks.

4.7. ID Disclosure

In this attack, a node in the network discloses the identity of neighbors, tracks the current location of a target node, and uses this data for a range of purposes (e.g., this is actually the way some car rental companies track their own cars). One of the most famous scenarios of ID Disclosure is as follow: A global observer sends a "virus" to some neighbors of the target node. Whenever attacked by the virus, these neighbors periodically report the ID and the locations of the target node. This attack violates the requirement concerning not only the authentication but also the privacy.

In [42], authors propose a *holistic protocol* for secure data transmission and detecting misbehaviors sent by the authorized users. In their proposed work, the vehicle should register with nearby Road Side Unit (RSU). In Registration phase, the user presents the user name and password to the RSU, then the RSU provides Registration ID to the user, which consists of license number and the vehicle registration number. Then RSU authenticates the vehicle by verifying the provided certificate. If the authentication is failed, the data/node will be blocked. This type of protocol is holistic protocol concerning the whole rather than the individual parts. It aim to provide authentication, integrity, availability, confidentiality, and non-repudiation

properties for VANETs, thus, detect and prevent misbehaviors (e.g., virus).The main advantages in holistic protocol for secure data transmission in VANET are the less time consumption and the security assured for both outsider and insider attacks.

4.8. Denial of Service (DoS) and Distributed Denial of Service (DDos)

Denial of Service (DoS) [2], [3], [25], [34] is always one of the most serious level attacks in every network. The scenarios to perform are very diverse. The main aim is to prevent the authentic users to access the network services. In DoS attacks, attackers may transmit dummy messages to jam the channel and thus, reduce the efficiency and performance of the network. A part of or the total network is no longer available to legitimate users. Fig. 11 indicates that a malicious black car forges a large number of fake identities and transmits a dummy message "Lane close ahead" to a legitimate car behind it and even to an RSU to create a jam in the network.

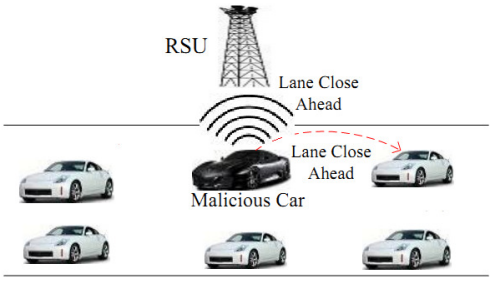

Fig. 11. Denial of Service (DoS) attack

The Distributed DoS (DDoS) is more severe than the DoS where a number of malicious cars attack on a legitimate car in a distributed manner from different locations and timeslots. Fig. 12 demonstrates that three malicious black cars attack on the car A from different locations and time so that A cannot communicate with the other vehicles.

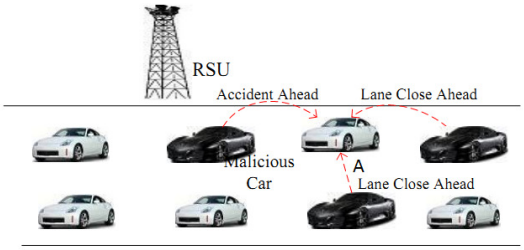

Fig. 12. Distributed Denial of Service (DDoS) Attack

One of DoS attack solutions is based on the support of OBU (OnBoard Unit) that is equipped in vehicles. There is a processing unit that has the role to suggest to the OBU to switch channel, technology, or to use frequency hopping technique or multiple transceiver in the case of DoS attack [34]. The work in [34] present a distributed and robust defense against DoS attacks where a malicious node forges a large number of fake identities, i.e., Internet Protocol (IP) addresses in order to disrupt the proper functioning of fair data transfer between two fast-moving vehicles. In the proposed approach, these fake identities are analyzed through the medium of the consistent existing IP address information. All the vehicles exchange frequently beacon packets to claim their presence and be aware of the neighbors. Each node periodically keeps and updates a record of its database by exchanging the information with the community. If a node detects in its record that there are some similar IP addresses, these identic IP addresses are likely evidences of a DoS attack. The authors developed a model for DoS prevention called *IP-CHOCK* that prove the significant strength in locating malicious nodes without the requirement of any secret information

exchange or special hardware support. Simulation results depict an encouraging detection rate that will be even enhanced whenever optimal numbers of nodes are forged by the attackers.

4.9. Black Hole Attack

A black hole [2], [3], [30], [38] is an area where the network traffic is redirected. However, either there is no node in that area or the nodes reside in that area refuse to participate in the network. In a black hole attack, a malicious node introduces itself for having the shortest path to the destination node and thus, cheats the routing protocol. Instead of taking a look on routing table firstly, this hostile node advertises rapidly that it has a fresh route for the route request. In consequence, attacker node wins the right of replying to the route request and thus it is able to intercept the data packet or retain it. When the forged route is successfully established, it depends on the malicious node whether to drop or forward the packets to wherever it wants.

Fig. 13 illustrates an example where the node A wants to send data packets to node F but does not know the route to F. Therefore, A initiates the route discovery process. As a malicious node, D claims that it has active route to F and pretends that it must be next-node if A wants to send packets to F. Depending on the routing protocol (e.g., Ad hoc On-demand Distance Vector (AODV) or Optimized Link State Routing (OLSR) [38]), an attacker builds its own method to fits in the data routes.

Gray Hole attack is known as a variation of Black Hole attack, in which the malicious node misleads the network by agreeing to forward the packets but it sometimes drops them for a while and then switches to its normal behavior. It is very difficult to figure out such kind of attack.

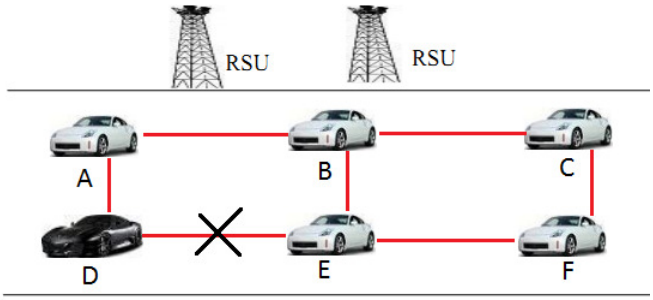

Fig. 13. Black hole attack

Existing solutions to black hole attacks [39] consider designing protocols in which there are more than one route from the source to the destination, or conceptualizing a Real-time Intrusion Detection system that adopts specification-based detection technique as well as processes countermeasures to reduce the damage. However, these solutions might be suitable to MANETs rather than VANETs, because MANETs have several mobile nodes and higher end-to-end delay to find additional nodes or paths. Another solution is to use packet sequence numbers in a packet header so that if any packet is lost, the destination can simply identify it from the missing packet sequence number.

4.10. Wormhole Attack

Wormhole [2], [22] is a severe attack in VANETs and other ad hoc networks that could be considered as a variation of Black Hole attack. In this attack, two or more malicious nodes create a tunnel to transmit data packets from one end to the malicious node at the other end and these

packets are broadcasted to the network. Owing to the nature of wireless transmission, a malicious node is capable creating a wormhole even for packets not addressed to it, simply by overhearing them in wireless environment and then tunneling them to the colluding node at the other end of the wormhole. The wormhole allows the attacker getting a very dominant role in comparison to other nodes, and it can exploit this position in a variety of ways, for example, to gain unauthorized access, disrupt routing, or perform a Denial of Service (DoS) attack, thus, threaten the security of transmitting data packets.

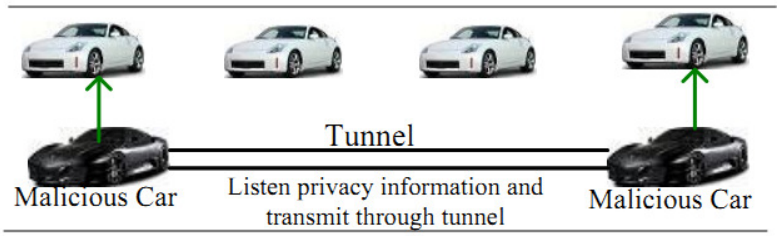

Fig. 14. Wormhole attack [2]

Wormhole attacks disrupt the multicast and broadcast operations for transmitting messages in VANETS, particularly in on-demand routing protocols such as AODV (Ad hoc On- demand authentication and protection mechanisms for routing packets and thus, is affected by wormhole attacks. The malicious nodes or wormholes can gain unauthorized access to perform Denial of Service (DoS) attacks. Fig. 14 illustrates a wormhole attack where black malicious cars at two end of the network form a tunnel to transmit confidential information.

Packet leash [22] is a well-known approach to prevent wormhole attacks. There are two types of leashes: geographic leashes and temporal leashes. In [22], they designed an efficient authentication protocol, called TIK, for use with temporal leashes. TIK (TESLA with Instant Key disclosure) is an extension of the TESLA broadcast authentication protocol. The purpose of temporal leashes is to ensure that each packet has an upper bound of distance to travel (which is at most limited by the speed of light). All nodes are tightly synchronized with a clock and the clock difference between any two nodes is known by all other nodes in the network. TIK protocol is found on efficient symmetric cryptographic primitives whereby a message authentication code is a symmetric cryptographic primitive. Accurate time synchronization between communicating parties is essential in TIK. It also requires each node to know a public value for each sender node, thus allows scalable key distribution. An attack is detected by calculating the differences between the packet travel distance and allowed distance to travel. If an attacker retransmits the packet by the wormhole, it will most likely delay it long enough so that the corresponding key has been no longer valid because the sender has disclosed it. The receiver, thus, will reject the packet.

An efficient approach called, *HEAP* [40], which is an improvement of previously proposed packet leashes method, used to detect the wormhole attacks in the AODV routing protocol of VANETs, which is more secure and has low overhead. Instead of using local leashes, the HEAP uses geographical leashes, which is more effective to detect malicious nodes. However, geographical leashes limit the packets travel distance. They only authorize packets, which travel less than a specific distance and thus, sometimes too severely prevent passing of packets that may be not affected by wormhole but travel farther than specific value. To eliminate this problem, HEAP assumes that although the distance passed by packets is more than the threshold, packets should not be dropped if process of packet traveling from source to destination is correct. HEAP method is very suitable for VANETs because it has a better performance compared to other authentication methods. HEAP is applicable for all unicast, multicast, and broadcast applications. We can also use HEAP as authenticator for all types of packets.

4.11. Malware and Spam

Malware and spam attacks, such as viruses and spam messages, can cause serious disruptions in the normal VANETs operations. This kind of attack is normally executed by malicious insiders rather than outsiders. For instance, an attacker sends a big amount of spam messages in the network to consume the bandwidth and to increase the transmission latency. It is not easy to control such kind of behavior because of the lack of necessary infrastructure and centralized administration. Meanwhile, malwares are just like viruses that hamper the normal operation of the network. VANET get infected normally when OnBoard Units (OBU) of vehicles and RoadSide Units (RSUs) perform software updates. Embedded anti-malware frameworks are still a problematic issue in VANETs research community.

4.12. Man in the Middle Attack (MiMA)

As the name suggests, in this attack, malicious vehicle listen to the communications between two vehicles, pretends to be each of them to reply the other and inject false information between vehicles. Fig. 15 demonstrates a Man in the Middle attack scenario, in which the malicious vehicle C is eavesdropping the communication between vehicles B and D as well as sending wrong information received from A to the vehicle E.

In order to deal with this kind of attacks, reasonable solutions are confidential communications (e.g., by powerful cryptography) to avoid the fact that an attacker can eavesdrop the communication among the others, and a secure authentication and data integrity verifications (e.g., by hash functions) to prevent messages modifications. Several specific solutions that assure these purposes have been presented in the previous parts.

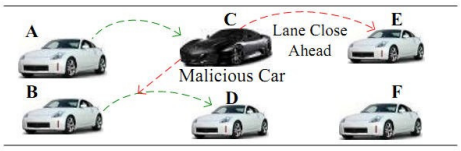

Fig. 15. Man in the middle attack [3]

5. SUMMARY OF ATTACKS' CHARACTERISTICS

In this section, we intend to characterize VANETs attacks by three attributes: (1) Type of attacker, (2) Violated Security Properties, (3) Class of attacks.

Table 2: Summary of VANETs security attacks

Attack	Type of attacker	Violated Security Properties	Class of attacks
Sybil	I.*.A.*	Authentication	NA
Bogus Info Bus telegraph	I.R.A.*	Integrity Authentication	AA
Impersonation Masquerade	*.*.A.L	Authentication	NA, MA
Timing	I.M.A.*	Integrity Authentication	TA
GPS Spoofing Hidden vehicle Tunnel	I.R.A.L I.M.A.L I.R.A.L	Authentication Authentication Authentication	NA, AA AA NA, AA
Illusion	I.R.A.L	Authentication	NA
ID Disclosure	I.R.A.L	Authentication Privacy	NA MA
DoS & DDoS	*.M.A.L	Availability	NA
Black Hole	I.M.A.L	Availability	NA
Wormhole	I.M.A.E	Availability	NA
Malware & Spam	I.M.A.*	Availability	NA
MiMA	*.*.A.L	Confidentiality Authentication	NA

5.1. Type of attacker

Inspired by [3], [8], we characterize an attacker by ***Membership. Motivation. Method. Scope*** where:

- ***Membership*** stands for Insider (I) or Outsider (O)
- ***Motivation*** for Malicious (M) or Rational (R)
- ***Method*** for Active (A) or Passive (P)
- **Scope** for Local (L) or Extended (E)
- A star (*) indicates that the corresponding field can take any value.

A more detailed explanation of this characteristic is presented in section 2. For example, an attacker I.R.A.L is an insider who behaves rationally, and performs active attacks in restricted areas.

5.2. Violated Security Properties

In section 3, we have reminded security requirements in VANETs. Caused by an attack, one or some requirements could not be satisfied. Therefore, for each attack, we point out what requirements are possibly not satisfied to evaluate the danger level of this attack as well as to warn designers in designing VANETs.

5.3. Class of attacks

We inherit the classification in [2] that characterizes attacks into five classes as illustrated in Table 1- Section 2.

5.4. Summary

Table 2 lists all attacks presented in section 4 with their corresponding three attributes.

6. CONCLUSION AND PERSPECTIVES

Risks caused by security attacks are one of the major security issues for the VANETs that are constraining the deployment of the vehicular ad hoc networks. In this paper, we presented an up-to-date collection of attacks damaging VANETs, sampled the practical scenarios, discussed the existing solutions to deal with attacks, and characterized each attack to have a thorough look over it. Our study is useful for VANETs researchers as a study on the state of the art and for designers in building the architecture or framework parameters of VANETs security. From this paper, we want to clear that: For the strong security of VANETs communication, we not only need the secured communication frameworks but also we need powerful routing algorithms those can facilitate the detection of malicious vehicles in networks and mitigate them.

Nowadays, in VANETs research community, many security solutions have been proposed to overcome security challenges caused by attacks [5], [25]. These solutions can be classified into three main approaches: Public Key Approaches, Symmetric and Hybrid Approaches and ID-based Cryptography. All of these approaches aim to construct a strong security framework for VANETs and thereby prevent security attacks. However, they will be carefully taken into consideration to adapt with particular features of VANETs. For example, a powerful cryptography is essential but it can provoke additional latencies in networks. This consequence is not encouraged in such a dynamic in topology network like VANETs that constantly wish for rapid communications.

In our perspectives, we intend to construct an intrusion detector for VANETs to alert the attacks in the case performing. This work can be done by applying the system of BRO [32] or MMT tools [33] in considering properties that is possibly collected in attacks.

REFERENCES

[1] Sherali Zeadally, Ray Hunt, Yuh-Shyan Chen, Angela Irwin, Aamir Hassan, “Vehicular Ad Hoc Networks (VANETs): Status, Results, and Challenges”, in Telecommunication Systems, Volume 50, Issue 4, pp 217-241, 2012.

[2] Irshad Ahmed Sumra, Iftikhar Ahmad, Halabi Hasbullah, Jamalul-lail bin Ab Manan, “Classes of attacks in VANET”, in Tenth International Conference on Wireless and Optical Communications Networks (WOCN), pp 1 - 5, 2013.

[3] Al-kahtani, Salman bin Abdulaziz, Al Kharj, “Survey on security attacks in Vehicular Ad hoc Networks (VANETs)”, in 6th International Conference on Signal Processing and Communication Systems (ICSPCS), pp 1 - 9, 2012.

[4] Kadam Megha V, “Security Analysis in VANETs: A Survey”, in International Journal of Engineering Research and Technology (IJERT), Vol. 1 Issue 8, October - 2012.

[5] Mahmoud Al-Qutayri, Chan Yeun and Faisal Al-Hawi, “Security and Privacy of Intelligent VANETs”, in Computational Intelligence and Modern Heuristics, book edited by Al-Dahoud Ali, 2010.

[6] J.T. Isaac, S. Zeadally, and J.S. Cmara, “Security attacks and solutions for vehicular ad hoc networks”, in IET Communications, pp. 894-903, 2009.

[7] Xiaodong Lin, Rongxing Lu, Chenxi Zhang, Haojin Zhu, Pin-Han Ho, and Xuemin (Sherman) Shen, “Security in Vehicular Ad Hoc Networks ”, in IEEE Communications Magazine , pp. 88-95, 2008.

[8] M. Raya, J. Pierre Hubaux, “Securing vehicular ad hoc Networks”, in Journal of Computer Security, vol.15, January 2007, pp. 39-68.

[9] I.Ahmed Soomro, H.B.Hasbullah, J.lb.Ab Manan, “Denial of Service (DOS) Attack and Its Possible Solutions in VANET”, in WASET, issue 65, 2010 ISSN 2070-3724.

[10] I.Chen Chen, Xin Wang, Weili Han, and Binyu Zang, "A Robust Detection of the Sybil Attack in Urban VANETs ", in Distributed Computing Systems Workshop, ICDCS Workshops '09. 29th IEEE International Conference, 2009, pp. 270-276, 2009.
[11] Chim Tat Wing, "Secure and Privacy-preserving Protocols for VANETs", in PhD thesis at The University of Hong Kong, August 2011.
[12] Lei Zhang, "Research on Security and Privacy in Vehicular Ad Hoc Networks", in PhD thesis at Universitat Rovira i Virgili, June 2010.
[13] J.Douceur, "The Sybil Attack", in First International Workshop on Peer-to-Peer Systems, 2002, pp. 251-260.
[14] J.Newsome, E.Shi, D.Song and A.Perrig, "Loc & Defenses", in International symposium on information processing in sensor networks, 2004, pp. 259-268.
[15] Gilles Guette, Bertrand Ducourthial, "On the Sybil attack detection in VANET ", in IEEE International Conference on Mobile Ad hoc and Sensor Systems, 2007, pp. 1-6.
[16] Bin Xiao, Bo Yu, Chuanshan Gao, "Detection and localization of Sybil nodes in VANETs", in DIWANS '06, pp. 1-8.
[17] S. S. Manvi, M. S. Kakkasageri, D. G. Adiga, "Message Authentication in Vehicular Ad hoc Networks: ECDSA Based Approach", in International Conference on Future Computer and Communication, 2009, pp. 16-20.
[18] Jinyuan Sun, Yuguang Fang, "A defense technique against misbehavior in VANETs based on threshold authentication", in Military Communications Conference MILCOM 2008. IEEE, 2008, pp. 1-7.
[19] Tat Wing Chim, S.M. Yiu, L.C.K. Hui and V.O.K Li, "Security and Privacy Issues for Inter-vehicle Communications in VANETs", in Sensor, Mesh and Ad Hoc Communications and Networks Workshops, 2009, pp. 1-3.
[20] T.W. Chima, S.M. Yiu, Lucas C.K. Hui, Victor O.K. Li, "SPECS: Secure and privacy enhancing communications schemes for VANETs", in Journal of Ad Hoc Networks 9, 2011, pp. 189-203.
[21] Chenxi Zhang, Rongxing Lu, Xiaodong Lin, Pin-Han Ho, and Xuemin (Sherman) Shen, "An Efficient Identity-Based Batch Verification Scheme for Vehicular Sensor Networks", in IEEE INFOCOM 2008 proceedings, 2008, pp. 816-824.
[22] Y.C. Hu, A. Perrig and D.B Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks", in INFOCOM. Twenty- Second Annual Joint Conferences of the IEEE Computer and Communications, 2003, pp. 1976-1986.
[23] Nai-Wei Lo, Hsiao-Chien Tsa, "Illusion Attack on VANET Applications - A Message Plausibility Problem", in Globecom Workshops, 2007, pp. 1-8.
[24] Soyoung Park, B. Aslam, D. Turgut and C.C. Zou, "Defense against Sybil attack in vehicular ad hoc network based on roadside unit support", in Military Communications Conference, MILCOM, 2009, pp. 1-7.
[25] B. Parno and A. Perrig, "Challenges in Securing Vehicular Networks", in Hot Topics in Networks (HotNets-IV), 2005.
[26] T. Leinmuller, E. Schoch, F. Kargl, C. Maihofer, "Improved security in Geographic ad hoc routing through autonomous Position Verification ", in ULM University, 2009.
[27] I.Ahmed Soomro, H.B.Hasbullah,J.lb.Ab Manan, "User requirements model for vehicular ad hoc network applications ", in International Symposium on Information Technology 2010 (ITSim 2010), 2010.
[28] G. Guett, C. Bryce, "Using TPMs to Secure Vehicular Ad-Hoc Networks (VANETs) ", in IFIP 2008, WISTP 2008, LNCS 5019, 2008, pp.106-116.
[29] Zhou L, Chao H-C, "Multimedia Traffic Security Architecture for the Internet of Things ", in IEEE Network 2011, 2011, pp. 29-33.
[30] Raja Mahmood RA, Khan AI, "A Survey on Detecting Black Hole Attack in AODV-based Mobile Ad Hoc Networks ", in International Symposium on High Capacity Optical Networks and Enabling Technologies, 2007, pp. 18-20.
[31] GMT Abdalla, SM Senouci, "Current Trends in Vehicular Ad Hoc Networks ", in Proceedings of UBIROADS workshop, 2007.
[32] Vern Paxson, "Bro: A System for Detecting Network Intruders in Real- Time", in Proceedings of the 7th USENIX Security Symthosium, San Antonio, Texas, 1998.
[33] Bachar Wehbi, Edgardo Montes de Oca, Michel Bourdelles, "Events- Based Security Monitoring Using MMT Tool ", in Software Testing, Verification, and Validation, 2008 International Conference, 2012, pp. 860-863.

[34] Karan Verma, Halabi Hasbullah, Ashok Kumar, "Prevention of DoS Attacks in VANET", in Wireless Personal Communications, November 2013, Volume 73, Issue 1, pp 95-126.
[35] Adil Mudasir Malla and Ravi Kant Sahu, "Security Attacks with an Effective Solution for DOS Attacks in VANET", in International Journal of Computer Applications, March 2013, Volume 66 - Number 22.
[36] M.Raya, P. Papadimitratos, and JP. Hubaux, "Securing Vehicular Communications", in IEEE Wireless Communications Magazine, Special Issue on Inter-Vehicular Communications, 2006, pp. 8-15.
[37] Ram Shringar Raw, Manish Kumar, Nanhay Singh, "Security issues and solutions in Vehicular Ad hoc Network: A review approach", in David C. Wyld (Eds) : ICCSEA, SPPR, CSIA, WimoA, 2013, pp. 339347.
[38] Vimal Bibhu, Kumar Roshan, Kumar Balwant Singh, Dhirendra Kumar Singh, "Performance Analysis of Black Hole Attack in Vanet ", in Computer Network and Information Security, 2012, pp. 47-54.
[39] R.A. Raja Mahmood, A.I. Khan, "A Survey on Detecting Black Hole Attack in AODV-based Mobile Ad Hoc Networks ", in International Symposium on High Capacity Optical Networks and Enabling Technologies, 2007, pp. 1-6.
[40] Seyed Mohammad Safi, Ali Movaghar, Misagh Mohammadizadeh, "A novel approach for avoiding wormhole attacks in VANET", in First Asian Himalayas International Conference on Internet, 2009, pp. 1-6.
[41] Irshad Ahmed Sumra , Jamalul-lail Ab Manan , Halabi Hasbullah, "Timing Attack in Vehicular Network", in Recent Researches in Computer Science, 2011, pp. 151-155.
[42] TamilSelvan, Komathy Subramanian, Rajeswari Rajendiran, "A Holistic Protocol for Secure Data Transmission in VANET ", in International Journal of Advanced Research in Computer and Communication Engineering, 2013, pp. 4840-4846.

ACKNOWLEDGEMENTS

Grateful acknowledgment is dedicated to Prof. Ana CAVALLI and doctoral student Khalifa TOUMI who contributed valuable comments in reviewing this paper.

AUTHORS

Vinh Hoa LA is currently a PhD student at Software-Networks Department in Telecom SudParis /Institut Mines-Telecom (France). He received an engineering degree in Information Technology, major: Information and Communication Systems in July 2012 in Hanoi University of Science and Technology in Vietnam. Benefiting the scholarship "Bourse Master Île de France", he has been in France since September 2012 for the second year of Master program in Informatics, specialized in Networks (Réseaux) at University Pierre and Marie Curie- Paris 6. He received the Master degree in September 2013. His research interests include Sensor/ Mobile Ad hoc Network Security, Security Validation, Intrusion Detection, Interoperability in Multi-Organization-Environment.

Ana Rosa Cavalli has obtained her Doctorat d'Etat es Mathematics Science and Informatics, from the University of Paris VII, in 1984. From 1985 to 1990, she was a researcher in the department Languages and Switch Systems, at CNET (Centre National d'Etudes des Telecommunications), where she worked on software engineering and formal methods. She is Full Professor at TELECOM & Management SudParis (ex Institut National des Telecommunications) since 1990. She is the director of the Software for Networks department. She is also responsible of the research team "Verification and test of services and protocols" and the AVERSE team, in the CNRS research laboratory SAMOVAR. Her research interests are on specification and verification, testing methodologies for conformance and interoperability testing, active testing and monitoring techniques, the validation of security properties and their application to services and protocols. She has published more than 120 papers in journals and international conferences of high quality.