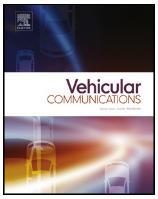
Contents lists available at ScienceDirect

Vehicular Communications

www.elsevier.com/locate/vehcom



Survey on VANET security challenges and possible cryptographic solutions

Mohamed Nidhal Mejri[a,*], Jalel Ben-Othman[a], Mohamed Hamdi[b]

[a] L2TI, Université Paris 13, Sorbone Paris cité, France
[b] Sup'Com, Université de Carthage, Tunisia

ARTICLE INFO

Article history:
Received 29 January 2014
Received in revised form 6 May 2014
Accepted 9 May 2014
Available online xxxx

Keywords:
Vehicular Ad hoc Networks (VANETs)
IEEE 802.11p
Security
Cryptography
Attacks

ABSTRACT

In the near future, it is expected that vehicles which increasingly become an intelligent systems will be equipped with radio communications interfaces. Thus, vehicular networks can be formed and they are commonly known as VANETs (Vehicular Ad hoc NETworks), a use case of mobile ad hoc networks where cars are the mobile nodes. As VANETs exhibit several unique features such as the high mobility of nodes, short connection times, etc. conventional security mechanisms are not always effective. Consequently, a wide variety of research contributions have been recently presented to cope with the intrinsic characteristics of vehicular communication. This paper provides a summary of the recent state of the art of VANETs, it presents the communication architecture of VANETs and outlines the privacy and security challenges that need to be overcome to make such networks safety usable in practice. It identifies all existing security problems in VANETs and classifies them from a cryptographic point of view. It regroups, studies and compares also the various cryptographic schemes that have been separately suggested for VANETs, evaluates the efficiency of proposed solutions and explores some future trends that will shape the research in cryptographic protocols for intelligent transportation systems.

1. Introduction

In recent years, the development of ITS (Intelligent Transportation System) [1] has made a big step. In addition to entertainment services on board, the main aim is to improve road safety and driving conditions. The automakers have realized the potential of the interconnection of their vehicles. To broaden the perception of recognition events that cannot be detected by traditional sensors or by the conductor, embedded sensors were introduced. Critical driving conditions can be detected and the information may be shared with nearby vehicles. To share this information, vehicles establish a spontaneous network, known as Vehicular Ad hoc NETworks (VANETs), using a direct mode of communication between vehicles called Inter-Vehicle Communications (IVC) [2]. Using this communication method, the vehicle can react by itself to avoid accidents by preventing other vehicles in its neighborhood in a transparent way to the driver. There are two types of communication in a VANET network [3]: V2V (Vehicle to Vehicle) where vehicles communicate directly and V2I (Vehicle to Infrastructure) which also refers in the literature as I2V communications where vehicles communicate directly with existing infrastructure, such as GSM, UMTS or WiMAX network via fixed equipment located on the road.

The architecture of vehicular ad hoc networks involves various hardware and software components. In a VANET network, vehicles are equipped with a unit called OBU (On Board Unit), mounted in the vehicle. On roads, units of infrastructure communication are called RSU (Road Side Unit) [4].

Besides the warning security applications and driver assistance, which form the essential purpose for which the VANET has emerged, there are applications for passenger comfort and online entertainment. Despite the facilities it offers, the wireless medium used in intelligent vehicular networks has some drawbacks that leave it vulnerable to different types of attacks that target this type of transmission medium, namely jamming, eavesdropping, interference, etc. [5]. In addition, and given the architecture of vehicular networks which involve almost the seven layers of the OSI reference model (Open System Interconnection), attacks and vulnerabilities exist almost at all levels, stretched from the physical to the application layer. Techniques and tools to deal with VANET security attacks are numerous. Among others, cryptography is one of the ways that solve, by some primitives, a lot of VANET systems security issues.

[*] Corresponding author.
E-mail addresses: mejri@univ-paris13.fr (M.N. Mejri), jalel.ben-othman@univ-paris13.fr (J. Ben-Othman), mmh@supcom.rnu.tn (M. Hamdi).

http://dx.doi.org/10.1016/j.vehcom.2014.05.001
2214-2096/© 2014 Published by Elsevier Inc.

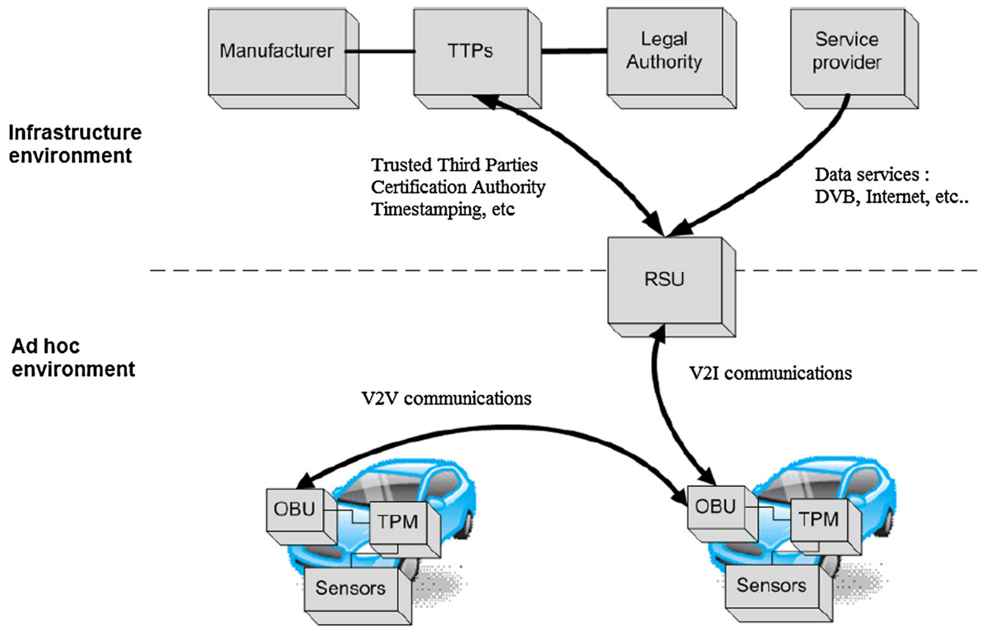


Fig. 1. VANET components (modified from [13]).

This paper is organized into seven sections. After the introduction, Section 2 is devoted to related work. In Section 3 we present the state of the art. Section 4 discusses challenges and security in VANETs. Section 5 presents cryptographic primitives and tools. Section 6 provided possible cryptographic solutions to the security challenges of VANETs already mentioned. Section 7 concludes the paper and gives direction to future work.

2. Related work

The major motivation that led us to carry out this work is to provide in the same paper a recent summary about VANET state of art and a study about VANETs security challenges and their possible related cryptographic solutions. Unlike other studies, our work includes and evaluates all recent existing cryptographic solutions that have been proposed separately for each problem. To the best of our knowledge, most research works on the VANETs security domain were either papers that address a specific problem or general surveys. There is no previous work that has focused all its studies on linking VANETs security issues with related cryptographic techniques which can entirely solve or reduce problems and their impact. However, some papers that are considered to be among the first works in the field have especially treated also some security issues. Among these papers, we quote [2], in which Blum and Eskandarian were interested in the problem of intentionally collusion that can be caused between smart vehicles. In [1,6] Maxim Raya et al. have been interested in the classification of attacks, the presentation of the attacker model, they presented also some attacks for the first time such as hidden vehicle, tunnel, wormhole, Bush Telegraph. In this paper they defined the requirements that must be respected to secure messages exchange in Vehicular networks. Group communications Security issues were also discussed.

In the survey papers [7,5,8] respectively of B. Mishra, A. Dhamgaye and S. Zeadally and their co-authors, they present the state of the art and review challenges and general proposals for VANETs security.

In papers [9,10] respectively of M.S. Al-Kahtani and Irshad Ahmed Sumra and their co-authors, some possible attacks against the security of a VANET network and their possible solutions are succinctly presented.

In [11], Maria Elsa Mathew et al. have presented a recent classification of VANETs attacks and a category set of their possible solutions. Also, A. Rawat et al. presented in [12] some attacks targeting VANETs and their related solutions.

In [13] Jose Maria d. Fuentes et al. glance some works which cover safety aspects of VANETs. The mentioned works study the security issues with a cryptographic primitives point of view without going into details or presenting solutions to mentioned problems.

Among the works in relation with the security of Vehicular networks, but focused on a specific issue, we quote: [14] of Bin Xiao et al. reserved for the detection and localization of Sybil attack in VANET nodes. P. Golle et al. [68] treat correcting malicious data entered in VANETs. Irshad Ahmed Sumra et al. [64] have been interested into "timing attacks". [15] of Seyed Mohammad Safi et al. focused into avoiding the wormhole attack. [16,17] and [18] respectively of S. RoselinMary, Li He and Adil Mudasir Malla and their co-authors have been dedicated to the DOS attack (denial of service) in a VANET environment. [19] of Sapna S. Kaushik, was reserved to privacy protection issues in VANETs. In [20], L. Gollan et al. were interested into the use of digital signatures as a means of authentication between cars.

Research in the field of VANETs is currently very active and varied as it touches on several axis at the same time, namely: wireless communications, protocols for physical and MAC layers, routing protocols and security. The following section will detail the state of the art and recent advances of all these aspects.

3. VANETs state of art

3.1. Overview

The large and rapid changes that know all the domains in the world not excluded the transport sector. Today, the fleet is growing, the roads are becoming more dangerous by the effect of congestion and increase the likelihood of collusion. According to the statistics of the National French Inter-ministerial Road Safety Observatory, published in 2013 annual report [21], there were 65,556 accidents (bodily injury) in 2012 against 65,024 in 2011. Therefore, securing traffic becomes not only a necessity but also an obligation. It is necessary to satisfy this requirement and others that ITS appeared. The Intelligent Transportation Systems aim to provide solutions

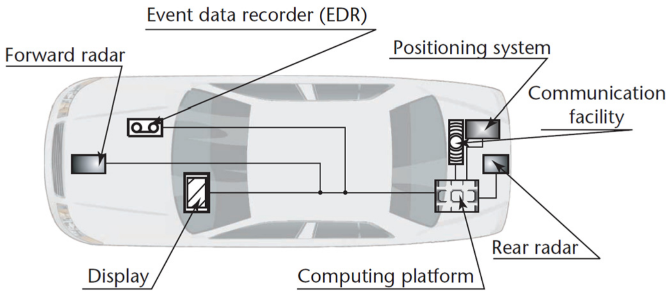


Fig. 2. Smart vehicle [22].

to road safety of passengers and the traffic congestion problems. They improved also comfort and driving conditions by integrating information technology in transport systems. We distinguish two possible types of communications:

1. Vehicle To Vehicle (V2V) are communications between vehicles in ad hoc mode [19]. In this mode, a vehicle can receive, transmit or exchange valuable traffic information such as traffic conditions and road accidents with other vehicles.
2. Vehicle To Infrastructure (V2I): used to broadcast between the network infrastructure and vehicles, and for the exchange of useful information about road conditions and safety measures to be taken into account [19]. In this mode, a vehicle establishes a connection with the RSU to connect and communicate with external networks such as the Internet. V2I links are less vulnerable to attacks and require more bandwidth than V2V links.

In ITS, a node can be a vehicle equipped with a radio system operating in the wireless short range, reserved for ad hoc network, it can be also a road equipment to communicate with mobile ad hoc nodes, and connect them to network infrastructure [8]. The integrated unit in the vehicle is named OBU (On Board Unit) and the roadside unit is named RSU (Road Side Unit). Fig. 1 describes the infrastructure and Ad hoc environments which form a simplified VANET network. The Ad hoc part is mainly composed of vehicles equipped with sensors, the OBU and TPM (Trusted Platform Module) [1], where the infrastructure part includes the manufacturer, the Third Units: TTP (Trusted Third Party), service providers on board and legal authorities. In the infrastructure part, the RSU acts as a bridge between ad hoc and infrastructure parts.

3.2. Smart vehicle

An intelligent vehicle as it was designed in [22], incorporates basically a set of sensors (front radar, reversing radar, etc.) that receive useful environmental information that generally the driver alone is unable to perceive. We find also a positioning system such as GPS (Global Positioning System) for example, which is essential for locating and driving assistance. A smart vehicle is obviously equipped with a communication system (can be multi-interface), a computing system, an event recording device which is a device whose functioning is similar to the black box of an aircraft.

Mainly, and for security measures, Hubaux et al. propose in [22] that a smart vehicle must be equipped with an ELP (Electronic License Plate) or with ECN (Electronic Chassis Number) which represent the electronic identity of the vehicle instead of the conventional identification by license plates. The ITS current terminology includes some features such as transceiving, display and interactivity with the driver in a single unit called OBU. Fig. 2 shows the different components that can be integrated in a smart vehicle.

Critical Safety of Life	SCH	SCH	Control Channel (CCH)	SCH	SCH	Hi-Power Public Safety
ch 172 5.860GHz	ch 174 5.870GHz	ch 176 5.880GHz	ch 178 5.890GHz	ch 180 5.900GHz	ch 182 5.910GHz	ch 184 5.920GHz

Fig. 3. DSRC in USA, 7 channels of 10 MHz.

SCH	SCH	SCH	SCH	CCH
ch 172 5.860GHz	ch 174 5.870GHz	ch 176 5.880GHz	ch 178 5.890GHz	ch 180 5.900GHz

Fig. 4. DSRC in Europe, 5 channels of 10 MHz.

3.3. VANETs standards

In addition to the facility of the production process, and the reduction of costs and the time to market, normalization and standardization in communications and information technology help also to ensure the interoperability and the rapid implementation of new technologies. For VANETs, standardization affects virtually all the different layers of the OSI (Open System Interconnection) model which is a communication system integrating all the features from the physical to the application layer. It should be noted that in the literature, often DSRC (Dedicated Short Range Communications) [23], WAVE (Wireless Access in Vehicular Environments) or even IEEE 802.11p [24] are used to designate the entire protocol stack of standards dealing with VANETs.

3.3.1. DSRC

For a maximum of interoperability and for the purpose of standardization of frequencies with which the VANETs work, the U.S. government represented by the FCC (Federal Communication Commission) attributed the band 5850 to 5925 GHz (75 MHz band wide). This band is known as Dedicated Short Range Communications (DSRC). The use of the DSRC band is not subject to a license, but rather to strict rules of use. According to [23], the DSRC band is divided into seven channels of 10 MHz, respectively numbered 178, 172, 174, 176, 180, 182, 184. The channel 178 is the CCH channel (Control CHannel). The other six are SCH channels (Service CHannels). Service channels 172 and 184 are respectively reserved to High Availability and Low Latency (HALL), and for high power and public safety (Fig. 3). In Europe the DSRC band is regulated by the ETSI (European Telecommunications Standards Institute) [25], and only the channels 180 of CCH and 172, 174, 176, 178 of SCH are used (Fig. 4).

3.3.2. WAVE

According to the latest ITS standards fact sheets of IEEE published in [26], the WAVE IEEE 1609 family (Standard for Wireless Access in Vehicular Environments) defines an architecture and a complementary set of standardized protocols, services and interfaces that allow all WAVE stations to operate in a VANET environment and establish Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) communications. The WAVE architecture defines also the security of exchanged messages. WAVE Standards form together the basis for the implementation of a wide set of applications in the transportation domain, they include vehicles safety, automatic tolls, improved navigation, traffic management and many other applications. The WAVE IEEE 1609 standards family is organized as follows:

IEEE P1609.0: This draft is the definition guide for the Architecture of Wireless Access in Vehicular Environments (WAVE). It defines how IEEE 1609 standards family work together and the necessary services for the multi-channel DSRC devices to be able to communicate in a high mobile environment.

IEEE P1609.1 (Resource Manager): This standard defines data flows and resources, it describes the basic components of the WAVE system architecture. It defines also the command messages and storage data formats. IEEE 1609.1 specifies also the device types that can be supported by the On Board Unit.

IEEE Std 1609.2 (Security Services for Applications and Management Messages) defines the processing method and the formats of secure messages used within WAVE and DSRC system. This standard describes some methods for securing WAVE application messages and management messages, It describes also the functions necessary to support security of messages and the anonymity and privacy of the vehicle.

IEEE Std 1609.3 (Networking Services): This standard describes services for the network and transport layers, these services include routing and addressing with the support of WAVE secure data exchange. It describes also the WAVE Short Messages (WSM) protocol. It provides an efficient alternative specific to WAVE architecture to directly support IP applications. In addition, IEEE 1609.3 standard defines the Management Information Base (MIB) for WAVE protocols family.

IEEE Std 1609.4 (Multi-Channel Operations): This standard is an enhancement to 802.11 MAC to be able to support WAVE. It describes wireless multi-channel radio operations which use the IEEE 802.11p protocol (medium access control and physical layers) for WAVE architecture. It specifies interval timers, priority access parameters, control channel and service channel operations. It defines also management services, channel routing and switching parameters.

Draft IEEE P1609.5 (Layer Management): This draft is under work, it will describe communication management services for Vehicle to Vehicle (V2V) and for Vehicle to Infrastructure (V2I) communications for the WAVE Environment.

Draft IEEE P1609.6 (Remote Management Services): This draft is under work too, it will provide the management of interoperable services. It includes a remote management and identification services for WAVE devices (OBU and RSU), using WAVE management services of IEEE Std 1609.3 and also identification services with the WSM (WAVE Short Message) protocol defined by IEEE Std 1609.3. Thus, it offers an additional middle layer between application and transport layer for more additional facilities.

IEEE Std 1609.11 (Over-the-Air Data Exchange Protocol for Intelligent Transportation Systems (ITS)): Defines services and secure messages required for the use of secure electronic payment formats.

IEEE Std 1609.12 (Provider Service Identifier Allocations (PSID)): This document specifies the identifier values that have been allocated for use by the WAVE systems.

The different standards of the 1609 WAVE architecture and their integration with the OSI reference model are summarized in Fig. 5.

3.3.3. IEEE 802.11p

In addition to the IEEE 1609 standards, IEEE has expanded its family of IEEE 802.11 protocols by adding 802.11p to accommodate vehicular networks, in accordance with the DSRC band. The definitions of the physical and medium access layers for VANETs are specified by the standard IEEE 802.11p-2010 [24], who adapted *PHY* and *MAC* layers of the IEEE 802.11-2007 [27] to be suitable for vehicular networks. IEEE 802.11p is specially based on the IEEE 802.11a for the definition of the *PHY* layer and on IEEE802.11e for the definition of the QoS [28].

IEEE 802.11p PHY: The IEEE 802.11p PHY is based on the OFDM (Orthogonal Frequency Division Multiplexing) with flow rates of 3, 4, 5, 6, 9, 12, 18, 24 and 27 Mbps, and a channel width of 10 MHz. Litters transmissions can reach 1000 m [29]. A WAVE equipment in a VANET switches between *CCH* and *SCH* channels 10 times per second (10 Hz).

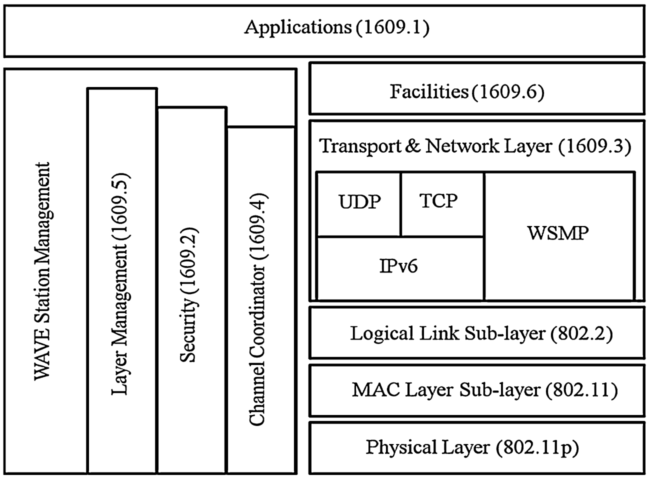

Applications (1609.1)
WAVE Station Management
Layer Management (1609.5)
Security (1609.2)
Channel Coordinator (1609.4)
Facilities (1609.6)
Transport & Network Layer (1609.3)
UDP
TCP
IPv6
WSMP
Logical Link Sub-layer (802.2)
MAC Layer Sub-layer (802.11)
Physical Layer (802.11p)

Fig. 5. WAVE architecture [23].

IEEE 802.11p MAC: The MAC layer of IEEE 802.11p uses EDCA (Enhanced Distributed Channel Access) which is an improvement of the former DCF (Distributed Coordination Function), used in most of the IEEE Std 802.11 standards [30]. To ensure more chance to safety messages so they can be transmitted within a reasonable time, the EDCA introduces the management of QoS concept through the notion of access categories (AC: Access category). IEEE 802.11p defines four access categories according to the type of traffic: Background traffic (AC0 or BK), Best Effort traffic (AC1 or BE), Video traffic (AC3 or VI) and Voice traffic (AC3 or VO). Access category AC3 is the highest (see Fig. 6).

CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) is the method used by EDCA to access the channel. In EDCA [28,4], with a simplified manner and without going into too much detail, if a node is ready to transmit, it senses the medium, if the later is free for an *AIFS* (Arbitration Inter-Frame Space) period, the node must defer transmission by selecting a random backoff time.

The backoff procedure of 802.11p EDCA works as follows:

1. The node selects a backoff value uniformly distributed in the interval $[0, \mathrm{CW}]$. The initial value of the Contention Window (CW), is $\mathrm{CW}_{\mathrm{min}}$,
2. The value of CW increases ($\mathit{Next\_Value} = 2 * \mathit{Actual\_Value} + 1$), if the sending attempt fails, until the CW reaches $\mathrm{CW}_{\mathrm{max}}$ value, the maximum number of retry attempts is fixed to 7,
3. The backoff value will be reduced when the channel is idle,
4. If the value of backoff reaches 0, the transmission is done immediately.

The waiting time $AIFS_K$ for an access category K is calculated as follows:

$$AIFS_K = SIFS + AIFSN_K * t_{slot}$$

where *SIFS* (Short Inter Frame Space) $= 32$ μs and t_{slot} (Time slot) $= 13$ μs for the IEEE 802.11p PHY layer with OFDM 10 MHz, as defined in [24].

Different *AIFSN* (Arbitration Inter-Frame Space Number) and CW values are selected for different types of access categories *ACs* and for each use case with the *CCH* and *SCH* channels. Table 1 presents all of these values, which are calculated from [31] data.

It should be noted that in the literature, and in several studies [28,32,4], there is a confusion about the value of $\mathrm{CW}_{\mathrm{max}}$. As based on the IEEE 802.11p and for the OFDM PHY layer with 10 MHz, the value of CW_{max} is 1023. While the IEEE 1609.4 specification

Please cite this article in press as: M.N. Mejri et al., Survey on VANET security challenges and possible cryptographic solutions, Veh. Commun. (2014), http://dx.doi.org/10.1016/j.vehcom.2014.05.001

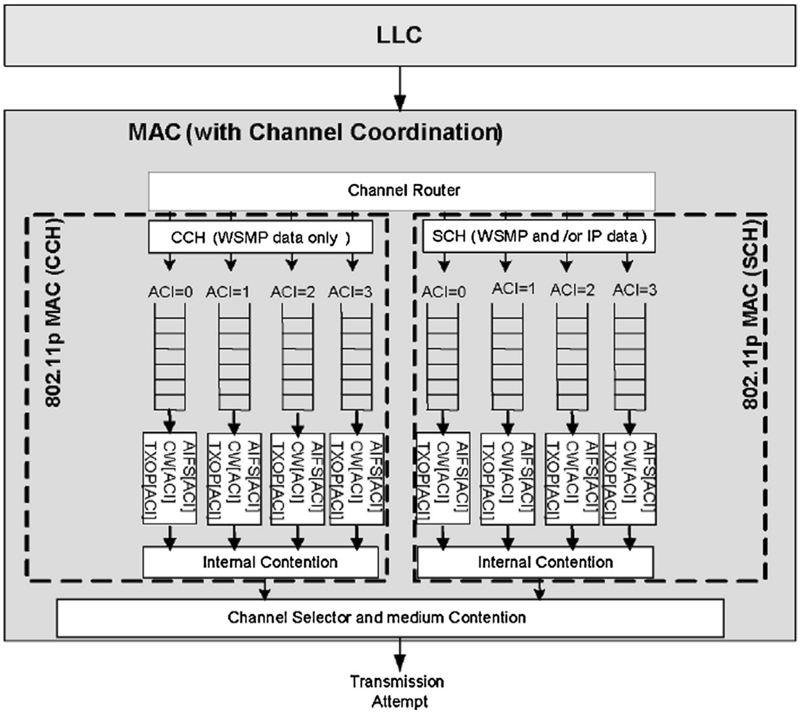


Fig. 6. Access categories in EDCA [24].

Table 1
EDCA parameters set used on CCH and SCH WAVE channels.

	SCH			CCH		
AC	CW_{min}	CW_{max}	*AIFSN*	CW_{min}	CW_{max}	*AIFSN*
BK	15	511	7	15	511	9
BE	15	511	3	7	15	6
VI	7	15	2	3	7	3
VO	3	7	2	3	7	2

standard [31] indicated (see Table 1) that the value of CW_{max} to use is 511.

3.4. Characteristics of VANETs

VANETs are a wireless networks where nodes are the fixed road units or the highly mobile vehicles. Nodes communicate with each other in ad hoc mode and communicate with fixed equipment on the roads in infrastructure mode. Thus, the characteristics of VANETs are basically a mixture of wireless medium characteristics and the characteristics of the different topologies in ad hoc and infrastructure modes. These characteristics are:

- *High mobility*: The high mobility of VANET nodes is one of the most important features. In normal operation of the network, nodes move all the time with different speeds and directions. According to [5,8], the high mobility of nodes reduces the mesh in the network (fewer routes between nodes). Compared to MANET, VANET mobility is relatively high. In the literature, Quite researches such as [33–36] have been specially devoted to study the impact of mobility factor in ad hoc networks and especially for vehicular networks.
- *Dynamic topology*: Given the high mobility, VANET topology is changing rapidly, it is therefore dynamic and unpredictable. The connection times are short especially between nodes moving in opposite directions. This topology facilitates the attack of the entire network, and makes difficult the detection of malfunction.
- *Frequent disconnections*: The dynamic topology and the high mobility of nodes as well as other conditions such as climate, the density of traffic cause frequent disconnections of vehicles from the network.
- *Availability of the transmission medium*: The air is the transmission medium of VANETs. Although the universal availability of this wireless transmission medium which is one of the great advantages in IVC, becomes the origin of some security issues, related to both the nature of transmission in wireless environment and to the security of communications using an open support.
- *Anonymity of the support*: Data transmission using a wireless medium is generally anonymous. If we leave aside the restrictions and regulations of use, anyone equipped with a transmitter operating in the same frequency band can transmit and hold the band [2].
- *Limited bandwidth*: The standardized DSRC band (5.850–5.925 GHz) for VANET can be considered as limited, the width of the entire band is only 75 MHz. Restrictions of use in some countries suggest that these 75 MHz are not all allowed. The maximum theoretical throughput is 27 Mbps.
- *Attenuations*: DSRC band has also transmission problems related to digital transmission with such frequencies, such as reflection, diffraction, dispersion, different types of fading, Doppler effect, losses and propagation delays due to multipath reflections.
- *Limited transmission power*: The transmission power is limited in the WAVE architecture, which limits the distance that data can reach. This distance is up to 1000 m. However, in certain specific cases such as emergency and public safety, it is allowed to transmit with a higher power [23].
- *Energy storage and computing*: Unlike other types of mobile networks, VANETs do not suffer from problems of energy, computing capacity or storage failure. However, real-time processing requirement of large amount of information is a challenge to keep in mind.

3.5. Routing protocols in VANETs

Routing protocols aim to ensure the selection of the best route for packets from source to destination in a timely manner [5]. The flow of data in a wireless environment, infrastructureless (especially V2V communications) and with high mobility is a difficult task to solve. In fact, routing is considered as one of the difficult problems of VANETs. According to [5], there are two main methods of routing in VANETs: hop by hop routing and source routing. Basically, all existing MANET's routing protocols can be optimized to be used for IVC [37,38], taking into account the specific characteristics of vehicular networks. VANETs routing protocols can be classified into the following six main categories [38,39]. For each category, some examples of VANETs routing protocols are given.

3.5.1. Topology based routing protocols

In this family we use information of the links (roads) to route packets. Protocols discover routes and prepare routing tables before sending packets. Generally, topology based protocols do not function properly for networks which exceed one hundred nodes [39]. In this family we distinguish 3 types of protocols:

- Proactive routing protocols: In these protocols, also called "table-driven", each node maintains one or more tables containing routing information for all destinations [40]. To keep routing tables updated, this class requires a periodic exchange of control packets between nodes.
- Reactive/on-demand routing protocols: In this family also known as "on-demand driven", the path computation is done only on request. Then the routing operation consists of two phases: the route discovery phase to route data and the updating phase executed when the network topology changes.
- Hybrid routing protocols: Hybrid protocols combine the mechanisms of proactive and reactive protocols. They use the technique of proactive protocols just for the neighbors discovery phase. For the rest of the nodes they act as reactive protocols.

Several "topology based protocols" exist in the literature, such as OLSR [41], TBRPF, FSR [38] and DSDV [42] as proactive protocols. DSR [41] and AODV [43] as reactive protocols. ZRP and HARP as hybrid protocols [38].

3.5.2. Position based geographic routing protocols

To select the next hop destination these protocols use data provided by positioning systems (e.g. GPS). So, no overall routes between sources and destinations must be created and updated [44]. In this category we find: VGPR, GPSR and MIBR [38].

3.5.3. Cluster based routing protocols

In this category, the neighbors vehicles form a cluster. Each cluster has a "cluster-head", which is responsible of management functions intra- and inter-cluster. The training of the cluster and cluster-head selection are critical required steps for the proper functioning of the network. For VANETs, and due to the "high mobility", cluster management is considered as a greedy process. In this category we find: CBLR, CBR, HCB and CBDRP [38].

3.5.4. Broadcast routing protocols

In this class of protocols, a flooding mechanism is used, where each node broadcasts messages to all its neighbors except the original sender. The flooding mechanism ensures that the message will reach every node in the network. This protocol category is suitable for a small number of mobiles. Its performance drops rapidly with the increase of the network size. "Broadcast Routing protocols" is a routing method frequently used in VANETs, to share the traffic, weather, emergency messages, information between vehicles, and to provide advertisements and announcements. In this category we cited: EAEP, DV-CAST and SRB [38].

3.5.5. Geocast routing protocols

The basic principle of these protocols is to send messages to all vehicles in a specific geographic area [45]. The use of these protocols is very useful in the case of informational VANETs applications, connected to a given region. Research in this area is booming. As examples of such routing protocols we cite: DTSG [46], ROVER and DTSG [38].

3.5.6. Infrastructure based routing protocols

The "Infrastructure based routing protocols" are protocols including routing mechanism based on methods designed primarily for infra-structured networks, and after they have been adapted to VANETs use case. This category refers RAR and SADV [38], which use a static network node as a relay.

3.6. VANETs projects

The main motivations for launching national or continental VANET projects are reaching a reasonable road safety and well manage the transport sector, while ensuring accidents reduction and minimizing the waiting times in traffic. Several research and industrial ITS projects are active throughout the world. VANET protocols research project, affect various international organizations such as IEEE, IETF, ETSI, ISO, SAE, ASTM. As already shown, the IEEE developed the WAVE protocol stack, containing the IEEE 1609 standards family and including an extension of the famous 802.11 for ITS applications. On the other hand, the IETF is working on extensions of IP (IPv6, Mobile IP) and auto-configuration for VANETs. ISO also develops CALM standard for vehicle networks. The C2C-CC (Car-to-Car consortium) [47] develop and test VANETs protocols. In Europe, ETSI is working on the adaptation of ISO, IETF standards essentially. Interoperability and integration of these projects are the subject of intense discussions and studies. Among VANETs industrial projects [6,48] we cite: VII, CICAS and IVBSS in the USA; CVIS, SafeSPOT, CARAVAN [49], COOPERS, PReVENT, GST, DRiVE, HIGHWAY, FleetNet, SeVeCom [47] and GeoNet in Europe; PREDIT in France; NoW in Allemagne; SmartWay and VIC in Japan; and ITSIndia in India.

Most of the mentioned projects include the integration of V2V and V2I communications [48]. For example, PReVENT helps the driver to avoid accidents or mitigate their impacts. GST (Global System for Telematics) focuses on the creation of an open standard for on-board telematic services. The CVIS (Cooperative Vehicle Infrastructure Systems) project focuses on road safety and integrates V2V and V2I communications. The DRiVE project (Dynamic Radio for IP Services in Vehicular Environments) focuses on the exclusive use of existing infrastructure for the implementation of the IVC system, it is the convergence of different cell technologies and high-speed UMTS networks, DVB-T and DAB develop innovative IP services to vehicles [50].

3.7. VANETs applications

ITS applications include basically applications for coordination of driving systems, cooperation for collision avoidance, notifications danger of the road. Comfort applications for travelers are also an innovative ITS applications category, they include the provision of mobile internet access, a variety of on-board services. VANET applications can be classified into Several family of classifications. These classifications range from two to several categories according to the degree of accuracy.

In [51], they classify applications into only two categories: Safety and Infotainment. In [1] VANET applications are also classified into Safety related applications and Other applications. In

[28] they extended the classification into: Road safety applications, Traffic efficiency applications, and Value added applications. In [48] the classification is according to the involved element: driver, vehicle, passenger and infrastructure. Thus, we distinguish four families of ITS applications:

- Driver-oriented applications: To help drivers make better use of the road if it receives information about the dangers ahead, traffic, etc..
- Vehicle-oriented applications: Allowing to provide information to their vehicles to increase automation and improve road safety.
- Passenger-oriented applications: For the comfort of the user with new on-board services (e.g. infotainment, Internet access).
- Infrastructure-oriented applications: In order to make better use of highway infrastructure.

In general, we conclude that most of the research papers in VANET are practically in agreement that the main applications dedicated for vehicular networks can be grouped into three categories:

1. *Applications for road safety*: In order to improve travel safety and reduce road accidents, VANET applications provide collision avoidance and road work, detection of mobile and fixed obstacles and dissemination of weather information. In this category of applications, we find e.g.: Slow/Stop Vehicle Advisor, Emergency Electronic Brake Light [7], Post Crash Notification, “Road Hazard Control Notification” Cooperate Collision Warning.
2. *Applications for driver assistance*: They aim to facilitate driving and assist the driver in specific situations such as overtaking vehicles, prevention of channel outputs, detection and warning of traffic congestion, warning of potential traffic jams, etc. In this category we find e.g.: Congested Road Notification, Parking availability notification, Toll booth collections [7].
3. *Applications of passengers comfort*: These applications are for the comfort of the driver and passengers, they essentially provide services such as mobile Internet access, messaging, discussion between vehicles, collaborative network games, etc. In the remainder of this section we limit ourselves to the description of some services and examples of applications of vehicle-to-vehicle communication systems.

Given their importance, it is absolutely essential to secure VANETs against all attacks that may occur. In the next sections we study the most existing VANETs security challenges and their possible cryptographic solutions.

4. VANETs security challenges

In their article “Threat of Intelligent Collisions” [2], Jeremy Blum and Azim Eskandarian ask an important question: “A wireless network of intelligent vehicles can make a highway travel safer and faster. But can hackers use the system to cause accidents?”. By this question they mark the importance that automakers must give to VANETs security. Safety in VANETs is crucial because it affects the life of people. It is essential e.g. that the vital information cannot be modified or deleted by an attacker. Securing VANETs systems must be able also to determine the responsibility of drivers while maintaining their privacy [8]. Communications passing through a vehicular network as well as information about the vehicles and their drivers must be secured and protected to ensure the smooth functioning of intelligent transportation systems [50].

The consequences of a security breach in VANETs are critical and dangerous. In addition, with a highly dynamic environment characterized by frequently instantaneous cars arrival and departure, and short periods connection durations, the deployment of a complete security solution is practically hard, it faces constraints and specific configurations. Although, the need for secure data transmission solutions in VANETs has been tipped as they appear, it is recently that this issue has aroused great interest and some solutions have been proposed.

In addition to the high mobility, the dynamic network topology and the use of wireless media which are the basis of the most important security breaches, other factors are also important, namely the diversity of the VANET involved entities.

4.1. Involved entities in VANETs security

From security point of view, the entities directly involved in the security of VANETs are:

1. *The driver*:
The driver is the most important element in the VANET safety chain because it is ubiquitous and he has to make vital decisions. In addition, all used cases currently scheduled for VANET applications make the driver as an interactive component with the driving assistance systems.
2. *The vehicle (OBU)*:
Although it does not reflect the reality, The OBU refers to the driver and the vehicle at the time in the literature. In a VANET network, we can distinguish two kind of vehicles: the normal vehicles that exist among network nodes and operate in a normal way, and the malicious vehicles.
3. *Road Side Unit (RSU)*:
As in the case of the OBU, we can distinguish normal RSU terminals, which operate in a normal way, and malicious RSU terminals.
4. *Third Parties*:
We denote by third parties (may be trusted or semi-trusted), all digital equivalents of stakeholders in a direct way in intelligent transportation system. Among these third parties, we quote: the regulator of transport, vehicle manufacturers, traffic police, and judges. They all have their respective secrets/public key pairs. These public keys can be integrated for example into the OBU which is supposed an inviolable device.
5. *The Attacker*:
In the context of VANET security, the attacker is one (or more) compromise entity that wants to violate successfully the security of honest vehicles by using several techniques to achieve his goal. An attacker can also be a group of vehicles that cooperate together. An attacker may be internal (an authentic vehicle of the VANET network) or an external vehicle. It can also be classified as rational (the attacker follows a rational strategy in which the cost of the attack should not be more than the expected benefit) or irrational (a suicide bomber is an example of irrational strategy) [1,52]. An attacker can be either active and made his attack with an exposed manner or passive and his actions cannot be detected.

4.2. Classification of VANETs attacks

Like any other communication and data processing systems, VANETs are exposed to various types of threats and attacks. The absence of the energy problem and the ability of an OBU to accommodate dozens of microprocessors give the vehicle an important capacity of processing and computing. Compared to a regular ad hoc network [8], this represents two significant benefits for

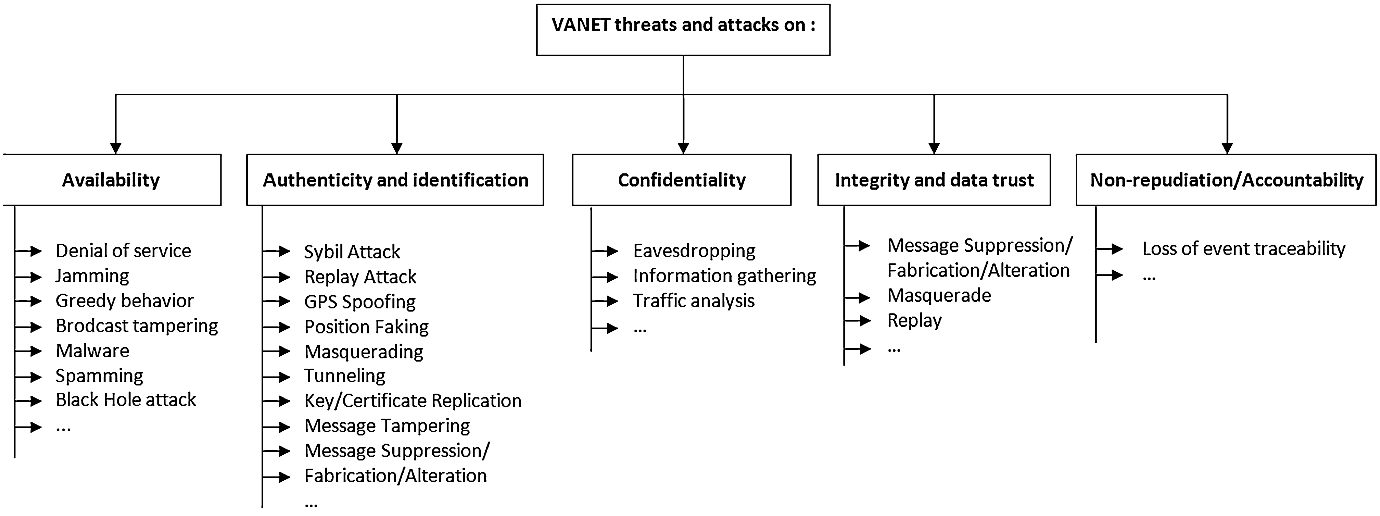


Fig. 7. Examples of VANET threats and attacks.

VANET nodes. Due to the high mobility in VANETs, the two mentioned advantages affect the feasibility of attacks. Thus, there are possible attacks in an ad hoc network that will be impossible for VANETs and vice versa.

Given the diversity of VANETs possible threats and attacks, and in the interests of clarity and simplification, it is necessary to classify them. Several classifications have been proposed in the literature [53,5]. In this paper we propose the use of a cryptographic related classification, which suite the better the presentation of the rest of our work: cryptographic solutions to VANETs security issues. This classification is as follows:

4.2.1. Attacks on availability

Availability is a very important factor for VANETs. It guarantees that the network is functional, and useful information is available at any functioning time. This critical security requirement for VANETs, which main purpose is to ensure the users' lives, is an important target for most of the attackers. Several attacks are in this category, the most famous are the Denial of Service attacks (DoS).

4.2.2. Attacks on authenticity and identification

Authenticity is a major challenge of VANETs security. All existing stations in the network must authenticate before accessing available services. Any violation or attack involving the process of identification or authentication exposes all the network to a serious consequences. Ensure authenticity in a vehicular network is to protect the authentic nodes from outside or inside attackers infiltrating the network using a falsified identity [8]. The importance of identification–authentication process comes from the fact that it is frequently used whenever a vehicle needs to join the network or a service. There are several types of attacks in this category.

4.2.3. Attacks on confidentiality

Confidentiality is an important security requirement for VANETs communications, it ensures that data are only read by authorized parties [5]. In the absence of a mechanism to ensure the confidentiality of the exchanged data between nodes in a vehicular network, exchanged messages are particularly vulnerable to attacks such as the improper collection of clear information [8]. In these cases, the attacker can gather information on the location of the vehicle and its routes, on users privacy, etc.

The information collected in the absence of a confidentiality mechanism may affect the privacy of individuals, knowing that it is difficult to detect this kind of attack, since it is virtually passive and user currently is not aware of the collection. However, in the case where the exchanged messages do not contain any sensitive information, Raya and Hubaux state in [1] that confidentiality is not necessary.

4.2.4. Attacks on integrity and data trust

The integrity of exchanged data in a system is to ensure that these data have not been altered in transit. Integrity mechanisms help therefore to protect information against modification, deletion or addition attacks. In the case of VANETs, this category targets mainly V2V communications compared to V2I communications because of their fragility. One of the possible techniques which facilitate this kind of attacks is the manipulation of in-vehicle sensors [13].

4.2.5. Attacks on non-repudiation/accountability

Non-repudiation in computer security means the ability to verify that the sender and the receiver are the entities who claim to have respectively sent or received the message [54]. Otherwise, the non-repudiation of data origin proves that data has been sent, non-repudiation of arrival proves that they were received. In a VANET context and since the manipulated data related to the safety and privacy of the users, it should be always possible to verify all hardware and software changes of security settings and applications (update, modification, addition, etc.) [55].

4.3. Examples of attacks

As it has been summarized in Fig. 7 and already mentioned in the previous paragraph, there are several varieties of possible attacks in a vehicular network. In the following sections, we detailed the most existing attacks and vulnerabilities, which were presented separately in [5,8,9,12,13,15,16]. The possible potential solutions from a cryptographic point of view will be presented later in this study.

4.3.1. Attacks on availability

- *Denial of Service attacks*: The Denial of Service (DoS) attacks actually include a family of attacks targeting the availability of network services, which can have serious consequences especially for VANETs applications. Because of their impacts, DOS attacks are classified as a dangerous class of attacks. They can be performed by internal or external malicious nodes to the network [8]. In these attacks, the attacker tries to block the principal means of communication and aims to interrupt services, so they will not be available to legitimate users [5]. As an example, flooding the control channel with high volumes of messages generated by intentionally manufacturing [16]. The network nodes (OBU and RSU) will not be able to handle the huge amount of received data. DDoS attack (Distributed Denial of Service) is a variant of DOS attacks [56], it is a distributed attack ordered by a main attacker who plays the role of "attack manager" with other agents who may be also victims unknowingly. The action methods of DDoS attacks are in most cases flooding the network and the results are always disastrous. Jamming, greedy behavior, blackhole attack, are examples of DOS attacks.

- *Jamming attack*: The jamming attack, is a physical level of Denial of Service attack. Jamming in its basic definition is the transmission of a signal to disrupt the communications channel, it is usually intentional [57]. This lowers the signal to noise ratio (SNR: Signal to Noise Ratio) for the receiver. Unintentional interference is called "interference" and occurs when a transmission is made in a frequency band that is already in use and operational.

  For a successful adaptive jamming attack, the jammer must act at the same time that the activity of the useful signal to jam. It must also choose the most effective signal transmission model that merges the best the receiver. In a VANET network, jamming once successful, can have inevitable consequences. Some research works such as [29,57] have looked for some techniques to reduce the effect of jamming for mobile ad hoc networks.
- *Greedy behavior attack*: The Greedy attack is an attack on the functionality of the MAC layer according to the architecture of the OSI model. The greedy node does not respect the channel access method and always tries to connect to the media. The main purpose is to prohibit other nodes to use the support and services. According to [58], a greedy behavior node tries also to minimize its waiting time for faster access to the channel and penalize other non-compromised nodes. Greedy behavior causes overload and collision problems on the transmission medium, which produces delays in authorized users services. Greedy behavior is independent and hidden to upper layers, then it cannot be detected by mechanism designed for those layers.
- *Blackhole attack*: The Blackhole attack is a conventional attack against the availability in ad hoc networks, it exists also for VANETs. In Blackhole attack, the malicious node receives packets from the network, but it refuses to participate in the operations of routing data. This disrupts the routing tables and prevents the arrival of vital data to recipients mainly because the malicious node always declares being part of the network and able to participate, which is not the case practically [8,9]. The effect of this type of attacks is more dangerous for VANETs than other mobile networks. A Blackhole node can e.g. redirect the traffic that receives to a specific node which does not exist in fact and this causes data loss [5]. Blackhole attack can also be used as a first phase of a man in the middle attack that we detailed later.
- *Grayhole attack*: This attack consists in removing only the data packets of certain applications that are vulnerable to packets loss [59]. GrayHole is considered as a Blackhole attack variant.
- *Sinkhole attack*: This attack consists that the malicious node attracts neighboring nodes so their packets go through it, this helps to eliminate or modify the received packets before retransmitting them eventually. The Sinkhole attack can be used to mount other attacks as Grayhole and Blackhole [60].
- *Wormhole attack*: Wormhole is a denial of service attack, it requires the participation of at least two nodes. It simply consists that an attacker A sends a message to an attacker B geographically far from him, that B broadcasts completely. This message suggests to neighboring nodes of B, that A is their neighbor [61]. This attack allows two or more legitimate nodes and non-neighbors (their radio transmission areas do not overlap) to exchange control packets between them [15], to create non-existent roads.
- *Malware attack*: Given the existence of a software components to operate the OBU and RSU, the possibility of infiltration of malware (malicious software) is possible in the network during the software update of VANET units [5,9]. The effect of a malware is similar to the effect of viruses and worms in an ordinary computer network, except that in a VANET network, disruption of normal functionality is always followed by serious consequences.
- *Broadcast tampering attack*: In this type of attack, the attacker tries to make and inject fake security alert messages in the network. This may hide the true safety messages to legitimate users, it can cause also accidents and seriously affect the overall network security [8]. In general this type of attack is possible for a legitimate node.
- *Spamming attack*: As in a web environment, the spam messages such as advertisements e.g. have no utility for users. In a VANET network which is a mobile radio environment, this type of attack aims to consume bandwidth and cause voluntary collisions. Given the lack of a centralized management of the transmission medium, this makes more difficult the control of such attacks [5,8].

4.3.2. Attacks on authenticity and identification

- *Sybil attack*: The idea of the sybil attack as presented for the first time in [62] is that a malicious entity can present multiple identities at once. One of the direct means by which two entities can convince a third that they are distinct is to run, at the same time, some tasks that one entity cannot do it alone. To ensure the identity of a node, several techniques have been proposed such as testing resources based on computational, storage and communication challenges. The Sybil attack is a dangerous attack in a VANET environment, given the disastrous consequences it can cause.
- *GPS spoofing/position faking attack*: In a VANET, the position information is of crucial importance, it must be accurate and authentic [5]. This attack consists on providing neighbors node a false location information. The exact location information can easily be obtained from a system such as GPS, whence the name of the attack: GPS spoofing. Each vehicle of a VANET is equipped with a positioning system (receiver), then the attack can be achieved using a transmitter generating localization signals stronger than those generated by the real satellites [9]. Successful GPS spoofing attack can facilitates other attacks such as attacks against applications which use the position of the node as an identification method.
- *Node impersonation attack*: Every vehicle has a network ID which allows to distinguish it among the other node of the VANET [9]. This identifier becomes especially important in case of problems. In the impersonation attack, the attacker obtains a valid ID and passes for another legitimate vehicle in the network. This constitute a violation of authentication process in the network.
- *Tunnelling attack*: The tunneling attack is almost similar to the wormhole attack [8]. In this attack, attackers use the same network to establish a private connection (tunnel), while in the Wormhole the attackers (assumed to be external) use a different radio channel for the exchange of packets. The Tunneling attack connects two distant parts of the vehicular network by using an additional communication channel such as a tunnel [12]. Thus, the victims of two distant parts of the network can communicate as neighbors.

- *Key and/or Certificate Replication attack*: The attack consists in the use of duplicate keys and or certificates which used as proof of identification and to create ambiguity which make more difficult to authorities to identify a vehicle, especially in the case of dispute.

4.3.3. *Attacks on confidentiality*

- *Eavesdropping attack*: In wireless networks such as VANETs, listening to the media is an attack easy to carry out. In addition, it is passive and the victim is not aware of the collection. Eavesdropping attack is against confidentiality, it is without imminent impact on the network [5]. Through this attack, several types of useful information can be collected such as location data that can be used for tracking vehicles.
- *Traffic analysis attack*: In a VANET, the traffic analysis attack is a passive serious threat against confidentiality and privacy of the users. The attacker analyzes collected information after a phase of listening to the network, it tries to extract the maximum of useful information for its own purposes.

4.3.4. *Attacks on integrity and data trust*

- *Masquerading attack*: In this attack, the attacker is hidden using a valid identity (called a mask), and tries to form a Blackhole or produce false messages that have the appearance of coming from an authentic node. For example, to slow down the speed of a vehicle or require it a lane change. A malicious node attempts to act as an emergency vehicle e.g. and thus cheat the other vehicles.
- *Replay attack*: This is a classic attack, it consists in replaying (broadcast) a message already sent to take the benefit of the message at the moment of its submission. Therefore, the attacker injects it again in the network packets previously received. This attack can be used e.g. to replay beacons frames [63], so the attacker can manipulate the location and the nodes routing tables. Unlike other attacks, replay attack can be performed by non-legitimate users.
- *Message Tampering/Suppression/Fabrication/Alteration*: As its name implies, this attack is against integrity it consists in modifying, deleting, constructing or altering existing data. It can occur by modifying a specific part of the message to be sent [12]. For example, the attacker falsifies received data indicating that the route is congested, and changes them to deceive users, so it indicates that there is no congestion and traffic on the road is normal. In this attack, the attacker can also delete a part of the message, alter or make new messages which help him achieving its intended purpose of the attack.
- *Illusion attack*: A direct application of the fabrication of messages attack is the Illusion attack, which is an attack against integrity and data trust. It consists in placing voluntarily sensors which generate false data [11]. These data can move normally in the network and require drivers interaction to make decisions. Authentication mechanisms are not able to detect this attack, because the attacker connects to the network in an authentic way.

Masquerading, replay, tampering, deleting, manufacturing, alteration, and illusion of messages can be also considered as attacks against the authenticity and identification.

4.3.5. *Attacks on non-repudiation and accountability*

- *Loss of events traceability*: Despite its importance, we have not seen any document that addresses this attack that we find quite feasible in a VANET environment. In fact, this non-repudiation attacks consists of taking action, allowing subsequently an attacker to deny having made one or more actions. This kind of attack is essentially based on the erasure of actions traces and creating confusion for the audit entity. Some attacks can serve as preliminary to non-repudiation attack such as Sybil attack and duplication of keys and certificates.

4.3.6. *Other attacks*

- *Attacks on privacy*: These attacks represent a major violation of privacy of drivers and VANET users. Several studies in the literature [19,5] classify the attacks of privacy as a separate category for VANETs. As a practical example we find:
  - Tracking: the pursuit of a vehicle during its journey.
  - Social Engineering: Known e.g. whether a vehicle at a definite moment is in the garage or in circulation.
- *Timing attack*: The timing attack is to delay the transmission of messages with high requirements on propagation delay, and transmit them e.g. after adding time preventing their treatment in a normal way. Some classifications such as in [64,9], consider also this category as a separate family of attacks.
- *Brute force attack*: The Brute force attack can be against the confidentiality of exchanged messages or the encryption keys. It can be also against the identification or authentication process. This attack can be performed e.g. while trying to find the network ID of the vehicle by dictionary researching process. In a VANET environment where connection times are relatively short, Brute force attack is not easy to conduct, since it is time consuming and resource intensive.
- *Man in the middle attack*: The man in the middle attack can be achieved in several contexts. As its name indicates, the attacker is inserted between the transmitter and the receiver. In the case of VANETs, the attacker is a vehicle which is inserted between two vehicles that communicate. The attacker controls the communication between the two victims [9], while they believe that they are in direct communication with each other. In the literature, the man in the middle attack is used to violate the authentication and or the integrity and non-repudiation mechanisms.

5. Cryptographic primitives and tools

5.1. *Cryptographic primitives*

We denote by cryptographic primitives, all the security services which cryptography provided. Modern cryptography offers several security techniques such as confidentiality, authentication, integrity, non-repudiation, secret sharing, etc. To satisfy these security services, cryptography uses methods such as encryption/decryption algorithms, Keys generation and exchange protocols, hash functions, digital signature and a lot of other techniques. In the following we mainly rely on the famous reference [69] of Bruce Schneier for the presentation of the different cryptographic primitives.

- *Confidentiality*: It is the first problem that has been posed to cryptography. Confidentiality is to ensure that messages can only be read by those who are authorized. In a VANET, the information exchanged is mostly public, except those related to the privacy of users.
- *Authentication*: It allows the receiver to verify the origin of the data, and if the issuer is the one who claims to be. A VANET user should not be able to pass for someone else. The digital signature is one of the most used solutions for authentication problems.
- *Integrity*: It means that the receiver is able to ensure that the received message is the message that has been issued and it has not been altered in transit. An attacker should not be able to modify messages. One way hash functions form the basis solutions set for integrity problems. It should be noted

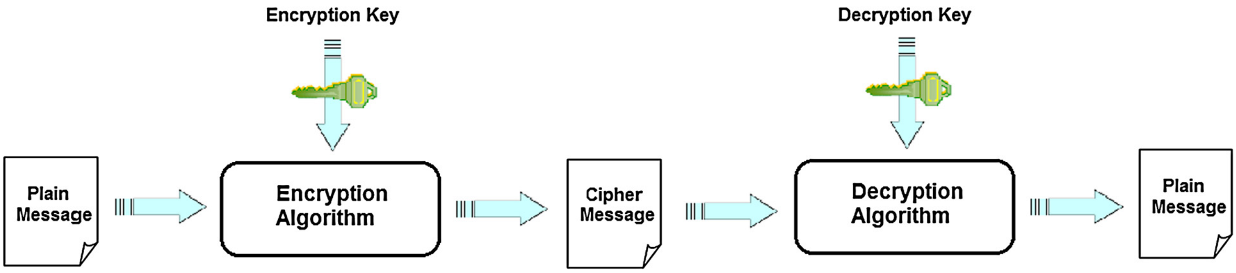


Fig. 8. The principle of encryption decryption.

that in the literature, the term "authenticity" means both authentication and integrity, and it is often confused in use with authentication.

- *Non-repudiation*: It is to ensure that a player cannot deny having done an action. In a VANET context, a vehicle should not be able to deny sending a warning e.g. or having done an attack.

5.2. *Encryption/decryption*

The principle of encryption and decryption of a message, described schematically in Fig. 8, is as follows:

- An algorithm for encryption/decryption, which is a set of information operations processing based on mathematical functions, receives as input a clear message and an encryption key, then as a result it outputs an encrypted message.
- The encryption/decryption algorithm receives as input an encrypted message and a decryption key, then as a result it outputs the corresponding clear message.

5.3. *Symmetric cryptography*

Also called secret key cryptography. For this technique, the decryption key can be easily calculated from the encryption key, in practice it takes the same. Security in symmetric cryptography is based on the ability to keep the key secret between communicating parties. If the key is revealed the system is compromised. The requirement that both parties have access to the secret key is one of the main drawbacks of symmetric cryptography in comparison to asymmetric one.

5.4. *Asymmetric cryptography*

Also known as public key cryptography. The principle of Functioning is as follows:

- Each user has a pair of keys, one private key that he must keep secret, and the other public key that he must make it available to the public.
- If we encrypt with the public key, only the private key can decrypt and vice versa.
- It is practically impossible (time and resources) to determine e.g. the private key knowing the public one and vice versa.

Asymmetric cryptography can also be used in encryption, but compared to symmetric algorithms it is usually slower. It is mainly used in the key exchange procedures and in digital signature authentication tool through digital certificates. The public key cryptography solves several problems which secret key cryptography does not succeed.

Several proposed public key cryptography based solutions for some security issues in VANETs will be discussed later.

5.5. *PKI, digital certificates and timestamping*

The management of private and public keys for a large number of users requires the establishment of a PKI: Public Key Infrastructure, which is a set of software, hardware and procedures components [65]. A PKI can provide several security services, the most important is to be a trust third party between digital counterparts. PKI ensures that role through the certification authority (CA), so it signed, delivers and keep up to date digital certificates which represent a digital ID for an entity.

In fact, a certificate is an electronic file (can be stored in many forms), which binds together a public key with an identity with the guarantee of the certification authority. A certificate allows to authenticate and sign (signing certificates) and also encrypt messages (encryption certificates). Timestamping is also among the services that PKI can provide. It certify that an event (send/receive/signing a message, ...) happens at a given time. The timestamping faces basically to authentication and non-repudiation attacks.

In a VANET context, several solutions e.g. propose the creation of a PKI related to VANETs named VPKI (Vehicular Public Key Infrastructure) [6,13], and propose the use of digital certificates as a method of rapid authentication in a vehicular network. This proposed solution will be discussed later for some related attacks.

6. VANETs security challenges against cryptographic solutions

The question that we will try to respond in this section is: what security problems among those existing in the VANET can the cryptography and its strong primitives and services solve? We summarize in Table 2 all recent existing attacks for VANETs. For each attack, we define the affected services and we describe the related possible cryptographic solutions. The solutions are proposed without going into details of the advantages and disadvantages of each solution, only the technical aspect of the solution is detailed.

7. Conclusions

Vehicular Ad hoc NETworks (VANETs) are becoming popular in Intelligent Transportation Systems, they have been designed to provide road safety and services for passengers comfort. Given their importance related to the safety of humans' lives, VANETs attract attackers and represent a favorite target for several types of attacks which consequences vary from negligible to severe. Therefore, securing VANETs poses a great challenge.

In this paper, and after reviewing the various recent aspects of VANETs sate of art such as standardization, routing protocols, projects and applications, we identify all existing security issues in VANETs and classify them from a cryptographic point of view. Also, we regroup, study and compare the various cryptographic solutions that have been separately proposed for these attacks and evaluate their efficiency.

Table 2
Cryptographic solutions for VANETs attacks and vulnerabilities.

Attacks	Compromised services	Cryptographic solutions
Jamming	Availability	– Switch the transmission channel and use the frequency hopping technique FHSS (Frequency Hopping Spread Spectrum) which involves cryptographic algorithms to generate pseudo-random numbers for the hopping algorithm. This proposal requires a modification of the used standard which currently allows only the OFDM [18].
Eavesdropping	Confidentiality	– Encrypt only data which has paramount importance and which manipulation puts in risk the privacy of the driver (positioning data, vehicle identification data, ...).
Traffic analysis	Confidentiality	– Same proposition as eavesdropping. – Use algorithms such as VIPER for V2I communications [12].
DOS	Availability	– Use bit commitment and signature based authentication mechanisms [17], which reduces the impact of almost of DOS attacks.
Sybil attack	Authentication Availability	– Deploy a central Validation Authority (VA), which validates entities in real time. Validation process can be direct or indirect. In direct validation, the node which wants to authenticate, establish a direct connection with the VA. In the indirect method, an entity already enabled can accept an incoming entity. The VA can use temporary certificates [9]. The use of the validation technique makes the VA a privileged target of attacks. – In the case of the presence of authentic and secure links with trusted nodes, [14] proposes to reduce the effect of the sybil attack by validating unknown nodes with the method of secure location verification. For this method, [6] proposes the use of approved certification. – Strengthening the authentication mechanism by the use of distance bounding protocols based on cryptographic techniques such as bit commitment and zero-knowledge [22,66,55,67].
Message tampering/ suppression/fabrication/ alteration	Availability Integrity Non-repudiation	– Use a vehicular PKI (VPKI) or a zero-knowledge techniques for the authentication between vehicles and for signing warning messages [2,55,52]. – Establish group communications [19,52]. Keys can be managed by a Group Key Management system (GKM). This causes that an intruder could not be able to communicate with the group.
Broadcast tampering	Integrity	– Given that this attack can be performed by a legitimate node of the network, cryptographic primitives are enable to prevent it. However, a non-repudiation mechanism may exist.
Brute force	Confidentiality	– Use strong encryption and key generation algorithms unbreakable within a reasonable running time [8]. This prohibits access to information to those who are not allowed.
Timing attack	Availability	– Use the timestamping mechanism for packets of delay-sensitive applications. For this proposition, we encountered the problem of time synchronization between the entities.
Replay	Authentication Integrity	– Use timestamping technique for packets which their replay is dangerous [8]. For this proposition, we encountered the problem of time synchronization between entities.
Key and/or certificate replication	Confidentiality Authentication	– Use certified and disposable keys. – Check the validity of digital certificates in real time via CRL (Certificate Revocation List) [1], which represents a real hard problem in VANETs. – Use cross certification between the different certification authorities involved in VANETs security scheme [6].
Illusion attack	Authentication Integrity	– The hardware equipment and the software must be accessible only by authorized. – Updates or reading operations from the sensors must be authenticated and verified e.g. by a challenge/response mechanism. – Use trusted hardware for which it is piratically impossible to change existing protocols and values, except by authorized [55].
GPS spoofing/Position faking	Authentication Privacy	– Use bit commitment and signature based mechanisms with positioning systems to accept only authentic location data [17,67,22].
Man in the middle attack	Authentication Confidentiality Integrity	– Use a strong authentication methods such as digital certificates and zero-knowledge.
Loss of event traceability	Non-repudiation	– Same proposition as illusion Attack.
Tracking/Social engineering	Privacy	– Use always variables MAC and IP addresses to separate the addresses from the identities of vehicles and drivers [1]. MAC and IP addresses allocation must be managed by robust algorithms.
Node impersonation	Integrity Authentication Non-repudiation	– Use variables MAC and IP addresses for V2V and V2I communications [6]. – Authenticate via digital certificates [9]. – Strengthening the authentication mechanism using distance bounding protocols based on cryptographic techniques such as bit commitment and zero-knowledge [22,66,55,67].

Table 2 (*Continued*)

Attacks	Compromised services	Cryptographic solutions
Greedy Blackhole Grayhole Sinkhole Wormhole Malware Masquerading Spamming Tunneling	Availability Authentication Integrity Confidentiality Non-repudiation	– For these attacks, cryptography does not offer real solutions, but certain suggested actions can reduce disastrous effects, such as digital signature of software and sensors. – Use trusted hardware for which it is piratically impossible to change existing protocols and values, except by authorized [55].

Even an important interest has been given by the research community to this topic, it is noteworthy that the use of new cryptographic concepts, including homomorphic encryption and ID-based cryptography, has to be more efficiently exploited in other future works to cover the weaknesses of the existing schemes and adapt to the intrinsic features of vehicular communication. Thus, our research serves as one step closer towards the design and development of effective security schemes to support the protection of critical services based on VANETs.

References

[1] M. Raya, J.-P. Hubaux, Securing vehicular ad hoc networks, J. Comput. Secur. 15 (1) (2007) 39–68.

[2] J. Blum, A. Eskandarian, The threat of intelligent collisions, IT Prof. 6 (1) (2004) 24–29.

[3] O. Trullols, M. Fiore, C. Casetti, C.-F. Chiasserini, J.M. Barcelo Ordinas, Planning roadside infrastructure for information dissemination in intelligent transportation systems, Comput. Commun. 33 (4) (2010) 432–442.

[4] S. Biswas, J. Misic, V. Misic, DDoS attack on wave-enabled VANET through synchronization, in: Global Communications Conference (GLOBECOM), 2012 IEEE, IEEE, 2012, pp. 1079–1084.

[5] A. Dhamgaye, N. Chavhan, Survey on security challenges in VANET, Int. J. Comput. Sci. 2 (2013) 88–96, ISSN 2277-5420.

[6] M. Raya, P. Papadimitratos, J.-P. Hubaux, Securing vehicular communications, IEEE Wirel. Commun. 13 (5) (2006) 8–15.

[7] B. Mishra, P. Nayak, S. Behera, D. Jena, Security in vehicular adhoc networks: a survey, in: Proceedings of the 2011 International Conference on Communication, Computing & Security, ACM, 2011, pp. 590–595.

[8] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, A. Hassan, Vehicular ad hoc networks (VANETs): status, results, and challenges, Telecommun. Syst. 50 (4) (2012) 217–241.

[9] M.S. Al-kahtani, Survey on security attacks in vehicular ad hoc networks (VANETs), in: 6th International Conference on Signal Processing and Communication Systems (ICSPCS), 2012, IEEE, 2012, pp. 1–9.

[10] I.A. Sumra, I. Ahmad, H. Hasbullah, J.-L. bin, Ab Manan, Behavior of attacker and some new possible attacks in vehicular ad hoc network (VANET), in: 3rd International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2011, IEEE, 2011, pp. 1–8.

[11] M.E. Mathew, A.R.K. P, Threat analysis and defence mechanisms in VANET, Int. J. Adv. Res. Comput. Sci. Softw. Eng. 3 (1) (2013) 47–53, ISSN 2277-128X.

[12] A. Rawat, S. Sharma, R. Sushil, VANET: security attacks and its possible solutions, J. Inform. Oper. Manag. 3 (1) (2012) 301–304.

[13] J.M. d. Fuentes, A.I. González-Tablas, A. Ribagorda, Overview of security issues in vehicular ad-hoc networks, in: Maria Manuela Cruz-Cunha, Fernando Moreira (Eds.), Handbook of Research on Mobility and Computing, IGI Global, 2010.

[14] B. Xiao, B. Yu, 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, ACM, 2006, pp. 1–8.

[15] S.M. Safi, A. Movaghar, M. Mohammadizadeh, A novel approach for avoiding wormhole attacks in VANET, in: First Asian Himalayas International Conference on Internet, 2009, AH-ICI 2009, IEEE, 2009, pp. 1–6.

[16] S. RoselinMary, M. Maheshwari, M. Thamaraiselvan, Early detection of dos attacks in VANET using attacked packet detection algorithm (apda), in: International Conference on Information Communication and Embedded Systems (ICICES), 2013, IEEE, 2013, pp. 237–240.

[17] L. He, W.T. Zhu, Mitigating dos attacks against signature-based authentication in VANETs, 2012 IEEE International Conference on Computer Science and Automation Engineering (CSAE), vol. 3, IEEE, 2012, pp. 261–265.

[18] A.M. Malla, R.K. Sahu, Security attacks with an effective solution for dos attacks in VANET, Int. J. Comput. Appl. 66 (22) (2013), ISSN 0975-8887.

[19] S.S. Kaushik, Review of different approaches for privacy scheme in VANETs, Int. J. 5 (2) (2012), ISSN 2231-1963.

[20] L. Gollan, I.L. Gollan, C. Meinel, Digital signatures for automobiles, in: Systemics, Cybernetics and Informatics, SCI, Citeseer, 2002.

[21] ONISR, Onisr-bilan provisoire 2012, http://www.securite-routiere.gouv.fr/.

[22] J.-P. Hubaux, S. Capkun, J. Luo, The security and privacy of smart vehicles, IEEE Secur. Priv. 2 (3) (2004) 49–55.

[23] DSRC, Dsrc, http://grouper.ieee.org/groups/scc32/dsrc/.

[24] I.C. Society, 802.11p-2010 – IEEE standard for information technology – local and metropolitan area networks – specific requirements – part 11: Wireless lan medium access control, (mac) and physical layer (phy) specifications amendment 6: wireless access in vehicular environments.

[25] ETSI, European Telecommunications Standards Institute (ETSI), http://www.etsi.org.

[26] ITS, ITS standards fact sheets of IEEE, http://www.standards.its.dot.gov/factsheets/factsheet/80, seen, April 19, 2014.

[27] I.C. Society, 802.11-2007 – IEEE standard for information technology – telecommunications and information exchange between systems – local and metropolitan area networks – specific requirements – part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications.

[28] L. Miao, K. Djouani, B.J. van Wyk, Y. Hamam, Evaluation and enhancement of IEEE 802.11 p standard: a survey, Mob. Comput. 1 (1) (2012).

[29] A. Hamieh, J. Ben-Othman, L. Mokdad, Detection of radio interference attacks in VANET, in: Global Telecommunications Conference, 2009, GLOBECOM 2009, IEEE, 2009, pp. 1–5.

[30] J. Rezgui, S. Cherkaoui, O. Chakroun, Deterministic access for dsrc/802.11 p vehicular safety communication, in: 7th International Wireless Communications and Mobile Computing Conference (IWCMC), 2011, IEEE, 2011, pp. 595–600.

[31] I.V.T. Society, 1609.4-2010 – IEEE standard for wireless access in vehicular environments (wave)–multi-channel operation (revision of IEEE STD 1609.4-2006).

[32] Y. Wang, A. Ahmed, B. Krishnamachari, K. Psounis, IEEE 802.11 p performance evaluation and protocol enhancement, in: IEEE International Conference on Vehicular Electronics and Safety, ICVES 2008, IEEE, 2008, pp. 317–322.

[33] M.S. Hossain, M. Atiquzzaman, Stochastic properties and application of city section mobility model, in: Global Telecommunications Conference, 2009, GLOBECOM 2009, IEEE, 2009, pp. 1–6.

[34] T. Camp, J. Boleng, V. Davies, A survey of mobility models for ad hoc network research, Wirel. Commun. Mob. Comput. 2 (5) (2002) 483–502.

[35] A. Mahajan, N. Potnis, K. Gopalan, A. Wang, Urban mobility models for VANETs, in: 2nd IEEE International Workshop on Next Generation Wireless Networks, 2006.

[36] D.R. Choffnes, F.E. Bustamante, An integrated mobility and traffic model for vehicular wireless networks, in: Proceedings of the 2nd ACM International Workshop on Vehicular ad hoc Networks, ACM, 2005, pp. 69–78.

[37] J. Luo, J.-P. Hubaux, A survey of inter-vehicle communication, Tech. Rep EPFL, Lausanne, Switzerland.

[38] J. Kakarla, S. Siva Sathya, B.G. Laxmi, B. Ramesh Babu, A survey on routing protocols and its issues in VANET, Int. J. Comput. Appl. 28 (4) (2011), ISSN 0975-8887.

[39] L.K. Qabajeh, M.L.M. Kiah, M.M. Qabajeh, A scalable and secure position-based routing protocols for ad-hoc networks, Malays. J. Comput. Sci. 22 (2) (2009) 99–120.

[40] A.G. Dludla, N. Ntlatlapa, T. Nyandeni, M. Adigun, Towards designing energy-efficient routing protocol for wireless mesh networks, in: Southern Africa Telecommunication Networks and Applications Conference (SATNAC 2009), Swaziland, 30 August–2 September 2009, 2009, pp. 1–2.

[41] F.D. Rango, J.-C. Cano, M. Fotino, C. Calafate, P. Manzoni, S. Marano, OLSR vs DSR: a comparative analysis of proactive and reactive mechanisms from an energetic point of view in wireless ad hoc networks, Comput. Commun. 31 (16) (2008) 3843–3854.

[42] Philippe Jacquet, Paul Muhlethaler, Thomas Clausen, Anis Laouiti, Amir Qayyum, Laurent Viennot, Optimized link state routing protocol for ad hoc networks, in: Multi Topic Conference, 2001. IEEE INMIC 2001. Technology for the 21st Century. Proceedings. IEEE International, IEEE, 2001, pp. 62–68.

[43] M. Osman, The performance of aodv routing protocol based on dropped packet and throughput metrics: a simulation and comparative study for VANET, Int. J. Manag. Inform. Technol. 4 (2) (2013) 265–279.

Please cite this article in press as: M.N. Mejri et al., Survey on VANET security challenges and possible cryptographic solutions, Veh. Commun. (2014), http://dx.doi.org/10.1016/j.vehcom.2014.05.001

[44] Z. Wang, L. Liu, M. Zhou, N. Ansari, A position-based clustering technique for ad hoc intervehicle communication, IEEE Trans. Syst. Man Cybern., Part C, Appl. Rev. 38 (2) (2008) 201–208.

[45] R. Jain, A. Puri, R. Sengupta, Geographical routing using partial information for wireless ad hoc networks, IEEE Pers. Commun. 8 (1) (2001) 48–57.

[46] H. Rahbar, K. Naik, A. Nayak, Dtsg: dynamic time-stable geocast routing in vehicular ad hoc networks, in: 9th IFIP Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net), 2010, IEEE, 2010, pp. 1–7.

[47] C2C-CC, Car2car project, http://www.car-2-car.org/.

[48] B. Ducourthial, F. El Ali, et al., Architecture pour communication véhicules—infrastructure, in: CFIP'2009, 2009.

[49] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, K. Sezaki, Caravan: providing location privacy for VANET, Tech. rep., DTIC Document, 2005.

[50] H. Hasbullah, I. Ahmed Soomro, J.-l. Ab Manan, Denial of service (dos) attack and its possible solutions in VANET, WASET J. 65 (2010) 411–415.

[51] S.-Y. Wang, C.-C. Lin, K.-C. Liu, W.-J. Hong, On multi-hop forwarding over wbss-based IEEE 802.11 (p)/1609 networks, in: IEEE 20th International Symposium on Personal, Indoor and Mobile Radio Communications, 2009, IEEE, 2009, pp. 3040–3044.

[52] J. Domingo-Ferrer, Q. Wu, Safety and privacy in vehicular communications, in: Privacy in Location-Based Applications, Springer, 2009, pp. 173–189.

[53] ETSI, Intelligent transport systems (its), security, threat, vulnerability and risk analysis (tvra), Technical Report ETSI TR 102 893 V1.1.1, 2010-03.

[54] B. Schneier, Applied Cryptography. Protocols, Algorithms, and Source Code in C, John Wiley & Sons, Inc., 1996.

[55] D. Singelee, B. Preneel, Location verification using secure distance bounding protocols, in: IEEE International Conference on Mobile Adhoc and Sensor Systems, IEEE, 2005, p. 7.

[56] L. Buttyan, J.-P. Hubaux, Security and Cooperation in Wireless Networks: Thwarting Malicious and Selfish Behavior in the Age of Ubiquitous Computing, Cambridge University Press, 2008.

[57] R. Minhas, M. Tilal, Effects of jamming on IEEE 802.11 p systems, Chalmers University of Technology, 2010.

[58] A. Hamieh, J. Ben-Othman, A. Gueroui, F. Naït-Abdesselam, Detecting greedy behaviors by linear regression in wireless ad hoc networks, in: IEEE International Conference on Communications, 2009, ICC'09, IEEE, 2009, pp. 1–6.

[59] Michele Nogueira, Helber Silva, Aldri Santos, Guy Pujolle, A security management architecture for supporting routing services on WANETS, IEEE Trans. Netw. Serv. Manag. 9 (2) (2012) 156–168.

[60] A. Burg, Ad hoc network specific attacks, in: Seminar Ad hoc Networking: Concepts, Applications, and Security, 2003, Technische Universitat Munchen, 2003.

[61] W.R. Jr. Pires, T.H. de Paula Figueiredo, H.C. Wong, A.A.F. Loureiro, Malicious node detection in wireless sensor networks, in: 18th International Parallel and Distributed Processing Symposium, 2004, Proceedings, IEEE, 2004, p. 24.

[62] J.R. Douceur, The sybil attack, in: Peer-to-Peer Systems, Springer, 2002, pp. 251–260.

[63] B. Parno, A. Perrig, Challenges in securing vehicular networks, in: Workshop on Hot Topics in Networks (HotNets-IV), 2005, pp. 1–6.

[64] I.A. Sumra, J.-L. Ab Manan, H. Hasbullah, Timing attack in vehicular network, in: Proceedings of the 15th WSEAS International Conference on Computers, World Scientific and Engineering Academy and Society (WSEAS), 2011, pp. 151–155.

[65] S. Choudhury, K. Bhatnagar, W. Haque, Public Key Infrastructure Implementation and Design, John Wiley & Sons, Inc., 2002.

[66] S. Brands, D. Chaum, Distance-bounding protocols, in: Advances in Cryptology—EUROCRYPT'93, Springer, 1994, pp. 344–359.

[67] M. Wolf, Vehicular security mechanisms, in: Security Engineering for Vehicular IT Systems, Springer, 2009, pp. 121–165.

[68] Philippe Golle, Dan Greene, Jessica Staddon, Detecting and correcting malicious data in VANETs, in: Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks, ACM, 2004, pp. 29–37.

[69] Brouce Schneier, Applied Cryptography. Protocols, Algorithms, and Source Code in C, John Wiley & Sons, Inc, 1996.