4

Security Issues in Vehicular Ad Hoc Networks

P. Caballero-Gil
University of La Laguna
Spain

1. Introduction

Communications are becoming more wireless and mobile than ever. Thus, in the near future, we can expect that vehicles will be equipped with wireless devices, which will enable the formation of Vehicular Ad Hoc NETworks (VANETs). The main goal of these wireless networks will consist in providing safety and comfort to passengers, but their structure will be also taken advantage with many different aims, such as commercial, access to Internet, notification, etc.

From a general point of view, the basic idea of a VANET is straightforward as it can be seen as a particular form of Mobile Ad hoc NETwork (MANET). Consequently, in a first approach we could think on considering well-known and widely adopted solutions for MANETs and install them on VANETs. However, as explained in this chapter, that proposal would not work properly.

A VANET is a wireless network that does not rely on any central administration for providing communication among the so-called On Board Units (OBUs) in nearby vehicles, and between OBUs and nearby fixed infrastructure usually named Road Side Unit (RSU). In this way, VANETs combine Vehicle TO Vehicle (V2V) also known as Inter-Vehicle Communication (IVC) with Vehicle TO Infrastructure (V2I) and Infrastructure TO Vehicle (I2V) communications (see Figure 1).

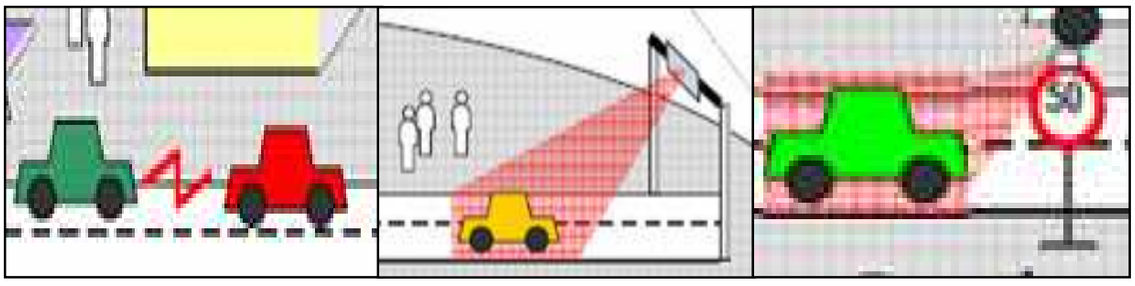


Fig. 1. V2V, V2I & I2V Communications

On the one hand, OBUs in vehicles will broadcast periodic messages with the information about their position, time, direction, speed, etc., and also warnings in case of emergency. On the other hand, RSUs on the roads will broadcast traffic related messages.

Additional communications can be also useful depending on the specific application. Among all these messages, routine traffic-related will be one hop broadcast, while emergency warnings will be transmitted through a multi hop path where the receiver of

each warning will continue broadcasting it to other vehicles. In this way, drivers are expected to get a better awareness of their driving environment so that in case of an abnormal situation they will be able to take early action in order to avoid any possible damage or to follow a better route.

VANETs are expected to support a wide variety of applications, ranging from safety-related to notification and other value-added services. However, before putting such applications into practice, different security issues such as authenticity and integrity must be solved because any malicious behaviour of users, such as modification and replay attacks with respect to disseminated traffic-related messages, could be fatal to other users.

Moreover, privacy-regarding user information such as driver's name, license plate, model, and travelling route must also be protected. On the other hand, in the case of a dispute such as an accident scene investigation, the authorities should be able to trace the identities of the senders to discover the reason of the accident or look for witnesses. Therefore, specific security mechanisms for VANETs must be developed (Hubaux et al., 2004).

Great attention both from industry and academia has been received to this promising network scenario, and standards for wireless communications in VANETs are nowadays under preparation. In particular, IEEE 802.11p is a draft standard for Wireless Access in Vehicular Environment (WAVE), and IEEE 1609 is a higher layer standard on which IEEE 802.11p is based. At a superior level, Communications, Air-interface, Long and Medium (CALM) range is an initiative to define a set of wireless communication protocols and air interfaces for the so-called Intelligent Transportation System (ITS).

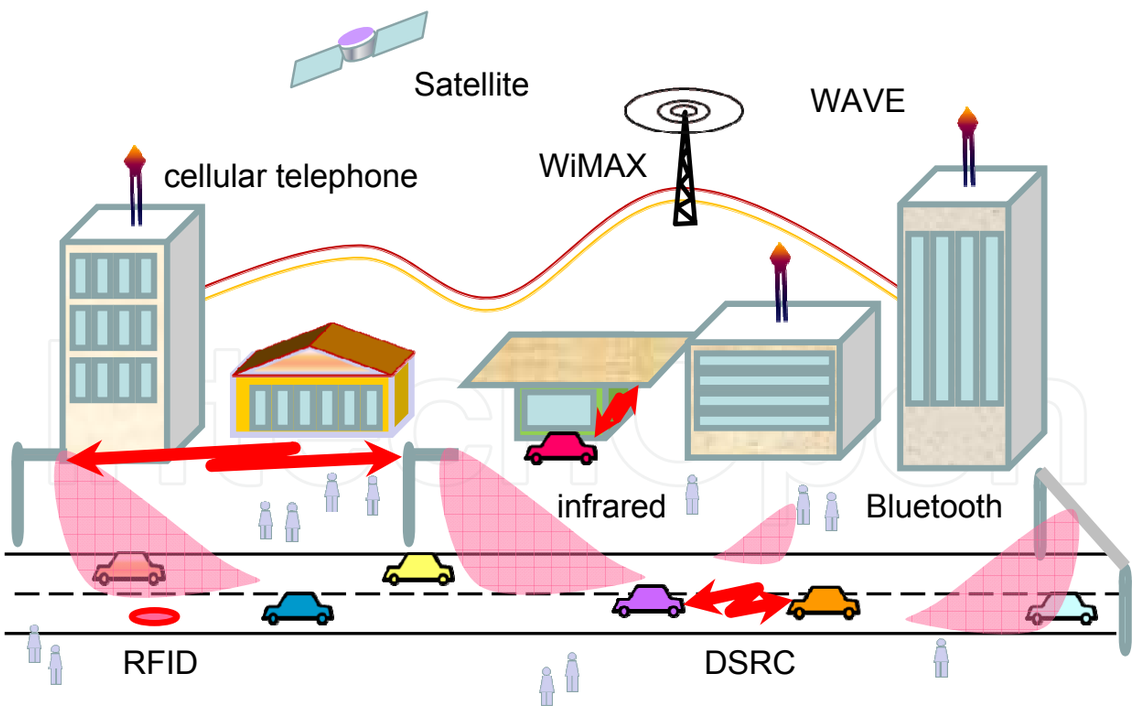


Fig. 2. Convergence of technologies

It is foreseeable that VANETs will combine a variety of wireless methods of transmission used by CALM and based on different types of communication media such as WAVE,

infrared, cellular telephone, 5.9 GHz Dedicated Short-Range Communication (DSRC), WiMAX, Satellite, Bluetooth, RFID, etc. The current state of all these standards is trial use (see Figure 2).

In this way, the field of vehicular applications and technologies will be based on an interdisciplinary effort from the sectors of communication and networking, automotive electronics, road operation and management, and information and service provisioning. Without cooperation among the different participants, practical and wide deployment of VANETs will be difficult, if not impossible.

In the future it could be expected that each vehicle will have as part of its equipment: a black box (EDR, Event Data Recorder), a registered identity (ELP, Electronic License Plate), a receiver of a Global Navigation Satellite System like GPS (Global Positioning System) or Galileo, sensors to detect obstacles at a distance lesser than 200 ms, and some special device that provides it with connectivity to an ad hoc network formed by the vehicles, allowing the node to receive and send messages through the network (see Figure 3). One of the most interesting components of this future vehicle is the ELP, which would securely broadcast the identity of the vehicle.

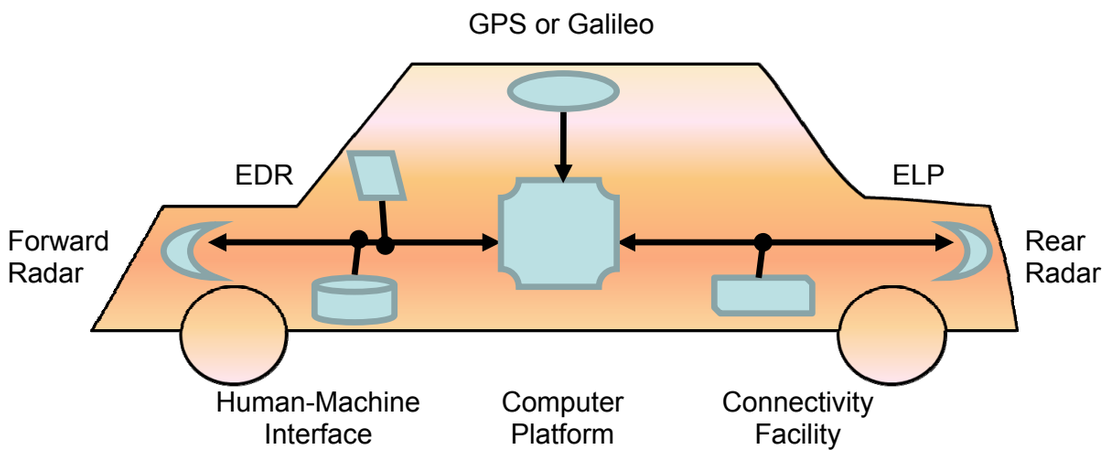


Fig. 3. Components of a future vehicle

Two hypotheses that are necessary to guarantee the protection of a VANET are that security devices are reliable and tamper-proof, and that the information received through sensors is also trustworthy. It is generally assumed by most authors that messages sent through the VANET may be digitally signed by the sender with a public-key certificate.

This certificate is assumed to be emitted by a Certification Authority (CA) that is admitted as reliable by the whole network. The moments corresponding to the vehicle purchase and to the periodic technical inspections are proposed to be respectively associated to the emission and renovation of its public-key certificate. In general, symmetric authentication is acknowledged by most authors as not a valid option due to important factors in VANETs such as time and scalability (Raya & Hubaux, 2005).

Different security challenges of vehicular networks are here addressed, paying special attention to the application of several known security primitives such as symmetric and asymmetric cryptography, strong authentication, data aggregation and cooperation enforcement.

In particular, the chapter is organized as follows. A brief summary of the main characteristics of VANETs is included in Section 2. Section 3 classifies their most important applications while Section 4 describes several security threats and challenges in VANETs. The following section introduces definitions of basic cryptographic requirements and drafts of several solutions that other researchers have proposed to provide these networks with security. Section 6 briefly describes some security schemes here proposed to protect VANET authenticity, privacy and integrity. Finally, Section 7 concludes the chapter by highlighting conclusions and open problems.

2. Characteristics

There are several general security requirements, such as authenticity, scalability, privacy, anonymity, cooperation, stability and low delay of communications, which must be considered in any wireless network, and which in VANETs are even more challenging because of their specific characteristics such as high mobility, no fixed infrastructure and frequently changing topology that range from rural road scenarios with little traffic to cities or highways with a huge number of communications.

Consequently, VANET security may be considered one of the most difficult and technically challenging research topics that need to be taken into account before the design and wide deployment of VANETs (Caballero-Gil, Hernández-Goya & Fúster-Sabater, 2009).

Among the main key technical challenges the following issues can be remarked:

- The lack of a centralized infrastructure in charge of synchronization and coordination of transmissions makes that one of the hardest tasks in the resulting decentralized and self-organizing VANETs is the management of the wireless channel to reach an efficient use of its bandwidth.
- High node mobility, solution scalability requirements and wide variety of environmental conditions are three of the most important challenges of these decentralized self-organizing networks. A particular problem that has to be faced comes from the high speeds of vehicles in some scenarios such as highways. These characteristics collude with most iterative algorithms intended to optimize the use of the channel bandwidth or of predefined routes.
- Security and privacy requirements in VANETs have to be balanced. On the one hand, receivers want to make sure that they can trust the source of information but on the other hand, this might disagree with privacy requirements of the sender.
- The radio channel in VANET scenarios present critical features for developing wireless communications, which degrade strength and quality of signals.
- The need for standardization of VANET communications should allow flexibility as these networks have to operate with many different brands of equipment and vehicle manufacturers.
- Real-time communication is a necessary condition because no delay can exist in the transmission of safety-related information. This implies that VANET communication requires fast processing and exchange of information.
- The existence of a central registry of vehicles, possible periodic contact with it, and qualified mechanisms for the exigency of fulfilment of the law are three usual assumptions that are necessary for some proposed solutions.
- Communication for information exchange is based on node-to-node connections. This distributed nature of the network implies that nodes have to relay on other nodes to

make decisions, for instance about route choice, and also that any node in a VANET can act either as a host requesting information or a router distributing data, depending on the circumstances.

Another interesting characteristic is the dependency of confidentiality requirements on specific applications. On the one hand, secret is not needed when the transmitted information is related to road safety, but on the other hand, it is an important requirement in some commercial applications (Caballero-Gil et al., 2010).

As aforementioned, VANETs can be seen as a specific type of MANET. However, the usual assumption of these latter networks about that nodes have strict restrictions on their power, processing and storage capacities does not appear in VANETs. Another difference with respect to pure MANETs is that in vehicular networks, we can consider that access to a fixed infrastructure along the roadside is possible when RSU is available either directly or through routing.

When developing a simulation of a VANET (see Figure 4), some special features have to be considered:

- Each vehicle generally moves according to a road network pattern and not at random like in MANETs.
- The movement patterns of vehicles are normally occasional, that is to say, they stop, move, park, etc.
- Vehicles must respect speed limitations and traffic signals.
- The behaviour of each vehicle depends on the behaviour of its neighbour vehicles as well as on the road type.
- VANETs can provide communication over 5-10 Km.
- Two nodes cannot exist in the same location at the same time.
- Nodes usually travel at an average speed lower than 120 Km/h.

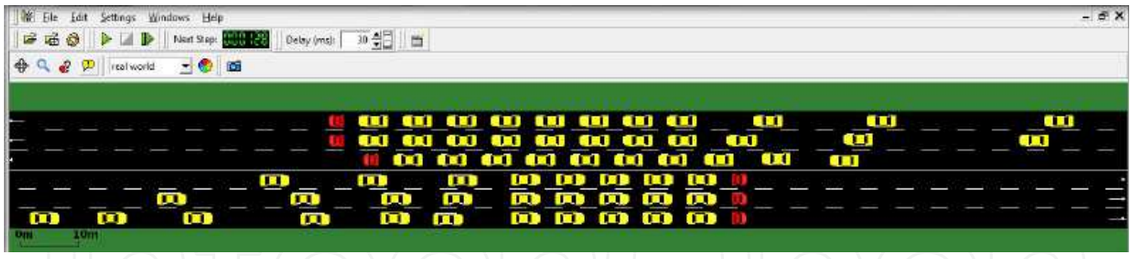


Fig. 4. Example of simulation

Despite the aforementioned differences between MANETs and VANETs, some security tools designed for their use in MANETs have been evaluated for their possible application in VANETs (Füßler et al., 2007).

Such as it happens in MANETs, in VANETs the nodes are in charge of package routing. Up to now, several routing protocols originally defined for MANETs have been adapted to VANETs following different approaches.

Reactive protocols designed for MANETs such as Ad hoc On-demand Distance Vector (AODV) and Dynamic Source Routing (DSR) have been modified to be used in VANETs. Nevertheless, simulation results do not indicate a good performance due to the highly unstable routes. Consequently, we can conclude that those adaptations might be successfully used only in small VANETs.

In other routing protocols based on geographic location of nodes, the decisions related to package routing are taken based on street guides, traffic models and data collected with global positioning systems available in the vehicles.
According to simulations, this type of protocols based on geographic information seems to be the most promising for its use in different types of sceneries such as cities and highways. In particular, in VANETs it might be useful to send messages only to nodes in a precise geographic zone. Specific routing protocols with this characteristic have been designed, and mentioned in the bibliography as geocast routing. This way to proceed allows disseminating information only to interested nodes (for instance, in case of an accident, only to proximal vehicles, and in case of an advertisement, only to nodes that are in the zone of the advertised service). In (Li & Wang, 2007) a comparative study among different routing schemes is presented.
Also like in MANETs, routing in VANETs basically follows two ways of action:

- Proactive: All vehicles periodically broadcast messages on their present states (beacons) containing their ELP, position, timestamp, speed, etc., and resend such messages if it is necessary.
- Reactive: Each vehicle sends messages only after it detects an incident, generates a request, or must resend a received message.

We have an example of how to take advantage of the proactive mode when a parked vehicle is witness of an accident thanks to its sensors, and stores the corresponding data in its EDR, so that they could be later used to determine liabilities.
In the proactive mode, the frequent beacons are very costly. Furthermore, they imply the possibility of their use to track vehicles. This fact leads to the necessity of a solution that might consist in encrypted beacons. The high frequency of those beacons combined with the higher computational cost of asymmetric cryptography suggests the application of a hybrid solution combining it with symmetrical cryptography. This hybrid solution also seems the best option, independently of the routing protocol, for some specific applications.

3. Applications

After full deployment of VANETs, when vehicles can directly communicate with other vehicles and with the road side infrastructure, several safety and non-safety applications will be developed. Although less important, non-safety applications can greatly enhance road and vehicle efficiency and comfort.

3.1 Safety-Related

A possible application of VANETs for road safety, besides the warning dissemination of accidents or traffic jumps that constitute their main application, is the warning dissemination of danger before any accident or traffic jump has taken place. This would be the case for example of a high speed excess or a violation of a traffic signal (such as a traffic light or a stop sign). In these cases, when some vehicle detects a violation through its sensors, it must activate the automatic dissemination of warning messages communicating the fact to all neighbour vehicles in order to warn them about the danger.
An additional difficulty of this application is due to the fact that the dangerous vehicle is in motion. This implies that it is not clear what any vehicle that receives the message can do to avoid the danger without being able to identify the actual location of the guilty vehicle.

Another related application of VANETs in road safety is the warning dissemination of emergency vehicle approach.
The situations of vehicles that have suffered an accident or have met a traffic jump can be dealt in the same way as any other detection of anything that might be classified as an obstacle, such as extremely slow vehicles, results of possible natural phenomena on the road, stones, bad conditions of the pavement due to works on the road, or bad meteorological conditions like low visibility. In all these cases we have that the corresponding information is important for road safety, and that the incident can be characterized by a certain location and moment.
Consequently, in these cases of applications for driver assistance, the aforementioned hypothesis referring to the existence of a Global Navigation Satellite System in vehicles is fundamental because it allows locating both the own location and that of the detected incident (see Figure 5).

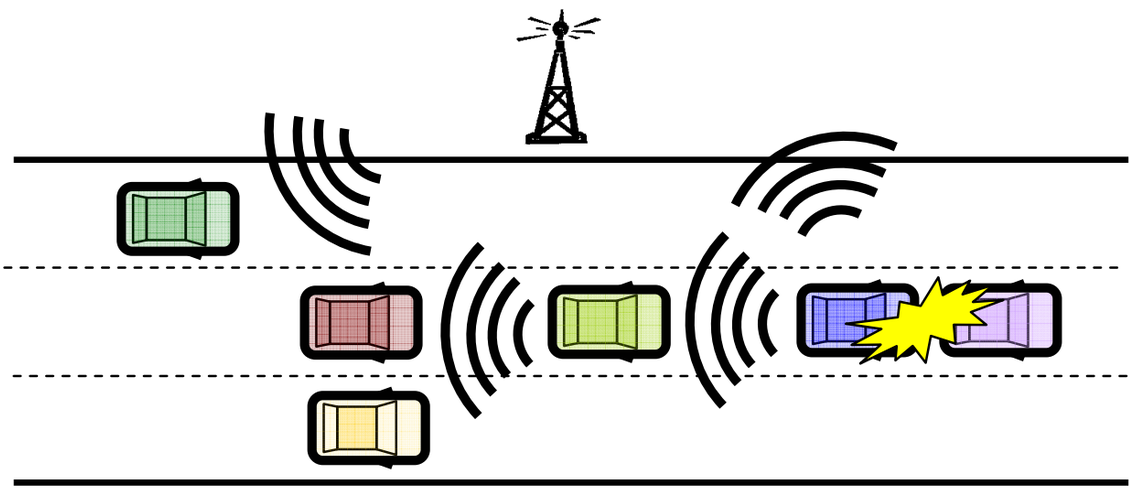


Fig. 5. Accident warning

Given the importance of the warnings of incidents for road safety, in these cases it would be advisable the use of an evaluation system of messages previous to their massive dissemination. For example, we could stipulate that in the scenery of the incident at least a minimum number of vehicles higher than a pre-established threshold activates or signs the same warning. This can be implemented for example by means of a voting scheme among the vehicles in the area nearby the incident.
In addition, note that with this proposal, possible Denegation of Service (DoS) attacks and sending of false warnings are prevented. In this sense, note that, although privacy is an important aspect in VANETs, its protection cannot stop the use of information by the authorities in order to establish responsibility in case of accident (Caballero-Gil et al., 2010).
On the other hand, it is foreseeable that the reception of a warning of abnormal and/or potentially dangerous incident will have influence in the behaviour of the other drivers. For that reason, in these schemes it is necessary to consider possible attacks based on trying to inject or to modify messages in order to obtain an effect like for example a road free of vehicles.
In order to inform cars in their vicinity to warn their drivers earlier of potential hazards, so that they have more time to react and avoid accidents, vehicles exhibiting abnormal driving

patterns, such as a dramatic change of direction, send messages including information derived from many sources like sensors, devices ABS, ESP, etc., use of airbags, speed, acceleration or deceleration of vehicle, as well as information originating from other sources like radars or video monitors, and SOS telephones or traffic lights used as repeaters to extend the dissemination rank of warnings.

From the combination of all these data, neighbouring vehicles can directly identify in many cases the type of incident by means of the interpretation of this information. A similar approach can be applied at intersections where cars communicate their current position and speed, making it possible to predict possible collisions between cars.

There is another important case that does not correspond exactly to a warning of an incident with a determined location and moment, but has also important implications in road safety. That is the case of a warning of the presence of an emergency vehicle like police, ambulance, fire-fighters, etc. In this case, the warning should include location, moment and foreseeable destiny or route of the emergency vehicle, and the objective is that the other vehicles can receive this information with enough time to clear the path of emergency vehicles in real-time, hence saving crucial time.

3.2 Non-safety-related

There is a whole variety of non-safety applications included in Value-Added Services (VASs), which can be provided through a VANET. Passengers in vehicles who spend a very long period in transit might be interested in certain application domain for vehicular networks consisting in the provision of many different types of information. Such information could be data about the surrounding area such as nearby businesses, services, facilities or road conditions, different entertainment-oriented services like Internet access (see Figure 6) or sharing multimedia contents with neighbours (Franz et al., 2005), and advertisement services (Lee et al., 2007). This diversity of possible applications comes from the fact that vehicular networks can be considered a form of pervasive network, that is to say, they operate anywhere and at any time.

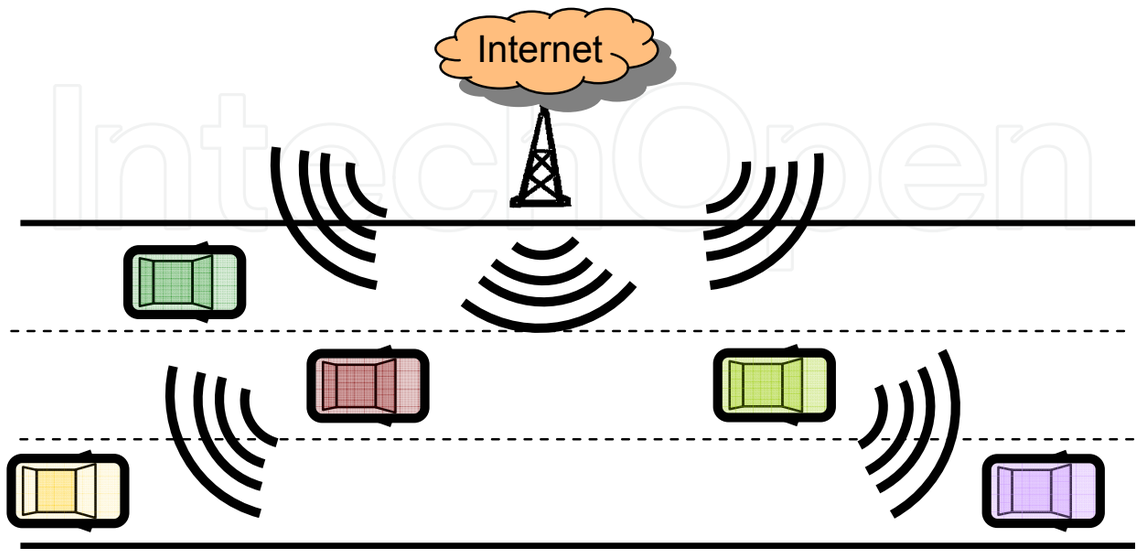


Fig. 6. Internet access

Vehicular networks could be also used for traffic monitoring. In particular, traffic authorities might be interested in obtaining information about road users so that for example they could get traffic flows to deduce current congestion levels and detect potential traffic jams.
In general, dissemination of that type of information among nodes can be used to manage traffic, not only in the aforementioned cases when an incident occurs, but also in normal conditions, when it can be used for the optimization of traffic flow.
Therefore, on the one hand, VANETs could be used for traffic management by extending drivers' horizons and supporting driving manoeuvres so that they provide drivers with information they might have missed or might not yet be able to see, in order to help them in decision making. A special traffic management application is a lane positioning system that uses inter-vehicle communication to improve GPS accuracy and provide lane-level positioning. Such detailed positioning allows the provision of services such as lane departure warning, as well as lane-level navigation systems.
On the other hand, if junctions are equipped with a controller that can either listen to communication between vehicles or receive messages from arriving vehicles, then the controller would be able to build an accurate view of the traffic at the junction through the aggregation of the received data corresponding to traffic conditions in the area, and could therefore adapt its behaviour to optimize the throughput. Traffic management applications could be also used to allow emergency vehicles to change traffic lights at signalized intersection in order to synchronize adequately to the objective of clearing the path.
An approach similar to the general case of traffic monitoring could be extended by the use of audio and video devices, which could be used for terrorist activities monitoring.
Closely related to traffic monitoring and a current particularly useful application of VANETs is traffic management. For instance, V2I solutions for road tolling are already deployed in certain places in the world to allow paying for road usage on congested roads, with prices depending on congestion levels. In the future, vehicular networks could enable that drivers are charged for their specific usage of the road network (Cottingham et al., 2007).
The idea of autonomous vehicles that are able to operate in urban areas while obeying traffic regulations is part of a collection of revolutionary applications called coordinated driving applications. This special type of safety-related applications improves performance and safety of participant vehicles through their collaboration with each other. Proposed coordinated driving applications focus mainly on three scenarios: adaptive cruise control, platooning and intersection management.
The simplest coordination application is adaptive cruise control, which performs control manoeuvres in order to maintain a safe distance for each vehicle to the vehicle in front by using forward sensors, wireless communication and cooperation among vehicles.
In a platoon, V2V communication is used to coordinate platoon members through a leader or a teamwork model in which autonomous vehicles follow a decentralized management scheme. The main benefits of platoon applications are: increase of road capacity and efficiency, reduction in congestion, energy consumption and pollution, and enhancement of safety and comfort. Demonstrations of cars travelling in platoons have already proven the feasibility of such a radical approach in certain protected settings. In particular, (Hedrick et al., 1994) and (Gehring & Fritz, 1997) have demonstrated the technique of coupling two or more vehicles together electronically to form a train.
Finally, the third mentioned coordinated driving application is intersection management for collaborative collision avoidance of autonomous vehicles while reducing delay in

comparison to traffic lights or stop signs. This interesting application allows improving road safety through cooperative driving in dangerous road points where certain circumstances exist according to which several vehicles compete for a common critical point that all have to go over so that the VANET can offer support for certain driving manoeuvres. That is the case for example of the access to a highway or a road intersection without visibility or traffic lights, where it is convenient that vehicles act co-ordinately through group communications in order to avoid accidents.

Each application implies several important differences in the security schemes that are used. In order to use VANETs as practical support for advertisement dissemination, a system of incentives must be defined both for the advertiser and for the nodes of the VANET, so that both gain when disseminating the advertisements through the network (Caballero-Gil et al., 2009). In this sense, the VANET can offer several advantages because the driver would be aimed to listen to advertisements, and even to help in their dissemination, if it obtains something in return, for example, some valuable good as gasoline. Obviously, in these cases it is necessary to define measures to prevent possible frauds of those who try to gain without receiving/redistributing the advertisements.

A similar incentive-based approach might be used for other Value-Added Services, like for example, the supply and demand of useful information like alternative routes, near parking zones, gas stations, hotels, restaurants, access points to Internet, etc. In all these cases it is fundamental that the information is encrypted in order to prevent access to non-authorized users who have not paid for the service. These other VAS applications have some similarities and differences with respect to the described advertising support service.

Both in the case when the information is a warning of incident or emergency vehicle, and in the case of dissemination of publicity or other VAS, it is remarkable that the messages have a definite origin (crashed/in traffic jump/emergency/VAS applicant vehicle, or advertiser business) but do not have a unique and definite destiny, what has clear implications in security issues. In fact, in all those cases the objective is to disseminate the message to the largest number of nodes but with different optimization criteria. In order to achieve such a goal the origin broadcasts the message to all the vehicles within its neighbourhood.

There are several authors (Dousse et al., 2002); (Wischof et al., 2005) who have proposed different algorithms to optimize the propagation of information through a VANET depending on the road type, traffic density, vehicles speed, etc. For example, in highways, the authors of (Little & Agarwal, 2005) consider the possible formation of vehicle blocks, with more or less frequent gaps between blocks. Since these gaps could cause a temporal fragmentation of the network, in order to solve the problem, the authors propose the use of vehicles against the sense of the march for spreading communications.

4. Threats

VANETs represent a challenge in the field of communication security, as well as a revolution for vehicular safety and comfort in road transport. In some of the aforementioned applications, messages can influence on driver behaviour, and consequently on road safety. In other cases like certain VASs, they can have economic consequences. In any of these cases, VANET deployment must consider the possible existence of adversaries or attackers who try to exploit the different situations, for example by injecting false, modified or repeated messages or by impersonating vehicles. Therefore, the security of communications in VANETs is an essential factor to preventing all these threats.

Even though some physical security measures can help to defend certain vehicular components against manipulations, tamper-protection instruments rarely can help to identify attacks or threats. Hence, even perfect tamper-proof components like ELPs could be stolen and installed into another vehicle to carry out impersonation attacks. Consequently, it is necessary to develop security algorithms that help to guarantee the correct and secure operation of VANETs.

An attacker can be seen as an entity who wants to spread false information, interrupt communications, impersonate legitimate nodes, compromise their privacy, or take advantage of the network without cooperating in its normal operation.

Attacks can be categorized on the basis of the attackers, into internal or external. Also they can be classified according to their behaviour, into passive or active attackers.

External attackers are mainly nodes outside the network who want to get illegitimate access mostly to inject erroneous information and cause the network to stop functioning properly. Internal attackers are legitimate nodes that have been compromised, so that they launch attacks from inside the network mostly to feed other nodes with incorrect information. In general, internal attacks are more severe then external attacks.

On the other hand, most passive attackers are illegitimate eavesdroppers, or selfish nodes that do not cooperate with the purpose of energy saving. In contrast to active attacks, in general passive attackers do not try to actively interfere with communications. In active attacks, misbehaving nodes spend some energy to perform a harmful action.

Most usual active attacks are malicious attempts to introduce invalid data into the network or to produce communication failures. Both types of attackers can have a direct influence on the correct functioning of the network. On the one hand, active malicious nodes can directly cause network traffic to be dropped, redirected to a different destination or to take a longer route to the destination by increasing communication delays. On the other hand, selfish nodes can severely degrade it by simply not participating in the network operations.

Malicious nodes can execute two of the most harmful actions in VANETs: DoS and integrity attacks.

DoS attacks, and especially jamming, are relatively simple to launch yet their effects can be devastating, bringing down the whole VANET. Jammers deliberately generate interfering transmissions to prevent communication in the VANET. Since the network coverage area, e.g., along a highway, is well-defined, jamming is a low-effort exploit opportunity because such an attacker can easily, without compromising cryptographic mechanisms and with limited transmission power, partition the vehicular network.

With respect to integrity attacks, especially interesting are spoofing where malicious nodes impersonate legitimate nodes, and transmission of false information to contaminate the communication network.

Consider, for example, an attacker that masquerades an emergency vehicle to mislead other vehicles, or impersonates RSU to spoof false service advertisements or safety hazard warnings. In conclusion, fundamental security functions in vehicular networks should always include correct authentication of the origin of data packets and of their integrity (Caballero-Gil et al., 2009); (Caballero-Gil & Hernández-Goya, 2009). To achieve this, most authors assume that vehicles will in general sign each message with their private key and attach the corresponding certificate. Thus, when another vehicle receives this message, it verifies the key used to sign the message and the message.

Selfish behaviour of any node acting as a relay forwarding other nodes traffic can also seriously impair communications in the network because it can drop messages that might be valuable or even critical traffic notifications or safety messages.
There exists a different type of attacks whose main objective is the privacy of nodes. In this case, the attacker either passively or actively, and internally or externally, tries to extract data such as time, location, vehicle identifier, technical descriptions, or trip details. Afterwards, based on those data, the attacker tries to derive private information about the attacked node.

5. Security background

Among the main cryptographic requirements to solve security issues in VANETs are:

- Availability: The network must be available at all times in order to send and receive messages. Two possible threats to availability are for example DoS and jamming attacks. Another availability problem might be caused by selfish nodes that do not provide their services for the benefit of other nodes in order to save their own resources like battery power.
- Confidentiality: Secrecy must be provided to sensitive material being sent over the VANET, like in certain commercial applications.
- Integrity: Messages sent over the network should not be corrupted. Possible attacks that would compromise their integrity are malicious attacks or signal failures producing errors in the transmission.
- Authenticity: The identity of the nodes in the network must be ensured. Otherwise, it would be possible for an attacker to masquerade a legitimate node in order to send and receive messages on its behalf.
- Non-Repudiation: A sender node might try to deny having sent the message in order to avoid its responsibility for its contents. Non-repudiation is particularly useful to detect compromised nodes.

It is almost impossible to protect all the aforementioned characteristics against the wide variety of existing threats. Furthermore, different applications have specific security requirements to take into consideration. As a result of this diversity, many different approaches exist that focus on different properties.
Authentication is a must in order to achieve the necessary trust in vehicular ad hoc networks. The existence of an authentication service makes it more difficult for attackers to join the network in the first place and thus increases the cost of misbehaviour. Hence, by verifying the authenticity of any node before exchanging information, mobile nodes reduce the amount of undesired data. For example, users of many VAS applications should obtain authentication credentials by subscribing to the service.
According to the DSRC protocol, the security overhead of this type of schemes is usually bigger than the message contents. Consequently, such an issue has to be well addressed due to the limited wireless channel bandwidth available in VANETs. Symmetric cryptography usually implies less communication overhead than asymmetric cryptography. Consequently, we might think that symmetric cryptography is a good solution, but due to the huge amount of network members in VANETs, it seems not appropriate as a generalized solution for all communications.
For comfort/commercial-related packets, sent information should be encrypted. However, safety-related messages have a different management due to their strict requirements on

delay, reliability and dissemination. In fact, urgent safety-related messages must be automatically sent and checked through tamper-proof devices so that they are not encrypted/decrypted them. What is really important for such type of information is that it must be truly reliable, what implies the need of aggregation schemes for checking not only possible unintentional transmission errors but also probable intentional fraud attempts.
There are safety related events that can be detected by a single vehicle's sensors. In that case local sensor information is aggregated and if there is a matching event, a message is sent out (Doetzer et al., 2005).
Most researchers in security of VANETs (Parno & Perrig, 2005); (Raya & Hubaux, 2007) propose a Public Key Infrastructure (PKI) solution, with anonymous or pseudonymous certificates issued by a CA. This solution assumes that each vehicle is assigned a public/private key pair that is stored in a tamper-proof device.
Every time a vehicle sends a message, it includes its signature produced with its private key together with the public-key certificate signed by the CA. So, digital signatures are added to each message, and messages are not always encrypted. Its main drawback is the big computational need and bandwidth overhead of all communications. Furthermore, since messages are not always encrypted, even outsiders can eavesdrop and possibly create movement profiles. In this way, the receiver can verify the integrity and authenticity of each message and signer.
In order to reduce overhead, some authors have proposed to attach certificates only if new neighbours are discovered (Papadimitratos et al., 2008). Also to meet the overhead requirements in terms of either processing or bandwidth, Elliptic Curve Cryptography has been chosen for the IEEE 1609 trial standard. On the other hand, the authors in (Choi et al., 2005) suggest a system based exclusively on symmetric cryptography. The main problem of their proposal is that vehicles have to contact always the base station to decrypt and verify messages.
Some other authors (Zarki et al., 2002) outline security and privacy issues in VANETs but do not present a security infrastructure. Regarding routing protocols, authors of (Rudack et al., 2002) focus on the impacts of vehicular traffic dynamics on them. With respect to node authentication, (Caballero-Gil et al., 2009) proposes differentiated services according to privacy and efficiency needs. Finally, the first to investigate the potential of ring signatures to achieve anonymity and untraceability in mobile networks were the authors of (Freudiger et al., 2008).

6. Security proposal

In this section group formation is proposed as a valid strategy to strengthen privacy and provide authenticity, privacy and integrity protection, while reducing communications in VANETs. To make it possible, group management within the network must be very fast to minimize time lost in that task (Johansson, 2004).
In particular, we propose location-based group formation according to dynamic cells dependent on the characteristics of the road, and especially on the average speed. In this way, any vehicle that circulates at such a speed will belong to the same group within its trajectory. It is also proposed here that the leader of each group be the vehicle that has belonged to the same group for the longest time (see Figure 5).
According to our proposal, V2V between groups will imply package routing from the receiving vehicle towards the leader of the receiving group, who is in charge of broadcasting

it to the whole group if necessary. If the cells have a radio that is greater than the wireless coverage of the OBU, the group communication may be carried out by proactive Optimized Link State Routing (OLSR).

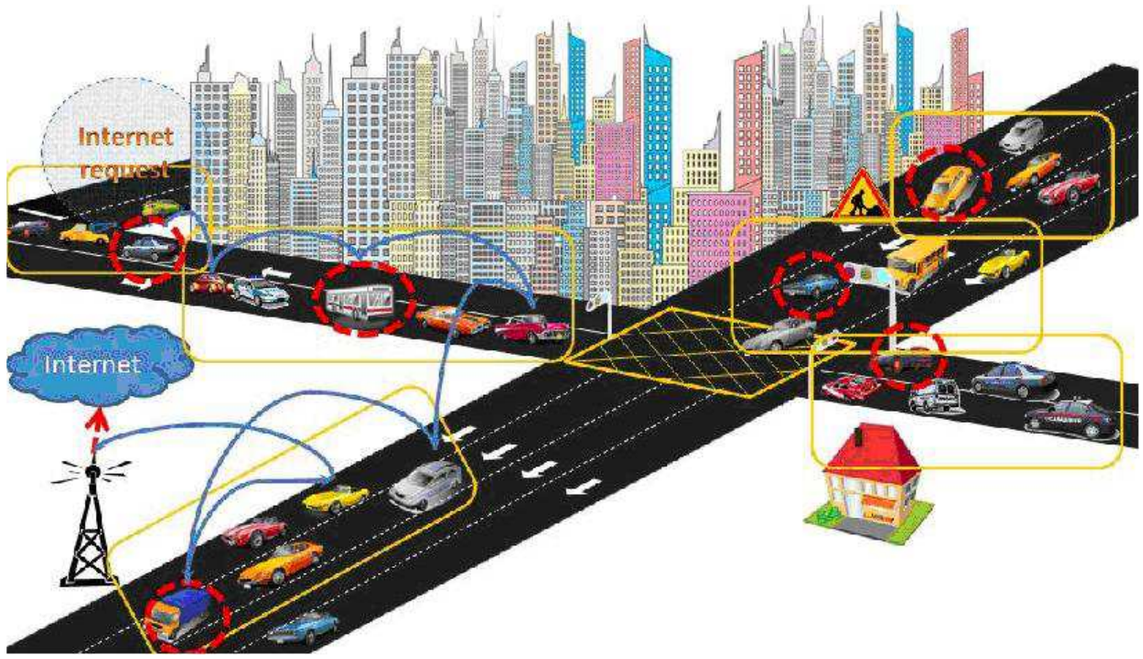


Fig. 5. Proposal structure

In the two phases corresponding to group formation and node joining, each new node has to authenticate itself to the leader through asymmetric authentication. Later, the leader sends a shared secret key to it, encrypted with the public key of the new node. In particular, this secret key is shared among all the members of the group, and used both for V2V within the group and for V2V between groups, as it is explained in the following sections.

We propose the application of different cryptographic primitives for node authentication, while paying special attention to the efficiency of communications and to the need of privacy. In this way, we distinguish four different ways of authentication, which are analyzed in the following subsections.

6.1 I2V authentication

Since privacy-preserving authentication is not necessary in I2V, we propose for such a case the use of Identity-Based Cryptography because it provides a way to avoid the difficult public-key certificate management problem.

Identity-Based Cryptography is a type of public-key cryptography in which the public key of a user is some unique information about the identity of the user (e.g. the ELP in VANETs).

The first implementation of an Identity-Based scheme was developed in (Shamir, 1984), which allowed verifying digital signatures by using only public information such as the users' identifier. A possible choice for VANETs could be based on the modern schemes that include Boneh/Franklin's pairing-based encryption scheme (Boneh & Franklin, 2001), which is an application of Weil pairing over elliptic curves and finite fields.

6.2 V2I authentication

Unlike I2V communication, in V2I communications privacy is an essential ingredient. Here we propose a challenge-response authentication protocol based on a secret-key approach where each valid user is assigned a random key-ring with k keys drawn without replacement from a central key pool of n keys (Xi et al., 2007).

According to the proposed scheme, during authentication each user chooses at random a subset with c keys from its key-ring, and uses them in a challenge-response scheme to authenticate itself to the RSU in order to establish a session key, which is sent encrypted under the RSU's public key.

This scheme preserves user privacy due to the feature that each symmetric key is with a high probability (related to the birthday paradox and dependent on the specific choice of parameters) shared by several vehicles.

When a vehicle wants to communicate with the RSU, it sends an authentication request together with a set of c keys taken at random from its key-ring and a timestamp. All this information is then encrypted by the established session key. Note that a set of keys, instead of only one key, is proposed for authentication, because there is a high probability for the OBU to have one key shared by a large amount of vehicles. This makes it difficult to identify a possible malicious vehicle if just one key is used. However, there is a much lower probability that a set of keys be shared by a large number of vehicles, and so it is much easier to catch a malicious vehicle in the proposal.

After the RSU gets the authentication request from the vehicle, it creates a challenge message by encrypting a random secret with the set of keys indicated in the request, by using Cipher-Block Chaining (CBC) mode. Upon receiving the challenge, the vehicle decrypts the challenge with the chosen keys and creates a response by encrypting the random secret with the session key. Finally, the RSU verifies the response and accepts the session key for the next communications with the vehicle.

In the first step, in order to make easier the task of checking the key subset indicated in the request by the RSU, we propose a tree-based version where the central key pool of n keys may be represented by a tree with c levels (Buttyán et al., 2006). Each user is associated to k/c leaves, and each edge represents a secret key.

In this way, the key-ring of each user is formed by several paths from the root to the leaves linked to it. During each authentication process the user chooses at random one of its paths, which may be shared by several users. In this way, to check the keys, the RSU has to determine which first-level key was used, then, it continues by determining which second-level key was used but by searching only through those second-level keys below the identified first-level key.

This process continues until all c keys are identified, what at the end implies a positive and anonymous verification. The key point of this proposal is that it implies that the RSU reduces considerably the search space each time a vehicle is authenticated.

6.3 V2V authentication inside groups

At the stages of group formation and group joining, each new node has to authenticate itself to the group leader by using public-key signatures (Sampigethava et al., 2006).

After group formation or group joining, the group leader sends a secret shared key to every new member of the group, encrypted with the public key of this new node (see Figure 6). Such a secret group key is afterwards used for any communication within the group both for node authentication and for secret-key encryption if necessary (e.g. for commercial applications).

In this way, the efficiency of communications inside the group is maximized because on the one hand certificate management is avoided, and on the other hand, secret-key cryptography is in general more efficient than public-key. Note that the use of a shared secret key also contributes to the protection of privacy.

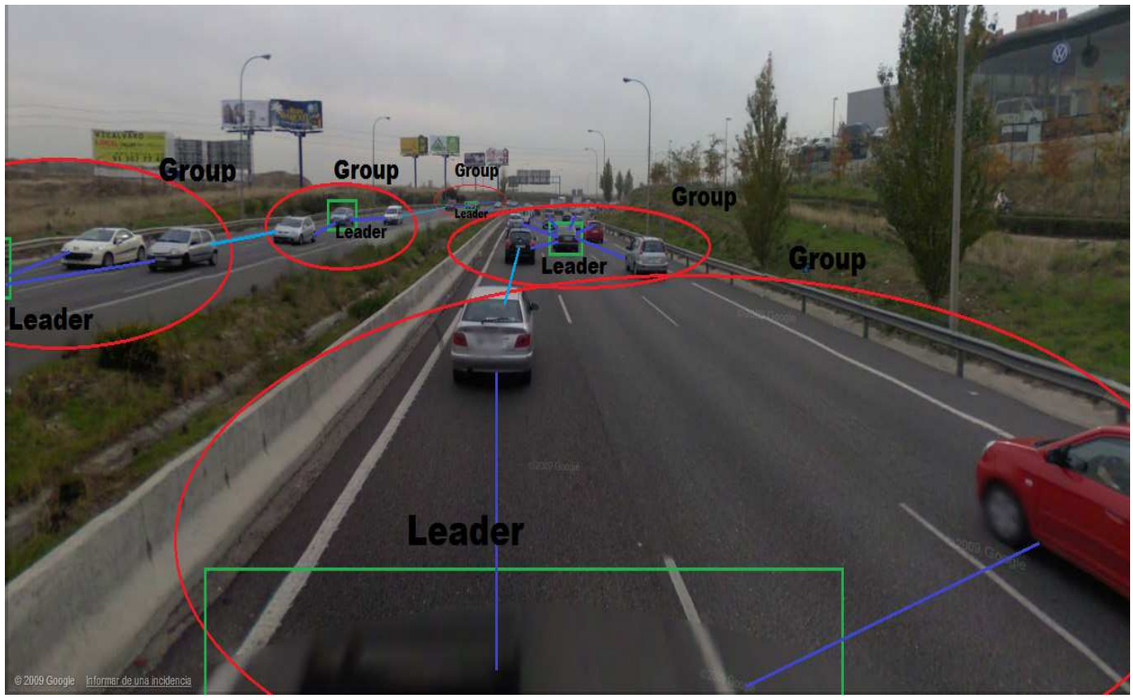


Fig. 6. Group-based organization

6.4 V2V authentication between groups

In order to protect privacy, group signatures might be proposed for node authentication between groups. A group signature scheme is a method for allowing a member of a group to anonymously sign a message on behalf of the group so that everybody can verify such a signature with the public key of the group. This group signature identifies the signer as a valid member of the group and does not allow distinguishing among different group members. This concept was first introduced in (Chaum & van Heyst, 1991).

Essential for a group signature scheme is the group leader, who is in charge of adding group members and has the ability to reveal the original signer in the event of disputes. In this proposal, the group leader issues a private key to each vehicle within the group, which uniquely identifies each vehicle, and at the same time allows it to compute a group signature and prove its validity without revealing its identity.

In this way, any vehicle from any group will be able to communicate with any vehicle belonging to other group anonymously. In particular, a proposal for group signature might be based on the cryptographic primitive of bilinear pairings, which was also proposed for I2V authentication.

6.5 Privacy

In order to guarantee the privacy of mobile nodes, they must be both anonymous and untraceable. Our proposal allows both saving communications and preserving privacy

mainly thanks to the management of communications through groups. Group keys and symmetric cryptography are used for one-hop communications inside groups.

In order to protect privacy of group members and to avoid the need of group managers, ring signatures might be used in communications between groups. Since each node of a VANET is assumed to have a public/private key pair, the knowledge of the public keys of the other nodes in the group is sufficient to create a ring signature without any interaction, so it can be performed by any member of any group (Rivest et al., 2001). Hence, unlike group signatures, ring signatures have no group managers and do not require any coordination among ring members. In this way, it would be difficult to determine which of the group members' keys was used to produce the ring signature. Also, it would be impossible to revoke the anonymity of an individual signature, and any group of nodes might behave as a group without any additional setup. Furthermore, ring signatures can be constructed with any public-key cryptographic scheme, and are usually based on combining functions.

Both membership management and group support in the absence of any infrastructure are complex research issues. Consequently, a model to describe group membership dynamics is essential. In particular it is necessary to provide efficient and flexible mechanisms for group formation within the highly dynamic scenario of the VANETs. The capability of creating and dynamically manage the membership of groups in such a mobile scenario is, at the same time, a critical issue and a challenging research area.

The problem of group key establishment can be dealt in different ways. A first solution that might be considered is key transport, which consists in allowing a group leader to create a group key and multicast it to all members. This solution involves just one round but focuses most computational load on the group leader, which is also a possible point of failure. As a second possible solution, key agreement might also be considered but in general it involves several operations and rounds of multicasts or anycasts among all group members (Rafaeli, & Hutchison, 2003). A third interesting solution (Boyd, 1997) is the combination of key transport and key agreement where the leader plays a special role but it is not exactly who chooses the group key. In such a protocol, the group key is generated with a combining function on some number contributed by the leader together with the outputs of a one-way function over the contribution of each other node. First, all members except the leader multicast their contributions, then the group leader sends its contribution encrypted with the public key of each group member, and finally each member decrypts such a contribution and generates the group key.

Group memberships in VANETs are likely to change very fast. Hence another challenge in secure group management is the efficient handling of join and leave operations of members. The simplest approach for a join operation would be based on a key transport process to transfer the existing group key to the new member. Also, if the key must be changed during each joining operation, the necessary process is not too complex since it is possible to send the new group key through multicast to the old group members encrypted with the old group key. However, changing the group key after a member leaves is far more complicated since the old key cannot be used to distribute a new one, because the leaving member knows the old key. Therefore, for the sake of simplicity, it can be assumed that when a member leaves a group it is not necessary to update the group key.

Another critical problem of group management is the definition of group memberships. Regarding this issue, group formation will take place in the VANET as soon as vehicle density exceeds a threshold. Two other characteristics of the proposal are that the cell size

depends on the transmission range of vehicles (around 300m), and the closest vehicle to the cell centre is considered the group leader.

6.6 Integrity

The trustworthiness of messages sent by a node is determined by the trustworthiness of the sender because messages from any node are trusted if and only if node authentication is valid. Apart from checking node authenticity, in vehicular networks it is extremely important to validate also the trustworthiness of data since, although in most cases identities of the nodes are irrelevant, correctness of the data they send is fundamental. For example, a simple attack based on transmitting fraudulent data about road congestion or vehicle position can be quite damaging and hence must be avoided.

In our proposal, a pervasive communication system is assumed in which mobile nodes automatically exchange information upon meeting. However, instead of doing message dissemination in VANETs through direct flooding, an approach based on location-based data aggregation is assumed so that message dissemination is delegated only to selected vehicles, which in our proposal are the group leaders. The data that group leaders disseminate are computed through a data aggregation scheme using those data received from members of its group that share a similar view of their environment. In this way, data aggregation helps both to improve security and efficiency of VANETs.

The data aggregation scheme here proposed is based on the most consistent version of data with respect to the collected information. In order to obtain such a version, one solution might be based on that versions of data obtained from other nodes receive scores according to nodes trustworthiness, and in this case the collector node accepts just those data with the highest scoring. However, due to the large size and mobility of VANETs, such reputation schemes carried out by nodes are not appropriate. We only consider a type of reputation scheme where nodes that are the source of incorrect information are detected by the RSU, which stores such information and scores nodes trustworthiness.

Data aggregation requires that group leaders crosscheck information concerning an event by comparing messages received from several sources with the data obtained from their own sensors, which are always considered trustworthy. After this step, instead of independent safety-related messages reporting the same event and sent by individual nodes, aggregated messages signed by a group with a ring signature are sent by the group leader. Thus, all the overhead will be grouped in one message as an alternative to be spread over several messages, resulting in a more efficient channel usage. In addition, once a vehicle receives such a combined message, it can trust data after the ring signature verification because the combined signature implies that all the involved signers agree on the content of the message.

Another possible useful application of data aggregation schemes in VANETs is the exploitation of data exchanged among vehicles in order to produce knowledge that can be used later by the nodes. For example, such data might allow detecting potentially dangerous road segments or determining the areas with a higher probability to find an available parking space. Furthermore, within this secondary application of data aggregation schemes it would be possible to exchange aggregated data between vehicles in order to improve their respective knowledge. According to this idea, each node should collect aggregated data, according to a map concept named Local Dynamic Map (LDM), which must reflect all relevant static and dynamic information in the vicinity, organized as a four layer structure with increasing dynamics. Furthermore, every time a vehicle moves towards some place, it

should merge its LDM with the LDM of its group neighbours in order to try to build an LDM containing information about its destination and route.

7. Conclusion

VANETs represent a challenge in the field of communications security, as well as a revolution for vehicular safety, comfort and efficiency in road transport. In this chapter we have briefly described different security characteristics and services for VANETs.
Some basic ideas of some tools that can be used to improve communication security in VANETs have been here presented. We have addressed several important security issues with a special focus on efficiency and self-organization in our proposal.
The main goals of any design for VANETs should be: wide applicability, node privacy, efficient group management, strong authentication, and data verification. In order to reach them, any solution has to combine well-known building blocks (e.g. PKI, ring signatures, identity-based schemes) according to a modular design that includes several components specifically devoted to authentication, encryption, group management, data aggregation, simulation, safety-related/value-added applications, etc.
A brief description of several proposed security schemes has been given. In particular, for I2V authentication, since there is no need of privacy, Identity-Based cryptography seems the best option to avoid certificates management. In the remaining cases, privacy is a must. In V2I a challenge-response authentication protocol using a secret-key approach based on random key-trees might be a good scheme as it provides an efficient solution for anonymous authentication. In this chapter, groups have been proposed as the most efficient way to save communications. On the one hand, in order to provide privacy between groups, we proposed group or ring signatures. On the other hand, for V2V inside groups, secret-key authentication is the basis of the proposed solution.
Since security in VANETs is yet a work in progress, many questions are open. Some of those questions are the concrete definitions of proposals, the analysis of interactions among existing schemes, and the implementation of the different proposed algorithms in order to be able to compare different possible solutions to choose the best option for a wide practical deployment of VANETs.

8. Acknowledgment

This research has been supported by the Spanish Ministry of Education and Science and the European FEDER Fund under TIN2008-02236/TSI Project, and by the Agencia Canaria de Investigación, Innovación y Sociedad de la Información under PI2007/005 Project.

9. References

Boneh D. & Franklin M. K., (2001), Identity-Based Encryption from the Weil Pairing. *Proceedings of CRYPTO 2001*, Advances in Cryptology: Lecture Notes in Computer Science Vol. 2139, pp. 213-229, California, USA, August 2001

Boyd, C., (1997), On key agreement and conference key agreement, *Proceedings of the Information Security and Privacy: Australasian Conference*. Lecture Notes in Computer Science, Vol. 1270. Springer, pp. 294–302

Buttyán L.; Holczer T. & Vajda I., (2006), Optimal Key-Trees for Tree-Based Private Authentication, *Proceedings of the 6th International Workshop Privacy Enhancing Technologies– PET*, Lecture Notes in Computer Science Vol. 4258 Springer, pp. 332-350, Cambridge, UK, June 2006

Caballero-Gil, P. & Hernández-Goya, C. (2009), Designing Communication-Oriented Node Authentication for VANETs, *Proceedings of Mobiquitous - International Conference on Mobile and Ubiquitous Systems: Networks and Services*, Toronto, Canada, July 2009

Caballero-Gil, P.; Caballero-Gil, C.; Molina-Gil, J. & Fúster-Sabater, A., (2010), On Privacy and Integrity in Vehicular Ad Hoc Networks, *Proceedings of the International Conference on Wireless Networks (ICWN'10)*, Las Vegas, USA, July 2010

Caballero-Gil, P.; Caballero-Gil, C.; Molina-Gil, J. & Hernández-Goya, C. (2009), Flexible Authentication in Vehicular Ad hoc Networks, *Proceedings of APCC IEEE Asia Pacific Conference on Communications*, Vol. 208, pp. 876-879, Shanghai, China, October 2009

Caballero-Gil, P.; Hernández-Goya, C. & Fúster-Sabater, A., (2009), Securing Vehicular Ad-Hoc Networks, *International Journal on Information Technologies & Security*, Vol. 1, (25-36)

Caballero-Gil, P.; Hernández-Goya, C. & Fúster-Sabater, A., (2009), Differentiated Services to Provide Efficient Node Authentication in VANETs, *Proceedings of the International Conference on Security and Management SAM-WorldComp2009*, pp. 184-187, Las Vegas, Nevada, USA, July 2009

Caballero-Gil, P.; Molina-Gil, J., Caballero-Gil, C. & Hernández-Goya, C., (2010), Security in Commercial Applications of Vehicular Ad-Hoc Networks, *Proceedings of Financial Cryptography and Data Security '10*, Lecture Notes in Computer Science, Vol. 6052, pp. 427, Springer-Verlag, Tenerife, Spain, January 2010

Caballero-Gil, P.; Molina-Gil, J., Hernández-Goya, C. & Caballero-Gil, C., (2009), Stimulating Cooperation in Self-Organized Vehicular Networks, *Proceedings of APCC IEEE Asia Pacific Conference on Communications*, Vol. 82, pp. 346-349, Shanghai, China, October 2009

Chaum D. & van Heyst E., (1991), Group signatures, *Proceedings of EUROCRYPT '91*, Advances in Cryptology, Lecture Notes in Computer Science Vol. 547, pp. 257-265, Brighton, UK, April 1991

Choi, J.Y.; Jakobsson, M. & Wetzel, S., (2005), Balancing auditability and privacy in vehicular networks, *Proceedings of the 1st ACM international workshop on quality of service and security in wireless and mobile networks Q2SWinet,* Montreal, Canada, October 2005

Cottingham, D.; Beresford, A. & Harle, R., (2007), A Survey of Technologies for the Implementation of National-Scale Road User Charging, *Transport Reviews*, Vol. 27, No. 4, (July 2007) (499-523)

Doetzer, F.; Kosch, T. & Strassberger, M., (2005), Classification for traffic related intervehicle messaging. *Proceedings of the 5th IEEE International Conference on ITS Telecommunications*, Brest, France, June 2005

Dousse, O.; Thiran, P. & Hasler, M., (2002), Connectivity in ad-hoc and hybrid networks, *Proceedings of Infocom*, pp. 1079-1088, New York, USA, June 2002

Franz, W.; Hartenstein, H. & Mauve, M. (2005), *InterVehicle-Communications Based on Ad Hoc Networking Principles – The FleetNet Project*, Universitätsverlag Karlsruhe, ISBN 3-937300-88-0

Freudiger, J.; Raya, M. & Hubaux, J.-P., (2009), Self-organized Anonymous Authentication in Mobile Ad Hoc Networks, *Proceedings of the Conference on Security and Privacy in Communication Networks (Securecomm),* pp. 350-372, Athens, Greece, September 2009

Füßler, H.; Schnaufer, S.; Transier, M. & Effelsberg W. (2007). Vehicular Ad-Hoc Networks: From Vision to Reality and Back. *Proceedings of the Fourth IEEE/IFIP Annual Conference on Wireless On demand Network Systems and Services (WONS)*, Obergurgl, Austria, January 2007

Gehring O. & Fritz, H., (1997), Practical results of a longitudinal control concept for truck platooning with vehicle to vehicle communication, *Proceedings of the 1st IEEE Conference on Intelligent Transportation System (ITSC'97)*, pp. 117–122, Boston, USA, November 1997

Hedrick, J.K.; Tomizuka, M. & Varaiya, P., (1994), Control issues in automated highway systems, *IEEE Control Systems Magazine*, Vol. 14, No. 6, (December 1994) (21–32)

Hernández-Goya, C.; Caballero-Gil, P.; Molina-Gil, J. & Caballero-Gil, C. (2009). Cooperation Enforcement Schemes in Vehicular Ad-Hoc Networks, *Proceedings of the 11th International Conference on Computer Aided Systems Theory EUROCAST 2009*, Lecture Notes in Computer Science, No. 5717, pp. 429-436, Springer-Verlag, Las Palmas de Gran Canaria, Spain, February 2009

Hubaux, J.P.; Capkun, S. & Luo, J., (2004), Security and privacy of smart vehicles. IEEE Security & Privacy, Vol. 2, No. 3, (May 2004) (49–55)

Johansson, T. & Carr-Motyckova, L., (2004), Bandwidth-constrained Clustering in Ad Hoc Networks, *Proceedings of the Third Annual Mediterranean Ad Hoc Networking Workshop*, Turkcell, Turkey, June 2004

Lee, S.; Pan, G.; Park, J.; Gerla, M. & Lu, S. (2007). Secure incentives for commercial ad dissemination in vehicular networks. *Proceedings of ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC)*, Montreal, Canada, September 2007

Li, F. & Wang, Y., (2007), Routing in vehicular ad hoc networks: A survey. *IEEE Vehicular Technology Magazine*, Vol. 2, No. 2 (June 2007) (12–22)

Little, T.D.C. & Agarwal, A., (2005), An Information Propagation Scheme for VANETs. *Proceedings of the 8th Intl. IEEE Conf. on Intelligent Transportation Systems (ITSC2005)*, Vienna Austria, September 2005

Molina-Gil, J.; Caballero-Gil, P. & Caballero-Gil, C., (2010), Group Proposal to Secure Vehicular Ad-Hoc networks, *Proceedings of the International Conference on Security and Management SAM*, Las Vegas, USA, July 2010

Papadimitratos, P.; Calandriello, G.; Hubaux, J.-P. & Lioy, A., (2008) Impact of Vehicular Communication Security on Transportation Safety, *Proceedings of the IEEE INFOCOM. Mobile Networking for Vehicular Environments*, pp. 1-6, Phoenix, USA, April 2008

Parno, B. & Perrig, A., (2005), Challenges in securing vehicular networks, *Proceedings of the ACM Workshop on Hot Topics in Networks (HotNets-IV)*, Maryland, USA, November 2005

Rafaeli, S. & Hutchison, D., (2003), A survey of key management for secure group communication, *ACM Computing Surveys,* Vol. 35, No. 3, (September 2003) (309–329)

Raya, M. & Hubaux, J.-P., (2005). The security of vehicular ad hoc networks. *Proceedings of the ACM Workshop on Security of Ad Hoc and Sensor Networks*, pp. 11–21

Raya, M. & Hubaux, J.-P., (2007), Securing vehicular ad hoc networks, *Journal of Computer Security*, Special Issue on Security of Ad Hoc and Sensor Networks, Vol. 15, No. 1, (39–68)

Rivest, R.L.; Shamir, A. & Tauman, Y., (2001), How to leak a secret, *Proceedings of the Asiacrypt*, Lecture Notes in Computer Science, Vol. 2248, Springer, pp. 552, Queensland, Australia, December 2001

Rudack, M.; Meincke, M. & Lott, M., (2002), On the Dynamics of Ad Hoc Networks for Inter Vehicle Communications (IVC), *Proceedings of the International Conference on Wireless Networks, WORLDCOMP*, Las Vegas, USA, July 2002

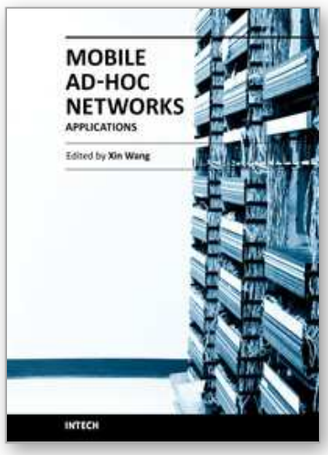
Sampigethava, K.; Huang, L.; Li, M.; Poovendran, R.; Matsuura, K. & Sezaki, K., (2006), CARAVAN: Providing Location Privacy for VANET, *Proceedings of the 3rd ACM International workshop on Vehicular ad hoc networks (VANET)*, California, USA, September 2006

Shamir A., (1984), Identity-Based Cryptosystems and Signature Schemes, *Proceedings of CRYPTO 84,* Advances in Cryptology, Lecture Notes in Computer Science Vol. 7, pp. 47-53, California, USA, August 1984

Wischof, L.; Ebner, A. & Rohling, H., (2005), Information dissemination in self-organizing intervehicle networks, *IEEE Transactions on intelligent transportation systems*, Vol. 6, No. 1, (March 2005) (90–101)

Xi Y.; Sha K.; Shi W.; Scnwiebert, L. & Zhang T., (2007), Enforcing Privacy Using Symmetric Random Key-Set in Vehicular Networks, *Proceedings of the Eighth International Symposium on Autonomous Decentralized Systems ISADS*, pp. 344-351, Arizona, USA, March 2007

Zarki, M.E.; Mehrotra, S.; Tsudik, G. & Venkatasubramanian, N., (2002), Security issues in a future vehicular network, *Proceedings of the European Wireless 2002 Conference*, Florence, Italy, February 2002



Mobile Ad-Hoc Networks: Applications

Edited by Prof. Xin Wang

ISBN 978-953-307-416-0
Hard cover, 514 pages
Publisher InTech
Published online 30, January, 2011
Published in print edition January, 2011

Being infrastructure-less and without central administration control, wireless ad-hoc networking is playing a more and more important role in extending the coverage of traditional wireless infrastructure (cellular networks, wireless LAN, etc). This book includes state-of the-art techniques and solutions for wireless ad-hoc networks. It focuses on the following topics in ad-hoc networks: vehicular ad-hoc networks, security and caching, TCP in ad-hoc networks and emerging applications. It is targeted to provide network engineers and researchers with design guidelines for large scale wireless ad hoc networks.

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

IntechOpen