Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2013, Article ID 834596, 10 pages
http://dx.doi.org/10.1155/2013/834596

Research Article

Design and Implementation of an Application for Deploying Vehicular Networks with Smartphones

P. Caballero-Gil, C. Caballero-Gil, and J. Molina-Gil

Department of Statistics, Operations Research and Computing, University of La Laguna, 38271 Tenerife, Spain

Correspondence should be addressed to P. Caballero-Gil; pcaballe@ull.es

Received 11 May 2013; Revised 2 November 2013; Accepted 18 November 2013

Academic Editor: Shukui Zhang

A vehicular ad hoc network (VANET) is a wireless network that provides communications between nearby vehicles. Among the different types of information that can be made available to vehicles through VANETs, road traffic information is the most important one. This work is part of an experimental development of a wireless communication platform oriented to applications that allow improving road efficiency and safety, managing and monitoring road traffic, encouraging cooperative driving, and offering pedestrian services and other added-value uses. The proposed system consists of smartphones, sensors, and Wi-Fi hotspots 2.0, as well as complementary functionalities including access to network infrastructure via 3G, GPRS, and 4G. The developed wireless network prototype allows taking advantage of the potential benefits of VANETs. At the same time, the use of smartphones does not require large money investments either in public or restricted areas. The first implementations with smartphones have been useful to test the behaviour of the proposal in a real environment. We have also implemented a large-scale simulation by using NS-2 simulator. From the obtained data, we have estimated the minimum requirements necessary for the correct working of a VANET and the problems that can happen in case of possible attacks or communication overhead.

1. Introduction

There is an urgent need to improve traffic management throughout the world, particularly in large urban areas. The growing congestions, gradual increase of pollution, and concern for improving vehicle safety have prompted governments and automobile industry to explore the potential of intelligent transportation systems (ITS). However, the development of the theoretical standard IEEE802.11p for Vehicular Ad-Hoc Networks, which will offer many environmental, economic, and mobility advantages, has been physically impossible due to the enormous cost that would imply for users and institutions to adapt vehicles and roads. On the one hand, roads would require including road side units (RSUs), and on the other hand, users' vehicles would have to include on board units (OBUs).

In this paper, we propose a new approach for the deployment of VANETs using current Information and Communications Technologies (ICTs). The wide deployment of ICTs involves that different pieces of technology, such as mobile phones, sensors, and wireless technology, have become ubiquitous mainly due to the significant reduction in their prices. This type of technology has a potential that has not yet been explored for the implementation of ITS applications without any deployment of RSUs and OBUs.

In order to address the development and implementation of new vehicular applications by combining these devices, it is critical to have an overview of all the involved technologies. The field of vehicular communications can offer huge advantages for drivers, pedestrians, traffic managers, transportation service providers, traders, and so forth. However, it can suffer many types of attacks that can endanger human lives or decrease transport efficiency in strategic times and/or locations. For this reason, the design and development of the proposed application are to be run on current devices, taking into account safety and security systems, in both communications and relayed information.

This paper describes a set of tools for the implementation of the proposal in the Android platform. It consists of a set of applications forming a secure communication system for spontaneous and self-organizing networks based on smartphones, which does not require any infrastructure in

vehicles or on roads because its operating mode is completely distributed and decentralized. In particular, our proposal is based on Wi-Fi Direct in order to reduce the costs to zero, because today existing smartphones all over the world offers such connectivity and its use has no cost at all. Besides, other communication techniques such as 3G/4G can provide higher transmission speed, longer transmission distance, and larger network throughput. By combining Wi-Fi Direct and 3G/4G technology, we ensure communications everywhere and at every moment.

Here, we present the design of a secure communications system in a spontaneous and self-organized vehicular ad hoc network, without any infrastructure either on roadside or in vehicles, using only mobile devices. In particular, we present a hybrid software platform that integrates different types of wireless technologies, such as Wi-Fi Direct, Bluetooth, and 3G/4G, and focussed on different ITS applications:

(1) safety applications to avoid crashes, announce road hazards and serious traffic infringement, report about approximation of emergency vehicles, and so forth,

(2) applications for traffic management and monitoring, which allow warning and/or avoiding traffic jams,

(3) value-added applications for management of parking lots, geolocated advertising platform, weather information, optimized public transport, and so forth.

The rest of the paper has been organized as follows. Section 2 covers related research on security and applications of VANETs. The technology required by the system specifications is presented in Section 3. Section 4 contains a detailed description of VAiPho structure, including explanations of its main applications. Security issues related to information content and user anonymity are analysed in Section 5 considering different possible attacks, while Section 6 provides some details on simulation a real implementation of the proposal. Finally, conclusions are presented in Section 7.

2. State of the Art

The first prerequisite to be considered when designing a tool to create a self-organizing vehicular network for increasing road safety and passenger comfort is the accuracy and reliability of transmitted information. Thus, security is one of the most important topics to be taken into account when a communication system is designed for VANETs [1]. In the bibliography we can find several proposed schemes for self-organizing VANETs [2–4] and MANETs [5–7], which try to solve all or part of the security problems existing in these types of networks. However, a different approach is presented in this paper, where a practical and secure way to deploy VANETs nowadays is proposed. The work [8] has the same objective as this work, but it does not address the main aspect of connection security.

User privacy is an important issue that needs to be addressed for the development of vehicular networks. Our proposal uses a random pseudonym generator to guarantee with a high probability that it is not possible to track a vehicle either from other vehicles or from road infrastructures, and that coincidences between two generated pseudonyms could exist but are unlikely. In [9] a pseudonym-based scheme is proposed where the authors try to solve the privacy problem caused when GPS coordinates and speeds of vehicles are sent in the beacons. In our proposal, none of those data are sent in beacons. The more recent work [10] proposes a distributed traceable pseudonym management scheme based on a blind signature.

Nowadays, many centralized GPS software navigators offer traffic services based on information provided by local road authorities, police departments, and systems that track traffic flow. However, neither of them are real-time data as they do not reflect the events that have just produced, nor respect users' privacy, so people are reluctant to use them. Regarding the congestion detection problem, Google Traffic [11], TomTom [12], Sygic [13], and Waze [14] are solutions to detect traffic congestions. The main difference with our proposal is that all of them need a data connection (LTE, 3G, or GPRS) to work. Another disadvantage is that users completely lose their privacy because they have to provide information on their locations to the companies that support the service. Furthermore, sometimes user privacy is violated because those data are stolen from the servers of the companies.

With respect to the search for free parking spaces, recently other authors have proposed different solutions. However, unlike this paper, most of them are related to paid parking. References [15, 16] are proposals involving that a device is installed in the passenger door, and when an empty parking space is found, this information is reported to a centralized server through 3G or GPRS. In [17], the authors propose a solution where users can find empty parking spaces managed by RSUs. Reference [18] presents another system for the management of parking spaces in a radius, but its goal is not on how the information is obtained and transmitted through the network but on how it is managed.

Since the solution to find a parked car is quite easy to implement, several applications for it can be found in the different mobile platform markets [19, 20]. However, we want to clarify that such an application is simply an added value of the proposal, and not its main goal.

The main starting point of this paper is the idea that the introduction of a complete model of VANETs would be extremely expensive both for users, who would have to buy and install some devices in their vehicles, and for the state, which would have to deploy RSU on the roads to support VANET services. Therefore, this work proposes a self-organizing VANET based only on communications between vehicles, with no infrastructure. The idea is that this model can serve as a quick introduction to a more complex and complete VANET, all this with good levels of reliability and security.

Our main goal is to define a simple and scalable model for VANETs, where users can cooperate through their mobile devices to obtain updated information of interest about the traffic area in order to choose the best updated route to their destinations. Our proposal takes into account that the integration of VANETs will be gradual, so that at the beginning there will not be any kind of RSU, and the VANET

Figure 1: Minimum system specifications.

will start from a few vehicles, to grow to a larger number of vehicles. This growth will be faster or slower depending on the usability and offer of added-value services that the software for VANETs provides to the users. Thus, in this paper we focus on the first phase of VANET deployment. As soon as the VANET infrastructures are fully deployed, the proposed solution should be checked to avoid unnecessary communications so that the high number of communications does not degrade the network.

3. Used Technology

The system here proposed, called VANET in Phones (VAiPho), has been fully developed and tested for Windows Mobile. We know that this technology is obsolete so here we present a partially development for Android. Mobile application development has gone multiplatform, so we know that VAiPho will have to be developed for iOS and Windows Phone platform too. However, none of both platforms allow creating direct communications with other OS smartphones, so the implementation in these platforms will depend on the required opening of the native libraries.

The following technology (see Figure 1) is necessary for the optimal use of VAiPho.

Bluetooth/Bluetooth Low Energy. To connect the device with the vehicle, providing automatic activation of VAiPho services without requiring the user's attention.

Wi-Fi Direct. IEEE 802.11 b/g/n. For the direct exchange of information about possible events between different wireless devices.

Location Services. They include information from mobile phone towers, GPS antenna, and nearby Wi-Fi nodes to obtain the geographic coordinates where the different events happen as well as the speed and direction of the involved vehicle.

Storage Space. With the required capacity for storing the necessary apps, maps and data about users, and information.

Battery. To run the application and communicate with other nodes.

As we can see, VAiPho uses the powerful application platform capabilities of today's mobile devices. Thus, it is not expensive at all for users. Furthermore, people are used to working with mobile devices, so the user interface of VAiPho is not strange for users, which avoids the usual difficulties of learning to use new devices.

Most of the VAiPho information exchanges are performed using the Wi-Fi Direct standard. This standard is highly suitable for this type of communication because devices can connect directly to each other quickly and conveniently in order to do different tasks such as synchronization and sharing of data. The IEEE 802.11p standard of wireless communications [21] was specifically designed for the deployment of VANETs and therefore it is more appropriate for this type of communications. However, nowadays there are no devices capable of broadcasting in the frequency range that IEEE 802.11p uses. For this reason, VAiPho uses Wi-Fi Direct, which is based on the IEEE 802.11 family of standards for wireless local area network operation and has the ability to communicate under the IEEE 802.11b/g/n standard.

4. Application Structure

VAiPho structure consists of three main parts that have been implemented in different applications in order to test each one separately to find problems individually before integrating them into VAiPho implementation, as shown in Figure 2.

Bluetooth Launcher. It runs several services to detect available connections in the smartphone. It is a light program in charge of detecting Bluetooth, NFC, or charger connection to launch other services when the user is inside the car. It is especially useful if the device is connected with the Bluetooth hands-free car kit.

Smart Navigator. It launches the automatic application that is responsible for detecting and forwarding the events that happen on the road.

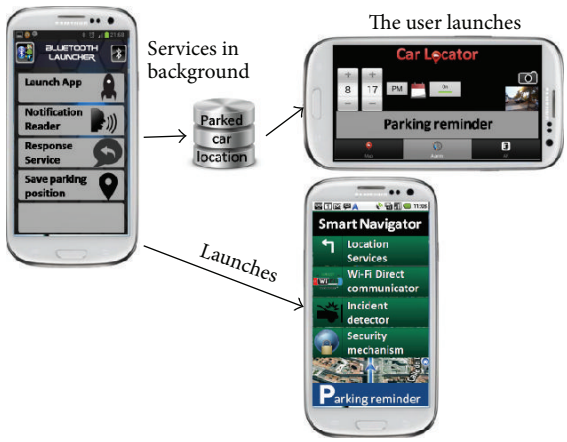

Figure 2: VAiPho structure.

Figure 3: Interface of Bluetooth Launcher.

Car Locator. It is designed to show the information saved by the Bluetooth Launcher about the car's position.

Geolocated Advertising. It is the source of VAiPho commercial profit.

This section presents these modules so that their internal structure is fully detailed.

4.1. Bluetooth Launcher. Bluetooth Launcher allows the automatic starting of the application via Bluetooth when the mobile phone connects to the hands-free car kit. This application is one of the most important parts of VAiPho from the point of view of road safety because it ensures that users keep the focus on driving, as distraction is a major cause of deaths on the road. For this reason, Bluetooth Launcher, which is a very light application, is a service that listens for the smartphone connections, so that when the smartphone connects with the hands-free car kit through Bluetooth, NFC, or charger, it automatically launches a navigation application (see Figure 3). In this way, it does not require the driver attention, which prevents possible distractions if the driver forgets to turn it up.

Bluetooth Launcher automatically launches the listening services when the user powers on the smartphone and, from then, it runs in background. It hardly consumes any resources because its unique function is to listen to a registry and to launch other applications like the Smart Navigator, if the device connects to the car through Bluetooth, NFC, or charger.

Another important characteristic of Bluetooth Launcher is that it reads the notifications aloud. Thereby, the user can listen to the notifications from chat apps like WhatsApp, Line, Viber, and so forth, or from SMS. It also shows these notifications in the smartphone screen with large fonts. Furthermore, it allows easily answering those messages without the need of using hands with the smartphone.

We are aware that the priority of mobile phones is to make phone calls and high battery consumption would cause discomfort to users. This fact has been taken into account when implementing Bluetooth Launcher, so it has very low battery consumption and it is not a drawback for VAiPho.

4.2. Smart Navigator. Smart Navigator is the main application of VAiPho. It is also the most complex one because it involves many different tasks. VAiPho requires both connectivity with other phones via Wi-Fi Direct and GPS. Thus, connectivity using standard interfaces is necessary. Besides, VAiPho uses GPS information, like maximum lane speed, vehicle speed, and geographic coordinates, in order to detect possible congestions or empty parking spaces. This information has to be processed, stored, and sent to other vehicles. For that purpose, the Smart Navigator implements the following functionalities: starting the wireless interface, creating an ad hoc network or connecting to other devices, loading data from the database and password file, loading and starting the client beaconing and the server, starting the maps app, and starting the incident detector.

The process followed when the Smart Navigator launched involves the following steps. First, the Wi-Fi Direct interface is launched and begins receiving and sending beacons from and to the network. If the interface finds a node, it connects with it via Wi-Fi Direct. Then, it creates and fills the database with user data like private/public key pair, secret key, pseudonym, and so forth. These security issues are detailed in Section 5. Then, the system is ready to communicate and exchange information about events with other devices in the range of transmission. This entire process is automatic and transparent to the user, and just a voice message indicates to the driver that VAiPho has begun.

Once the communication system is set, the GPS navigator is started and an incident detector system is launched. The main goal of Smart Navigator is to detect an abnormal situation automatically in order to produce the corresponding event warning and alert the driver and other users about that situation. This process uses GPS software to obtain data such as speed and location. Specifically for the real device implementation of this work we have used the Google Maps API.

Smart Navigator has the target of detecting possible congestions on the roads automatically, so it uses the function of the SDK that allows retrieving the actual location and speed as well as the speed limit of the current road. With this information, the event detector of VAiPho finds out whether the vehicle is travelling at an unusually low speed

and, in such a case, it concludes that the vehicle is stuck in a traffic jam. Once detected the incident, the process generates an event warning including the road name, direction of car movement, and geographic location in which the incident is located. This event is stored in the database and relayed to other vehicles. Thanks to these automatic event detections and the cooperation among devices, it is possible to know more about road conditions. This information is relayed to other vehicle, which can play different roles depending on their situation regarding the detected event. On the one hand, if the vehicle that receives the warning can confirm it because it is travelling on the same road and has also detected the same event, nodes use the data aggregation scheme described in Section 5, in order to avoid network overload. On the other hand, if a vehicle receives the warning but it cannot detect the event because it is not circulating on the same road where the event has been detected, or it is on the same road but far away from the incident, there are two possibilities.

(a) The road is not part of the receiver vehicle route: in this case, the vehicle acts as a simple packet transmitter and relays the packet to all the vehicles within its range of transmission.

(b) The road is part of the receiver vehicle route: this case takes more processing time because first the vehicle has to determine whether the busy road is in its route, and if so, it has to compute whether it is better to choose an alternative route or to keep the same one. If the system determines that it is better to use an alternative route, the new route is calculated.

Many security issues have been taken into account to implement all these processes because any attacker could try to generate false events, or to modify the contents of real packets, or even to deny relaying packets in order to attack the network operation. Therefore, communications among vehicles and information about detected events relayed in the network should provide evidence of being truthful. For this purpose, a security module presented in Section 5 has been created and added to VAiPho. In this section we explain possible attacks and how VAiPho resists each of them.

There is another important task of Smart Navigator, which is the detection of parking space availability. In this application, the procedure is simple. When a driver turns on the car, the mobile device synchronizes to the GPS signal and obtains the geographic coordinates where the vehicle is parked before it leaves the space. Then, Smart Navigator broadcasts these geographic coordinates as a potential empty parking space. Received events of parking spaces have a short expiration time that is configurable by the user. The default value is set to 1 minute in the implementation. Frauds and errors cannot be controlled for parking events because there are several situations where a vehicle can leave a certain location that is not a valid public parking space, such as a private outdoor parking space or a prohibited parking space. For this reason, when the tool announces a parking space, it indicates that it is a potential empty parking space, but there is no guarantee that the space continues to be available when the receiver reaches it. In order to use this tool, it is necessary

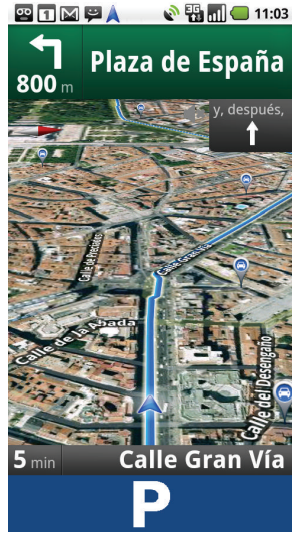

Figure 4: Driver Interface of Smart Navigator.

to launch the search for an empty parking space. When an empty parking space is detected, it is shown on the map and a voice message is then launched.

Figure 4 shows the interface that is displayed when the user is driving. It is very similar to that used by conventional GPS navigation applications. In order to prevent distracted driving, this interface not only uses icons on the maps but also voice messages. Therefore, when it detects traffic congestion or a possible empty parking space, an icon on the screen is shown and a voice message indicating congestion on the route or available parking is heard.

4.3. Car Locator. This application has a simple interface, which is shown when the user is not driving (see Figure 5). When the user turns off the car, the geographic coordinates where the vehicle is parked are stored in the database in order to help the user to find the parked vehicle. Often, it is difficult for users to find the places where they parked their cars, especially in large and unknown cities. In these cases, Car Locator uses the geographic coordinates of the parked vehicle stored in the database in order to draw a walking route to the car on the map.

Additionally, the users can check the events that are updated and stored in their mobile phones. In particular, Car Locator module provides a tool to locate where the vehicle is parked, if both Bluetooth Launcher was active when the car was parked and the parking space had location service coverage. For this purpose, Car Locator module provides a parking remainder button, marked with word *find*, which the users have to click on to locate their cars. This module launches the GPS navigator on walking mode to show the place where the vehicle is located and the route on the map between the user current location and the car. Figure 5 shows the case when the application indicates that the information on the vehicle location is available.

4.4. Geolocated Advertising. Companies or users that are interested in advertising through this tool may contact the

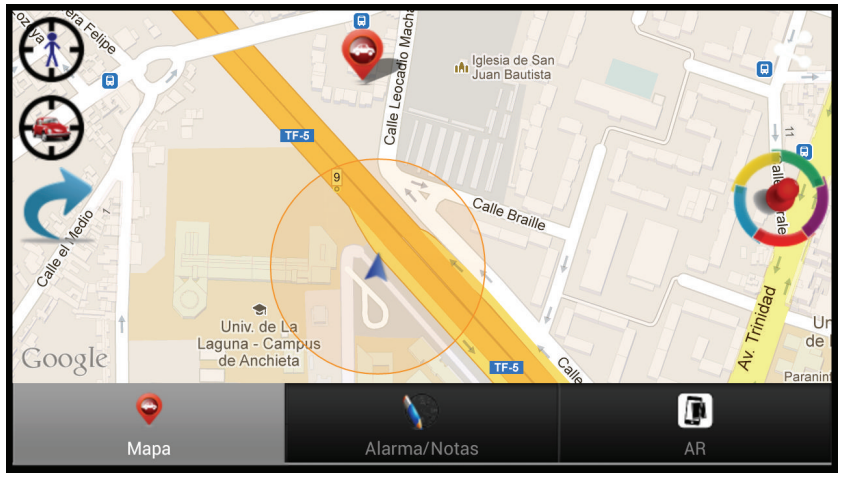

Figure 5: Pedestrian Interface of Car Locator.

administrators because VAiPho allows providing geolocated advertising as source for commercial profit. In particular, all registered users or companies can contract geolocated advertising.

Advertising data include name of the company, message, X coordinate, Y coordinate, area of interest, expiration date, and commercial logo. The message is limited to a short number of characters in order to be easily showed and read by the application. This information is processed and checked and, after the payment, the user receives a packet containing the advertising information and its certificate. The user then has to download the Geolocated Advertising application and store it in a predetermined path in its device. Afterwards, its device will broadcast the advertising information to all nearby VAiPho users, who will receive it if it is so defined in their advertising filters.

5. Security Mechanisms

An important challenge in VANETs is security, not only regarding the users that take part in the network but also the involved communications. Moreover, the relay information can affect driver decisions because they can reduce their speed and/or choose alternative routes based on a received report. Thus, a security scheme is necessary to determine whether the available road traffic information to the driver is trustful or not. Besides, the quality of communications in VANETs can be degraded if the number of noncooperative vehicles is very large. For this reason, VAiPho includes several security mechanisms to prevent possible attacks against data integrity and user privacy.

5.1. Reliability. The definition of trust relationships between users to define which devices are reliable inside the network is an important issue. In order to reach this purpose, a trust graph according to which key certificates are distributed is proposed. For this goal, people interested in VAiPho must register in the application, which allows generating a file of signatures and certificates that are required to use the application.

VAiPho is a self-management tool based on the trust between users defined through key certificates signed by the users who trust the corresponding key and owner. The more signatures a key certificate has received, the greater the trust from other nodes that can be used during its life in the network. Therefore, we can find a similarity between our network and social networking sites like Facebook, Twitter, and so forth. In this way, VAiPho operates according to what is called viral marketing; that is to say, it uses techniques based on preexisting social networks. In order to facilitate the registration process, VAiPho will use the APIs of the social networks (Facebook, Twitter, Google+) to enable the registry of the user in VAiPho services.

Furthermore, VAiPho allows users not involved in any social network to use their email account for trust goal. They can log in the application and register to get their pair of public and private keys in order to start using VAiPho. Once the users register their email credentials, the tool imports their contacts from their email accounts and searches in this list other users registered in the system. The resulting list is then displayed to the new users so that they can confirm who of these users will be used to sign their certificates. During the signing process, VAiPho website exchanges the generated certificates so that each user holds the signature generated by itself and the signatures produced by its friends. Each time a new mutual authentication is done, the application may download an updated file containing the certificates generated by the users and its friends, which is needed to generate the certificate graph of the trust network to allow secure communications within the network.

Users can download the application from Google Play. Once the application is installed on their devices, it generates the files containing the cryptographic information and stores them in a protected path.

5.2. Privacy and Legitimacy. Privacy and legitimacy are the most important issues regarding VANET security.

On the one hand, in VANETs it is completely undesirable that, through the communications, any attacker can track a

user. In centralized systems using long reach communications the situation could be even worse because an attacker could track all the vehicles at the same time from a single site. VAiPho mechanism does not use long reach communications so this centralized attack is not possible. However, the particular Wi-Fi Direct signal that VAiPho uses for communication could be tracked. In order to protect user privacy, the application uses variable pseudonyms associated with the phone MAC address as identifiers. In particular, VAiPho application changes its pseudonym in random time periods and warns about these changes through the beacons only to those nodes with which it is authenticated.

On the other hand, it is necessary to ensure that the device corresponds to a legitimate user of the VAiPho network. Checking this in a fully distributed network, where there is no central infrastructure to control identities, is complex. In this work, the mechanism to verify the authenticity of users is based on a zero-knowledge proof, which is an interactive method for one user to prove to another that it knows a secret, without revealing anything about it. Specifically, in VAiPho the secret is the public key of a third user that both communicating parties know according to their certificate graph. Hence, public keys are specially selected to fulfil the requirements of the used zero-knowledge proof. In this way, it is necessary that both users share a friend's public key to make authentication possible. Thus, it is important that users maintain their certificate repositories updated. According to the so-called rule of 6 degrees of separation [22], nodes in this type of network have in their local repository at least one node in common with a high probability. VAiPho automatically revokes certificates of users who repeatedly show bad behaviour, and information about revocations is exchanged between authenticated users.

5.3. Integrity. One of the most important issues in security is to be able to ensure that information relayed in the network is trusted. An attacker could simulate a nonexistent traffic congestion in order to convince other users not to choose a route and in this way to have the road free of vehicles. VAiPho uses a data aggregation mechanism to avoid this type of possible fraud. The procedure is as follows. When the application installed in a device detects an abnormal situation such as a speed much lower than expected for a long time, it sends a traffic congestion warning to its neighbouring devices. If neighbour applications detect that their speed is abnormal too, they sign the received information, corroborating it. When the promoter application receives a minimum number of signatures, it adds them to an aggregated packet with the information and sends it to all neighbours, who widespread the data [23].

Therefore, traffic congestions must be detected by different VAiPho users, which must sign the traffic event with their private key in order to allow the aggregation of these signatures in a single packet. Thus, we ensure that not only a vehicle has detected an incident but also that several vehicles have corroborated it. This security mechanism eliminates the possibility of spreading false traffic congestions created by a single attacker and avoids possible confusion generated by the system when a vehicle stops on the side of the road due to different reasons such as a flat tire or a vehicle failure.

The minimum number of required signatures depends on the deployment level of the VAiPho application, that is to say, the higher the number of vehicles with VAiPho, the greater the number of required signatures. This will also mean that the larger the number of VAiPho devices in the network, the lower the possibility of attack. In order to calculate the threshold number of required signatures, VAiPho checks the time since its first authentication in the current journey and computes the average number of users per minute. In the current VAiPho implementation, this average is lower than one per minute, so the number of required signatures is two. If the number is between one and four per minute, the number of required signatures is four, and if the average is higher than four per minute, the number of required signatures is five.

5.4. Availability. Since in VAiPho the packets are exchanged among vehicles using others as relaying nodes, an attacker could try to make that communications fail. This could cause a VANET to be broken into pieces so that the network cannot provide services such as packet forwarding. Thus, an attacker could launch a passive denial-of-service with the goal that the wireless network does not work properly.

In this sense, VAiPho includes a specific mechanism against these attacks, which uses encrypted exchange of data as a method to strengthen cooperation in relaying packets as it prevents passive nodes that do not cooperate in relaying packets to get benefit from encrypted information.

In this way, VAiPho application ensures that only those vehicles that belong to the network and help in its operation benefit from information relayed in it. The encrypted exchange of data prevents users who want to benefit from the VANET without helping in forwarding information because such a passive attack would degrade the functionality of tool and compromise the connectivity of the network.

6. Experimental Analysis

Simulation data and real implementation settings are briefly presented in this section to demonstrate that VAiPho is successful in accomplishing the goals of automatically detecting and warning about traffic congestions and helping people to find empty parking spaces. Furthermore, through the experimental analysis we have checked that the goal is accomplished in a safe way, both regarding data integrity and user privacy.

These proof-of-concept tests were intended to evaluate whether deploying VANETs through mobile phones can fulfil specific characteristics of VANETs such as hybrid architecture, high mobility, dynamic topology, scalability problems, and intermittent and unpredictable communications.

The first test consisted in checking that communications between smartphones with Wi-Fi Direct by using the IEEE 802.11b/g/n standard are feasible by using a simple client-server application between devices, when circulating with vehicles in urban environments or motorways at different speeds, using different numbers of devices. These tests were successful. After this, we created several simulations of the

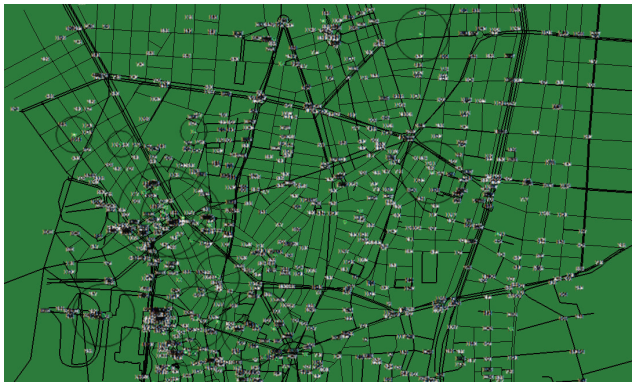

Figure 6: VAiPho simulation with SUMO and NS-2.

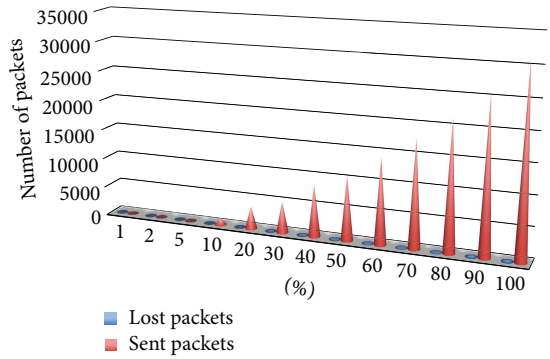

Figure 7: Numbers of packets in VAiPho simulation.

proposal by using SUMO and NS-2 in order to estimate the minimum number of vehicles that are required to deploy the network. Finally, we implemented and are now improving the complete set of applications that form VAiPho for Android smartphones.

6.1. Simulation. The main target of the simulations was to determine the minimum density of cars necessary to ensure the appropriate deployment of VANETs.

From the obtained results, we concluded that VAiPho is feasible in urban environments with a minimum percentage of vehicles that allow disseminating the information over the network. Under these conditions, both the feasibility and effectiveness of the approach were shown through the results.

In the first part of the simulation with NS-2 [24] and SUMO [25] (see Figure 6), the most relevant options selected for the demonstration were total number of vehicles: 600–15000, number of vehicles with OBUs: 1%–100%, simulation time: 100–216000 seconds, authentication period: 20 seconds, and distance between relay nodes: 75 meters.

The implemented simulations of VAiPho were studied in three different development levels: vehicle mobility, node energy, and Peer-TO-Peer (P2P) communication.

(i) The vehicle mobility level manages the node movement according to the movement pattern, which defines roads, lanes, different speed limits for each lane, traffic congestions, and so forth.

(ii) The node energy level is used to distinguish between vehicles with and without OBUs because vehicles without OBUs are on the road but do not make any contribution to the communications.

(iii) The P2P communication level is responsible for the definition of which nodes are in the transmission range of the retransmitting node at any time.

The simulations allowed us to know the number of connections in the network related to the percentage of vehicles with OBUs. From this information, the minimum number of vehicles with OBUs that is necessary to exchange information can be extracted. On the other hand, the percentage of vehicles with OBU necessary to avoid a drop in the quality of communications can be also estimated.

The simulations were run for different percentages of nodes with the same topology in order to illustrate the vehicular P2P network evaluation. Within the information obtained from the simulations (see Figure 7), we have the number of packets that have been generated, sent, broadcast, received, lost, and so forth by each node. Also, other computed information is the number of generated or lost packets in the whole network, which types of nodes generate packets and forward them, and so forth. In addition to all this information, another interesting aspect of simulations is that it provides a detailed image of what happens in each moment in the VANET thanks to the use of the NS-2 display. The traffic model was shown through the SUMO tool while the information was represented using the TraceGraph tool.

6.2. Real Implementation. Many communication tests have been made using the IEEE802.11b/g/n standard with VAiPho in mobile phones inside cars in urban environments.

The first conclusions of these tests are twofold. On the one hand, vehicles with VAiPho traveling in opposite directions do not have enough time to establish communications. On the other hand, vehicles in the same direction or inside cities, where the speed is lower, have enough time to establish communications and to exchange the data required by the proposal. Thus, the described system can be seen as a first approach to the real deployment of some interesting VANET applications with currents devices, which could be analysed as a proof of concept of the future WAVE-based VANETs [26].

For the evaluation, we built a set of VAiPho applications in different smartphones with Android using Java. Some videos showing how this tools works in real devices, vehicles, and roads can be found on the website [27].

The application has shown to be effective for traffic congestion recognition, parking detection, and parked vehicle finding. It also works well regarding authentication of users, protection of user privacy, and exchange of secret information with other devices. Devices running VAiPho that receive some information, display and forward such information correctly.

In particular tests showed good performance in:

Automatic Recognition and Warning of Traffic Congestions. The scenery is as follows. A vehicle is stuck in a traffic

jam. VAiPho application running on a device inside the car automatically detects it and broadcasts a warning message. Another device inside a car on the same route and direction detects the same traffic congestion and signs the received message, and the signed message is broadcast so that a third device displays the traffic congestion both on the screen and through voice messages.

Automatic Detection and Announcement of Empty Parking Spaces. The scenery is as follows. A vehicle leaves a parking space and broadcasts the announcement of an empty parking space. Nearby vehicles receiving this information forward it to other vehicles, and if they are looking for empty parking spaces, they show this information to the drivers on the map and through prompt messages.

Route to Parked Vehicle. The scenery is as follows. A vehicle is parked in a parking space and then the user leaves it. Afterwards, the user presses the parking reminder button and the tool shows the route on foot to the vehicle.

Geolocated Advertising. Advertisements are broadcast in their area of validity.

Systems for traffic congestion detection and warning were tested through several devices playing different roles. In this way, real traffic congestion situations were simulated. Different devices inside vehicles were in charge of detecting, signing, and aggregating the events, receiving those packets and checking the corresponding signatures in them before warning the driver and relaying the information. Figure 7 shows the number of packets that were sent and lost during the test. In order to check the parking detection tool, one of the cars was parked and turned off. After that, the car was started and when the device synchronized with GPS, it stored and broadcast the geographic coordinates to other devices in its range of emission. Those vehicles receiving this information, which had previously launched the Car Locator application, show the empty parking space on the map.

7. Conclusion

This paper presents an advanced implementation of a tool for deploying VANETs with current devices, called VAiPho. This application encourages the fast development of vehicular networks, which so far have not been possible to implement. It solves the problem of starting and deploying VANETs, involving, at the same time, maximum efficiency policies, information and user security, and minimum cost. Therefore, its development can act as an engine for other innovative projects in ITS.

In order to provide several VANET facilities, VAiPho involves several algorithms and corresponding software that can be run on current devices like smartphones, phablets, or tablets equipped with Wi-Fi Direct and location services. In particular, the main target of VAiPho is the development of both security applications and information services to prevent traffic accidents, enhance traffic management and mobility, improve transport efficiency, and so forth.

According to the experimental analysis, the proposed application can be effectively deployed in urban situations for specific applications using nowadays smartphones. The obtained results show that VAiPho guarantees efficiency and security of communications and is a powerful tool for several VANET applications. This is still a work in progress, so many aspects like the addition of new features and the implementation in other mobile platforms such as iOS and Windows Phone are being now developed.

Acknowledgments

This research was supported by the Spanish MINECO and the FEDER Fund under Projects TIN2011-25452 and IPT-2012-0585-370000.

References

[1] M. Raya and J. P. Hubaux, "The security of VANETs," in *Proceedings of the 2nd ACM International Workshop on Vehicular Ad Hoc Networks (VANET '05)*, pp. 93–94, Cologne, Germany, September 2005.

[2] C. Adler, S. Eichler, T. Kosch, C. Schroth, and M. Strassberger, "Self-organized and context-adaptive information diffusion in vehicular ad hoc networks," in *Proceedings of the 3rd International Symposium on Wireless Communication Systems (ISWCS '06)*, pp. 307–311, Valencia, Spain, September 2006.

[3] S. Panichpapiboon and W. Pattara-Atikom, "Connectivity requirements for a self-organizing vehicular network," in *Proceedings of the IEEE Intelligent Vehicles Symposium*, pp. 968–972, Eindhoven, The Netherlands, June 2008.

[4] L. Wischhof, *Self-organizing communication in vehicular ad hoc networks [Ph.D. thesis]*, University of Hamburg, Hambourg, Germany, 2007.

[5] S. Capkun, L. Buttyán, and J.-P. Hubaux, "Self-organized public-key management for mobile ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 2, no. 1, pp. 52–64, 2003.

[6] H. V. D. Parunak and S. Brueckner, "Stigmergic learning for self-organizing mobile ad-hoc networks (MANET's)," in *Proceedings of the 3rd International Joint Conference on Autonomous Agents and Multiagent Systems (AAMAS '04)*, pp. 1324–1325, New York, NY, USA, July 2004.

[7] Y. Park, Y. Park, and S. Moon, "Anonymous cluster-based MANETs with threshold signature," *International Journal of Distributed Sensor Networks*, vol. 2013, Article ID 374713, 9 pages, 2013.

[8] S. Dornbush and A. Joshi, "StreetSmart traffic: discovering and disseminating automobile congestion using VANET's," in *Proceedings of the IEEE 65th Vehicular Technology Conference Spring (VTC '07)*, pp. 11–15, Dublin, Ireland, April 2007.

[9] L. Buttyán, T. Holczer, and I. Vajda, "On the effectiveness of changing pseudonyms to provide location privacy in VANETs," in *Security and Privacy in Ad-hoc and Sensor Networks*, Lecture Notes in Computer Science, pp. 129–141, Springer, Berlin, Germany, 2007.

[10] X. Zhu, Y. Lu, B. Zhang, and Z. Hou, "A distributed pseudonym management scheme in VANETs," *International Journal of Distributed Sensor Networks*, vol. 2013, Article ID 615906, 9 pages, 2013.

[11] Google Maps, Traffic option, http://maps.google.com.

[12] TomTom, http://www.tomtom.com.

[13] Sygic GPS Navigation, http://www.sygic.com.

[14] Waze, http://www.waze.com.

[15] CityPark, Israel, https://play.google.com/store/apps/details?id=com.citypark.

[16] S. Mathur, T. Jin, N. Kasturirangan et al., "ParkNet: drive-by sensing of road-side parking statistics," in *Proceedings of the 8th ACM/USENIX Annual International Conference on Mobile Systems, Applications and Services (MobiSys '10)*, pp. 123–136, San Francisco, Calif, USA, June 2010.

[17] R. Panayappan, J. M. Trivedi, A. Studer, and A. Perrig, "VANET-based approach for parking space availability," in *Proceedings of the 4th ACM International Workshop on Vehicular Ad Hoc Networks (VANET '07)*, pp. 75–76, Montréal, Canada, September 2007.

[18] G.-Y. Chang, J.-P. Sheu, and C.-Y. Chung, "Zooming: a zoom-based approach for parking space availability in VANET," in *Proceedings of the IEEE 71st Vehicular Technology Conference-Spring (VTC '10)*, Taipei, Taiwan, May 2010.

[19] Car Finder, Android, https://play.google.com/store/apps/details?id=com.slickapps.

[20] Car Finder, iPhone, https://itunes.apple.com/es/app/encuentra-tu-coche-conar/id370836023?mt=8.

[21] D. Jiang and L. Delgrossi, "IEEE 802.11p: towards an international standard for wireless access in vehicular environments," in *Proceedings of the IEEE 67th Vehicular Technology Conference-Spring (VTC '08)*, pp. 2036–2040, Singapore, May 2008.

[22] J. Wu and S.-H. Yang, "SmallWorld model-based polylogarithmic routing using mobile nodes," *Journal of Computer Science and Technology*, vol. 23, no. 3, pp. 327–342, 2008.

[23] J. Molina-Gil, P. Caballero-Gil, and C. Caballero-Gil, "Aggregation and probabilistic verification for data authentication in VANETs," *Information Sciences*, 2013.

[24] NS-2, The Network Simulator, http://isi.edu/nsnam/ns.

[25] SUMO, Simulation of Urban MObility, http://sumo.sourceforge.net.

[26] WAVE, "Wireless access in vehicular environments," IEEE 1609 Working Group, http://vii.path.berkeley.edu/1609_wave/.

[27] P. Caballero-Gil, C. Caballero-Gil, and J. Molina-Gil, "VAiPho—VANET application for mobile phones to avoid traffic jams," PCT/ES2011/000220, University of La Laguna, Spain, 2010, http://www.vaipho.com.