# Secure V2V Communication with Identity-based Cryptography from License Plate Recognition

Tudor Andreica and Bogdan Groza
Faculty of Automatics and Computers, Politehnica University of Timisoara, Romania
Email: andreica_tudor@yahoo.com, bogdan.groza@aut.upt.ro

***Abstract*—The deployment of secure vehicle-to-vehicle communication is essential for recent technologies such as autonomous driving and traffic optimizations. In this paper we experiment with the use of license plates as a mean to identify vehicles and use this identification number to bootstrap security based on identity-based cryptographic schemes. Since the deployment of the public-key infrastructure may be difficult at a large scale for the automotive environment, the use of identity-based cryptography may offer benefits since it does not require public-key certificates. We present experiments based on Android smartphones in order to determine the feasibility of deploying this technology. Our experiments are concerned with both the impact of the underlying cryptographic primitives and the range at which license plates can be recognized by smartphone cameras.**

***Index Terms*—V2V Communication, Identity-based cryptography, Security**

## I. Introduction and motivation

With the use of electronic units and smart devices, the automotive environment has changed dramatically and will likely remain in a continuous change for the upcoming years. Modern cars contain dozens of electronic control units (ECUs) with various functions, ranging from safety to entertainment. Step by step, vehicles are turning into moving computers and car manufacturers have to invest massively in new trends. One of the mega-trends in the automotive world is autonomous driving. It is expected that in the upcoming years the roads will host self-driven cars, which do not require any human inputs for driving and controlling the car. But to achieve the highest level of autonomy, vehicles need to be equipped with different types of sensors and cameras that sense the environment and perceive surroundings. In addition, inter-vehicle communication will help cars to have a complete overview of their surroundings. By using car-to-car communication technologies, vehicles can exchange useful information, including various warnings, e.g., blind-spot warning, collision warning, etc. In this context, a significant concern for the inter-vehicle communication is to ensure security. Potential attack surfaces in connected cars are discussed in [17].

Without proper security mechanisms, malicious attacks can lead to catastrophic situations. Moreover, the proposed security schemes need to consider numerous constraints such as limited computing power and bandwidth in case of wireless communications. Nonetheless, since the public-key infrastructure (PKI) is not universally adopted it is also hard to bootstrap security in V2V (vehicle-to-vehicle) communication. In this paper, we propose the use of identity-based cryptography with vehicle identities extracted from license plates, i.e., registration plates. Identity-based cryptography was proposed long ago in order to remove the need for public-key certificates [22]. We find such a solution to be more convenient for the addressed scenario. Our experimental setup, which consists of two smartphones and a car, is depicted in Figure 1. We discuss more on existing technologies, the scenarios that we address and related work next.

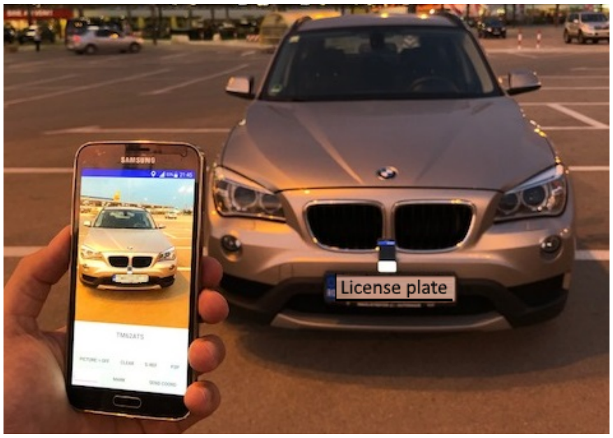


Fig. 1: The smartphones and the car from our experiments

### A. Context and related work

*Vehicle-to-everything (V2X)* communication is the technology that enables a vehicle to exchange information with other smart entities, such as road units, pedestrians or other traffic participants. V2X is a communication system that includes further more specific communication types as vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), vehicle-to-pedestrian (V2P) or vehicle-to-grid (V2G). As the infrastructure for V2X is not fully available, in our work, we consider only the first communication type (V2V) which is mediated by smartphones in our practical setup.

For our scenario, we consider two types of vehicular communication which are described next. *Inter-vehicle communication* is the communication type where a vehicle exchanges messages with other vehicles that are located in the immediate vicinity. However, if the distance between cars is too large, communication may not be possible. In particular, since we use license plate recognition, the cars may not be in sight. Thus, the second type of communication is the *routing-based* *communication* which covers the previous drawback. This type of communication, offers the possibility for two cars, that are at a distance, to exchange information by the use of an intermediate node. In this scenario, other cars will route the messages toward the recipient.

Due to the prime importance of security in V2X communication, there are many research works and projects that focus on this topic. We discuss next examples of such research on the development of security for inter-vehicular communications. A phone-to-phone communication system based on Wi-Fi interface is described in [26]. The authors presented a phone-based communication scheme that can be used in V2V communication and makes use only of the already existing smartphones capabilities. Secure Vehicular Communication (SeVeCom) [13] was a project whose aim was to define and implement security requirements for the inter-vehicle communications. Another research project focusing on security aspects of V2X communications was Open Vehicular Secure Platform project (OVERSEE) [7]. The OVERSEE team provided a secure and open in-vehicle platform which offers isolation between independent applications (including V2X applications) and protects the vehicle against potential failures and attacks. Preparing Secure Vehicle-To-X Communication Systems (PRESERVE) [24] was another project targeting the security of V2X communications.

Furthermore, being a critical topic, security in V2X is also considered in various research papers. A survey on security challenges in Vehicle Ad hoc Networks (VANETs) is described in [4]. Several issues, cyber security standards and concepts for V2X and V2V communications are presented in [10], [15], [20]. Threats to availability, authenticity and confidentiality in VANETs and possible attacks were discussed in [31], [28]. In [31] a survey on the results obtained in recent research works is presented, focusing on security and other key areas of VANETs. Moreover, the authors describe some recent VANET deployments in European Union, US and Japan. Security aspects in the connected cars with focus on the In-Vehicle Network were discussed in [12]. An adaptive safety/security approach was proposed in [29]. The authors considered jointly the security, safety and performance issues of the connected cars. A session key establishment protocol for inter-vehicle communication based on a blockchain public key infrastructure and side-channels (visual and audio) is proposed in [19]. A blockchain-based security framework for connected and autonomous vehicles is presented in [18]. Security concepts based on group signatures schemes for vehicle communications are considered in [8], [3]. A comprehensive survey on pseudonym schemes in VANETs can be found in [16]. Identity-based cryptography is also proposed in several works as potential security solution for vehicular communications. A survey that addresses the use of Identity-Based schemes in vehicular ad-hoc network is in [23].

Sun et al. [27] suggest a security protocol for vehicular communication which relies on group signatures and identity-based signatures. Their proposal consists in using group signatures for the V2V communication and identity-based signatures for the communication between vehicles and Roadside Units (RSUs). Other proposals for identity-based security systems in VANETs are presented in [2], [25], [11]. In [32] an identity-based signature with batch verification is presented, which significantly improves the speed performance of the signature verification procedure since traffic participants can verify multiple signatures at the same time. Adopting cryptographic security leads to many challenges related to computational power and bandwidth, a good overview can be found in [21].

## II. Scenarios and proposed solution

We begin with a description for some scenarios that we consider relevant and are addressed by our work. Then we discuss the communication interfaces and the setup components that we used in our work. Finally, we detail the cryptographic primitives and our protocol design.

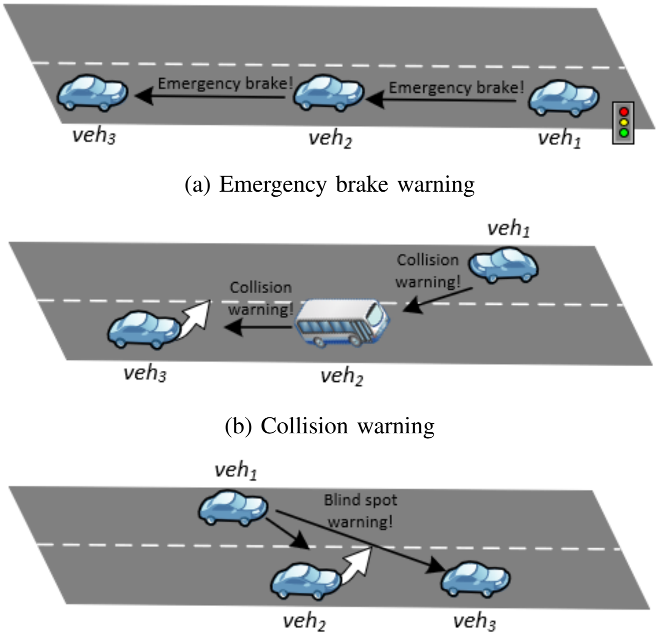
### A. Addressed scenarios

The US Department of Transportation has described in [9] some of the safety related scenarios which may immediate benefit from V2V communication. We also consider these scenarios as a starting point in our work. A graphical depiction is given in Figure 2. We give a brief description of them in what follows:

1) The first scenario, described in Figure 2a, accounts for the situation when a driver needs to brake suddenly. Sending an emergency brake warning message toward the vehicle from behind can save precious time (up to a few seconds), which can be used by the receiver car to start the braking earlier. Time may be crucial for the car that receives the warning to stop successfully and avoid a collision. Subsequent to the reception of a warning message, a car can forward the warning to the other cars from behind, decreasing the possibility of a crash.
2) Overtaking can be a dangerous procedure depending on conditions. Figure 2b illustrates a situation where a driver wants to overtake the car in front but does not observe that another vehicle is coming on the opposite lane. In this situation, $veh_1$ can easily send a warning message to $veh_2$, which in turn, transmits the message further toward $veh_3$.
3) The third scenario targets the blind spots that may appear whenever a driver wants to change the driving lane. As depicted in Figure 2c, the vehicle driving on the overtaking lane, can notify the other vehicles of its presence, thus avoiding the possibility of a crash that may happen due to a blind spot.

### B. Communication interfaces

In our protocol and experiments we have chosen Wi-Fi Direct as communication technology between devices. Wi-Fi is a radio technology which relies on the IEEE 802.11 set of protocols and offers high speed data communication. There are several modes and versions of Wi-Fi. One of them is Wi-Fi Direct which enables devices to connect directly without



(a) Emergency brake warning

(b) Collision warning

(c) Blind spot warning

Fig. 2: Some warning scenarios that we consider based on [9]

requiring a wireless access point or router and it offers the possibility to communicate at typical Wi-Fi speeds. A further benefit of Wi-Fi Direct is that for a peer-to-peer connection, which can be used for direct data transfer between devices, only one of the participating devices has to be Wi-Fi Direct compliant. In order to be compliant with Wi-Fi Direct, a device needs to embed a software enabled access point (Soft AP), which permits the device to act like a host. This means that if other devices get in the Wi-Fi Direct range of the host, they can easily connect to it and start the communication procedure. Starting with Android 4.0, Google introduced support for the Wi-Fi Direct technology, offering the possibility for developers to use Wi-Fi Direct in their developed Android applications. However, for now, Android does not support Wi-Fi ad-hoc mode. This is an inconvenience because we consider the ad-hoc mode as essential in the V2V communication. We discuss more later on how we implemented Wi-Fi Direct communication in our application. We also provide measurements results with respect to the time required by two smartphones to establish a Wi-Fi Direct communication session.

Since Wi-Fi Direct can have some impediments as a solution for V2V communication, we consider that other alternatives, such as wireless mobile telecommunication technology, may be a good choice. These technologies were already taken into consideration for inter-vehicular communications [1], [30]. 5G technology for direct V2V communication is discussed in [14]. Several companies from the automotive and telecommunication industries have founded the 5G Automotive Association (5GAA)[1] whose aim is to offer solutions for the future mobility services. The 5G is considered as a key technology to support V2X communications.

### C. Setup components

For our experimental setup we have used two Android based smartphones. The reason for choosing smartphones is that they are ubiquitous inside cars, their capabilities are comparable to the in-vehicle infotainment units and they were easily available to us. Modern vehicles are equipped with high-performance cameras which can be used for this purpose. So, the proposed technology can be ported without problems to in-vehicle cameras.

The first smartphone that we used is a Samsung Galaxy S5 with a Quad-core 2.5 GHz Krait 400 CPU, 16 GB of flash memory, 2 GB RAM, 16 Megapixels main camera, it runs Android 6.0.1 and is compliant with Wi-Fi Direct. The second smartphone is a Samsung Galaxy S7, which is also compliant with Wi-Fi Direct, and is equipped with a Octa-core (4x2.3 GHz Mongoose & 4x1.6 GHz Cortex-A53) CPU, 32 GB of flash memory, 4 GB of RAM, 12 Megapixels main camera and has Android 7.0 as operating system. Table I provides an overview for the specifications of the devices that we used in our experiments.

### D. Cryptographic protocol

As stated in the introductory section, our protocol relies on identity-based primitives. Regular cryptographic schemes, e.g., RSA, can be used to bootstrap authentication and confidentiality in V2V communications, but the management of cryptographic public-keys remains a challenging task. Identity-based cryptography may be a suitable choice for securing inter-vehicle communications as it can ease the handling of the cryptographic keys. The main advantage of the identity-based schemes is that the public keys of the parties can be computed using their identification information. This information is a publicly known string that can represent an email address, an IP address, an unique identification number, etc. We consider that license plates can be used as identities for vehicles and derive keys from them for the underlying cryptographic algorithms.

However, given the fact that in V2X communication a vehicle needs to transmit approximately 10 safety messages per second, the performance of the cryptographic schemes is a critical concern. Therefore, as identity-based schemes will not satisfy the timing constraints, they will be used to establish a symmetric session key when two cars get within the communication range. The symmetric key can be further used to assure authentication at a faster rate. In order to establish a shared key between two parties, we chose to build our protocol on the station-to-station (STS) protocol, described by Diffie et al. in [6]. This protocol relies on the Diffie-Hellman key-exchange [5]. As expected, we change the signature in it with an identity-based signature to avoid the need for a public-key certificate. Also we renounce to the encryption of the signature since we are not interested in keeping the communication anonymous (this can be changed according to specific needs).

[1] https://5gaa.org/

TABLE I: Devices used in our experiments

| Device | Android | CPU | Memory | WLAN | GPS | Main camera |
|---|---|---|---|---|---|---|
| Samsung S5 | 6.0.1 | Quad-core<br>2.5 GHz<br>Krait 400 | 16 GB,<br>2 GB RAM | Wi-Fi 802.11 a/b/g/n/ac, dual-band, Wi-Fi Direct, hotspot | GPS with A-GPS, GLONASS, BDS | 16 MP, f/2.2, 31mm (standard), 1/2.6", 1.12um, PDAF |
| Samsung S7 | 7.0 | Octa-core<br>(4x2.3 GHz Mongoose &<br>4x1.6 GHz Cortex-A53) | 32 GB,<br>4 GB RAM | Wi-Fi 802.11 a/b/g/n/ac, dual-band, Wi-Fi Direct, hotspot | GPS with A-GPS, GLONASS, BDS | 12 MP, f/1.7, 26mm (wide), 1/2.55", 1.4µm,<br>dual pixel PDAF, OIS |

In what follows, we detail the protocols that has to be executed between vehicles in order to establish a communication session. We consider two distinct situations that need to be treated in a different manner. The first situation implies the connection between two vehicles that are within range (both visually to make license plate recognition feasible and to establish a wireless connection). For the second situation, we consider that vehicles that are not close enough for the first scenario, can communicate using a common neighbour car which plays the role of a router. In order to start a communication session, both vehicles need to be connected to the vehicle that performs the routing procedure. For example, this situation may occur in the scenario depicted in Fig 2a. We consider that a car which already has a connection with another, can request information about other vehicles that are in the vicinity of its peer. Thus, a vehicle is informed about other vehicles that are not within its communication range and has the possibility to start a communication session with them. However, for both situations, the aim of the protocols is to establish a symmetric session key between two parties, thus, enabling them to use symmetric building blocks for a secure communication.

*Handshake in the two-vehicle-scenario.* The handshake procedure is graphically depicted in Figure 3. The procedure starts when two vehicles get in the communication range. The first vehicle, i.e., $veh_1$, that initiates the communication with the other vehicle, i.e., $veh_2$, reads $veh_2$'s license plate, generates a random value $x$ and sends the Diffie-Hellman key-share $\alpha^x$ toward $veh_2$. The message is signed by $veh_1$ with an identity-based signature scheme (IBS), i.e., $s'_{veh_1} = \mathsf{IBS}(\mathrm{sk}_{veh_1}, m'_{veh_1})$. The signature is performed using $veh_1$'s secret key $\mathrm{sk}_{veh_1}$. Vehicle $veh_2$ reads $veh_1$'s license plate, and, based on this, derives its public key and verifies the received signature. Subsequent, $veh_2$ generates a random number $y$ and computes the symmetric session key $\mathrm{K}_{ses} = \alpha^{xy}$. Using the session key, $veh_2$'s information (e.g. GPS coordinates, vehicle speed, etc.) together with the recipient's license plate number are encrypted and concatenated to $\alpha^y$ that are transmitted back toward $veh_1$. This message is accompanied by $veh_2$'s identity-based signature, performed on the current message and the previously received one, i.e. $s_{veh_2} = \mathsf{IBS}(\mathrm{sk}_{veh_2}, m'_{veh_1}, m_{veh_2})$ . In the last step, $veh_1$ verifies the received signature, computes the session key $\mathrm{K}_{ses}$ and decrypts the received information. Afterward, a reply for $veh_2$ is prepared. The session key is used to encrypt $veh_1$'s information, a timestamp and the recipient's license plate number, which subsequently are used as inputs for the signing procedure that is performed using a Message Authentication Code (MAC) algorithm and the session key. Eventually, the message is send to $veh_2$ and at this point, the communication session can go on, using only the symmetric schemes, i.e. similar to step 3.

**I) Handshake in the two-vehicle scenario**

$veh_1 \Rightarrow veh_2$: *read license plate*

1. $veh_1 \rightarrow veh_2$: $m'_{veh_1} = \{\alpha^x\}$,

$$s'_{veh_1} = \mathsf{IBS}(\mathrm{sk}_{veh_1}, m'_{veh_1})$$

$veh_2 \Rightarrow veh_1$: *read license plate*

2. $veh_2 \rightarrow veh_1$:

$$m_{veh_2} = \{\alpha^y, \{\mathrm{info}_{veh_2}, \mathrm{LP}_{veh_1}\}_{\mathrm{K}_{ses}}\},$$

$$s_{veh_2} = \mathsf{IBS}(\mathrm{sk}_{veh_2}, m'_{veh_1}, m_{veh_2})$$

3. $veh_1 \rightarrow veh_2$: $m''_{veh_1} = \{\mathrm{info}_{veh_1}, \mathrm{T}_{veh_1}, \mathrm{LP}_{veh_2}\}_{\mathrm{K}_{ses}}$,

$$s''_{veh_1} = \mathsf{MAC}(\mathrm{K}_{ses}, m''_{veh_1})$$

Fig. 3: Protocol procedures for handshake in two-vehicle scenario

*Handshake for the routing based scenario (three vehicles).* The steps of the handshake are suggested in Figure 4. We assume that $veh_1$ is connected with $veh_2$ and they exchange messages. They can share information which may include lists with the other vehicles that are in their vicinity and are connected to them. Thus, e.g., $veh_2$ sends to $veh_1$ a list of vehicles ($veh_i$ for $i = 1, ..., n$) that are connected to $veh_2$. In addition to the vehicle list, further information about each of the vehicle, such as GPS position and the probable trajectory, can be send. Based on this information, $veh_1$ can request to $veh_2$ to intermediate a handshake between $veh_1$ and one of the vehicles $veh_i$ from the received list, in order to establish a communication session. In this context, $veh_2$ transmits towards $veh_1$ an encrypted message with their shared symmetric session key $\mathrm{K}_{ses_{12}}$ which includes the license plate number of $veh_i$ ($\mathrm{LP}_{veh_i}$). The message is authenticated with a MAC, i.e., $s'_{veh_2} = \mathsf{MAC}(\mathrm{K}_{ses_{12}}, m'_{veh_2})$. Subsequent to the message reception, $veh_1$ generates a random number $x$ and sends back the exponential $\alpha^x$, signed with an identity-based signature as $s'_{veh_1} = \mathsf{IBS}(\mathrm{sk}_{veh_1}, m'_{veh_1})$. Vehicle $veh_2$ receives the message and appends to it the encrypted license plate number of $veh_1$. The new message is authenticated using a MAC, which is generated with the session key $\mathrm{K}_{ses_{2i}}$ (that is shared between $veh_1$ and $veh_i$), and is sent towards $veh_i$. The later generates a random value $y$ and computes the symmetric session key as $\mathrm{K}_{ses_{1i}} = \alpha^{xy}$. Further, $veh_i$ computes the exponential $\alpha^y$ and adds its vehicle information and the recipient's license plate number in an encrypted form. The message is transmitted back to $veh_2$ accompanied by $veh_i$'s identity-based signature, computed over the current message and the previous received message. Vehicle $veh_2$ will forward the received message toward $veh_1$, but before transmission, a MAC is computed and attached to the message, i.e. $s'''_{veh_i} = \mathsf{MAC}(\mathrm{K}_{ses_{12}}, m'''_{veh_2})$. The session key that is to be shared between $veh_1$ and $veh_i$ is now computed also by $veh_1$. The key is used to encrypt $veh_1$'s information together with a timestamp and the recipient's license plate and finally to compute a MAC over the previous data. As the message will be routed towards $veh_i$ by $veh_2$, an additional MAC using $\mathrm{K}_{ses_{12}}$ is performed. In a final step, $veh_2$ forwards the received message towards $veh_i$, and in this moment a communication session is established between $veh_1$ and $veh_i$.

## III. Implementation and results

In this section we discuss experimental result concerning license plate recognition and computational performance for the underlying cryptographic primitives.

### *A. Recognizing license plates and exchanging data*

We have implemented an Android application which can be used to read license plates and communicates using Wi-Fi Direct with other devices. For the license plate recognition, we used the Mobile Vision API [2] which offers the possibility to find objects in photos and videos. The framework provides several APIs and subpackages, but for our needs we have used only the text detector. The text recognition API may be used to read blocks of text using a smartphone's camera. For our purposes, we take into consideration only the texts which satisfy the license plate text format from our country. Therefore, we have added a filter which checks for text patterns that are used for the license plates from our country, but it can be easily changed to include text patterns from other countries as well. So, in our experiments, only the character groups that were composed of two letters, two digits and three letters (e.g. AC12XYZ) were passing the filter. In this way, we were able to read the license plates and avoid the unintended reading of other texts.

**II) Handshake in routing based scenario (three vehicles)**

$veh_2 \to veh_1$: *list of vehicles from* $veh_2$ *vicinity*

$veh_1 \to veh_2$: *request handshake with* $veh_i$

1. $veh_2 \to veh_1$: $m'_{veh_2} = \{\mathrm{LP}_{veh_i}\}_{\mathrm{K}_{ses_{12}}}$,
$$s'_{veh_2} = \mathsf{MAC}(\mathrm{K}_{ses_{12}}, m'_{veh_2})$$
2. $veh_1 \to veh_2$: $m'_{veh_1} = \{\alpha^x\}$,
$$s'_{veh_1} = \mathsf{IBS}(\mathrm{sk}_{veh_1}, m'_{veh_1})$$
3. $veh_2 \to veh_i$:
$$m''_{veh_2} = \{m'_{veh_1}, s'_{veh_1}, \{\mathrm{LP}_{veh_1}\}_{\mathrm{K}_{ses_{2i}}}\},$$
$$s''_{veh_2} = \mathsf{MAC}(\mathrm{K}_{ses_{2i}}, m''_{veh_2})$$
4. $veh_i \to veh_2$: $m_{veh_i} = \{\alpha^y, \{\mathrm{info}_{veh_i}, \mathrm{LP}_{veh_1}\}_{\mathrm{K}_{ses_{1i}}}\}$,
$$s_{veh_i} = \mathsf{IBS}(\mathrm{sk}_{veh_i}, m'_{veh_1}, m_{veh_i})$$
5. $veh_2 \to veh_1$: $m'''_{veh_2} = \{m_{veh_i}, s_{veh_i}\}$,
$$s'''_{veh_i} = \mathsf{MAC}(\mathrm{K}_{ses_{12}}, m'''_{veh_2})$$
6. $veh_1 \to veh_2$:
$$m''_{veh_1} = \{\{\mathrm{info}_{veh_1}, \mathrm{T}_{veh_1}, \mathrm{LP}_{veh_i}\}_{\mathrm{K}_{ses_{1i}}},$$
$$\mathsf{MAC}(\mathrm{K}_{ses_{1i}}, \{\mathrm{info}_{veh_1}, \mathrm{T}_{veh_1}, \mathrm{LP}_{veh_i}\}_{\mathrm{K}_{ses_{1i}}}\},$$
$$s''_{veh_1} = \mathsf{MAC}(\mathrm{K}_{ses_{12}}, m''_{veh_1})$$
7. $veh_2 \to veh_i$: $m^{iv}_{veh_2} = \{m''_{veh_1}\}$,
$$s^{iv}_{veh_2} = \mathsf{MAC}(\mathrm{K}_{ses_{2i}}, m^{iv}_{veh_2})$$

Fig. 4: Protocol procedures for handshake in three-vehicle scenario

As communication protocol we chose to use Wi-Fi Direct. Hence, for our implementation, we have used the Android's Wi-Fi peer-to-peer (P2P) framework [3], which complies with Wi-Fi Direct. For the connection between the smartphones we made use of the smartphones names which are displayed when devices have Wi-Fi Direct enabled. In our application, the smartphone continuously scans for other available Wi-Fi peers. When a known peer is found in the list, the smartphone initiates the connection procedures and tries to connect to the respective peer. Normally, when a user receives a connection request from another device, the user needs to accept the connection, otherwise the connection cannot be established. The need of human interaction while establishing Wi-Fi Direct connections was a drawback for our scenario. We managed to

[2] https://developers.google.com/vision/

[3] https://developer.android.com/training/connect-devices-wirelessly/wifi-direct

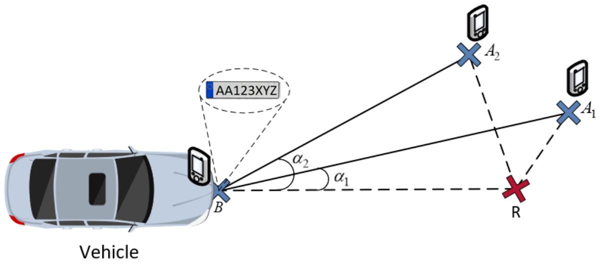


Fig. 5: Angle calculation

overcome it by using a Java Class, available on Github [4], that can intercept approval requests and accept or decline them, before the user is notified. Hence, we managed to establish Wi-Fi peer-to-peer connections without any human interaction. Subsequent to a successful connection, for data exchange, we have used regular Java sockets.

We conducted experiments in order to establish the distance at which license plates can be read. For this, we used two smartphones. We placed the first one on the car, above the front license plate, and used the second smartphone to read the license plate. Subsequent to a successful license plate reading, the license plate number, along with the GPS location and the zooming value were sent via Wi-Fi Direct to the smartphone that was placed on the car. Next, the received GPS location was used in conjunction with the location of the receiver smartphone to compute the distance between the two devices. The GPS location point consists of the latitude and longitude coordinates. In order to compute the distance between two GPS points, we have used the *great-circle distance* formula. So, we computed distances in the following way:

$$distance = acos(sin\varphi_1 \cdot sin\varphi_2 + cos\varphi_1 \cdot cos\varphi_2 \cdot cos\Delta\lambda) \cdot R$$

where $\varphi_1$, $\lambda_1$ and $\varphi_2$, $\lambda_2$ are the latitude and longitude in radians of two points, $\Delta\lambda$ is the absolute difference between $\lambda_1$ and $\lambda_2$ and $R$ is earth's radius ($\approx$ 6371 km).

Further, we considered important to measure in our experiments the angle at which the license plates were read and recognized. The procedure for computing the angles is depicted in Figure 5. For computing the angle, we used an additional point, that must be located exactly on the same line with the car, being collinear with the points corresponding to the front and rear license plates. Thus, taking into consideration the first point which is the car's location, the second point, which is the user's location and the reference point, a triangle is created. We determined the distance between the three points ($A_1$, $B$ and the reference point $R$) and then we computed the angle $\alpha_1$ which has been formed between the two edges of the triangle, i.e., the edge from $B$ to $A_1$ and the edge from point $B$ to $R$. When performing a new reading, e.g., from point $A_1$, the same procedure is done, with the only difference that point $A_1$ is swapped with $A_2$. All the computations were performed by the device corresponding to point $B$. The reference point is set up prior to license plate readings, using the same smartphone. We added the option in our Android application to define a reference point. The steps to set up a reference point are very simple, i.e., the user must go to the desired point and press a button in the application. Then the smartphone sends the GPS coordinates to the other smartphone which marks the received point as reference point and uses it in the angles computations.

### B. Experiments on distance for license plate recognition

One specific target of our analysis is to establish the reading accuracy. The results are presented in Table II. We have calculated the reading accuracy, taking into consideration the distance at which the license plates were read. We have analyzed both smartphones, as they are equipped with different cameras. Our expectations were to obtain dissimilar results. Based on the numbers, Samsung S5 has an overall better reading accuracy than S7. S5 performed better the readings at a distance higher than 25 meters, while S7 won at lower distances. In Figure 6 we depict the distances and the zooms at which the readings were performed. The blue points correspond to the Samsung S5 while the red points correspond to the Samsung S7 smartphone. All the readings were performed during daylight in good weather condition. There are many factors which can influence the accuracy of the readings. Finally, besides the distance at which the readings were performed we have also computed the angle at which the license plates were read. The results are depicted in Figure 7. Samsung S5 performed readings at a distance up to 50 meters. The maximum angles at which the license plate could be read were up to 60 degrees. On the other side, though S7 had inferior results in terms of distance, reaching a maximum distance of 42 meters, it improves with readings at angles of almost 75 degrees.

TABLE II: Accuracy of license plates readings

| **Device** | **Accuracy** | | | **Total no. of readings** |
|---|---|---|---|---|
| | Overall | <25 meters | 25–50 meters | |
| Samsung S5 | 89.90 % | 85.15 % | 94.85 % | 198 |
| Samsung S7 | 75.38 % | 90.00 % | 56.14 % | 264 |

### C. Experimental results on computational performance

We implemented Shamir's identity-based signature scheme [22] in Android Studio and ran it on our devices to evaluate its execution speed. We used a 2048-bit key for the signature scheme. In addition to the identity-based signature we have evaluated also HMAC-SHA256, as MAC schemes were considered in our protocol. The results are presented in Table III. As we expected, Samsung S7 has outperformed Samsung S5 with a significant difference. S7 needed an average time of 2.42 ms and 1.18 ms to perform the operations of signing, respectively verification, while S5 required an average time of 12.09 ms for the signing procedure and 9.50 ms for the verification procedure. For the HMAC computation, the difference is smaller. S5 needs approximately 0.22 ms for calculation while S7 performs the computations in 0.12 ms.

[4] https://github.com/mdabbagh88/alljoyn_java

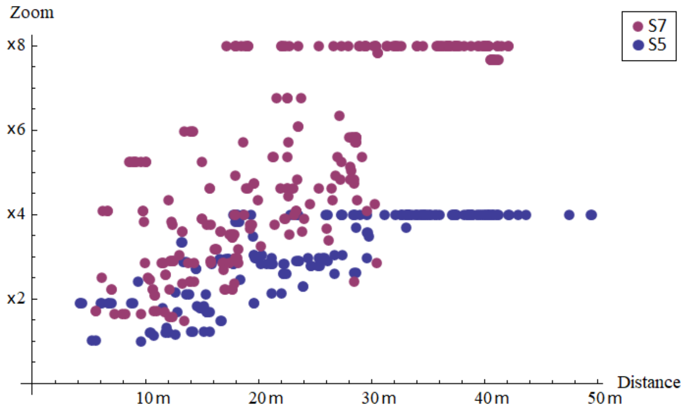


Fig. 6: Distances at which the license plates were read and the needed camera zoom

TABLE III: Execution time of the Shamir signature on the evaluated devices

| Device | Operation | | |
|---|---|---|---|
| | Shamir IBS Sign | Shamir IBS Ver | HMAC-SHA256 |
| Samsung S5 | 12.09 ms | 9.50 ms | 0.22 ms |
| Samsung S7 | 2.42 ms | 1.18 ms | 0.12 ms |

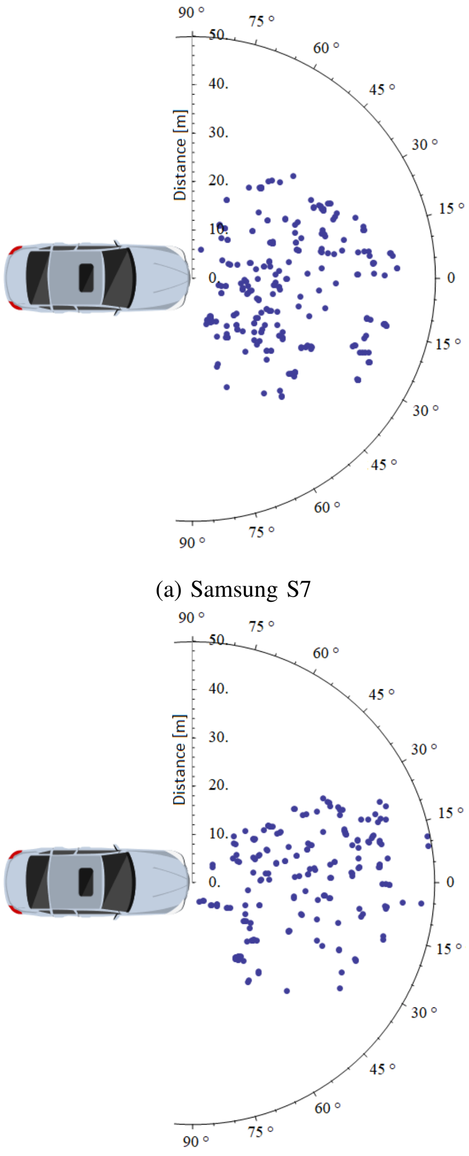
We have also evaluated the required time to establish a Wi-Fi Direct communication session. In order to establish a communication session, our Android application searches for the available Wi-Fi Direct enabled devices which are within range and when a known smartphone is discovered, the connection procedure is started. In our measurements, we have examined the required time between the moment when a device starts the discovery procedure until the moment in which the connection with another device is established. We have also included the time needed to connect to a known peer once it was discovered. The results are shown in Table IV. The first row contains the measurements in the situation in which S5 started the connection procedure and has connected to S7, while the situation from the second row is vice versa.

TABLE IV: Required time to establish a Wi-Fi direct communication session

| | Connection w/o discovery | Connection with discovery |
|---|---|---|
| S5 - S7 | 14.65 ms | 3550.42 ms |
| S7 - S5 | 51.39 ms | 2481.28 ms |

## IV. Conclusions

Identity-based signatures, with identities extracted from vehicle license plates, remove the need for the PKI and certificates that are harder to manage. Our experimental results show that identification based on license plate number can be done with high accuracy at a range of around 50 meters. This of course depends on the quality of the smartphone camera, e.g., sensor and lens. Computational requirements are within reach for modern smartphones in case of basic communication scenarios. If the number of participants is high or the vehicles status reports need to be send too often, then symmetric-key primitives may be the only alternative. Clearly, more investigations will be needed in this direction which we leave as potential future work.



(a) Samsung S7

(b) Samsung S5

Fig. 7: Distances and angles at which licence plates were read

**Acknowledgments.** This work was supported by a grant of Ministry of Research and Innovation, CNCS-UEFISCDI, project number PN-III-P1-1.1-TE-2016-1317, within PNCDI III (2018-2020).

## References

[1] G. Araniti, C. Campolo, M. Condoluci, A. Iera, and A. Molinaro. Lte for vehicular networking: a survey. *IEEE Communications Magazine*, 51(5):148–157, 2013.

[2] G. Baldini, V. Mahieu, I. N. Fovino, A. Trombetta, and M. Taddeo. Identity-based security systems for vehicular ad-hoc networks. In *2013 International Conference on Connected Vehicles and Expo (ICCVE)*, pages 672–678. IEEE, 2013.

[3] B. K. Chaurasia, S. Verma, and S. Bhasker. Message broadcast in vanets using group signature. In *2008 Fourth International Conference on Wireless Communication and Sensor Networks*, pages 131–136. IEEE, 2008.

[4] A. Y. Dak, S. Yahya, and M. Kassim. A literature survey on security challenges in vanets. *International Journal of Computer Theory and Engineering*, 4(6):1007, 2012.

[5] W. Diffie and M. Hellman. New directions in cryptography. *IEEE transactions on Information Theory*, 22(6):644–654, 1976.

[6] W. Diffie, P. C. Van Oorschot, and M. J. Wiener. Authentication and authenticated key exchanges. *Designs, Codes and Cryptography*, 2(2):107–125, 1992.

[7] A. Groll, J. Holle, M. Wolf, and T. Wollinger. Next generation of automotive security: secure hardware and secure open platforms. 2010.

[8] J. Guo, J. P. Baugh, and S. Wang. A group signature based secure and privacy-preserving vehicular communication framework. In *2007 Mobile Networking for Vehicular Environments*, pages 103–108. IEEE, 2007.

[9] J. Harding, G. Powell, R. Yoon, J. Fikentscher, C. Doyle, D. Sade, M. Lukuc, J. Simons, J. Wang, et al. Vehicle-to-vehicle communications: readiness of v2v technology for application. Technical report, United States. National Highway Traffic Safety Administration, 2014.

[10] I. Ivanov, C. Maple, T. Watson, and S. Lee. Cyber security standards and issues in v2x communications for internet of vehicles. 2018.

[11] P. Kamat, A. Baliga, and W. Trappe. An identity-based security framework for vanets. In *Proceedings of the 3rd international workshop on Vehicular ad hoc networks*, pages 94–95. ACM, 2006.

[12] P. Kleberger, T. Olovsson, and E. Jonsson. Security aspects of the in-vehicle network in the connected car. In *2011 IEEE Intelligent Vehicles Symposium (IV)*, pages 528–533, 2011.

[13] T. Leinmüller, L. Buttyan, J.-P. Hubaux, F. Kargl, R. Kroh, P. Papadimitratos, M. Raya, and E. Schoch. Sevecom-secure vehicle communication. Technical report, 2006.

[14] J. Lianghai, M. Liu, A. Weinand, and H. Schotten. Direct vehicle-to-vehicle communication with infrastructure assistance in 5g network. 08 2017.

[15] X. Lin, R. Lu, C. Zhang, H. Zhu, P.-H. Ho, and X. Shen. Security in vehicular ad hoc networks. *IEEE communications magazine*, 46(4):88–95, 2008.

[16] J. Petit, F. Schaub, M. Feiri, and F. Kargl. Pseudonym schemes in vehicular networks: A survey. *IEEE Communications Surveys Tutorials*, 17(1):228–255, 2015.

[17] J. Petit and S. E. Shladover. Potential cyberattacks on automated vehicles. *IEEE Transactions on Intelligent Transportation Systems*, 16(2):546–556, 2015.

[18] G. Rathee, A. Sharma, R. Iqbal, M. Aloqaily, N. Jaglan, and R. Kumar. A blockchain framework for securing connected and autonomous vehicles. In *Sensors*, 2019.

[19] S. Rowan, M. Clear, M. Gerla, M. Huggard, and C. M. Goldrick. Securing vehicle to vehicle communications using blockchain through visible light and acoustic side-channels. *arXiv preprint arXiv:1704.02553*, 2017.

[20] M. Saed, S. Bone, and J. Robb. Security concepts and issues in intra-inter vehicle communication network. In *Proceedings of the International Conference on Security and Management (SAM)*, page 1. The Steering Committee of The World Congress in Computer Science, Computer …, 2014.

[21] T. Schütze. Automotive security: Cryptography for car2x communication. In *Embedded World Conference*, volume 3, pages 4–24. Citeseer, 2011.

[22] A. Shamir. Identity-based cryptosystems and signature schemes. In *Workshop on the theory and application of cryptographic techniques*, pages 47–53. Springer, 1984.

[23] N. I. Shuhaimi and T. Juhana. Security in vehicular ad-hoc network with identity-based cryptography approach: A survey. In *2012 7th International Conference on Telecommunication Systems, Services, and Applications (TSSA)*, pages 276–279. IEEE, 2012.

[24] J. P. Stotz, N. Bißmeyer, F. Kargl, S. Dietzel, P. Papadimitratos, and C. Schleiffer. PRESERVE - D1.1 - Security Requirements of Vehicle Security Architecture, June 2010.

[25] J. Sun, C. Zhang, Y. Zhang, and Y. Fang. An identity-based security system for user privacy in vehicular ad hoc networks. *IEEE Transactions on Parallel and Distributed Systems*, 21(9):1227–1239, 2010.

[26] X. Sun, S. Hu, L. Su, T. F. Abdelzaher, P. Hui, W. Zheng, H. Liu, and J. A. Stankovic. Participatory sensing meets opportunistic sharing: Automatic phone-to-phone communication in vehicles. *IEEE Transactions on Mobile Computing*, 15(10):2550–2563, 2015.

[27] X. Sun, X. Lin, and P.-H. Ho. Secure vehicular communications based on group signature and id-based signature scheme. In *2007 IEEE International Conference on Communications*, pages 1539–1545. IEEE, 2007.

[28] P. Tyagi and D. Dembla. Investigating the security threats in vehicular ad hoc networks (vanets): towards security engineering for safer on-road transportation. In *2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, pages 2084–2090. IEEE, 2014.

[29] M. Villarreal-Vasquez, B. Bhargava, and P. Angin. Adaptable safety and security in v2x systems. In *2017 IEEE International Congress on Internet of Things (ICIOT)*, pages 17–24. IEEE, 2017.

[30] A. Vinel. 3gpp lte versus ieee 802.11p/wave: Which technology is able to support cooperative vehicular safety applications? *IEEE Wireless Communications Letters*, 1(2):125–128, 2012.

[31] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan. Vehicular ad hoc networks (vanets): status, results, and challenges. *Telecommunication Systems*, 50(4):217–241, 2012.

[32] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen. An efficient identity-based batch verification scheme for vehicular sensor networks. In *IEEE INFOCOM 2008-The 27th Conference on Computer Communications*, pages 246–250. IEEE, 2008.