Hindawi
Mobile Information Systems
Volume 2017, Article ID 3041749, 13 pages
https://doi.org/10.1155/2017/3041749

Research Article

An Analysis of the Privacy Threat in Vehicular Ad Hoc Networks due to Radio Frequency Fingerprinting

Gianmarco Baldini, Raimondo Giuliani, and Eduardo Cano Pons

European Commission, Joint Research Centre, Ispra, Italy

Correspondence should be addressed to Gianmarco Baldini; gianmarco.baldini@jrc.ec.europa.eu

Received 21 September 2016; Revised 29 December 2016; Accepted 16 January 2017; Published 15 February 2017

Academic Editor: Candelaria Hernández-Goya

In Vehicular Ad Hoc Networks (VANETs) used in the road transportation sector, privacy risks may arise because vehicles could be tracked on the basis of the information transmitted by the Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) communications implemented with the Dedicated Short Range Communications (DSRC) standards operating at 5.9 GHz. Various techniques have been proposed in the literature to mitigate these privacy risks including the use of pseudonym schemes, but they are mostly focused on data anonymization at the network and application layer. At the physical layer, the capability to accurately identify and fingerprint wireless devices through their radio frequency (RF) emissions has been demonstrated in the literature. This capability may generate a privacy threat because vehicles can be tracked using the RF emissions of their DSRC devices. This paper investigates the privacy risks related to RF fingerprinting to determine if privacy breaches are feasible in practice. In particular, this paper analyzes the tracking accuracy in challenging RF environments with high attenuation and fading.

1. Introduction

Road safety has been and remains a high priority in Europe and in July 2010, the European Commission adopted the Policy Orientations for Road Safety 2011–2020, which identified the main strategic objectives to improve road safety. One of the strategic objectives is to promote the deployment of Intelligent Transport Systems (ITS). A considerable amount of work has been done and is still ongoing, with the implementation of the Action Plan for the deployment of Intelligent Transport Systems and the ITS Directive (Directive 2010/40/EU) which provides the legal framework for the deployment of various ITS applications and services across Europe. One of the essential elements of the ITS paradigm is the design and deployment of cooperative wireless networks among the vehicles like V2V and V2I collectively called Vehicle-to-Everything (V2X).

Some ITS applications can only be based on V2V networks because they need to exchange messages among vehicles or they get information from other systems like the Global Navigation Satellite System (GNSS). One example is collision avoidance. Other applications require V2I communications to connect to remote fixed servers and distribute information to the vehicles and their users like road conditions. Finally, some applications require both V2V and V2I networks to exchange information between the fixed infrastructure and vehicles. A list of the applications and the relation to V2X is provided in [1]. One of the most common V2X wireless communication technologies proposed by the industry is the DSRC operating at 5.9 GHz. This paper deals with V2X communication based on ETSI standards, which define two basic messaging services included in the communications stack as a common reusable middleware. These are the Cooperative Awareness Basic Service, defining the Cooperative Awareness Message (CAM), and the Decentralized Environmental Notification Basic Service (DENM). CAM messages are exchanged among ITS stations (e.g., vehicles) to notify their presence, position, and status in a single-hop distance through the wireless channel. Additional details on the ETSI standards are provided in Section 3.

The periodic broadcast of CAM messages from an ITS station (e.g., a vehicle) could potentially endanger the privacy of the drivers of the vehicle, as a malicious eavesdropper could track the vehicles on the basis of the broadcasted CAM messages. As a consequence, support for anonymity in V2X communication is desirable, but it may not be easy to achieve because a certain level of linkability between the messages and the transmitting DSRC device is anyway needed. For example, some applications may require the authentication of the messages to ensure that they come from a trusted entity.

Various anonymization schemes have been proposed in research literature to mitigate privacy risks in VANETs. One of the most common is the adoption of a pseudonym scheme where the real identity of the DSRC device (and consequently the vehicle where it is operating) in the broadcast messages is replaced by a pseudonym. The pseudonym, or pseudonymous credential, allows authentication of a specific entity without knowing the holders' real identity. The use of pseudonyms in VANETs has been proposed by various authors and a recent survey by [2] identifies the most common pseudonyms schemes. On the other side, these schemes are implemented at network or application level and they do not address the issue that the DSRC wireless device can be also identified by its RF emissions.

Extensive research has been performed on the identification of electronic components and systems from their radio frequency emissions. The concept lies in the fact that electronic circuits and RF components (e.g., filters, amplifiers) have unique characteristics acquired in the manufacturing process, which can be detected and extracted by the radio frequency emissions using statistical analysis. The identification of electronic components and systems is called RF fingerprinting or RF-DNA fingerprinting (see [3]) because the intrinsic characteristics of the electronic components can be conceptually associated with the DNA of a human being.

As discussed in the related work section (Section 2) of this paper, the anonymization schemes in VANETs, which have been proposed until now, did not address or investigate the possibility that the DSRC device is identified from its own RF fingerprinting, even if this potential risk has been raised in [2] but not explored further. The goal of this paper is to address this research gap: to evaluate how relevant is the privacy risk derived from the tracking of RF fingerprint of a specific DSRC device (and vehicle) in a road transportation scenario. In particular, we evaluate the accuracy of the identification and verification algorithms in Non-LOS (NLOS) conditions where wireless propagation can be impacted by attenuation and fading effects.

The novelty of this paper in comparison to literature is the following. (1) For the first time, the privacy threat related to RF fingerprinting is investigated for VANETs. (2) For the first time, the RF fingerprinting of DSRC devices at 5.9 GHz is performed. (3) For the first time, the performance of fingerprinting in a fading environment is evaluated for DSRC devices at 5.9 GHz.

The structure of this paper is the following. Section 2 provides a literature review on privacy in Vehicular Ad Hoc Network (VANET) and RF fingerprinting. Section 3 gives a brief overview of the DSRC standard. Section 4 provides a description of the scenario, which could generate privacy threats on the basis of the collected RF fingerprints. Section 5 provides a description of the methodology, the experimental environment, and the algorithms used in this paper to collect the RF emissions, evaluate them, and use them to classify and identify the DSRC devices. In particular, in Section 5, the test bed configuration and the RF receiver (e.g., a software defined radio) are described impersonating the privacy attacker used to collect and process the messages transmitted by the DSRC devices. The test bed configuration includes the parameters used for sampling and filtering. Section 6 provides the results of the evaluation of the privacy risks related to the tracking accuracy on the basis of fading and attenuation effects at the RF level. Finally Section 7 concludes the paper.

2. Related Work

This section describes the related work on the topic of privacy in VANETs and RF fingerprinting.

The issue of privacy in VANETs based on DSRC at 5.9 GHz is related to the fact that the DSRC CAM messages (which will be described in detail in Section 3) are broadcasted by the DSRC module in the vehicle to the neighboring vehicles and road infrastructures stations with a very high frequency. To support vehicle liability and safety in VANETs, any broadcast message from a vehicle must contain a verifiable identity as well as authentic data that may include accurate vehicle location. As a consequence, the message broadcast in VANET can reveal the vehicle's identity or activities by correlating the traversed locations or the start point and end point of the trip. For example, even if the exact identity of a driver is not known during a trip, the end point (e.g., home) can be used to trace the identity of the person and tracking the vehicle can provide hints on his/her activities. To summarize, VANETs represent a very good case study to address privacy risks in mobile communications.

Location privacy protection schemes for mobile networks and more specifically for VANETs can be generally classified as regulatory, policy-based, and anonymity-based approaches as described in [4]. There is already an extensive literature on the privacy mitigation or privacy enhancing techniques for regulatory (e.g., informed consent) and policy-based approaches (see [5]). In this paper we focus on anonymity-based approaches because we investigate privacy risks related to the physical layer.

As described in [4, 6], one of the most popular approaches to protect privacy in mobile networks is based on the concept of pseudonym.

Pseudonym is an identity anonymization technique, where the real identity of the vehicle is replaced by a pseudonym. The pseudonyms are regenerated periodically to avoid tracking by a message receiver in a specific area. In other words, if the vehicle uses the same pseudonym for a long time, the vehicle can be still tracked by an observer by the correlation of the messages (see [6]). In VANETs, pseudonyms can mitigate privacy risks but not completely remove them because the identity of the vehicles could be still determined by other attributes (e.g., color, model) or if the frequency of the messages is not high enough. The appropriate calculation of the frequency of the pseudonyms is still an open research problem as discussed in [2].

Regardless of the pseudonym frequency in the CAM messages broadcasted by the vehicle, the identity of the

DSRC 5.9 GHz device could also be determined through RF fingerprinting.

There has been considerable research activity on the exploitation of RF emissions to uniquely identify and possibly authenticate electronic circuits and components. Most of the surveyed research papers exploit the small but significant differences in the electronic circuits, which impact the RF emissions. These differences are generated during the manufacturing process(es) or the assembly phase either in the single components or the whole system (e.g., a mobile phone). Thus they become an intrinsic property of the electronic components or circuits, which are visible in the RF emissions both intentional and unintentional. The RF emissions are digitally analyzed and processed using statistical analysis algorithms. This technique exploits the increased power of radio frequency digitizers to support analysis of digitized RF emissions with high granularity. These basic concepts have been applied to various types of electronic circuits using different algorithms. In [7], the authors apply fingerprinting to RFID devices. The RF emissions are digitized and an extensive set of features is used to classify the sample. In particular the authors use variance, kurtosis, skewness, and Shannon entropy. Extensive sets of RFID samples were analyzed and classified and various algorithms were applied including k-nearest neighbors (kNN) and Support Vector Machine (SVM). The results show that the level of accuracy can be very high (even up to 99%). Beyond RFID, the application of similar fingerprinting techniques has been used for other wireless communication standards as well as integrated circuits and components. In [8], the authors have applied RF fingerprinting techniques by passively monitoring and exploiting the intrinsic features of ICs' unintentional RF emissions without requiring any modification to the device being analyzed. The authors in [8] use features based on instantaneous amplitude (IA), instantaneous phase (IP), and instantaneous frequency (IF) and then apply Fisher's (two-class) linear discriminant analysis (LDA) for classification and identification. Other authors have also applied RF fingerprinting to other wireless communication standards like WiFi in [9]. WiFi is similar to the ITS DSRC standard investigated in this paper, even if the frequency range is different (5.9 GHz of DSRC instead of 2.4 GHz of WiFi) and the DSRC standard is designed to support the specific features (e.g., mobility) of VANETs. A comparison of WiFi with DSRC at 5.9 GHz with the detailed description of the differences at the physical layer is provided in [10]. Authors have also applied RF fingerprinting to cellular networks like Global Systems Communications (GSM) in [11], where the possibility of RF tracking has also been mentioned. Most of the identified papers implement the RF fingerprinting in almost ideal conditions and they obtain a very high accuracy of 99% or more, which could point out a serious privacy threat because the tracking of the device would be quite accurate. On the other side, these almost ideal conditions are based on (a) the usage of high-end equipment (e.g., spectrum analyzer and oscilloscopes) for the capture of RF signals and (b) a testing environment in Line of Sight (LOS) conditions with absence of fading effects. In practical scenarios as the one investigated in this paper in Section 4, these conditions are usually not met because a privacy attacker could be obliged to use less expensive equipment (like an Universal Software Radio Platform (USRP) Software Defined Radio (SDR)) and it would be subject to attenuation and fading effects because the DSRC signals must be tracked at a distance. Note that some papers have investigated the impact of White Gaussian Noise on the RF fingerprinting in a simulated way but not fading effects apart from the recent paper of [12] where a fading model has been applied but not to DSRC devices. As a consequence, a novel aspect of this paper is the application of fading models to RF fingerprinting for DSRC devices.

To complete this survey on the related work, we need to highlight an issue, which impacts the RF fingerprinting process for the context of tracking and privacy. The RF fingerprints collected with one receiver are not portable to another receiver because each receiver introduces its own fingerprints or signal bias, which interferes with the identification or verification of the wireless device to be tracked. In other words, the RF fingerprints collected with one receiver cannot be used to track a wireless device using another receiver. As described in [13], these differences impact the identification or the verification accuracy not only when receivers with different quality are used (high-end receiver and low-end receivers) but also across receivers of the similar quality. This is still an open research problem at the time of writing this paper. As described in Section 4, this imposes a limit on the capabilities of a malicious entity, which want to implement the privacy threat by tracking because it can only use one receiver, which limits the tracking range.

3. DSRC Standard

In this section, we provide a brief description of the protocols and standards used in Europe for the V2V and V2I DSRC communication standards at 5.9 GHz in Europe. In this paper, we have investigated the European variant (ETSI ITS Protocol Stack) of the DSRC communication standards defined in ETSI.

ETSI standards define two basic messaging services included in the communications stack as a common reusable middleware. These are the Cooperative Awareness Basic Service, defining the CAM, and the DENM. CAM messages are exchanged among ITS stations (e.g., vehicles) to notify their presence, position, and status in a single-hop distance through the wireless channel. DENM messages can be transmitted in a multihop way to cover a concrete geographic dissemination area. DENM are used to provide a notification service about road status. For example, a DENM message is triggered by a certain ITS application that detects a relevant driving environment or traffic event (e.g., a hazard on the road).

The overall structure of the ETSI ITS Protocol Stack is provided in Figure 1 where the physical and Media Access Control (MAC) layers are defined by the ITS-G5 Protocol (see ETSI ES 202 663), which is largely based on IEEE 802.11p. The facilities layer defines the CAM and DENM messages described above.

The choice to adopt a standard of the 802.11 family was because it is a stable standard supported by experts in wireless

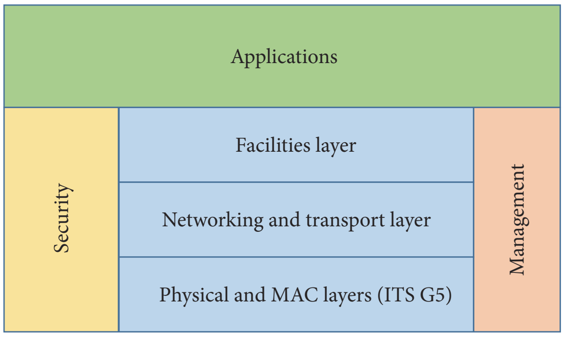

Applications
Security
Facilities layer
Networking and transport layer
Physical and MAC layers (ITS G5)
Management

Figure 1: Layers of the ETSI ITS Protocol Stack.

technology with a large market base. A stable standard is required to guarantee interoperability between vehicles made by different manufacturers and the roadside infrastructure in different geographic areas. On the other side, the DSRC standard cannot be the same of 802.11a because it has different operational requirements as described in [14], in particular,

(1) The high mobility of the vehicles

(2) A longer range of operation of up to 1 Km in comparison to WLAN, which is around 100/200 meters

(3) The potential presence of multipath fading due to other vehicles or urban environment

(4) The presence of multiple overlapping ad hoc networks, which require extremely high quality of service (QoS)

(5) A special beaconing frame

To support these special requirements, 802.11p is different from 802.11a in the following specific features [15]:

(i) One-half the data rates of 802.11a, to have a greater resistance with respect to the channel delay spread due to the double guard time of 1.6 μs

(ii) Improved transmission mask

(iii) Improved receiver performance requirements in adjacent channel rejections

(iv) Control channel and six service channels

Because of these differences, the parameters used to fingerprint device based on WLAN WiFi standards (e.g., 802.11a) cannot be used directly for devices based on the 802.11p standard and this paper is the first in research literature to apply RF fingerprints to this type of devices.

4. Operational Scenario

A pictorial description of the operational scenario is provided in Figure 2. A vehicle equipped with a DSRC device operating at 5.9 GHz is driving along a road and a malicious entity would like to track the vehicle. To perform the tracking, the malicious entity can use an RF receiver. At periodic intervals, the malicious entity collects the RF signals emitted from the DSRC devices and cars on the road. To effectively track the vehicle using fingerprinting, the malicious entity must be able to distinguish the specific DSRC device among the other DSRC devices present on the road on the road and verify its identity through the RF fingerprints. This is possible only if the received signal strength from the specific DSRC device is high enough to support the verification of the identity and if the fingerprints of the different devices on the road are different enough. If this verification is not possible at each collection of the RF signal, the malicious entity will not be able to track the device.

In this context, the privacy threat becomes a problem of verification of identity based on the quality of the RF fingerprinting, and the threat implementation can be based both on machine learning algorithms and on wireless propagation models.

In other words, the tracking can be implemented by comparing the collected emissions using a supervised machine learning algorithms (e.g., SVM). An initial set of RF emissions is used as a training set against which the malicious entity compares other RF emissions at different times, which corresponds to different positions of the vehicle to be tracked. Section 5 provides a description of the overall methodology on how the signals are collected and processed and the machine learning algorithm is applied to implement the tracking.

The tracking range is one of the most critical elements for tracking. If the vehicle is moving at a high speed (e.g., 100 Km/h), a limited range of the RF receiver used by the malicious entity will decrease the tracking effectiveness. The normal operating range of the DSRC communication is between 10 meters and 1 Km, but a malicious attacker can increase the range at which the fingerprints are collected using an amplifier or high directional antennas (pointed in the direction of the vehicle) to increase the gain. On the other side, additional electronic components can also increase the cost and the difficulty of implementing the attack. Additional details on the potential gains and the related costs will be provided in Section 6.

In LOS conditions, the range is based on Free Space Path Loss (FSPL), which is calculated by the following formula:

$$\text{FSPL}\,(\text{dB}) = 20\log_{10}(d) + 20\log_{10}(f) + 92.45, \quad (1)$$

where d is the distance expressed in Km and f is expressed in GHz. At the operating frequency of 5.9 GHz of DSRC, the equation becomes

$$\text{FSPL}\,(\text{dB}) = 20\log_{10}(d) + 107.867 \quad (2)$$

which gives an FPSL of 107.867 at a distance of 1 Km. Note that this is only the FSPL and other factors will introduce additional gains or loss. These factors include the shape of the transmitting and receiving antennas and the front end of the receiver. The receiver system used by the malicious receiver can compensate for the distance from the vehicle by using antenna with high gain (10–30 dB) or an RF amplifier (20–30 dB gain). On the basis of (2), a cumulative gain of 40 dB translates to an increase of the distance between receiver and vehicle of a factor of 100. We note that this calculation is done in Free Space Path Loss conditions. In a practical scenario, the

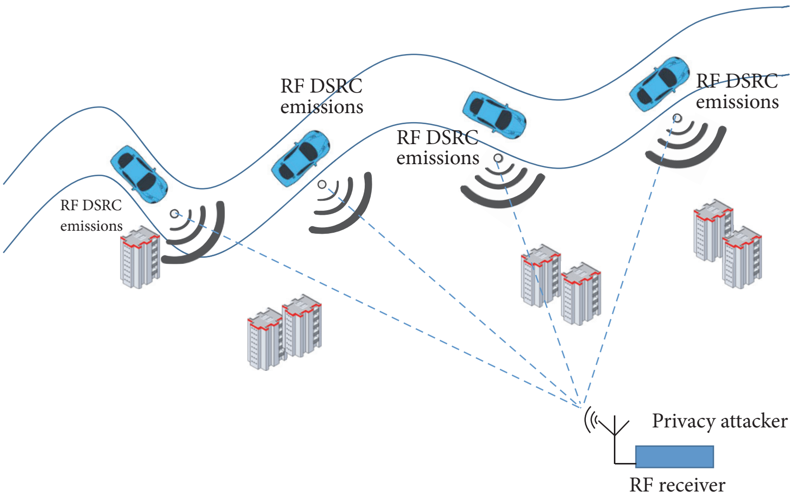


Figure 2: Scenario for the privacy threat based on tracking of the RF fingerprints of the vehicle.

presence of obstacles on the wireless propagation path will introduce attenuation and fading effects, which can strongly decrease the distance at which it is possible to track in an accurate way the vehicle from its RF emissions. The analysis of the impact on the tracking range due to attenuation or fading is provided in Section 6.

We note that the collected RF emissions at different positions of the vehicle can differ in power. For example, the malicious attacker can collect the RF emissions of the specific DSRC device of a vehicle at the beginning of the trip in LOS conditions when the car is still and the observer is near the car or during the normal driving of the car in difficult wireless propagation conditions. How the different received power of the collected RF signal impacts the tracking accuracy is evaluated in Section 6.

The scenario is based on a single observer equipped with a RF receiver. Multiple RF receivers synchronized through Global Positioning Systems (GPS) or other means could be used to collect the RF observables and extend the tracking range, but this is not achievable at the time of writing this paper because of the issue of portability already described in Section 2. The fingerprints collected by one receiver cannot be used by another receiver and the malicious entity would not be able to exploit the additional receivers to extend the tracking range. As a consequence, the scenario is based on a single receiver.

A final note about the terminology used in the subsequent sections of this paper. In RF fingerprinting, a distinction is usually made between verification and identification:

(i) In this context, *verification* is the function of the recognition system to verify the identity of a DSRC device from its RF observables. This can be achieved by comparing the collected RF observables to an initial reference.

(ii) In this context, *identification* is the function of the recognition system to determine the identity of a DSRC device among a set of RF observables. This can be achieved by comparing the reference device fingerprint with all the collected RF observables.

While identification is an important function in the study of RF fingerprinting, in this paper, we focus only on verification because the privacy threat originates from the tracking of the DSRC device, which is implemented by repeated verifications of the RF collected observables against the initial reference.

5. Methods, Materials, and Algorithms

5.1. Methodology. The overall methodology, experimental setup, and algorithms used to track the vehicle through its RF fingerprinting are described in this section.

The analysis of the feasibility to track vehicles through the RF fingerprinting of the DSRC devices is performed using the following steps:

(1) The RF observables of four DSRC devices of the same model and brand are collected in LOS conditions. The RF signal in space emitted by each DSRC devices is down converted and digitalized using a receiver with Analog to Digital Converter (ADC) capability. A detailed description of the test bed to collect the RF measurements is provided in Section 5.2.

(2) From the digitized RF observables, the transmission bursts defined by ITS-G5 physical layer (based on 802.11p as described in Section 3) are extracted, synchronized, and normalized. This step is needed to ensure that the bursts transmitted by each DSRC device can be effectively compared and that there is no bias introduced by different power levels or measurement distances. In the privacy threat scenario, the tracking accuracy can be negatively impacted if the bursts are not properly synchronized and normalized. In other words, this step must also be performed by the privacy attacker to support the tracking process

and impact the privacy attack. The Variance Trajectory technique is used to effectively determine the beginning and the end of the burst and it is widely used in RF fingerprinting (e.g., see [9]).

(3) From the RF observables, statistical features are extracted. The extraction of statistical features like variance, entropy, skewness, and kurtosis is a common approach in RF fingerprinting as described in [7, 16] and others. Rather than performing the verification process and tracking on the raw data derived from the RF observables, a subset of features is selected and used as a representation of the DSRC devices. In other words, the subset of features becomes the RF fingerprinting of the DSRC device. The advantage of using the subset of statistical features rather than the raw data is that the verification process is much faster and it is feasible even with a limited observation time (which translates to a limited number of bursts). In the specific scenario addressed in this paper, the timely performance of the verification process is quite important because the privacy attacker may have a limited time to collect RF observables while the vehicle is driving along the route.

(4) A supervised machine learning approach based on SVM is used to execute the verification process. A test set is compared to the training set. The training set is based on the RF observables collected initially while the test set is representative of the RF observable collected during the tracking process. The SVM machine learning algorithm is well described in the literature and it is only briefly described in Section 6.

(5) To simulate difficult wireless propagation conditions for the collection of RF observables, Gaussian noise and multipath fading are applied to the RF observables. A description of the Gaussian noise and the fading model (e.g., Rayleigh) is given in Section 6.2.

(6) Feature selection: not all the statistical features provide the same level of verification accuracy. As described in [7, 16], the most appropriate statistical features for verification must be selected. In this paper, we use the sequential forward selection (SFS) method to select the best features. See [17] for a detailed description of this technique. The basic concept of this technique is that features are sequentially added to an empty candidate set until the addition of further features does not decrease the verification accuracy.

(7) Parameter tuning of the machine learning algorithm: even if the best selection of features has been identified, some parameters of the machine learning algorithm must be tuned to improve the verification accuracy. In the case of SVM, these parameters are the scaling factor and box constraint. See Section 5.4 for a description of the meaning of these parameters and [18] for a detailed description of the SVM algorithm. To avoid the risk of overfitting the feature selection and the choice of the scaling factor and box constraint are executed using a 10-fold method where each collection of statistical fingerprints (one for each DSRC device) is divided into ten blocks. Nine blocks from each device are used for training and one block is *held out* for classification. The training and classification process is repeated ten times until each of the ten blocks has been *held out* and classified. Thus, each block of statistical fingerprints is used once for classification and nine times for training. Final cross-validation performance statistics are calculated by averaging the results of all folds.

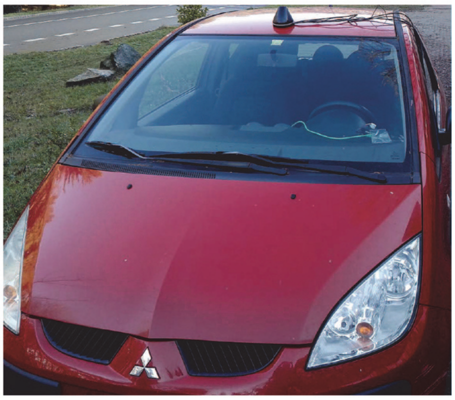


Figure 3: Installation of the DSRC device on the vehicle.

5.2. Test Bed and Materials. The test bed used to collect the RF observables is composed of four DSRC devices operating at 5.9 GHz and implementing the ITS G5 physical layer. The channel at 5.86 GHz was selected to collect the measurements. The modulation was consistent with the DSRC/802.11p standard based on OFDM and QPSK. Each DSRC device is installed in a vehicle and configured and connected through a laptop for the setup and configuration. The antenna is positioned on the rooftop of the car as shown in Figure 3. The connection between the DSRC device and the laptop was through LAN. The DSRC device is configured through the laptop to transmit periodically CAM messages with a specific content. The DSRC devices transmit a specific data payload (i.e., the testing payload to ensure repeatability across DSRC devices) with a bandwidth of 5 MHz. The frequency of transmission of the CAM messages was set to 10 Hz as recommended in the ETSI standard [19] to support the applications based on CAM. These applications require high frequency in order to ensure low reception latency after first contact. An example of this application is the Intersection Collision Warning, where the vehicles equipped with DSRC need to exchange CAM messages quite frequently to ensure a low latency of 100 ms as described in Table 1 of [19].

The RF signal in space, which is transmitted by the DSRC devices, is collected using a USRP SDR receiver of type N210, equipped with XCVR2450 front end, both locked to the GPS time and 10 MHZ reference to ensure repeatability in the collection of RF observables. The SDR receiver was equipped

Table 1: Experimental setup: test bed summary.

USRP type	N2100
USRP gain	5
USRP front end	XCVR2450
USRP gain	5
Sampling frequency	10 MS/sec IQ
Sample recording time	60 seconds
Link frequency	5.86 GHz
Synchronization	GPS using ublox NEO6Q (min 4 sat, min 30 min lock)
Start of experiment	1455727526 (UNIX epoch)

with an ublox NEO6Q GPS receiver. The SDR receiver is positioned around 5 meters from the vehicle and the DSRC antenna to replicate a privacy attacker positioned on the roadside.

To ensure consistency with a practical scenario, where the DSRC devices could transmit different data payloads, only the preamble of the DSRC burst was used for RF fingerprinting, which is invariant to the data payload. This is consistent with related work for 802.11a fingerprinting like [9] or WiMaX [3] where the preamble is also used. The USRP N210 has a fixed sample rate of 100 MSamples per second with full In-phase/Quadrature (I/Q). More details about the device can be found in the technical specifications in [20]. We configured it with a digitally decimated rate of 10 MHz I/Q, which was adequate for the bandwidth of the DSRC devices under tests.

Once the four sets of samples were collected, the real-valued signal samples were first converted to I/Q samples and then synchronized and normalized offline to extract the 802.11p bursts. For the initial training phase, we collected 1000 bursts for each DSRC device. In this process, the real-valued signal samples were also checked and validated to ensure that the CAM messages were properly transmitted and received. Note that, in this experimentation and paper, we were only interested in the physical layer of the DSRC messages and not in the performance of the V2X communication at the network level because the identification information (and the related privacy threat) is specific to the RF fingerprinting of the DSRC device. For this reason, simulators like NS2 were not used in this experiment.

Note that the collection of the RF signals from the DSRC devices was implemented in LOS conditions as described above and at a short distance between receiver and DSRC transmitter. The evaluation of the performance of the RF fingerprinting in more challenging environments from the wireless propagation point of view is done in Section 6.1 for longer distances between the DSRC transmitter and the USRP receiver and in Section 6.2 for different fading conditions like urban or highway areas or different speeds of the vehicle.

The parameters of the scenario are presented in Table 1.

5.3. Statistical Features. Then we applied the statistical features described in Table 2 to each single burst for each DSRC device. The first column in the table is the name of the statistical feature, the second column is the description of the statistical features, and the third column points to the formula, which defines the feature. Finally the fourth column provides the numeric identifier of the feature used in the rest of the paper (e.g., for graphs and tables in the results section). This set of statistical features is similar to the set of features used in [7]. In these expressions the variable S_{TD} is the instantaneous amplitude (IA):

$$\text{Variance}\left\{S_{TD}\right\} = \frac{1}{N-1}\sum_{i=1}^{N}\left(S_{TD}-\mu\right)^2 \tag{3}$$

$$\text{Skewness}\left\{S_{TD}\right\} = \frac{1}{\sigma^3}\sum_{i=1}^{N}\left(S_{TD}^3-\mu^3\right) \tag{4}$$

$$\text{Kurtosis}\left\{S_{TD}\right\} = \frac{1}{\sigma^4}\sum_{i=1}^{N}\left(S_{TD}^4-\mu^4\right) \tag{5}$$

$$H_{\text{ShannonEntropy}}\left\{S_{TD}\right\} = -\sum_{i=1}^{N}\left(S_{TD}^2 * \ln\left(S_{TD}^2\right)\right) \tag{6}$$

$$H_{\text{LogEnergy}}\left\{S_{TD}\right\} = \sum_{i=1}^{N}\ln\left(S_{TD}^2\right). \tag{7}$$

5.4. Machine Learning Algorithms and Parameters Optimization. As described previously, a supervised machine learning approach was used for verification of the identity of the DSRC device and therefore the tracking function.

The SVM is a very well-known technique in supervised machine learning and it has been used in this paper because SVM has demonstrated its effectiveness for RF fingerprinting in [11] and other sources. On the basis of a set of training samples (in our case these are the RF observables from the DSRC devices and the derived statistical features), SVM assigns each sample to one of two categories in the training phase. This makes SVM a nonprobabilistic binary linear classifier. The resulting SVM model is a representation of the samples as points in space, mapped so that the samples of the separate categories are divided by a clear gap that is as wide as possible. In the testing phase (the tracking phase in our context) new samples are then mapped into that same space and predicted to belong to a category (e.g., the DSRC device) based on which side of the gap they fall on.

From a formal point of view, let us assume that we have n labeled examples $(x_1, y_1), \ldots, (x_n, y_n)$ with labels $y_i \in \{1, -1\}$. We want to find the hyperplane H (in a proper d-dimensional space K) defined by $\langle w, x\rangle + b = 0$ (i.e., with parameters (w, b)), which satisfies the following conditions:

(1) The scale of (w, b) is fixed so that the plane is in canonical position with respect to $\{x_1, \ldots, x_n\}$. That is,

$$\min_{i\le n} \quad \left|\langle w, x_i\rangle + b\right| = 1. \tag{8}$$

(2) The plane with parameters (w, b) separates the $+1$'s from the -1's. That is,

$$y_i\left(\langle w, x_i\rangle + b\right) \ge 0 \quad \forall i \le n. \tag{9}$$

Table 2: Identifiers of the statistical features.

Statistical feature	Feature description	Related equation	Feature identifier
Variance	The variance is the mean squared variance of a distribution from its mean	Equation (3)	1
Skewness	The skewness characterizes the degree of asymmetry of a distribution around its mean	Equation (4)	2
Kurtosis	Kurtosis measures the relative peakedness or flatness of a distribution	Equation (5)	3
Shannon Entropy	Shannon Entropy is the expected value of the information contained in a signal based on the definition by Shannon	Equation (6)	4
Log Energy Entropy	Log Energy Entropy is the expected value of the information contained in a signal based on a logarithmic scale	Equation (7)	5

(3) The plane has a maximum margin $\rho = 1/|w|$, that is, minimum $|w|^2$.

We can redefine $\langle w, x\rangle + b = 0$ to the following equation:

$$w \bullet \phi(x) + b = 0, \tag{10}$$

where $\phi(x)$ represents a proper mapping of x into the space K; $w = [w_1; w_2; \ldots; w_d]$ denotes a d-dimensional real vector normal to H; and b is a real parameter such that $|b|/\|w\|$ is the perpendicular distance of the origin from H. $\bullet$ is the scalar product between two vectors.

The problem of finding the hyperplane H becomes an optimization problem, which can be reformulated to the following equation:

$$\min_{(w,b,\xi)} \quad \frac{1}{2} W^T W + C \sum \xi_i, \tag{11}$$

where ξ_i are the slack variables and i is in the range of 1 to N_{Train}, which is the number of training vectors. The slack variables are subject to $\xi_i > 0$ and they account for the presence of classification errors. The parameter C (which we will call box constraint in the rest of the paper) allows the SVM user to control the weight of these errors in the previous equation (11) and it is one of the two parameters to be tuned in the training process.

The second parameter to be tuned is related to the kernel function, which is used to define the shape and format of the hyperplane. Various kernel functions are available in the literature including linear, polynomial, and Radial Basis Function (RBF).

In this paper, we use SVM with RBF as a kernel function because it has demonstrated its effectiveness for fingerprinting classification in [11] and other references. In addition, this kernel has a number of good features, since it can properly handle the cases in which the relation between class labels and features is nonlinear in classification problems (which is indeed our case).

The definition of the RBF is the following:

$$K\left(\mathbf{x}_i, \mathbf{x}_j\right) = e^{-\gamma \|\mathbf{x}_i - \mathbf{x}_j\|^2}. \tag{12}$$

The γ scaling factor is the second parameter to be tuned together with C box constraint parameter.

To summarize, the application of SVM in this context requires the optimization of the statistical features and the parameters of the SVM and the RBF, which are the scaling factor γ from equation (12) and the box constraint C parameter from (11).

The optimization of the statistical features is based on the sequential forward selection algorithm as described in Section 5, which has been applied to the features described in Table 2 on all the bursts collected in the training phase.

The sequential forward selection algorithm must be based on a criterion against which the optimum value is identified. In machine learning, the following parameters are defined:

(i) T_p is the number of true positive matches where the machine learning algorithm has correctly identified a sample (e.g., a collected RF signal in our context) as belonging to the correct class.

(ii) T_n is the number of true negative matches where the machine learning algorithm has correctly identified a sample as not belonging to the correct class.

(iii) F_p is the number of false positive matches where the machine learning algorithm has identified a sample as belonging to a class while it is not true.

(iv) F_n is the number of false negative matches where the machine learning algorithm has identified a sample as not belonging to the class while this is not true.

The combination of the different parameters can define different metrics to evaluate the effectiveness of a machine learning algorithm. In this case, we use the verification accuracy as a criterion, which is calculated as

$$\text{Accuracy} = \frac{T_p + T_n}{\text{TotalPopulation}}, \tag{13}$$

where T_p is the number of true positives and T_n is the number of true negatives resulting from the application of the SVM machine learning algorithm to the problem of verifying that the collected RF observables are representative of the same DSRC device evaluated in the training phase. The total population represents the total population of samples (which is the sum of T_p, T_n, F_p, and F_n). While this metric is indeed

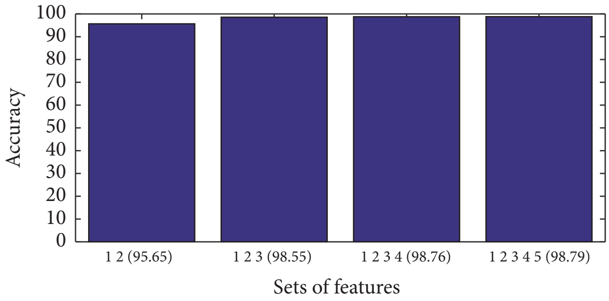


Figure 4: Bar plot of the overall accuracy for different sets of features.

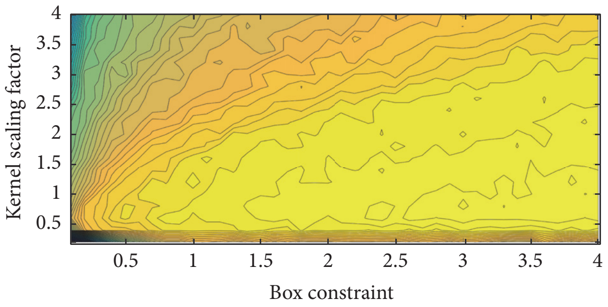


Figure 5: Bidimensional plot of the accuracy on the basis of the scaling factor and the box constraint.

valuable to evaluate the feasibility of tracking a vehicle, the robustness of the model used in machine learning should also be based on other metrics.

Beyond accuracy, in this paper, we will also use Receiver Operative Characteristics (ROC) and the Equal Error Rate (EER) metrics to evaluate the verification accuracy and the tracking performance as presented in Section 6.

The ROC is calculated as ROC-like performance curve is generated here by plotting F_p versus T_p as the verification threshold changes.

The EER corresponds to the point on the ROC curve where F_p versus T_p are equal. This metric is frequently used as a summary statistic to compare the performance of various classification systems. In general, lower EERs indicate better system classification performance.

The sequential forward selection algorithm with the criterion of verification accuracy was applied to all four DSRC devices under test and the results were averaged. The results of the algorithm based on a 10-fold method identify the combination of features $[1, 2, 3, 4, 5]$ as the best set of features.

Other combinations of features also provide great verification accuracy. Figure 4 provides the accuracy results for an incremental set of features.

This result was obtained in LOS conditions.

The values of accuracy identified in Figure 4 were obtained with fixed values of the scaling factor (i.e., 1) and box constraint (1), which were chosen at random. These parameters must be optimized. This is achieved by trying different combinations of values of these parameters in a specific range. The results are shown in Figure 5.

From the figure, we obtain an optimum scaling factor of 0.8 and a box constraint of 3.8 (the maximum value in Figure 5). With these values, the features combination $[1, 2, 3, 4, 5]$ provides an average verification accuracy of 99.5, which is extremely high and it would permit the implementation of the privacy threat with great efficiency because the privacy attacker could track the DSRC device and vehicle with almost ideal accuracy. Note that these results were obtained in LOS conditions, with a long collection time (i.e., to collect 1000 bursts) and with no path loss attenuation, which is not feasible from a practical point of view. This would mean that the privacy attacker is near the vehicle and it can collect the burst for a considerable amount of time. For example, in the test setup used by the authors, the 1000 bursts were collected in a timeframe of 60 seconds.

While this ideal case has been useful to identify the best set of parameters, in the next section, we investigate a more realistic scenario where the privacy attacker is far from the vehicle and (s)he can collect RF observables for a limited period of time.

6. Results of the Analysis on Privacy Threats Using RF Fingerprinting

In this section, we investigate the feasibility of the implementation of the privacy threat in more realistic scenarios than the previous section. Note that, in the analysis presented in the subsequent subsections, we will use the optimal set of features and machine learning parameters for scaling factor and box constraint already calculated in Section 5.4.

The first scenario is when the privacy attacker implements the attack in an area with no fading effects but only with path loss attenuation.

6.1. Path Loss Attenuation. In this scenario, the privacy attacker collects and processes RF observables at a distance from the vehicle, but the propagation path is still LOS and no fading effects are present.

The collection of RF observables at a distance from the tracking target can be simulated by adding Additive White Gaussian Noise (AWGN) to the samples. Decreasing values of the resulting Signal to Noise Ratio (SNR) simulate an increasing distance from the tracking target as described in the following paragraph.

The received signal in an AWGN channel can be expressed as

$$r(t) = \alpha s(t) + n(t), \tag{14}$$

where $s(t)$ is the transmitted signal and $n(t)$ is the complex noise signal with Gaussian distribution and spectral density noise N_0. The attenuation in (14) is a complex value represented by $\alpha = |\alpha| e^{j\phi}$. Furthermore, the received SNR is a metric used for system evaluation and follows the relationship $\text{SNR} = P_R/P_N = f_s E_b \log_2(M)/BN_0$, where P_R and P_N are the received power and noise power, respectively. Also, the parameters f_s, E_b, B, and M are the symbol rate, bit energy, channel bandwidth, and modulation order, respectively.

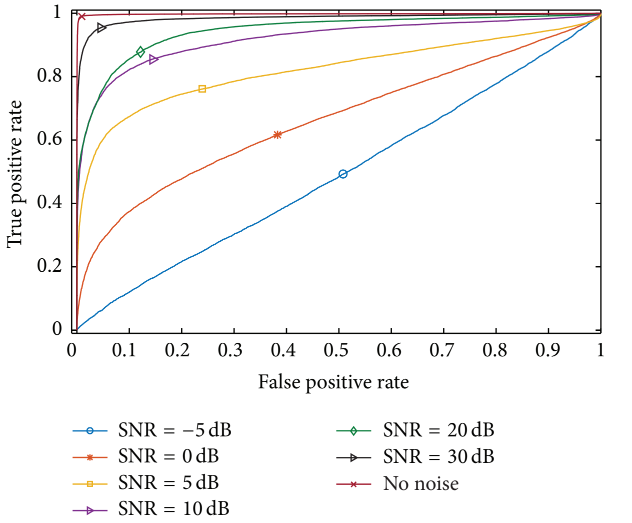


Figure 6: ROC curves between DSRC 3 and 4 for different values of attenuation.

The distance and the related attenuation are represented in the subsequent sections and graphs as SNR expressed in dB.

Figure 6 describes the impact of attenuation for the accuracy verification between two DSRC devices. The figure describes the ROC for different values of SNR in a scenario where we need to track a vehicle equipped with device DSRC 3 and distinguish it from another vehicle equipped with device DSRC 4 whose RF observables are collected during tracking. The more the central point of the ROC is near the center of the figure, the more difficult it is to track the vehicle because its RF fingerprints cannot be distinguished from the other vehicle.

The EERs were also calculated for all the combinations of devices, which corresponds to the scenario of tracking each DSRC and vehicle from the others.

From Figures 6 and 7, we can see that the accuracy decreases significantly for some DSRC devices around values of SNR of 5 dB and below. This means that a privacy attacker, which can only collect RF observables with a SNR of 5 dB and below, will not be able to effectively track the DSRC vehicle because the verification accuracy would be too low (i.e., getting near random choice).

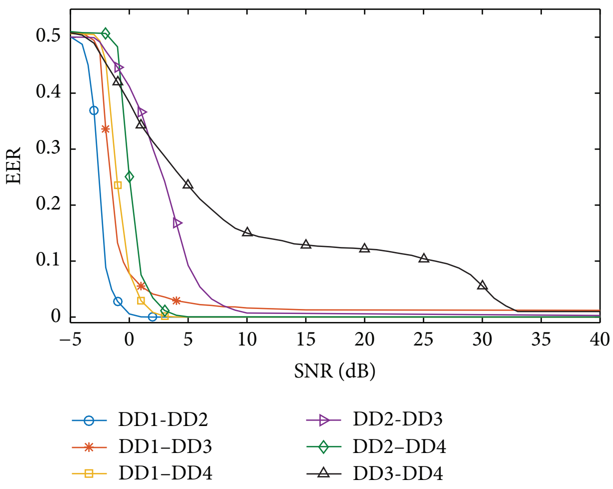


Figure 7: EERs for different values of SNR and different set of DSRC devices.

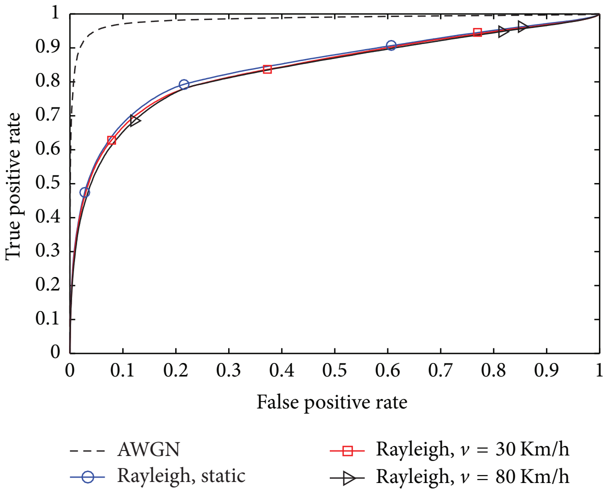


Figure 8: ROCs with Rayleigh Doppler.

Table 3: Differences in accuracy for samples with different values of SNR.

Baseline SNR	SNR	SNR	SNR
Baseline 40 dB	38	36	34
	−10.5	−29	−42.25
Baseline 30 dB	28	26	24
	−8.5	−10	−10

As described in Section 4, the privacy attacker could collect the RF fingerprints at slightly different distances or conditions because the vehicle will move along the route while the privacy attacker may be still. The privacy attacker can compensate the different distances by using a receiver with adaptive gain or by calibrating the amplifier so that the SNR of the collected RF signals is still relatively constant during tracking. For example, the privacy attacker could collect the RF signals in the initial observation used for the training phase of the machine learning algorithm with a slightly different SNR from other collection phases. To evaluate the impact on the tracking accuracy due to difference between the initial collection of RF signals and the subsequent collections, we performed an analysis of the performance of the machine learning algorithms with different sets of data with different values of SNR.

Table 3 shows the differences in tracking accuracy between the two scenarios for different values of SNR and between DSRC devices DSRC 3 and DSRC 4. We note that the accuracy becomes progressively worst with the decrease of the SNR of the samples collected in the second scenario. One of the reasons for the significant drop of the accuracy even for few dBs is because the different values of SNR have an impact on the fingerprints because some of the adopted

Table 4: Accuracy for different number of samples.

Number of samples	Accuracy
10	94
20	95
40	94.5
100	93.5
200	95.5

statistical features (e.g., variance or entropy) are proportional to the noise in the signal. In other words, observables taken with different SNR do have also limited portability because the adopted statistical features are depending on the noise in the signal. As a consequence, a privacy attacker could find it difficult to distinguish between DSRC devices and track a specific vehicle. While this is relatively obvious from the definition of the statistical features in (3) to (7), this analysis shows another challenge for a privacy attacker and it can limit the feasibility of privacy attack based on RF fingerprints in a practical scenario. An obvious solution would be to select only statistical features, which are invariant to Gaussian noise (e.g., skewness defined in (4)), but this would limit the set of potential statistical features for fingerprinting. In addition, statistical features, which are invariant to noise, can be instead dependent on fading effects. The privacy attacker could implement an adaptive gain control function in the receiver to ensure that the collected samples have the same SNR even if the vehicle is moving. The adaptive gain function would regulate the RF amplifier of the receiver to maintain the SNR of the collected samples constant. Obviously, the presence of an adaptive gain function would increase the cost and complexity of the tracking system used by the privacy attacker.

Finally, we evaluated the potential loss of accuracy when the observation time to collect the samples is decreased. Table 4 shows the value of accuracy in high SNR conditions for increasing number of samples (i.e., DSRC bursts), which are proportional to longer observation times. Sets of test samples of different lengths (from 10 samples to 200 samples) are tested against a training matrix of 1000 samples in the presence of limited noise. We notice that the accuracy has minor variations in relation to the number of samples. This is expected because the accuracy is dependent on other factors like SNR or fading, which are invariant in this analysis. To give an idea of the practical observation time, the 1000 bursts of the training set were collected in 60 seconds. Then, the smallest set of 10 samples can be collected in 0.6 seconds. This collection time is based on the specific DSRC setup used in our test bed. In a future deployment of DSRC systems, the frequency of the DSRC bursts can change, but it will be in a similar frequency range (see [10]).

6.2. Impact of Fading. Beyond attenuation due to distance in LOS conditions, a practical scenario for a privacy attack must also consider the presence of obstacles on the path between the vehicle and the privacy attacker. In this scenario, a model, which is only based on Gaussian noise, is not adequate to describe the scenario because fading effects will be present. Buildings or road infrastructure will introduce different types of fading, which can also impact the tracking accuracy.

This section performs an analysis of the fading effects for tracking accuracy. The fading effect is explained here. The radio channel is the transmission medium between the transmitter and the receiver. In DSRC communications, the received signal is composed of a large number of transmitted replicas, which present LOS and/or NLOS components. Furthermore, the transmitted signal can be reflected, diffracted, and scattered due to different obstacles existent in the communication surroundings. In addition to multipath propagation, the RF signal in vehicular networks is impaired by Doppler shifts due to the large relative velocity between the DSRC transmitter and receiver units (i.e., the vehicles). Thus, the need of a channel representation that realistically models all of these phenomena is of paramount importance for vehicular communications [21–23].

The most basic channel is the AWGN channel model, whose impact has been analyzed in Section 6.1. A more realistic channel model for vehicular communications considers the time and frequency variations suffered by the propagated signals. Therefore, the normalized channel impulse response of the DRSC channel is expressed in the complex baseband as

$$h(t,\tau) = \frac{1}{\sqrt{N(t)}} \sum_{k=0}^{N(t)-1} a_k(t) e^{-j\phi_k(t)} \delta(t - \tau_k(t)), \qquad (15)$$

where $N(t)$ is the number of multipath components, which varies with time. The time-dependent variables, $a_k(t)$ and $\tau_k(t)$, represent the amplitude and position of the kth multipath component, respectively. The term $a_k(t)$ is modeled as a random variable with Rayleigh distribution in this work. Furthermore, the variable $\phi_k(t)$ depends on the time and the Doppler spread and can be modeled as

$$\phi_k(t) = 2\pi f_c (t - \tau_k(t)) - \phi_{D_k}, \qquad (16)$$

where f_c is the carrier frequency of the DSRC system and $\phi_{D_k} = \int_t 2\pi f_{D_k}(t) dt$ is the Doppler frequency component expressed in terms of the frequency variation function, $f_{D_k}(t)$. The Doppler shift occurs when the transmitter and/or the receiver are in relative motion. The maximum Doppler shift is obtained from the expression $f_{\max} = f_c v / c_0$, where v is the relative transmitter-receiver speed and c_0 is the speed of light.

In this work, an empirical channel model specified in ITU for vehicular test environments is used. In particular, a six-tap model with relative delays $\tau_k = \{0, 310, 710, 1090, 1730, 2500\}$ ns and average power values $P_k = \{0, -1, -9, -10, -15, -20\}$ dB is implemented for the simulation analysis. In addition, three relative speeds between the vehicle and the RF receiver (which implements the privacy threat) have been considered, $v = \{0, 30, 80\}$ Km/h. The simulation with different speeds is useful to evaluate if high relative speeds (i.e., 80 Km in this case) can hamper the effectiveness of the privacy attacker. This Rayleigh model can be used to represent an urban environment, where numerous obstacles can hamper the capability of a privacy attacker to collect the RF fingerprints from the DSRC device in the vehicle. In comparison, the AWGN-only model can be used for a highway scenario in a rural environment, where the receiver of the privacy attacker does not have obstacles between it and the vehicle.

There are a number of studies, which investigated the typical values of the fading parameters. The studies are also based on experimental measurements as in [22, 24]. The values chosen for the analysis presented in this paper are in the range of values suggested by the cited references.

The ROC was calculated between two DSRC devices in the presence of the Rayleigh fading effects. The results are shown in Figure 8.

Figure 8 shows that fading has a relevant impact on the verification accuracy and tracking and can severely limit the tracking range of a privacy attacker.

In comparison to the simple model based only on Gaussian noise (i.e., the AWGN curve in Figure 8), the fading introduces an additional loss of accuracy, which can severely limit the tracking accuracy. As a consequence, a privacy attacker should position himself/herself in a LOS condition with the vehicle; otherwise the tracking of the vehicle will not be feasible. From Figure 8, we also note that the speed of car (relative to the privacy attacker) is not relevant for the tracking accuracy because the ROC curves at 30 and 80 Km/h are quite similar. This is also an important result because it proves that the speed of the vehicle is not a significant factor for the implementation of the privacy threat based on RF fingerprinting.

7. Conclusions and Future Developments

This paper has investigated the potential privacy threat based on the tracking of vehicles through the RF fingerprints of their DSRC 5.9 GHz devices. The fingerprints were generated on the basis of selected statistical features and the optimum set of statistical features was identified. To the knowledge of the authors, this is the first time that the fingerprinting of 5.9 GHz DSRC devices is performed and it is applied to the privacy context. The analysis was conducted both for LOS scenarios and for NLOS scenarios where attenuation or fading effects are present. The results of the analysis show that the impact of attenuation and fading is quite significant and it can strongly hamper the capability of tracking the vehicles especially in a challenging environment from the RF point of view. This paper identifies the key challenges, which must be overcome by a privacy attacker to implement a privacy threat. Future developments by the authors will investigate additional statistical features, which can be more robust against the presence of noise and fading effects.

Competing Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

References

[1] K. Dar, M. Bakhouya, J. Gaber, M. Wack, and P. Lorenz, "Wireless communication technologies for ITS applications," *IEEE Communications Magazine*, vol. 48, no. 5, pp. 156–162, 2010.

[2] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym schemes in vehicular networks: a survey," *IEEE Communications Surveys and Tutorials*, vol. 17, no. 1, pp. 228–255, 2015.

[3] M. D. Williams, S. A. Munns, M. A. Temple, and M. J. Mendenhall, "RF-DNA fingerprinting for airport WiMax communications security," in *Proceedings of the 4th International Conference on Network and System Security (NSS '10)*, pp. 32–39, Melbourne, Australia, September 2010.

[4] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, "AMOEBA: robust location privacy scheme for VANET," *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 8, pp. 1569–1589, 2007.

[5] R. Neisse, G. Steri, I. N. Fovino, and G. Baldini, "SecKit: a model-based security toolkit for the internet of things," *Computers & Security*, vol. 54, pp. 60–76, 2015.

[6] J. Bou Abdo, T. Bourgeau, J. Demerjian, and H. Chaouchi, "Extended privacy in crowdsourced location-based services using mobile cloud computing," *Mobile Information Systems*, vol. 2016, Article ID 7867206, 13 pages, 2016.

[7] C. Bertoncini, K. Rudd, B. Nousain, and M. Hinders, "Wavelet fingerprinting of radio-frequency identification (RFID) tags," *IEEE Transactions on Industrial Electronics*, vol. 59, no. 12, pp. 4843–4850, 2012.

[8] W. E. Cobb, E. D. Laspe, R. O. Baldwin, M. A. Temple, and Y. C. Kim, "Intrinsic physical-layer authentication of integrated circuits," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 1, pp. 14–24, 2012.

[9] W. C. Suski II, M. A. Temple, M. J. Mendenhall, and R. F. Mills, "Using spectral fingerprints to improve wireless network security," in *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM '08)*, pp. 2185–2189, December 2008.

[10] Y. J. Li, "An overview of the DSRC/WAVE technology," in *Quality, Reliability, Security and Robustness in Heterogeneous Networks: 7th International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness, QShine 2010, and Dedicated Short Range Communications Workshop, DSRC 2010, Houston, TX, USA, November 17–19, 2010, Revised Selected Papers*, vol. 74 of *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, pp. 544–558, Springer, Berlin, Germany, 2012.

[11] J. Hasse, T. Gloe, and M. Beck, "Forensic identification of GSM mobile phones," in *Proceedings of the 1st ACM Workshop on Information Hiding and Multimedia Security (IH and MMSec '13)*, pp. 131–140, ACM, Montpellier, France, June 2013.

[12] W. Wang, Z. Sun, S. Piao, B. Zhu, and K. Ren, "Wireless physical-layer identification: modeling and validation," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 9, pp. 2091–2106, 2016.

[13] S. U. Rehman, K. W. Sowerby, and C. Coghill, "Radio-frequency fingerprinting for mitigating primary user emulation attack in low-end cognitive radios," *IET Communications*, vol. 8, no. 8, pp. 1274–1284, 2014.

[14] R. A. Uzcátegui and G. Acosta-Marum, "Wave: a tutorial," *IEEE Communications Magazine*, vol. 47, no. 5, pp. 126–133, 2009.

[15] 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 (VTC '08)*, pp. 2036–2040, IEEE, Singapore, May 2008.

[16] Q. Xu, R. Zheng, W. Saad, and Z. Han, "Device fingerprinting in wireless networks: challenges and opportunities," *IEEE Communications Surveys and Tutorials*, vol. 18, no. 1, pp. 94–104, 2016.

[17] J. Kittler, "Feature selection and extraction," in *Handbook of Pattern Recognition and Image Processing*, pp. 59–83, Academic Press, 1986.

[18] N. Cristianini and J. Shawe-Taylor, *An Introduction to Support Vector Machines and Other Kernel-Based Learning Methods*, Cambridge University Press, 2000.

[19] ETSI, *ETSI TS 102 637-2, Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Co-Operative Awareness Basic Service*, ETSI, Sophia Antipolis Cedex, France, 2010.

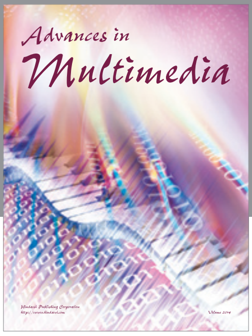
[20] E. Research, "USRP N200/N210 networked series specifications," 2016, https://www.ettus.com/content/files/07495_Ettus_N200-210_DS_Flyer_HR_1.pdf.

[21] G. Acosta-Marum and M. A. Ingram, "Six time- and frequency-selective empirical channel models for vehicular wireless LANs," *IEEE Vehicular Technology Magazine*, vol. 2, no. 4, pp. 4–11, 2007.

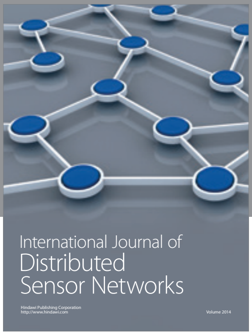
[22] I. Sen and D. W. Matolak, "Vehicle-vehicle channel models for the 5-GHz band," *IEEE Transactions on Intelligent Transportation Systems*, vol. 9, no. 2, pp. 235–245, 2008.

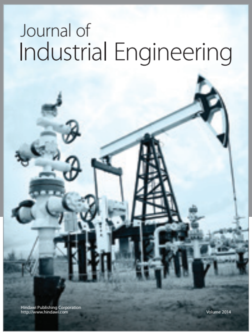
[23] A. Paier, J. Karedal, N. Czink et al., "Characterization of vehicle-to-vehicle radio channels from measurements at 5.2 GHz," *Wireless Personal Communications*, vol. 50, no. 1, pp. 19–32, 2009.

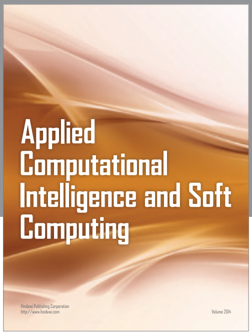
[24] V. M. Rodrigo-Peñarrocha, J. Reig, L. Rubio, H. Fernández, and S. Loredo, "Analysis of small-scale fading distributions in vehicle-to-vehicle communications," *Mobile Information Systems*, vol. 2016, Article ID 9584815, 7 pages, 2016.

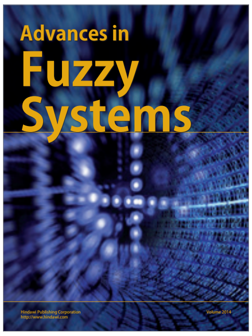

Advances in
Multimedia

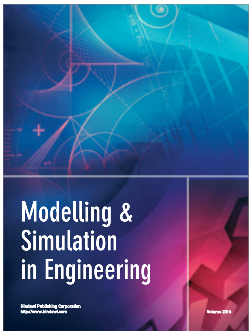
The Scientific
World Journal

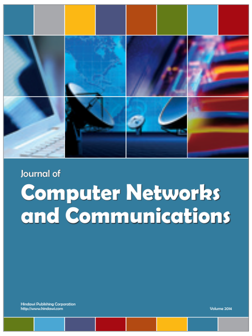

International Journal of
Distributed
Sensor Networks

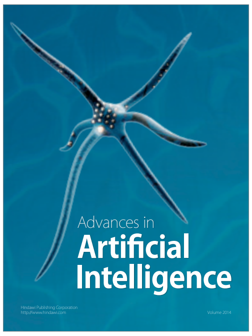

Journal of
Industrial Engineering

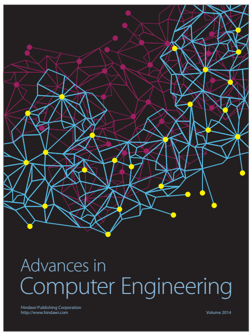

Applied
Computational
Intelligence and Soft
Computing


Advances in
Fuzzy
Systems

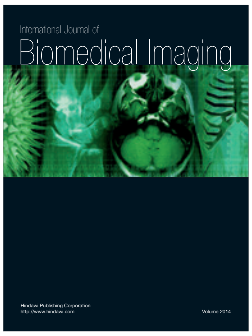

Modelling &
Simulation
in Engineering

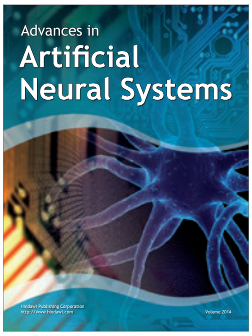

Journal of
Computer Networks
and Communications

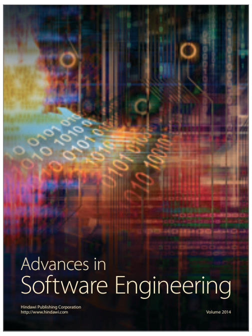

Advances in
Artificial
Intelligence


Advances in
Computer Engineering

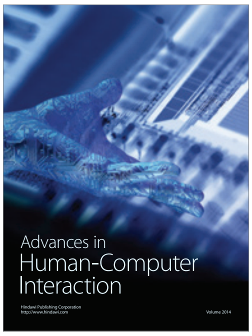
International Journal of
Computer Games
Technology

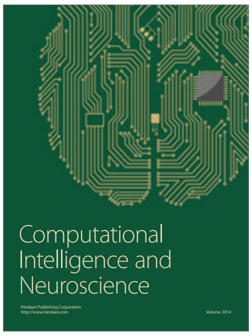

International Journal of
Biomedical Imaging


Advances in
Artificial
Neural Systems


Advances in
Software Engineering

Journal of
Robotics


Advances in
Human-Computer
Interaction


Computational
Intelligence and
Neuroscience

International Journal of
Reconfigurable
Computing

Journal of
Electrical and Computer
Engineering