In VANETs We Trust?

Characterizing RF Jamming in Vehicular Networks

Oscar Puñal
UMIC Research Centre
RWTH Aachen University
Mies-van-der-Rohe Str. 15
Aachen, Germany
punal@umic.rwth-aachen.de

Ana Aguiar
Faculty of Engineering
University of Porto, Instituto de
Telecomunicações
R. Dr. Roberto Frias s/n
Porto, Portugal
anaa@fe.up.pt

James Gross
UMIC Research Centre
RWTH Aachen University
Mies-van-der-Rohe Str. 15
Aachen, Germany
gross@umic.rwth-aachen.de

ABSTRACT

In this paper we study the impact of RF jamming on 802.11p car-to-car communications. We build a jammer on a software defined radio and implement constant, reactive and pilot jamming patterns, whose effectiveness is first measured in an anechoic chamber. We perform extensive experiments in two relevant outdoor scenarios, namely a straight road in an open space as well as a dense building scenario with a crossroad and characterize the performance of 802.11p communications under the impact of constant and reactive RF jamming. The constant jammer is able to dramatically disrupt communication regardless of the scenario. The reactive jammer exhibits a low impact in scenarios with reduced line-of-sight as its jamming success greatly depends on the relative position of the nodes. It is, however, very effective in open-space scenarios. In general, we observe that RF jamming can cause large communication-blind areas. Under these conditions, critical safety applications would simply fail in their purpose of timely warning dissemination.

Categories and Subject Descriptors

C.2.0 [Computer Communication Networks]: General- Security and protection (e.g., firewalls)

General Terms

Experimentation, Measurement, Performance, Reliability

Keywords

Vehicular networks, security, RF jamming

1. INTRODUCTION

Vehicular Ad-Hoc Networks (VANETs) have attracted the interest of researchers and industry during the last decade due to their potential to improve road safety [23] and traffic coordination [29]. If these expectations become reality, the messages exchanged by

these applications require timely and reliable delivery and VANETs will become a critical infrastructure.

Standardization efforts have recently lead to the approval of the IEEE 802.11p amendment [3], partially addressing those issues. The 802.11a physical layer (PHY) was extended, reducing the channel bandwidth from 20 MHz to 10 MHz to better cope with multipath fading, and the medium access control (MAC) layer of 802.11e is mandatory to provide channel access priority. In addition, works like [19] and [16] recommend the use of short packets and robust modulations, respectively.

Since VANETs are expected to support a wide range of safety critical applications, security threats at several layers of the protocol stack have been intensively researched, e.g. in [5, 9]. However, only few works [22, 13] have addressed the case of malicious interference attacks, i.e. radio frequency (RF) jamming, on VANETs (see Section 9 for a discussion). RF jamming has also been extensively studied in the context of generic 802.11 networks without accounting for the specificities of car-to-car communications. Besides the differences in PHY design of 802.11p compared to other 802.11 amendments, the propagation conditions of VANET are fundamentally different due to the highly dispersive and rapidly changing vehicular environment. Hence, we expect differences both in the impact of jamming and on the detection feasibility of jamming attacks by previously proposed methods. Moreover, due to the different nature of the envisioned applications (warning dissemination, ad-hoc node to node and multi hop), different types of attacks need to be considered. Therefore, experiments in uncontrolled vehicular scenarios are necessary to characterize the vulnerability (and its geographic extent) of VANETs in various propagation environments.

The major contributions of this article are twofold: 1) a description of the implementation of various state-of-the-art OFDM jamming patterns (constant, reactive and pilot) on a software-defined radio platform and the characterization of their effectiveness in an anechoic chamber; 2) extensive measurements of the impact of various RF jamming patterns on the packet delivery rate in two relevant outdoor scenarios, namely a straight road in an open space and a crossroad in a dense building scenario.

The rest of the paper is structured as follows. In Sections 2 and 3 we provide background information on 802.11p and on RF jamming, respectively. Section 4 briefly describes the approach taken in the paper. In Section 5 we describe the chosen jamming patterns and their implementation on hardware as well as the selected 802.11p devices. Measurement results from an anechoic chamber are presented in Section 6. In Section 7 we describe the results of the outdoor experiments. In Section 8 we discuss the impact of our

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

VANET'12, June 25, 2012, Low Wood Bay, Lake District, UK.
Copyright 2012 ACM 978-1-4503-1317-9/12/06 ...\$10.00.

results and future research directions. We present related work in Section 9 and conclude our work in Section 10.

2. IEEE 802.11P BACKGROUND

IEEE 802.11p [3] is part of the Wireless Access in Vehicular Environments (WAVE) standard and defines PHY and MAC layer functionalities.

2.1 Spectrum and Physical Layer

802.11p adopts the PHY from 802.11a with some modifications (Table 1) which are intended to increase the robustness of the signal to the highly dispersive vehicular environment. Communication takes place in the 5.9 GHz band, where the total bandwidth is divided into seven service channels (SCH) and one control channel (CCH). Each channel is divided into 64 OFDM subcarriers, of which 48 are used for transmitting data and 4 are used for time and frequency synchronization, and channel estimation (pilot subcarriers). The remaining 12 subcarriers are disabled to accommodate the frequency guard bands of the signal.

Parameter	802.11p	802.11a
Channel bandwidth	10 MHz	20 MHz
subcarrier spacing	156.25 kHz	312.5 kHz
Data rates	3 to 27 Mbps	6 to 54 Mbps
Slot/SIFS/DIFS time	13/32/58 μ s	9/16/34 μ s
Preamble	32 μ s	20 μ s
PLCP header (1 OFDM symbol)	8 μ s	4 μ s

Table 1: Comparison of 802.11p and 802.11a PHY parameters.

On the CCH beacon frames are broadcasted to advertise services offered on specific SCHs. The CCH is also intended for the transmission of safety critical messages. The access to CCH/SCH is done in a FDMA/TDMA fashion as specified by the *Multi-Channel Operations* of IEEE 1609.4 [4]. The latter indicates that access time is equally allocated for CCH and SCH. Specifically, out of every 100 ms, 50 ms are allocated for listening or transmitting over CCH and the remaining 50 ms for communication over SCH. It is important to guarantee reliable communication on the CCH, since the SCH is accessed over that channel and dedicated attacks may allow the attacker to block communication on all the channels.

Every 802.11p packet consists of preamble, PLCP, MAC and WSMP (WAVE Short Message Protocol) headers, and the payload. The PLCP header is transmitted using the most robust modulation, while MAC and WSMP headers are transmitted with the same modulation and coding as used for the payload. The preamble consists of 10 short training symbols, a guard interval and 2 long training symbols and has a total duration of 32 μ s (Fig. 1). It is used by the receiver to perform several tasks to assure the correct decoding of the incoming packet. During the short training phase a known bit sequence is transmitted with a periodicity of 1.6 μ s over 12 subcarriers evenly distributed over the bandwidth. This information is exploited to detect the signal, calibrate the automatic gain control (AGC), perform coarse frequency offset estimation, and synchronize the clocks of sender and receiver. The two long training symbols use 52 subcarriers to transmit a different bit sequence and are used to estimate the channel and perform a fine frequency offset estimation and a fine time synchronization. The preamble is followed by the PLCP header (8 μ s), which contains information about the modulation used for MAC header and payload (*RATE* field). It further tells the receiver how long the remaining transmission is going to last (*LENGTH* field). A parity bit is also available to detect errors in the previous PLCP header fields. If the parity bit indicates that

the PLCP header is free of errors, the receiver continues decoding incoming data for the time indicated in the *LENGTH* field.

Figure 1: IEEE 802.11p preamble and PLCP header [15].

2.2 Medium Access

The medium access in 802.11p is regulated by the CSMA/CA protocol. If a node wants to transmit a packet, it must first sense the medium idle for a certain time interval. The medium is considered idle if the detected energy is below the carrier sensing threshold. Although the setting of this threshold is not standardized, it is typically set to the same value as the receiver sensitivity. The IEEE 802.11 standard (paragraph 17.3.10.5) [15] further indicates that if the sensed energy level is above the threshold but no packet preamble is detected, the threshold is increased by 20 dB. Most commercial 802.11 devices do not consider the medium busy if they cannot detect a compliant preamble [25, 12], which is the case for our 802.11p devices. Note that the jamming signals that we use do not impact channel access at the transmitter and can only be effective at the receiver.

3. JAMMING 802.11 COMMUNICATIONS

A jammer is a device that does not comply to legitimate PHY or MAC protocols and intentionally tries to impede communication by interfering with transmitter or receiver. Deceptive jammers [28] are devices that emit standard compliant signals bypassing the default medium access policy, but in this work we focus exclusively on RF jamming attacks that can be performed on 802.11 communications. Before proceeding, we extend the classification of RF jamming methods for wireless communication in [28]:

Constant Jammer A constant jammer continuously transmits radio signals (either noise or modulated signals). This jammer is very effective but has a high energy cost and probability of being detected.

Random Jammer A random jammer features a random on/off pattern, being more energy efficient at the cost of a reduced attack efficiency.

Reactive Jammer A reactive jammer transmits radio signals only upon detection of a certain level of energy on the channel. This jammer is energy efficient and difficult to detect, as it is not present unless overlapping with the legitimate communication [24].

Pilot Jammer An OFDM pilot jammer emits radio signals by placing energy exclusively on the pilot subcarriers [10]. Given frequency synchronization between jammer and legitimate transmission, this attack is more energy efficient than a jammer employing the whole available bandwidth [10].

4. CHARACTERIZING VANET JAMMING

Vehicular ad-hoc communications are on the way to become the infrastructure for a plethora of applications that will improve traffic safety and efficiency. As a consequence, it will become a potential target for malicious attacks. Although there are several previous studies on VANET security, most have focused on higher layers of the protocol stack and only few have addressed the issue of RF jamming.

We take a first step at filling this gap by characterizing the impact of RF jamming on VANET communications. We impersonate a jammer, implementing various jamming methods on software defined radio and compare their performance. First, we assess the impact of these jammers on 802.11p communication in the static and multipath-free environment of an anechoic chamber. This allows us to understand how packet decoding is affected in each case and to quantify the difference in effectiveness of the various attacks.

In a second step, after identifying communication topologies that are relevant for VANET applications, we perform outdoor experiments to measure the damage caused by jammers. We conduct experiments with a constant and a reactive jammer in an open area and in a dense urban scenario with a crossroad. We show that a jammer can create a blind area of 250 m if transmitter and receiver are not close to each other. The blind area is reduced to 170 m around the jammer if the vehicles are moving close to each other. Moreover, we show that a crossroad in a dense urban scenario can be turned to a blind area by a constant jammer located inside a building 30 m away from that crossroad.

5. MEASUREMENT EQUIPMENT

In this section, we introduce the devices that were used for the experiments and describe their RF characteristics. We also describe how the various jamming patterns were obtained with a state-of-the-art SDR platform.

5.1 802.11p Hardware: NEC Linkbird

We used NEC Linkbird 802.11p [11] devices as sender and receiver in all experiments. These devices are reference implementations of the WAVE standard and have been widely used in other VANET experiments [18, 7]. All reported measurements were carried out at carrier frequency 5.86 GHz, which corresponds to the lowest channel (Ch. 172) of the frequency band allocated to 802.11p communications and is meant for public safety communications [3]. This channel was used as the jammer device only operates up to this frequency as described in Section 5.2. However, all results obtained in this work apply to the standard CCH as well.

Initially, we carried out a series of measurements to establish a mapping between the received signal strength indicator (RSSI) as reported by the Linkbird devices and the corresponding signal-to-noise-and-interference ratio (SNIR). This was performed to improve the assessability and comparability of our further results. The RSSI as reported by the Linkbird devices is an instantaneous characterization of the received signal power in comparison to a current estimate of the noise and interference power of the channel. It is given by an integer value within a certain range and is maintained in a register once per packet reception. As it is a proprietary implementation, RSSI values from different vendors represent in general different physical circumstances. Therefore, we were interested in establishing a more objective base for our measurement campaigns. Nevertheless, it is important to stress that the noise and interference power is only an estimate that is generated by the vendors hardware. In particular, it only represents an *approximation* of the current noise and interference power as it is determined from

the current receiver sensitivity (which can be adapted within a certain range) as well as from channel measurements during idle times. Hence, especially in the presence of interference, the reported RSSI can fluctuate significantly even if the propagation scenario is static. A more detailed discuss of this is provided in Section 6.3. Hence, **all SNIR values** reported in this paper later do not correspond to the true SNIR as given by the physical properties of the transmission scenario but **are SNIR approximates**.

In order to determine the mapping from RSSI to SNIR we first determined the transmit power of the Linkbird devices. This was done by connecting a transmitter to a spectrum analyzer which allowed the determination of the output power of the device. Determining the power of an OFDM signal is in general a difficult task [8]. We used the *maxhold* function of the spectrum analyzer to obtain the power over the signal bandwidth across a sequence of 1000 packets with random payload. This method is considered as one of the most accurate approaches for measuring the power of an OFDM signal [8]. As a result we obtained a total power of 17.58 dBm when driven at full gain, which is the configuration used in all our experiments. Note that the maximum power reported by the device specification is 21 dBm.

Based on this value for the transmit power, we then proceeded to determine the mapping between RSSI and SNIR. For this we connected transmitter and receiver via a coaxial cable (2 dB attenuation) and increased the attenuation between them step-wise by adding passive attenuator elements. This allowed us to predict precisely the received signal power while on the other hand we recorded the average RSSI for a sequence of 10000 packets. By assuming the noise power to equal the lowest receiver sensitivity of -86 dBm, we came up with the following linear model (using least square fitting) for mapping an RSSI sample σ to a SNIR value γ (in dB): $\gamma = 0.8565 \cdot \sigma - 86.35$. We used this method to convert all RSSI values to SNR throughout the experiments.

5.2 Jammer Hardware: WARP Boards

There are different ways of implementing a jammer for 802.11 networks. One can rely on commercial RF jammers which are black-box devices with high output power characteristics usually used for military operations. By properly tuning protocol compliant devices (disabling CSMA/CA carrier sensing or back-off deferrals) one can also obtain *standard compliant* jammers [28, 20].¹ One can also use programmable devices like the platform proposed in [26], which is the selected approach in this work.

We used the Wireless Open-Access Research Platform (WARP) for implementing the jammer [2]. The WARP boards provide an 802.11-like OFDM design on FPGA and a 10 MHz bandwidth 802.11a/g RF transceiver, which allows transmission at frequencies up to 5.875 GHz, hence, covering 802.11p channels 172 and 174 [3]. The board is designed to provide approximately 18 dBm output power at the 2.4 GHz band when driven at full gain. As the transmit power in the 5.9 GHz band is not specified, we measured it with the spectrum analyzer following the steps used for the Linkbird devices and obtained a transmit power of 16.75 dBm. It is important to note that the WARP implementation of the preamble does not comply to the 802.11p PHY. We tested this by using a WARP device as receiver of 802.11p packets. Making sure that energy detection was triggered, we only experienced sporadic events indicating valid 802.11p signal detection, which we regard as false positives. The damage of this jamming signal is expected to be lower than if the signal would induce the legitimate receiver to lock onto decoding the interference signal. A jamming signal can have

¹We did not use a Linkbird device as jammer because we were not able to access the necessary features in firmware.

multiple frequency/time behavior patterns with different impact on the legitimate communication [27, 10]. We implemented three RF jamming patterns, namely constant, reactive, and (constant) pilot jamming, which we describe below. Figure 2 graphically represents the behavior of the selected jammer profiles time. Note that the timings in the figure are not to scale.

Figure 2: Time behaviour of different jammer patterns.

5.2.1 Constant Jammer

Our constant jammer continuously transmitted zero-payload packets (only constituted out of the preamble and the PLCP header) by an OFDM signal with QPSK modulation. As both the content of the packet and the modulation were fixed, the OFDM signal had a certain fixed shape in the time domain and lasted $\mathcal{T}_{\text{const}} = 64 \mu\text{s}$. Before the next packet could be transmitted, there was an idle time of $\mathcal{T}_{\text{prep}} = 10 \mu\text{s}$ required to set up the next transmission. Thus, the constant jammer was active about 85% of the time with an on/off switching frequency of about 26 kHz.

5.2.2 Reactive Jammer

The reactive jammer was designed to start transmitting upon sensing energy above a certain threshold. The default OFDM design of the WARP platform features an energy detection block, which compares the instantaneous energy measured at the receive antenna with a tunable threshold Θ_E . We set the threshold to $\Theta_E = -75 \text{ dBm}$ as it proved a good trade-off between jammer sensitivity and false transmission detections. The detected energy was then compared with $(24 \text{ Byte})\Theta_E$ for a certain time $\mathcal{T}_{\text{detect}}$, which we set to $1.2 \mu\text{s}$. If during $\mathcal{T}_{\text{detect}}$ the energy remained above the threshold, a logical *one* was stored on a register. If the detected energy fell below the threshold a logical *zero* was stored. The content of the register was polled every $\mathcal{T}_{\text{poll}} = 10 \mu\text{s}$. If a logical one was read, the jammer started the transmission of a dummy zero-payload packet using an OFDM signal with QPSK modulation, like the constant jammer. The total reaction $\mathcal{T}_{\text{reaction}}$ is obtained as the sum of the detection time $\mathcal{T}_{\text{detect}} = 1.2 \mu\text{s}$, the register polling time $\mathcal{T}_{\text{poll}} = 10 \mu\text{s}$, and the preparation time $\mathcal{T}_{\text{prep}} = 10 \mu\text{s}$. As the delay introduced by the polling is not fixed and partially depends on the time the register has been storing a logical one without being polled, the introduced delay was found to be uniformly distributed in the range $[0-10] \mu\text{s}$. For the discussion of the results we consider that the overall reaction time is, in average, $16.2 \mu\text{s}$. Note that only one jamming signal is transmitted per detected 802.11p packet. Although this signal misses the beginning of the 802.11p preamble, it completely overlaps with PLCP, MAC and WSMP headers.

5.2.3 Constant Pilot Jammer

The third jamming pattern consisted of a (constant) pilot jammer as defined recently in [10], where only the four pilot OFDM subcarriers are interfered. Note that the pilot subcarriers in WARP's OFDM design are positioned as mandated by the 802.11p standard. The WARP transceiver attempted the transmission of dummy pack-

ets without employing any payload subcarrier, which theoretically results in an *infinitely* long transmission. However, we measured the exact duration of this transmission to be $\mathcal{T}_{\text{pilot}} = 2.04 \text{ ms}$. The total power used by the pilot jammer, which we measured to be 2.42 dBm , is significantly lower than that of a jammer employing all available subcarriers.

6. JAMMER EFFECTIVENESS

The first set of measurements that we conducted were performed in an anechoic chamber to cleanly characterize the impact of the selected jamming patterns on the 802.11p reception performance. Previous work [12, 14] have carried out similar studies on 802.11bg devices, and similar trends and observations can be expected, despite the differences in the PHY design of 802.11g and 802.11p. Nevertheless, this first step was of paramount importance because: 1) it provided an indicator of the performance of 802.11p communications under the presence of jamming that can be expected in the field experiments with the devices at hand; 2) it helped decide which jamming patterns to select for outdoor measurements; 3) it allowed us (as discussed later in Section 6.3) to discover and understand relevant features of the used 802.11p hardware that might not be clear; 4) it is the first attempt, to the best of our knowledge, to study the robustness of an 802.11p device to RF jamming.

6.1 Setup in Anechoic Chamber

We characterized the receiver response under various jamming profiles in terms of packet delivery rate (PDR) through measurements under static conditions. For this purpose, we used the anechoic chamber at the Faculty of Engineering at the University of Porto (FEUP), which provides a multipath-, and interference-free environment (see Fig. 3(a)).

The omni-directional antennas used in our measurements were designed to work in the 5.0-6.0 GHz band and have 6 dBi gain. We placed the transmitter antenna on a pole typically used for radiation pattern measurements and the jammer antenna on the pair pole. The receive antenna was placed on an empty cardboard box at a similar height as the other two antennas. Jamming device, transmitter, and receiver were placed outside the chamber connected via high performance cabling. We measured the distances and the path loss attenuation between all pairs of devices. Setup details are displayed in Figure 3(b). This setup was kept during all chamber experiments and the measured attenuation values were used to calculate the received signal power and jammer power at the receiver.

Using this setup and the parameterization indicated in Table 2, we configured the sending application to transmit sequences of 10000 packets and we measured the SNIR of all correctly received packets and the packet delivery rate (PDR). We reduced the effective output power of the jammer by adding attenuators between the RF output of the WARP board and its antenna to obtain different SNIR values at the receiver. We did not consider cable attenuations or antenna gains in the SNIR calculations, because they equally amplify transmitter and jammer signals.

6.2 Results in Controlled Environment

The PDR for different average SNIR² values are shown in Figure 3 for the different jamming patterns. The red curve represents the PDR obtained while the jammer was switched off. For the different jamming patterns the curves are shifted to the left, which shows – as expected – that a larger SNIR is required to achieve the same PDR if a jammer is active. When the reactive jammer was

²Recall from Section 5.1 that the SNIR values are obtained from the RSSI values by our introduced linear model.

Setup Parameters		
Linkbird	Data rate	6 Mbps (QPSK 1/2)
	P_{TX}	17.48 dBm
	Payload length	100 Byte (232 μ s)
	Packet generation rate	100 [packets/s]
Constant/Reactive	P_{TX}	16.75 dBm
	Signal duration	64 μ s
	Signal preparation time	10 μ s
Reactive	Detection time	1.2 μ s
	Total reaction delay	Unif. [11.2-21.2] μ s
	Energy detection threshold	-75 dBm
Pilot	P_{TX}	2.42 dBm
	Signal duration	2.04 ms
	Signal preparation time	10 μ s
General	Center frequency	5.860 GHz (Ch. 172)

Table 2: Setup parameters used in all our experiments.

active, the legitimate transmission required 10 dB more SNIR than in the *no-jammer* case to maintain the PDR at 100%. The effectiveness of this jamming pattern is significantly lower than that of the constant jammer. We explain this with the reaction delay of the reactive jammer, which we have measured to be around 16 μ s (Subsection 5.2) representing half of the packet's preamble (32 μ s). Hence, during the first half of the preamble there is no disturbance and the receiver can lock to the signal (time and frequency synchronization) and adapt the equalizer to the channel conditions eventually managing to adapt to the higher noise level during the second half of the preamble. In addition, as the reactive jammer only emits one signal per legitimate packet, the amount of payload bits interfered is lower than under the constant and pilot jammers.

The pilot jammer started to degrade the PDR performance at a 25 dB higher SNIR than in the *no-jammer* case. Recall that the total power measured over the 4 pilot carriers was only 2.42 dBm (14 dB less than constant jammer signal). Nevertheless, it performed only about 10 dB worse than the constant jammer over a significantly wide SNIR range, which confirms that the pilot jammer is an efficient jamming pattern against OFDM signals [10].

Finally, the constant jammer exhibited the most damaging impact leading to packet losses at 50 dB higher SNIR than without any jammer. For lower PDR values, this separation reduced to a 20 dB higher SNIR required for the same PDR. The curve for this jammer shows an unexpected behavior in the [30-50] dB range. Measurements with a higher SNIR granularity were carried out within this range to verify that the irregularity of the curve was not the consequence of a sporadic effect. All experiment repetitions revealed the same behavior, which is caused by the ambient noise immunity algorithm (ANI) implemented in the Atheros/Madwifi driver adopted by the Linkbird devices as discussed in Subsection 6.3.

For the subsequent field measurements we decided to apply only constant and reactive jammers as they provide upper and lower

Figure 3: Packet delivery rate (PDR) as function of the SNIR for various jamming patterns.

bounds, respectively, for the effectiveness of the considered jamming patterns.

6.3 Ambient Noise Immunity Algorithm

The Linkbird devices are equipped with Atheros cards, which employ a proprietary solution for interference compensation called Ambient Noise Immunity (ANI) [1]. This technique aims at reducing false packet detections, which happens every time the receiver considers an incoming interfering signal to be a valid 802.11p packet. This can negatively impact the performance of the 802.11 communication if the receiver is busy trying to decode interference, thereby missing legitimate signals. A false packet detection can be triggered by two different events. The dominant one is an observed large and sudden energy increase that exceeds a certain threshold referred to as coarse high threshold [1]. This is referred to as strong signal detection event. Furthermore, for weak incoming signals the packet detection is triggered if the receiver identifies statistically by means of correlation a periodic pattern somewhat similar to that of the short training symbols [1]. This is referred to as weak signal detection event.

In case the rate of false detections exceeds a *high* false detection threshold, the coarse high threshold is increased (i.e., which automatically reduces the sensitivity of the receiver) to a more robust configuration, which then requires a significantly larger interference power to trigger a (false) signal detection. If this first action doesn't reduce the number of false packet detections, the receiver progressively (in discrete steps) increases the coarse high threshold. Should the number of false packet detections remain above a *low* false detection threshold, the OFDM weak signal detection is completely disabled. If the number of false packet detections is satisfactory, then the weak signal detection is reactivated. Note that switching off the weak signal detection scheme may lead the receiver to ignore (weak) legitimate transmissions. This downside has been studied in [25], which reports performance degradations in OFDM-based 802.11 communications under the presence of the ANI algorithm. For more details about the algorithm we refer the reader to [1].

Figure 4 shows the time evolution of SNIR and PDR at the receiver under the presence of the constant jammer. First of all, note that the SNIR varies here although the propagation environment is kept completely constant. This is a result of the ANI algorithm, as it impacts the RSSI and hence, through the conversion by our linear model of Section 5.1 it also impacts the SNIR. This illustrates nicely that the SNIR values as obtained by our conversion are in

Figure 4: Ambient noise immunity: SNIR and PDR fluctuations under effect of constant jammer.

fact not the true physical SNIRs but instead depend on the assumption of the receiver at which power the noise and interference floor remains currently.

Furthermore, the figure is helpful to understand the ambient noise immunity adaptation steps. At the beginning we obtain very high SNIR reports due to the lack of previous background noise measurements and the corresponding setting of a very low noise floor value. We observe that high SNIR does not correlate with high PDR, which is the consequence of the false packet detections induced by the constant jammer. As a reaction to the unacceptable number of false packet detections, the receiver chooses higher interference immunity. This protection step increases the coarse high threshold which reduces the sensitivity. The consequent reduction in SNIR is interestingly linked to an increase in PDR, which reflects the benefits of ANI against interference. Afterwards, the algorithm iteratively probes different noise immunity levels. We observe two consecutive increases in average SNIR (18 dB and 30 dB) accompanied by a reduction of the PDR. This adaptation exhibits a clear periodic behavior within which we can roughly identify (apart from the initial peak) four to five different average SNIR values. We guess that these different SNIR levels map the five different interference immunity configurations indicated in [1] (Table 1).

This behavior explains the behavior of the PDR for the constant jammer in Figure 3. In that figure, at approx. 40 dB SNIR the ANI algorithm triggers an increase of the coarse high threshold to reduce the number of false packet detections caused by the larger energy detected from the jammer (strong signal detection). The resulting increase in immunity increases the PDR as discussed previously for Figure 4. Since it is not possible to precisely track the different steps of the algorithm during the experiments, we cannot provide a detailed reasoning for the steady increase in PDR between 40-30 dB SNIR. We believe, though, that this is related to the interactions between the increasing jammer power and the different false packet detection thresholds used. To some extent a similar behaviour can be observed for the pilot jammer.

7. FIELD MEASUREMENTS

We carried out experiments in two distinct scenarios: a straight road in an open area with no surrounding buildings, i.e., a nearly non-dispersive environment, and a crossroad surrounded by buildings, i.e., a highly dispersive environment. We refer to the first case in the following as **Open Space Scenario** while the second scenario is referred to as **University Campus Scenario**. In neither scenario we observed significant movement of persons, vehicles, or other objects besides the transmitter and receiver involved in the experiment. In all field experiments we used the same hardware set-

tings as in the lab (see Table 2). Transmitter, receiver and jammer were placed inside standard vehicles (unless differently indicated) and the antennas were located in the middle of the roof of each vehicle. Using these configurations we carried out experiments for different node topologies, which we describe next.

7.1 Topologies for Field Experiments

We configured two different topologies distinguished by the relative position of transmitter, receiver, and jammer. They were chosen to replicate traffic situations during which VANET communication is likely to be used for safety critical applications.

The first topology is characterized by a short and nearly constant distance between transmitter and receiver. We refer to it as **Platooning**. It mimics the situation of two vehicles following each other on a road where the dissemination of messages for control or warning can be critical. As the legitimate signal was stronger than the interference, communication is subject to higher SNIR values and so the PDR was expected to be high on average.

The second topology is characterized by a variable distance between transmitter and receiver which can become equal to the distance to the jammer. We refer to this setting as **Approaching**. It mimics vehicles moving along the same street in opposite directions like approaching a crossroad, potentially from different streets. In such situations communication for traffic coordination can be critical. In this setting the transmitter was not necessarily closer to the receiver than the jammer and the power of the legitimate signal was at the same level or even lower than that of the jammer. Hence, in this topology the SNIR values spread over a wider range than the ones considered in Figure 3.

We also used a setting in which one of the legitimately communicating vehicles stopped close to the jammer, i.e., had a variable distance to the other node and a constant small distance to the jammer. When using the constant jammer, we placed the transmitter next to the jammer to assess the effectiveness range of a jammer signal that experienced a similar path loss as the transmitter. When using the reactive jammer, we placed the receiver close to the jammer. In the latter case the jammer needed to sense a transmission to become active, and thus we wanted to investigate the range over which communication *to* a nearby vehicle could be blocked. With the constant jammer we assessed the range for which communication *from* a nearby vehicle was blocked. The results for these settings can be extrapolated to the case when the attacker "locks" onto one specific communicating node.

7.2 Open Space Scenario

Figure 5(a) shows an aerial view of the location chosen for the open space measurements. It is a 500 m wide, open field parking lot near the seafront in Leça da Palmeira in the outskirts of Porto. The location of the jammer is marked with a fire symbol, 180 m from the north end of the parking lot and slightly over 300 m from the south end. During the measurements, a few vehicles sporadically drove by (from north to south and vice-versa) at speeds up to 60 kph on a parallel street located 30 meters away from the parking lot.

7.2.1 Platooning

Figure 6(a) shows the time evolution of SNIR and PDR when transmitter and receiver started off at the north end of the parking lot (transmitter ahead) and drove south past the switched-off **jammer** to the south end of the parking lot. From there they turned and drove back to the starting point. The inter-vehicle distance was kept nearly constant yielding high SNIR reports with no packet losses.

Figure 6(b) shows the equivalent plot after turning on the **constant jammer**. A geographic visualization of the SNIR is shown in

Figure 5: Open space scenario - Platooning topology: Geographic visualization of the SNIR for three jammer behaviors: jammer switched off, constant jammer and reactive jammer.

Figure 6: Open space scenario - Platooning topology: Time evolution of SNIR and PDR.

Figure 5(b). We observed that the SNIR decreased very fast from time zero to 15 s due to the increasing interference caused by the constant jammer. Shortly after leaving the north end until 80 m behind the jammer (towards the south end) the communication was completely blocked. The jammer created a *blind area* of around 250 m, which was equivalent to 45 s at the speed of travel (approx. 30 kph). While turning at the end of the parking lot, both vehicles could communicate again for nearly 20 s (range of [60-80] s). From there they returned to the north end experiencing again a communication blackout of 250 m around the jammer.

We repeated the same movement pattern with the **reactive jammer**. SNIR and PDR are plotted in Figure 6(c) and a geographic visualization is provided in Figure 5(c). Recall that for the reactive jammer to be active it must first detect the transmitter; and to be able to impair packet delivery, it must also create sufficient interference power at the receiver. We observe that the period of no reception (PDR=0) started and ended without a corresponding decrease or increase in SNIR as observed for the constant jammer. This specific behaviour of the PDR as function of the SNIR can be exploited to detect the hidden activity of a reactive jammer. A communication breakdown of about 170 m in both directions around the reactive jammer, corresponding to around 30 s, is clearly visible in Figure 6(c). The interference range of the reactive jammer was shorter than for the constant jammer: 170 m vs 250 m. Even though the reactive jammer was less effective, it still caused a significant damage to the communication in this scenario.

The movement pattern used for these experiments is the best case for the legitimate communication, as transmitter and receiver are very close to each other. Still, the effects of both jamming patterns on car-to-car communication was alarming.

7.2.2 Approaching

We carried out experiments with the movement patterns corresponding to the Approaching topology but no packets were received during the whole experiment, so we do not show the results here. When the receiver and transmitter started at opposite ends of the parking lot and approached each other, even while crossing each-other near the jammer communication was not possible ac-

cording to our experiments for any jammer setting. This is because the jammer was closer to the receiver than the transmitter most of the time. Thus, the blind area for the Approaching topology was as large as the parking lot (ca. 500 m). Finally, we placed the transmitter next to the constant jammer and moved the receiver from the north to the south end and back. Again, only few packets were received, which revealed a jammed area of nearly 500 m. With the receiver next to the reactive jammer similar results were observed.

7.3 University Campus Scenario

Figure 9 shows the aerial view of the University Campus scenario. The center of the picture can be considered as a dense urban scenario, where a narrow street is surrounded by buildings and cars parked on the north side (see Figure 7(a)). The street to the north is wider, but it is also surrounded by buildings on both sides. A 35 m long and 14 m wide parking lot in the south, marked with a C, is completely surrounded by buildings (see Figure 7(b)). We placed the jammer inside a building (behind a window on the ground floor) close to that point. This represented an advantageous scenario for the legitimate communication, as placing the jammer outside would have caused higher interference at the receiver in any topology. The parking lot and the jammer location are indicated in Figure 7(b). The parallel east-west streets are interconnected by a passage that provides nearly line-of-sight (LOS). This can indirectly be seen in Figure 9, which shows SNIR reports from correctly received packets at the northern street that were received through that passage.

7.3.1 Platooning

The communication started at point A and finished at point C after two laps around the block. In Figure 8(b) we observe that the **constant jammer** had potential to disrupt the communication for a period of 20 s (50 s to 70 s) from inside a building on a side street at a distance of 33 m from the crossroads. This corresponded to creating a communication blind area of 167 m at a speed of 30 kph on an orthogonal road, including segments for which there is no line-of-sight. When approaching (or leaving) the jammed area, we observed a progressive reduction (or increase) of the SNIR from

Figure 8: University Campus - Platooning topology: Time evolution of SNIR and PDR.

Figure 7: University Campus: Propagation environment.

35 dB to 10 dB (or vice-versa). The measurement ended with both cars approaching the parking lot and stopping near the jammer, which explains the drop of PDR at the end of the measurement.

Figure 8(c) shows similar plots for a **reactive jammer**. In this case, transmitter and receiver started at point A and stopped at point B after two laps. We observed that this jamming pattern had only a very limited impact on the transmission. Since the reactive jammer was far away from the transmitter-receiver pair, the communication was characterized by a high SNIR. In addition, the reactive jammer only sensed the transmitter for a short period of time. It still had a noticeable impact that led to a reduction of the SNIR (lowered to 20/15 dB) and a slight decrease in PDR. The communication conditions were good enough to avoid significant packet losses, coinciding to what was expected from the jammer effectiveness characterized in Section 6.2.

7.3.2 Approaching

Figure 9: University Campus aerial view. Graphic SNIR reports for transmitter near constant jammer.

Figure 9 shows the relevant points for this measurement, as well as the SNIR measured at different points for the Approaching scenario under the impact of the **constant jammer**. Figure 10(b) shows the obtained time evolution of the SNIR and PDR. The trans-

mitter was initially located at the entrance of the parking lot (point D), next to the road and in LOS to the receiver (point A). The first and second gaps in Figure 10(b) correspond to the parts of the trajectory where the receiver was shadowed by the two large buildings. Then, between seconds 89 and 120, the vehicles could communicate (despite a poor PDR) around the north-west and the south-west corner of the trajectory. The vehicles stopped communicating 50 m from the intersection although the devices had LOS and the transmitter was 30 m closer to the receiver than the jammer. Communication was resumed on the second lap through the near LOS passage between the two large buildings. When the receiver approached the transmitter for the second time, the transmitter drove backwards to the end of the parking lot and the receiver entered the parking lot, where the measurement was stopped.

Figure 10(c) shows the impact of the **reactive jammer** in the same topology. Again, we observed a much more limited impact than that for the constant jammer. As the jammer was located close to the transmitter, it continuously detected energy that triggered a reactive transmission resulting in a reduced PDR even at high SNIR values. These SNIR reports did not reflect the signal of the reactive jammer, as it was always covered by the legitimate transmission. For this reason we obtained PDR drops down to 60% although high SNIR values (30 to 45 dB) were measured. Summarizing, the damage of a reactive jammer in a dense-urban scenario was remarkably low compared to its effectiveness in the open space scenario.

8. DISCUSSION

We have shown through extensive experiments that an RF jammer can severely impact VANET communication and the supported applications. Hence, if VANETs are to serve as infrastructure for human safety and traffic coordination, it is imperative to make them more robust in the presence of RF interference. Assuming that it is possible to detect the presence of a jammer, several actions can be undertaken at various layers of the protocol stack. At the application layer a warning can be sent to the user indicating that the system is malfunctioning and cannot be trusted. At the network layer, it may be feasible to route around the jammed area. At the channel management level, the operating channel can be switched to avoid the jammer. A shift in carrier frequency of 5 MHz was measured in [12] as enough separation to mostly overcome the impact of jamming. Unfortunately, the current 802.11p standard does not possess any means to change the control channel, which is clearly a single point of failure in a jamming scenario. The dynamic selection of the control channel could increase robustness by overcoming the impact of static jammers. However, it is not clear if the channel coordination task can be fast and efficient enough in vehicular environments, which are characterized by fast topology changes and potentially large number of nodes. In Section 6.3 we showed that

Figure 10: University Campus - Approaching topology: Time evolution of SNIR and PDR with transmitter near the jammer.

interference mitigation techniques as the Atheros proprietary ambient noise immunity algorithm (ANI) can increase resilience to constant RF jamming by up to 20 dB. Unfortunately, we were not able to characterize the impact of the ANI algorithm in our field experiments due to limited resources, but we shall address the matter in future work. The experiments conducted in Section 6.2 showed that the preamble of the 802.11p signal is very sensitive to RF jamming, in agreement with the observations in [12]. Thus, reliability could be increased if more robust preamble designs were available in 802.11p.

We have so far assumed that a jamming device could be identified, which unfortunately is not a trivial task especially under the severe delivery constraints of safety critical messages. For instance, the authors in [28] propose various statistical methods to detect RF jamming based on RSSI measurements. They track the time evolution of the RSSI and observe that the pattern of the sampled energy reports can be useful to separate information signal from jamming. However, they conclude that these metrics alone are not able to detect every type of RF jamming and propose the combined analysis of different metrics (e.g., geographic position, medium access delay, PDR and RSSI). As a result of our outdoor experiments we have observed that tracking the time evolution of SNIR and PDR could help to identify the presence of a reactive RF jammer. This jamming profile is difficult to detect [24], but it leads to a sudden drop in PDR in the presence of a steady high SNIR (see Fig. 6(c)), which might be useful for detecting the presence of a jammer. This approach and others need to be further explored.

This work provides a first characterization of different types of jammers and their diverse impact in vehicle-to-vehicle communication. While the results from the anechoic chamber may be used as realistic VANET RF jamming models for improving simulation accuracy and analysis, the results from the field trials will hopefully drive research on detection and mitigation methods, as well as system level considerations like leveraging cellular networks as a fall-back solution. We will make our data publicly available on *crawdad* to foster the re-use and fast progress on the topic.

9. RELATED WORK

To the best of our knowledge, the only previous works focusing on RF jamming attacks in VANETs are [13, 22]. The work in [13] presents an approach for detecting reactive RF jamming in 802.11p networks, but it does not assess the impact of RF jamming nor uses realistic VANET scenarios for evaluation. The authors in [22] study, by means of network simulations, the impact of RF jamming on the dissemination of geocast messages. The attacker model consists of an 802.11p device tuned as a reactive jammer that sends a short signal upon sensing energy on the medium. The authors show that reacting upon sensing energy above the card

sensitivity is significantly more efficient (up to 20%) than reacting only if the sensed SNIR is sufficient to decode the incoming packet. However, both attacks are able to block the dissemination of geocast messages in a simulated two lane highway. In a city scenario the situation changes as there are alternative paths to disseminate the messages around the jammer. While these results are consistent with our observations from the field measurements, our work is broader, covering a wider range of jammer profiles and their parameters. Moreover, our characterization provides a more realistic jammer model for such large scale simulation studies.

On the other hand, there is some related work on jamming at both MAC [6, 21] and PHY [14] for generic 802.11 WLANs. [12] studied the vulnerabilities of 802.11b/g hardware to RF interference, which are associated to timing recovery and dynamic range selection issues. The authors considered a jammer that emits DSSS or OFDM modulated non-compliant signals and showed that weak interference (30 dB less power than the legitimate signal) can significantly disrupt the communication by impeding time recovery. The *dynamic range* and the automatic gain control (AGC) are adapted to accommodate incoming energy into a certain voltage range, based on the energy level detected during the preamble of the packet. A random jammer can cause overflow/underflow problems, by starting/finishing transmission once the AGC has already been set [12]. In our work, we partially confirm the importance of correct time recovery by showing the degradation in effectiveness of the reactive jammer due to missing the first part of the preamble. As future work we will allow our reactive jammer to interfere completely with the payload to accurately assess the impact of missing the initial part of the preamble. In the same work, a narrow-band Zigbee jammer (5 MHz bandwidth) located 2 MHz from the operative 802.11b channel achieved a similar damage on the legitimate transmission. If the interferer was 5 MHz away from the operative channel the impact of the jammers almost vanished.

The authors in [17] present results for the error performance of 802.11b/g networks under the influence of RF jamming. Their results show that wide-band jamming damages OFDM-based 802.11g communications more severely (up to 7 dB) than they affect 802.11b (spread spectrum). The authors in [14] show that a constant wide-band noise signal is more efficient (3-4 dB) than a constant wide-band digitally modulated signal at disrupting 802.11g communications (16-QAM). The authors further show that the effectiveness of pulsed wide-band noise jamming (equivalent to random jamming with fixed on/off behaviour) is closely related to the pulse period and pulse duration. Their measurements show that a flow (1900 packets/sec) of BPSK modulated 250 Byte long packets can be completely corrupted with a 300 μ s pulsed signal with a period of 1 ms.

10. CONCLUSIONS

We studied the impact of a constant, a reactive, and a pilot RF jammer on 802.11p car-to-car communications through extensive laboratory experiments. Moreover, we provided an insight to the threats associated with constant and reactive jamming signals in various outdoor environments and for different vehicle moving patterns. In all our experiments we observed a negative impact of RF jamming, ranging from just slight reduction in PDR to communication blind areas up to 500 m. The constant jammer was significantly more damaging than the reactive jammer in all the considered scenarios and in open space environments both jammer profiles achieved a remarkably larger effectiveness than in dense urban scenarios. In general, we show that the impact of RF jamming should be considered in the design of reliable car-to-car communications to guarantee robust and trustful on-board safety applications. While this work is the first step in that direction, a better characterization of the jammer effectiveness is still required. Future work should include more detail in the evaluation of the jamming patterns to characterize the achievable resilience to jamming by means of a more robust PHY preamble design. Also, future work should consider the use of different 802.11p hardware to provide more generalizable statements.

11. ACKNOWLEDGMENTS

This research was partly funded by the DFG Cluster of Excellence on Ultra High-Speed Mobile Information and Communication (UMIC), German Research Foundation grant DFG EXC 89 and partly funded by the FCT project PEst-OE/EEI/LA0008/2011. We would also like to thank Henrique Salgado and João Oliveira of INESC Porto for helping us with the characterization of the hardware devices.

12. REFERENCES

- [1] Ambient Noise Immunity (ANI) Patent. <http://www.wipo.int/pctdb/en/wo.jsp?wo=2005067154>.
- [2] Rice University WARP Project. <http://warp.rice.edu>.
- [3] IEEE 802.11p – Wireless Access in Vehicular Environments, Amendment 6 to 802.11, July 2010.
- [4] IEEE Standard for Wireless Access in Vehicular Environments (WAVE)–Multi-channel Operation, July 2011.
- [5] A. Aijaz, B. Bochow, F. Dötzer, A. Festag, M. Gerlach, R. Kroh, and T. Leinmüller. Attacks on Inter Vehicle Communication Systems - an Analysis. In *Proc. of WIT*, 2006.
- [6] J. Bellardo and S. Savage. 802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions. In *Proc. of USENIX*, 2003.
- [7] M. Boban, T. T. V. Vinhoza, M. Ferreira, J. Barros, and O. Tonguz. Impact of Vehicles as Obstacles in Vehicular Ad Hoc Networks. *IEEE Journal on Selected Areas in Communications*, 29(1):15–28, 2011.
- [8] M. Briggs, J. Martinez, D. Bare, W. M. Ave, and A. R. Requirements. Power Measurements of OFDM Signals. In *Proc. of EMC*, 2004.
- [9] B. K. Chaurasia, S. Verma, and G. S. Tomar. Attacks on Anonymity in VANET. In *Proc. of CIC*, 2011.
- [10] T. Clancy. Efficient OFDM Denial: Pilot Jamming and Pilot Nulling. In *Proc. of ICC*, 2011.
- [11] A. Festag, R. Baldessari, W. Zhang, and L. Le. CAR-2-X Communication SDK - A Software Toolkit for Rapid Application Development and Experimentations. In *Proc. of ICC Workshops*, 2009.
- [12] R. Gummadi, D. Wetherall, B. Greenstein, and S. Seshan. Understanding and Mitigating the Impact of RF Interference on 802.11 Networks. In *Proc. of SIGCOMM*, 2007.
- [13] A. Hamieh, J. Ben-Othman, and L. Mokdad. Detection of Radio Interference Attacks in VANET. In *Proc. of GLOBECOM*, 2009.
- [14] I. Harjula, J. Pinola, and J. Prokkola. Performance of IEEE 802.11 Based WLAN Devices under Various Jamming Signals. In *Proc. of MILCOM*, 2011.
- [15] IEEE. 802.11 – Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 2007.
- [16] D. Jiang, Q. Chen, and L. Delgrossi. Optimal Data Rate Selection for Vehicle Safety Communications. In *Proc. of VANET*, 2008.
- [17] T. Karhima, A. Silvennoinen, M. Hall, and S.-G. Haggman. IEEE 802.11b/g WLAN Tolerance to Jamming. In *Proc. of MILCOM*, 2004.
- [18] T. Mangel, O. Klemp, and H. Hartenstein. 5.9 GHz Inter-Vehicle Communication at Intersections: A Validated Non-Line-of-Sight Path-Loss and Fading Model. *EURASIP Journal on Wireless Communications and Networking*, 2011.
- [19] A. Paier, D. Faetani, and C. Mecklenbrauker. Performance Evaluation of IEEE 802.11p Physical Layer Infrastructure-to-Vehicle Real-World Measurements. In *Proc. of ISABEL*, 2010.
- [20] K. Pelechrinis, I. Broustis, S. Krishnamurthy, and C. Gkantsidis. A Measurement-Driven Anti-Jamming System for 802.11 Networks. *IEEE/ACM Transactions on Networking*, 19(4):1208–1222, 2011.
- [21] K. Pelechrinis, M. Iliofotou, and S. Krishnamurthy. Denial of Service Attacks in Wireless Networks: The Case of Jammers. *IEEE Communications Surveys Tutorials*, 2011.
- [22] E. Schoch, F. Kargl, and T. Leinmüller. Vulnerabilities of Geocast Message Distribution. In *Proc. of Autonet*, 2007.
- [23] M. Segata and R. Lo Cigno. Emergency Braking: A Study of Network and Application Performance. In *Proc. of VANET*, 2011.
- [24] M. Strasser, B. Danev, and S. Čapkun. Detection of Reactive Jamming in Sensor Networks. *ACM Transactions on Sensor Networks*, 7(2):1–16, 2010.
- [25] I. Tinnirello, D. Giustiniano, L. Scalia, and G. Bianchi. On the Side-Effects of Proprietary Solutions for Fading and Interference Mitigation in IEEE 802.11b/g Outdoor Links. *Computer Networks*, 53(2):141–152, 2009.
- [26] M. Wilhelm, I. Martinovic, J. B. Schmitt, and V. Lenders. WiSec 2011 Demo: RFReact - A Real-Time Capable and Channel-Aware Jamming Platform. *ACM SIGMOBILE Mobile Computing and Communications Review*, 15(3):41–42, 2011.
- [27] W. Xu, K. Ma, W. Trappe, and Y. Zhang. Jamming Sensor Networks: Attack and Defense Strategies. *IEEE Network*, 20(3):41–47, 2006.
- [28] W. Xu, W. Trappe, Y. Zhang, and T. Wood. The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks. In *Proc. of MobiHoc*, 2005.
- [29] Y. Zhang and G. Cao. V-PADA: Vehicle-Platoon-Aware Data Access in VANETs. *IEEE Transactions on Vehicular Technology*, 60(5):2326–2339, 2011.