Investigating Bit Error Patterns for Radar Pulse Detection in IEEE 802.11

Claudio Pisa, Andres Garcia-Saavedra, and Douglas J. Leith

Hamilton Institute, NUI Maynooth
Maynooth, Ireland
claudio.pisa@uniroma2.it, {andres.garciasaavedra, doug.leith}@nuim.ie

***Abstract*—The shift towards use of the 5 GHz band by WiFi networks comes with the requirement that these networks coexist safely with existing systems using that band, e.g., meteorology, aeronautics or military radars. Regulatory bodies are mandating the implementation of Dynamic Frequency Selection (DFS) in wireless communication protocols to (i) detect radar operations and (ii) move away from channels populated by these. Conventional approaches to implementing such mechanisms, however, can result in massive underutilization of the radio channel since the radio must be kept silent for a large amount of time in order to ensure sufficient detection accuracy. This inevitably impacts the throughput capacity of the wireless network. In this paper, we consider whether bit-error patterns at the receiver of a WiFi link can be used for radar detection. In our experimental study, we adopt a pair-packet transmission technique to mitigate the interference inherent to the 802.11 protocol due to, e.g., other contending stations. Our initial results show that the observation of bit-error patterns due to radar interferences is indeed possible, establishing that the potential exists to design unobtrusive detection mechanisms that work transparently with existing network protocols without loss of network capacity.**

Keywords–Radar; 802.11; Interference management.

I. INTRODUCTION

The growing density of radio frequency (RF) transceivers operating in the ISM 2.4 GHz band (Industrial, Scientific and Medical radio band) is placing increasing pressure on the limited spectral resources available (up to 13 channels spaced 5 MHz apart) for e.g., IEEE 802.11b/g [1], ZigBee [2] or Bluetooth [3] users. This is encouraging greater utilization of the wider 5 GHz band (up to 25 channels of 20 MHz) for newer WiFi standards, first with IEEE 802.11n and ultimately with the advent of IEEE 802.11ac [4] which only uses this band.

The trend towards utilization of the 5 GHz band in commodity wireless devices potentially impacts the functioning of pre-existing communication systems, e.g. meteorological radars [5]. Weather radars periodically emit unidirectional electromagnetic pulses and listen for echoes, e.g., reflected by raindrops. Fig. 1 illustrates the regular behavior of a radar that emits bursts of pulses separated by a time equal to T_{PR}. For each transmitted pulse, the radar processes the echoes for a measurement time T_{meas} and then remains idle for an Inter-Measurement Gap time T_{IMG} before the next pulse is transmitted. For example, Fig. 2 shows measured weather radar traces taken with a Rohde & Schwarz FSL-6 *spectrum analyzer* near to Dublin airport in Ireland. These measurements show bursts of electromagnetic pulses, with $3ms$ inter-pulse separation time. From Fig. 2(b) it can be seen that on a larger time-scale the amplitude of transmissions is periodic in nature, with a period of approximately 20s. This is attributed to periodic rotation of the radar antenna, with high amplitudes corresponding to intervals when the radar antenna is directed towards the spectrum analyzer.

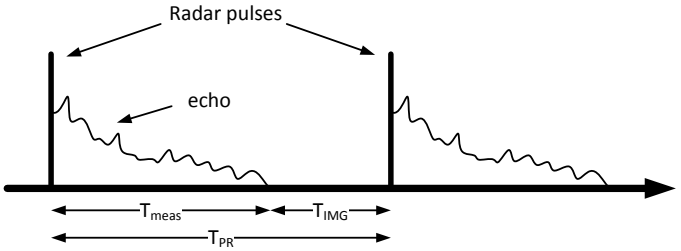
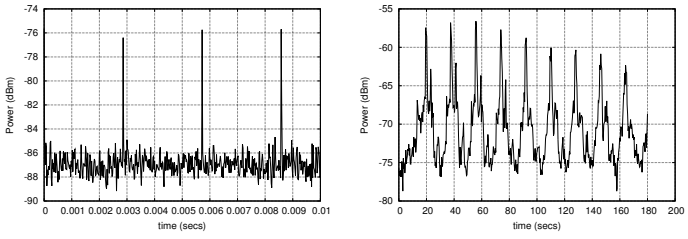


Figure 1: Schematic illustrating radar signals in the time domain.



(a) Small timescale. (b) Large timescale.

Figure 2: Weather radar time history near Dublin airport, Ireland.

In order to facilitate coexistence, Dynamic Frequency Selection (DFS) is enforced for unlicensed devices, e.g., through FCC [6] regulations in North America and ETSI [7] regulations in Europe. To meet these regulatory requirements, the IEEE 802.11h [1] amendment introduces DFS to the IEEE 802.11 PHY/MAC standard. However, although the 802.11h specifies the mechanisms for supporting DFS, the ultimate responsibility for implementing efficient radar detection schemes lies with the device manufacturer.

DFS mandates that the master device (e.g., the Access Point in a WLAN) monitors the channel for potential radar interference for at least the *channel availability check time*. A major issue with this requirement is that no transmissions can occur during this check time, which may be up to 10 minutes duration for some channels [7]. A further issue is that, even after the check time has elapsed, when using half-duplex radios, radar detection cannot be carried out while data is being transmitted/received. Hence, radar detection in future dense (and heavily loaded) wireless networks is likely to be problematic. Moreover, weather radar technology keeps

 ISBN: 978-1-61208-347-6

changing, with more complex and faster scan patterns that inflate the ratio of false positives in legacy wireless devices, scaling up dramatically the amount of sensing time needed and so of channel unavailability.

In this paper, we present initial results of our experimental evaluation of radar detection through *in-service* bit-error pattern recognition. The ability to detect (and react to) the presence of radar signals while a transmission is ongoing not only offers the potential to increase the spectrum efficiency, but also to improve the reliability of radar detection in heavily loaded networks.

The rest of the paper is structured as follow. A brief survey of related literature is given in Section II, the description of the experimental methodology in Section III, and a set of representative results in Section IV. Finally, in Section V we discuss the open issues to resolve in future work, and Section VI concludes the paper.

II. Related Work

Most of the related literature focuses on the design of off-line detectors. For instance, in [8] the authors develop a detector based on Compressive Sensing (CS), while [9] designs a radar detector based on a Constant False Alarm Rate (CFAR) and a Complex Approximate Message Passing (CAMP) algorithm. [10] evaluates a few algorithms based on a matched filtering technique and propose a method based on power detection in the time domain. However, these detectors, if implemented in a regular wireless device with a half-duplex transceiver, could only work while communication is not ongoing, which limits its applicability as explained above.

The coexistence between IEEE 802.11 transceivers implementing DFS and radars has been studied in [5], [11]. These evaluate DFS in the presence of a Doppler weather radar system and show that the 802.11 radio introduces an additive and uncorrelated noise into the radar system.

A few works analyze the radar detection probabilities. Within the FCC and ETSI standards, the computation of the detection probability was carried out initially using a basic random transmission model [12]. The authors of [13] perform a theoretical evaluation of the detection of radar pulses in time division duplexed systems, and compute the expected number of pulses occurring during the receive period of a transmission.

In contrast to all previous works, this paper is, to the best of our knowledge, the first attempt to experimentally assess radar detection via bit-error recognition over received packets.

III. Methodology

The key idea is to search for radar interference footprints, via inspection of bit error patterns, while packet processing is ongoing at the receiver. Fig. 3 illustrates this idea with a burst of eleven pulses (at the bottom) and three examples of data packet communication with different packet rates and lengths (at the top). Those packets, transmitted concurrently with one or more radar pulses, will be disrupted by a burst of bit errors (shown in black in the figure). The observation of this footprint, jointly with the knowledge of the underlying radar process, should make possible the detection of radar signals.

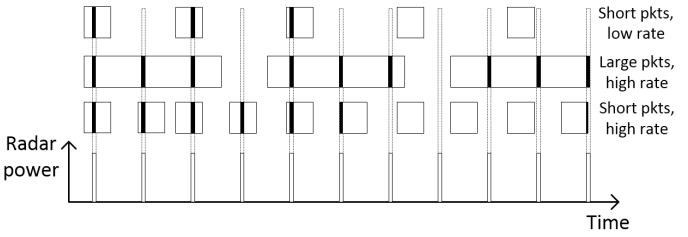
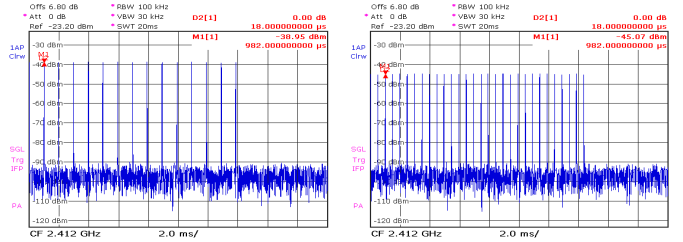


Figure 3: Radar interference footprint during packet reception.



(a) Radar test signal type 2 [7] (b) Radar test signal with double speed

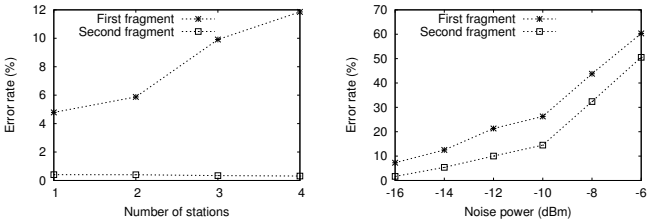
Figure 4: Measured traces while radar emulator is in operation.

The first step to study the feasibility of bit-error pattern recognition for radar detection requires a controlled environment. To this end, we programmed a Rohde&Schwarz SMBV100A *vector signal generator* to emulate the behavior of a radar. Unless otherwise stated, each pulse width is set to 1 μs, $PRF = 1/T_{PR} = 1000\ s^{-1}$ and we send bursts of 15 pulses, to mimic the behavior of a radar test signal type 2 [7]. Given the traces collected with our spectrum analyzer when our "radar emulator" is in operation, shown in Fig. 4, and their similarity with respect to those of Fig. 2, we validate this set-up for our experiments.

One of the main challenges in the detection of errors caused by the operation of radars is the ability to distinguish these from other sources of error, for instance those caused by another transmitter within the same WLAN, i.e., *collisions*. Collisions are part of the correct operation of the CSMA/CA MAC protocol in IEEE 802.11 and are caused by two or more stations selecting the same slot to transmit during the random backoff procedure. If a station is successful (i.e., its backoff counter reached zero before other senders), the other stations will defer their backoff while the channel is not *idle*. The physical layer (PHY) implements a Clear Channel Assessment (CCA) scheme based on a carrier-sense threshold for energy detection, and the MAC uses a Network Allocation Vector (NAV) parameter transported in each header to inform other stations about the duration of the ongoing transmission. A channel is idle only if the CCA fails to detect a carrier and if the NAV timer is zero. However, collisions are not the only cause of packet impairment. Nodes that are too far to be able to decode the NAV of concurrent transmissions whose energy level is below the CCA threshold (i.e., *hidden* nodes) could cause errors in theoretically successful transmissions as well. In order to narrow down the sources of interference to just those due to radar coexistence, we applied the technique proposed in [14]. To this end, we force each packet to be fragmented at the MAC layer to ensure that the second and subsequent fragments are protected from both collisions and

 ISBN: 978-1-61208-347-6

hidden nodes. The protection against collisions is granted by the NAV value used in the first fragment, which is set to the amount of time required to send all the fragments. Each fragment is sent back-to-back (separated by a SIFS interval) to the AP and individually acknowledged by the AP; given the fact that all stations should be able to hear the AP's transmissions, and therefore the NAV value carried within the acknowledgment frames, these fragments are protected against hidden nodes (similarly to the RTS/CTS scheme).



(a) Test link and other interfering links. (b) Test link and a source of noise.

Figure 5: Technique to narrow down sources of interferences.

We have run two simple experiments to validate this methodology; the results are shown in Fig. 5. In both experiments, we configure a laptop as a WiFi AP transmitting test traffic to another laptop, configured as a WiFi client. The AP sends 50 bursts of 3000 ICMP packets, with 1150 bytes of payload, generated with SING, an ICMP-packet generator which allows customization of the transmitted packets. The transmission power is set to 16dBm and we set a fragmentation threshold of 600 bytes to force the delivery of 2 fragments per packet (i.e., the first has to contend for channel access, the second is protected against collisions and hidden nodes). In the first experiment, the AP transmits the test traffic towards the client, while we increase the number of additional contending stations to the network. Fig. 5a depicts the ratio of bit errors for each of the pair of packets sent in each transmission opportunity. As we can see, the first fragment is severely affected by the growing number of collisions incurred by the additional contending stations. On the other hand, the second fragment is unaffected by this type of interference source. In the second experiment we switch the additional contending stations for the signal generator, to generate synthetic RF noise. Fig. 5b shows the error rate as a function of the power of the noise generated. The results indicate that both the first and second fragment experience the same effects upon a noisy environment. These two experiments serve as validation for this technique to identify bit-error patterns due to radar signals while excluding those inherent to the IEEE 802.11 MAC protocol. In the following, we will apply this technique, along with our radar emulator, to study the bit-error patterns in received frames and its feasibility in the detection of radars in the environment.

IV. Measurements

We set up two laptops with an IEEE 802.11b/g Atheros AR5008 wireless card each using the driver madwifi 0.9.6 and separated by $100cm$. Note that we have disabled the IEEE 802.11.h capabilities from the driver to avoid that the legacy DFS operation affecting channel selection upon the observation of our radar signals. One laptop serves as WiFi AP and the other as a regular client. Each experiment consists of the transmission of a stream of packets from the AP to the client. Each UDP packet transports a 1796-byte payload with known information, which allows us to assess the error patterns occurring at the receiver. In the following, we summarize our initial results where we compare the trace given by the spectrum analyzer and the error pattern found in selected packets.

In the first experiment, each packet is sent at 1 Mbps (so they are of relatively long duration). Fig. 6 top shows how the end of a packet transmission collides with one pulse from the beginning of a radar burst. In Fig. 6 bottom we illustrate the results of the packet inspection at the receiver. We mark the beginning of the payload (the part that we process), each bit error found after decoding (we also zoom in the burst of errors) and the end of the packet. This figure shows that the footprint of the colliding radar pulse is clearly observable. However, in this case, the observation of one burst of errors is not sufficient to infer the presence of a radar signal.

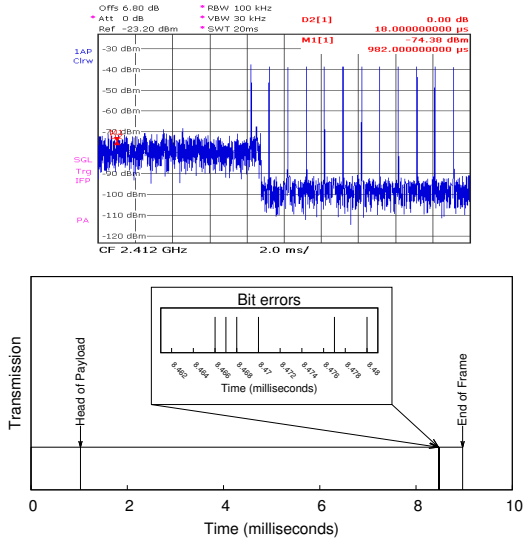


Figure 6: Radar traces and bit error patterns, PHY rate 1Mbps.

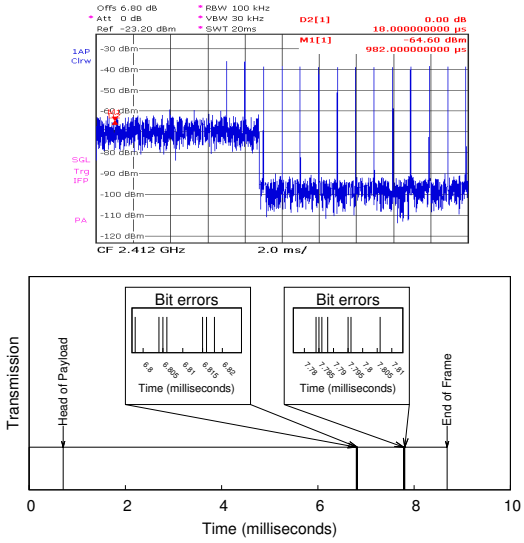


Figure 7: Radar traces and bit error patterns, PHY rate 1Mbps.

 ISBN: 978-1-61208-347-6

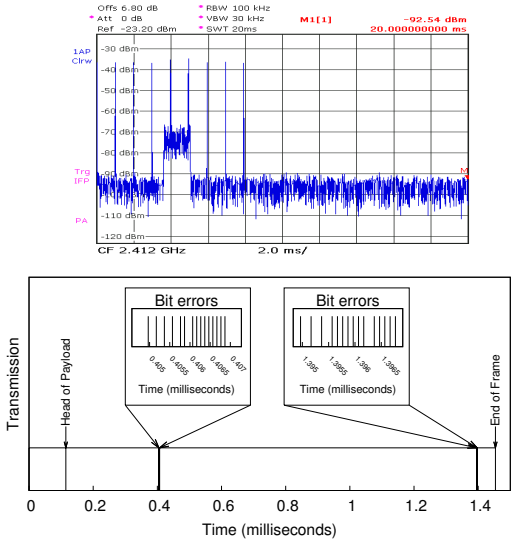


Figure 8: Radar traces and bit error patterns, PHY rate 6Mbps.

Fig. 7 shows the resulting packet processing of another packet sent at 1 Mbps where two pulses of a radar signal corrupts the payload of the data transmission. We can easily identify the radar footprint out of the packet inspection, i.e., two bursts of errors separated by $1ms$ (PRF of our test radar signal) with pulses of approximately $1\mu s$ duration.

We now configure the AP to transmit 6-Mbps packets. Similarly as before, Fig 8 depicts the results for a selected packet of this experiment which is corrupted by two radar pulses. This result allows a similar observation as in the previous case, that is, we found two burst of bit errors of approximately $1\mu s$ of duration and separated by $1ms$, matching the characteristics of the underlying radar test signal.

V. Open Questions

The experiments we have carried out so far unveil a clear footprint from radar interference which is observable while a packet reception is being processed. However, the heterogeneous (and random) nature of real-life data packet communications makes the actual design of a practical algorithm for radar detection through bit-error pattern recognition inherently challenging. The major challenge is indeed to discern the constant rate footprint of radar bursts from a decoupled data transmission, i.e., with independent rate/size distribution.

Fig. 3 illustrates this with three examples with different packet rates and packet lengths (although packet rate and length are constant in these examples, which will not be the case in general). First, a single large packet might be enough to observe a constant error burst rate that would trigger a radar presence alarm. However, the case with short packets requires a longer-term observation. Second, the analysis of consecutive packets from a high packet rate transmission could also be sufficient. However, slower rates (and/or heterogeneous distributions) might hide the presence of a radar given that most of its bursts could coincide with idle inter-frame spaces, not causing bit errors.

VI. Conclusions

Dynamic Frequency Selection (DFS) is a mandatory scheme for wireless communication protocols operating in the 5 Ghz band in order to mitigate the interference caused to coexistent systems such as radars. Unfortunately, conventional implementations may cause severe underutilization of resources and poor performance in heavy loaded networks. Motivated by this observation, we explore the feasibility of radar detection via duly observation of bit-error patterns in received packets. In this paper, we present the initial results of our experimental evaluation and discuss a series of open questions that need to be resolved to design an effective *in-service* detection mechanism.

Acknowledgment

Work supported by Science Foundation Ireland grant 11/PI/11771.

References

[1] IEEE Standard - Local and metropolitan area networks - Part 11: Wireless LAN Medium Access Control and Physical Layer specifications, IEEE Std. 802.11, 2012.

[2] IEEE Standard - Local and metropolitan area networks - Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs), IEEE Std., 2013.

[3] IEEE Standard - Loca Compressive Sensing.l and Metropolitan Area Networks - Part 15.1: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs), IEEE Std., 2005.

[4] IEEE Std 802.11ac-2013 (Amendment to IEEE Std 802.11-2012, IEEE Std. 802.11, 2013.

[5] A. L. Brandão, J. Sydor, W. Brett, J. Scott, P. Joe, and D. Hung, "5 GHz RLAN interference on active meteorological radars," in Vehicular Technology Conference, 2005. VTC 2005-Spring. 2005 IEEE 61st, vol. 2. IEEE, June 2005, pp. 1328–1332.

[6] FCC, "Federal Communications Commission Report and Order FCC 03 287 released November 18," 2003.

[7] ETSI, "EN 301 893 v1.7.1: Broadband Radio Access Networks (BRAN); 5 GHz high performance RLAN; Harmonized EN covering essential requirements of article 3.2 of the R&TTE Directive," June 2012.

[8] L. Anitori, M. Otten, and P. Hoogeboom, "Detection performance of compressive sensing applied to radar," in Radar Conference (RADAR), 2011 IEEE. IEEE, 2011, pp. 200–205.

[9] L. Anitori, M. Otten, W. van Rossum, A. Maleki, and R. Baraniuk, "Compressive cfar radar detection," in Radar Conference (RADAR), 2012 IEEE. IEEE, 2012, pp. 0320–0325.

[10] M. Wen and L. Hanwen, "Radar detection for 802.11 a systems in 5 ghz band," in Wireless Communications, Networking and Mobile Computing, 2005. Proceedings. 2005 International Conference on, vol. 1. IEEE, 2005, pp. 512–514.

[11] J. Kruys, ""dfs compliance criteria, status and prospects"," in Oaktree Wireless, 2009.

[12] ITU, "Recommendation ITU-R M.1652, International Telecommunications Union," 2003.

[13] B. W. Zarikoff and D. J. Leith, "Analysis of radar detection probabilities in time division duplexed systems," in Communications (ICC), 2012 IEEE International Conference on. IEEE, 2012, pp. 1698–1702.

[14] D. Giustiniano, D. Malone, D. J. Leith, and K. Papagiannaki, "Measuring transmission opportunities in 802.11 links," IEEE/ACM Transactions on Networking (TON), vol. 18, no. 5, 2010, pp. 1516–1529.

 ISBN: 978-1-61208-347-6