The 1st Workshop of COST Action IC0902
Cognitive Radio and Networking for Cooperative Coexistence of Heterogeneous Wireless Networks
November 23–25, 2010
Bologna, Italy

Contribution to Working Group 4

Wireless networks identification based on packet patterns analysis

Sergio Benco (*,**), Stefano Boldrini (*), Andrea Ghittino (**), Stefano Annese (**),
and Maria-Gabriella Di Benedetto, Senior Member, IEEE (*)

(*) "Sapienza" University of Rome, School of Engineering, DIET Dept., ACTS lab.
(**) CSP "ICT Innovation", Turin, Italy

Work presented by Sergio Benco

One of the fundamental tasks of a wireless device with cognitive radio functionalities is to extract relevant parameters from other wireless networks in range, through the so called spectrum sensing. This function is a key element in a cognitive radio system as it should be firstly performed before allowing unlicensed users to access a vacant licensed channel. Among other well know techniques already used to detect communicating primary users, the most simple and effective is based on energy detection. This work is part of a project called AIR-AWARE that aims at the definition of a software module able to classify a set of different wireless technologies in the ISM band thanks to an energy detector based algorithm [1].

In [1] experimental results showed that the AIR-AWARE module can perform wireless technology classification between WiFi and Bluetooth networks (ISM band) by analyzing the energy detector output and applying linear classifiers to the extracted features. This approach allows to perform the spectrum sensing using MAC sublayer protocol features (i.e. packet exchange patterns) so that the resulting algorithm can be fast and simple. In [1] the network scenario provided off-the-shelf WLAN cards (IEEE 802.11 b/g) that were exchanging large files over a TCP link. Using a self-developed packet sniffer, the authors extracted a packet diagram of the sniffed communication between these devices. The experimentation in [1] provided the WiFi (IEEE 802.11b) real traffic mixed with simulated Bluetooth (IEEE 802.15.1) traffic in order to evaluate linear classifiers performances. The results of technology classification showed a good separability of classes generated by the features (i.e. packet duration and inter-frame space) characterizing these two ISM band technologies.

Following studies [2] investigated real traffic feature extraction in a Bluetooth network with the AIR-AWARE module implemented through an SDR architecture: the USRP2. In the Bluetooth case, thanks to the adopted TDD/TDMA multiplexing scheme, two different features have been discovered. The first feature was the packet duration related to the time slot duration (625 μs) and its multiplies (3 and 5 slot packets). The second feature consisted of packet inter-arrival measurement with which we were able to detect the slot duration and even the link type (data or voice).

In this work we used the same algorithms and SDR spectrum sensing equipment introduced in [2] to analyze IEEE Std. 802.11 a/b/g real traffic packet patterns. Using the USRP2, we would overcome the limitations determined by the use of WLAN boards as in [1] and exploit the great flexibility offered by an SDR architecture. The experimental setup consisted of two IEEE 802.11 a/b/g transceivers (Po = 10 *dBm*, Compex WLM54AGP23, Atheros chipset on Alix 3d2 mainboard, driver MadWifi) connected by an infrastructured BSS topology (AP ↔ STA). The traffic generated in the trials was obtained by connecting a PC host to the Internet through the wireless link under test. The physical channel between wireless devices, consisted of RF coaxial cables that connect the devices through a RF splitter/combiner (4 ports). The sensing device (USRP2) was attached to the splitter to sense the packet exchange (figure 1). The USRP2 hosts the XCVR2450, a dual band (2.4 *GHz* - 5 *GHz*) daughterboard. In all the captures the USRP2 is tuned on the AP channel and it captures the traffic using an I&Q sampling scheme [2]. The resulting data is then elaborated through software modules that implement the energy detector and feature extractor (i.e. SIFS extractor).

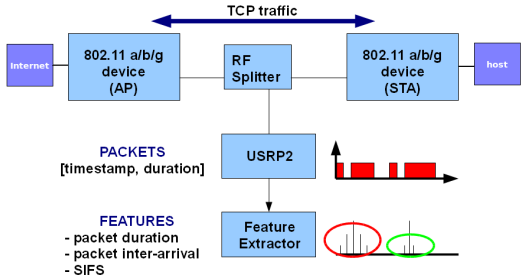

Figure 1: Experimental setup to extract the IEEE 802.11 a/b/g MAC sublayer features

In order to measure the link losses a USRP was used as signal generator. A reference tone (2.4 *GHz* and 5 *GHz*) was sent from AP and STA endpoint respectively so that a spectrum analyzer could measure the power received in the other endpoints. The link between AP and STA provides an attenuation of about 66 *dB*. The attenuation towards the sensing device from the AP was 48 *dB* and from the STA was 51 *dB*. The difference between energy received from data packets (AP) and from ACKs (STA) allows to easily verify the source of each captured packet in the short-term energy diagram (see Figure 2). The adopted energy detection algorithm consisted of C code and MATLAB scripts to provide two different diagrams: the short-term energy diagram and the packet diagram. The first one allows to visualize the short-term energy being received over the whole 25 *MHz* USRP2 bandwidth (centered at channel 1, 2.4 *GHz* and at channel 120, 5 *GHz*). The second diagram is obtained by applying a predefined threshold to the short-term energy diagram. The energy values that falls over the threshold are recorded in the packet diagram as "1" (packet) otherwise are considered "0" (noise). Considering [3], we put the energy detector threshold 10 *dB* over the noise floor to obtain the packet exchange pattern. To estimate the noise floor a MA filter of 500 points was applied to the short-term energy when no useful signal was sent in the link. In this way the noise short-term energy level resulted of -154.3 ± 0.5 *dBJ* (N = 20, 50% overlap). As in [2] the features extractor takes the packet diagram (timestamp, duration) as input and measures silence gaps between consecutive packets to find Short Inter-Frame Spaces (SIFS). The IEEE Std 802.11 provides the following constant values as SIFS duration between DATA and ACK packets:

Link type	SIFS [*μs*]
IEEE 802.11a	16
IEEE 802.11b	10
IEEE 802.11g	16*

*Table 1: SIFS values for each type of 802.11 link, * 802.11g OFDM provides 10 μs but an extra 6 μs postamble is added to the OFDM frame*

The experimental data produced the following short-term energy diagram in the presence of a 802.11g link (see figure 2).

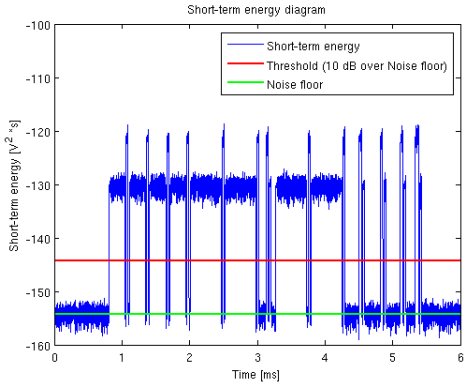

Figure 2: Short-term energy during a 802.11g (54 Mb/s) communication

The short-term energy in figure 2 illustrates the characteristic packet pattern of a 802.11g link at 54Mb/s, showing MAC frames of 1480 bytes and their ACKs spaced by a SIFS. The following table 2 resumes the detected SIFS duration and SIFS counter for each link type (see also table 1) in a sensing time of 1 *s* with a short-term energy resolution equal to 0.4 *μs* (N=20, overlap=50%).

Link type	SIFS mean duration (*μs*)	Confidence interval T-student (95%) (*μs*)	Transmitted SIFS (% detected)	Sensing time (*ms*)
802.11a (6 Mb/s)	15.641	± 0.00694	1710 (100%)	1000
802.11a (54 Mb/s)	15.626	± 0.00719	1564 (100%)	1000
802.11b (1 Mb/s)	9.943	± 0.02549	98 (100%)	1000
802.11b (11 Mb/s)	10.093	± 0.01151	773 (100%)	1000
802.11g (54 Mb/s)	15.384	± 0.01027	2528 (100%)	1000

Table 2: SIFS extraction results using three types of 802.11 links

The experimental results have shown that the USRP2 sampled data can be usefully exploited to sense a 802.11 link in order to extract the SIFS feature. This one represents a characterizing parameter of the IEEE 802.11 Standard thus allowing multi-technology classification based on energy detection [1]. The USRP2 demonstrated a good flexibility in presence of IEEE 802.11 real traffic with good resolutions and using the same features extraction algorithms already developed for Bluetooth [2].
Further studies will consider a mixed real traffic scenario where Bluetooth and 802.11 links take place. In this case the linear classification algorithms used in [1] will be further improved to cope with real time decisions.

References

[1] M.-G. Di Benedetto, S. Boldrini, C.J. Martin Martin, and J. Roldan Diaz, "Automatic network recognition by feature extraction: a case study in the ISM band", March 21, 2010 [Proceedings of the 5th International Conference on Cognitive Radio Oriented Wireless Networks and Communications, Special Session on Cognitive Radio and Networking for Cooperative Coexistence of Heterogeneous Wireless Networks, June 9-11, 2010, Cannes, France]

[2] Sergio Benco, Stefano Boldrini, Andrea Ghittino, Stefano Annese, Maria-Gabriella Di Benedetto, "Identification of packet exchange patterns based on energy detection: the Bluetooth case", July 15, 2010 [Proceedings of the 3rd International Workshop on Cognitive Radio and Advanced Spectrum Management, November 8-10, 2010, Rome, Italy]

[3] Daniel Denkovski, Mihajlo Pavloski, Vladimir Atanasovski, Liljiana Gavrilovska, "Parameter settings for 2.4 GHz ISM spectrum measurements", July 15, 2010 [Proceedings of the 3rd International Workshop on Cognitive Radio and Advanced Spectrum Management, Special Session on Spectrum Measurements and Sensing, November 8-10, 2010, Rome, Italy]