3rd International Workshop on Cognitive Radio and Advanced Spectrum
Management, November 08-10, 2010, Rome, Italy,
Best Paper Award.

Identification of packet exchange patterns based on energy detection: the Bluetooth case

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

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

Abstract — A time-domain recognition of different wireless technologies may be obtained using energy detection. In this work, an energy detector was implemented using the Universal Software Radio Peripheral SDR platform. The energy detector output allows the formation of a packet presence/absence diagram. Experimental results indicate that the observation of Bluetooth packet exchange patterns reveals technology-specific MAC layer procedures, leading to the conclusion that technology recognition can be obtained on the basis of time domain technology-specific features.

Keywords — cognitive networking; network discovery; automatic network classification; energy detection; universal software radio peripheral

I. Introduction

Automatic classification amongst different technologies in the ISM band based on MAC features was first analyzed in [1], in the framework of the AIR-AWARE Project. This project aims at creating a black box – the AIR-AWARE module – capable of classifying technologies, as well as different types of interference in play. Many wireless technologies, such as Wi-Fi (IEEE Std 802.11), Bluetooth (IEEE Std 802.15.1) and ZigBee (IEEE Std 802.15.4), operate in the ISM 2.4 *GHz* band. Every technology has its own particular MAC sublayer behaviour, as defined by the Standard specifications. Recognition of this behaviour can reveal that the corresponding technology is currently present in the air. Thanks to this approach, the recognition can be done using a generic device, such as an energy detector. This device does not have to demodulate the received signal, it only detects how much energy is present in the air in time (i.e. with a reasonable sampling frequency), to determine whether a packet is currently being sent or not. By analyzing then the time-domain diagram of presence vs. absence of packets, it can recognize features that are specific of different technologies. In this way, it can reveal those technologies that may be currently active in the area. In this work, the ISM 2.4 *GHz* band is taken into account, and the Bluetooth technology [2, 3] is analyzed in order to extract technology-specific features.

A "Universal Software Radio Peripheral" (USRP2) Software Defined Radio (SDR) platform is used for energy detection. The USRP2 output consists in received signal samples used by the energy detector to obtain the temporal pattern of the short-term energy. This trend leads to a diagram that indicates the presence vs. absence of packets, the packet durations, the "silence" gaps, and the instants at which the packets start (i.e. the packet timestamps). Based on [2] and [3], some Bluetooth features are proposed and recognized in the diagram. These features are technology-specific, i.e. they are peculiar to Bluetooth and allow to distinguish it from the other technologies operating in the same ISM band. This fact is important for the automatic recognition and technology classification, that is, the final goal of the AIR-AWARE Project.

The paper is organized as follows. Section II contains a detailed description of the USRP2 mentioned before, while in Section III it is described how it was used for energy detection. Section IV presents how the construction of the packet diagram was obtained from the energy detection, the analysis of this diagram, and the proposed features for the Bluetooth technology. In Section V the experimental results are reported, and these results are then discussed in Section VI, which also contains a guideline for proposed future directions.

II. The Universal Software Radio Peripheral SDR platform

The input data used by the energy detector were obtained through an SDR called USRP2. This hardware has recently gained growing attention by the research community given its low cost and open source vision. This kind of SDR comes in two versions: the USRP that is able to work with a bandwidth of 8 *MHz*, and the USRP2 that has an improved receiver bandwidth (up to 25 *MHz*). The USRP2, adopted in this work, consists in: a) a motherboard that hosts two 100 *MSamples/s* ADCs (14 bits) and two 400 *MSamples/s* DACs (16 bits); b) an FPGA (Xilinx Spartan 3); c) a Gigabit Ethernet controller; d) two slots: one for the receiver (RX) channel and one for the transmitter (TX) channel. These slots enable great flexibility in the USRP2 RF stage, given the simplicity in changing daughterboard (that can implement a RX, or a TX, or a transceiver) to adapt the USRP2 to a broad variety of applications (DVB, GSM/UMTS, Wi-Fi, etc.).

Manuscript submitted July 15, 2010. This work was developed under the trilateral agreement of "Sapienza" University of Rome, "Politecnico di Torino", and the CSP "ICT Innovation" (Turin, Italy). This work was supported in part by the European Commission in the framework of COST Action IC0902: Cognitive Radio and Networking for Cooperative Coexistence of Heterogeneous Wireless Networks.

For references please contact the INFOCOM Department, School of Engineering, "Sapienza" University of Rome, Via Eudossiana 18, 00184, Rome, Italy. E-mail address: dibenedetto@newyork.ing.uniroma1.it.

In the presented experimental set-up, a dual channel (TX/RX) board was used, the XCVR2450 that is able to demodulate signals in the ISM and UNII bands (2.400-2.483 *GHz* and 4.9-5.8 *GHz*). The adopted antenna was a dual band 2.400-2.483 *GHz* and 4.9-5.8 *GHz* vertical antenna, with a gain of 3 *dBi* in the lower band. The experimental set-up is completed by: two Bluetooth USB adapters (20 *dBm* Class 1 devices) for the ACL-based file transfer sensing test case; a headset and a cellular phone for the SCO-based voice transmission sensing test case. The transmitting Bluetooth devices were placed at a distance of about 1 *m* from the sensing device to get a strong-enough signal in both data and voice transmission test cases. In these scenarios the objective of this work was to analyze the simplest sensing case, i.e. the detection of Bluetooth activity generated by only two communicating Bluetooth devices.

The adopted USRP2 is able to calculate in real time the FFT over a 25 *MHz* wide bandwidth, thus allowing us to have an easy-to-deploy SDR-based spectrum analyzer. The receiver bandwidth of about 25 *MHz* is obtained using a quadrature sampling process. This configuration provides a couple of ADCs that can work with a phase difference of exactly $\pi/2$, to produce an In-phase (I) and a Quadrature (Q) sampled signal. Each USRP2 ADC can offer a Nyquist frequency of 50 *MHz*. Due to the adopted quadrature sampling scheme, the complex samples (I+jQ) can, however, perfectly reconstruct a signal whose bandwidth is 100 *MHz* (100 *MSamples/s* I&Q). The received signal, sampled with a bit depth of 14 bits, is then stored in 32 bits floating point variables (16 bits for I and 16 bits for Q) that can be further analyzed by software. Multiplying this value of 4 *Bytes/Sample* by the sampling rate gives a throughput of 3200 *Mb/s*. However, to make use of a Gigabit Ethernet interface, the received sequence has to be decimated by a minimum factor of 4 by the FPGA; this results in an 800 *Mb/s* data flow. In this way using quadrature sampling the USRP receiver bandwidth becomes 25 *MHz*.

Given that the Bluetooth technology provides FHSS (1600 *hops/s*) spread with a channel hopping code over 79 channels of 1 *MHz* each, the ideal way for detecting Bluetooth is to sense the entire 80 *MHz* bandwidth. In our set-up, the USRP2 bandwidth was set to its maximum value of 25 *MHz*. In this band a set of 22 Bluetooth channels was sensed, excluding Bluetooth channels on the edges of the selected band due to some RF impairments.

Considering only 22 channels (out of 79) we have to allow a huge loss of transmitted packets that cannot be detected. In order to maintain as simple as possible our sensing device, we avoided employing an array of USRP2 and we adopted a best effort approach using a portion of Bluetooth bandwidth. The samples captured by the USRP2 were then processed by the energy detector, consisting of MATLAB scripts described in Section III.

III. Energy Detection

The detection of a random signal immersed in AWGN noise is a well-known problem of detection theory [4]. When the received signal is unknown, a standard assumption consists in modelling it as a zero-mean WSS random Gaussian process with variance σ_s^2. Noise can be modelled as Additive White Gaussian Noise (AWGN) with variance σ_n^2. The sufficient statistic T(**r**), i.e. the expression of energy detector, is then:

$$T(\mathbf{r}) = \sum_{i=1}^{N} |r_i|^2 \qquad (1)$$

where **r** is the received sequence, r_i is the ith sample of the sequence, and N is the time window length. Energy detection can also be viewed as an estimator of the variance from a set of N consecutive samples, that results in $T'(\mathbf{r}) = T(\mathbf{r})/N$. $T(\mathbf{r})$ represents short-time energy.

The USRP2 is not conceived as a measurement tool and its output consists of pure numbers that are related to the internal ADC quantization levels. In order to translate USRP2 output sample values onto a Volt scale, the USRP2 has to be calibrated. We calculated the USRP2 input-output characteristic by sending a known input tone (a 2.402 *GHz* carrier modulated by a 150 *KHz* tone) at the antenna connector and by observing the corresponding output sampled data.

Finally, for a short-term energy value to be obtained, $T(\mathbf{r})$ in (1) was multiplied by the sampling period T_S, that is:

$$E_N(\mathbf{r}) = \sum_{i=1}^{N} |r_i|^2 \cdot T_S \qquad (2)$$

Short-term energy was computed with overlapping of 50 % of the window length, while the window length was chosen equal to N=250 samples that give us sufficient resolution in both short-time energy space and time (Figure 1). The green line on Figure 1 indicates the average noise value (noise floor). As described in Section IV, this leads to the choice of the adopted threshold (red line in Figure1).

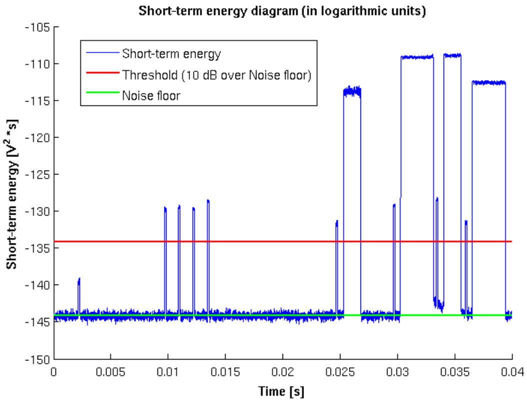

Figure 1 - Short-term energy diagram vs. time

IV. Packet Pattern Analysis and Feature Extraction

A sequence of “high” values of short-term energy indicates that for a certain period of time a useful signal was present over the air interface, i.e. a packet was sent. Conversely, a sequence of “low” values indicates silence, i.e. an inter-packet interval. “High” vs. “low” values are determined against a threshold that must be fixed, where values above vs. below threshold are high vs. low values, respectively. The threshold was fixed by adding 10 *dB* to the measured noise floor, i.e. the average detected energy in the absence of any received signal in the ISM 2.4 *GHz* band. This value was inspired by the rule adopted in the IEEE Std. 802.15.4 receiver ED feature. In our set-up, the computed noise floor was -144.2 *dBJ,* so the threshold was set at -134.2 *dBJ*. Considering that noise peaks may generate high values and the shortest packet defined in the Bluetooth Standard lasts 68 μs (ID packet), a simple packet filter was implemented by discarding all false positive packets lasting less than 50 μs. An example of the obtained packet diagram is illustrated in Figure 2.

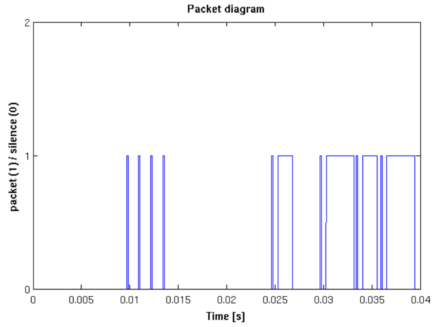

Figure 2 – Packet diagram (with reference to Figure 1)

Based on the packet diagrams, an analysis on possible MAC sub-layer Bluetooth features was carried out. Bluetooth technology uses a TDMA/TDD scheme to assure access to users. The slot duration is fixed at T_{SLOT} = 625 μs. Another important characteristic of Bluetooth is that packets may occupy 1, 3 or 5 time slots. These three packet types have minimum and maximum allowed lengths. The NULL packet and the POLL packet, that are control packets used for the Acknowledgment (ACK) and for the Polling of the intended recipients, respectively, have a fixed length of 126 bits. At a bitrate of 1 *Mb/s* as specified by [2], durations corresponding to the above packet lengths are as reported in Table I.

TABLE I. BLUETOOTH PACKET DURATIONS

	Fixed duration	**Min duration**	**Max duration**
Time slot	625 μs		
ID packet	68 μs		
NULL / POLL packet	126 μs		
1-time slot packet		126 μs	366 μs
3-time slot packet		1250 μs	1622 μs
5-time slot packet		2500 μs	2870 μs

In the voice transmission case (SCO link), packets are 1-time slot only. The piconet Master provides the Slave with periodic reserved time slots that occur every 2, 4 or 6 time slots, for so-called HV1, HV2 or HV3 packets, respectively; this corresponds to T_{SCO} values of 1.25 *ms*, 2.50 *ms* or 3.75 *ms* respectively. This configuration enables a two-way 64 *kb/s* PCM encoded symmetric voice transmission. How to take advantage of these characteristics in order to characterize Bluetooth and permit its recognition? Based on the previous analysis of the Bluetooth protocol, two features are proposed: a) packet duration; b) packet inter-arrival interval.

The first proposed feature arises from the following consideration. If sensing is performed during a data transmission or a voice call, one can expect that the link manager should segment the data by filling efficiently one of the possible packet formats it can send. If that is true, the predominant packet duration values will assume their maximum allowed value and the detected packet durations will be concentrated around the values reported in the first and last columns of Table I.

Regarding the second proposed feature, since the system is TDMA/TDD based, we expect that the packet inter-arrival time will be concentrated around T_{SLOT} (625 μs), given that the energy detector shows all the packets exchanges between the two communicating devices. In the long run, this reveals a frequent inter-arrival period corresponding to one slot duration. Multiple of 625 μs may also be present, corresponding to multi-slot packets.

V. EXPERIMENTATION

The Bluetooth technology provides two different typologies of communication based on specialized transport layer protocols. The first one is the ACL (Asynchronous Connection-Less), able to transport data in a reliable way thanks to acknowledgment packets (NULL packets) and retransmission schemes (ARQ). The second one is called SCO (Synchronous Connection-Oriented), able to convey voice streams (64 *kb/s* PCM) by keeping a constant delay (no retransmissions). These scenarios were reproduced in the following way. To obtain an ACL data link we chose to connect two hosts using two Bluetooth adapters (Class 1 devices) and to transmit one large file between them. Using 2.0 version EDR capable devices, the complete transmission of this file lasted several seconds, that is long enough to sense hundreds of packets with the USRP2 placed at about 1 *m* from each device. For the other scenario, the employed devices were: a cellular phone (Nokia N73, 2.0 EDR) and a headset (Nokia BH-100, 2.0 EDR) placed similarly to the previous set-up. In the SCO voice link case, the transmission was established by setting up a voice call.

The first analysis performed on ACL-based data transmission provided the distribution of packet duration values over a certain period of time. We chose to sense 3 *s* of file transfer, corresponding to over 500 captured ACL data packets in a 25 *MHz* bandwidth. Using packet diagrams as in Figure 2, the histogram of Figure 3 was obtained.

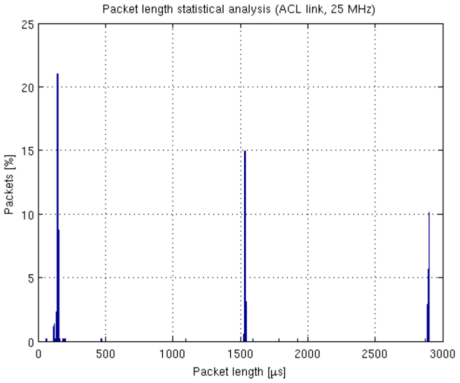

Figure 3 - Packet length statistics (ACL link, 25 *MHz*)

From the histogram one observes that most values are well concentrated around three values centred at: 144 μs, 1540 μs and 2890 μs. These values are related to the duration of the NULL/POLL packets and to the maximum durations of the 3 and 5-time slot packets (see Table I). This is reasonable since the Bluetooth transport layer does its best to encapsulate data into packets as efficiently as possible, and ACKs are needed. The presence of these three peaks indicates that the proposed feature is Bluetooth-specific. As expected, packet length distribution is clearly different in the voice case, since the only packet type in use is the 1-time slot. Results of measurements are shown in Figure 4.

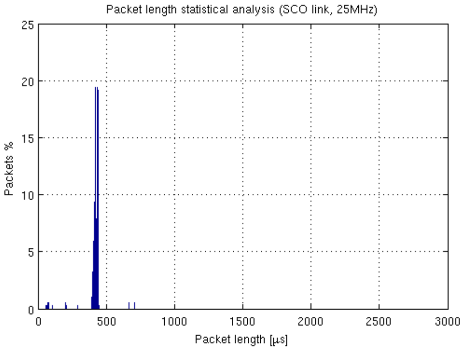

Figure 4 - Packet length statistics (SCO link, 25 *MHz*)

As expected, the packet length distribution in a SCO link is concentrated around one value (430 μs) with 58% of packets in the range 420–440 μs. The 430 μs value can be reconducted to the 1-time slot packet maximum duration of 366 μs. The good grouping of measurements confirms the proposed feature.

Based on the packet length distribution, it is possible to define a recognition time as the period from sensing start to detection of the nth Bluetooth packet. When N consecutive packets belonging to 1-slot OR 3-slot OR 5-slot classes are detected, the classifier raises a flag. The following cases were analyzed: N=10, N=25, N=50. Bandwidth was set to one the following values: 1, 5, 10, 25 *MHz* (first Bluetooth channel i.e. 1 *MHz* bandwidth, first 5 channels i.e. 5 *MHz* and so on), and was obtained by filtering the original sequence (sampled at 25 *MS/s*). Figure 5 shows the resulting recognition time graph.

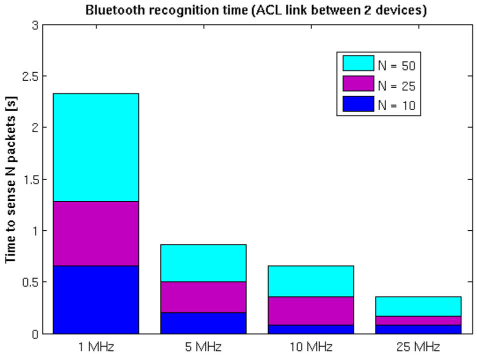

Figure 5 - Recognition time by varying N and bandwidth

As expected, the time to sense N packets grows as the considered bandwidth gets smaller. However from 25 *MHz* to 5 *MHz* this period remains small, compared to the one corresponding to 1 *MHz* bandwidth. Hence, a bandwidth of 5 *MHz* may be a good compromise between bandwidth and time to sense, when considering a FHSS technology such as Bluetooth. With only 5 *MHz* of bandwidth the packet length distribution becomes as shown in Figure 6. Note that the three peaks are preserved, even if slightly attenuated.

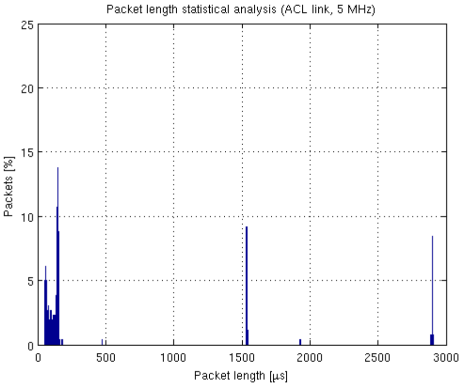

Figure 6 - Packet length statistics (ACL link, 5 *MHz*)

The increased number of occurrences of short length packet between 50 μs (the false positive packet filtering mentioned before) and the first peak can be interpreted as the effect of channels at bandwidth edge. The captured energy that falls in this portion of bandwidth determines low SNR packets close to detection threshold. In that case the fast fading can produce a multitude of threshold crossings, resulting in a huge amount of false positive short length packets. Since this happens, however, only around zero values, it does not affect our conclusions.

Packet inter-arrival time period was defined as the difference between timestamps of two consecutive detected packets. Results for an ACL link are reported in Figure 7.

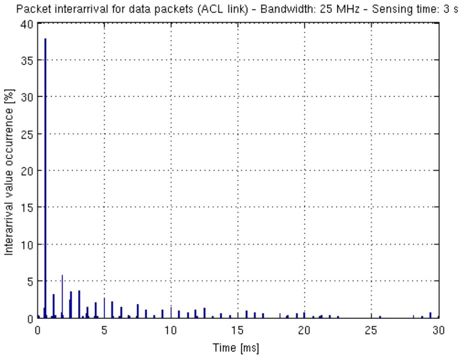

Figure 7 - Packet inter-arrival time (ACL link)

Even in this case a peak value stands out. This inter-arrival peak value is at 628 μs, closely resembling slot duration of 625 μs, [2] (there is only a difference of about 0.48% between these two values). The other peaks are extremely lower than the one at 628 μs. It is important to note that they are spaced of about one slot duration.

During voice transmission, the observed packet inter-arrival histogram is as in Figure 8. Note the regularities of the synchronous voice link that clearly arise.

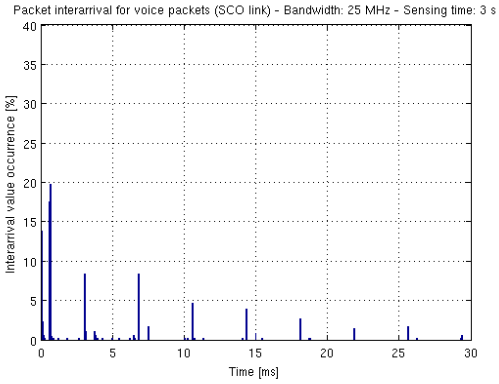

Figure 8 - Packet inter-arrival time (SCO link)

More precisely, the fundamental value of 625 μs can be recognized in the main peak at 643 μs. These two values differ of about 2.8%. Other peaks are present at 3070, 3770, 6860, 7490, 10600 μs, etc. This inter-arrival sequence reveals that the sensed communication was an HV3-based SCO link [2] with a T_{SCO} of 3750 μs (625+3125 μs). This behaviour is made clearer in Figure 9.

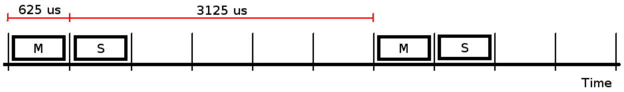

Figure 9 - Packet inter-arrivals in an HV3 packet exchange

Figure 9 shows slot occupation by Master and Slave HV3 packets. Naturally the energy detector cannot differentiate between Master and Slave packets. In this case the interesting value that can be extracted by an inter-arrival calculation is the time period between the last Slave voice packet and the following Master voice packet that results in 3125 μs. This value differs from the observed second peak in Figure 8 (3070 μs) by only 1.76%. Both Figures 7 and 8 reveal that the other proposed feature, i.e. packet inter-arrival period, is also valid, because of the presence of a well recognizable inter-arrival behaviour (i.e. the presence of peaks at specific time values) that is Bluetooth-specific.

VI. DISCUSSION OF RESULTS AND FUTURE DIRECTIONS

The AIR-AWARE Project aims at designing a black box capable to automatically detect and classify different radio technologies in the ISM band, using the output of an energy detector. This paper addresses the feature extraction problem in the Bluetooth technology case.

Using the USRP2, we computed the short-time energy diagram and the corresponding packet diagram; in this way we extracted Bluetooth packet timestamps and packet durations. Considering the Bluetooth MAC sub-layer Standard specifications, we proposed two technology-specific features: packet duration and packet inter-arrival period.

Reference Bluetooth communication scenarios were analyzed: data and voice links. Using this real traffic data we first calculated the distribution of packet lengths in both the data and voice link cases. In the data transfer case (ACL link) we found that, packet duration values were well concentrated at three values that corresponded to the three main types of packets (1, 3 or 5 time slots). This behaviour is recognizable even with smaller bandwidths. Similarly, in the voice transmission case (SCO link) the histogram shows a single peak around which 58% of packets concentrate; this peak can be related to the duration of 1- slot packets.

As for the second proposed feature, i.e. packet inter-arrival period, we found in the histogram a prevalent peak, centered at the time slot duration value. There are also secondary peaks at values multiple of time slot duration. These secondary peaks are evident especially in the voice transmission case. The proposed features seem to be valid for the purpose of this work, since they show a MAC sub-layer behaviour that is Bluetooth-specific, and that may permit its recognition in an heterogeneous networks scenario.

Further investigation should consider a testing case in the presence of other wireless technologies such as Wi-Fi and ZigBee, also against features proposed in [1] for the Wi-Fi case.

ACKNOWLEDGMENT

This work was supported in part by COST Action IC0902 "Cognitive Radio and Networking for Cooperative Coexistence of Heterogeneous Wireless Networks", funded by the European Science Foundation.

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] IEEE Std 802.15.1 – 2005, IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 15.1: Wireless medium access control (MAC) and physical layer (PHY) specifications for wireless personal area networks (WPANs), June 14, 2005

[3] Bluetooth SIG, *Specification of the Bluetooth system*, December 17, 2009

[4] S. M. Kay, *Fundamentals of Statistical Signal Processing. Vol. II: Detection Theory*, Prentice-Hall, Upper Saddle River, NJ, 1998

[5] Z. Ye, G. Memik, and J. Grosspietsch, “Energy Detection using Estimated Noise Variance for Spectrum Sensing in Cognitive Radio Networks”, *WCNC 2008 proceedings*