Bluetooth automatic network recognition – the AIR-AWARE approach

Stefano Boldrini*

Sapienza University of Rome,
School of Engineering,
DIET Department,
Via Eudossiana, 18-00184 Rome, Italy
Email: boldrini@newyork.ing.uniroma1.it
*Corresponding author

Sergio Benco, Stefano Annese and Andrea Ghittino

CSP s.c. a r.l. 'ICT-Innovation',
Via Livorno, 60-10144 Turin, Italy
Email: sergio.benco@csp.it
Email: stefano.annese@csp.it
Email: andrea.ghittino@csp.it

Maria-Gabriella Di Benedetto

Sapienza University of Rome,
School of Engineering,
DIET Department,
Via Eudossiana, 18-00184 Rome, Italy
Email: gaby@acts.ing.uniroma1.it

Abstract: Automatic network recognition and classification may prove to be an important concept in the framework of cognitive radio and networks. For practical implementations, these operations must be carried out in a simple way by using simple devices and algorithms that require low computational load. The AIR-AWARE approach proposes to use MAC sub-layer features for technology recognition purposes where a rudimentary device like an energy detector is used for technology-specific feature extraction. The aim of this work is automatic Bluetooth classification. To this purpose, two MAC features reflecting properties, related to the time-varying pattern of MAC packet exchanges, are proposed. Experimental data obtained by using the Universal Software Radio Peripheral as energy detector show that the two proposed features are capable of highlighting MAC sub-layer behaviour peculiar to Bluetooth. These features may therefore lead to successful Bluetooth recognition and the results obtained provide support to the validity of the AIR-AWARE approach.

Keywords: cognitive networking; network discovery; automatic network classification; energy detection; USRP; universal software radio peripheral; Bluetooth automatic recognition; adaptive communications systems.

Reference to this paper should be made as follows: Boldrini, S., Benco, S., Annese, S., Ghittino, A. and Di Benedetto, M-G. (2014) 'Bluetooth automatic network recognition – the AIR-AWARE approach', *Int. J. Autonomous and Adaptive Communications Systems*, Vol. 7, No. 4, pp.378–392.

Biographical notes: Stefano Boldrini obtained his Bachelor's degree in Telecommunications Engineering in 2006 from University of Trento and his Master of Science in Telecommunications Engineering in 2010 from Sapienza University of Rome. Currently, he is a PhD student in Information and Communication Engineering at Sapienza University of Rome, and his main research topics are cognitive radio and cognitive networking, with particular focus on automatic wireless network recognition and classification.

Sergio Benco received his Bachelor' degree and Master of Science in Telecommunication Engineering from Sapienza University of Rome, Italy, in 2006 and 2010, respectively. In 2010, he obtained a research grant from CSP – ICT Innovation focused on automatic wireless network recognition. He is currently working as a Consultant Engineer in the INLAB group (CSP – ICT Innovation) and as affiliated researcher in the ACTS lab of Sapienza University of Rome, DIET department. His research activities focus on spectrum sensing techniques for software defined radio.

Stefano Annese received the Telecommunication Engineering degree from the Politecnico di Torino, Italy, in 2004. Since then he works for CSP – ICT Innovation as Junior Researcher and then as a Senior Reserchер on broadband wireless technologies. He is currently the Integrated Networks Laboratory Manager in the Research and Development department. His research activities are focused on the first three layers protocols in wireless networks. He is the co-author of one patent.

Andrea Ghittino received the Telecommunication Engineering degree (summa cum laude) from the Politecnico di Torino, Italy, in 2000. He works for CSP – ICT Innovation since then and he is currently the Networks and Wireless Communications Area Manager in the Research and Development department. His research activities are focused on protocols and quality of service management in wireless networks. He is the co-author of one patent.

Maria-Gabriella Di Benedetto obtained her PhD in Telecommunications in 1987 from Sapienza University of Rome, Italy. In 1991, she joined the Faculty of Engineering of Sapienza University of Rome, where currently she is a Full Professor of Telecommunications. She has held visiting positions at the MIT, the University of California, Berkeley, and the University of Paris XI, France. In 1994, she received the Mac Kay Professorship award from the University of California, Berkeley. Her research interests include wireless communication systems and speech. From 1995 to 2000, she directed four European projects on UMTS design. Since 2000, she has been active in fostering the development of UWB communications in Europe, and recently increased activity in cognitive networks. She currently coordinates COST Action IC0902 and participates in the Network of Excellence ACROPOLIS.

In October 2009, she received the Excellence in Research award 'Sapienza Ricerca', under the auspices of President of Italy. In October 2009, she received the Excellence in Research award 'Sapienza Ricerca', under the auspices of President of Italy, Giorgio Napolitano.

Portions of the data reported here were presented at the Third International Workshop on Cognitive Radio and Advanced Spectrum Management – CogART 2010, as published in Benco et al. (2010), that received the CogART 2010 Best Paper Award.

1 Introduction

An important concept in the context of cognitive radio and cognitive networking is wireless network recognition. In fact, a cognitive radio, in order to adapt and reconfigure its parameters based on the environment in which it is set, must be able to recognise the environment, i.e., to determine if there are other active wireless networks in that precise instant in that area. This is, therefore, a problem of wireless network detection and recognition. The *AIR-AWARE Project*, 'born' at the DIET Department of Sapienza University of Rome, and first mentioned in Di Benedetto et al. (2010), addresses this problem. The main scope of this project is to reach automatic network recognition and classification in a simple way, by using simple devices and algorithms that require a low computational load.

This keyword, *simple*, was practiced in the AIR-AWARE Project using MAC sub-layer features. In fact, every wireless network presents a MAC behaviour that is defined by its own standard and, most important, that is characteristic and peculiar of that single technology. This implies that an analysis of packet exchange patterns can reveal the tecnology present over the air at a certain time, leading to network recognition. To do so, it is therefore necessary to identify MAC features for each wireless technology.

To keep the *AIR-AWARE module* as simple as possible, a 'rudimentary' device must be used for feature detection. Therefore, this project intends to use an energy detector (ED) in order to obtain, through sensing and calculation of the short-term energy, a time-domain packet diagram.

The industrial, scientific and medical (ISM) 2.4 GHz unlicensed band is the most widely used band for a lot of widespread wireless technologies. Examples are Wi-Fi (IEEE Standard 802.11, 2007), Bluetooth (IEEE Standard 802.15.1, 2005) and ZigBee (IEEE Standard 802.15.4, 2006). In this work, the Bluetooth technology was analysed, and two MAC sub-layer features were identified that can highlight and distinguish this type of network among others in the same frequency band. The universal software radio peripheral (USRP) software defined radio (SDR) was used as ED in order to obtain the necessary packet diagram. Using these simple device and recognition procedures, an identification of packet exchange patterns specific of Bluetooth was carried out.

The paper is organised as follows. Section 2 defines energy detection and explains how packet diagrams were obtained based on time-varying energy profiles. Section 3 contains a brief overview of Bluetooth technology, the analysis of its MAC behaviour,

the proposed features and how they were applied to the case under analysis. In Section 4, the USRP platform and the experimental set-up are presented. Results of experimentation are presented in Section 5, while Section 6 contains a discussion of the results obtained and future directions of this research investigation.

2 Energy detection and packet diagrams

In the general framework of spectrum sensing, the ED approach has gained great interest due to its flexibility and relative low complexity (Mariani et al., 2010). The ED is based on the computation of received energy in a predefined time window (averaged over N samples of received signal). This operation gives rise to a sequence of energy values that we indicate as energy samples. These energy samples are then compared against a threshold that depends on noise level. Note that energy detection does not require any prior knowledge on spectrum occupancy, and this provides a beneficial flexibility towards wireless technology identification.

Detection of random signals in presence of additive white Gaussian noise (AWGN) is a traditional problem that has been solved by detection theory. Under the hypothesis that the useful signal is unknown and is modelled as a zero-mean wide-sense stationary (WSS) Gaussian process with variance σ_s^2, whereas noise is AWGN with variance σ_w^2, the sufficient statistic $T(\mathbf{r})$, i.e., the expression of ED input–output characteristic, is:

$$T(\mathbf{r}) = \sum_{n=1}^{N} |r_n|^2 \tag{1}$$

In equation (1), $\mathbf{r}$ represents the received vector of complex samples r_n and N the number of samples used in each energy calculation (i.e., window length). The window length N must be selected based on a trade-off between resolution in average energy vs. time-varying energy patterns. The short-term energy function is obtained from the product of equation (1) by the ED sampling period T_s, where NT_s = window duration, i.e.

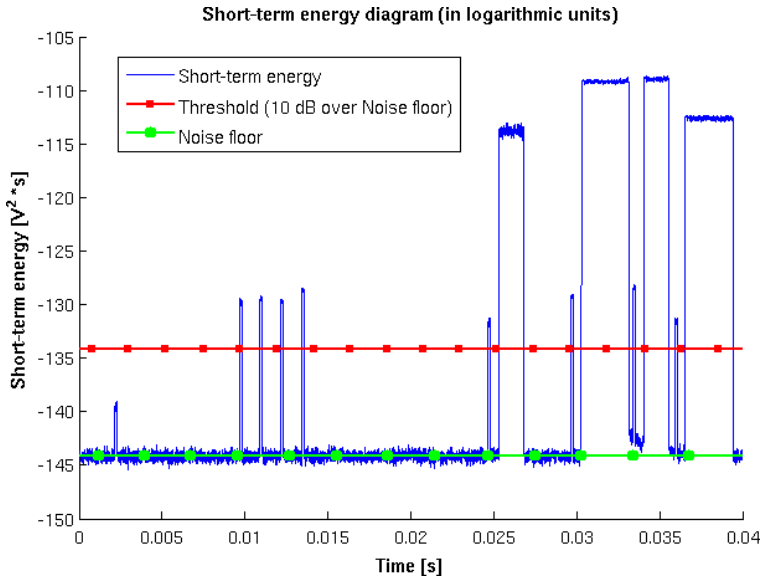
$$E_N(\mathbf{r}) = \sum_{n=1}^{N} |r_n|^2 T_\mathrm{s} \tag{2}$$

Since the sampling frequency was 25 MHz (as further described in Section 4), the sampling period was $T_\mathrm{s} = 40$ ns. Based on Bluetooth packet duration, as explained later in Section 3, a reasonable window duration was 10 μsec, and therefore, in order to obtain this value, a rectangular window N of 250 samples was used. This number of samples offers a good trade-off between E_N values and average values. In other words, N value is not 'too high', otherwise E_N would be computed considering too many samples, not permitting to follow in an accurate way the changes in the short-term energy; it is also not 'too low', otherwise the mean in the short-term energy computation would refer to a very low number of samples. Furthermore, consecutive E_N windows

were overlapped by 50% in order to improve time resolution to 5 μsec instead of 10 μsec.

An example of short-term energy diagram is depicted in Figure 1. The E_N diagram of Figure 1 was obtained by capturing the data transfered between two nearby (about 1 m) Bluetooth devices. The signals were captured by USRP2 that was positioned about half way between the two Bluetooth devices. The USRP2 bandwidth was set at 20 MHz and centred at 2.412 GHz.

Figure 1 A short-term energy diagram obtained after capture of Bluetooth data signals, short-term energy values are expressed in logarithmic units (see online version for colours)



In Figure 1, the line over the noise level represents the estimation of the average noise power called noise floor (green line on figure). This value was calculated using a moving average filter applied on recorded E_N data when no signal was being transmitted.

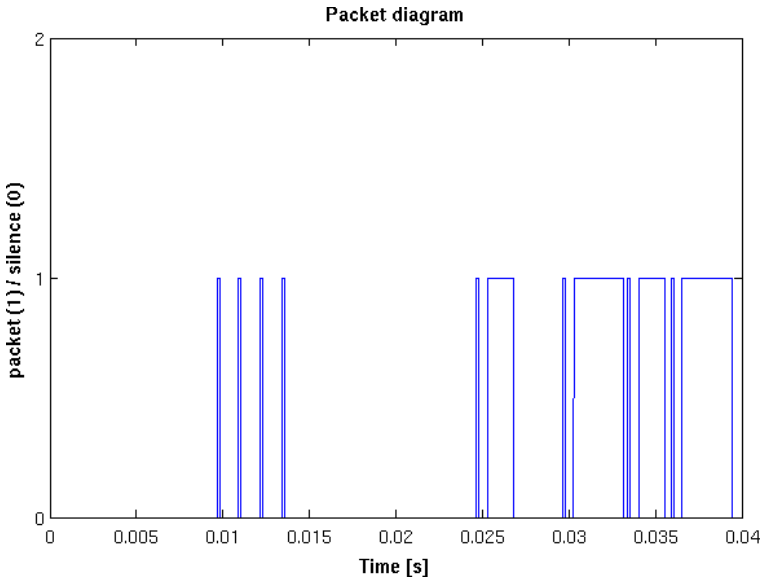
Short-term energy diagrams are used to generate packet diagrams. A packet diagram shows the presence (logical value '1') or absence (logical value '0') of a packet, sent over the air by a device, containing either control data or user data. Note that distinguishing data vs. control packets is not relevant for the scope of this work given that the analysis focuses on MAC packet exchange patterns, regardless of their content.

To obtain the packet diagram, an appropriate threshold value must be determined. All energy values below the threshold are considered as 'low', i.e., the sensed energy is too low to be considered as energy transmitted by a device in the surrounding area. Similarly, energy values above the threshold are considered as 'high', i.e., the

sensed energy is high enough to be considered as energy transmitted by a device in the surrounding area, and as such must be part of a sent packet. The noise floor was obtained by averaging the detected energy in absence of any received signal in the ISM 2.4 GHz band. The threshold value was determined by adding 10 dB to the noise floor. This choice was inspired by the energy detection adopted in ZigBee (IEEE Standard 802.15.4, 2006). The validity of this choice was also confirmed by Denkovski et al. (2010), that indicates that a 10 dB margin is a recommended choice for parameter settings of a USRP2 device operating in the 2.4 GHz ISM band. In particular, the measured noise floor was −144.2 dBJ, and therefore the threshold value was set at −134.2 dBJ.

Based on the above threshold, the packet diagram was obtained by deciding, as previously indicated, whether short-term energy values were 'low' or 'high'. A sequence of 'high' values 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. Figure 2 shows an example of packet diagram that is directly derived from Figure 1.

Figure 2 Example of packet diagram, corresponding to the energy profile of Figure 1 (see online version for colours)



For each detected packet a vector (timestamp, duration) is stored, where 'timestamp' is the packet arrival time instant and 'duration' is the packet duration. This vector is used to extract time-domain technology-specific features, as discussed in Section 3.

Note that during both data and voice transfers, the described sensing algorithm was tested by capturing enough data to statistically analyse the features and their potential separability capabilities in a multi-standard feature classifier.

3 Bluetooth MAC features

Bluetooth technology is described in IEEE Standard 802.15.1 (2005) and is used for wireless personal area networks (WPANs). For the purpose of this work, it is important to notice its particular and peculiar MAC sub-layer behaviour. A Bluetooth network is organised into clusters of devices called piconets. Within a piconet, communication can be established only between a master device and a slave device (there are up to seven slave devices in a piconet). Bluetooth uses a time division duplex/time division multiple access (TDD/TDMA) packet communication scheme. Communication is slotted, and time slot duration is fixed at T_{SLOT} of 625 μsec. Bluetooth packets can occupy one-, three- or five-time slots. In each case, packet duration may vary between a minimum and a maximum value that is reported in Table 1 (for a 1 Mb sec^{-1} bitrate). Packets containing control data occupy only one-time slot, and have in general a fixed duration, as indicated in Table 1 (for a 1 Mb sec^{-1} bitrate). These minimum, maximum and fixed durations, as defined by IEEE Standard 802.15.1 (2005), are important for the scope of this work. Note on Table 1 the 68 μsec fixed duration of the ID packet, that is the shortest Bluetooth packet.

A common packet exchange pattern consists of DATA – ACK packets, that are exchanged between the master and a slave. DATA packets have no predetermined durations: packets are filled with all the data that must be sent (and the necessary overhead), always respecting the duration rules defined by the standard. For the acknowledgement, a control packet called NULL packet is used. This packet has a fixed size of 126 bits, i.e., a fixed duration of 126 μsec, at a 1 Mb sec^{-1} bitrate. For completeness, there is another control packet, the POLL packet, used for polling, that has the same fixed duration of the NULL packet.

Table 1 Bluetooth packet durations

	Fixed duration (μsec)	*Minimum duration (μsec)*	*Maximam duration (μsec)*
Time slot	625		
ID packet	68		
NULL/POLL packet	126		
One-time slot packet		126	366
Three-time slot packet		1,250	1,622
Five-time slot packet		2,500	2,870

When the Bluetooth communication is used for voice transmission, i.e., a so, called synchronous connection-oriented (SCO) link is established, DATA packets are one-time slot only. Furthermore, the master provides the slave reserved time slots following the scheme reported in Table 2. These reserved slots permit to obtain a two-way 64 kb sec^{-1} pulse code modulation (PCM) encoded symmetric voice communication.

This MAC sub-layer behaviour, that is characteristic of Bluetooth, can be exploited in order to reach its recognition in a simple way, starting from the obtained packet diagram. As seen before, the shortest packet defined in Bluetooth technology is the ID packet, whose duration is fixed at 68 μsec. This means that all detected packets whose duration is less than 68 μsec can be discarded, because they cannnot be Bluetooth

packets. For this reason, a simple packet filter was implemented using MATLAB, and all packets with a duration lower than 50 μsec were discarded, considering them as 'false positive packets'. The choice of 50 μsec instead of 68 μsec for the packet filter threshold added some tolerance to the packet identification procedure.

Table 2 Bluetooth SCO link details

Packet type	*Reserved time slot every … (time slot)*	T_{SCO} *value (msec)*
HV1	2	1.25
HV2	4	2.50
HV3	6	3.75

The packet diagram was then ready to be used for Bluetooth recognition. According to the MAC sub-layer feature approach of the AIR-AWARE Project, two MAC features were proposed:

1 packet duration

2 packet inter-arrival interval

The reason for selecting the first feature was based on the consideration that one can expect a link manager to segment data by efficiently filling the available packet formats. If that is true, it can be expected that predominant packet duration values will assume their maximum allowed values, and the detected packet durations will be concentrated around the values reported in the first and last columns of Table 1.

The selection of the second feature derives from the structure of the TDD/TDMA system, i.e., a slotted time-axis. For this reason, it can be expected that packet inter-arrival interval values be concentrated around T_{SLOT} (625 μsec) or its multiples, when single-slot vs. multi-slot packets are detected.

These two proposed features can be calculated from the packet diagram in a very simple way. Despite this simplicity, they can highlight and reveal a MAC sub-layer behaviour that is characteristic of Bluetooth, leading to successful recognition.

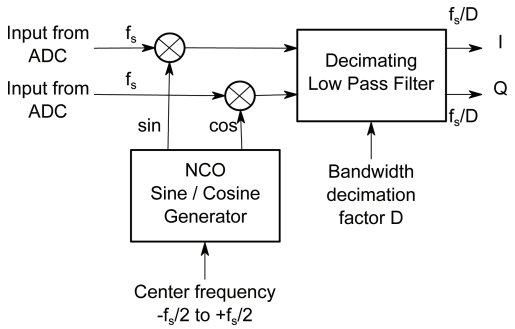
4 Experimental set-up

The USRP is a widely used SDR platform developed by Ettus Research LLC (a subsidiary of National Instruments Corp.). This device has gained great interest from the research community thanks to its excellent integration with the open source GNU Radio SDR framework. In this work, the USRP version 2 (or simply USRP2) and GNU Radio version 3.2 have been used.

The USRP2 is an hardware platform for SDR applications that hosts a mainboard with a field programmable gate array (FPGA) (Xilinx Spartan 3-2000, a RISC 32 bit microprocessor), two 100 MS sec^{-1} 14 bit analog to digital converters (ADCs) (LTC2284), two 400 MS sec^{-1} 16 bit digital to analog converters (DACs) (AD9777), a secure digital (SD) card reader to load FPGA firmware and drivers and a Gigabit Ethernet controller to connect the host computer. The radio frequency (RF) and intermediate frequency (IF) stages of the USRP2 can be changed by switch the

daughterboard being used. There is a wide range of USRP2 daughterboards to cover almost every radio application. The GNU Radio environment allows to control all the fundamental parameters of the USRP2, such as: digital down converter (DDC) frequency, FPGA decimation, programmable gain amplifier (PGA) gain, local oscillator (LO) offset, sampling multiplexer (MUX) scheme, halfband filters and the precision of the data sent and received from the computer. One fundamental aspect of a SDR hardware is represented by the sampling scheme and speed. The USRP2 adopts a quadrature sampling scheme that is depicted in Figure 3 realised by a DDC in the FPGA, that consists of a numerically-controlled oscillator (NCO), a four-stage decimating cascaded integrator-comb (CIC) filter and two halfband filters (HBFs). The quadrature sampling scheme doubles the bandwidth of the transceiver thus enabling a receiver bandwidth of 100 MHz from the 100 MS sec^{-1} ADC sampling frequency (f_s) and it produces two streams: the in-phase and the quadrature baseband signals (I and Q).

Figure 3 The DDC scheme of the USRP2



The Gigabit Ethernet interface guarantees a full-duplex data rate of 125 MB sec^{-1} that allows an equivalent complex RF bandwidth of about 31.25 MHz. Due to this choice the data rate processed by the FPGA has to be decimated by a minimum factor of 4 or greater thus determining a maximum RF receiver bandwidth of about 25 MHz. If the USRP2 decimation value is an odd integer, the resulting DDC filtering consists of CIC filters with no HBFs, introducing aliasing out of $f_s/2$. Using an even rate but not multiple of 4 results in one halfband filter (a low rate HBF with 31 taps that decimates by a fixed rate of 2). Finally, the adoption of a decimation factor multiple of 4 determines the use of CIC filters (decimating in the range 1–128) and of both available halfband filters, the low rate one and the higher rate seven taps one. The use of these two filters results in a fixed decimation rate of 4 (the minimum aliasing-free decimation rate) and the use of one of the available CIC permits to reach higher decimation. Given the 100 MSamples sec^{-1} 14 bit ADC converters and the decimation rate of 4, the used sampling frequency was 25 MHz, that corresponds to a sampling period of 40 ns (as previously mentioned in Section 2).

In this work, the down-converted stream consisted of 16 bit complex samples (16 bits for real and 16 bits for the imaginary part) at the maximum allowed RF bandwidth (25 MHz). The resulting data flow (of ADC sample values) was then recorded in a binary file using the GNU Radio libraries. The actual short-term energy calculation was performed using MATLAB scripts with real traffic data inputs. The equipment used in this work was thus consisting of:

- a USRP2 device
- an XCVR2450 (2.4 GHz – 5 GHz) daughterboard
- a vertical antenna (dual band 2.4 GHz –5 GHz, 3 dBi gain)
- a host PC with a GNU/Linux OS (Ubuntu) and GNU Radio 3.2
- two Bluetooth enhanced data rate (EDR) devices (data rate: 2 Mb sec^{-1}).

In the experimental set-up, the USRP2 was placed less than 1 m away from the two communicating Bluetooth devices. The Bluetooth technology is characterised (see also Section 3) by narrow band channels of 1 MHz used in a frequency hopping spread spectrum (FHSS) over 80 MHz of total bandwidth. The frequency hops are triggered by a pseudo-random noise (PN) code, that determines a uniform distribution of the transmitted packets over the entire bandwidth. As previously mentioned, the received signal passes through a cascade of HBF and CIC filters and this results in a signal spectrum flat enough just for a bandwidth of about 20 MHz. This means that the USRP2 can capture only 20 Bluetooth channels out of 80, losing about $3/4$ of total transmitted packets.

The sensing algorithm was tested using signals produced by commercial Bluetooth devices with embedded antennas. Due to this non-ideal RF condition, the experimental set-up was characterised by very low ranges (and consequently high signal-to-noise ratios, SNRs) between Bluetooth devices and the sensing device. In this way, the detection of all exchanged packets (in the considered band) was guaranteed. Consequently, the focus can be reduced exclusively on Bluetooth packet presence/absence patterns analysis, that is the scope of this work.

The parameters used in this work to set-up the USRP2 were the following. The PGA gain was 40 dB, the USRP2 centre frequency was 2.412 GHz and the bandwidth was 20 MHz wide (decimation value of 4). The capture was driven by GNU radio companion file sink module to record the received complex samples in a vector.

5 Experimental results

The considered scenario was characterised by two communicating Bluetooth EDR devices using either the (asynchronous connection-less) ACL link or the SCO link. The Bluetooth communicating devices were located at a distance of about 1 m from each other. During Bluetooth communications, the USRP2 was placed close to the communicating devices (at a distance < 1 m) to guarantee a strong received signal. In this way, it was possible to collect and analyse a large set of different real scenario captures.

The packet duration feature measured over an ACL link (established by a file transfer between two Bluetooth EDR devices) can be observed in Figure 4. Given the proximity of transmitter and receiver, and the absence of interferers within range, the SNR was reasonably high, and it was therefore straightforward to capture all the exchanged packets (almost 500) in the observing time (about 3 sec). It was possible to verify the existence of three packet duration classes, corresponding to the one-,

three- and five- slot packet durations provided by a Bluetooth ACL link. Note on Figure 4 that each class average value results as a full-payload slot value. To be rigorous, a data packet length should be modelled as a random variable. Hovewer, the observed real data show very frequent occurrences of slot maximum values (high peaks in the histogram).

Figure 4 Histogram for the packet duration feature measured over an ACL link (see online version for colours)

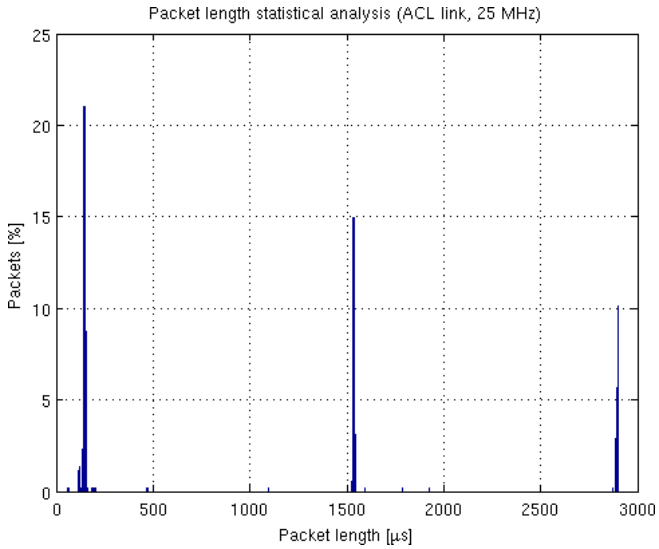
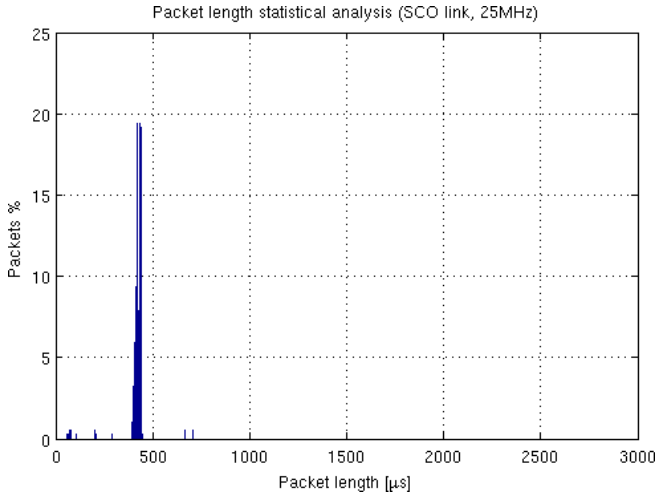


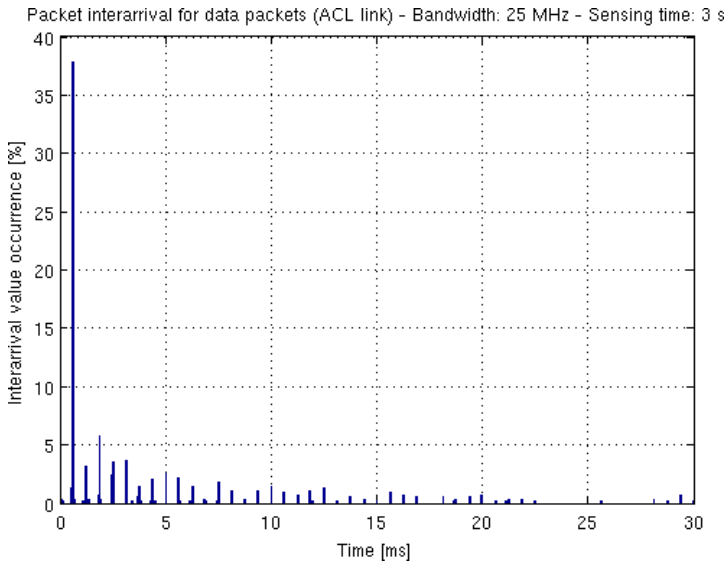
Figure 5 Histogram for the packet duration feature measured over an SCO link (see online version for colours)



Similar to the ACL case, in the voice (SCO) link of Figure 5 there is one main peak, corresponding to a specific packet duration class. The measured average packet duration in a voice link is about 430 μsec. In this case, the packet duration distribution shows increased spread, although well concentrated at a specific value, and may thus prove to be still useful for technology classification purposes.

As for the second feature, packet inter-arrival interval for the ACL case follows a trend tending to randomness due to several uncontrollable elements: frequency hopping over a larger bandwidth than the considered one, packet losses and related retransmissions, intrinsic randomness of the data transfer. However, even in the ACL link, the slotted structure of the packet exchange may arise, showing a periodicity that follows multiples of a timeslot duration (625 μsec). Figure 6 shows the histogram for the packet inter-arrival feature measured over an ACL link, where the periodicity corresponds to almost exactly T_{SLOT} (628 μsec).

Figure 6 Histogram for the packet inter-arrival feature measured over an ACL link (see online version for colours)



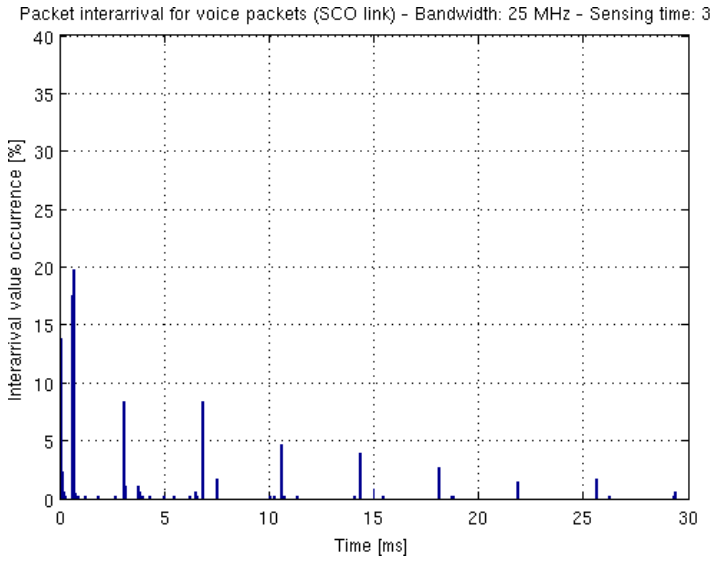
For SCO links, the packet inter-arrival interval feature is even more interesting because of the synchronous nature of the link and the presence of reserved periodic slots for voice packets (as explained in Section 3). The resulting histogram is plotted in Figure 7.

From real data, the packet duration and the packet inter-arrival interval features appear to offer an excellent separability property. This happens both in the data link (ACL) and in the voice link (SCO). Using these features should guarantee good separability of Bluetooth MAC features from other wireless technology MAC features, based on a simple ED capable of providing packet diagrams from which the proposed features can be directly and easily extracted with low-complexity algorithms.

Note that in condition of interference, that might occur frequently considering that the analysed band is the 2.4 GHz ISM band, the packet diagram might be influenced and changed by the overlapping of other technologies packets. But this happens not only by using this MAC features approach, i.e., it is not a limitation introduced by

the proposed approach. In fact this happens even if the adopted approach is spectrum sensing (Mate et al., 2011; Yucel and Arslan, 2009; Zeng et al., 2008). In that case, interference caused by other technologies signals might significantly affect the received signal (Shi and de Francisco, 2011), leading to more difficulties in the process of technology recognition and automatic classification. In other words, difficulties caused by interference must be considered for both approaches: the MAC features approach as well as the spectrum sensing one.

Figure 7 Histogram for the packet inter-arrival interval feature measured over a SCO link (see online version for colours)



6 Discussion of results and future directions

The scope of AIR-AWARE is to create a black-box, the AIR-AWARE module, able to detect, recognise, distinguish and classify different wireless technologies operating in the ISM 2.4 GHz band. We proposed to carry out network recognition and automatic classification in a simple way, i.e., using MAC sub-layer technology-specific features based on energy detection.

This work analysed the Bluetooth technology. Two MAC features were proposed: packet duration and packet inter-arrival interval. The USRP2 device was used as ED, in order to compute a short-term energy diagram, from which a MAC packet diagram was obtained. Based on packet diagram patterns, the two proposed features were computed. Data links (ACL link) as well as voice links (SCO link) were taken into consideration.

An analysis of the obtained results for the first feature (packet duration) was carried out for both ACL and SCO links. In ACL links, packet duration values were well concentrated around three main peaks corresponding to the three main packet types (one-, three- or five- time slot packets). In SCO links, a similar behaviour was observed: the histogram presented a single main peak, around which about 58% of packets were concentrated; this peak can be related to the duration of one-time slot packets.

The second feature (packet inter-arrival interval) histogram presented a prevalent peak, centred at the time slot duration value for both ACL and SCO links. Secondary peaks at multiples of time slot duration were also present; these secondary peaks were particularly evident in the voice transmission case (SCO link).

In conclusion, the two proposed features seem to be valid for the purpose of Bluetooth network recognition, since they are capable of highlighting a MAC sub-layer behaviour that is specific and peculiar to Bluetooth.

Noise uncertainty should be considered in future investigations, where the use of blind combined ED (BCED) methods should be tested. As described in Zeng et al. (2010), the BCED algorithm may overcome noise estimation problems (blind method), while maintaining the flexibility of the ED.

Further investigation should focus on testing cases where the presence of interference provoked by other wireless technologies such as Wi-Fi and ZigBee are taken into consideration. Possible Wi-Fi recognition features as proposed in Di Benedetto et al. (2010) should also be considered and tested in particular for Bluetooth vs. Wi-Fi recognition. Recognition of underlay networks like UWB (Di Benedetto and Giancola, 2004; Di Benedetto and Vojcic, 2003) based on MAC features (De Nardis and Di Benedetto, 2003; Di Benedetto et al, 2005; Di Benedetto et al., 2007) will form the object of future work, with the aim of integrating the AIR-AWARE module with recognition capabilities beyond the ISM band.

Acknowledgements

This work was partly supported by COST Action IC0902 'Cognitive Radio and Networking for Cooperative Coexistence of Heterogeneous Wireless Networks', funded by the European Science Foundation, and partly by European Commission Network of Excellence ACROPOLIS 'Advanced coexistence technologies for radio optimisation in licensed and unlicensed spectrum'.

References

Benco, S., Boldrini, S., Ghittino, A., Annese, S. and Di Benedetto, M-G. (2010) 'Identification of packet exchange patterns based on energy detection: The bluetooth case', *Applied Sciences in Biomedical and Communication Technologies (ISABEL), 2010 Third International Symposium on* pp.1–5, DOI: 10.1109/ISABEL.2010.5702776∼CogART2010BestPaperAward.

De Nardis, L. and Di Benedetto, M-G. (2003) 'Medium access control design for UWB communication systems: review and trends', *Journal of Communications and Networks*, Vol. 5, pp.386–393.

Denkovski, D., Pavloski, M., Atanasovski, V. and Gavrilovska, L. (2010) 'Parameter settings for 2.4 GHz ism spectrum measurements', *Applied Sciences in Biomedical and Communication Technologies (ISABEL), 2010 3rd International Symposium on* pp.1–5, DOI: 10.1109/ISABEL. 2010.5702772.

Di Benedetto, M-G., Boldrini, S., Martin, C.J.M. and Diaz, J.R. (2010) 'Automatic network recognition by feature extraction: a case study in the ism band', *Cognitive Radio Oriented Wireless Networks Communications (CROWNCOM), 2010 Proceedings of the Fifth International Conference on*, pp.1–5.

Di Benedetto, M-G., De Nardis, L., Giancola, G. and Domenicali, D. (2007) 'The Aloha access $(UWB)^2$ protocol revisited for IEEE 802.15.4a', *ST Journal*, Vol. 4, pp.131–141.

Di Benedetto, M-G., De Nardis, L., Junk, M. and Giancola, G. (2005) '$(UWB)^2$: uncoordinated, wireless, baseborn, medium access control for UWB communication networks', *Journal on Special Topics in Mobile Networks and Applications*, Vol. 10, pp.663–674, DOI: 10.1007/s11036-005-3361-z.

Di Benedetto, M-G. and Giancola, G. (2004) *Understanding Ultra Wide Band Radio Fundamentals*. Prentice Hall Communications Engineering and Emerging Technologies Series. Prentice-Hall PTR, p.528, ISBN: 0-13-148003-0.

Di Benedetto, M-G. and Vojcic, B. (2003) 'Ultra-wideband (UWB) wireless communications: a tutorial', *Journal of Communications and Networks*, Vol. 5, pp.290–302.

IEEE standard for information technology-telecommunications and information exchange between systems-local and metropolitan area networks-specific requirements – part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications, *IEEE Std 802.11-2007 (Revision of IEEE Std 802.11-1999)*, (December 2007), pp.C1–1184, DOI: 10.1109/IEEESTD. 2007.373646.

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). *IEEE Std 802.15.1-2005 (Revision of IEEE Std 802.15.1-2002)* (2005).

IEEE standard for information technology-telecommunications and information exchange between systems-local and metropolitan area networks-specific requirements part 15.4: Wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (WPANS), *IEEE Std 802.15.4-2006 (Revision of IEEE Std. 802.15.4-2003)* (2006).

Mariani, A., Giorgetti, A. and Chiani, M. (2010) 'Energy detector design for cognitive radio applications', *Waveform Diversity and Design Conference (WDD), 2010 International*, pp.000053–000057, DOI: 10.1109/WDD.2010.5592343.

Mate, A., Lee, K-H. and Lu, I-T. (2011) 'Spectrum sensing based on time covariance matrix using GNU radio and USRP for cognitive radio', *Systems, Applications and Technology Conference (LISAT), 2011 IEEE Long Island*, pp.1–6, DOI: 10.1109/LISAT.2011.5784217.

Shi, X. and de Francisco, R. (2011) 'Adaptive spectrum sensing for cognitive radios: an experimental approach', *Wireless Communications and Networking Conference (WCNC), 2011 IEEE*, pp.1408–1413, DOI: 10.1109/WCNC.2011.5779366.

Yucek, T. and Arslan, H. (2009) 'A survey of spectrum sensing algorithms for cognitive radio applications', *Communications Surveys Tutorials, IEEE*, Vol. 11, No. 1, pp.116–130, ISSN: 1553-877X, DOI: 10.1109/SURV.2009.090109.

Zeng, Y., Liang, Y-C. and Zhang, R. (2008) 'Blindly combined energy detection for spectrum sensing in cognitive radio', *IEEE Signal Processing Letters*, Vol. 15, pp.649–652.

Zeng, Y., Liang, Y-C., Hoang, A.T. and Zhang, R. (2010) 'A review on spectrum sensing for cognitive radio: challenges and solutions', *EURASIP Journal on Advances in Signal Processing*, Vol. 2010, Article ID 381465, 15 pages, doi: 10.1155/2010/381465.