Identifying Sources of Interference in RSSI Traces of a Single IEEE 802.15.4 Channel

Sven Zacharias, Thomas Newe, Sinead O'Keeffe, Elfed Lewis
Department of Electronic and Computer Engineering
University of Limerick
Limerick, Ireland
{Sven.Zacharias, Thomas.Newe, Sinead.OKeeffe, Elfed.Lewis}@ul.ie

***Abstract*—This paper presents the possibility of using RSSI readings to monitor a single IEEE 802.15.4 channel in the 2.4 GHz ISM band. An overview of the main sources of interference - namely Wireless Local Area Networks (WLANs), Bluetooth devices and microwave ovens - is given. Finally, an algorithm to classify one second of RSSI readings into one of these device classes is presented. The algorithm classifies 762 of 790 samples (96.46 %) correctly, having its worst precision with 97.41 % for the Bluetooth device class and its worst recall/sensitivity with 84.21 % for the microwave oven class. This algorithm gives an overview of interfering wireless devices without the need of changing the channel and thus allowing a continuous message reception.**

Keywords-IEEE 802.15.4; Radio Signal Strength Indicator (RSSI); 2.4 GHz ISM band; interference; coexistence; Wireless Sensor Network (WSN)

I. INTRODUCTION

Wireless Sensor Networks (WSNs) are small, embedded, in-expensive, low-power networks that are going to be widely deployed in the near future. They can be used in many applications in homes, offices and all sorts of urban environments. Today's most suitable wireless transfer technologies for WSNs are based on the IEEE 802.15.4 standard [1], since it provides a simple, low-power stack for the Physical and Medium Access Control (MAC) Layer. The IEEE 802.15.4 (2003) standard can physically operate in the three free Industrial, Scientific and Medical (ISM) frequency bands offering 27 channels: one at 868 MHz, ten in the 915 MHz band and 16 in the 2.4 GHz band. The only frequency band available worldwide is 2.4 GHz, which is the most used ISM band, utilized by many technologies and therefore the band is crowded [2]. Since wireless sensor nodes are power-constrained, energy saving by means of avoiding retransmissions or unnecessary on-times of the radio is an important task. Finding sources of interference allows avoiding collisions and therefore retransmissions can be reduced. This helps to have more reliable and energy efficient WSNs.

In the following section, a discussion of related work is given. Then the properties of Radio Signal Strength Indicator (RSSI) values are presented. Afterwards, the common sources of interference in WSNs are described, namely: Wireless Local Area Networks (WLANs), Bluetooth devices (BT) and microwave ovens (MWOs). For each device class, a short summary is given and then meaningful features for the detection are highlighted. Based on that, an algorithm is developed to identify the just mentioned device classes by RSSI readings of a single WSN channel. Subsequently, an evaluation and discussion of the algorithm is given. The paper ends with conclusions showing the potential fields of application for this work.

II. RELATED WORK

The coexistence of IEEE 802.15.4 with other IEEE standards has already been partly considered in the standard itself (Annex E). To avoid packet loss, the ZigBee standard recommends spectrum scanning with the help of RSSI readings for network channel management [3]. The scheme is only based on noise floor measurements on different channels and changes to a less used channel. There is no classification of sources of interference.

Boano et al. are using RSSI readings to improve the channel simulation [4] and to recreate interference [5]. Especially [5] gives a good overview of the possibilities of RSSI readings and the sources of interference (as in this work, WLAN, BT and MWO are researched). Emulations of the different sources of interference are presented, but no classification is used.

Rayanchu, Patro and Banerjee use an off-the-shelf WLAN interface card to measure the spectrum in the 2.4 GHz band and to identify devices [6]. Since IEEE 802.11 wireless network interface cards have different technical properties compared to IEEE 802.15.4 radios, their identification method differs from the one presented here. Their presented solution performs full spectrum scans and their classification of devices is based on a decision tree created with the help of machine learning.

Chowdhury and Akyildiz propose spectrum sensing with the help of a sensor node and an offline interference source classification approach. They scan the full spectrum and identify WLANs and MWOs by matching the observed spectral pattern with a stored reference shape. Their approach scans the full spectrum, thus the sensor node cannot receive while performing the scan. Their number of researched devices for WLANs and MWOs is rather small. They further suggest a scheme to choose the channel, packet scheduling times and sleep-awake cycles [7].

The algorithm presented here only needs the readings of a single channel and thus, the measuring sensor node is connected to the network all the time. Also, the number of researched devices is high for an approach using sensor nodes.

III. RSSI READINGS

The IEEE 802.15.4 standard defines that an "Energy Detection" (ED) value must be measured for the "network layer as part of a channel selection algorithm. It is an estimate of the received signal power within the bandwidth of an IEEE 802.15.4 channel. No attempt is made to identify or decode signals on the channel. The ED time shall be equal to 8 symbol periods." This ED value is also widely known as the RSSI value. Since no identifying or decoding takes place, the RSSI can be used either to detect noise on a channel, or to indicate the quality of an incoming packet when measured while receiving.

Many applications and protocols for WSNs use the RSSI values to detect traffic or interference on the channel and to estimate transmission distances. Thus, RSSI is an enormously useful metric when used as a link quality estimator [8] or as part of a link quality estimator [9], and therefore, for routing. In addition, localization [10], channel management [7] and other systems rely heavily on RSSI readings.

In this work, RSSI readings from the Tmote Sky [11] sensor node are used. The data sheet of the built-in CC2420 radio chip [12] states a dynamic range from -100 to 0 dBm with an accuracy of ±6 dB and a linearity of ±3 dB. The RSSI is read over an 8 symbol period, which is 128 µs long in average. The quality of these RSSI readings was researched in [13] and the effects of the antenna pattern are shown in [14].

IV. SOURCES OF INTERFERENCE

The main sources of interference for WSNs in the 2.4 GHz band in urban environments and their effects on WSN deployments are reviewed in literature [15, 16]. In the literature and from the authors' experience, the main sources of interference are given as:

A. *Wireless Local Area Networks*

The term WLAN or Wi-Fi is commonly used to describe a collection of different technologies based on the IEEE 802.11 standard and its amendments [17]. In the following, the 802.11b, g and n standard [18] are of interest, since these operate in the 2.4 GHz band. Dependent on national restrictions there are up to a maximum of 14 (11 in North America) channels available. The IEEE 802.11b and g channels are 22 MHz wide and their channel center frequencies are only 5 MHz away from each other, thus they overlap each other. Channel 14 is an exception being 12 MHz away from its predecessor (see Figure 5). IEEE 802.11n works basically on the same channels but supports 40 MHz wide bundled channels and multiple-input multiple-output (MIMO), which is based on multiple antennas. Although spread spectrum modulated signals are used, a single 2 MHz wide WSN channel within the 22 MHz wide WLAN channel shows a clear peak in the RSSI readings of the Tmote Sky sensor node on WLAN sending activity. Hence the transmitting time and temporal length can be roughly detected. Since this work concentrates on single channel measurements the spectral properties cannot be used for identification.

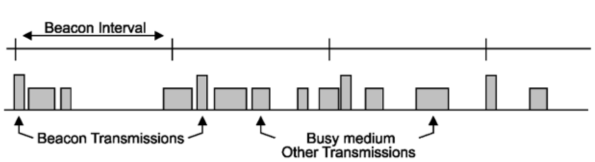

Figure 1. Beacon transmissions on a busy network [17].

The data rates of the previous mentioned standards are 1, 2, 11, 54 and 150 Mbit/s. Although there are different data rates, the standard specifies beacons, send by the Access Point (AP), which are different to normal traffic.

1) Beacon Frames: Every AP periodically sends a beacon frame to announce its network and to maintain connection to all clients in range. To allow all network interface cards to see the network, this beacon is send with the lowest data rate (1 or 2 Mbit/s) for highest compatibility. The smallest theoretical beacon has a body of around 30 bytes and 28 bytes of management frame. It has a measureable transfer time of roughly 0.5 or 0.25 ms. Most beacon frames are over 100 bytes in length and therefore, they are clearly traceable. The default behavior is to send ten beacons per second. The authors observed that all scanned WLANs (six in an office and 16 in a domestic environment) used a beaconing frequency of 10 Hz. This frequency is assumed for the remainder of this work. The beacons are good indicators of the presence of a WLAN on the channel and can be clearly seen in the RSSI readings as shown in Figure 6 (a). When the channel is heavily used the beacons become harder to identify as the standard does not provide reserved timeslot for beacons (see Figure 1 and Figure 6 (b)). This means that the AP has to access the communication medium by using the CSMA/CA algorithm as all participants do, resulting in the possibility of delayed beacons. As the AP is further away from the measuring sensor node, the beacons get increasingly lost in the data traffic.

2) Non-Beacon Frames: All other traffic in the WLAN can be, depending on the network possibilities, transferred at a higher speed and is therefore harder to identify as WLAN traffic. Some small packets can even be too fast to be measured using 11 kHz RSSI readings. This traffic has no dominant pattern, due to the various amounts of different protocols and applications.

B. *Bluetooth Devices*

BT [19] (IEEE 802.15.1) is designed to be a low-cost, medium-power, robust, short-range communication platform for Wireless Personal Area Networks (WPANs). It also operates in the 2.4 GHz band using 79 different 1 MHz wide channels (see Figure 5). It supports different sending classes with different sending powers. There are different versions of BT available, supporting different data rates up to 3

Mbit/s for Version 2.0 + Enhanced Data Rate (EDR) onwards. Since BT uses Adaptive Frequency Hopping (AFH) it is the least interfering technology presented here. BT changes the channel 1,600 times a second. This results in a time of 0.625 ms between the hops, called a slot, which is still traceable with a sampling rate of 11 kHz. A BT signal is characterized by its short spikes, due to the channel hops. The transmissions are organized by a Time Division Multiple Access (TDMA) scheme. BT supports two types of physical links: Synchronous Connection-Oriented (SCO) links and Asynchronous Connection-Less (ACL) links. SCO links are normally used for voice transfer and are strictly based on single slot packets. ACL links are packet based and can use one, three or five slots (see Figure 2). The traffic load and therefore the channel usage depend very much on the used application profile and wireless environment. The traffic can be low (regular traffic as for a wireless input device) to high (burst traffic as for file transfer (FTP)) or evenly spread transfer of audio as used for wireless headsets (see Figure 6 (d) and Figure 6 (e)). The actual transfer spikes of BT in the RSSI readings are the most reliable method for identification. The discovery and connection phase has not been investigated in this work.

C. *Microwave Ovens*

MWOs are a widely used household appliance working in the 2.4 GHz band with high power to warm food by dielectric heating. The common center frequency of MWOs is around 2.45 GHz with a spread width of at least 5 MHz and the average output power is around 800 W (the precise specification of a model can normally be found at the type plate at the back of the MWO). Through shielding most of the output power is kept in the cooking chamber of the device, but some waves are emitted to the environment. Measurements of the spectrum and the timing patterns of different MWOs can be found in [20].

MWOs consist of a single magnetron tube that emits high frequency waves. Since the magnetron works always with full power the user-set power level is achieved by controlling on and off periods. This results in off times between some heating phases (see Figure 3). These heating phases (shown in Figure 6 (c)) consist of wave emitting periods that are typically based on the frequency of the power supply (50 Hz in Europe or 60 Hz in North America). The periodical channel blocking differs very much to the signals used for digital, wireless communication and can be easily identified. For the rest of this paper, it is assumed that the MWO is

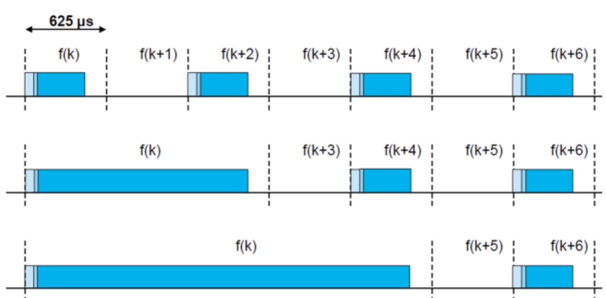

Figure 2. Single- and multi-slot packets used by Bluetooth [19].

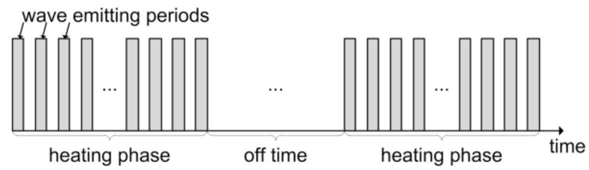

Figure 3. Simplified illustration of the wave emissions of a microwave oven operating with user setting "medium power".

measured in a heating phase, because in the off times no waves are emitted.

D. *Other Wireless Sensors Networks*

Other WSNs operating on the same channel also have the potential to jam communications. The identification of other WSNs by RSSI readings would be possible (see Figure 6 (f)), but is not needed, since a single channel RSSI scanner can still receive messages. Even if the other WSN uses a different MAC protocol the message will still be received, but it might not be interpretable. Since the protocols used for WSNs are very variable, a time based classification based on RSSI readings would be quite complex to cover all possible patterns.

E. *Other Devices*

There are more devices active in the 2.4 GHz band, for example: Digital Enhanced Cordless Telecommunications (DECT) phones, wireless input devices not based on BT, or wireless video cameras, but they are beyond the scope of this paper.

V. IDENTIFYING DEVICES IN THE TIME DOMAIN

A. *Experimental Setup*

To develop a decision algorithm to identify the class of an interfering device, a data base of RSSI readings was created. All samples have been collected with a single Tmote Sky sensor node running ContikiOS 2.5 [21]. For measuring the Frossi Scanner [3, 22] has been used, recording RSSI readings with an average sampling rate of 11,321 Hz. With the help of MATLAB [23] 790 samples, each one second long, have been cut. These samples consist of scans of different channels in two WLAN environments, two MWOs, four BT devices, and another Tmote Sky sensor node sending short messages. All samples have been checked manually by viewing a plot to make sure that the sample is feasible and classifiable. This data base forms the foundation for the later stated detection rates. Its detailed composition is shown in Table 1.

B. *Data Analysis*

The main part of the data analysis was done offline in MATLAB. Additionally WEKA [24] was used, but the suggested trees and rules have not been used with the present algorithm, since they leak domain knowledge and are purely based on statistics. Some thresholds have been incorporated in the algorithm presented here.

```
// 1 second of RSSI readings
IF max(Readings) < 15
THEN return(NOISE);
IF ( (max(FFT.power).index between(48Hz,52Hz))
     OR
     (max(FFT.power).index between(98Hz,102Hz))
     AND (Usage between(30%,70%) )
THEN return(MWO);
IF ( (max(UsageLength) < 625 µs) OR
     (RaisingFlanks/count(RaisingFlanks)
      >= 0.286)) AND ((Usage <= 10%) AND
     (FFT.Power[10HZ]/sum(FFT.Power) <= 0.035) )
THEN return(BT);
IF ( (Usage between(1%,30%)) AND
     (max(ClearanceLengths) <= 100ms) )
THEN return(WLAN);
return(UNKNOWN);
```

Listing 1. Pseudocode of classification algorithm.

TABLE I. COMPOSITION OF THE USED DATA BASE OF RSSI READINGS.

Label	Type of device	Samples
WLAN	22 WLANs (partly overlapping, office and domestic environment)	640
MWO	2 different models of microwave ovens (manufacturers: Matsu, Bush)	19
BT	Laptop (Dell Wireless 370 Bluetooth Mini-card), Mobile Phone (Motorola Razr v3i), Headset (Samsung WEP-470), Wireless Mouse (Apple Magic Mouse)	121
WSN	Tmote Sky	10

C. Algorithm

The algorithm takes one second of RSSI readings as input and classifies it as WLAN, MWO, BT or unknown device. There is also the chance of an early return in the case where there is no signal present. In the following the algorithm is briefly described, an overview of the algorithm is given in Listing 1. The steps are worked through sequentially. If a classification matches, the result is returned and the algorithm ends.

1) Input: 1 s (~11,300 samples) of RSSI readings with values in the range of [0…100]. The dBm values can be computed as the RSSI values minus 100.

2) Noise: If no reading has a value greater or equal to 15, there is no classifiable signal present. In the following all values under 15 mean a free channel, while higher values are considered as usage of the channel. The default Clear Channel Assessment (CCA) threshold of the radio is 23. But the threshold of 15 allows the algorithm to work with weaker signals and is still far enough away from the noise floor.

3) MWO: The algorithm states that the signal is generated by a MWO if the following conditions are fulfilled: The maximum period power of the signal, found by a discrete Fourier transform, is between 48 and 52 or between 98 and 102 (based on European 50 Hz mean frequency). And the channel is used between 30 % and 70 % of the time.

4) BT: The algorithm states that the signal is generated by a BT device if the following conditions are fulfilled: The channel is never used longer than a single BT slot or the distance between rising flanks is mainly the [1…5] times of a slot time. And the channel is used less than 10 % of the time and the 10 Hz period power found by a discrete Fourier transform divided by the maximum power of all periods is less or equal to 0.035.

5) WLAN: The algorithm states that the signal is generated by a WLAN if the following conditions are fulfilled: The usage of the channel is between 1 % and 30 % and the maximum time of a clear channel is less than 100 ms (100 ms are the standard delay between to beacons).

6) UNKNOWN: If none of the previous conditions are fulfilled, the source of the signal is unknown.

D. Discussion of the Classification Results

The algorithm described performs well on the previously mentioned data base with 28 wrongly classified data sets out of 790 in total (3.54 %). The detailed confusion matrix is given in Table 2. Samples of WSNs were used to check the behavior of the classifier for unknown signals and to proof the exclusiveness of the classes, thus the precision value for WSNs is not meaningful. There is no class for WSNs since there is no need to detect them with RSSI readings (as explained in Section IV-D).

Since the signal is either binarized (channel used or clear) or normalized, as the FFT results, the distance to the interference source should be unimportant. The algorithm can be easily implemented on a personal computer. With an input of just one second of RSSI readings it is performed fast and can adapt quickly to changes in the wireless neighborhood. Unfortunately, at the moment, it is too complex to run on a sensor node. The memory of the node cannot handle the data.

The presence of multiple sources of interference is a challenge for the detection algorithm and the present algorithm only returns a single class. First trials showed that depending on the sources of interference different cases occur.

Since MWOs do not monitor or react to traffic on the medium, they overlay the signals of WLANs and BT devices and the algorithm will most likely not identify other sources of interference, due to the dominance of the MWO. The interference range of a MWO is quite limited, thus further away from the MWO the MWO signal will decline quickly and the other signals will become dominant and will be detected by the algorithm.

WLAN and BT are much more complex in there coexistence, since both of them react to the usage of the

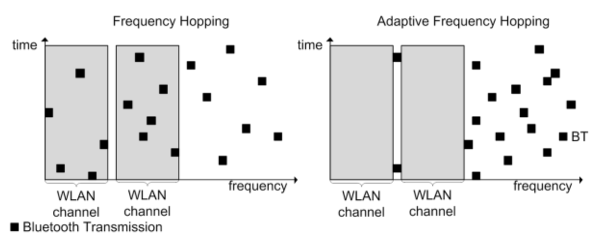

Figure 4. Simplified functional principle of Adaptive Frequency Hopping (AFH) compared to Frequency Hopping (FH).

medium. WLAN is quite widely spread, thus it can stand narrow band interference like BT. BT uses AFH and changes to un- or less used channels when many collisions occur on a channel. The principle of AFH is shown in Figure 4. Additionally, adaptive power control and Channel Quality Driven Data Rate (CQDDR) are used by BT to reduce interference. In the real world there are still some BT transmissions on the channels used by WLAN. But since there are many factors (distance to the sources of interference, data traffic and protocols used, and the just name interference avoiding technologies of BT) the interplay of BT and WLAN is not fully covered by the presented algorithm. In case of signals of BT and WLAN it will mostly classify the signal as WLAN, since WLAN is the dominant source of interference. According to [15], WLANs lead to much more lost packets than BT devices and so the algorithm returns the most relevant source of interference. Nevertheless, the detection of multiple sources of interference is a possible future enhancement for the presented algorithm.

New classes of devices as mentioned in Section IV-E, like wireless DECT phones and other proprietary devices operating in the 2.4 GHz band could be added. The algorithm needs further testing with more devices. Also the quality of the RSSI readings across different nodes of the same and different models could be compared. According to [13] the RSSI readings across different sensor nodes are comparable and hence the usage of other nodes as measurement devices is feasible.

As a short sanity check for the results, the authors went to another location and measured with a different Tmote Sky on channel 12 that was used by WLANs. All samples measured were classified correctly as WLANs. More consolidation of the results will be done in near future.

VI. Conclusions

This paper reviews the possibility of using RSSI readings to monitor the wireless channel. The main sources of wireless interference are introduced, and finally an algorithm to classify one second of RSSI readings into a device class is presented.

The results presented here can be used in many applications. The features of the signals highlighted here, can help to better simulate interference for improved channel models. The algorithm could run on the base station of a WSN enabling the base station to perform a funded centralized channel management. Channel sensing is also an important step for Cognitive Radios [25]. With the knowledge of the channel number the identification results could be improved further. An additional full spectrum scan could considerably improve the classification, but the ability to received messages without interruption on the channel would be lost. To the best of the authors' knowledge this is the first algorithm using a time series of RSSI readings of only a single channel to classify the wireless neighbors of a wireless sensor node.

Acknowledgment

The authors wish to thank the following for their financial support: The Embark Initiative and Intel, who fund this research through the Irish Research Council for Science, Engineering and Technology (IRCSET) postgraduate Research Scholarship Scheme.

References

[1] *IEEE Standard 802.15.4™-2003*, IEEE Computer Society Std., 2003.

[2] G. Zhou, J. A. Stankovic, and S. H. Son, "Crowded spectrum in Wireless Sensor Networks," in *Proceedings of 3rd Workshop on Embedded Networked Sensors (EmNets)*, 2006.

[3] ZigBee Specification, ZigBee Alliance Std., January 2008.

[4] C. Boano, K. Römer, F. Österlind, and T. Voigt, "Demo abstract: Realistic simulation of radio interference in COOJA," in *Proceedings of the European Conference on Wireless Sensor Networks (EWSN)*, 2011.

[5] C. Boano, T. Voigt, C. Noda, K. Römer, and M. Zuniga, "Jamlab: Augmenting sensornet testbeds with realistic and controlled interference generation," in *10th International Conference on Information Processing in Sensor Networks (IPSN), 2011*, April 2011, pp. 175 –186.

[6] S. Rayanchu, A. Patro, and S. Banerjee, "Airshark: Detecting non-WiFi RF devices using commodity WiFi hardware," in *Internet Measurement Conference (IMC)*, Berlin, Germany, November 2011.

[7] K. Chowdhury and I. Akyildiz, "Interferer classification, channel selection and transmission adaptation for Wireless Sensor Networks," in *IEEE International Conference on Communications, 2009. ICC '09*, June 2009, pp. 1 –5.

[8] K. Srinivasan and P. Levis, "RSSI is under appreciated," in *In Proceedings of the Third Workshop on Embedded Networked Sensors (EmNets)*, 2006.

[9] N. Baccour, A. Koubaa, L. Mottola, M. Zuniga, C. Boano, and M. Alves, "Radio link quality estimation in Wireless Sensor Networks: A survey," *ACM Transaction on Sensor Networks*, 2011.

[10] A. Boukerche, H. A. B. F. Oliveira, E. F. Nakamura, and A. A. F. Loureiro, "Localization systems for Wireless Sensor Networks," in *Algorithms and Protocols for Wireless Sensor Networks*, A. Boukerche, Ed. John Wiley & Sons, Inc., Hoboken, New Jersey, 2009, pp. 307 – 340.

[11] Moteiv Corporation, *Tmote Sky - Ultra low power IEEE 802.15.4 compliant wireless sensor module*, 2006.

[12] *CC2420 2.4 GHz IEEE 802.15.4 / ZigBee-ready RF Transceiver*, Chipcon, June 2004, datasheet.

[13] Y. Chen and A. Terzis, "On the mechanisms and effects of calibrating RSSI measurements for 802.15.4 radios," in *7th European Conference on Wireless Sensor Networks (EWSN)*, 2010, pp. 256–271.

[14] M. Holland, R. Aures, and W. Heinzelman, "Experimental investigation of radio performance in Wireless Sensor Networks," in *2nd IEEE Workshop on Wireless Mesh Networks (WiMesh)*, IEEE, 2006, pp. 140–150.

[15] A. Sikora and V. Groza, "Coexistence of IEEE 802.15.4 with other systems in the 2.4 GHz-ISM-band," in *Proceedings of the IEEE Instrumentation and Measurement Technology Conference (IMTC)*, vol. 3, May 2005, pp. 1786 –1791.

[16] Jennic - Technology for a changing world, "Co-existence of IEEE 802.15.4 at 2.4 GHz," Application Note Revision 1.0, February 2008.

[17] *IEEE Standard 802.11™-2007*, IEEE Computer Society Std., 2007.

[18] *IEEE Standard 802.11n™-2009*, IEEE Computer Society Std., 2009.

[19] *Bluetooth Specification Version 2.1 + EDR*, Bluetooth SIG, Inc. Std., July 2007.

[20] P. Gawthrop, F. Sanders, K. Nebbia, and J. Sell, "Radio spectrum measurements of individual microwave ovens volume 1," NTIA Report 94-303-1, Tech. Rep., March 1994.

[21] A. Dunkels, B. Gronvall, and T. Voigt, "Contiki - a lightweight and flexible operating system for tiny networked sensors," in *29th Annual IEEE International Conference on Local Computer Networks*, IEEE, 2004, pp. 455–462.

[22] C. A. Boano, J. Eriksson, F. Österlind, and A. Dunkels "Contiki projects: Frossi scanner," http://contikiprojects.svn.sourceforge.net/viewvc/contikiprojects/sics.se/frossi-scanner/, [April 2012].

[23] MATLAB, *version 7.9.0.529 (R2009b)*. Natick, Massachusetts: The MathWorks Inc., 2009.

[24] M. Hall, E. Frank, G. Holmes, B. Pfahringer, P. Reutemann, and I. H. Witten, "The weka data mining software: An update," *SIGKDD Explorations*, vol. 11, no. 1, 2009.

[25] T. Yucek and H. Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications," *IEEE Communications Surveys & Tutorials*, vol. 11, no. 1, pp. 116–130, 2009.

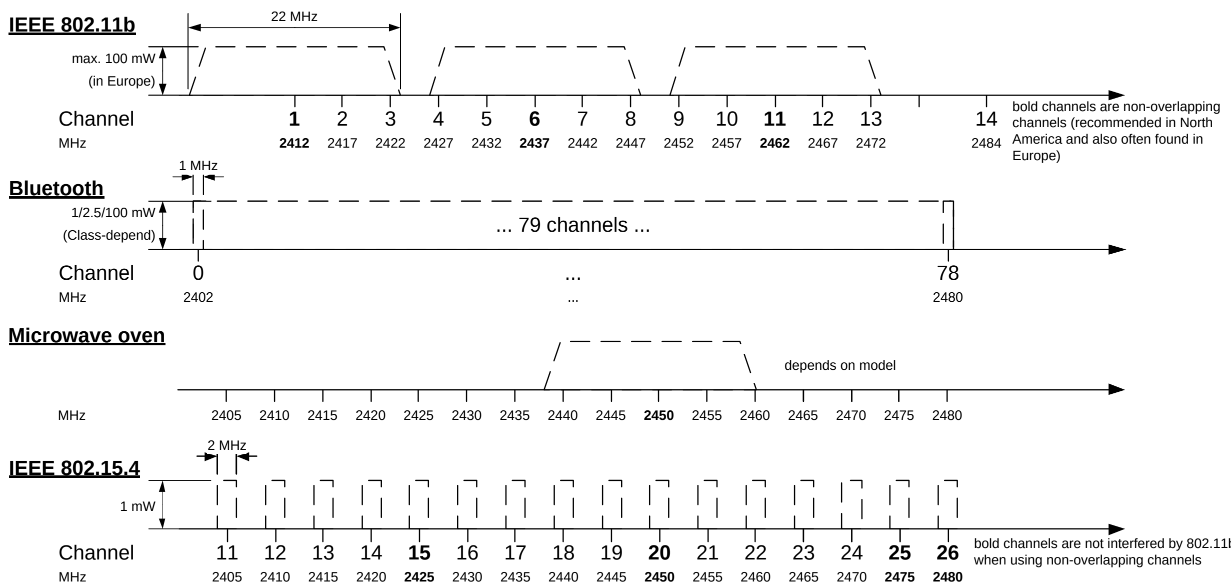

Figure 5. Overview of the usage of the 2.4 GHz spectrum by different standards/devices. Do not scale spectral mask or output power from this drawing.

TABLE II. CONFUSION MATRIX OF IDENTIFIED CLASSES.

		Predicted class					
		WLAN	***BT***	***MWO***	***UNKNOWN***	***Precision***	***Recall/Sensitivity***
Actual class	***WLAN***	623	3	0	14	99.05 %	97.34 %
	BT	3	113	0	5	97.41 %	93.39 %
	MWO	3	0	16	0	100.00 %	84.21 %
	WSN	0	0	0	10	34.45 %	100.00 %

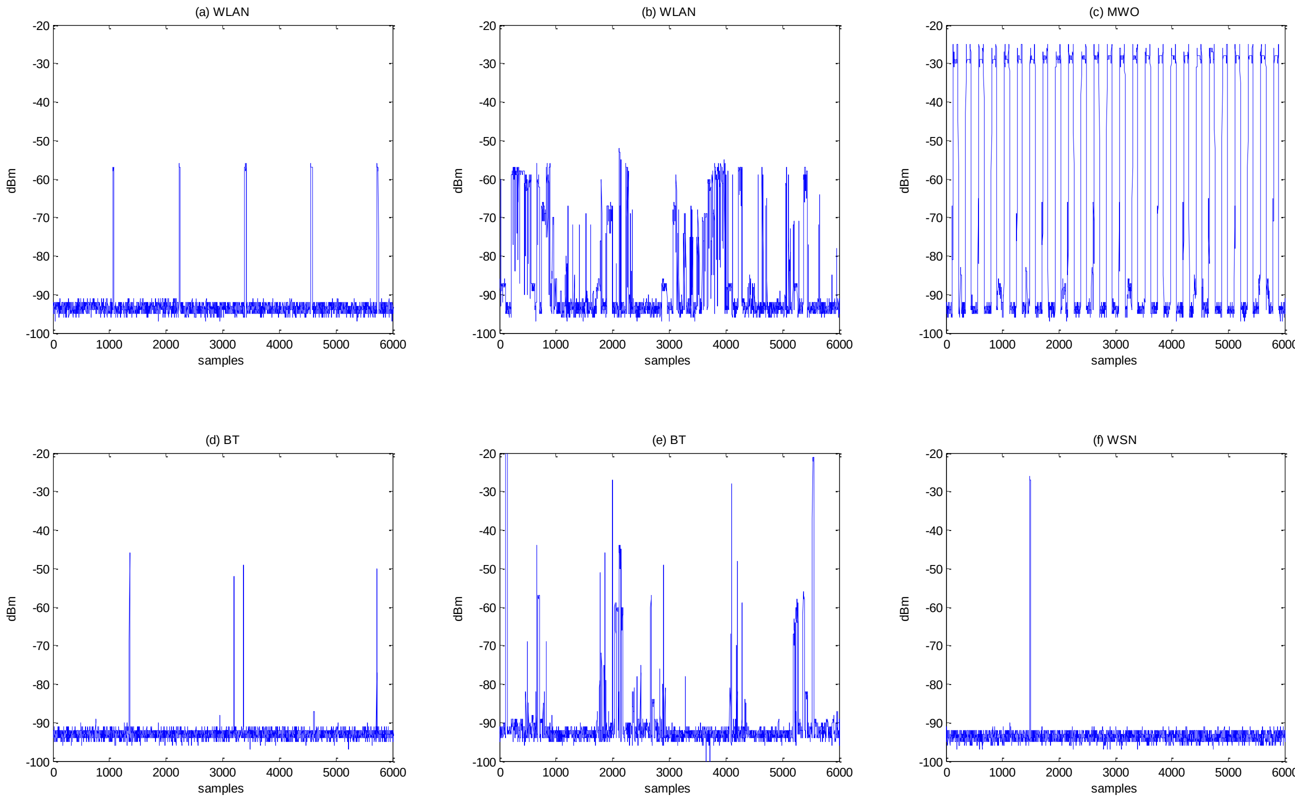

Figure 6. Overview of typical RSSI time series (0.5 s) of different devices. (a) WLAN beacons. (b) WLAN data traffic. (c) MWO heating phase. (d) Low traffic BT using only single-slot packets. (e) High traffic BT using multi-slot packets. (f) WSN sending a 22-byte-long message.