Interference Measurements in IEEE 802.11 Communication Links Due to Different Types of Interference Sources

Jan-Willem van Bloem*, Roel Schiphorst*, Taco Kluwer† and Cornelis H. Slump*
*University of Twente, Enschede, The Netherlands, P.O. Box 217, 7500 AE
Telephone: +31 53 489 2780, Email: {j.w.h.vanbloem, r.schiphorst, c.h.slump}@ewi.utwente.nl
†Radiocommunications Agency Netherlands , PO Box 450, 9700 AL, Groningen, The Netherlands
Telephone: +31 50 587 7207, Email: taco.kluwer@agentschaptelecom.nl

Abstract—**The number of wireless devices (smartphones, laptops, sensors) that use the 2.4 GHz ISM band is rapidly increasing. The most common communication system in this band is Wi-Fi (IEEE 802.11 b/g/n). For that reason coexistence between Wi-Fi and other systems becomes more and more important. In this paper we have investigated the influence on Wi-Fi communication for different interference sources, *i.e.*, wireless Audio/Video (A/V) transmitter, microwave and Bluetooth. A measurement tool has been developed to measure this influence both at the Physical (PHY) Layer and at the link layer to assess the overall Quality of Service (QoS). At link layer the tool allows to analyze the received packets types and sub fields; a sophisticated approach to analyze interference mechanisms compared to traditional packet sniffers that focus on throughput and packet error rate only. In addition, this tool allows to identify the type of interference source based on the occurring interference mechanisms at these lower two layers of the OSI protocol stack The experimental results show severe impact of A/V transmitters which causes significant overall QoS degradation of WiFi communication in contrast to microwave and Bluetooth interference.**

I. Introduction

The number of wireless devices (smartphones, laptops, sensors) that use the 2.4 GHz ISM band is rapidly increasing. In many urban areas not only many Wi-Fi networks can be found, also other systems like Bluetooth, Zigbee, microwaves and wireless A/V transmission systems use this band. On the other hand there is only a limited amount of spectrum available. So it is very likely that interference between systems in this band will occur. Due to the rapid increase of wireless devices, interference is expected to become even more important. In this paper we address this issue by providing measurement results where the performance degradation of a Wi-Fi communication link due to a nearby interferer source has been measured. For this purpose we have implemented a setup to analyze both the spectrum (physical layer) and data packets (link layer) in the Wi-Fi communication link. Spectrum sensing can be used to measure the utilization of a Wi-Fi channel. Moreover each wireless communication standard has it own RF signature, so spectrum sensing can also be used to identify the interferer source. Although the utilization of a band can be analyzed it is still unknown what the quality is of the wireless link. To measure the quality and to know if there is congestion, data packets have to be analyzed. Here the retry rate and the number of control frames, used to manage the wireless link, can be used for this purpose.

The paper is organized as follows. First, section II provides theoretical background and related work on monitoring Quality of Service (QoS). In section III the measurements setup for experiments in a controlled environment is described. In section IV the monitoring results are presented for both PHY and link layer. Section V concludes the paper.

II. Monitoring Quality of Service

The OSI protocol stack of the IEEE 802 standard consists of five layers where the lower two layers involve the wireless aspects of communication, *i.e.* the PHY layer and the link layer. In addition, at the link layer all WLAN technologies are based on Carrier Sense Multiple Access (CSMA) which in turn can rely on different implementations of the Clear Channel Assessment (CCA) detection algorithm, *e.g.* energy detection; as a drawback CCA algorithms are typically not designed to handle interference [1]. This makes WLAN link layer in particularly vulnerable to interference, *i.e.* packet

978-1-61284-683-5/12/$31.00 ©2012 IEEE

transmissions can be deferred if the interference signal adequately resembles a WLAN signal.

To assess the overall Wi-Fi QoS the monitoring must take place at the lower two layers as these layers are responsible for the wireless link. At the PHY layer this entails a threshold-based approach to determine spectrum occupation. On the other hand, at the link layer the total frame rate and retry frame rate have been found to be good parameters for quantifying the level of utilization and network degradation [2]. In addition, monitoring of the proportions of the different link frame types can be used to monitor the overhead in a Wi-Fi network, *i.e.*, data, management and control (*e.g.* Clear To Send (CTS), Request To Send (RTS), and Acknowledgment (AKC)) frames.

Not much related literature has been found. First, in [2] a description of the overall Wi-Fi QoS monitoring is provided by Mass Consultants commissioned by the British regulator Ofcom; here monitoring takes place at various locations in the UK and live readings are obtained. Furthermore, in [3] the total QoS is assessed using a cognitive radio approach. However, the impact of interference and coexistence issues are not addressed in [2], [3].

A. Performance Evaluation of 802.11 with Interference

Much of the literature on coexistence issues is focused on Bluetooth interference only addressing interference mitigation in the 2.4 GHz ISM band. Here the basic mechanism to mitigate interference between Bluetooth and other technologies is Frequency Hopping Spread Spectrum (FHSS). This entails Bluetooth transmissions to take place in an ad hoc fashion using frequency hopping (1600 hops/sec) between 79 channels of 1 MHz each. However, coexistence between Bluetooth and IEEE 802.11 remains an important issue and because of its relevance the IEEE 802.15 Working Group has set up the Task Group 2 (TG2), which is engaged in the development of coexistence mechanisms [4]; here two classes of coexistence mechanisms have been defined: on one hand collaborative techniques *e.g.* Time Division Multiple Access (TDMA) and on the other hand non-collaborative techniques such as Adaptive Frequency Hopping (AFH). Note that owing to the AFH mode the degradation of Wi-Fi systems due to Bluetooth is expected to be lower when compared to systems lacking such mechanisms (*e.g.* A/V transmitters). A performance analysis of Bluetooth interference without AHF on IEEE 802.11b/g/n systems is provided in [5]–[7] showing packet losses up till 25%. An extensive evaluation of Bluetooth interference in AFH mode on IEEE 802.11g systems is described in [8] with packet losses up till 7%.

Another important source of interference are microwave ovens introducing wide-band interference throughout the 2.4 GHz ISM band. Experimental studies are conducted on microwave oven interference in [7], [9]–[11] describing mainly the spectrum characteristics and detection/mitigation issues on the PHY layer. In [6] a theoretical framework is provided including a microwave simulation model; here it is shown for instance that a 600W microwave produces worse case up till 10% packet loss for a Wi-Fi traffic load of $\lambda_w = 0.1$.

There is another important interference source classified as jamming [1], [12], *e.g.* A/V transmitters. Experimental studies show the severe impact of jamming as a 3 dB increment in signal interference power causes an increase in Packet Error Rate (PER) from 0% to 30%. The jamming interference is a continuous narrow band signal which deteriorates the Orthogonal Frequency-Division Multiplexing (OFDM)-modulated symbols of the IEEE 802.11g/n systems but on the other hand also leaves many carrier frequencies intact. However, the performance of the connection degrades very quickly and the different coding rates and modulation methods show no effect on the jamming tolerance. Furthermore, the interference power levels are incremented so that jamming terminates the Wi-Fi connection at a Signal to Jammer Ratio (SJR) of -1 dB for OFDM.

B. Contributions

The main contributions of this paper are:

- A measurement setup to assess the congestion and spectrum utilization of the 2.4 GHz ISM band by simultaneously monitoring on both PHY and link layer; this setup is novel, not found in literature. Moreover the tool can be applied to any interferer source.
- The behavior of the PHY and link layer mechanisms under different interference conditions, *i.e.* A/V transmitter, microwave and Bluetooth.

III. Measurement Setup

In this setup we use passive methods to monitor the influence of an interferer source (see Figure 1). Passive means that the measurement setup only receives signals. For the experiments a connection is set up between Wi-Fi client and Access Point (AP)

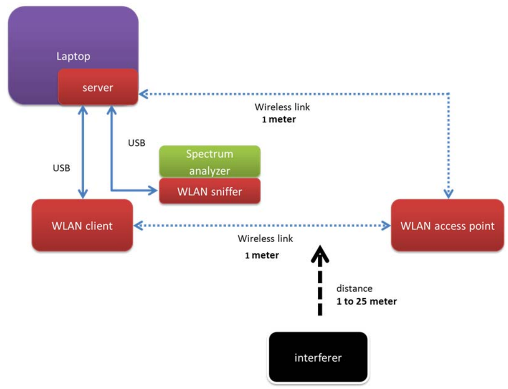


Fig. 1. The measurement setup for simultaneously monitoring PHY and link layer performance.

to start with; the same holds for the Wi-Fi server and AP. In addition a network load is applied in the network between server and client. Next, monitoring is activated which entails on one hand logging Wi-Fi packets by applying packet sniffing software and on the other hand - simultaneously - monitoring the 2.4 GHz ISM band by employing the CRFS spectrum analyzer. While monitoring is ongoing the influence of the interference source can be investigated; this is an extension of the UK survey [2]. The influence is assessed for three different interference sources using this setup, *i.e.* A/V transmitter, microwave, and active Bluetooth devices. The details regarding the measurement configuration are listed below:

- The measurement setup is deployed in a quiet environment (*i.e.* abandoned building in remote area) without any nearby devices active in the 2.4 GHz ISM band.
- In the Wi-Fi network client, AP and server are within a radius of 1 meter.
- The AP transmits in 802.11g mode with a data speed of 54 MBits/sec.
- The field strengths are measured and depicted in dBm. The CRFS equipment measures the spectrum every 200 ms.
- The sniffer application filters the packets by link destination address. So it allows to measure both the raw packets transmitted by the client and server. The sniffer software is specially developed for this purpose.
- To generate the Wi-Fi traffic data between client-server the Iperf open source tool is used.
- CRFS settings: a frequency sweep between $2400 - 2483$ MHz with a resolution of 4 kHz.
- Wi-Fi channel 11: $2451 - 2473$ MHz is used.

Note that in 802.11g mode a typical throughput of 3.1 Mbyte/sec is possible for the user. This results in around 2100 data frames/sec. In our experiments we offered Wi-Fi traffic load of around 10%. Moreover, as transport layer protocol UDP mode was chosen instead of TCP, because it allows to study the Wi-Fi interference better. The reason for this is that TCP has control algorithms that set back the frame rate to a lower level, when the packet loss rate increases. Moreover, UDP is connectionless and the PER could be easily measured. It should be noted that both UDP and TCP packets will be retransmitted when they are lost.

IV. Results

A/V Transmitter Interference. Using the described measurement setup the A/V transmitter interference (*i.e.* jamming) experiment is carried out. To investigate the Wi-Fi QoS as function of interference source power the A/V transmitter is first positioned at large distance (25m) from the client/AP; in a gradual continuous manner the A/V transmitter is moved in direction of the client/AP. Note that due to the indoor structure of the measurement environment the interference power level is used as performance metric for monitoring QoS instead of distance. To start with the A/V transmitter is turned on after 20 seconds of monitoring which is visible in the RF statistics plot depicted in Figure 2. From that point onwards the A/V transmitter is approaching the client/AP and this is visible in Figure 2 by the slope of the maximum received power curve indicating an increase from -155 dBm to -100 dBm. After 115 seconds of monitoring the nearby A/V interferer enforces the Wi-Fi connection to breakdown at a SJR of -1 dB due to the

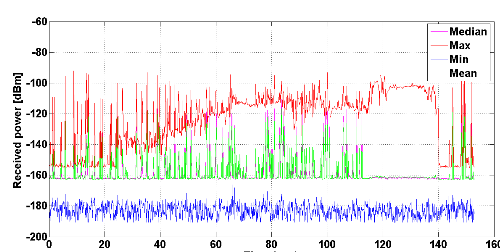
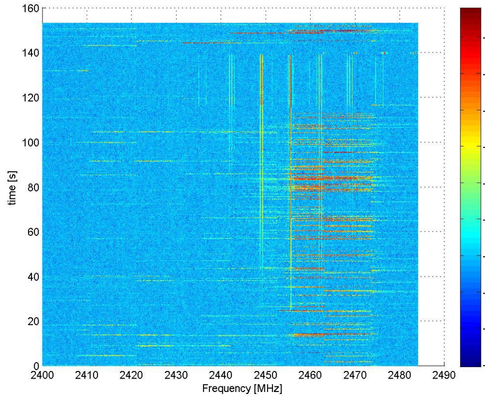
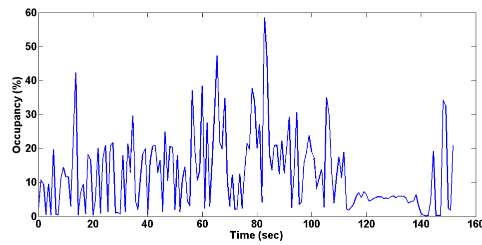


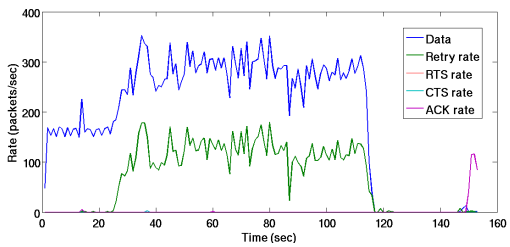
Fig. 2. The mean (green curve), median (purple curve), minimum (blue curve) and maximum signal strengths (red curve) as function of time. Here the maximum curve corresponds to the A/V transmitter signal's power, the median to the Wi-Fi signal power and the minimum signal curve to the noise.



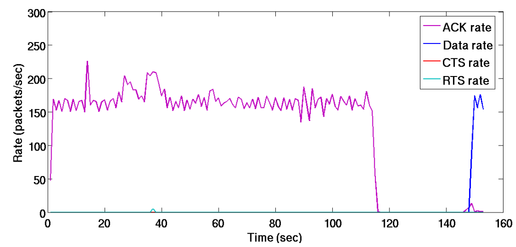
(a) PHY layer: spectrogram (received power in dBm). The A/V transmitter signals are visible as narrow-band vertical artifacts.



(b) PHY layer: spectrum occupancy of WLAN channel 11



(c) Link layer: the transmitted packets with destination client.

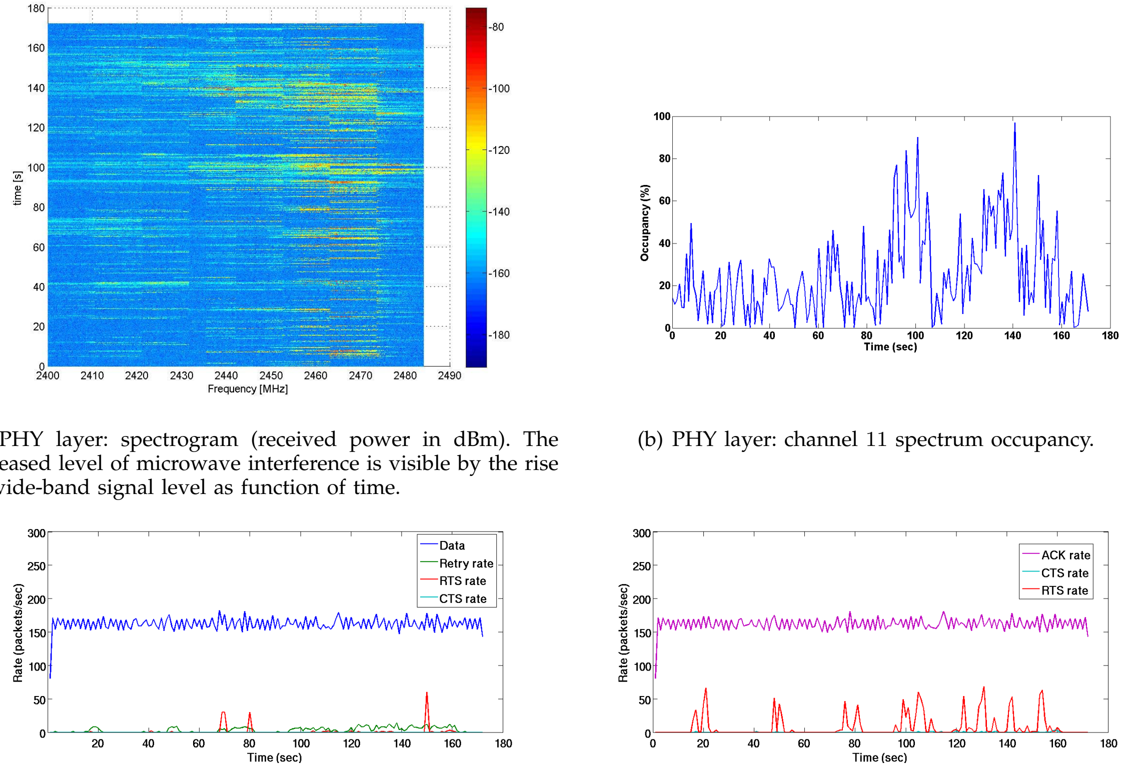


(d) Link layer: the transmitted packets with destination server.

Fig. 3. The A/V transmitter interference experiment: PHY and link layer monitoring results carried out in parallel.

high level of jamming interference power of almost -100 dBm (at a distance of around 10m). A period of Wi-Fi inactivity follows until the A/V transmitter is manually turned off (at 140 sec) which triggers the Wi-Fi network to automatically restore the connection after 142 seconds of monitoring. The RF monitoring results depicted in the spectrogram of Figure 3(a) and its corresponding occupancy plot in Figure 3(b) provide the following information: the active A/V transmitter can be identified in the spectrogram by narrow-band artifacts in vertical direction starting at 20 seconds; furthermore the figures clearly show Wi-Fi activity on channels 11 till the moment of network breakdown. According to the link layer observations in Figure 3(c) and Figure 3(d) both server and client communicate at a rate of 170 frames/sec in normal transmission mode; in addition, whilst the A/V transmitter is turned on the retry rate increases to a level of 150 frames/sec and inherently the data frame rate increases by the same amount as shown in Figure 3(c). On the other hand, the ACK packet rate remains solid around a rate of 170 frames/sec (see Figure 3(d)) which indicates the eventual successful transmission of data frames. This process continues till network breakdown indicated by a sharp downwards transition of data frame rate in Figure 3(c). The results are compared with the experiments conducted in [1] which show a connection breakdown at a SJR of -1 dB and the similar narrow-band artifacts are observed in the RF spectrum. However, the Wi-Fi QoS at the link layer is beyond the scope of [1] and cannot be compared.

Microwave Oven Interference. In this experiment a microwave oven is used as interference source which is placed at one meter distance from the client/AP whilst it heats up a glass of water. Similar as for the A/V transmitter experiment the Wi-Fi QoS is assessed as function of interference power level, *i.e.* the mode of the microwave is shifted up from mode 1 to 5 (till 700 Watt). The microwave influence is displayed by the lifted levels of signal strengths throughout the 2.4 GHz ISM band depicted in the spectrogram of Figure 4(a) and in the occupancy plot of Figure 4(b). This effect is best illustrated for the two highest modes (from 82 -



(a) PHY layer: spectrogram (received power in dBm). The increased level of microwave interference is visible by the rise in wide-band signal level as function of time.

(b) PHY layer: channel 11 spectrum occupancy.

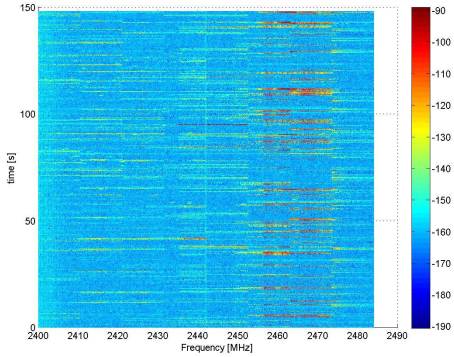
(c) Link layer: packets with destination client.

(d) Link layer: packets with destination server.

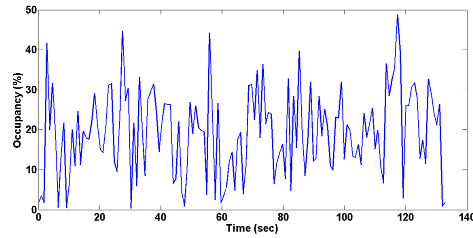
Fig. 4. Monitoring results using the microwave oven interference.

110 seconds and from 110 - 160 seconds). Regarding link layer monitoring, Figure 4(c) shows the microwave impact during the two highest modes of interference, *i.e.* the retry rate is at a significant higher level of 6.95% (amount of packet loss). Furthermore, Figure 4(d) shows peaks in the RTS/CTS curve - occurs irrespective of the mode - once the microwave oven is activated. The Wi-Fi QoS monitoring results at the link layer are in line with the simulation model in [6] under comparable conditions, *i.e.* a 600W microwave at 0.5m, $\lambda_w = 0.1$.

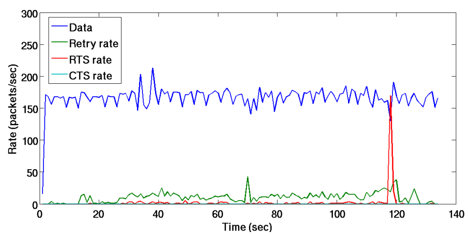
Bluetooth Interference. The influence of an active Bluetooth connection is tested in an experiment where an unidirectional data transfer at 1 Mb/sec between two v2.0 Bluetooth devices; both devices are within 1 meter of each other. Interference experiments are carried out with Bluetooth interference at distances ranging from 1m to 15m and monitoring results show distance independent characteristics (see [5]); for this purpose one particular experiment is highlighted, *i.e.* Bluetooth device communication at 1m distance from client/AP. Here Bluetooth is switched on from 15 seconds to 130 seconds of monitoring. Regarding the RF spectrum readings, artifacts are visible scattered throughout the spectrum in Figure 5(a) once Bluetooth is turned on, *i.e.* frequency hopping becomes active and deploys the entire 2.4 GHz ISM band. However, the channel occupancy of the active Wi-Fi channel is low (*i.e.* less then 50 percent) and thus is affected only to a small extent by the ongoing Bluetooth communication as shown in Figure 5(b). This is in line with the link layer results in Figure 5(c) which show a low retry rate and an unaffected data frame rate; note that Figure 5(d) shows a rise in RTS/CTS traffic once Bluetooth becomes active. Regarding the link layer, the 7% average packet loss (*i.e.* retry rate) is identical to the experiments in [8] where an experiment is carried out with an AFH-enabled Bluetooth interference source positioned at 1m distance. Note that the focus in [8] is not on overall QoS, thus the other monitoring results cannot be compared.



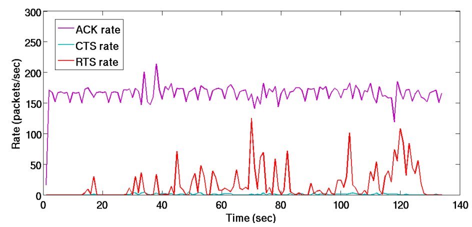
(a) PHY layer: spectrogram (received power in dBm). The Bluetooth interference is visible by the scattered artifacts due to the FHSS hopping mechanism.



(b) PHY layer: channel 11 spectrum occupancy.



(c) Link layer: packets with destination client.



(d) Link layer: packets with destination server.

Fig. 5. Monitoring results for Bluetooth interference.

V. Conclusion

A measurement setup is employed to assess the interference of different sources. This setup allows to analyze interference mechanisms in more detail at various levels of the OSI model, not found in literature. Traditional packet sniffers only focus on throughput and packet error rate, whereas the presented tool allows to analyze the received packets types and sub fields; a much sophisticated approach to analyze interference mechanisms.

References

[1] I. Harjula, J. Pinola, and J. Prokkola, "Performance of IEEE 802.11 based WLAN devices under various jamming signals," in *Military Communications Conference, 2011 - MILCOM 2011*, nov. 2011, pp. 2129 –2135.

[2] A. Wagstaff, "Estimating the utilisation of key licence-exempt spectrum bands," Mass Consultants Ltd, Tech. Rep. Issue 3, Apr. 2009.

[3] J. Sydor, "CORAL: A WiFi based cognitive radio development platform," in *Wireless Communication Systems (ISWCS), 2010 7th International Symposium on*, sept. 2010, pp. 1022 –1025.

[4] "http://www.ieee802.org/15/pub/TG2.html."

[5] G. V. Dyck, N. Golmie, R. E. V. Dyck, A. Soltanian, A. Tonnerre, and O. Rebala, "Interference evaluation of bluetooth and IEEE 802.11b systems," *in ACM Wireless Networks 2003*, vol. 9, pp. 202–211, 2003.

[6] C. Chiasserini and R. Rao, "Coexistence mechanisms for interference mitigation in the 2.4-GHz ISM band," *Wireless Communications, IEEE Transactions on*, vol. 2, no. 5, pp. 964 – 975, sept. 2003.

[7] R. Gummadi, D. Wetherall, B. Greenstein, and S. Seshan, "Understanding and mitigating the impact of RF interference on 802.11 networks," in *In Proc. of Sigcomm07*, 2007, pp. 385–396.

[8] N. Golmie, N. Chevrollier, and O. Rebala, "Bluetooth and WLAN coexistence: challenges and solutions," *Wireless Communications, IEEE*, vol. 10, no. 6, pp. 22 – 29, dec. 2003.

[9] T. Taher, M. Misurac, J. LoCicero, and D. Ucci, "Microwave oven signal interference mitigation for Wi-Fi communication systems," in *Consumer Communications and Networking Conference, 2008. CCNC 2008. 5th IEEE*, jan. 2008, pp. 67 –68.

[10] G. Li, S. Srikanteswara, and C. Maciocco, "Interference mitigation for WLAN devices using spectrum sensing," in *Consumer Communications and Networking Conference, 2008. CCNC 2008. 5th IEEE*, jan. 2008, pp. 958 –962.

[11] A. Kamerman and N. Erkocevic, "Microwave oven interference on wireless LANs operating in the 2.4 GHz ISM band," in *Personal, Indoor and Mobile Radio Communications, The 8th IEEE International Symposium on*, vol. 3, sep 1997, pp. 1221 –1227 vol.3.

[12] K. Pietikainen, A. Silvennoinen, M. Hall, and S.-G. Haggman, "IEEE 802.11g tolerance to narrowband jamming," in *Military Communications Conference, 2005. MILCOM 2005. IEEE*, oct. 2005, pp. 1825 –1830 Vol. 3.