

LUND UNIVERSITY

A framework for interference analysis of heterogeneous radio networks

Stranne, André; Edfors, Ove; Molin, Bengt-Arne

Published in:
2004 IEEE 15th International Symposium on Personal, Indoor and Mobile Radio Communications (IEEE Cat. No.04TH8754)

2004

Link to publication

Citation for published version (APA):
Stranne, A., Edfors, O., & Molin, B.-A. (2004). A framework for interference analysis of heterogeneous radio networks. In *2004 IEEE 15th International Symposium on Personal, Indoor and Mobile Radio Communications (IEEE Cat. No.04TH8754)* (pp. 1168-1172). IEEE - Institute of Electrical and Electronics Engineers Inc..

Total number of authors:
3

General rights
Unless other specific re-use rights are stated the following general rights apply:
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.
• Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
• You may not further distribute the material or use it for any profit-making activity or commercial gain
• You may freely distribute the URL identifying the publication in the public portal

Read more about Creative commons licenses: https://creativecommons.org/licenses/

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

LUND UNIVERSITY

PO Box 117
221 00 Lund
+46 46-222 00 00

A FRAMEWORK FOR INTERFERENCE ANALYSIS OF HETEROGENEOUS RADIO NETWORKS

André Stranne[1,2], Ove Edfors[1], Bengt-Arne Molin[3]

[1]Dept. of Electroscience, Lund University, Box 118, SE-221 00 Lund, Sweden
[2]TeliaSonera AB, Box 85, SE-201 20 Malmö, Sweden
[3]Axis Communications AB, Emdalav. 14, SE-223 69 Lund, Sweden
E-mail: andre.stranne@es.lth.se

Abstract— **The increasing use of unlicensed frequency bands for radio communications calls for investigations of the interference between coexisting radio networks. The wide variety of radio interfaces makes such investigations hard to perform. In this paper we present a general framework for the analysis of heterogeneous interfering radio networks, where the networks are modeled with individual properties for the packet types used, transmitted power distributions in time and frequency from the packet transmissions, and with path loss between network nodes. By using closed form expressions for the throughput of the networks, important mechanisms limiting their performance can be investigated. The closed form expressions enable fast and flexible analysis to be performed without extensive computer simulations. To illustrate the use of the framework we analyze an example system of interfering IEEE 802.11b and Bluetooth networks.**

Keywords— **Heterogeneous radio networks, interference analysis, throughput, coexistence, IEEE 802.11b, Bluetooth.**

I. Introduction

The use of radio technology for data communications has been increasing for some time. For example, systems such as Wideband Code Division Multiple Access (WCDMA), Wireless Local Area Networks (WLANs) and Wireless Personal Area Networks (WPANs) are currently being deployed in many countries and in many types of environments. Within and between many of these systems interference is a major issue.

In cellular systems the network deployment and the interference situation is controlled by the network operators using, e.g., network planning and admission control policies. The understanding of the impact of interference in these networks can be used to optimize the networks, which translates to reduced investment costs for the operators.

In unlicensed frequency bands, where different networks must share the spectrum resource in a fair way, there is no central point of control. In these bands the systems must be designed to cope with interference of different kinds and to adapt to current interference situations. Since the various radio interfaces used in these bands differ a great deal in terms of modulation, coding, transmit power, receiver sensitivities, spread spectrum techniques, medium access control (MAC) frame structures, retransmission schemes, access control methods etc., the analysis of interference between different radio networks is far from trivial.

In this paper we apply a general analytical framework for the analysis of heterogeneous interfering radio networks, which can be used to investigate important mechanisms limiting the performance of a wide class of radio networks. The framework provides closed form expressions for the throughput of the interfering networks, which allows for fast and flexible interference analysis, avoiding extensive simulations. We illustrate the use and the flexibility of the framework by applying it to a system of interfering IEEE 802.11b and Bluetooth networks, performing an analytical coexistence analysis.

Previous work addressing coexistence problems in unlicensed bands has mainly been based on simulations, although some analytical results have been reported. For the coexistence of multiple Bluetooth networks, analytical results have been presented by, e.g., El-Hoiydi in [1]. These results are based on packet collisions in time and frequency and are limited to single packet lengths. The extension to multiple packet lengths was treated by Florén et al. in [2]. Howitt performs a more detailed analysis of Bluetooth networks using a single packet length in [3], considering, e.g., radio link properties and adjacent channel interference, and a similar approach is used in [4] to analyze the coexistence of Bluetooth and IEEE 802.11b networks, which is also done in a detailed way by Conti et al. in [5]. In [6] a general framework for analysis of interfering networks is presented, where both multiple packet lengths and radio link properties are taken into account, providing closed form expressions for the throughput of the interfering networks. In [6], the framework is applied to a homogeneous system of interfering Bluetooth networks, and in this paper we show how the framework can be used in the analysis of heterogeneous radio networks.

The outline of the paper is as follows. In Section II the network model is introduced and, in Section III, the method of analysis is presented. In Section IV the use of the framework is illustrated by analyzing an example system of interfering Bluetooth and IEEE 802.11b networks. Finally, some concluding remarks are given in Section V.

II. Network Model

To be able to model heterogeneous radio networks in a general way we reuse parts of the system model described in [6]. Here, a system consists of a collection of networks with units communicating by transmitting packets, as illustrated in Fig. 1. As shown in the figure, a microwave oven can also be modeled as a packet transmitting network, but only as a source of interference in the system. The networks are assumed to be 'unaware' of each other, which means that they sometimes interfere by transmitting packets simultaneously in the same or partly overlapping fre-

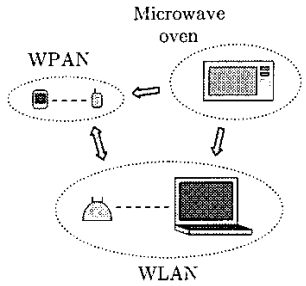


Fig. 1. Three interfering networks. The arrows indicate interference.

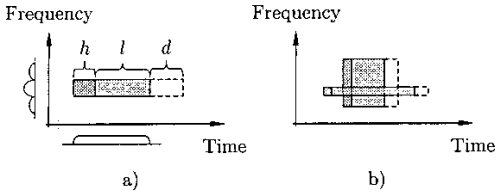


Fig. 2. a) A packet with the transmitted power distribution in time and frequency. b) Two interfering packets overlapping in time and frequency.

quency bands. Within the networks we assume that there is exactly one packet transmission at a time, which means that we will obtain performance results for networks with full traffic load in the worst case interference environment.

Each network in the system has a set of available packet types that can be used for packet transmissions. The packet types can have different lengths, carry different amounts of data, can be transmitted with different transmit power levels and with different transmit power spectra, and they can have different robustness properties against interference. More specifically, a packet consists of a header with length h, a payload with length l, and a guard interval with length d, as shown in Fig. 2a. The parameter $L = h + l + d$ is used for the total lengths of the packets including guard interval. Since payload data can be transmitted with different data rates we use D for the number of uncoded bits of payload data transferred per unit time in a packet. Finally, indexing all packet types used by a network, a packet of type i in the set of packet types is transmitted by the network units with a probability r_i on one of q randomly selected frequency channels. Note that a network using a single fixed channel for its transmissions will use $q = 1$, which is just a special case of this random frequency hopping scheme.

With this system model, each network will produce its own type of interference in the spectral and temporal domains, affecting the throughput of other networks sharing the same spectrum. The interference is characterized both by the set of channels used for packet transmissions and how the power is distributed in time and frequency when a packet is transmitted, as illustrated in Fig. 2a.

III. Interference Analysis

A network in the system, e.g., the WPAN or the WLAN network in Fig. 1, will have its communication performance affected by the interference from the other networks in the vicinity. As a measure of communication performance we will use the ensemble average network throughput in the analysis, which can be associated with the data transfer rate of the networks. The throughput of a reference network using M packet types is given by [6]

$$R = \frac{\sum_{k=1}^{M} r_k D_k l_k \Pr\{\text{success}; k\}}{\sum_{n=1}^{M} r_n (h_n + l_n + d_n)}, \tag{1}$$

where $\Pr\{\text{success}; k\}$ is the probability for successful reception of type k packets by the reference network. It can be seen that the expression depends both on the M specified packet types and the probabilities for successful reception of each type of packet. If the received signal power is strong enough compared to the noise level and there is no interference in the system, $\Pr\{\text{success}; k\}$ will be 1 for all packet types. Then, R will attain its maximum value depending on the lengths of the packet payloads, the payload data rates etc. The problem now is to evaluate $\Pr\{\text{success}; k\}$ when there is interference from other networks in the system.

The probabilities of successful packet receptions will depend on the mechanisms assumed to cause packet losses. In this paper we will make the assumption that the outcome of packet receptions is determined by the per-packet signal-to-noise and interference ratio (SNIR), γ, at the receiver. More specifically, we will assume that if the useful signal is not strong enough compared to the noise and interference, the packets are lost. To find the probability of a packet received with γ above a specified threshold $\gamma_{\min}$, i.e., the probability of successful packet reception, the probability distribution function (PDF) of γ must be determined.

To simplify the analysis, we do not determine the PDF of γ in the general case where the useful signal power, C, and the total interfering power, I, both vary with time. Instead we only consider fixed distances between all network units and no fading, which means that the received useful power C at a receiver is a fixed deterministic quantity given by the transmitted useful power, the distance attenuation and some additional losses at the receiver. Consequently, the average SNIR of a packet can be written as

$$\gamma = \frac{C}{N_{\text{noise}} + E_I / (L - d)}, \tag{2}$$

where N_{noise} is a deterministic noise power parameter and E_I is the total interfering energy received during the reception of the packet. Here, the only varying quantity is E_I which, e.g., depends on the overlap in time and frequency between the received packet and interfering packets, as illustrated in Fig. 2b. Using (2), we can now translate the condition for successful packet reception, $\gamma > \gamma_{\min}$, into $E_I < E_{I,\max}$, and focus on the received interfering energy in the rest of the analysis.

Thus, to find the probability of successful packet reception $\Pr\{\text{success}\}$, we will calculate the PDF of the received

interfering energy, $f_{E_I}(e)$, and then integrate over the PDF from zero up to the threshold $E_{I,\max}$, i.e.,

$$\Pr\{\text{success}\} = \int_{e=0}^{E_{I,\max}} f_{E_I}(e)de. \quad (3)$$

Calculating $f_{E_I}(e)$ is not a simple problem since it includes taking all possible overlaps in time into account, as well as the power leakage between all pairs of channels that can be used. However, closed form expressions for the PDF can be obtained by focusing on a single interferer and carefully following the implications of its packet transmissions. The details about this calculation, which is not included here due to space limitations, can be found in [7].

IV. Coexistence Analysis Example

Using the system model and the method of analysis described above we will now perform an analysis of a system consisting of a collection of IEEE 802.11b and Bluetooth networks. To be able to perform the analysis we must first determine appropriate system model parameters.

A. Bluetooth Network Model

Starting with Bluetooth, three of the packet types defined in the standard [8] are used, namely DH1, DH3 and DH5. We assume that they are equally probable of being selected for transmissions within the Bluetooth networks. Thus, we have

Packet sel. prob.	$r =$	[1/3 1/3 1/3]
Header length	$h =$	[150 158 158] μs
Payload length	$l =$	[200 1448 2696] μs
Guard interval length	$d =$	[275 269 271] μs
Payload bit rate	$D =$	[1 1 1] bits/μs,

and a channel set consisting of 79 channels with all channels equally probable of being selected. The Bluetooth networks use packet-based frequency hopping over the channels in the channel set, which means that there is a pseudo-random change of channel after each packet transmission.

The link budget for the Bluetooth networks is assumed to be given by

Radiated power	EIRP =	0 dBm
Path loss (ref. units)	$L_{\text{PL.ref}} =$	40 dB
Path loss (int. units)	$L_{\text{PL.interf}} =$	[40 50 54] dB
Receiver loss	$L_{\text{r}} =$	2 dB
Min. received SNIR	$\gamma_{\min} =$	20 dB,

where the path loss figures 40, 50 and 54 dB correspond to typical path loss in a line-of-sight (LOS) situation for distances of 1, 3 and 5 meters at 2.4 GHz. We have used the path loss model given by eq. (12) in [9], with parameters $S_0+b = 40$ dB and $a = 2.0$. Furthermore, we have assumed a transmit power of 2 dBm and transmitter losses of 2 dB to obtain an effective isotropically radiated power (EIRP) of 0 dBm. The propagation loss between the units of the reference network has been set to 40 dB which corresponds to a distance of approximately 1 m. In the calculations below we consider three scenarios where the distances between the units of the reference network and the units of the interfering networks are either 1, 3 or 5 meters.

To find the parameter $E_{I,\max}$, we assume that the Bluetooth receivers in the system are characterized by the parameters

Noise figure	$F_{\text{sys}} =$	20 dB
Noise bandwidth	$B =$	60 dBHz
Ref. noise pow. dens.	$N_0 =$	-174 dBm/Hz,

which result in a noise power of $N_{\text{noise}} = F_{\text{sys}} + B + N_0 = -96$ dBm. It should be noted that current Bluetooth receiver implementations generally have lower noise figures than 20 dB.

For successful packet reception, the received SNIR must be above the specified threshold $\gamma_{\min} = 20$ dB, and using (2) the corresponding thresholds for the amounts of tolerable interfering energy, for each of the three Bluetooth packet types are $E_{I,\max} =$ [0.22 1.0 1.8] pJ.

B. IEEE 802.11b Network Model

The IEEE 802.11b networks [10] use a single wideband carrier in the ISM-band at 2.4 GHz and no frequency hopping. Consequently, we define the channel set used by each IEEE 802.11b network to consist of only one channel. In this example we assume that only the 11 Mb/s mode of transmission is used for transmitting packets, and that the RTS-CTS handshaking mechanism is not used. We also assume that three types of packets are used with 40, 500 and 1500 bytes of payload data, and that they are equally likely to be selected for transmission.

The carrier sense multiple access mechanism with collision avoidance (CSMA/CA) must be given some special consideration, since it affects the idle time ('guard interval'), d, between packet transmissions. With short preambles the total overhead adds up to 121 μs for all three packet types, and the lengths of the payloads become 30 μs, 364 μs and 1091 μs. However, the idle time between consecutive packets is random in CSMA/CA. In fact, it also depends on the probability for successful packet reception since a random back-off procedure is initiated whenever a packet is lost. Thus,

Packet sel. prob.	$r =$	[1/3 1/3 1/3]
Header length	$h =$	[121 121 121] μs
Payload length	$l =$	[30 364 1091] μs
Idle time	$d =$	Determined by Pr{success}
Payload bit rate	$D =$	[11 11 11] bits/μs.

The determination of d can be made by the use of a Markov model, as shown in Section IV-C. When a packet has been successfully received it is acknowledged by an ACK-frame with length $h_{\text{ACK}} + l_{\text{ACK}} = 106$ μs. However, to simplify the analysis in this example, we assume that no ACK-frame is transmitted.

To continue, the IEEE 802.11b link budget is given by

Radiated power	EIRP =	20 dBm
Path loss (ref. units)	$L_{\text{PL.ref}} =$	60 dB
Path loss (int. units)	$L_{\text{PL.interf}} =$	[40 50 54] dB
Receiver loss	$L_{\text{r}} =$	2 dB
Min. received SNIR	$\gamma_{\min} =$	10 dB.

Here we have assumed an EIRP of 100 mW. The propagation loss between the units of the reference network has

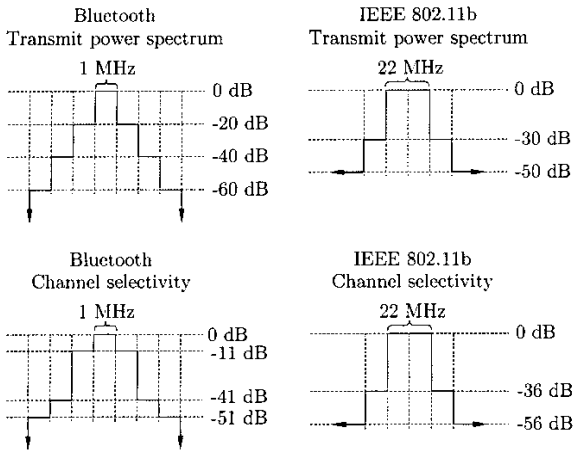


Fig. 3. Models of Bluetooth and IEEE 802.11b transmit power spectra and receiver channel selectivities.

been set to 60 dB corresponding to a distance of approximately 10 m using the path loss model in Section IV-A.

The IEEE 802.11b receivers are assumed to be characterized by the parameters

Noise figure	$F_{\text{sys}} =$	7 dB
Noise bandwidth	$B =$	74 dBHz
Ref. noise pow. dens.	$N_0 =$	-174 dBm/Hz,

which results in a noise power of $N_{\text{noise}} = -93$ dBm. From (2), the thresholds for the amounts of tolerable interfering energy for the three packet lengths used by the IEEE 802.11b networks are $E_{I,\max} = [\ 0.94 \quad 3.1 \quad 7.6\ ]$ pJ.

Lastly, we need to model the leakage of power between overlapping frequency channels. To get an estimate of the performance in the worst case interference situation, we use the models of the transmit power spectra and the receiver channel selectivities of the Bluetooth and IEEE 802.11b transceivers shown in Fig. 3. These models roughly correspond to what is given in the specifications.

Note that the IEEE 802.11b networks are assumed only to use clear channel assessment (CCA) mode 2 in this example, which means that the network nodes consider the channel busy and hold transmissions only when an IEEE 802.11b carrier is detected. This also means that the IEEE 802.11b networks must be set to use different and adequately separated frequency channels so that they do not detect each others carriers. For simplicity, we have also assumed that there is no internal interference within the IEEE 802.11b networks.

C. Analysis

We start by analyzing a single Bluetooth reference network in the vicinity of interfering IEEE 802.11b networks. The idle time between IEEE 802.11b packets is affected by the transmissions from the Bluetooth reference network, since the Bluetooth transmissions can make the IEEE 802.11b packet transmissions fail. Consequently, given a single Bluetooth network at a certain distance from an IEEE 802.11b network, the idle time in the IEEE 802.11b network must first be calculated.

To calculate the IEEE 802.11b idle time parameter d, we use a Markov model with six states corresponding to the different sizes [10] of the contention window (CW) in number of slots, CWSize = [31 63 127 255 511 1023], where a slot is 20 μs. The transition probabilities in the Markov model are given by the packet type selection probabilities, r, and the successful packet reception probabilities, Pr{success}, for the three IEEE 802.11b packet types.

To calculate Pr{success} we use the expressions derived in [7] to obtain the probabilities [0.76 0.70 0.63] for a distance of 1 m to the Bluetooth units, [0.82 0.87 0.93] for 3 m, and [1.0 1.0 1.0] for 5 m. Note that for 1 m, shorter packets have higher probabilities of successful receptions, whereas for 3 m, the situation is reversed. For a distance of 5 m to the Bluetooth network, all packet types are received correctly. The stationary probabilities for the corresponding distances are then calculated, and show that the states corresponding to smaller CWs become more probable as the distance to the interferer is increased. The idle time between two IEEE 802.11b packets consists of a SIFS interval of 10 μs, an ACK-frame time of 106 μs, a DIFS interval of 50 μs, and a uniformly distributed random number of slots, A, from 0 to CWSize. Thus, d = SIFS+ACK+DIFS+A, where the probabilities for all possible values of A are now known.

The throughput results from the calculations are shown in Fig. 4 as a function of number of interfering IEEE 802.11b networks for different distances to the Bluetooth reference network. It can be seen in the figure that all three curves indicate significant throughput reductions with the number of interferers. There is, however, only a weak dependence on the distance to the interferers, up to 5 meters. The Bluetooth throughput is shown to be reduced to about 50 % for two IEEE 802.11b interferers.

Even though it is hardly visible in Fig. 4, for up to 4 interferers the calculated throughput is slightly higher for a distance of 1 m to the interferers than for 3 and 5 m. Generally, it can be expected that the throughput is increased with larger distances to the interferers since the received interfering power is then reduced. However, it is in fact not only the power that is affected by the distance to the interferers but also the idle time intervals in the IEEE 802.11b networks. The more the IEEE 802.11b networks are affected by the interference from the Bluetooth reference network (i.e., the closer they are), the more the CSMA/CA mechanism makes the IEEE 802.11b networks back off to produce less interference back on the Bluetooth network. The detailed interaction between the two network types is however beyond the scope of this paper.

Note that the results are shown for numbers of networks up to 20 in Fig. 4, which is currently a very high number of IEEE 802.11b networks deployed in a limited area, and also far more networks than the number of separated channels available in the ISM-band. In USA, the ISM-band at 2.4 GHz allows for 14 channels in total to be used by IEEE 802.11b networks, of which only 3 channels are completely separated.

To analyze the performance of an IEEE 802.11b reference network in the vicinity of interfering Bluetooth networks

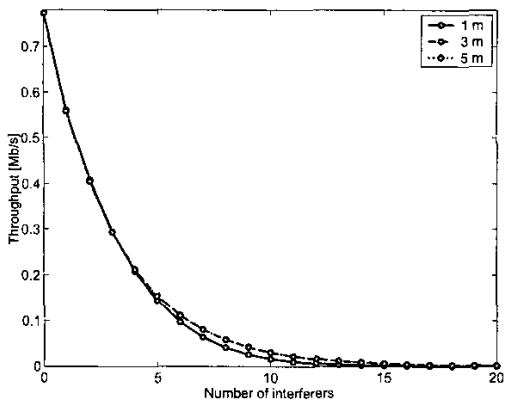


Fig. 4. Throughput of a Bluetooth reference network as a function of number of interfering IEEE 802.11b networks for distances of 1 (solid curve), 3 (dashed) and 5 m (dotted) between reference network units and interferers. Note that the maximum throughput of about 770 kb/s is a result of the specific mix of packet types used in this example.

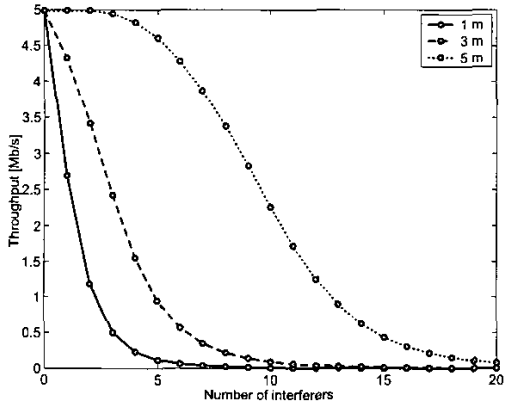


Fig. 5. IEEE 802.11b network throughput as a function of number of interfering Bluetooth networks. Results are shown for distances between reference network and interfering network units of 1 (solid curve), 3 (dashed) and 5 m (dotted). Here, the mix of packet types used results in a maximum throughput of about 5 Mb/s.

we use the same method as described above, calculating first the influence of the Bluetooth interference on the idle time distribution in the IEEE 802.11b network and then the IEEE 802.11b throughput. In Fig. 5, the throughput of an IEEE 802.11b network has been plotted as a function of number of interfering Bluetooth networks for distances between reference and interfering units of 1, 3 and 5 m. It can be seen in the figure that when the Bluetooth networks are close to the IEEE 802.11b reference network, throughput decreases very rapidly with the number of interferers. With the interferers at a distance of 1 m from the reference network, the throughput is reduced to about 50 % for a single interferer. For distances of 3 and 5 meters, the corresponding numbers of interferers are 3 and 9, respectively. Here, the throughput of the IEEE 802.11b network is affected by the Bluetooth interference both in terms of packet losses due to collisions, but also indirectly in terms of larger idle times when packet losses occur.

The system model does not take into account receiver nonlinearities limiting the performance of, especially, Bluetooth receivers under strong interference. Taking these into account would result in lower calculated performance. However, preliminary measurements on IEEE 802.11b throughput under Bluetooth interference support the obtained results.

V. Conclusions

In this paper a framework is presented for interference analysis of coexisting packet radio networks. The framework allows for multiple packet lengths being used by the networks and also radio link properties to be included in the analysis. An example system of coexisting Bluetooth and IEEE 802.11b networks is analyzed to illustrate the use of the closed form expressions and the strength of the framework.

Using the analytical framework important mechanisms limiting the performance of heterogeneous interfering radio networks can be investigated. This can be useful both in the analysis of existing radio networks, but also in the design of new radio interfaces. Some extensions of the system model, e.g., to handle less than full traffic load can easily be incorporated in the analysis, while other extensions, e.g., to include other propagation models and fading are more complex, and leave much room for future work.

References

[1] A. El-Hoiydi, "Interference between Bluetooth networks–Upper bound on the packet error rate," *IEEE Communications Letters*, vol. 5, pp. 245–247, June 2001.

[2] F. Florén, A. Stranne, O. Edfors, and B.-A. Molin, "Throughput analysis of strongly interfering slow frequency-hopping wireless networks," in *Proceedings of the IEEE 53rd Vehicular Technology Conference*, vol. 1, pp. 496–500, 2001.

[3] I. Howitt, "Mutual interference between independent Bluetooth piconets," *IEEE Transactions on Vehicular Technology*, vol. 52, pp. 708–718, May 2003.

[4] I. Howitt, "Bluetooth performance in the presence of 802.11b WLAN," *IEEE Transactions on Vehicular Technology*, vol. 51, pp. 1640–1651, Nov. 2002.

[5] A. Conti, D. Dardari, G. Pasolini, and O. Andrisano, "Bluetooth and IEEE 802.11b coexistence: Analytical performance evaluation in fading channels," *IEEE Journal on Selected Areas in Communications*, vol. 21, pp. 259–269, Feb. 2003.

[6] A. Stranne, O. Edfors, and B.-A. Molin, "Energy-based throughput analysis of packet radio networks," in *Proceedings of the IEEE International Conference on Communications (ICC), (accepted for publication)*, 2004.

[7] A. Stranne, "An analysis of the throughput of packet radio networks," Tech. Rep. No. 34, ISSN 1402-8662, Department of Electroscience, Lund University, Mar. 2003.

[8] "Specification of the Bluetooth system (core)," Feb. 2001. Bluetooth SIG, http://www.bluetooth.com.

[9] G. J. M. Janssen, P. A. Stigter, and R. Prasad, "Wideband indoor channel measurements and BER analysis of frequency selective multipath channels at 2.4, 4.75, and 11.5 GHz," *IEEE Transactions on Communications*, vol. 44, pp. 1272–1288, Oct. 1996.

[10] "IEEE 802.11 wireless LAN medium access control (MAC) and physical layer (PHY) specifications: Higher-speed physical layer extension in the 2.4 GHz band," Sept. 1999. IEEE, http://www.ieee.org.