Wireless Networks 9, 201–211, 2003

Interference Evaluation of Bluetooth and IEEE 802.11b Systems

N. GOLMIE *, R.E. VAN DYCK, A. SOLTANIAN, A. TONNERRE and O. RÉBALA
National Institute of Standards and Technology, Gaithersburg, MD 20899, USA

Abstract. The emergence of several radio technologies, such as Bluetooth and IEEE 802.11, operating in the 2.4 GHz unlicensed ISM frequency band, may lead to signal interference and result in significant performance degradation when devices are colocated in the same environment. The main goal of this paper is to evaluate the effect of mutual interference on the performance of Bluetooth and IEEE 802.11b systems. We develop a simulation framework for modeling interference based on detailed MAC and PHY models. First, we use a simple simulation scenario to highlight the effects of parameters, such as transmission power, offered load, and traffic type. We then turn to more complex scenarios involving multiple Bluetooth piconets and WLAN devices.

Keywords: WPANs, Bluetooth, IEEE 802.11b, interference

1. Introduction

The proliferation of mobile computing devices including laptops, personal digital assistants (PDAs), and wearable computers has created a demand for wireless personal area networks (WPANs). WPANs allow closely located devices to share information and resources. A key challenge in the design of WPANs is adapting to a hostile radio environment that includes noise, time-varying channels, and abundant electromagnetic interference. Today, most radio technologies considered by WPANs (Bluetooth Special Interest Group [2], and IEEE 802.15) employ the 2.4 GHz ISM frequency band, which is also used by Local Area Network (WLAN) devices implementing the IEEE 802.11b standard specifications [9]. It is anticipated that some interference will result from all these technologies operating in the same environment. WLAN devices operating in proximity to WPAN devices may significantly impact the performance of WPAN and vice versa.

The main goal of this paper is to present our findings on the performance of these systems when operating in close proximity to each other. Our results are based on detailed models for the MAC, PHY, and wireless channel. Recently, a number of research activities has led to the development of tools for wireless network simulation [1,16]. While some of these tools include a PHY layer implementation, it is often abstracted to a discrete channel model that does not implement interference *per se*. Therefore, in order to model interference and capture the time and frequency collisions, we chose to implement an integrated MAC-PHY module.

Efforts to study interference in the 2.4 GHz band are relatively recent. For example, interference caused by microwave ovens operating in the vicinity of a WLAN network has been investigated [17] and requirements on the signal-to-noise ratio (SNR) are presented by Kamerman and Erkocevic [11]. In addition, there has been several attempts at quantifying the impact of interference on both the WLAN and Bluetooth performance. Published results can be classified into at least three categories depending on whether they rely on analysis, simulation, or experimental measurements.

Analytical results based on probability of packet collision were obtained by Shellhammer [13], Ennis [4], and Zyren [18] for the WLAN packet error and by Golmie [6] for the Bluetooth packet error. In all these cases, the probability of packet error is computed based on the probability of packet collision in time and frequency. Although these analytical results can often give a first order approximation on the impact of interference and the resulting performance degradation, they often make assumptions concerning the traffic distributions and the operation of the media access protocol, which can make them less realistic. More importantly, in order for the analysis to be tractable, mutual interference that can change the traffic distribution for each system is often ignored.

On the other hand, experimental results, such as the ones obtained by Kamerman [10], Howitt et al. [8], and Fumolari [5] for a two-node WLAN system and a two-node Bluetooth piconet, can be considered more accurate at the cost of being too specific to the implementation tested. Thus, a third alternative consists of using modeling and simulation to evaluate the impact of interference. This third approach can provide a more flexible framework. Zurbes et al. [19] present simulation results for a number of Bluetooth devices located in a single large room. They show that for 100 concurrent web sessions, performance is degraded by only 5%. Golmie et al. [7] use a detailed MAC and PHY simulation framework to evaluate the impact of interference for a pair of WLAN devices and a pair of Bluetooth devices. Similar results have been obtained by Lansford et al. [12] for the case of colocated WLAN and Bluetooth devices on the same laptop. Their simulation models are based on a link budget analysis and a theoretical calculation of the BER (Q function calculation). The work in this paper is an extension of [7].

* Corresponding author.
E-mail: nada.golmie@nist.gov

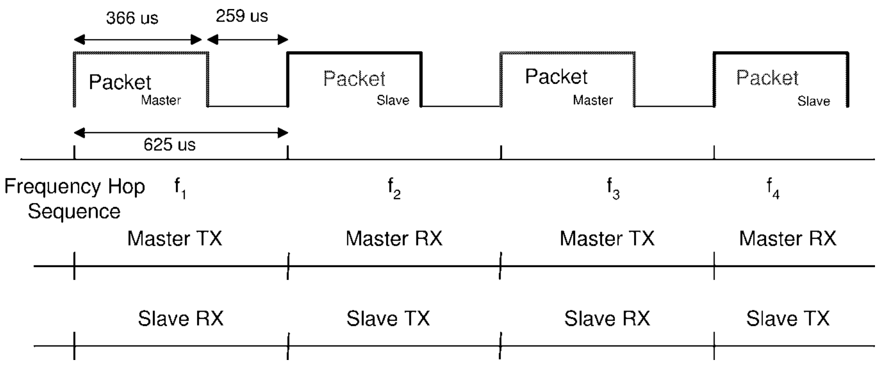


Figure 1. Master TX/RX hopping sequence.

This paper is organized as follows. In section 2, we give some general insights on the Bluetooth and IEEE 802.11 protocol operation. In section 3, we describe in great detail our modeling approach for the MAC, PHY and wireless channel. In section 4, we evaluate the impact of interference on both Bluetooth and WLAN performance and present simulation results. Concluding remarks are offered in section 5.

2. Protocol overview

2.1. Bluetooth

In this section, we give a brief overview of the Bluetooth technology [2] and discuss the main functionality of its protocol specifications. Bluetooth is a short range (0–10 m) wireless link technology aimed at replacing non-interoperable proprietary cables that connect phones, laptops, PDAs and other portable devices together. Bluetooth operates in the ISM frequency band starting at 2.402 GHz and ending at 2.483 GHz in the USA and Europe. 79 RF channels of 1 MHz width are defined. The air interface is based on an antenna power of 1 mW with an antenna gain of 0 dB. The signal is modulated using binary Gaussian Frequency Shift Keying (GFSK). The raw data rate is defined at 1 Mbit/s. A Time Division Multiplexing (TDM) technique divides the channel into 625 μs slots. Transmission occurs in packets that occupy an odd number of slots (up to 5). Each packet is transmitted on a different hop frequency with a maximum frequency hopping rate of 1600 hops/s.

Two or more units communicating on the same channel form a piconet, where one unit operates as a master and the others (a maximum of seven active at the same time) act as slaves. A channel is defined as a unique pseudo-random frequency hopping sequence derived from the master device's 48-bit address and its Bluetooth clock value. Slaves in the piconet synchronize their timing and frequency hopping to the master upon connection establishment. In the connection mode, the master controls the access to the channel using a polling scheme where master and slave transmissions alternate. A slave packet always follows a master packet transmission as illustrated in figure 1, which depicts the master's view of the slotted TX/RX channel.

There are two types of link connections that can be established between a master and a slave: the Synchronous Connection-Oriented (SCO), and the Asynchronous Connection-Less (ACL) link. The SCO link is a symmetric point-to-point connection between a master and a slave where the master sends an SCO packet in one TX slot at regular time intervals, defined by T_{SCO} time slots. The slave responds with an SCO packet in the next TX opportunity. T_{SCO} is set to either 2, 4 or 6 time slots for HV1, HV2, or HV3 packet formats, respectively. All three formats of SCO packets are defined to carry 64 Kbit/s of voice traffic and are never retransmitted in case of packet loss or error.

The ACL link is an asymmetric point-to-point connection between a master and active slaves in the piconet. An Automatic Repeat Request (ARQ) procedure is applied to ACL packets where packets are retransmitted in case of loss until a positive acknowledgement (ACK) is received at the source. The ACK is piggy-backed in the header of the returned packet where an ARQN bit is set to either 1 or 0 depending on whether or not the previous packet was successfully received. In addition, a sequence number (SEQN) bit is used in the packet header in order to provide a sequential ordering of data packets in a stream and filter out retransmissions at the destination. Forward Error Correction (FEC) is used on some SCO and ACL packets in order to correct errors and reduce the number of ACL retransmissions.

Both ACL and SCO packets have the same packet format. It consists of a 72-bit access code used for message identification and synchronization, a 54-bit header and a variable length payload that contains either a voice or a data packet depending on the type of link connection that is established between a master and a slave.

A repetition code of rate 1/3 is applied to the header, and a block code with minimum distance, $d_{\min}$, equal to 14, is applied to the access code so that up to 13 errors are detected and $\lfloor (d_{\min} - 1)/2 \rfloor = 6$ can be corrected. Note that uncorrected errors in the header and the access code lead to a packet drop. Voice packets have a total packet length of 366 bits including the access code and header. A repetition code of 1/3 is used for HV1 packet payload. On the other hand, DM and HV2 packet payloads use a 2/3 block code where every 10 bits of information are encoded with 15 bits. DH and HV3 packets do not have any encoding on their payload. HV packets do

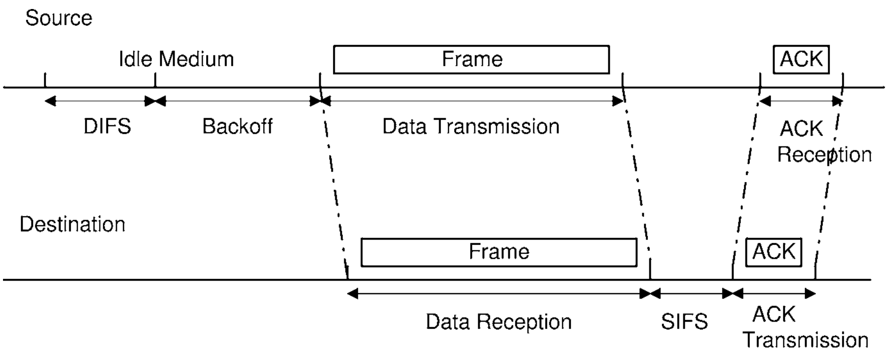


Figure 2. WLAN frame transmission scheme.

Table 1
Summary of error occurrences in the packet and actions taken in case errors are not corrected.

Error location	Error correction	Action taken
Access code	$d_{\min} = 14$	Packet dropped
Packet header	1/3 repetition	Packet dropped
HV1 payload	1/3 repetition	Packet accepted
HV2 payload	2/3 block code	Packet accepted
HV3 payload	No FEC	Packet accepted
DM1, DM3, DM5 payload	2/3 block code	Packet dropped
DH1, DH3, DH5 payload	No FEC	Packet accepted

not have a CRC in the payload. In case of an error occurrence in the payload, the packet is never dropped. Uncorrected errors for DM and DH packets lead to dropped packets and the application of the ARQ and SEQN schemes. Table 1 summarizes the error occurrences in the packet and the actions taken by the protocol.

2.2. *IEEE 802.11b*

The IEEE 802.11 standard [9] defines both the physical (PHY) and medium access control (MAC) layer protocols for WLANs. In this sequel, we shall be using WLAN and 802.11b interchangeably.

The IEEE 802.11 standard calls for three different PHY specifications: frequency hopping (FH) spread spectrum, direct sequence (DS) spread spectrum, and infrared (IR). The transmit power for DS and FH devices is defined at a maximum of 1 W and the receiver sensitivity is set to −80 dBmW. Antenna gain is limited to 6 dB maximum. In this work, we focus on the 802.11b specification (DS spread spectrum) since it is in the same frequency band as Bluetooth and the most commonly deployed.

The basic data rate for the DS system is 1 Mbit/s encoded with differential binary phase shift keying (DBPSK). Similarly, a 2 Mbit/s rate is provided using differential quadrature phase shift keying (DQPSK) at the same chip rate of 11×10^6 chips/s. Higher rates of 5.5 and 11 Mbit/s are also available using techniques combining quadrature phase shift keying and complementary code keying (CCK); all of these systems use 22 MHz channels.

The IEEE 802.11 MAC layer specifications, common to all PHYs and data rates, coordinate the communication between stations and control the behavior of users who want to access the network. The Distributed Coordination Function (DCF), which describes the default MAC protocol operation, is based on a scheme known as carrier-sense, multiple access, collision avoidance (CSMA/CA). Both the MAC and PHY layers cooperate in order to implement collision avoidance procedures. The PHY layer samples the received energy over the medium transmitting data and uses a clear channel assessment (CCA) algorithm to determine if the channel is clear. This is accomplished by measuring the RF energy at the antenna and determining the strength of the received signal commonly known as RSSI, or received signal strength indicator. In addition, carrier sense can be used to determine if the channel is available. This technique is more selective since it verifies that the signal is the same carrier type as 802.11 transmitters. In all of our simulations, we use carrier sense and not RSSI to determine if the channel is busy. Thus, a Bluetooth signal will corrupt WLAN packets, but it will not cause the WLAN to defer transmission.

A virtual carrier sense mechanism is also provided at the MAC layer. It uses the request-to-send (RTS) and clear-to-send (CTS) message exchange to make predictions of future traffic on the medium and updates the network allocation vector (NAV) available in stations. Communication is established when one of the wireless nodes sends a short RTS frame. The receiving station issues a CTS frame that echoes the sender's address. If the CTS frame is not received, it is assumed that a collision occurred and the RTS process starts over. Regardless of whether the virtual carrier sense routine is used or not, the MAC is required to implement a basic access procedure (depicted in figure 2) as follows. If a station has data to send, it waits for the channel to be idle through the use of the CSMA/CA algorithm. If the medium is sensed idle for a period greater than a DCF interframe space (DIFS), the station goes into a backoff procedure before it sends its frame. Upon the successful reception of a frame, the destination station returns an ACK frame after a Short interframe space (SIFS). The backoff window is based on a random value uniformly distributed in the interval $[\mathrm{CW}_{\min}, \mathrm{CW}_{\max}]$, where $\mathrm{CW}_{\min}$ and $\mathrm{CW}_{\max}$ represent the Contention Window parameters. If the medium is determined busy at any time during the backoff slot, the backoff procedure is suspended. It is resumed after the medium has been idle for the duration of the DIFS period. If an ACK is not received within an ACK timeout interval, the station assumes that either the data frame or the ACK was lost and needs to retransmit its data frame by repeating the basic access procedure.

Errors are detected by checking the Frame Check Sequence (FCS) that is appended to the packet payload. In case an error is found, the packet is dropped and is then later retransmitted.

3. Integrated simulation model

In this section, we describe the methodology and platform used to conduct the performance evaluation. The simulation environment consists of detailed models for the RF channel, the PHY, and MAC layers developed in C and OPNET (for the MAC layer). These detailed simulation models constitute an evaluation framework that is critical to studying the various intricate effects between the MAC and PHY layers. Although interference is typically associated with the RF channel modeling and measured at the PHY layer, it can significantly impact the performance of higher layer applications including the MAC layer. Similarly, changes in the behavior of the MAC layer protocol and the associated data traffic distribution can play an important factor in the interference scenario and affect the overall system performance.

Figure 3 shows a packet being potentially corrupted by two interference packets. Consider that the desired packet is from the WLAN and the interference packets are Bluetooth (the figure is equally valid if the roles are reversed, except that the frequencies of the packets will be different). For interference to occur, the packets must overlap in both time and frequency. That is, the interference packets must be within the 22 MHz bandwidth of the WLAN. In a system with many Bluetooth piconets, there may be interference from more than one packet at any given time. We define a period of stationarity (POS) as the time during which the interference is constant. For example, $t_i \leqslant t \leqslant t_{i+1}$ is such a period, as is $t_{i+1} \leqslant t \leqslant t_{i+2}$.

Even during a POS where there is one or more interferers, the number and location of bit errors in the desired packet depends on a number of factors: (1) the signal-to-interference ratio (SIR) and the signal-to-noise ratio at the receiver, (2) the type of modulation used by the transmitter and the interferer, and (3) the channel model. For this reason, it is essential to use accurate models of the PHY and channel, as described below. Just because two packets overlap in time and frequency does not necessary lead to bit errors and the consequent packet loss. While one can use (semi-)analytic models instead, such as approximating Bluetooth interference on WLAN as a narrowband tone jammer, the use of detailed signal processing-based models better allows one to handle multiple simultaneous interferers.

In order to simulate the overall system, an interface module was created that allows the MAC models to use the physical layer and channel models. This interface module captures all changes in the channel state (mainly in the energy level). Consider the Bluetooth transmitter–channel–receiver chain of processes. For a given packet, the transmitter creates a set of signal samples that are corrupted by the channel and input to the receiver; interference may be present for all or only specific periods of stationarity, as shown in figure 3. A similar chain of processing occurs for an 802.11b packet. The interface module is designed to process a packet at a time.

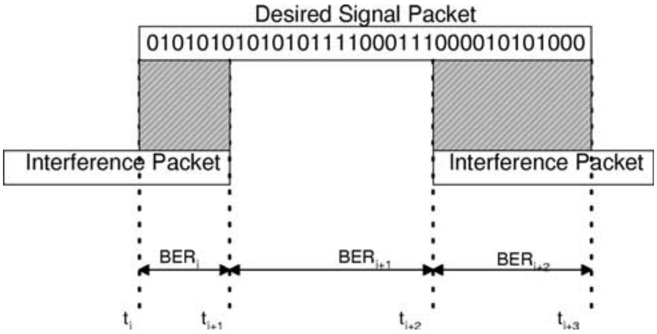


Figure 3. Packet collision and placement of errors. The bit error rate (BER) is roughly constant during each of the three indicated periods.

At the end of each packet transmission, the MAC layer generates a data structure that contains all the information required to process the packet. This structure includes a list of all the interfering packets with their respective duration, timing offset, frequency, and transmitted power. The topology of the scenario is also included. The data structure is then passed to the physical layer along with a stream of bits representing the packet being transmitted. The physical layer returns the bit stream after placing the errors resulting from the interference.

3.1. MAC model

We used OPNET to develop a simulation model for the Bluetooth and IEEE 802.11 protocols. For Bluetooth, we implemented the access protocol according to the specifications [2]. We assume that a connection is already established between the master and the slave and that the synchronization process is complete. The Bluetooth hopping pattern algorithm is implemented. Details of the algorithm are provided in section 2.1. A pseudo-random number generator is used instead of the implementation specific circuitry that uses the master's clock and 48-bit address to derive a random number.

For the IEEE 802.11 protocol, we used the model available in the OPNET library and modified it to bypass the OPNET radio model and to use our MAC/PHY interface module. We focus in this study on the Direct Sequence mode which uses a fixed frequency that occupies 22 MHz of the frequency band. The center frequency is set to 2.437 GHz.

At the MAC layer, a set of performance metrics are defined including probability of packet loss. Packet loss measures the number of packets discarded at the MAC layer due to errors in the bit stream. This measure is calculated after performing error correction.

3.2. PHY model

The transmitters, channel, and receivers are implemented at complex baseband. For a given transmitter, inphase and quadrature samples are generated at a sampling rate of $44 \cdot 10^6$ per second. This rate provides four samples/symbol for the 11 Mbit/s 802.11 mode, enough to implement a good receiver. It is also high enough to allow digital modulation of the Bluetooth signal to account for its frequency hopping. Specifically, since the Bluetooth signal is approximately 1 MHz wide, it can be modulated up to almost 22 MHz, which is more than enough to cover the 11 MHz bandwidth (one-sided) of the 802.11 signal. The received complex samples from both the desired transmitter and the interferer(s) are added together at the receiver.

While there are a number of possible Bluetooth receiver designs, we chose to implement the noncoherent limiter-discriminator (LD) receiver [3,14]. Its simplicity and relatively low cost should make it the most common type for many consumer applications. Details of the actual design are given in [15].

In the 802.11b CCK receiver, each group of eight information bits chooses a sequence of eight consecutive chips that forms a symbol. As before, the inphase and quadrature components of these chips are transmitted. The receiver looks at the received symbol and decides which was the most likely transmitted one. While one can implement this decoding procedure by correlating against all 256 possible symbols, we chose a slightly sub-optimal, but considerably faster architecture similar to the Walsh–Hadamard transform; again details can be found in [15].

3.3. Channel model

The channel model consists of a geometry-based propagation model for the signals, as well as a noise model. For the indoor channel, we apply a propagation model consisting of two parts: (1) line-of-sight propagation (free-space) for the first 8 m, and (2) a propagation exponent of 3.3 for distances over 8 m. Consequently, the path loss in dB is given by

$$L_\mathrm{p} = \begin{cases} 32.45 + 20\log(f \cdot d) & \text{if } d < 8 \text{ m}, \\ 58.3 + 33\log\left(\dfrac{d}{8}\right) & \text{otherwise}, \end{cases} \tag{1}$$

where f is the frequency in GHz, and d is the distance in meters. This model is similar to the one used by Kamerman [10]. Assuming unit gain for the transmitter and receiver antennas and ignoring additional losses, the received power in dBmW is

$$P_\mathrm{R} = P_\mathrm{T} - L_\mathrm{p}, \tag{2}$$

where P_T is the transmitted power also in dBmW. Equation (2) is used for calculating the power received at a given point due to either a Bluetooth or an 802.11 transmitter, since this equation does not depend on the modulation method.

The main parameter that drives the PHY layer performance is the signal-to-interference ratio between the desired signal and the interfering signal. This ratio is given in dB by

$$\mathrm{SIR} = P_\mathrm{R} - P_\mathrm{I}, \tag{3}$$

where P_I is the interference power at the receiver. In the absence of interference, the bit error rate for either the Bluetooth or WLAN system is almost negligible for the transmitter powers and ranges under consideration.

To complete the channel model, noise is added to the received samples, according to the specified SNR. In decibels, the signal-to-noise ratio is defined by $\mathrm{SNR} = P_\mathrm{R} - S_\mathrm{R}$, where P_R is the received signal power, and S_R is the receiver's sensitivity in dBmW; this latter value is dependent on the receiver model and so is an input parameter. Additive white Gaussian noise (AWGN) is used to model the noise at the receivers.

3.4. Model validation

The results obtained from the simulation models were validated against experimental and analytical results.

Since the implementation of the PHY layer required choosing a number of design parameters, the first step in the validation process is comparing the PHY results against theoretical results. Complete BER curves of the Bluetooth and 802.11b systems are given in [15]; for the AWGN and flat Rician channels without interference, all the results match very closely to analytical bounds and other simulation results. Also, the simulation results for both the MAC and PHY models were compared and validated against analytical results for packet loss given different traffic scenarios [6].

For the experimental testing, we use the topology in figure 4 and compare the packet loss observed for Bluetooth voice and WLAN data with the simulation results in figure 5. The experimental and simulation results are in good agreement.

4. Simulation results

We present simulation results to evaluate the performance of Bluetooth in the presence of WLAN interference and vice versa. First, we consider the effects of parameters such as transmitted power, offered load, hop rate, and traffic type on interference. Second, we look at two realistic interference scenarios to quantify the severity of the performance degradation for the Bluetooth and WLAN systems.

4.1. Factors effecting interference

We first consider a four node topology consisting of two WLAN devices and two Bluetooth devices (one master and one slave) as shown in figure 4. The WLAN access point (AP) is located at (0, 15) m, and the WLAN mobile is fixed at (0, 1) m. The Bluetooth slave device is fixed at (0, 0) m and the master is fixed at (1, 0) m.

In an effort to control the interference on Bluetooth and WLAN, we define two scenarios. In the first scenario, we let the mobile be the generator of 802.11 data, while the AP is the sink. In this case, the interference is from the mobile sending data packets to the AP and receiving acknowledgments (ACKs) from it. Since most of the WLAN traffic is

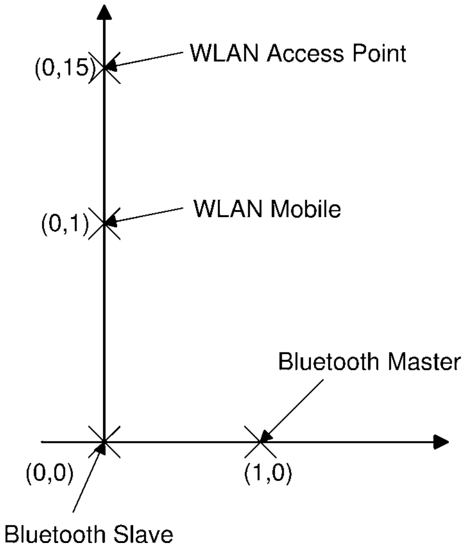


Figure 4. Topology 1. Two WLAN devices and one Bluetooth piconet.

Table 2
Summary of the scenarios.

Scenario	Desired signal	Interferer signal	WLAN AP	WLAN mobile
1	Bluetooth	WLAN	Sink	Source
2	WLAN	Bluetooth	Source	Sink

originating close to the Bluetooth piconet, both the master and the slave may suffer from serious interference. In the second scenario, the traffic is generated at the AP and received at the WLAN mobile. Because the data packets are generally longer then the ACKs, this is a more critical scenario for the WLAN then when the mobile is the source. Table 2 summarizes the two scenarios.

For Bluetooth, we consider two types of applications, voice and data. For voice, we assume a symmetric stream of 64 Kbit/s each way using HV1 packet encapsulation. For data traffic, we consider a source that generates DM5 packets. The packet interarrival time is exponentially distributed, and its mean in seconds is computed according to

$$t_{\mathrm{B}} = 2 \times n_{\mathrm{s}} \times \frac{T_{\mathrm{s}}}{\lambda}, \tag{4}$$

where λ is the offered load; n_{s} is the number of slots occupied by a packet. For DM5, $n_{\mathrm{s}} = 5$. T_{s} is the slot size equal to 625 μs.

For WLAN, we use the 11 Mbit/s mode and consider a data application. Typical applications for WLAN could be ftp or http. However, since we are mainly interested in the MAC layer performance, we abstract the parameters for the application model to packet size and offered load and do not model the entire TCP/IP stack. We fix the packet payload to 12,000 bits which is the maximum size for the MAC payload data unit, and vary λ. The packet interarrival time in seconds, t_{W}, is exponentially distributed, and its mean is computed according to

$$t_{\mathrm{W}} = \frac{192/1{,}000{,}000 + 12{,}224/11{,}000{,}000}{\lambda}, \tag{5}$$

where the 192-bit PLCP header is sent at 1 Mbit/s and the payload at 11 Mbit/s. Unless specified otherwise, we use the configuration and system parameters shown in table 3.

Table 3
Simulation parameters

Simulation parameters	Values
Propagation delay	5 μs/km
Length of simulation run	30 s
Bluetooth parameters	
ACL Baseband Packet Encapsulation	DM5
SCO Baseband Packet Encapsulation	HV1
Transmitted Power	1 mW
WLAN parameters	
Transmitted power	25 mW
Packet header	224 bits
Packet payload	12,000 bits

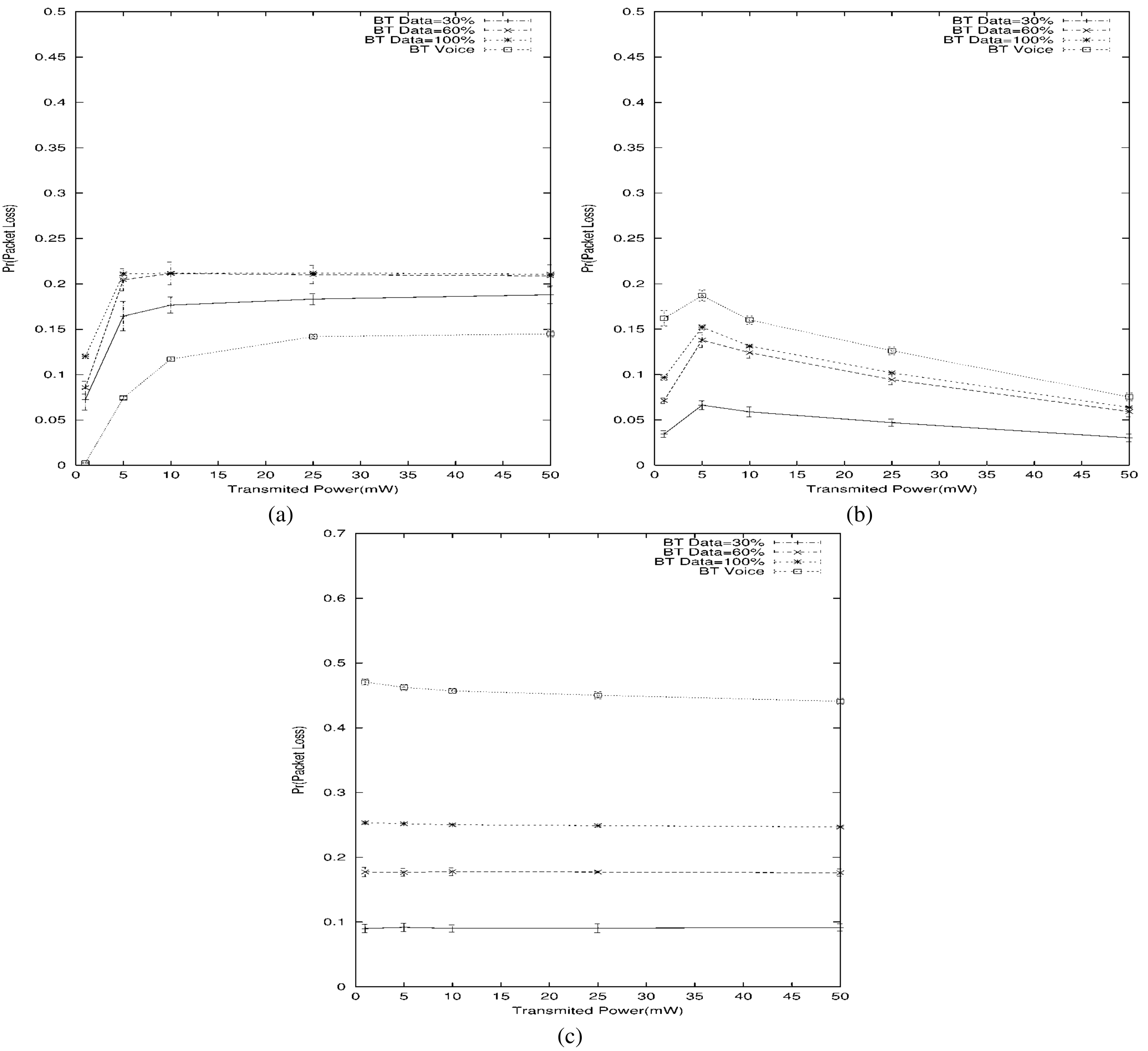
For scenarios 1 and 2, we run 15 trials using a different random seed for each trial. In addition to plotting the mean value, confidence intervals, showing plus and minus two standard deviations, are also included. From figures 5 and 6, one sees that the statistical variation around the mean values are very small. In addition to the comparisons with analytical and experimental results described in section 3.4, this fact provides further validation for the results.

4.1.1. WLAN transmission power

First, we look at the effect on Bluetooth of increasing the WLAN transmission power in scenario 1; that is, increasing the interferer transmission power on the victim signal. Since power control algorithms exist in many WLAN implementations, it is important to consider how varying the transmitted power changes the interference. However, since Bluetooth was designed as a low power device, we fix its transmitter power at 1 mW for all simulations.

We fix WLAN λ to 60% for different Bluetooth traffic types and values of λ. In figure 5(a), we note a saturation effect around 10 mW. A threshold, which is close to 22/79, corresponds to the probability that Bluetooth is hopping in the WLAN occupied band. Thus, increasing the WLAN transmission power beyond 10 mW does not affect the Bluetooth packet loss. Between 1 and 5 mW, a small change in the WLAN transmitted power triples the Bluetooth packet loss. Please note the relative positions of the packet loss curves for different values of λ between 1 and 5 mW; as λ increases, the packet loss is higher. Also, note that Bluetooth voice has the lowest packet loss, partly due to its short packet size. A second reason for the low loss probability is that voice packets are rejected only if there are errors in the access code or packet headers, cf. table 1. A packet may be accepted with a relatively large number of bit errors in the payload, which may lead to a substantial reduction in subjective voice quality.

Figure 5(b) shows the probability of packet loss for the WLAN mobile device. This corresponds to ACKs being



(a)

(b)

(c)

Figure 5. WLAN $\lambda = 60\%$. (a) Scenario 1. Probability of packet loss for the Bluetooth slave. (b) Scenario 1. Probability of packet loss for the WLAN mobile. (c) Scenario 2. Probability of packet loss for the WLAN mobile.

dropped at the WLAN source. The general trend is that the packet loss decreases as the WLAN transmitted power increases. However, we notice a slight "bump" between 1 and 5 mW. This is due to the effect of closed-loop interference. The WLAN source increases its transmitted power and causes more interference on the Bluetooth devices; as a result, there are more retransmissions in both the Bluetooth and WLAN piconets, which causes more lost ACKs at the WLAN source.

Next, we consider the effect of increasing the WLAN transmission power on the WLAN performance in scenario 2. From figure 5(c), we observe that even if the WLAN transmission power is fifty times more than the Bluetooth transmission power (fixed at 1 mW), the packet loss for the WLAN does not change. This leads us to an interesting observation on power control. Basically, we note that increasing the transmission power does not necessarily improve the performance. However, decreasing the transmission power is usually a "good neighbor" strategy that may help reduce the interference on other devices.

4.1.2. Offered load

The offered load, also referred to in some cases as duty cycle, is an interesting parameter to track. Consider scenario 1 where Bluetooth is the interferer and fix the WLAN transmission power to 25 mW. We observe that for the WLAN, the packet loss is proportional to the Bluetooth offered load as shown in figure 6. For λ equal 20%, 50%, and 100%, the packet loss is 7%, 15%, and 25%, respectively. This observation has been confirmed analytically in [6], where the packet error is shown to depend not only on the offered load of the interferer system but also on the packet sizes of both systems. Also note that the probability of loss for the 30% WLAN of-

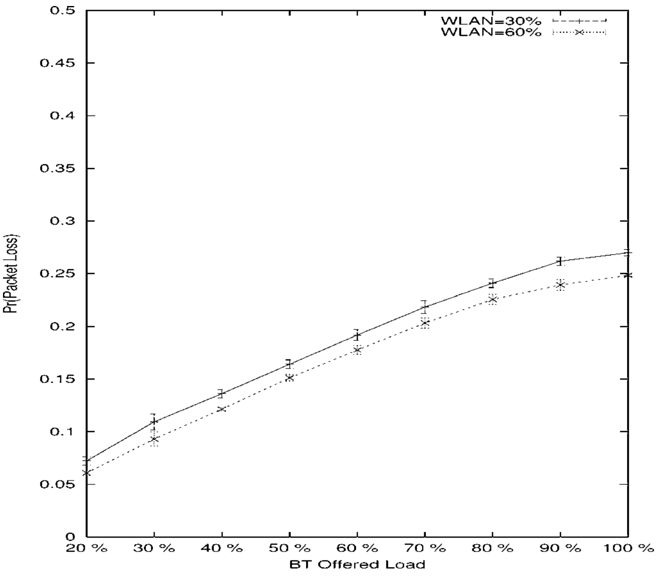


Figure 6. Scenario 2. Probability of packet loss for the WLAN mobile.

fered load is slightly higher than for the 60% WLAN offered load. However, this difference is statistically insignificant.

The significance of the packet size is apparent in figures 5(a) and (c), where short Bluetooth voice packets lead to less packet loss for Bluetooth but cause more interference for WLAN. However, for the WLAN 11 Mbit/s rate, the effect of changing the WLAN packet size over the range 1,000 to 12,000 bits has very little effect on the performance of both the WLAN and Bluetooth, and that is due to the relatively short transmission time of the WLAN packet. At the 1 Mbit/s rate, WLAN packets of the same bit lengths take considerably longer to transmit, and the effect of packet size is somewhat more pronounced. For a further discussion of the 1 Mbit/s case, please see [7].

4.1.3. Bluetooth hop rate

In order to highlight the effect of the Bluetooth hop rate on WLAN, we use different packet types, DM1, DM3, and DM5; these packets occupy 1, 3, and 5 time slots, respectively. The Bluetooth hop rate is determined by the number of time slots occupied by a packet. Thus, the hop rate is 1600, 533, and 320 hops/s for DM1, DM3, and DM5 packets, respectively. The offered load for Bluetooth is set to 100%. The results in table 4 clearly indicate that a faster hop rate leads to higher packet losses (44%, 28%, and 26% for DM1, DM3 and DM5, respectively). Note that the results are rather insensitive to the WLAN offered load.

4.1.4. Bluetooth traffic type

The question here is, whether Bluetooth voice effects WLAN more than Bluetooth data, and vice versa. We use three types of packets for voice encapsulation, namely, HV1, HV2, and HV3. HV1 represents the worst case of interference for WLAN as shown in table 5 with 44% packet loss. HV2 and HV3, which contain less error correction and more user information, are sent less often and, therefore, interfer less with WLAN (25% and 16% for HV2 and HV3, respectively). The WLAN packet loss with Bluetooth data interference is 19%. Please note that the results do not depend on the WLAN offered load.

Table 4
Scenario 2. Probability of WLAN packet loss versus Bluetooth hop rate.

BT	WLAN $\lambda = 30\%$	WLAN $\lambda = 60\%$
DM1	0.449	0.449
DM3	0.286	0.277
DM5	0.269	0.248

Table 5
Scenario 2. Probability of WLAN packet loss versus Bluetooth traffic type.

BT		WLAN $\lambda = 30\%$	WLAN $\lambda = 60\%$
Voice	HV1	0.446	0.470
	HV2	0.253	0.257
	HV3	0.166	0.169
Data, $\lambda = 60\%$		0.191	0.177

Table 6
Scenario 1. Probability of Bluetooth packet loss versus Bluetooth traffic type.

BT		WLAN $\lambda = 30\%$	WLAN $\lambda = 60\%$
Voice	HV1	0.077	0.141
	HV2	0.075	0.149
	HV3	0.069	0.136
Data, $\lambda = 60\%$		0.2089	0.210

On the other hand, the probability of packet loss for Bluetooth data (20%) is higher than for Bluetooth voice (7%) as shown in table 6. Note that doubling the WLAN offered load to 60% doubles the Bluetooth voice packet loss. Also, since all three types of voice packets suffer the same packet loss, it is preferable to use HV3, which causes less interference on the WLAN. The error correction coding in HV1 and HV2 packets may provide greater range in a noise-limited environment, but this coding is far too weak to protect the packets from interference. Instead, it is the frequency hopping ability of Bluetooth that limits the damage done by the WLAN.

4.1.5. Bluetooth transmission power

While most Bluetooth devices will be operating at 1 mW, the specification also allows higher transmitter powers. Table 7 shows the probability of packet loss for both Bluetooth and the WLAN for three values of the BT transmitter power and two types of Bluetooth traffic. As expected, higher transmitter powers lead to more lost WLAN packets, regardless of the BT traffic type. Increasing the power from 1 to 10 mW leads to approximately a 50% increase in WLAN loss. Conversely, the Bluetooth packet error rate decreases. It still not clear how beneficial this decrease is for Bluetooth; even a loss probability of 0.0335 may lead to unacceptable voice quality.

4.1.6. Bluetooth packet error correction

So far, the results shown for the Bluetooth data are with DM5 packets, which use a 2/3 block code on the packet payload. In order to show the effect of error correction on the probabil-

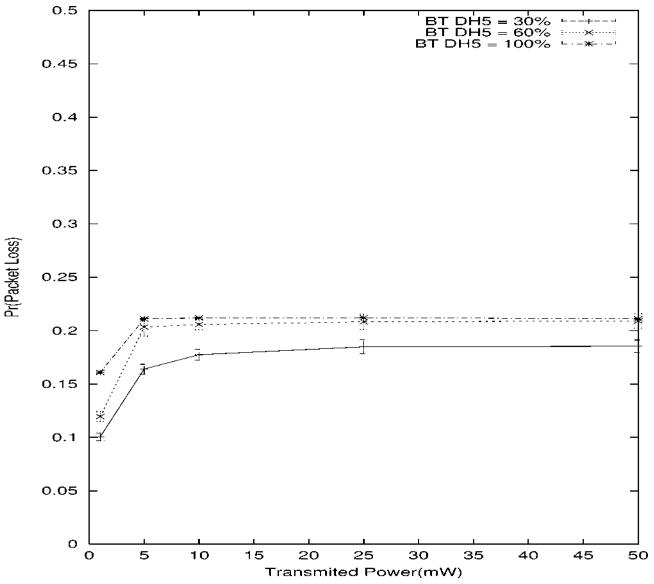


Figure 7. Scenario 1. Probability of packet loss for the Bluetooth slave.

Table 7
Scenario 2. Probability of packet loss versus Bluetooth transmission power (mW). WLAN $\lambda = 60\%$.

BT traffic	BT power (mW)	BT loss probability	WLAN loss probability
$\lambda = 60\%$	1	0.2125	0.0961
	2.5	0.2085	0.1227
	10	0.1733	0.1358
Voice	1	0.1417	0.1253
	2.5	0.1179	0.1609
	10	0.0335	0.1977

ity of packet loss, we repeat scenario 1 and compare the results given in figures 5(a) and 7, obtained with DM5 and DH5 packets, respectively. As expected, the probability of packet loss for DM5 packets (figure 5(a)) is slightly less than for DH5 packets (figure 7) for WLAN transmission powers less than 5 mW. Thus, for low levels of interference, a 2/3 block code can reduce the probability of loss by 4%. However, for WLAN transmission powers above 5 mW, the probability of packet loss is the same for both DM5 and DH5 packets.

4.2. *Realistic interference topologies*

In this section, we consider two practical interference topologies. While they appear to be somewhat different, they actually complement each other. The first one has the WLAN device, in the midst of the Bluetooth piconets, acting at the source, while the second one has the WLAN access point acting as the source.

4.2.1. *Topology 2*

We first look at the topology illustrated in figure 8. It consists of one WLAN AP located at (0, 15) m, and one WLAN mobile at (0, 0) m. The WLAN traffic is generated at the mobile, while the AP returns acknowledgments. The distance between the WLAN AP and mobile is $d_{\mathrm{W}} = 15$ m. There are ten Bluetooth piconets randomly placed, covering a disk. The center of the disk is located at $(0, 0)$ and its radius is $r = 10$ m. We define d_{B} as the distance between a Bluetooth master and slave pair. $d_{\mathrm{B}} = 1$ m for half of the master and slave pairs, while $d_{\mathrm{B}} = 2$ m for the other half of the master and slave pairs.

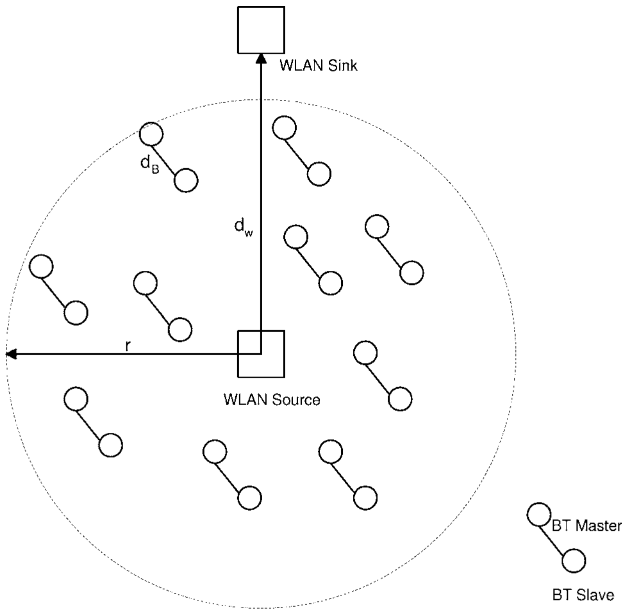


Figure 8. Topology 2. Two WLAN devices and ten Bluetooth piconets.

Table 8
Experiment 3 results.

BT traffic	WLAN λ	BT loss		WLAN loss
		$d_{\mathrm{B}} = 1$ m	$d_{\mathrm{B}} = 2$ m	
$\lambda = 30\%$	30%	0.056	0.157	0.121
	60%	0.060	0.188	0.170
$\lambda = 60\%$	30%	0.057	0.243	0.405
	60%	0.061	0.247	0.381
Voice	30%	0.009	0.104	1
	60%	0.008	0.106	1

In this case, the main interference on Bluetooth is caused by the WLAN source located in the center of the disk; the aggregation of the ten piconets affects the WLAN source. We found that when the WLAN system is not operating, the Bluetooth packet loss is negligible (less than 1%). Table 8 gives the packet loss for the Bluetooth and WLAN devices. The packet loss for the Bluetooth devices is averaged over the master and slave devices and split into two groups: piconets with $d_{\mathrm{B}} = 1$ m and piconets with $d_{\mathrm{B}} = 2$ m. For WLAN, the packet loss is measured at the source. It is effectively zero at the sink.

We observe that the WLAN packet loss depends on the Bluetooth traffic load value, λ. As λ is varied from 30% to 60%, the WLAN packet loss is significantly changed from 12% to 40%. However, the WLAN packet loss is insensitive to the WLAN offered load. Consistent with previous results, Bluetooth voice represents the worst case interference scenario for WLAN.

In general, the Bluetooth packet loss for $d_{\mathrm{B}} = 1$ m is less than for $d_{\mathrm{B}} = 2$ m. The reason is that when the Bluetooth signal is stronger (over a shorter distance), the impact of interference is less significant.

4.2.2. Topology 3

We next consider the topology given in figure 9. It includes one WLAN AP and four WLAN mobile devices. The WLAN AP is located at (0, 15) m, and it is the source of the traffic generation. The four WLAN mobile devices are placed on a two-dimensional grid at $(-1, 1)$, $(1, 1)$, $(-1, -1)$, and $(1, -1)$ m. In this topology, there are four Bluetooth piconets, each consisting of a master–slave device pair. The placement of the Bluetooth devices is as shown in the figure.

In this case, we are looking at the effect of Bluetooth piconets on the four WLAN sink devices. The packet loss measure for WLAN is averaged over the four devices. As shown in table 9, the impact of WLAN interference on Bluetooth is minimal, given that the WLAN source is far from the Bluetooth piconets. As expected, the WLAN packet loss depends on the Bluetooth traffic conditions, and it is rather insensitive to the WLAN traffic activity. With Bluetooth voice, the WLAN packet loss is close to 84%. It is 57% for Bluetooth data with WLAN loads of $\lambda = 30, 60\%$.

5. Concluding remarks

We presented results on the performance of Bluetooth and WLAN operating in the 2.4 GHz ISM band based on detailed channel, MAC, and PHY layer models for both systems. The evaluation framework used allows us to study the impact of interference in a closed loop environment where two systems are affecting each other, and explore the MAC and PHY layer interactions in each system.

We are able to draw some useful conclusions based on our results. First, we note that power control may have limited benefits in this environment. Increasing the WLAN transmission power to even fifty times the power of Bluetooth is not sufficient to reduce the WLAN packet loss. On the other hand, limiting the WLAN power, may help avoid interference to Bluetooth. Second, using a slower hop rate for Bluetooth (i.e. longer packet sizes) may cause less interference to WLAN. Third, Bluetooth voice represents the worst type of interference for WLAN. In addition, the WLAN performance seems to degrade as the Bluetooth offered load is increased. Finally, the use of error correcting block codes in the Bluetooth payload does not improve performance. The errors caused by interference are often too many to correct.

Overall, the results are dependent on the traffic distribution. Yet, there may be little room for parameter optimization especially for the practical scenarios. Not only does the complexity of the interactions and the number of parameters to adjust make the optimization problem intractable, but choosing an objective function is very dependent on the applications and the scenario. Thus, achieving acceptable performance for a particular system comes at the expense of the other system's throughput. Therefore, we believe that the primary solutions to this problem lie in the development of coexistence mechanisms.

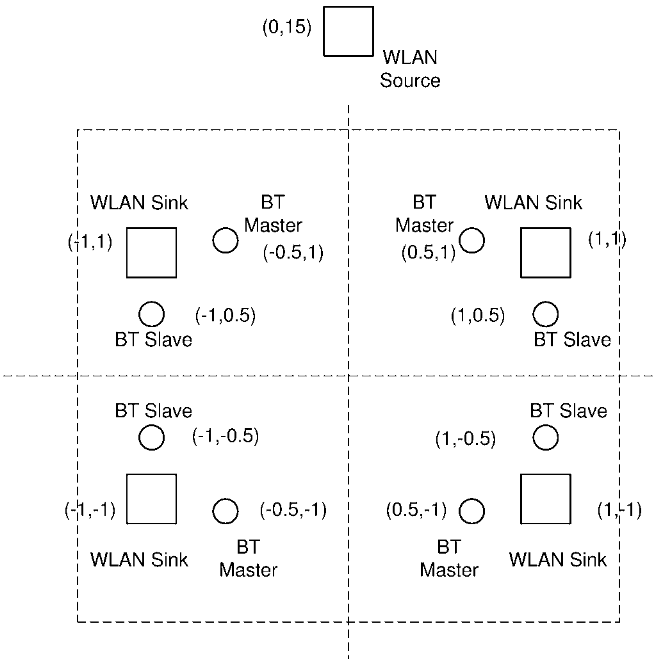


Figure 9. Topology 3. Five WLAN devices and four Bluetooth piconets.

Table 9
Experiment 4 results.

BT traffic	WLAN λ	BT loss	WLAN loss
$\lambda = 30\%$	30%	0.007	0.574
	60%	0.006	0.580
$\lambda = 60\%$	30%	0.007	0.576
	60%	0.006	0.580
Voice	30%	0.002	0.836
	60%	0.001	0.828

References

[1] BlueHoc: Bluetooth Performance Evaluation Tool, Open-Source (2001) `http://oss.software.ibm.com/developerworks/opensource/~bluehoc`

[2] Bluetooth Special Interest Group, Specifications of the Bluetooth system, Vol. 1, v.1.0B Core, and Vol. 2, v1.0B Profiles (December 1999).

[3] T. Ekvetchavit and Z. Zvonar, Performance of phase-locked loop receiver in digital FM systems, in: *Ninth IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*, Vol. 1 (1998) pp. 381–385.

[4] G. Ennis, Impact of Bluetooth on 802.11 direct sequence, IEEE P802.11 Working Group Contribution, IEEE P802.11-98/319 (September 1998).

[5] D. Fumolari, Link performance of an embedded Bluetooth personal area network, in: *Proceedings of IEEE ICC'01,* Helsinki, Finland (June 2001).

[6] N. Golmie and F. Mouveaux, Interference in the 2.4 GHz ISM band: Impact on the Bluetooth access control performance, in: *Proceedings of IEEE ICC'01*, Helsinki, Finland (June 2001).

[7] N. Golmie, R.E. Van Dyck, and A. Soltanian, Interference of Bluetooth and IEEE 802.11: Simulation modeling and performance evaluation, in: *Proceedings of the Fourth ACM International Workshop on Modeling, Analysis, and Simulation of Wireless and Mobile Systems, MSWIM'01*, Rome, Italy (July 2001).

[8] I. Howitt, V. Mitter and J. Gutierrez, Empirical study for IEEE 802.11 and Bluetooth interoperability, in: *Proceedings of IEEE Vehicular Technology Conference (VTC)* (Spring 2001).

[9] IEEE Standard 802-11, IEEE standard for wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specification (June 1997).

[10] A. Kamerman, Coexistence between Bluetooth and IEEE 802.11 CCK: Solutions to avoid mutual interference, IEEE P802.11 Working Group Contribution, IEEE P802.11-00/162r0 (July 2000).

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

[12] J. Lansford, A. Stephens and R. Nevo, Wi-Fi (802.11b) and Bluetooth: Enabling coexistence, IEEE Network Magazine (September/October 2001).

[13] S. Shellhammer, Packet error rate of an IEEE 802.11 WLAN in the presence of Bluetooth, IEEE P802.15 Working Group Contribution, IEEE P802.15-00/133r0 (May 2000).

[14] M.K. Simon and C.C. Wang, Differential versus limiter-discriminator detection of narrow-band FM, IEEE Transactions on Communications COM-31(11) (November 1983) 1227–1234.

[15] A. Soltanian and R.E. Van Dyck, Physical layer performance for coexistence of Bluetooth and IEEE 802.11b, in: *Virginia Tech. Symposium on Wireless Personal Communications* (June 2001).

[16] M. Takai, R. Bagrodia, A. Lee and M. Gerla, Impact of channel models on simulation of large scale wireless networks, in: *Proceedings of ACM/IEEE MSWIM'99*, Seattle, WA (August 1999).

[17] S. Unawong, S. Miyamoto and N. Morinaga, Techniques to improve the performance of wireless LAN under ISM interference environments, in: *Fifth Asia-Pacific Conference on Communications, 1999 and Fourth Optoelectronics and Communications Conference*, Vol. 1 (1999) pp. 802–805.

[18] J. Zyren, Reliability of IEEE 802.11 WLANs in presence of Bluetooth radios, IEEE P802.11 Working Group Contribution, IEEE P802.15-99/073r0 (September 1999).

[19] S. Zurbes, W. Stahl, K. Matheus and J. Haartsen, Radio network performance of Bluetooth, in: *Proceedings of IEEE International Conference on Communications, ICC 2000*, New Orleans, LA, Vol. 3 (June 2000) pp. 1563–1567.

Nada Golmie received the M.S.E degree in computer engineering from Syracuse University, Syracuse, NY, in 1993, and the Ph.D. degree in computer science from University of Maryland, College Park, MD, in 2002. Since 1993, she has been a research engineer at the advanced networking technologies division at the National Institute of Standards and Technology (NIST). Her research in traffic management and flow control led to several papers presented at professional conferences, journals and numerous contributions to international standard organizations and industry led consortia. Her current work is focused on the performance evaluation of protocols for Wireless Personal Area Networks. Her research interests include modeling and performance analysis of network protocols, media access control, and Quality of Service for IP and wireless network technologies. She is the vice-chair of the IEEE 802.15 Coexistence Task Group.

E-mail: nada.golmie@nist.gov

Robert E. Van Dyck received the B.E and M.E.E degrees from Stevens Institute of Technology, Hoboken, NJ, in 1985 and 1986, respectively, and the Ph.D. degree in electrical engineering from the North Carolina State University at Raleigh in 1992. Since June 2000, he has been a member of the Advanced Network Technologies Division of the National Institute of Standards and Technology, Gaithersburg, MD. Prior to that, he was an Assistant Professor in the Department of Electrical Engineering, the Pennsylvania State University, University Park, PA. During 1999, he was a Summer Faculty Research Fellow at Rome Laboratory. His other previous affiliations include GEC-Marconi Electronic Systems, Wayne, NJ (1995–1996), the Center for Computer Aids for Industrial Productivity, Rutgers University, Piscataway, NJ (1992–1995), the Computer Science Corporation, Research Triangle Park NC, (1989), and the Communications Laboratory, Raytheon Co., Marlborough, MA (1985–1988). His present research interests are in self-organization of sensor networks, multimedia communications and networking, and source and channel coding for wireless communications.

Amir Soltanian received his M.S. degree from Sharif University of Technology, Tehran, Iran, in 1994. He has been working in the industry for 6 years doing research on GSM receivers. Currently, he is a guest researcher at National Institute of Standards and Technology. His current research is the study of the interference cancellation methods for the physical layer of the Bluetooth and IEEE802.11 WLAN.

Arnaud Tonnerre is a graduate student at the École Nationale Supérieure des Telecommunications (ENST) in Bretagne, France. He is currently doing an internship at the National Institute of Standards and Technology (NIST) in Gaithersburg, MD. He will receive the Diplome d'Ingenieur in June 2003. His research interests are in wireless personal area networks.

Olivier Rébala received a computer science degree from the Institut supérieur d'informatique, de modélisation et de leurs applications (ISIMA) in Clermont-Ferrand, France, in September 2001. He is currently a Guest Researcher at the National Institute of Standards and Technology (NIST) in the advanced networking technologies division. His research interests includes the performance evaluation of wireless networking protocols.