

**IEEE P802.15**  
**Wireless Personal Area Networks**

---

Project	IEEE P802.15 Working Group for Wireless Personal Area Networks		
---------	--	--	--

---

Title	Impact of Interference on the Bluetooth Access Control Performance: Preliminary Results		
-------	---	--	--

---

Date	September 22, 2000		
------	--------------------	--	--

---

Source	Nada Golmie and Frederic Mouveaux NIST 100 Bureau Dr. Stop 8920 Gaithersburg MD, 20899	Voice:	(301) 975-4190
		FAX:	(301) 590-932
		E-Mail:	nada@nist.gov

---

Re	[]		
----	----	--	--

---

Abstract	[We attempt to quantify the performance of the Bluetooth access control layer when the radio is operating in close proximity to an IEEE 802.11 system or other Bluetooth piconets. We use a combined approach of probability analysis and simulation in order to capture the interference environment and give some preliminary performance results in terms of packet loss and access delay for voice and data traffic and different packet encapsulations.]		
----------	---	--	--

---

Purpose	[The main goal of this paper is to present our initial findings on the performance of Bluetooth in an interference environment based on a detailed simulation model of the Bluetooth access control layer.]		
---------	---	--	--

---

Notice	This document has been prepared to assist the IEEE P802.15. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein.		
--------	---	--	--

---

Release	The contributor acknowledges and accepts that this contribution becomes the property of IEEE and may be made publicly available by P802.15		
---------	--	--	--

---

## I. INTRODUCTION

The main goal of this paper is to present our initial findings on the performance of a Bluetooth access control system when its radio is operating in close proximity to an IEEE 802.11 system or other Bluetooth piconets. Related work that appeared in the literature have focused so far on either simulation [1] or probability analysis techniques [2][3] in order to derive packet error measures for Bluetooth or 802.11 radios operating in interference environments. We use a combined approach of probability analysis and simulation in order to capture the interference environment and evaluate the performance of the Bluetooth access layer consisting of the baseband and L2CAP protocols used above the RF channel. Our results are based on a detailed simulation model of the Bluetooth access control layer. Our goal is to give additional insights on the impact of interference on higher layer protocols, namely the effect of using different packet encapsulations, error correction algorithms, and retransmissions on the Bluetooth access delay, packet loss, and the number of errors contained in a voice packet.

This paper is organized as follows. In section II, we present our interference analysis and the probability that a packet containing error is received at the Bluetooth node. In section III, we evaluate the impact of WLAN interference on the Bluetooth performance and present simulation results. Concluding remarks are offered in section IV.

## II. INTERFERENCE ANALYSIS

Interference in the 2.4 GHz band is receiving more attention lately. Zurbes et. al. present simulation results of the Bluetooth radio performance and the impact of 100 co-located sessions [1]. Kamerman reports on tolerable interference levels between Bluetooth and 802.11 devices for various scenarios and device positions [4]. His analysis is based on a simple path loss model and Signal to Interference (SIR) requirements for Bluetooth and 802.11 receivers. Furthermore, the probability of an 802.11 packet error in the presence of a Bluetooth piconet has been derived by Ennis [2], then extended by Zyren [5] and Shellhammer [3]. The formulation developed by Shellhammer allows for varying the offset of the packet overlap time.

In this paper we are mainly concerned with evaluating the Bluetooth performance in an interference environment. Therefore, we consider a Bluetooth receiver node as our reference and derive the probability that a packet containing errors (at least one error),  $P(PE)$ , is received at this node. The interfering signal is assumed to be other Bluetooth signals from adjacent piconets or WLANs.

A collision occurs when both the Bluetooth and the interfering packets overlap in time and frequency. This collision is detected at the Bluetooth receiver in the form of SIR that depends on the power transmitted, the distance traveled, and the path loss model used. The SIR then translates into a Bit Error Rate (BER) according to the GFSK carrier modulation and the Bluetooth receiver implementation used.

### A. Case I: WLAN Interference

Figure 1 illustrates the timing of the Bluetooth packets with respect to WLAN packets. Let  $f_B$  and  $f_W$  be the frequencies used to transmit the Bluetooth and WLAN packets respectively. We denote by  $T_B$  and  $T_W$ , the Bluetooth and the WLAN packet transmission periods respectively. In order to determine the position of the Bluetooth packet with respect to the WLAN packet when both systems use the same frequency ( $f_B = f_W$ ), we define two variables  $X_B$  and  $X_W$  that represent the interval from a time reference  $t_{reference}$  until the start of a Bluetooth packet and WLAN packet respectively. Let  $T_C$  represent the time interval when both WLAN and Bluetooth packets overlap. We denote by  $T_{WI}$  the interval between two WLAN packets including the packet transmission time  $T_W$  and a backoff period,  $T_{Backoff}$ .  $T_{Backoff}$  is the sum of several variables such as SIFS, DIFS, the ACK transmission time, and  $C_W$ . Similarly, we denote by  $T_{BI}$ , the interval between two Bluetooth packet transmissions. Due to the slotted structure of the Bluetooth

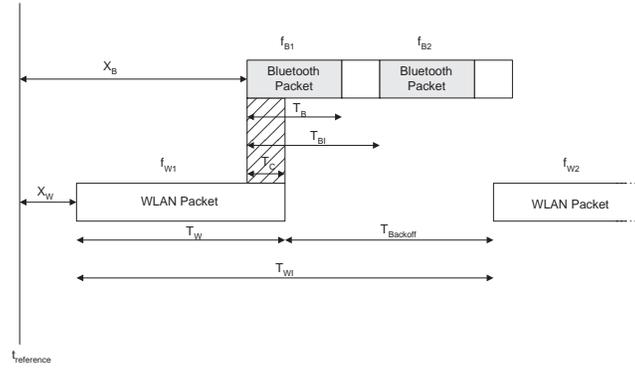


Fig. 1. Collisions at the Bluetooth Receiver Node

channel, a packet transmission occurs at the boundary of a Bluetooth time slot. We assume that  $X_B$  is a random variable that is uniformly distributed between zero and  $T_{BI}$ . Similarly, we assume that  $X_W$  is a random variable that is uniformly distributed between zero and  $T_{WI}$ .  $X_B$  and  $X_W$  are continuous random variables, however they are quantified to the resolution of a Bluetooth symbol period at the rate of a symbol (or a bit) per  $\mu s$  [3].

$$X_B \sim U(0, T_{BI}) \quad (1)$$

$$X_W \sim U(0, T_{WI}) \quad (2)$$

Thus, the probability that a Bluetooth packet overlaps in time and frequency with a WLAN packet depends on:

- The position of the WLAN packet with respect to the Bluetooth packet, i.e.  $X_B$ , and  $X_W$
- The transmission frequencies,  $f_B$  and  $f_W$  of the Bluetooth and WLAN systems respectively

The probability mass function of  $X_B$  is equal to  $p_{X_B}(k) = \frac{1}{T_{BI}}$  where  $k = 1, 2, \dots, T_{BI}$ . Similarly, the probability mass function of  $X_W$  is equal to  $p_{X_W}(l) = \frac{1}{T_{WI}}$  where  $l = 1, 2, \dots, T_{WI}$ . Both the Bluetooth and WLAN systems have a frequency hopping span of 79 channels. The probability that a WLAN system lands on the same frequency as a Bluetooth system depends on a discrete random variable  $f_W$  whose probability mass function is  $p_{f_W}(j) = \frac{n}{79}$  where  $j$  varies between 1 and 79 and  $n$  determines the number of overlapping channels. For FH  $n = 1$ , while for DS WLAN systems,  $n = 22$ .

Expressing  $P(PE)$  as a joint probability of frequency and packet overlap yields:

$$P(PE) = \sum_{k=0}^{T_{BI}} \sum_{l=0}^{T_{WI}} P(PE | X_B = k; X_W = l; f_W = j) \times p_{X_B}(k) p_{X_W}(l) p_{f_W}(j) \quad (3)$$

where  $P(PE | X_B = k; X_W = l; f_W = j)$  depends on  $T_C$  and BER. Thus, we write:

$$P(PE | X_B = k; X_W = l; f_W = j) = 1 - (1 - BER)^{T_C} \quad (4)$$

Therefore,

$$P(PE) = \left(\frac{n}{79}\right) \left(\frac{1}{T_{WI}}\right) \left(\frac{1}{T_{BI}}\right) \sum_{k=0}^{T_{BI}} \sum_{l=0}^{T_{WI}} (1 - (1 - BER)^{T_C}) \quad (5)$$

The value of  $T_C$  depends on  $X_B$ ,  $X_W$ ,  $T_W$ , and  $T_B$ . We distinguish five cases.

$$T_C = \begin{cases} \min(T_B, T_W) & \text{if } 0 = X_B - X_W \\ \min(T_B, \max(0, X_W + T_W - X_B)) & \text{if } T_B - T_W \leq 0 < X_B - X_W \\ \min(T_W, \max(0, X_B + T_B - X_W)) & \text{if } X_B - X_W < 0 < T_B - T_W \\ \max(0, X_B + T_B - X_W) & \text{if } X_B - X_W < 0 \leq T_W - T_B \\ \max(0, X_W + T_W - X_B) & \text{if } T_W - T_B < 0 < X_B - X_W \end{cases} \quad (8)$$

The assumptions that we make are summarized as follows:

- A Bluetooth packet does not collide with more than one WLAN packet. There is no loss of generality for FH systems, since two consecutive packets use different transmission frequencies. For DS systems, we base our assumption on the premise that  $T_{WI} > T_{BI}$ .
- The WLAN system is operating under maximum load conditions. That is, there is always a WLAN packet to be sent. In this case we do not consider the effect of Bluetooth interference on WLAN and how it may alter the WLAN traffic distribution.
- The WLAN CCA is limited to carrier sense functionality capable of detecting other WLAN devices of the same kind (either FH or DS) but cannot detect the presence of Bluetooth devices.
- A hop time for WLAN is equal to the packet transmission duration which represents a worst case scenario.

### B. Case II: Bluetooth Interference

In this case we consider  $n + 1$  piconets. Piconet  $piconet_0$ , contains the Bluetooth reference receiver where P(PE) is computed. As in Case I, P(PE) is given by the joint probability of frequency and packet time overlap, denoted by  $P_f$  and  $P_t$  respectively.  $P_f$  represents the probability that  $k$  out of  $n$  piconets will be sharing the same frequency as  $piconet_0$  and is given by:

$$P_f = \sum_{k=1}^n \binom{n}{k} \frac{1}{79^k} \left(1 - \frac{1}{79}\right)^{n-k} \quad (7)$$

Similarly, we let  $X_{Bi}$  represent the packet overlap offset of  $piconet_i$  with respect to  $piconet_0$  (without loss of generality we can set  $X_{B0} = t_{reference}$ ), where  $i$  varies between 1 and  $n$ . Using a similar argument as in Case I,  $X_{Bi}$  are continuous random variables that are quantified to the resolution of a Bluetooth symbol period at the rate of a symbol (or a bit) per  $\mu s$ .

$$X_{Bi} \sim U(-T_{BI}, T_{BI}) \quad (8)$$

Thus, the probability mass function of  $X_{Bi}$  is equal to  $p_{X_{Bi}}(l) = \frac{1}{2T_{BI}}$  where  $l = 1, 2, \dots, 2T_{BI}$ . For  $k$  overlapping piconets we can write the probability of packet time overlap,  $P_t$ , as follows:

$$P_t = \frac{1}{(2T_{BI})^k} \left[ \sum_{l_1 \geq 0}^{T_B} \cdots \sum_{l_k \geq 0}^{T_B} (1 - (1 - BER)^{T_B - \min_{i=1}^k l_i}) + \sum_{l_1 > -T_B}^{-1} \cdots \sum_{l_k > -T_B}^{-1} (1 - (1 - BER)^{T_B + \max_{i=1}^k l_i}) \right] \quad (9)$$

Simple combinatorial manipulation leads to further simplifications and we can write:

$$P_t = \frac{1}{(2T_{BI})^k} \left[ \sum_{l=0}^{T_B} \mathcal{A}_l (1 - (1 - BER)^{T_B - l}) + \sum_{l=0}^{T_B - 1} \mathcal{C}_l (1 - (1 - BER)^{T_B - 1 - l}) \right] \quad (10)$$

where  $\mathcal{A}_l$  and  $\mathcal{C}_l$  are defined as:

$$\mathcal{A}_l = (T_B - l + 1)^k - (T_B - l)^k \quad (11)$$

$$\mathcal{C}_l = (T_B - l)^k - (T_B - l - 1)^k \quad (12)$$

Finally, we write P(PE) as:

$$P(PE) = P_f \times P_t \quad (13)$$

### III. SIMULATION RESULTS

We used *OPNET*<sup>1</sup> to develop a simulation model for the Bluetooth protocol. We partially implement the Baseband and L2CAP layer according to the specifications [6] and use the configuration and system parameters shown in Table I. We assume that a connection is already established between the master and the slave and that the synchronization process is complete. The connection type is either SCO for voice or ACL for data traffic.

TABLE I  
SIMULATION PARAMETERS

Bluetooth Parameters	Values
Propagation delay	5 $\mu$ s/km
Length of simulation run	1000 seconds
Length of run prior to gathering statistics	10 % of simulated time
Data Rate	1 Mbits/s
ACL Baseband Packet Encapsulation	DM5
SCO Baseband Packet Encapsulation	HV1 and HV3
Number of Devices	2 (1 Master, 1 Slave)
Processing delay	0 ms
WLAN Interference Parameters	
Average Packet Size	1000 bytes
$T_W$ @ 1 Mbits/s	8000 $\mu$ s
$T_W$ @ 11 Mbits/s	823 $\mu$ s
$T_{Backoff}$ @ 1 Mbits/s	1802 $\mu$ s
$T_{Backoff}$ @ 11 Mbits/s	2750 $\mu$ s

We present simulation results to evaluate the performance of Bluetooth in presence of WLAN interference. In this case we do not simulate the details of the WLAN MAC behavior, but rather model interference according to the probability of packet error, P(PE), obtained in Equation 5. Given that this P(PE) does not map directly into a probability of packet loss due different packet encapsulations and different error correction schemes, we implement a packet error process applied to the Bluetooth receiver in two steps. First, we compute the probability of packet collision (frequency and packet time overlap), and the collision time  $T_C$ .

<sup>1</sup>OPNET is a trademark of OPNET Technologies Inc.

If  $T_C$  is equal to 0, no error is generated. In case  $T_C > 0$ , then  $T_C * Bit Rate$  gives the number of potential bit errors. The second step consists of applying a BER on each bit in  $T_C$ .

In [3], the BER is assumed to be a constant function of SIR. In fact early measurements and results [4] suggest that below an Signal-to-Noise Ratio (SNR) threshold of 10 dB, the bit error rate is close to 0.5 and above that threshold it is close to 0. This observation is consistent with classical results for GMSK [7] which is very similar to the Bluetooth waveform. For our simulations, we chose to vary the probability of BER between 0 and 0.5 without making any further assumptions on the network topology and the resulting SIR. We note that given a WLAN transmitter will often have a 20 dB power advantage over a Bluetooth one, the SIR will significantly dominate in determining performance over the SNR computation comprising path loss, fading and other effects. However, it is our goal to incorporate a detailed channel and transceiver models in order to correlate the transmitted power and network topology to the BER computation.

All simulations are run for 1000 seconds of simulated time and the first 10 % of the data is discarded. The performance measurements are logged at the slave device. The metric we use includes access delay, packet loss, and number of errors in accepted packet payloads. The access delay is the time required for a packet to reach its destination after that packet is generated at the source. This delay includes retransmission delay due to packet loss. The packet loss is the number of packets discarded due to noncorrected errors divided by the total number of packets transmitted. We use 95th percentile instead of the mean for the access delay and number of errors in the packets in order to capture the delay and error distributions with higher accuracy.

Note that we are in the process of compiling the results for the impact of Bluetooth interference on Bluetooth (Case II) and hope to have them in time for inclusion in the next revision of this contribution.

TABLE II  
IP TRAFFIC: MESSAGE SIZE DISTRIBUTION

Message Size (bytes)	64	128	256	512	1024	1518
Probability	0.6	0.06	0.04	0.02	0.25	0.03

A. Experiments

We present the results from two different simulation experiments that show the impact of WLAN interference on Bluetooth devices for different applications, namely voice and data traffic. For the interference signal, we use 802.11 devices implementing FH at 1 Mbits/s and DS at both 1 and 11 Mbits/s. The packet length for each of the FH, DS and data rates are summarized in Table I.

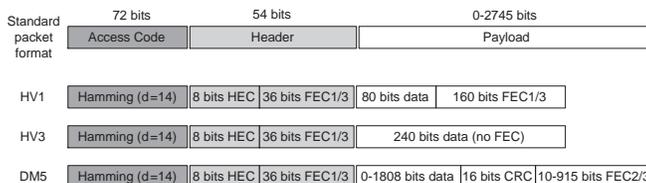


Fig. 2. Bluetooth Packet Format

**Experiment 1** - we consider a voice application generating a symmetric stream of 64 kbits/s each way. We use two different types of packet encapsulation, *HV1* and *HV3* as shown in Figure 2. Both types of packets have a total size of 366 bits including a header and an access code of 126 bits. *HV1* uses a payload of 80 information bits and a 1/3 FEC rate. *HV1* packets are sent every  $T_{SCO} = 2$  or  $1250 \mu s$ . *HV3* uses

a payload of 240 information bits and packets are sent every  $T_{SCO} = 6$  or  $3750 \mu\text{s}$ . Neither *HV1* or *HV3* have a CRC in the payload. In case of an error occurrence in the payload the packet is never dropped. A 1/3 FEC is applied to the packet header while a Hamming code ( $d = 14$ ) is applied to the access code. Uncorrected errors in the header and access code lead to a packet drop. In addition, for *HV1* packets, errors in the payload are corrected using a 1/3 FEC rate.

**Experiment 2** - we focus on a LAN access application. This is typically a connection between a PC and an Access Point or between two PCs and allows for exchanging TCP/IP or UDP-like traffic. Both slave and master devices generate IP packets according to the distribution presented in Table II. The packet interarrival time is exponentially distributed with a mean equal to 29.16ms which corresponds to a load of 30 % of the channel capacity (248 kbits/s for both directions). Packets are encapsulated with *DM5* Baseband packets. A 2/3 FEC rate is used to correct payload errors as shown in Figure 2. Errors in the header or access code are corrected by a 1/3 FEC and a hamming code respectively. Uncorrected errors lead to dropping packets.

Table III summarizes the error occurrences in the packet and the actions taken by the protocol. In order to show the impact of FEC on the packet payload, we disable the FEC for some simulations but keep the packet length unchanged.

TABLE III  
SUMMARY OF ERROR OCCURRENCES IN THE PACKET AND ACTIONS TAKEN IN CASE ERRORS ARE NOT CORRECTED

Error Location	Error Correction	Action Taken
Access Code	Hamming Code, $d = 14$	Packet is dropped
Packet Header	1/3 FEC	Packet is dropped
HV1 payload	1/3 FEC	Packet is accepted
HV3 payload	No FEC	Packet is accepted
DM5 payload	2/3 FEC (or disabled)	Packet is dropped

## B. Results

In this section, we present the simulation results obtained for the experiments previously described.

**Experiment 1** - Figure 3 gives the packet loss for the voice traffic using either an *HV1* or *HV3* packet encapsulation. Note that these packets are dropped in case of an uncorrected error occurring in the header or the access code. We observe that for FH WLAN signal interference, the packet loss is extremely low ( $\approx 0.05\%$ ). This is due to a low probability of frequency overlap ( $1/79$ ). The packet loss increases to 1.25 % for DS interference at 1 Mbits/s due to the wider DS channel that spans 22 Bluetooth channels. A DS interference system operating at 11 Mbits/s leads to a packet loss of 3.45 %. The difference in packet loss between 1 Mbits/s and 11 Mbits/s DS interference, is mainly due to  $T_C$  being more often greater than 0. There is no difference in packet loss between *HV1* and *HV3* encapsulation since both packet types have the same error correction scheme applied on the header and the access code.

However, the difference in encapsulation is captured in Figure 4 where we plot the 95th percentile of the number of errors in the accepted packet payload. This metric illustrates the advantage of using an *HV1* packet where a 1/3 FEC rate is applied to errors in the payload instead of an *HV3* packet where no FEC is used. There are, obviously, fewer errors in the payload when *HV1* is used at the expense of an increased overhead (FEC processing), and lower channel utilization (*HV1* packets are sent more frequently).

**Experiment 2** - Figure 5 shows the packet loss incurred by data traffic. The packet loss reaches 13.46 % for 11 Mbits/s DS interference, while it is 7.26 % and 0.36 % for 1 Mbits/s DS and FH interference systems

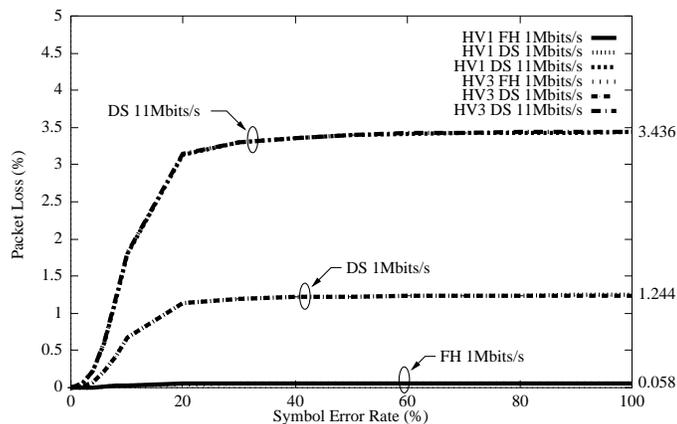


Fig. 3. Experiment 1: Voice Traffic - Packet Loss

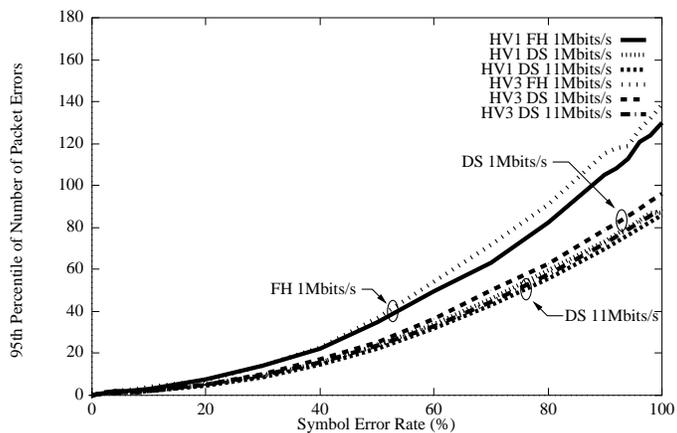


Fig. 4. Experiment 1: Voice Traffic - Number of Errors in Packet Payloads Accepted

respectively. In general, we observe higher loss rates than for voice traffic due to a longer Bluetooth packet that occupies 5 time slots as opposed to 1 slot for *HV1* and *HV3* packets. The effect of FEC is apparent from the packet loss results obtained for 11 Mbits/s DS interference when FEC is disabled. For BER values below 20 %, using FEC reduces the packet loss by almost 10 % (for  $BER = 2\%$ ). For BER values greater than 20 %, the FEC has limited impact on the packet loss.

Figure 6 shows the impact of packet loss on access delays. Since the packet loss for 1 Mbits/s FH interference is rather low, we note no major change in the delays. However losses incurred for 1 and 11 Mbits/s DS interference lead to increasing the delay by a factor of 1.5 and 2 (from 0.01 to 0.015 and 0.02 seconds respectively) due to packet loss and retransmission.

#### IV. CONCLUDING REMARKS

We presented some initial results on the performance of Bluetooth in the presence of WLAN interference based on a probability of packet collision in frequency and packet overlap time at the Bluetooth receiver. The results obtained clearly show that packet loss due to interference may be significant (up to 13% for data traffic and 3% for voice applications) and may lead to performance degradation. Access delays are doubled for data traffic and the number of errors in voice packets is increased considerably (up to 140 errors

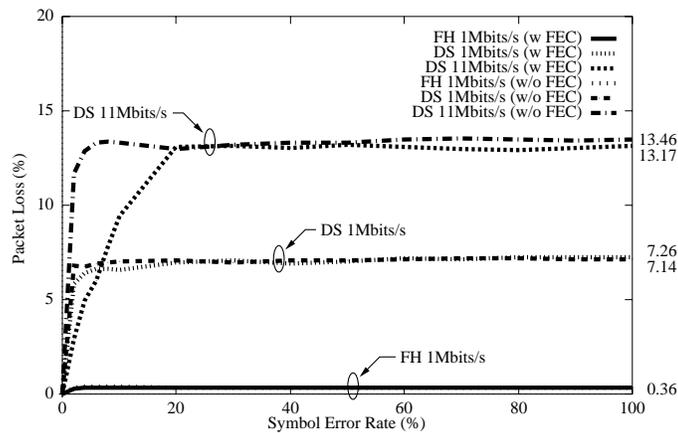


Fig. 5. Experiment 2: LAN Access Traffic - Packet Loss

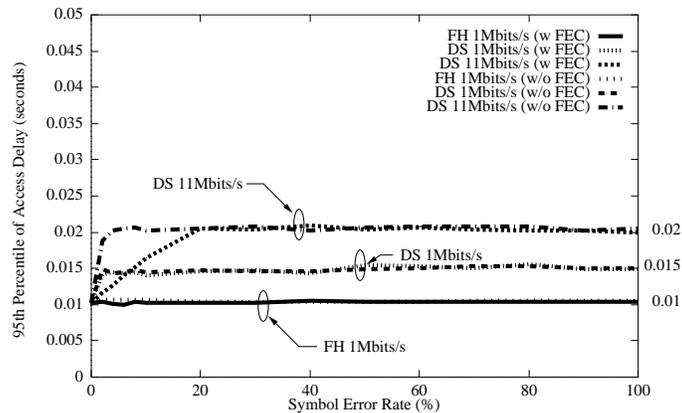


Fig. 6. Experiment 2: LAN Access Traffic - Access Delay

in the packet payload). Our future work includes incorporating a detailed channel and transceiver models into our packet error model in order to correlate the transmitted power and network topology to the BER. In addition, we plan to investigate an evaluation framework where both WLAN and Bluetooth interference can be studied together. This may unravel various intricate effects about the traffic distribution and the overall system performance of Bluetooth and WLAN operating in the 2.4 GHz frequency band.

### REFERENCES

- [1] Zurbes, S.; Stahl, W.; Matheus, K.; Haartsen, J. , "Radio network performance of bluetooth ," in *Proceedings of IEEE International Conference on Communications, ICC 2000*, New Orleans, LA, June 2000, vol. 3, pp. 1563–1567.
- [2] G. Ennis, "Impact of Bluetooth on 802.11 Direct Sequence," in *IEEE P802.11 Working Group Contribution, IEEE P802.11-98/319*, September 1998.
- [3] S. Shellhammer, "Packet Error Rate of an IEEE 802.11 WLAN in the Presence of Bluetooth," in *IEEE P802.15 Working Group Contribution, IEEE P802.15-00/133r0*, Seattle, Washington, May 2000.
- [4] A. Kamerman, "Coexistence between Bluetooth and IEEE 802.11 CCK: Solutions to avoid mutual interference," in *IEEE P802.11 Working Group Contribution, IEEE P802.11-00/162r0*, July 2000.
- [5] J. Zyren, "Reliability of IEEE 802.11 WLANs in Presence of Bluetooth Radios," in *IEEE P802.11 Working Group Contribution, IEEE P802.15-99/073r0*, Santa Rosa, California, September 1999.

- [6] Bluetooth Special Interest Group, "Specifications of the Bluetooth System, vol. 1, v.1.0B 'Core' and vol. 2 v1.0B 'Profiles'," December 1999.
- [7] M. K. Simon and C. C. Wang, "Differential detection of Gaussian MSK in a mobile radio environment," in *IEEE Trans. Veh. Technology*, November 1984, vol. 33, pp. 307–320.