LUND UNIVERSITY

Throughput of IEEE 802.11 FHSS networks in the presence of strongly interfering Bluetooth networks

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

Published in:
13th IEEE International Symposium on Personal Indoor and Mobile Radio Communications. PIMRC 2002. Proceedings (Cat. No.02TH8637)

DOI:
10.1109/PIMRC.2002.1046681

2002

THROUGHPUT OF IEEE 802.11 FHSS NETWORKS IN THE PRESENCE OF STRONGLY INTERFERING BLUETOOTH NETWORKS

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

[1]Dept. of Electroscience, Lund University, Box 118, SE-22100 Lund, Sweden

[2]Telia Research AB, Box 94, SE-201 20 Malmö, Sweden

[3]Axis Communications AB, Scheelev. 34, SE-223 63 Lund, Sweden

{andre.stranne, fredrik.floren}@es.lth.se

Abstract— **In this paper the impact of interference from Bluetooth networks on the throughput of IEEE 802.11 FHSS networks is investigated. This is done by deriving an analytical approximation of the throughput of slow frequency-hopping systems. The derivation in itself provides valuable insights into the mechanisms of interference between systems employing the frequency-hopping technique. In deriving the approximation, it is assumed that packet collisions result in total loss of all information contained in the packets involved in the collisions, regardless of the distance between the networks. The results indicate that the Bluetooth networks may have a negative effect on the throughput of an IEEE 802.11 network using long packet types.**

Keywords— **Slow FHSS, Bluetooth, IEEE 802.11**

I. Introduction

Presently, and certainly in the coming years, a variety of radio systems must coexist in the unlicensed 2.4 GHz ISM-band. In this band, some type of spread-spectrum technique must be used, e.g., direct-sequence spread spectrum (DSSS) or frequency-hopping spread spectrum (FHSS). Systems that use FHSS are, e.g., Bluetooth [1] and WLAN systems based on the IEEE 802.11 FHSS standard [2].

With the expected increase of the number of Bluetooth units present in consumer electronics in the near future, the interference between systems using different types of spread-spectrum techniques is a topic of significant interest. In this paper we have chosen to focus on the interference between FHSS systems by deriving an analytical approximation of the throughput of such systems.

The system model enables this analytical derivation since it is assumed that collisions always result in total loss of the data in the colliding packets. Although realistic in relatively few cases, this assumption will make it possible to derive a useful analytical approximate expression for the throughput of the systems.

With our approach, the main idea is to first find the approximate probability of a certain number of packet collisions between one reference network and one interfering network, and from that derive an expression for the throughput when multiple interfering networks are present. The throughput is given as a function of the number of adjacent interfering networks, the lengths of the available packet types, and the probability that a unit transmits a packet of a certain type.

The major contribution of this paper is an analysis, which is performed using a simple expression, of the throughput degradation of FHSS networks in close proximity of each other. In addition, the derivation of the approximation yields valuable insights into the mechanisms of interference between FHSS networks.

In the literature, the topic of this paper, i.e., the interference between different types of FHSS systems, have received little attention. However, the interference between FHSS and DSSS systems has been investigated. For example, work on the interference between IEEE 802.11 DSSS and Bluetooth has been performed analytically in [3, 4], empirically in [5, 6], and by use of simulations in [7].

This paper is organized as follows. In Section II the system model is presented and in Section III the approximation of the throughput of FHSS networks is derived. The investigation of the impact of the interference between FHSS systems is performed in Section IV, and in Section V some conclusions and final remarks are presented.

II. System Model

A system is defined to consist of N networks, and a network is defined to consist of an arbitrary number of units that communicate without interference. Specifically, there is exactly one ongoing transmission within a network at a time. This implies that units within a network are coordinated in some manner.

How the resources are divided between the network units, or the resulting throughput of a specific unit, is not of interest here; the performance of the networks and of the system is considered as a whole. The term network transmission is used for a transmission by any unit within a network.

Networks transmit packets that consist of the following components: a header of length h_i, a payload of length l_i, and a guard interval of length d_i, where i refers to the ith packet type. The components of a type i packet can be seen in Figure 1. The interval $h_i + l_i$, during which the transmitter is active, i.e., transmitting, is referred to as the *active interval*. In contrast, the transmitter is idle during the guard interval. The lengths L_i, l_i, h_i, and d_i

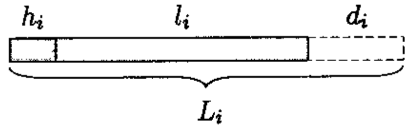

Fig. 1. Definition of a packet and its components: header, payload, and guard interval. Their lengths are h_i, l_i and d_i, respectively, and the sum of the lengths equals L_i.

are here specified in seconds, and when referring to the entire packet length, $L_i = h_i + l_i + d_i$ is used.

The probability of selecting a packet of type i for transmission is denoted r_i. The packet types and their corresponding probabilities that are used by a network are henceforth referred to as its *packet type distribution.*

Further, it is assumed that networks always have packets to transmit and networks are only idle during the guard interval. The reason for using guard intervals is that the hardware cannot shift frequency instantaneously.

When a new packet is to be sent, a packet type is selected from the set of available packet types and a new frequency channel is also selected. The new channel is selected from a set of q channels and all channels are selected with the same probability. In other words, we employ a packet-based *slow* frequency-hopping scheme. The scheme is termed slow since hops are not performed after each symbol or parts of a symbol, but after each packet. We further assume that networks select their channels independently of other networks.

It should be noted that transmissions are not synchronized between networks, i.e., there is no coordination between networks of the start of packet transmissions.

To proceed, the terms *overlap* and *collision* are defined as follows. An overlap between two packets occurs when their active intervals, at some point in time, are transmitted simultaneously, whereas a collision is an overlap on the same frequency channel. Hence, a collision implies an overlap but the converse is not necessarily true.

Should there occur a collision, all packets involved in the collision will be destroyed and the information contained in the colliding packets is lost. On the other hand, if no collisions occur packets are assumed to be correctly received.

III. Approximation of Throughput for Slow FHSS Systems

The method employed for obtaining an expression for the throughput of FHSS systems is the introduction of a variable-length reference packet, for which an approximation of the probability of successful transmission is found.

Consider a system of N networks. One of these networks will act as a reference network and the other $N-1$ networks will act as interferers. It is assumed that the interferers all use the same packet type distribution although extending the analysis to a case without this restriction poses no major difficulties.

Assume that the reference network transmits a packet of a certain type on one of the q channels. If any of the interfering networks' packets overlap with the reference packet a collision might occur. The probability of successful transmission will therefore depend on the length of the active interval of the reference packet and not on the length of its guard interval. Let T be the length of the active interval of the reference packet and let $P(\mathrm{S};T)$ be the probability of successful transmission of a reference packet whose active interval length is T.

Given that the total number of interfering packets overlapping the reference packet is n, i.e., we condition on n overlaps, then the conditional probability for successful transmission is [8]

$$P(\mathrm{S}|n;T) = \left(1 - \frac{1}{q}\right)^n \qquad (1)$$

This follows since there are q channels available, and the interfering networks independently select a certain channel with probability $1/q$. Hence, the probability for not selecting a channel is $1-1/q$. For the transmission to be successful, neither of the n overlapping packets may be transmitted on the same channel as the reference packet, thus, (1) is obtained. Note that since the number of overlaps is given, this probability is independent of T. The n overlaps are generated by the $N-1$ interfering networks, and each interfering network can generate multiple overlaps during its transmissions if the active interval of the reference packet is sufficiently long.

To obtain an expression for $P(\mathrm{S};T)$, the probability of n overlaps during the transmission of the reference packet must be calculated since the condition on n can then be removed. Let $p_{\mathrm{tot}}(n;T)$ be the probability function for the number of overlaps during an active interval of length T. The condition on (1) is removed by summing the product of (1) and $p_{\mathrm{tot}}(n;T)$ over n, which gives

$$P(\mathrm{S};T) = \sum_{n=0}^{\infty} p_{\mathrm{tot}}(n;T)\left(1 - \frac{1}{q}\right)^n. \qquad (2)$$

To find the probability function $p_{\mathrm{tot}}(n;T)$, $p_j(n;T)$ is defined as the probability of interfering network j transmitting n packets overlapping the reference packet's active interval. It is assumed that all interfering networks transmit independently, which gives, by convolution of the individual probability functions,

$$p_{\mathrm{tot}}(n;T) = p_1(n;T) * p_2(n;T) * \ldots * p_{N-1}(n;T). \qquad (3)$$

This is the probability function of the sum of the number of overlaps generated by the interfering networks.

Since it has been assumed that all interfering networks use identical packet type distributions, all $p_j(n;T)$ are equal, i.e., $p_j(n;T) = p(n;T)$ for all j. By letting $p^{(k)}(n;T)$ denote the convolution of k replicas of the function $p(n;T)$ with each other, (3) becomes

$$p_{\mathrm{tot}}(n;T) = p^{(N-1)}(n;T). \qquad (4)$$

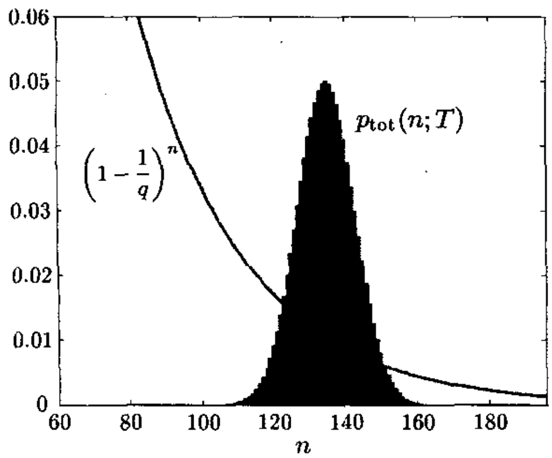

Fig. 2. Example of the Gaussian-like shape of the probability function for the number of overlaps during the reference packet's active interval, $p_{tot}(n;T)$, and the conditional probability of successful transmission $(1-1/q)^n$

Combination of (2) and (4) gives the probability of successful transmission of the reference packet as

$$P(\mathrm{S};T) = \sum_{n=0}^{\infty} p^{(N-1)}(n;T)\left(1-\frac{1}{q}\right)^n \tag{5}$$

Although the probability function of the sum of the number of overlaps $p^{(N-1)}(n;T)$ is possible to evaluate, it is quite tedious and the result is difficult to analyze. Therefore, the term $(1-1/q)^n$ is approximated with its Taylor series expansion about the mean of the number of overlaps, i.e., about $\bar{n}_{\text{tot}} = \sum_{n=0}^{\infty} n p_{\text{tot}}(n;T)$.

By applying the approximation, (2) reduces to

$$P(\mathrm{S};T) = \sum_{n=0}^{\infty} p_{\text{tot}}(n;T)\left(1-\frac{1}{q}\right)^n \approx \left(1-\frac{1}{q}\right)^{\bar{n}_{\text{tot}}}, \tag{6}$$

and the approximation of $P(\mathrm{S};T)$ is denoted $\tilde{P}(\mathrm{S};T)$, i.e.,

$$\tilde{P}(\mathrm{S};T) = \left(1-\frac{1}{q}\right)^{\bar{n}_{\text{tot}}} \tag{7}$$

The exact expressions is illustrated in Figure 2, where it can be seen how (2) is calculated: For every n, $(1-1/q)^n$ and $p_{\text{tot}}(n;T)$ are multiplied and the products are then summed. The probability function $p_{\text{tot}}(n;T)$ is obtained by convolving $p(n;T)$ with itself the number of times representing the number of interfering networks present, and $p_{\text{tot}}(n;T)$ will after a few convolutions exhibit the Gaussian-like shape that can be seen in Figure 2. This figure indicates that when the mean number of overlaps is large, $(1-1/q)^n$ will be fairly constant for the n for which $p_{\text{tot}}(n;T) \neq 0$, which yields an accurate approximation for large $\bar{n}_{\text{tot}}$. For small $\bar{n}_{\text{tot}}$, the steep gradient of $(1-1/q)^n$ will, in combination with the relative narrowness of $p_{\text{tot}}(n;T)$, i.e., the variance of the number of overlaps, result in a small error in this case as well.

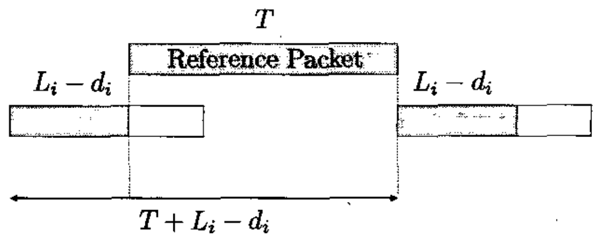

Fig. 3. The critical time, $T + L_i - d_i$, for overlaps from a type i packet during the transmission of a reference packet of length T.

Using the average packet length $\sum_{k=1}^{M} r_k L_k$, where M denotes the number of available packet types, the average number of packets transmitted by a single interfering network during the interval T can be calculated as

$$\bar{n}(T) = \frac{T}{\sum_{k=1}^{M} r_k L_k}. \tag{8}$$

Per definition, a fraction r_i of the interfering packets are of type i. Hence, the average number of type i packets is

$$\bar{n}_i(T) = r_i \bar{n}(T). \tag{9}$$

By consulting Figure 3, it can be seen that for interfering type i packets the time interval $T + L_i - d_i$ needs to be taken into account when counting the number of overlapping packets, resulting in an average number of $\bar{n}_i(T+L_i-d_i)$ overlapping packets of type i. The interval $T + L_i - d_i$ is the time during which a start of transmission of a type i packet will generate an overlap, and, hence, possibly a collision. Since all $N-1$ interfering networks transmit independently, the average number of type i packet transmissions by all networks during that time interval is

$$\bar{n}_{i,\text{tot}}(T + L_i - d_i) = (N-1)\bar{n}_i(T + L_i - d_i). \tag{10}$$

Given the average number of overlapping packets of each type, the average total number of overlapping packets $\bar{n}_{\text{tot}}$ is given by the sum

$$\begin{aligned} \bar{n}_{\text{tot}} &= \sum\nolimits_{i=1}^{M} \bar{n}_{i,\text{tot}}(T + L_i - d_i) \\ &= (N-1)\frac{T + \sum_{i=1}^{M} r_i (L_i - d_i)}{\sum_{k=1}^{M} r_k L_k}, \end{aligned} \tag{11}$$

where $\sum_i r_i = 1$ has been used.

Substitution of (11) into (6) yields a closed form approximation of the probability of successful transmission of a packet whose active interval length is T

$$\tilde{P}(\mathrm{S};T) = \left(1-\frac{1}{q}\right)^{(N-1)\frac{T+\sum_{i=1}^{M} r_i (L_i - d_i)}{\sum_{k=1}^{M} r_k L_k}} \tag{12}$$

In order to calculate the throughput, assume that the reference network with probability ρ_k transmits a packet of type k where the length of the header, payload, and guard interval are denoted by τ_k, λ_k, and Δ_k, respectively. Furthermore, the sum of reference network's kth packet type components is denoted Λ_k, i.e., $\Lambda_k = \tau_k + \lambda_k + \Delta_k$, and U packet types are available.

The throughput is now obtained as the mean ratio of the channel time that is used for successful transmission of data in the payloads. Hence, the throughput is given by the ratio between the mean length of the successfully transmitted payloads and the mean packet length, including the guard interval. However, in order to take the different bit rates for the payloads into account, the probability of successful transmission of a packet type is also normalized with β_n, which is the bit rate used when transmitting the type n payload. The throughput can be written

$$R = \frac{\sum_{n=1}^{U} \beta_n \rho_n \lambda_n P(\mathrm{S}; \Lambda_n - \Delta_n)}{\sum_{k=1}^{U} \rho_k \Lambda_k}. \tag{13}$$

Finally, by using the approximation (12) in (13), the approximate throughput for the reference network becomes

$$\tilde{R} = \frac{\sum_{n=1}^{U} \beta_n \rho_n \lambda_n \left(1 - \frac{1}{q}\right)^{\left(\frac{\Lambda_n - \Delta_n + \sum_{i=1}^{M} r_i (L_i - d_i)}{\sum_{k=1}^{M} r_k L_k}\right)(N-1)}}{\sum_{k=1}^{U} \rho_k \Lambda_k}. \tag{14}$$

IV. Throughput of IEEE 802.11 FHSS in the Presence of Strongly Interfering Bluetooth Networks

In this section we investigate how the throughput of IEEE 802.11 FHSS networks is affected by interference from Bluetooth networks by mapping these two systems onto our system model. The throughput is calculated and plotted as a function of number of interfering Bluetooth networks using (14).

The IEEE 802.11 FHSS networks use either $\beta = 1$ Mb/s, corresponding to the 1 Mb/s PHY-mode, or $\beta = 2$ Mb/s, corresponding to the 2 Mb/s PHY-mode, for the transmission of the payloads. The header length, τ, is 192 μs and the guard interval length, Δ, is 224 μs. Since only one packet type is used, the subscripts on the packet component lengths have been omitted.

The throughput of networks transmitting packets with payloads of 4096 bytes, corresponding to hopping frequencies of 30 and 60 Hz, have been investigated. These two hopping frequencies are obtained when the 1 Mb/s and 2 Mb/s PHY-modes are used, respectively. A payload length of 4096 bytes is the maximum payload length allowed by the IEEE 802.11 FHSS standard [2].

	Bluetooth		802.11			
Parameter	long	short	4096 bytes		1500 bytes	
r/ρ	1	1	1	1	1	1
L/Λ [μs]	3380	630	33184	16800	12416	6416
h/τ [μs]	160	160	192	192	192	192
l/λ [μs]	3000	250	32768	16384	12000	6000
d/Δ [μs]	220	220	224	224	224	224
β [Mb/s]	1	1	1	2	1	2

TABLE I

802.11 PACKET TYPES CORRESPONDING TO PAYLOAD LENGTHS OF 1500 AND 4096 BYTES, AND BLUETOOTH PACKET TYPES.

In addition to the 4096 byte case, the throughput of networks transmitting payloads of the commonly used packet length of 1500 bytes is also investigated. This payload length in bytes corresponds to a hopping frequency of 81 Hz when the 1 Mb/s PHY-mode is used and 156 Hz when the 2 Mb/s PHY-mode is used. The number of channels used for frequency hopping is 79 for both the reference network and the interferers.

The interfering environment consists of a variable number of Bluetooth networks. Generally, Bluetooth networks can use three packet types, but it is assumed here that either the longest or the shortest packet type is used by all the interfering networks. Since the headers of all Bluetooth packets are equal, the long and short packet types represent the best and worst cases, respectively, for the IEEE 802.11 network. We note that a dwell time of only 630 μs, corresponding to a hopping frequency of 1600 Hz, is considerably smaller than the longest packet type used by the IEEE 802.11 networks.

The parameters for the IEEE 802.11 and Bluetooth packet types are summarized in Table I. In this table, r, L, h, l, and d are used for interfering Bluetooth networks and $\rho, \Lambda, \tau, \lambda$, and Δ are used for the reference network, i.e., the IEEE 802.11 network.

Consider first an IEEE 802.11 network using packets with payloads of 4096 bytes, i.e., packets of the type specified in the fourth and fifth column in Table I. The throughput of such a reference network, using the 1 Mb/s and the 2 Mb/s PHY-modes, is plotted in Figure 4 as a function of the number of interfering Bluetooth networks, which all use either long or short packets. For a given PHY-mode for the IEEE 802.11 network, the throughput is bounded by the worst case and the best case throughput, represented by the cases when the Bluetooth networks use the short or the long packet type, respectively. When the IEEE 802.11 networks use the 2 Mb/s PHY-modes, a throughput of half of the maximum or less is obtained for approximately 2 and 10 interfering networks when the interfering Bluetooth networks use the short or long packet types, respectively. If the IEEE 802.11 networks use the 1 Mb/s PHY-mode instead, the corresponding number of interfering networks is approx-

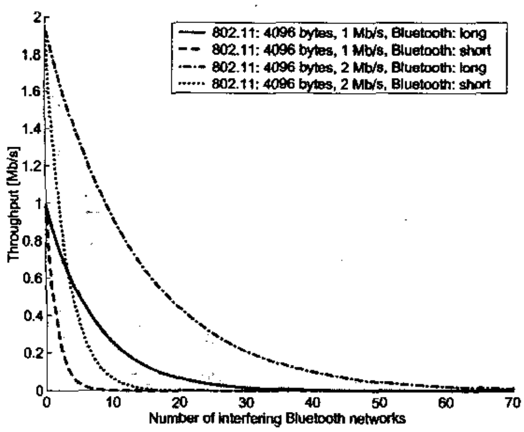

Fig. 4. Throughput of an IEEE 802.11 FHSS network, using the 1 or 2 Mb/s PHY-mode, as a function of the number of interfering Bluetooth networks. The IEEE 802.11 network uses packets with a payload of 4096 bytes and the Bluetooth networks use a hopping frequency of 300 Hz or 1600 Hz.

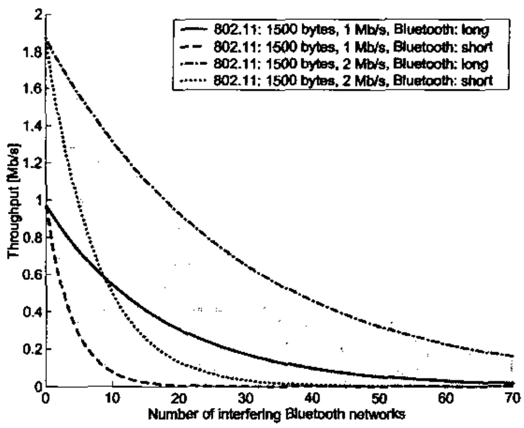

Fig. 5. Throughput of an IEEE 802.11 FHSS network, using the 1 or 2 Mb/s PHY-mode, as a function of the number of interfering Bluetooth networks. The IEEE 802.11 network uses packets with a payload of 1500 bytes and the Bluetooth networks use a hopping frequency of 300 Hz or 1600 Hz.

imately 1 and 5.

Next, the throughput of the 1500 byte IEEE 802.11 packets is calculated. The results for the two packet types in the sixth and seventh columns of Table I can be found in Figure 5. Half of the maximum throughput or less for the 2 Mb/s mode is obtained for 8 and 20 interfering networks when the interfering networks use the short or long packet types, respectively. The corresponding values for the 1 Mb/s mode are 3 and 13 interfering networks. It can be seen that the throughput loss of an IEEE 802.11 network using the 1500 byte packet size is not as severe as in the 4096 byte-case. This is because the hopping frequencies for the smaller packet size are 156 and 81 Hz, which is approximately double that of the 1500 byte case.

V. Conclusions

In this paper we have derived an analytical approximation of the throughput of interfering FHSS networks. In addition, the applicability of the approximation and the mapping of existing systems onto the presented system model is illustrated by investigating the throughput of an IEEE 802.11 FHSS wireless network in the close proximity of multiple Bluetooth networks. It can be concluded that an IEEE 802.11 FHSS network using a low hopping frequency may suffer in terms of throughput due to the higher hopping frequency of the Bluetooth networks. It should be noted that, in practice, the throughput for the two systems in the presence of each other may differ from what is presented in this paper since we have not taken into account a number of important aspects concerning the practical implementation of the systems.

VI. Acknowledgments

This work has taken place in the Personal Computing and Communication research program, founded by the Swedish Foundation for Strategic Research.

References

[1] J. Haartsen, "The Bluetooth radio system," *IEEE Personal Comm.*, vol. 7, pp. 28–36, Feb. 2000.

[2] "IEEE 802.11 wireless LAN medium access control (MAC) and physical layer (PHY) specifications." IEEE, 1999.

[3] I. Howitt, "WLAN and WPAN coexistence in UL band," *IEEE Trans. Veh. Technol.*, vol. 50, pp. 1114–1124, July 2001.

[4] C. Chiasserini and R. Rao, "Wireless networked digital devices: A new paradigm for computing and communication," in *Proc. IEEE Wireless Communications and Networking Conference*, vol. 1, pp. 94–99, 2000.

[5] R. Punnoose, R. Tseng, and D. Stancil, "Experimental results for interference between Bluetooth and IEEE 802.11b DSSS systems," in *Proc. 54th IEEE Vehicular Technology Conference*, vol. 1, pp. 67–71, 2001.

[6] M. Chandrashekhar, P. Choi, K. Maver, R. Sieber, and K. Pahlavan, "Evaluation of interference between IEEE 802.11b and Bluetooth in a typical office environment," in *Proc. 12th IEEE Symposium on Personal, Indoor and Mobile Radio Communications*, vol. 2, pp. 71–75, 2001.

[7] J. Lansford, A. Stephens, and R. Nevo, "Wi-Fi (802.11b) and Bluetooth: Enabling coexistence," *IEEE Network*, vol. 15, pp. 20–27, September/October 2001.

[8] G. L. Stüber and K. Yang, "Throughput analysis of a slotted frequency-hopped spread spectrum multiple access network," in *Proc. IEEE International Conference on Communications*, vol. 1, pp. 494–498, 1990.