Journal of Southeast University (English Edition) Vol.19 No.3 Sept. 2003 ISSN 1003—7985

Interference analysis and improvement of capacity reduction for FHSS networks in WPAN application environment

Ye Zhihui[1,2] Shen Lianfeng[1] Song Tiecheng[1]

([1] National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China)

([2] Institute of Communication Engineering, PLA University of Science and Technology, Nanjing 210016, China)

Abstract: The coexistence between Bluetooth system and IEEE 802.11 frequency hopping spread spectrum (FHSS) equipment is analyzed. Based on the capacity formulae and system simulation, the inter-affection between these networks is compared. A fragment adaptive solution of packet payload length is presented, which can be used to improve the capacity reduction of IEEE 802.11 FHSS network. Analysis results show that the IEEE 802.11 WLAN standard with its inherent mechanism supports this fragment length adaptive algorithm. With the increasing of Bluetooth interfering networks, this adaptive solution can effectively relieve capacity decreasing of IEEE 802.11 FHSS network. The capacity analysis method and adaptive algorithm adopted in this paper can also be generalized into other FHSS networks.

Key words: WPAN; frequency-hopping; network capacity; Bluetooth technology; IEEE 802.11 FHSS network; fragment adaptive of packet payload length

A wireless personal area network (WPAN) provides communication among computers, peripherals, electronic products, and household appliances, etc., constitutes personal networks and can connect to Internet. The 2.4 GHz industry science medical (ISM) frequency band becomes a favorable choice for low-cost wireless devices because of its global availability. The major systems operating at this band include WPAN such as IEEE 802.15 and Bluetooth, IEEE 802.11 WLAN standards, and the shared wireless access protocol (SWAP) developed by the Home Radio Frequency Working Group (HRFWG). These systems typically operate within short range, with frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS) technology as fundamental features. In addition, microwave ovens also operate on this band and cause serious interference on other devices. Thus, there exist various interferers in the operation environment of WPAN systems which result in great performance capacity reduction. Thus interference suppression becomes a crucial problem in the WPAN application environment[1-3].

Since FHSS technology can efficiently improve the performance of micro-cellular systems, flexibly build networks and powerfully resist far-near interferences, it is widely applied in short range wireless multimedia communication, especially in WPANs. The FHSS system uses orthogonal pseudo-random hopping patterns to avoid collision. However, in a distributing system, it is impossible to have ideal orthogonal patterns, which results in two or more users transmitting signals on the same frequency slot at the same time and causing hop collision or "hit". The probability of collision increases with the adding of networks to the system, especially for those FHSS networks with different standards. Systems performance reduction thus becomes inevitable.

Received 2003-06-03.

Foundation items: The National Natural Science Foundation of China (60072016); the Key Science Technology Research Project of the Ministry of Education (02171).

Biographies: Ye Zhihui (1967—), female, graduate; Shen Lianfeng (corresponding author), male, professor, lfshen@seu.edu.cn.

1 System Modeling and Capacity Analysis for FHSS Networks

Assume that an FHSS system consists of N networks, one of which is defined as the target network and the others $N-1$ as interference networks. To simplify the analysis, it is assumed that the target network is an IEEE 802.11 FHSS network and all interfering networks are Bluetooth networks, or vice versa. This will not affect generality of the analysis results. The self-interference within a network is ignored. It is also assumed that all users hop among the same q frequency channels and the packet transmission within any network is independent of all other networks.

There are many available packet types in an FHSS network applicable to different occasions. For example, twelve types of packets have been defined in

Bluetooth, including synchronous connection-oriented (SCO) packet for synchronous signals and asynchronous connection-less (ACL) packet for asynchronous signals[4]. Assume that the length of a transmitted packet in an FHSS network is composed of header (including preamble) h_i, payload l_i and guard field g_i, where i denotes the i-th packet type. Users transmit data during $h_i + l_i$, which is referred to as an active field, and remain idle during the guard field g_i. The total packet length is denoted as $L_i = l_i + h_i + g_i$. The probability for a network to transmit the i-th packet type is denoted as σ_i. While a new packet is being transmitted, the network selects a type from the packet type set and a new frequency channel from the q channel set with equal probability. Further assume that channel selection of a network is independent from each other.

If n packets of multiple networks in the same system are in active states simultaneously, they are referred to as overlapping packets. Collisions occur when the active target packet overlaps with the active interfering packets in the same frequency channel. It is assumed that all packets involved in collision will be destroyed and all packets without any collision are received correctly. Further assume that all interferers employ one kind of packet type distribution. When a packet transmitted by the target network (which is referred to as target packet from here on) collides with any packets transmitted by networks, packet loss occurs. Obviously, the probability of successful packet transmission depends on the length of the active field of the target packet denoted by T. The probability of successful target packets transmission with an active field length of T is denoted by $P(S;T)$.

If there are q available channels for all networks in the FHSS system, and each interfering network separately selects a specified channel with the probability of $1/q$, the probability of no selected is $1 - 1/q$. For a packet transmitted successfully, the n overlapping packets should not dwell at the same channel of target packet, thus, under the condition that the total number of interfering packets overlapping with the target packet is n, the conditional probability of successful transmission becomes

$$P(S|n;T) = (1 - 1/q)^n \tag{1}$$

The probability for the j-th interfering network transmitting n overlapping packets during the active field of the target packet is defined as $p_j(n;T)$. The $p_A(n;T)$ is the probability function of the number of overlapping packets during an active field of length T. Assume that all interfering networks transmit independently, and all interfering networks employ the same packet type distribution, thus all $p_j(n;T)$ are equal, that is $p_j(n;T) = p(n;T)$ for any j. Then we have

$$p_A(n;T) = p^{(N-1)}(n;T) \tag{2}$$

which is the probability of the total overlapping packets produced by interfering networks.

From (1) and (2), the probability of successful transmission of a target packet is

$$P(S;T) = \sum_{n=0}^{\infty} p_A(n;T)P(S|n,T) = \sum_{n=0}^{\infty} p^{(N-1)}(n;T)(1 - 1/q)^n \tag{3}$$

The expectation of the probability of the number of overlapping packets is computed as

$$E[n_A] = \sum_{n=0}^{\infty} np_A(n;T) \tag{4}$$

Using the Taylor expansion, Eq.(3) can be approximated as

$$P(S;T) = \sum_{n=0}^{\infty} p_A(n;T)(1 - 1/q)^n \approx (1 - 1/q)^{E[n_A]} \tag{5}$$

Let $\sum_{k=1}^{Q} \sigma_k L_k$ be the average packet length, where Q is the set of available packet types, hence, the average packets transmitted by single interfering network during T interval is

$$E[n(T)] = \frac{T}{\sum_{k=1}^{Q} \sigma_k L_k} \tag{6}$$

The average packets of the i-th type transmitted by interfering network is

$$E[n_i(T)] = \sigma_i E[n(T)] \tag{7}$$

The worst-case mean time, during which the transmission of a target packet may create an overlap and a collision is caused, may be denoted by $T + \sum_{i=1}^{Q} \sigma_i(L_i - g_i)$. Use this variable to modify the variable T in (7) to compute overlapping packets. Since all $N - 1$ networks transmission are independent from each other, the mean value of the i-th type packet transmitted during this interval by all interfering networks is

$$E\left[n_{i,A}\left(T + \sum_{i=1}^{Q} \sigma_i(L_i - g_i)\right)\right] = (N - 1)E\left[n_i\left(T + \sum_{i=1}^{Q} \sigma_i(L_i - g_i)\right)\right] \tag{8}$$

Summing up (8) over the number of total packet types Q, along with (6), the expectation of total overlapping packets $E[n_A]$ is derived as

$$E[n_A] = \sum_{i=1}^{Q} E\left[n_i\left(T + \sum_{i=1}^{Q} \sigma_i (L_i - g_i)\right)\right] = (N-1)\frac{T + \sum_{i=1}^{Q} \sigma_i (L_i - g_i)}{\sum_{k=1}^{Q} \sigma_k L_k} \quad (9)$$

where $\sum_{i=1}^{Q} \sigma_i = 1$ is employed.

Substituting (9) into (5), the probability for a packet with the active field T to transmit successfully is approximated as

$$P(S;T) \approx (1 - 1/q)^{B_1} \quad (10)$$

where $B_1 = (N-1)\dfrac{T + \sum_{i=1}^{Q} \sigma_i (L_i - g_i)}{\sum_{k=1}^{Q} \sigma_k L_k}$.

To compute capacity, assume that the target network transmits the k-th type packets with the probability of ρ_k. The header length, payload field and guard field are denoted by $\alpha_k, \beta_k, \eta_k$, respectively. The total length of the k-th type packet of the target network is $\lambda_k = \tau_k + \beta_k + \eta_k$ and M types are available. The system capacity is obtained by the rate of the mean length of payloads successfully transmitted to mean value of packet length, and is further generalized by the bit rate γ_n used in the n-th type of payloads. Hence, the system capacity can be written as

$$S = \frac{\sum_{n=1}^{M} \gamma_n \rho_n \beta_n P(S;\lambda_n - \eta_n)}{\sum_{k=1}^{M} \rho_k \lambda_k} \quad (11)$$

Finally, substituting (10) into (11), the capacity approximation of the target network becomes

$$S = \frac{\sum_{n=1}^{M} \gamma_n \rho_n \beta_n \left(1 - \frac{1}{q}\right)^{B_2}}{\sum_{k=1}^{M} \rho_k \lambda_k} \quad (12)$$

where $B_2 = (N-1)\dfrac{\lambda_n - \eta_n + \sum_{i=1}^{Q} \sigma_i (L_i - g_i)}{\sum_{k=1}^{Q} \sigma_k L_k}$.

2 Interference Analysis within FHSS Networks

In this section, the system model and capacity relation derived from above are employed to analyze the capacity reduction caused by co-interference within FHSS networks in WPAN application environment. The analysis includes the performance reduction of IEEE 802.11 FHSS network in the presence of Bluetooth interferers and the effect of IEEE 802.11 interferers on Bluetooth. And, the capacity of the target system is computed and simulated as the function of interfering network numbers.

Bluetooth adopts fast frequency hopping and short packet scheme, hop rate is generally 1 600 hops/s. Each time slot lasts 625 μs and the maximum length of single slot packets is 366 μs. The total number of hop channels q is 79. The modulating data rate is 1 Mbit/s now and will be 2 Mbit/s in future. The packet format of Bluetooth is shown in Fig.1. The lengths of access code and header are stabilized at 72 bits and 54 bits, respectively. The effective payload can vary from 0 to 2 745 bits[4-6].

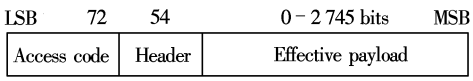

Fig.1 General packet format for Bluetooth

IEEE 802.11 FHSS network uses slow frequency hopping and long packet scheme. The minimum hop rate is 2.5 hops/s in the America, the maximum payload is 4 096 bytes, modulating data rate is 1 Mbit/s or 2 Mbit/s, the total number of hop channels q is 79[4]. Obviously, the maximum packet length of IEEE 802.11 FHSS is much larger than that of Bluetooth, and it is the key difference between the two standards. The packet format of IEEE 802.11 FHSS is shown in Fig.2.

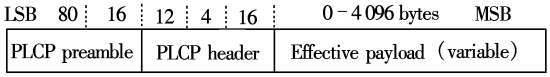

Fig.2 General packet format for IEEE 802.11 FHSS

First, the effect of IEEE 802.11 FHSS networks on Bluetooth is analyzed. Bluetooth is referred to as the target network in this case and its capacity is shown in Fig.3 as the function of interferers. Assume the target and interfering networks use one type of packets respectively.

Next, the IEEE 802.11 FHSS network is taken as the target network with a payload of either 2 048 bytes or 1 024 bytes at the modulating rate of 1 Mbit/s and 2 Mbit/s, respectively. The capacity curve is re-calculated. The header length α and guard field η are 192 μs and 224 μs, respectively. Only one type of interfering packets is considered. The results are shown in Fig.4 and Fig.5, respectively.

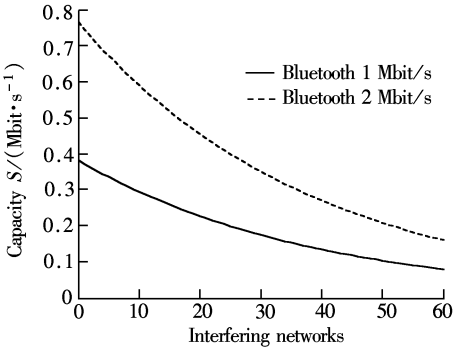

Fig.3 Capacity reduction of Bluetooth in the presence of IEEE 802.11 FHSS interferers

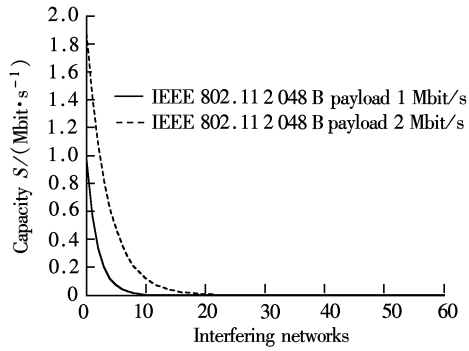

Fig.4 Capacity reduction of IEEE 802.11 FHSS network in the presence of Bluetooth interferers (the payload of target network is 2 048 bytes)

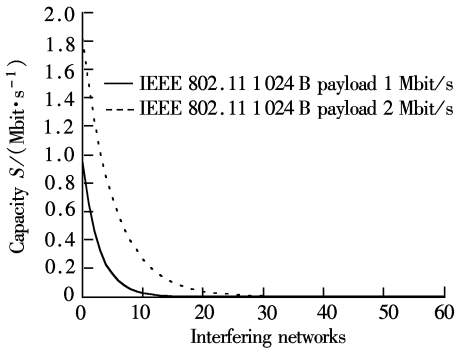

Fig.5 Capacity reduction of IEEE 802.11 FHSS network in the presence of Bluetooth interferers (the payload of target network is 1 024 bytes)

From Fig.3 to Fig.5, the capacities of both types of networks are shown to decrease with the increasing of interfering networks. However, the rate of decrease is much smaller in Bluetooth than in the IEEE 802.11 FHSS network. This means that Bluetooth has a superior performance of interference resistance because its short transmission packets can better avoid collisions. On the other hand, comparing the capacity curves of different payload lengths in IEEE 802.11 FHSS networks (see Fig.4 and Fig.5), the 1 024 bytes payload packets are more robust than those of the 2 048 bytes, that is, the IEEE 802.11 FHSS network with shorter payload length packets exhibits better robustness.

On the basis of the above analyses and simulations, we propose a method of adaptive fragment length for packets to mitigate the capacity reduction of IEEE 802.11 FHSS networks. This mechanism can be realized conventionally in the medium access control (MAC) layer.

3 The Scheme of Fragment Adaptive of Packet Payload Length

The main tasks for the MAC layer is to provide interface and protocol for the higher layer, and to deal with the effect of interferences not yet solved by the physical layer. The major anti-jamming techniques in MAC include MAC layer retransmission, carrier sense, and frequency diversity[7-10]. Many WLAN devices employ some retransmission techniques in the MAC. The ordinary one is the break-continue mechanism. Theoretically, retransmission can overcome all types of interference, while other techniques minimize numbers and overhead of retransmissions as possible. However, the repeating interfering packets can hit on all retransmitted packets of a packet, until the MAC layer discards it. The object of carrier sense is that, while a signal or interferer falling to a channel is detected, it halts the transmission of its own signal until the next best time. This method also avoids its interfering on other user signals. Carrier sense multiple access/collision avoidance (CSMA/CA) is a technique based on carrier sense and slot content which can improve the carrier sense information and reduce the effect of collision. But it presents less action on non-CSMA/CA interferers such as Bluetooth frequency hops or other microwave radiation such as from a microwave oven. To minimize the number of packet retransmissions, another anti-jamming technique often used by the MAC layer can change the operating frequencies of the system in order to increase the probability of the devices avoiding interferers. That is, trying to change the frequencies of the packets retransmitted for frequency hopping system; this can be realized by reducting its dwelling time.

Although all these MAC layer techniques have their own values and suitable fields, their drawbacks are also apparent, especially with the increasing of interfering networks, all retransmitted target packet may be destroyed by some repeating interferers until it is discarded by the MAC. From the viewpoint of relations between interferers and signals, and the feature of Bluetooth interferers, the transmission of

interfering packets is not influenced by the target packets being transmitted in the channels. Obviously, the collision probability caused by these interferences is proportional to the payload lengths of the target packets. The results of simulations from above also confirm this conclusion. Although we cannot change the length of IP packets, we can divide a large IP packet into small fragments transmitted separately. When there is no interferer, the fragment length of the target packet is fixed without segmenting. The inherent mechanism of IEEE 802.11 supports the realization of the fragment adaptive of target packet, although most IEEE 802.11 products have not employed it effectively[9]. To realize it, the target packet is transmitted without segmenting so as to minimize the overhead when few or none of the Bluetooth interfering networks are presented. And increasing of Bluetooth interferers, the fragment length of the target packets reduces until they can avoid the interferers and achieve successful transmission between the two bursts of interfering packets. Actually, this scheme employs an adaptive mechanism to reduce the mean value of the overlapping packets of interferers on the target packet so it further reduces the probability of hitting target packets. The scheme makes no assumptions about the attribution of interferers and avoids interference through its own inherent adaptive mechanism completely so that it is applicable to many interference situations.

In the scheme of target packet adaptive fragments, each packet is originally transmitted without segmenting. After each occurrence of transmission failure or collision, the fragment threshold of payload length is divided by two, until the minimum adaptive fragment length is reached. On the other hand, after continually receiving lots of correct packets, the fragment length threshold will be raised to decrease the overland and increase the effective transmission of data. The method for adaptive fragment of target packet is shown in Fig.6.

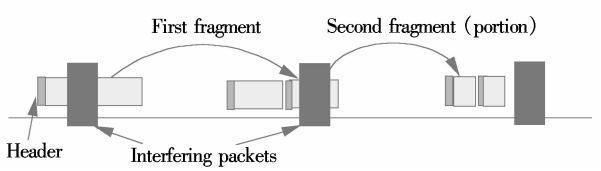

Fig.6 The scheme of adaptive fragment

Interference is not the only cause of transmission failure in IEEE 802.11 networks. In fact, the competition process is frequently the source of collision. The first failure of packet transmission is generally ascribed to competition and the following failures of retransmission are more likely caused by interference. Thus, the more reasonable mechanism is to delay the reduction of fragment length to the time after the second failure of retransmission occurs. Two schemes for reducing fragment threshold after the first and second failures are shown in Tab.1, in which the maximum payload length is 4 096 bytes.

In the next section, the effect on IEEE 802.11 FHSS networks of decreasing fragment length of target packets is analyzed and verified through simulation modeling. The minimum adaptive fragment length of IEEE 802.11 FHSS networks is 512 bytes, that is, the network keeps this payload length even though the target channel is further degenerated by the interferers. The reason behind it is that in this case, the header overhead occupies a significant portion of the packet, and little information is carried. Thus, the benefit from decreasing payload is littler and littler, instead of it, such frequent low data rate transmissions create increasingly interferences to other users. In our simulations, the maximum payload adopted is 4 096 byte and the modulating data rate is 1 Mbit/s, the total number of frequency channels is 79.

Tab.1 Threshold of fragment length

Fail numbers of packet transmission	Scheme 1/byte	Scheme 2/byte
0 — original transmission	4 096	4 096
1 — after first transmission failure	2 048	4 096
1 — after second transmission failure	1 024	2 048
2 — after third transmission failure	512	1 024
3 — after more than 3 transmission failure	512	512

4 The Interference Suppression Performance of Proposed Scheme

Here the effect of Bluetooth interferers on the length of target packets is analyzed through simulations. The results show that the adaptive fragment scheme can effectively decrease collision probability and enhance robustness in the presence of Bluetooth interferers by transmitting target packets within intervals between two interfering bursts.

Fig.7 shows the capacity of IEEE 802.11 FHSS network versus its packet segment length at 1 Mbit/s under different Bluetooth interferers. Five curves with the number of interferers ranging from 1, 4, 8, 16 and 32 are calculated. The results show clearly that the capacity of IEEE 802.11 FHSS network increasing with the increasing of payload length of packets when seldom or none interferers appear. However, with the increasing of Bluetooth interferers, the capacity loss can be substantially reduced by shortening the segment

length and this effect becomes more pronounced with more interferences. For example, when the number of interfering Bluetooth reaches 32, the segment length can be reduced from the maximum allowable 4 096 to 256 bytes so that the capacity can still be maintained at a fairly good value of about 0.2 Mbit/s.

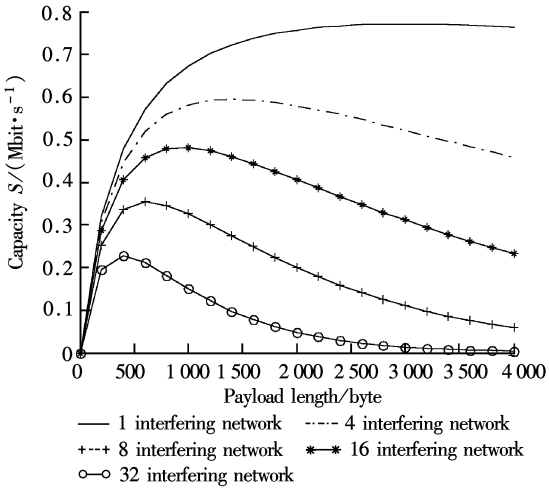

Fig.7 The capacity of IEEE 802.11 FHSS network versus its packet length in the presence of Bluetooth interferers

In fact, for a given number of interfering networks, there exists an optimal fragment length of the target packet. When the fragment length is shorter than this optimal value, the capacity drops rapidly because the header then occupies a significant portion of the packet and such frequent low efficiency transmissions increase interferences with other systems.

5 Conclusion

There are a large amount of devices operated in the 2.4 GHz ISM band, the major standards involved in FHSS technique are Bluetooth and IEEE 802.11 FHSS WLAN. With the increasing number of users, the co-interference between these two types of networks becomes more and more severe so that the network capacity is decreased. In this paper, the capacity model of Bluetooth and IEEE 802.11 FHSS networks is derived by analysis of FHSS network capacity. Simulations show that the capacity reduction of Bluetooth network is smoother in the presence of IEEE 802.11 FHSS interferers because of using short packets. Contrarily, the capacity of IEEE 802.11 FHSS network decreases rapidly in the presence of Bluetooth interferers because of its long packet length mechanism.

The inherent mechanism of IEEE 802.11 WLAN standards can effectively support fragment payload length transmission. A scheme of adaptive fragment of payload is proposed to resist Bluetooth interferers on the basis of the capacity modeling of the FHSS network. Results of analysis and simulation show that the adaptive transmission mechanism can effectively mitigate the capacity reduction of IEEE 802.11 FHSS networks. It is also shown that there exist optimal payload lengths for different Bluetooth interferers to provide optimal capacity.

References

[1] Golmie N, Mouveaux F. Interference in the 2.4 GHz ISM band: impact on the Bluetooth access control performance [A]. In: *IEEE International Conference on Communications* [C]. 2001, **8**: 2540 - 2545.

[2] Fainberg M, Goodman D. Analysis of the interference between IEEE 802.11b and Bluetooth systems [A]. In: *IEEE VTS 54th* [C]. 2002, **2**: 967 - 971.

[3] Howitt I. IEEE 802.11 and Bluetooth coexistence analysis methodology [A]. In: *IEEE VTS 53rd* [C]. 2001,**2**: 1114 - 1118.

[4] Bluetooth SIG. Bluetooth Technology Standard V1.1 [EB/OL]. http://www.bluetooth.com, 2001.

[5] Andrew S, Park R, Buehrer M. Throughput performance of an FHMA system with variable rate coding [J]. *IEEE Trans on Communications*, 1998, **46**(4): 521 - 532.

[6] Bray J, Charles. *Bluetooth: connect without cables* [M]. London: Prentice Hall PTR, 2002.

[7] Jean T. Dwell adaptive fragmentation: how to cope with short dwells required by multimedia wireless LANs [A]. In: *Proceeding of IEEE Global Telecommunications Conference* [C]. 2000, **1**: 57 - 61.

[8] Hedge M V, Stark W E. Capacity of frequency hop spread spectrum multiple access communication systems [J]. *IEEE Trans On Communications*, 1990,**38**(7): 1050 - 1059.

[9] Punnoose R, Tseng R, Stancil D. Experimental results for interference between Bluetooth and IEEE 802.11b DSSS systems [A]. In: *Proceeding 54th IEEE Vehicular Technology conference* [C]. 2001, **1**: 67 - 75.

[10] Stranne A, Floren R, Edfors O, et al. FHSS networks in the presence of strongly interfering Bluetooth networks [A]. In: *Proceeding of the 13th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications* [C]. 2002, **1**: 161 - 165.

WPAN 应用环境下跳频网络干扰分析及其容量改善

叶芝慧[1,2] 沈连丰[1] 宋铁成[1]

([1] 东南大学移动通信国家重点实验室, 南京 210096)
([2] 解放军理工大学通信工程学院, 南京 210016)

摘 要 对无线个域网应用环境下采用跳频方案的蓝牙网络和 IEEE 802.11 FHSS 网络之间的共存性问题进行了研究,通过容量分析和系统仿真,比较了它们的相互影响.在此基础上,提出了采用包负荷长度分段自适应的方法来提高 IEEE 802.11 FHSS 网络的抗干扰性能,并对所提方案进行了分析仿真.结果表明,IEEE 802.11 WLAN 标准的内在机制能够支持本文提出的方法,改善了抗干扰的鲁棒性,并且随着蓝牙干扰网络数量的增加,采用自适应方案的 IEEE 802.11 FHSS 网络的抗干扰性能明显增强,网络容量的下降得到有效缓解.文中所采用的容量分析和包负荷长度分段自适应方案也可以推广到其他 FHSS 网络.

关键词 无线个域网; 跳频; 网络容量; 蓝牙技术; IEEE 802.11 FHSS 网络; 包负荷长度分段自适应
中图分类号 TN914.41