文章编号:1006-2475(2018)10-0101-05

面向 ZigBee 无线传输的跳频扩频技术

郭皓星,闫连山,叶 佳

(西南交通大学信息科学与技术学院,四川 成都 611756)

摘要: ZigBee 技术虽然使设备的快速联网更加方便快捷,但其网络的安全完全依赖于网络密钥并缺乏有效的安全配置选项,导致密钥在设备配对过程中极易泄漏,并因此对用户信息安全造成极大的威胁。本文给出一种基于跳频扩频技术的 ZigBee 传输方法,该方法通过传输过程中载频的不断跳变使得密钥信息无法被跟踪截获,增强了 ZigBee 网络安全性。基于该方法,本文建立了 QPSK 跳频扩频传输系统模型并进行了仿真验证。仿真结果表明,使用跳频扩频技术的 QPSK 无线传输系统具有良好的可靠性。

关键词: ZigBee; 跳频扩频; 安全性; 模型仿真

中图分类号: TP391.9 **文献标识码:** A **doi**: 10.3969/j.issn.1006-2475.2018.10.020

Frequency Hopping Spread Spectrum Based on ZigBee Wireless Transmission

GUO Hao-xing, YAN Lian-shan, YE Jia

(School of Information Science and Technology, Southwest Jiaotong University, Chengdu 611756, China)

Abstract: Although ZigBee technology makes fast networking more convenient, its network security completely depends on the network keys and lacks effective security configuration options, which makes the leak of keys and the lack of user information security. Based on frequency hopping spread spectrum technology, a ZigBee transmission method is proposed, which makes it difficult to track and catch the information of keys and enhances the ZigBee network security. Based on the proposed method, the model of QPSK frequency hopping spread spectrum transmission system is established and verified by simulation. The simulation results show that the QPSK wireless transmission system with frequency hopping spread spectrum technology has a good reliability.

Key words: ZigBee; frequency hopping spread spectrum; security; modeling

0 引 言

近些年由于个人通信设备逐渐普及,短距离通信服务需求也随之增长,使用频率也大大提高,被应用于各种场景,如办公场景、家居场景、医院场景等室内应用场所[1]。作为无线通信的重要组成部分,短距离无线通信技术在可用频段上的多向发展使得无线通信技术可以为人们提供更加多样的服务,方便了人们的工作和生活[1]。

在大多数应用环境中,用户对无线传感器网络的安全性有很高的要求,因此,安全成为制约无线传感器网络进一步广泛应用的关键[1]。2004 年 12 月,ZigBee1.0 标准正式公布,该标准中体现了组网的安全。在此协议中,ZigBee 提供了高可靠性的安全服务[2]。它的安全服务所提供的方法包括密码建立、密码传输、帧保护和设备管理。这些服务构成了一个模块,用于实现 ZigBee 设备的各类安全策略[2]。

随后,针对 ZigBee 的加密算法被广泛研究。文献[3]提出了基于 ZigBee 协议中 AES 加密算法的轮操作和列混淆优化算法,提高了算法运行速度并降低了算法的复杂度,但是并没有实质性地提高加密算法的安全度;文献[4]提出了一种基于 ZigBee 的 MAC 层安全检测算法,用于筛查协议中的安全漏洞,但是该算法只能对协议中的漏洞进行挖掘和检测,并不能对发现的漏洞进行改进和优化;文献[5]提出了一种将 Diffie-Hellman 群组密钥协商协议应用于 ZigBee 网络的方案,该方案减少了 ZigBee 信息传输过程中的密钥交换次数,降低了传输过程中用户被盗取传输密

收稿日期:2018-03-29
基金项目:国家 863 计划项目(2015AA016903)
作者简介:郭皓星(1993-),女,山西太原人,西南交通大学信息科学与技术学院硕士研究生,研究方向:无线传感网络传输优化;闫连山(1971-),男,山东烟台人,教授,博士生导师,研究方向:光通信,物联网,软件定义网络。

钥的可能性，同时针对现有 ZigBee 网络采用对称密钥体制时内存占用过多，加解密过程中密钥查找时延过大及密钥易泄漏等不足，提出采用 RSA 算法的非对称密钥体制 ZigBee 安全改进方案。但是该方案所采用的密钥协议和密钥体制较为复杂，对 ZigBee 无线模块的续航和处理速度有更高的要求，并且在一定程度上降低了 ZigBee 无线模块的传输效率。

这些方案都是基于现有的 ZigBee 安全协议进行加密算法的密钥体制的研究，然而在十多年的发展过程中 ZigBee 的安全协议和密钥体制已较为成熟，很难有有效的突破[6-7]。本文通过对 ZigBee 无线传输过程中的信号传输载频进行跳变控制，在保证传输可靠性的前提下，提高 ZigBee 无线传输的安全性，并避免了繁琐的安全加密算法以及密钥传输处理。这使得在实际应用中，ZigBee 无线传输模块的处理速度不会被复杂的加密过程影响，从而避免传输效率的降低和续航能力的下降。同时，传输方式的变化降低了 ZigBee 无线传输的安全性对于密钥的依赖，并使得信号在传输过程中难以被跟踪捕捉，提高了 ZigBee 无线传输的安全性。最后，本文对 ZigBee 跳频扩频系统中的传输信号性能进行了详细分析。

1 跳频扩频通信系统原理

跳频扩频技术是指通过载波频率在一定的宽频带范围内依照特定图案或序列进行跳变、扩展信息传输所用的频带[8]。载波调制通过伪随机码发生器控制载波频率，使得携带了待传输信息的载波在一个远大于基带带宽 B 的频带内进行随机跳变，从而实现基带信号带宽到载波信号传输带宽的扩展[9]。在跳频扩频通信系统中，可用信道带宽被分割成大量相邻的互不重叠的频带[10]。在任意信号传输时间间隔内，传输信号可以占据多个可用的频隙，按照伪随机码发生器的输出序列随机选择传输频隙。跳频可以看作使用伪随机码序列的频移键控调制。

如图 1 所示，传统跳频系统通常采用 ASK 或 FSK 调制，经过频率发生器产生的扩频载波通过混频与基带信号结合并在信道内传输。在接收端使用同样的扩频载波与接收到的信号进行混频实现解扩，并通过 ASK 或 FSK 解调得到信息序列[8]。本文介绍的面向 ZigBee 传输的跳频扩频传输系统，是在传统跳频系统的基础上，使用了 ZigBee 的传输调制模式，并采用了 m 序列作为控制频率合成的伪随机序列。该系统既保留了跳频过程的随机性又符合 ZigBee 无线传输模型的要求。

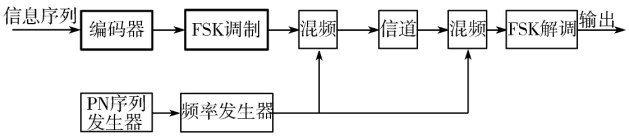

图 1 跳频扩频系统

2 QPSK 跳频扩频仿真系统设计

本方案设计传输情景为 ZigBee 与 Wlan 在同一室内相同视距同时传输[11]。本系统主要分为 5 个部分：信号生成模块、信号发送端、信号接收端、误比特率计算模块、跳频控制子模块。QPSK 跳频扩频系统结构如图 2 所示。

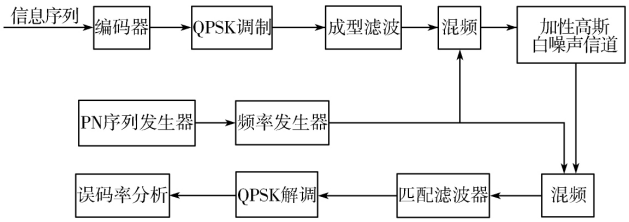

图 2 QPSK 跳频扩频系统

2.1 信号生成模块

信号生成部分采用了随机整数发生器，产生了维度为 10000 的随机 0、1 分布的二进制整数序列。根据调制方式选择每符号的比特数。

2.2 信号发送端

为了模拟 ZigBee 点对点传输的室内传输模型，本方案采用了 QPSK 调制方式[8]。

首先，将生成的随机 0、1 分布的二进制整数序列 bit_in 进行 QPSK 调制，生成 2 列正交序列，得到基带信号 base_QPSK。

由于 Matlab 运行内存分配的问题，在载波调制过程中，对载频进行了降频处理。在保证信号传输质量的前提下，取信号的传输载频为 90 MHz，传输速率取 ZigBee 在 2.4 GHz 频段的理论传输速率[12]，250 kbit/s。使用升余弦滤波器对经过 QPSK 调制的信号进行成型滤波，得到带通信号 QPSK_rc(t)。

由于 ZigBee 的带宽为 2 MHz，而 IEEE 802.11b 的带宽为 22 MHz，是 ZigBee 带宽的 11 倍[13-14]，因此 IEEE 802.11b 在 ZigBee 传输过程中对 ZigBee 的干扰可以认为是限带的加性高斯白噪声信号[13-14]。因此在传输过程中加入高斯白噪声以模拟 WiFi 对于 ZigBee 传输过程中的干扰。

生成一个与 QPSK_rc(t) 时长相等的载频信号，频率 f_c 由伪随机码发生器控制的频率选择器来决定。将待传输的带同信号 QPSK_rc(t) 调制到频率为 f_c 的载波上进行跳频传输。由于 f_c 受到由伪随机码

发生器控制的频率选择器的控制,因此 f_c 有可能因为生成的伪随机码超出选择范围而没有值,设定此种情况下 f_c 值为 1。

$$MixSig(t) = QPSK\_rc(t) \times Carrier(t_c) \quad (1)$$

式(1)中,MixSig(t)表示混频之后的待传输信号,Carrier(t_c)表示由频率发生器产生的跳频载波。

按照 ZigBee 的信道划分为 16 个[13-14],本方案将跳频传输过程设定了 16 次循环。在循环过程中,跳频过程中的扩频载波频率会避开输入的带通信号 QPSK_rc(t)的中心频率来进行频率的跳变,以防止扩频载波对于带通信号的串扰。

2.3　信号接收端

在接收端对扩频载波频率 f_c 以及接收到的信号进行判别和处理。

若 f_c 为 1,则接收端接收到的信号 Sign_rec(t)即等于加了噪声的带通已调信号 QPSK_rc(t)。

若 f_c 不为 1,则将经过信道传输的信号与扩频调制载波相乘进行解扩。

$$Sign\_rec(t) = MixSig(t) \times Carrier(t_c) \quad (2)$$

式(2)中,Sign_rec(t)表示接收端接收到后与跳频载波混频之后进行解扩的信号,MixSig(t)表示混频之后的待传输信号,Carrier(t_c)表示由频率发生器产生的跳频载波。

将解扩出的信号分别与两路正交相位相乘,得到 I_demo(t)和 Q_demo(t)两路经过调制的正交信号,其中,I_demo(t)和 Q_demo(t)中都包含 $4\pi f_1$ 的高频分量,经过匹配滤波将这 2 个高频分量滤除之后再合成即可得到最佳接收信号 match_demo,然后将匹配滤波得到的信号 match_demo 进行 QPSK 解调,得到经过跳频扩频传输接收的码元序列,并进行误比特判决和计数。

2.4　误比特率计算模块

在对接收信号 match_demo 进行 QPSK 解调之后得到接收到的比特序列 re_base。将比特序列 re_base 与信号发送端输入的待传输序列 bit_in 进行对比,并对错误的比特位进行计数。

将比较后得到的不同比特位数存入 n_error 变量中,然后将总误比特数与传输的总比特数相除,得到本次传输的误比特率。

2.5　跳频控制子模块

为了保证跳频序列的随机性,本方案使用了自相关性良好的伪随机码生成跳频序列[7-12]。

如图 3 所示,跳频控制子模块主要分为 3 个部分,分别是基带信号中心频率输入部分、伪随机序列生成部分和载波频率生成部分。该模块的具体运行流程如下:首先使用 5 位线性移位寄存器 m 序列发生器生成一个 m 序列。采用的生成多项式为:

$$f(x) = 1 + x^2 + x^5 \quad (3)$$

然后将生成的伪随机序列整形为一个 31 × 5 的矩阵 PNSeq,用 5 位伪随机码表示 1 ~ 31 之间的十进制整数,并通过数值运算得到一个 1 × 31 的十进制整数序列 reg。

为了对应 ZigBee 传输中的信道间隔,设置了 16 个间隔 df 为 5 MHz 的频点。之后按照时钟频率每循环一次取出一个之前运算得到的随机十进制整数序列 reg 中存放的随机数,并进行判定。若该随机数在 16 ~ 31,则与输入的带通信号 QPSK_rc(t)的中心频率 f_1 进行数值运算,得到跳频点 SaveFrq,否则,SaveFrq 为 1。

$$SaveFrq = f_1 + (num - 16) \times df \quad (4)$$

式(4)中,SaveFrq 表示频率产生器输出的跳频频率,df 表示每个跳频频率之间的频率间隔,df 取值 5 MHz,num 表示从随机整数序列 reg 中取出的随机数,f_1 表示待传输信号的基带频率。

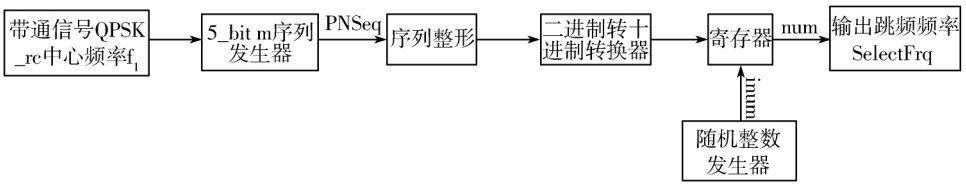

图 3　伪随机序列跳频发生器

3　系统性能分析

3.1　实验参数设置与波形

为了获取足够多的样本数量,并提高仿真计算效率,使用随机数发生器产生 100000 个数据点,分 10 次进行循环模拟,如图 4 所示。

将随机序列分成 I、Q 两路之后,使用中心频率 f_1 为 100 MHz 的载波进行载波调制,如图 5 所示。传输码率采用 ZigBee 的理论传输速率 250 kbps。上采样频率 f_s 为载波频率的 5 倍,采样间隔 dt 为 $1/f_s$。成型滤波使用升余弦滤波器,滚降系数取为 0.25。

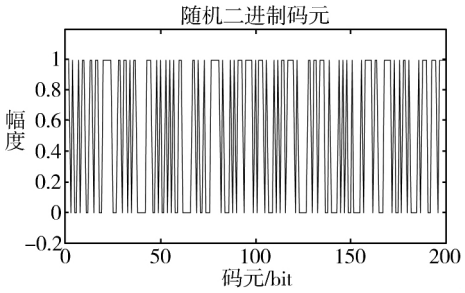

图 4 随机序列发生器产生的信号

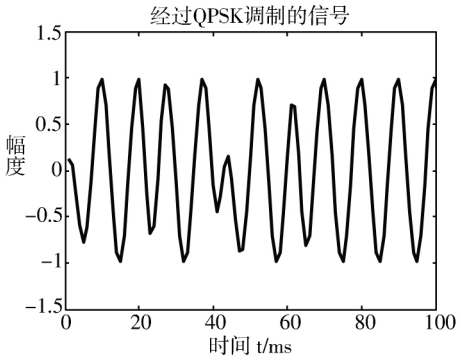

图 5 QPSK 调制信号

为了模拟传输过程中 WiFi 对于 ZigBee 干扰影响，本方案在传输信道对传输信号进行了高斯白噪声的叠加。由于 WiFi 和 ZigBee 的信道分布有部分重叠，因此在设计信道的噪声叠加时，在跳频传输模式下的高斯白噪声只在 3/4 数量的信道上进行了叠加。同时，为了测量跳频扩频传输对于传输误比特率的影响，取 EbNo 为 0 dB ~ 10 dB，进行测量比较。

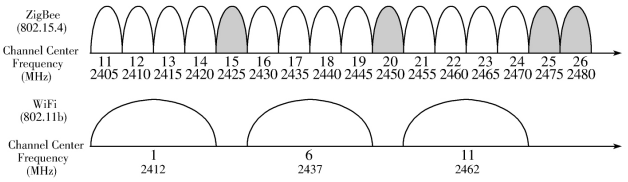

图 6 ZigBee 和 WiFi 的信道分布图

将加入噪声的信号调制到扩频载波上，已调信号的时域波形如图 7 所示。跳频时的扩频载波采用从跳频频率选择器返回的频率数值 SaveFrq 作为中心频率 f_c。其中，f_c 的取值范围为 100 MHz ~ 180 MHz，共 16 个频点，每个频点相隔 5 MHz[15]。接收端对接收到的信号进行解扩，解扩后信号的时域波形如图 8 所示。

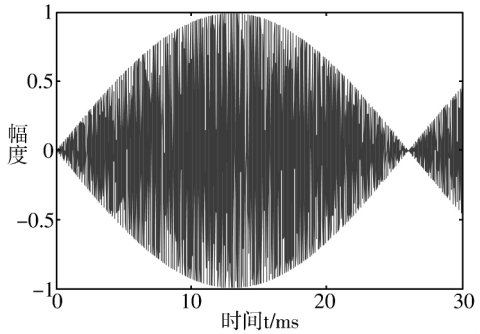

图 7 调制到扩频载波上的已调信号

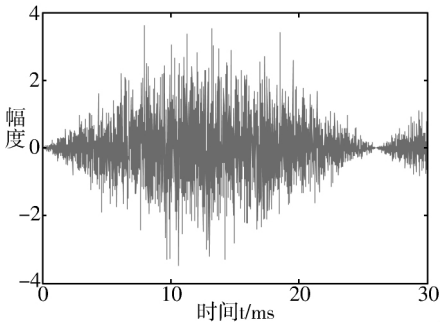

图 8 解扩信号

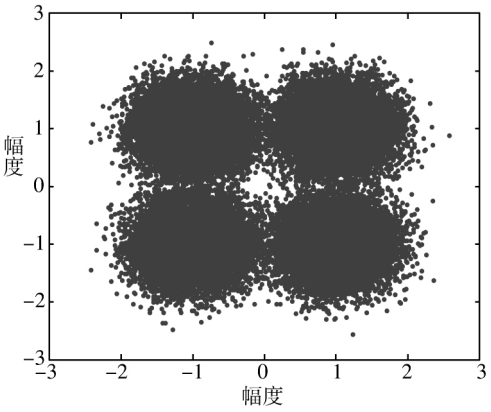

图 9 经过滤波解调后的 QPSK 信号

在进行信号接收时，考虑到 ZigBee 在传输过程中的信道冲突检测以及跳频过程中的信道切换时间，设置平均传输时延为 8 ms，并在接收端进行匹配滤波时对接收时钟进行校准调整。对滤波得到的带通信号 match_demo 进行 QPSK 解调，并对序列进行抽样判决。原序列和解调后序列如图 10 所示。

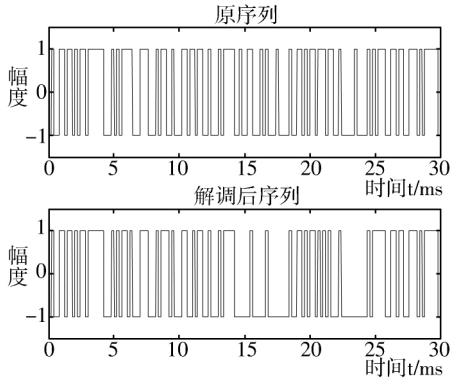

图 10 解调之后得到的码元序列

3.2 误比特率分析

为了分析跳频扩频传输对于 ZigBee 信号传输准确性的影响，本方案采用误比特率来进行评估。令 P_b 表示误比特率(Bit Error Rate，BER)，P_b 可以表示为：

$$P_b = Q\left(\sqrt{\frac{2Eb}{No}}\right) \tag{5}$$

其中，

$$Q(x)=\frac{1}{\sqrt{2\pi}}\int_x^{\infty}\exp\left(-\frac{u^2}{2}\right)du \tag{6}$$

假设信号传输的信道为加性高斯白噪声信道，Eb 表示接收端接收到的每 bit 信息的平均能量，No 表示接收端所接收到的噪声功率谱密度。

本方案在信号接收时采用了匹配滤波，为了提高同步精度，需要较高的采样点数。因此在计算信噪比时采用的是上采样信噪比的计算方式，在 EbNo 的基础上去掉调制方式和采样率对于信噪比的影响，得出的结果较为准确[16]。

$$SNR=EbNo+10\times\lg(k)-10\times\lg(rate) \tag{8}$$

其中，EbNo 表示 Eb/No。Eb 表示单位比特的能量，单位是 J。No 表示功率谱密度，单位是 W/Hz。SNR 表示 S/R，S 表示信号功率，单位是 W，N 表示噪声功率，单位是 W。rate 是信号的采样率，k 是调制阶数。

由于跳频传输过程中，传输载频会发生多次变化，可能会导致与基带信号发生串扰或者在调制过程中产生误码，为了分析跳频传输对于系统传输误比特率的影响，本方案将无跳频 QPSK 仿真误比特率与有跳频 QPSK 仿真误比特率进行比较。由图 11 可以看出，在跳频 QPSK 传输情况下，仿真误比特率与无跳频传输误比特率基本一致。因此，跳频传输可以在保证传输抗截获能力的基础上不影响系统的传输性能。

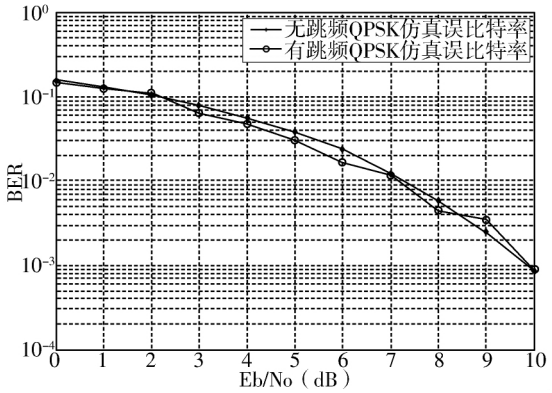

图 11　QPSK 误比特率分析

在无跳频情况下，使用安全密钥进行 ZigBee 传输时，只要获取当前空闲信道序号即可追踪到待传输的信号，获取到待传输信息的安全密钥，即可截获待传输的数据信息。而在跳频扩频系统模型下传输，由于跳频序列良好的伪随机性则无法通过获取当前空闲信道序号对待传输信号的信道编号进行截获。

4　结束语

本文以受到 802.11b 干扰的 ZigBee 传输模型为基础，给出了一种面向 ZigBee 无线传输的跳频扩频传输方案。使用 QPSK 调制方式对跳频扩频传输进行建模及仿真，并对传输误比特率进行了计算分析。在加入跳频扩频传输之后，传输误比特率与普通的 QPSK 传输仿真误比特率基本一致，说明跳频扩频传输在 QPSK 传输过程中并不会影响系统传输性能。同时，利用伪随机序列在不同频点之间的跳变，使得外部对于 ZigBee 信息的截取和捕捉变得更加困难，从而提高了 ZigBee 信息传输的安全性。

参考文献:

[1] 廖建名. 面向无线多媒体传感器网络 ZigBee 协议栈的分析与优化[D]. 北京:北京邮电大学, 2014.
[2] 李妤薇. 基于 ZigBee 的无线传感器网络协议研究与设计实现[D]. 南京:南京邮电大学, 2014.
[3] 张亚琳. 物联网中基于 ZigBee 协议的安全算法研究[D]. 广州:华南理工大学, 2012.
[4] 李景. 针对 ZigBee 协议 MAC 层安全的综合检测算法[D]. 北京:北京邮电大学, 2013.
[5] 王真. 基于矩阵概率检验的 ZigBee 协议安全检测方法研究[D]. 焦作:河南理工大学, 2015.
[6] 吴绍宏. ZigBee 安全体系结构及密钥分布关键技术研究[D]. 郑州:解放军信息工程大学, 2014.
[7] VIDGREN N, HAATAJA K, PATIÑO-ANDRES J L, et al. Security threats in ZigBee-enabled systems: Vulnerability evaluation, practical experiments, countermeasures, and lessons learned[C] // 2013 46th Hawaii International Conference on System Sciences. 2013: 5132-5138.
[8] 牛宪华. 跳频扩频序列理论与设计[D]. 成都:西南交通大学, 2012.
[9] CHANG C S, YANG G C, CHIANG M H, et al. Construction of synchronous-symmetric channel-hopping sequences over Galois extension field for cognitive radio networks[J]. IEEE Communications Letters, 2017, 21(6): 1425-1428.
[10] SHIH C F, XHAFA A E, ZHOU J. Practical frequency hopping sequence design for interference avoidance in 802.15.4e TSCH networks[C] // IEEE International Conference on Communications. 2015: 6494-6499.
[11] 朱晨. WLAN 对 ZigBee 传感器网络的干扰问题研究[D]. 济南:山东大学, 2017.
[12] 樊鹏博. 基于空间应用的 ZigBee 抗干扰协议的研究[D]. 西安:西安电子科技大学, 2015.
[13] 房发成. 短距离无线通信的干扰模型及共存方案设计[D]. 南京:南京邮电大学, 2014.
[14] 边玮. 基于 ZigBee 的多信道干扰避免研究与应用[D]. 呼和浩特:内蒙古大学, 2017.
[15] 陈艳萍. ZigBee 与 IEEE802.11b 的干扰问题研究[D]. 北京:北京邮电大学, 2013.
[16] MAGABLEH A M, JAFREH N. Exact expressions for the bit error rate and channel capacity of a dual-hop cooperative communication systems over Nakagami-m fading channels[J]. Journal of the Franklin Institute, 2018, 355(1): 565-573.