ZigBee同频攻击检测抑制模型研究

郁 滨 周伟伟*
(解放军信息工程大学 郑州 450001)

摘 要：针对ZigBee通信中易遭受同频攻击导致数据阻塞和失真问题，该文提出一种同频攻击检测模型。该模型利用信号频谱的高斯分布规律和同频攻击对变换域幅值的影响进行同频攻击检测。在此基础上，通过嵌入空闲频带信道跳变机制和基于可变退避周期及接入概率的自适应退避算法，给出了同频攻击检测抑制方案。实验结果表明，该文模型和方案可以有效抵御同频攻击。

关键词：信息安全；ZigBee；直接序列扩频；载波监听多路访问/冲突避免；同频攻击
中图分类号： TP309.1 **文献标识码**： A **文章编号**：1009-5896(2015)09-2211-07
DIO: 10.11999/JEIT141395

Co-channel Attack Detection and Suppression Model for ZigBee Network Nodes

Yu Bin Zhou Wei-wei
(*The Information Engineering University of PLA*, *Zhengzhou* 450001, *China*)

Abstract: Co-channel attack may cause data blocking and distortion in ZigBee networks. To resolve the issues, a model to detect co-channel attack is proposed. According to the Gauss distributed characteristics of the signal spectrum and the influence of co-channel attack on transform-domain amplitude, the proposed model can perceive whether the co-channel attack is existent in ZigBee network. On this basis, a scheme to detect and restrain co-channel attack is provided by embedding the free band channel-hop mechanism and self-adaption algorithm based on variable backoff cycle and access probability. Finally, experimental results indicate that the proposed model and scheme can inhibit the co-channel attack efficiently.

Key words: Information Security; ZigBee; Direct Sequence Spread Spectrum (DSSS); Carrier Sense Multiple Access with Collision Detection (CSMA/CA); Co-channel attack

1 引言

ZigBee无线信道的开放性使得攻击者可以释放大量同频干扰信号对ZigBee网络攻击破坏。MAC层网络帧传输采用传统的载波监听多路访问/冲突避免(CSMA/CA)[1–3]和直接序列扩频(DSSS)机制[4]，两者分别可以解决多节点的信道复用和宽频带传输问题。但是，CSMA/CA信道虚假检测和DSSS无法检测抑制同频攻击等缺陷使得节点数据阻塞或出现信号失真。目前，针对同频攻击的抑制技术主要分为时域同频攻击抑制和变换域同频攻击抑制。

时域同频抑制技术主要有3种[5–8]：第1种是对网络中数据的流量控制，如针对WLAN网利用AP站点同频宽带高增益信号对ZigBee的干扰问题，Hong等人[5]提出了一种基于集中流量控制理论的ZigBee抗同频干扰算法，该算法通过在两者之间建立共享服务器控制数据收发的流量，最大限度地避免数据冲突和干扰，保证在低误码率条件下数据吞吐量达到最优，但由于集中流量控制是在已知干扰可控情况下对网络实施的强制管控，该方法并不适用于存在恶意攻击的未知网络环境。第2种是对接收信号当前样本值进行线性预测，然后从实际采样的样本值中减去预测样本值[6,7]，该方案在扩频信号功率远远小于同频攻击信号功率时有效，但当扩频信号功率大于同频攻击信号时，其非高斯性会使自适应滤波器的稳定性和收敛速度明显下降。第3种是在扩频信号功率和同频攻击信号功率相当时，从采样观测数据中消除对扩频信号分量的估计，同时对当前样本值进行预测[8]，但该方法并不适用于扩频信号功率远远小于同频信号功率的情况。

变换域同频抑制主要包括基于子带变换和滤波器组的抑制技术[9]。变换域可以将时域滤波中的卷积转化为频域的积分相乘，解决时域无法实现的理想带通和带阻滤波等问题[10]。文献[11]提出了变换域中

2014-10-31收到，2015-01-30改回，2015-05-11网络优先出版
河南省科技攻关项目(132102210003)资助课题
*通信作者：周伟伟 1099471246@qq.com

的抗同频攻击基本理论架构，为抗同频攻击机制的研究奠定了基础，但并未给出如何在硬件和协议栈中实现抗同频攻击的具体方案。依据该抗同频攻击架构，在变换域中引入加窗离散傅里叶变换(DFT)可以减小信号变换后的频谱泄漏，但会使期望信号产生一定的失真[12]。针对期望信号的失真问题，利用延迟并行重叠加窗机制可以减小加窗对信噪比削弱的影响，但计算量成倍增加，影响系统的效能[13,14]。基于以上变换域信号处理机制，文献[15]提出了 ZigBee 马尔可夫链数值模型，定量分析了同频攻击对 ZigBee 通信的影响和频域的变化规律，指出同频攻击与 ZigBee 信号在带宽、变换域频幅特性等方面的差异性，但并未解决同频攻击的检测问题。

上述同频抑制技术均建立在同频攻击存在的基础上，缺乏根据网络受干扰程度自适应调整抗同频攻击的策略，增加了 ZigBee 通信的系统开销并影响网络通信性能。

本文结合 CSMA/CA, DSSS 扩频机制及同频攻击与 ZigBee 信号叠加后在频幅上的变化规律，提出一种基于幅值特性的同频攻击检测模型并设计了实现方案。最后，实验对比了在不同网络环境下本文方案与其他同频抑制方案的抗同频攻击性能。

2 MAC 层抗干扰机制分析与改进

在 MAC 层，DSSS 扩频机制中数据接收的误码率受载波信号功率谱密度、干扰和噪声信号功率谱密度的影响。ZigBee 接收端的误码率与扩频比 L 及扩频功率 P_{S} 成正相关，调节 L 和 P_{S} 可以增强系统的抗同频攻击能力。与此同时，同频攻击信号使频带重叠并导致 CSMA/CA 机制中数据冲突的概率增加，如何改进 CSMA/CA 和信道切换机制成为抑制同频攻击的关键。

2.1 信道切换机制研究

由于 ZigBee 未考虑同频攻击对数据传输的影响，网络中采用固定信道通信，当信道受到强窄带同频攻击时会产生严重干扰。改进后的信道切换机制完成由同频攻击干扰转换为邻频攻击干扰，其原理如图 1 所示。

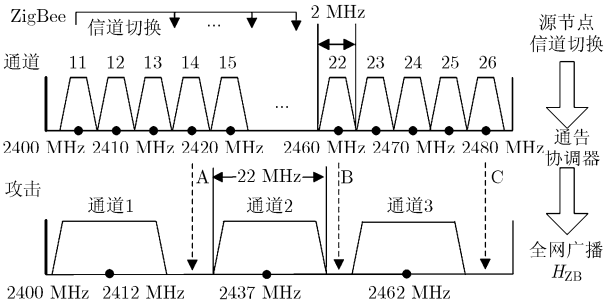


图 1 ZigBee 信道切换机制

信道切换机制无法抑制全频带的同频攻击，需要协议栈调用其他抑制措施。当 MAC 层侦测到图 1 所示的非全频带同频攻击时，调用信道切换机制在信道 11 与信道 26 之间跳变，跳变信道的中心频率为 $H_{\mathrm{ZB}}=2405+5(D_1 \bmod 16)$，$H_{\mathrm{ZB}}\in(2405,2480)$，其中 D_1 为硬件平台生成的随机数因子。切换后的信道频带与攻击信号 1~3 重叠时，重新调用上述跳变机制直到切换至如图虚线 A, C 所示的频段，由于空闲频带 B 并未完全覆盖信道 20, 21，信道切换机制将不会切换至 B 频段。

跳变节点信道切换成功后，等待与协调器建立连接，信道同步流程如图 2 所示。

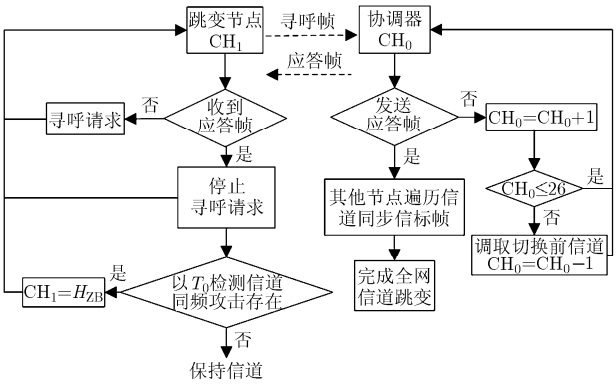


图 2 信道同步流程

当跳变节点切换至信道 CH_1 时，节点向协调器发送寻呼帧。协调器定时查询是否收到跳变节点的寻呼帧，若收到寻呼帧则向跳变节点返回应答帧，同时向全网发送同步信标帧。若未收到寻呼帧，则在信道 11 与信道 26 之间遍历，当收到寻呼帧时，将携带当前信道 CH_0 跳变信息的信标帧向全网广播。其他节点通过遍历信道同步信标帧，完成信道切换。经过固定周期 T_0 对网络状态重新检测，若受到同频攻击，则执行信道跳变；若未受到同频攻击，则保持当前信道。

2.2 CSMA/CA 抗干扰性改进

ZigBee 节点执行空闲信道扫描(CCA)时，由于同频攻击干扰和网络其他节点的虚假检测，各网络节点同时向信道发送数据，导致节点间数据阻塞。设计可变退避周期并依据不同概率接入信道，信道检测和数据发送流程如图 3 所示。

BE 为初始化退避指数，NB 为退避次数，CW 为发送窗，L_0 为信道能量指示表征的信道质量。虚线框中为接入机制的改进措施，改进后的 CSMA/CA 重新设置退避周期 T 并加入信道 CCA 检测概率 p_{AC}，退避周期 T 为

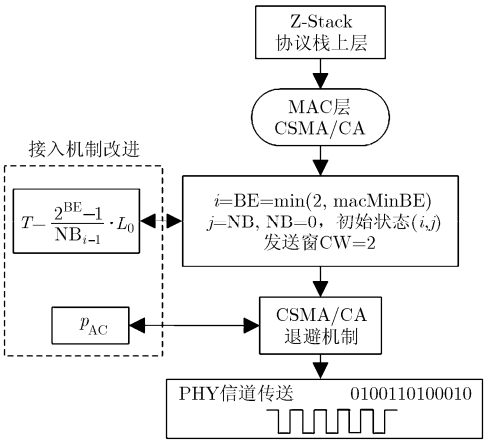


图 3　CSMA/CA 改进算法的帧发送流程

$$T=\frac{2^{\mathrm{BE}}-1}{\mathrm{NB}_{i-1}}\cdot L_0 \tag{1}$$

如式(1)所示，将 T 与退避指数 BE 、上一次的退避次数 NB_{i-1} 和信道质量 L_0 关联，则退避周期相同的概率为 $p_T=p_{\mathrm{BE}}\cdot p_{\mathrm{NB}_{i-1}}$。BE 和 NB_{i-1} 两者都相同时才会导致发送的退避周期相同，节点可通过上一次的退避次数来自适应地调整本次的退避时间。L_0 反映了信道当前发送数据的成功率和受干扰程度，将 L_0 与 T 绑定可以提高数据发送的效率。

当信道两次 CCA 检测通过时会立即进入帧发送模式。如果两个节点在退避周期相同时仍会出现同时占用信道的情况，导致数据阻塞。因此，在两次成功执行 CCA 检测后信道均空闲时，以概率函数 $p_{\mathrm{AC}}=H(\mathrm{Ad}\oplus D)$ ($0<p_{\mathrm{AC}}<1$) 接入信道，其中 $H(\cdot)$ 为单向杂凑函数，Ad 为 ZigBee 64 bit 硬件地址，D 为 CC2530 的随机数生成器生成的随机数。在接入信道前的时隙中增加信道接入概率可以大大减少同时检测到信道空闲所引起的数据帧干扰和冲突。

针对外部攻击干扰，本文设计自适应退避算法的 CSMA/CA 网络同步机制如图 4 所示。

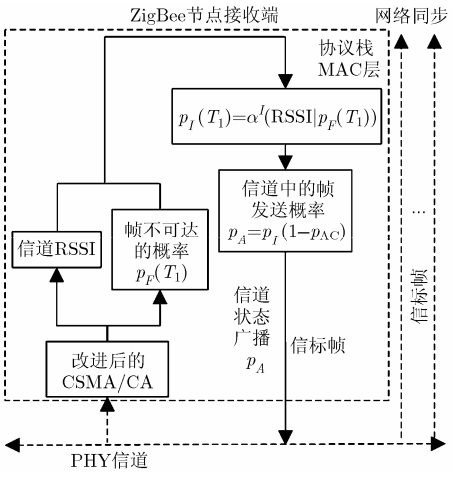


图 4 自适应退避算法的 CSMA/CA 网络同步机制

由于 ZigBee 通信采用消息应答机制，当节点未收到响应帧时，则发送数据帧阻塞。以周期 T_1 统计发送数据帧不可达的概率 $p_F(T_1)$ ，并与信道中实时信道的能量检测状态 RSSI 相结合，得出信道在网外同频攻击下的受干扰程度 $p_I(T_1)$。当 CCA 检测确定信道空闲时，为保证帧接入概率 p_A 依据网络受干扰程度进行自适应调整，设置 $p_A=p_I\cdot(1-p_{\mathrm{AC}})$。

ZigBee 各网络节点同步由协调器向全网广播的信标帧， CSMA/CA 依据该信道接入概率实时调整，同时配合反映退避指数和退避次数的退避周期 T，减小网内和网外同频攻击导致数据帧阻塞的概率。

3　同频攻击检测模型

同频攻击信号与 ZigBee 信号在频域的叠加破坏了原有信号幅值的高斯分布规律，使叠加后的信号频谱超出了原有信号的最大幅值。通过分析 DSSS 扩频机制中的时频域信号处理流程，同时利用 DSSS 的扩频特性和变换域定量分析计算实现对该幅值的求解。基于此，结合 ZigBee 信号处理特点设计同频攻击检测流程。

3.1 信号处理与分析

利用 ZigBee 中 DSSS 扩频信号各频域子带的线性无关性以及幅值满足高斯分布规律特性，将同频攻击的检测问题转化为对攻击干扰信号所引入的频域幅值变化的检测和判定，信号处理与分析流程如图 5 所示。

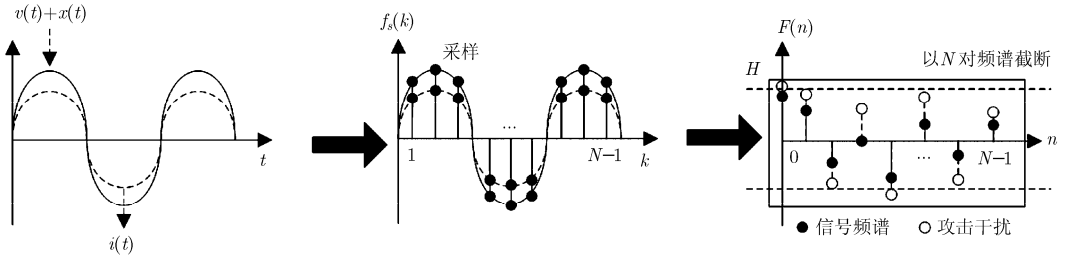
$v(t)$ 为噪声信号，$x(t)$ 为载波信号，$i(t)$ 为攻击信号，$f_s(k)$ 为采样信号，THD 为同频攻击检测门限值。初始信号 $f(t)$ 经 A/D 转换后采样生成信号序列 $f_s(k)$。如图 5(b)，截断后的信号序列包含 N 个采样点，对该序列周期扩展。经过归一化中心频率分别为 $f=2\pi n/N(n=0,1,\cdots,N-1)$ 的线性滤波器组处理后，其子带的离散频谱取样值 $F(n)$ 为信号频谱和攻击干扰的线性叠加。由于同频攻击对频域幅值特性的影响，可以通过信号的频域分析和计算，实现对 THD 的求解。

3.2 模型变换域门限值求解

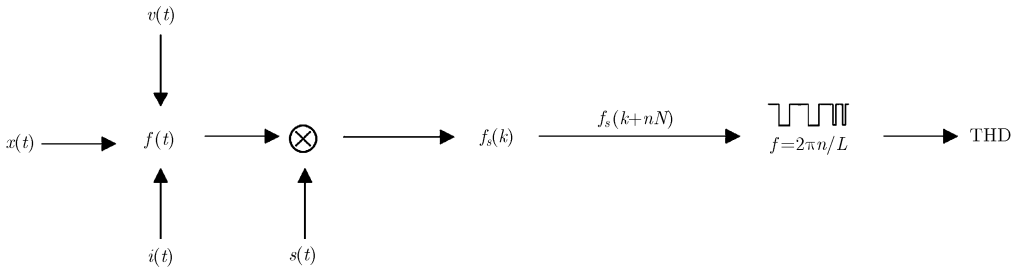
设输入信号为第 n 个截断信号序列，由于每个截断信号序列包含 N 个采样点，则该输入信号为

$$\boldsymbol{s}'(n)=[s(nN),s(nN+1),\cdots,s(nN+N-1)]^{\mathrm{T}} \tag{2}$$

令 $x=\mathrm{e}^{-2\pi j/N}$，$S_P(n)$ 是第 P 个子带的输出信号，则 $N-1$ 个子带的 DFT 输出为



(a)传输信号 (b)采样信号 (c)频域截断信号



(d)同频攻击检测

图 5 信号处理与分析流程图

$$\begin{bmatrix} S_0(n) \\ S_1(n) \\ \vdots \\ S_{N-1}(n) \end{bmatrix} = \frac{1}{\sqrt{N}} \begin{bmatrix} x^0 & x^0 & x^0 & \cdots & x^0 \\ x^0 & x^{1*1} & x^{2*1} & \cdots & x^{(N-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x^0 & x^{1*(N-1)} & x^{2*(N-1)} & \cdots & x^{(N-1)*(N-1)} \end{bmatrix} \cdot \begin{bmatrix} s(nN) \\ s(nN+1) \\ \vdots \\ s(nN+N-1) \end{bmatrix} \tag{3}$$

由式(3)可得，第 P 个子带的输出信号为

$$S_P(n) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} s(nN+k) \cdot x^{kp},\ p \in [0, N-1] \tag{4}$$

由扩频机制中 P 子带的扩频分量输出满足零均值高斯分布特性，故均值 $\sum_{k=0}^{N-1} \mathrm{E}\{s(nN+k)\} = 0$，由式(4)可得 P 子带的 DFT 分量均值输出为

$$\begin{aligned} \overline{S_P(n)} &= \mathrm{E}\{S_P(n)\} \\ &= \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \mathrm{E}\{s(nN+k)\} \cdot x^{kp} = 0 \end{aligned} \tag{5}$$

$S_P(n)$ 的方差为

$$\begin{aligned} \delta^2\{S_P(n)\} &= \frac{1}{N} \sum_{n=0}^{N-1} \left(S_P(n) - \overline{S_P(n)} \right)^2 \\ &= R_{S_{P_1}(n) S_{P_2}(n)} \\ &= \frac{1}{N} \sum_{a=0}^{N-1} \sum_{b=0}^{N-1} R_{s(nN+a)s(nN+b)} x^{(a-b)p} \end{aligned} \tag{6}$$

其中 a,b 为任意两次信号采样，$R_{S_{P_1}(n) S_{P_2}(n)}$ 为 $S_P(n)$ 的自相关函数。由 ZigBee 调制通信中各子带采样的不相关性可得任意两次采样的相关函数：

$$R_{s(nN+a)s(nN+b)} = P_{\mathrm{S}} \delta(a-b) \tag{7}$$

其中 $\delta(\cdot)$ 为单位冲激函数，P_{S} 为扩频功率，将式(7)代入式(6)，得

$$\delta^2\{S_P(n)\} = \frac{1}{N} \cdot N \cdot P_{\mathrm{S}} \delta(0) = P_{\mathrm{S}} \tag{8}$$

不同扩频子带 P 和 Q 的相关函数为

$$\begin{aligned} R_{S_P(n) S_Q(n)} &= \left(\frac{1}{\sqrt{N}} \right)^2 \cdot \sum_{a=0}^{N-1} \sum_{b=0}^{N-1} R_{s(nN+a)x^{ap} \cdot s(nN+b)x^{bq}} \\ &= \frac{1}{N} \cdot \sum_{a=0}^{N-1} \sum_{b=0}^{N-1} R_{s(nN+a) \cdot s(nN+b)} \cdot x^{ap-bq} \\ &= \frac{P_{\mathrm{S}}}{N} \cdot \sum_{a=0}^{N-1} x^{b(p-q)} = P_{\mathrm{S}} \delta(p-q) \end{aligned} \tag{9}$$

当 $p \neq q$ 时，由冲激函数的性质，式(9)为零，即不同扩频子带完全不相关。

假设同频攻击对 ZigBee 射频硬件部分影响较小，则噪声干扰分量为

$$V_P(n) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} v(nN+k) \exp(-\mathrm{j}2\pi kp / N) \tag{10}$$

由噪声干扰服从标准高斯分布，且高斯噪声的方差为 σ_V^2，可得噪声干扰分量的均值和方差为

$$\begin{aligned} \mathrm{E}\left\{V_P(n)\right\} &= \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \mathrm{E}\{v(nN+k)\} \\ &\quad \cdot \exp(-\mathrm{j}2\pi kp / N) = 0 \end{aligned} \tag{11}$$

$$\delta^2\left\{V_P(n)\right\}=\frac{1}{N}\sum_{n=0}^{N-1}\left(V_P(n)-\mathrm{E}\left\{V_P(n)\right\}\right)^2$$
$$=R_{V_{P_1}(n)\cdot V_{P_2}(n)}$$
$$=\sum_{a=0}^{N-1}\sum_{b=0}^{N-1}\sigma_V^2\cdot\delta(a-b)=\sigma_V^2 \qquad (12)$$

其中 $R_{V_{P_1}(n)\cdot V_{P_2}(n)}$ 为 $V_P(n)$ 的自相关函数。

由于通信信号和噪声信号均服从标准高斯分布，因此在不受同频攻击干扰时，输入信号的幅值 $\left|f_s(n)\right|=\left|S_P^{'}(n)+V_P(n)\right|$ 服从参数为 δ^2 的瑞利分布，而通信信号和噪声信号完全不相关，故 $\delta^2=\delta^2\{S_P^{'}(n)\}+\delta^2\{V_P(n)\}=P_{\mathrm{S}}+\sigma_V^2$。将瑞利分布幅值变换后，即 $\left|f_s(n)\right|^2=\left|S_P^{'}(n)+V_P(n)\right|^2$，则 $\left|f_s(n)\right|^2$ 服从参数 $\theta=1/2\delta^2=1/2(P_{\mathrm{S}}+\sigma_V^2)$ 的指数分布。指数分布中存在概率密度接近于零的临界点，可以利用该临界点作为检测同频攻击的门限值。本方案中设检测同频攻击的门限值为 THD，则由指数分布的概率分布求解：

$$p\left(\left|f_s(n)\right|^2<\mathrm{THD}\right)=1-\int_{\mathrm{THD}}^{+\infty}\theta\mathrm{e}^{-\theta x}\mathrm{d}x$$
$$=1+\mathrm{e}^{-\theta x}\mid_{\mathrm{THD}}^{+\infty} \qquad (13)$$

为便于计算，令 $\mathrm{THD}=\lambda/\theta$，则不同频谱幅值的概率分布如表 1 所示。

由概率表可知，在无同频干扰的情况下，仅受高斯噪声干扰的影响，频域内信号的幅度低于门限值 $\mathrm{THD}=6/\theta$ (即 $\lambda=6$)的概率为 0.99753，即频谱在不受同频攻击下幅值不超过 $6/\theta$。当 MAC 层检测到幅值超出 $6/\theta$ 时，网络遭受同频攻击。由以上分析，可将 MAC 层消息接收的同频攻击检测门限值设置为 $\mathrm{THD}=3/(P_{\mathrm{S}}+\sigma_V^2)$。

4　同频攻击检测抑制方案

依据本文提出的同频攻击检测模型，结合第 2 节中的同频攻击抑制措施，设计 ZigBee 同频攻击检测抑制方案如图 6 所示。

H 为是否受到同频攻击的参数，CH_1 为节点重新选择的信道。无线信号首先由接收端 MAC 层解扩并完成波形解调，计算最大幅值 $\mathrm{THD}^{'}$ 是否大于同频攻击检测门限值 THD。若小于 THD，则调用传统的 CSMA/CA 退避机制；若大于 THD，则由高频滤波器对高频幅波形裁切，将处理后的数据信号交付协议栈上层。由于滤波器不能完全滤除同频攻击干扰在解调时所形成的杂波，当节点检测到有同频攻击存在时发送端需要增大系统扩频比 L 扩展频谱所占的带宽，同时增强扩频信号的发射功率 P_{S} 以减小对有用信号的干扰。利用信道切换机制减小与同频攻击的频带重叠区域，自适应算法的 CSMA/CA 同步机制在全网中以固定周期同步更新可以及

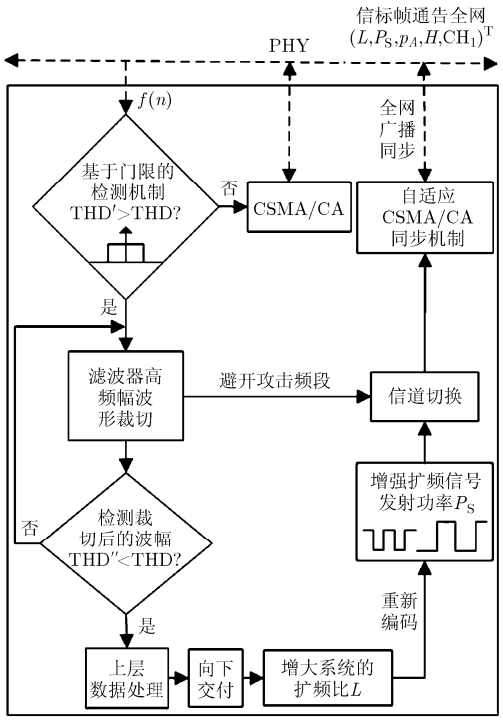


图 6 同频攻击检测抑制方案

时地评估信道受同频攻击干扰的程度，自适应地调整帧接入机制。$(L,P_{\mathrm{S}},p_A,H,\mathrm{CH})^{\mathrm{T}}$ 以信标帧的形式向全网广播完成网络节点参数更新和信道切换。

5　实验与结果分析

为验证本文提出方案的性能，在 ZigBee 硬件平台和 Z-Stack 固件中实现了同频攻击检测抑制方案，同时利用频谱分析仪和 CC2531 USB dongle 对本文方案和其他方案进行测试分析。

实验 1　不同方案的同频攻击抑制性能测试

通过频谱分析仪对采用不同方案的数据信号进行测试，如图 7 所示。

图 7(a)中在同频攻击条件下，采用正常扩频机制时，频域内信号完全被同频攻击干扰破坏。图 7(b)，图 7(c)与图 7(a)相比，对同频攻击信号抑制作用较明显，但缺乏对频带边缘的干扰抑制。图 7(d)可有效辨别信号并抑制同频攻击干扰，在边缘部分的波形恢复效果优于图 7(b)，图 7(c)。因此，相对于其他同频抑制方案，本文方案在频带边缘波形恢复上有优势。

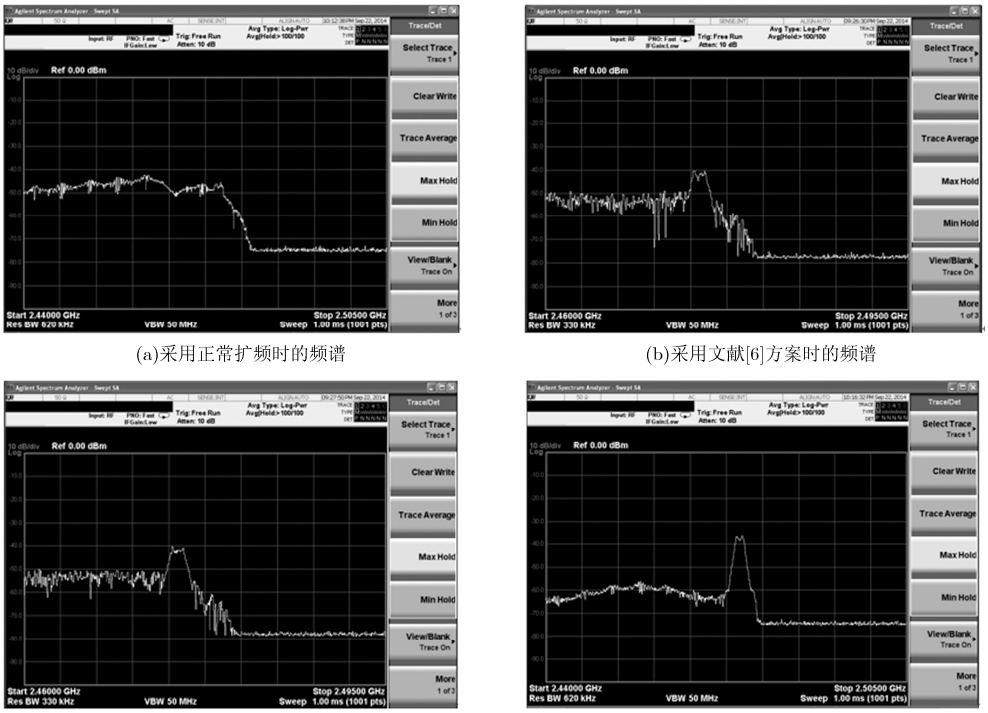
实验 2　自适应算法的 CSMA/CA 机制测试

在不同信道质量条件下由 package sniffer 对数据包解析和统计。在不同信噪比(SNR)和退避算法条件下的曲线特性如图 8 所示。

在同频攻击条件下，原 ZigBee 方案在信噪比较小时误码率较大，而当信噪比增大时，误码率变化曲线较平缓，仍保持在较大的范围内，严重影响

表 1 不同频谱幅值的概率分布

λ	1	2	3	4	5	6
p	0.63212	0.86467	0.95021	0.98169	0.99327	0.99753



(a)采用正常扩频时的频谱　(b)采用文献[6]方案时的频谱

(c)采用文献[12]方案时的频谱　(d)采用本文方案时的频谱

图 7 扩频功率特性频谱实验结果

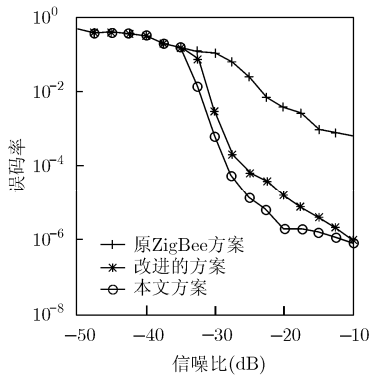


图 8 信噪比与误码率特征曲线

ZigBee 节点的正常通信；采用本文不考虑信道受干扰程度的改进方案在一定程度上减小了误码率，当信噪比高于−35 dB 时有明显的优势；本文优化后的方案误码率最低，但当信噪比高于−10 dB 时优化效果减弱。上述关系曲线表明，本文方案在原有协议基础上提高了网络的抗同频攻击性能。

6 结束语

本文在深入研究 DSSS 扩频和 CSMA/CA 机制的基础上，建立了基于频谱门限值的同频攻击检测模型，给出了门限值的计算公式，提出了一种 ZigBee 同频攻击检测抑制方案。相对于其他 ZigBee 干扰抑制方案，本文方案在网络遭受同频攻击时能及时检测并采取自适应手段抑制攻击信号对帧传输的影响。实验结果表明，本文模型和方案能有效检测抑制同频攻击。

参 考 文 献

[1] Wu Shan-shan, Mao Wen-guang, and Wang Xu-dong. Performance study on a CSMA/CA-based MAC protocol for multi-user MIMO wireless LANs[J]. *IEEE Transactions on Wireless Communications*, 2014, 13(6): 3153–3166.

[2] Tang Chong, Song Li-xing, and Balasubramani J. Comparative investigationon CSMA/CA-based opportunistic random access for internet of things[J]. *IEEE Internet of Things Journal*, 2014, 1(2): 171–179.

[3] Shrestha B, Hossain E, and Choi Kae-won. Distributed and centralized hybrid CSMA/CA-TDMA schemes for single-hop wireless networks[J]. *IEEE Transactions on Wireless Communications*, 2014, 13(7): 4050–4065.

[4] Spuhler M, GiustinianoD, and Lenders V. Detection of

reactive jamming in DSSS based wireless communications [J]. *IEEE Transactions on Wireless Communications*, 2014, 13(3): 1593–1603.

[5] Hong Kun-ho, Lee Su-kyoung, and Lee Kyoung-woo. Performance improvement in ZigBee-based home networks with coexisting WLANs[J]. *Pervasive and Mobile Computing*, 2014, 3(2): 1174–1192.

[6] Yang Wei-jun, Zhang Chao-jie, and Jin Xiao-jun. Adaptive median threshold algorithm used in FDIS of DSSS receivers [J]. *Journal of Systems Engineering and Electronics*, 2013, 24(1): 11–18.

[7] Poor H V. Active interference suppression in CDMA overlay system[J]. *IEEE Journal on Selected Areas in Communications*, 2001, 19(1): 4–20.

[8] Milstein L B. Interference suppression to aid acquisition in dirence-sequence-spread-spectrum communications[J]. *IEEE Transactions on Communications*, 1988, 36(11): 1200–1207.

[9] 李冲泥, 胡光锐. 利用基于滤波器组的重叠变换抑制扩频通信系统中的时变干扰[J]. 通信学报, 2001, 22(4): 26–29.
Li Chong-ni and Hu Guang-rui. Non-stationary interference excision in spread spectrum systems using the filter-bank based lapped transform[J]. *Journal on Communications*, 2001, 22(4): 26–29.

[10] 李冲泥, 陈豪, 胡光锐. 扩频通信中的自适应干扰抵消技术[J]. 空间电子技术, 1998(3): 47–51.
Li Chong-ni, Chen Hao, and Hu Guang-rui. The adaptive interference-cancellation technology in spread spectrum communication[J]. *Space Electronic Technology*, 1998(3): 47–51.

[11] Jones W W and Jones K R. Narrow band interference suppression using filter-bank analysis/synthesis techniques [C]. IEEE Military Communication Conference, San Diego, 1992: 898–902.

[12] 陈茉莉, 李舜酩, 饶新阳. 基于时域特征识别微频差信号[J]. 仪器仪表学报, 2012, 33(6): 1234–1239.
Chen Mo-li, Li Shun-ming, and Rao Xin-yang. Micro frequency difference signal identification based on time domain characteristics[J]. *Chinese Journal of Scientific Instrument*, 2012, 33(6): 1234–1239.

[13] 曾祥华, 李峥嵘, 王飞雪. 扩频系统频域窄带干扰抑制算法加窗损耗研究[J]. 电子与信息学报, 2004, 26(8): 1276–1281.
Zeng Xiang-hua, Li Zheng-rong, and Wang Fei-xue. Study on windowing degradation of frequency-domain narrowband interference suppression algorithms in spread spectrum system[J]. *Journal of Electronics and Information Technology*, 2004, 26(8): 1276–1281.

[14] Capozza P T, Holland B J, and Hopkinson T M. A single-chip narrow-band frequency-domain excisor for a Global Positioning System(GPS) Receiver[J]. *IEEE Journal of Solid-State Circuits*, 2000, 35(3): 401–411.

[15] Masry E. Closed-form analytical results for the rejection of narrow-band interference in PN spread-spectrum systems — Part I: linear prediction filters[J]. *IEEE Transactions on Communications*, 1984, 32(8): 885–896.

郁　滨： 男，1964 年生，教授，博士生导师，主要研究方向为无线网络安全和电磁防护.

周伟伟： 男，1990 年生，硕士生，主要研究方向为 ZigBee、信息安全技术.