电波科学学报
Chinese Journal of Radio Science
中文核心期刊要目总览
• 中国科技核心期刊
• 中国科学引文数据库（CSCD）
• 中国科技论文与引文数据库（CSTPCD）
• 中国学术期刊文摘数据库（CSAD）
• 中国学术期刊（网络版）（CNKI）
• 中文科技期刊数据库
• 万方数据知识服务平台
• 中国超星期刊域出版平台
• 国家科技学术期刊开放平台
• 荷兰文摘与引文数据库（SCOPUS）
• 日本科学技术振兴机构数据库（JST）

基于干扰认知的索引调制跳频抗干扰方法

施育鑫，李玉生，安　康

Index modulation based frequency hopping spread spectrum assisted with jamming cognition

SHI Yuxin, LI Yusheng, and AN Kang

在线阅读 View online: https://doi.org/10.12265/j.cjors.2022208

施育鑫, 李玉生, 安康. 基于干扰认知的索引调制跳频抗干扰方法[J]. 电波科学学报, 2023, 38(5): 757-763+852. DOI: 10.12265/j.cjors.2022208
SHI Y X, LI Y S, AN K. Index modulation based frequency hopping spread spectrum assisted with jamming cognition[J]. Chinese journal of radio science, 2023, 38(5): 757-763+852. (in Chinese). DOI: 10.12265/j.cjors.2022208

基于干扰认知的索引调制跳频抗干扰方法

施育鑫[1,2] 李玉生[1*] 安康[1]
(1. 国防科技大学第六十三研究所, 南京 210007; 2. 国防科技大学电子科学学院, 长沙 410000)

摘 要 为了提升无线通信的抗干扰能力, 应对样式更加多样的干扰攻击, 提出了一种基于干扰认知的索引调制跳频抗干扰方法. 合法发射机利用被认知的干扰信号所在的频点与活跃频点、静默频点的相互关系, 以进一步选择三种应对策略: 利用干扰、反制干扰或无需措施. 相比传统的索引调制跳频方法, 本文方法是一种更加灵活和有效的抗干扰手段. 此外, 推导了基于干扰认知索引调制跳频方法的误比特率近似闭式表达式, 所推导的理论分析结果与仿真结果拟合很好, 验证了理论分析的准确性. 相比传统的索引调制跳频方法, 所提方法能够有效提升误比特率性能, 从而提升系统的抗干扰能力.

关键词 索引调制; 干扰认知; 跳频; 抗干扰; 策略
中图分类号 TN918.4 **文献标志码** A **文章编号** 1005-0388(2023)05-0757-07
DOI 10.12265/j.cjors.2022208

Index modulation based frequency hopping spread spectrum assisted with jamming cognition

SHI Yuxin[1,2] LI Yusheng[1*] AN Kang[1]
(1. *The Sixty-third Research Institute, National University of Defense Technology, Nanjing* 210007, *China*; 2. *College of Electronic Science and Technology, National University of Defense Technology, Changsha* 410000, *China*)

Abstract In order to improve the anti-jamming capability of wireless communication and cope with interference attacks with more diverse jamming patterns, this paper proposes an index modulation based frequency hopping spread spectrum (IM-FHSS) method assisted with jamming cognition. In this method, the legitimate transmitter uses the interrelationship among the frequency point of recognized jamming signal, the active frequency point and the idle frequency point, to select "exploit jamming", "counteract jamming" or "no measures required" three kinds of strategies. Compared with the traditional index modulation based frequency hopping spread spectrum method, it is a more flexible and effective anti-jamming method. In addition, this paper derives an approximate closed-form expression for the bit error rate of the jamming cognition assisted IM-FHSS method. The simulation results show that the derived theoretical analysis fits well with the simulation results, which demonstrates the accuracy of the theoretical analysis. Moreover, the proposed method can effectively improve the bit error rate performance compared with the conventional IM-FHSS method, which effectively improves the anti-jamming capacity of the system.

Keywords index modulation; jamming cognition; frequency hopping; anti-jamming; strategy

0 引 言

无线信道的开放性, 使得合法通信信号极易受到各类有意和无意干扰的攻击[1]. 在有意干扰中, 无线信道中的恶意干扰方旨在阻止合法通信方访问无线信道资源, 破坏合法用户的可用性. 为了解决这一

收稿日期: 2022-09-21
资助项目: 国家自然科学基金 (U19B214, 61901502, 62201593); 军委科技委基础加强计划 (2019-JCJQ-JJ-212, 2019-JCJQ-JJ226); 人力资源与社会保障部博士后创新人才计划 (BX20200101); 国防科技大学校科研计划 (18-QNCXJ-029)
通信作者: 李玉生 E-mail: lys63s@163.com

问题，跳频扩频 (frequency hopping spread spectrum, FHSS) 被视为抗干扰通信的有效方法，得到广泛研究. FHSS 使用秘密的跳频图案来确定可用的频点，从而躲避干扰信号.

最近，反应式干扰器被认为是一种聪明而有效的方法，它只针对数据包的接收进行干扰[2]. 与主动干扰器相比，由于实际场景中数据包投递率 (packet delivery ratio, PDR) 是未知的，因此很难检测到反应式干扰器的存在[3]. 文献 [4] 指出利用低成本的软件定义无线电 (software defined radio, SDR)，可以为生成反应式干扰提供多种应用配置. 因此，在潜在的快速反应式干扰的严重威胁下，跳频通信采取的频点逃逸策略面临着现实挑战.

受到索引调制概念[5-7] 的启发，针对反应式干扰，文献 [8] 中提出了一种新型的跳频通信系统，称为基于索引调制跳频扩频 (index modulated based FHSS, IM-FHSS). 不同于频移键控中用于传输信号的频点位置相邻，在索引调制跳频通信中，用于传输信号的频点各自由相互正交的跳频图案决定. 当待传输比特确定后，即选定一组跳频图案的索引，根据该索引确定跳频图案活跃频点位置并输入能量. 在接收端，合法通信方通过比较所有跳频图案的频点能量关系来恢复比特信息. 注意到，采用反应式干扰的干扰方只跟踪并攻击活跃频点，以高效地攻击通信信号. 由于反应式干扰只攻击具有能量的频点，而活跃频点受到攻击时能量仍然显著大于其他静默频点，因此索引调制的跳频方法能够通过在反应式干扰中保持能量关系的不变性，从而具备了更强的抗干扰能力.

在文献 [9] 中，考虑了一种更具挑战性的反应式干扰，称为功率相关的反应式干扰. 功率相关的反应式干扰通过协作的干扰机获取功率信息，再调整干扰信号功率以达到能量抵消的效果. 通过功率优化算法设计，文献 [9] 给出了针对功率相关的反应式干扰的反制策略. 在文献 [10] 中，考虑了一种星座旋转的索引调制跳频方法，使得干扰者难以实现功率相关干扰，并同时实现了信息的安全传输.

然而，在现实干扰场景中，干扰方往往具有多种可选的干扰样式. 除了反应式干扰，还有例如单音干扰、多音干扰、部分频带干扰等定频干扰[11]. 在面对定频干扰的攻击时，传统 IM-FHSS 仅能效仿一般的跳频系统采取的策略，例如采取扩大跳频图案中的频点数、加大功率、删除被干扰频点等常规抗干扰措施，这些措施需要较高的能量代价或频谱资源代价，抗干扰的效率较低.

针对定频干扰的攻击，本文提出了一种基于干扰认知的 IM-FHSS 方法，有效地提升了 IM-FHSS 的抗干扰能力. 本文主要贡献如下：

1) 本文首次考虑了在干扰样式信息被认知条件下，IM-FHSS 的发射机在定频干扰下的反制策略. 针对定频干扰可能产生的三类情况，采取了利用干扰、反制干扰和无需调整三种应对策略. 相比传统的 IM-FHSS，本文方法提高功率、增加跳频带宽付出的代价更小.

2) 针对所提出的基于干扰认知的 IM-FHSS，给出了详细的性能理论分析. 具体的，本文推导了基于干扰认知的 IM-FHSS 在单频点攻击下的误比特率 (bit error rate, BER) 的近似闭式表达式. 同时，理论推导很容易扩展到多频点被攻击的情况.

3) 仿真结果表明，所推导的 BER 近似闭式表达式能够很好地拟合仿真结果，表明了理论分析的正确性. 同时，相比传统的 IM-FHSS，基于干扰认知的 IM-FHSS 能够在高信噪比 (signal noise ratio, SNR) 条件下有效改善 BER 性能，具备更强的抗干扰能力.

1 传统的 IM-FHSS 与系统模型

1.1 IM-FHSS 的基本结构

IM-FHSS 是一种具有抗反应式干扰能力的跳频方法，首先简要介绍其系统模型. 假设在每跳时间需要发送 m bit 信息，因此每跳需要使用的频点数为 $M=2^m$. 可用的频点是由 M 个相互正交的跳频图案决定的，并且这些图案是由伪随机序列得到的，干扰方无法获取. 随后，根据所发送的 m bit 信息，发射机从 M 个跳频图案确定的 M 个可用频点中选择一个频点作为活跃频点并调制符号，而其他 $M-1$ 个频点被设置为零，称为静默频点.

图 1 给出了 IM-FHSS 的时频示意图，其中 $M=4$，跳频图案中一共有 K 个频点. 由于 4 个跳频图案相互正交，因此跳频图案选择的 4 个频点不会发生重叠. 在发射机工作时，考虑 $m=2$ bit，并假设发送的信号为'00'，代表符号被调制在第 1 个跳频图案决定的频点上. 由于本文仅考虑抗干扰设计，该活跃频点上调制的符号能够传输的额外信息不在考虑范围内.

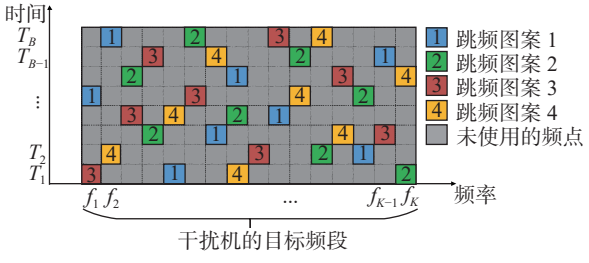

图 1 IM-FHSS 的时频示意图

Fig. 1 Time-frequency diagram of IM-FHSS

在接收机中，从 M 个可用频点获得的采样信号在高斯白噪声信道下可以用以下方式表示：

$$y(k)=\begin{cases} y_{\mathrm{A}}=\sqrt{E}x(k)+n_{\mathrm{A}}(k), \text{活跃频点} \\ y_{\mathrm{I}}^{(i)}=n_{\mathrm{I}}^{(i)}(k), \text{静默频点} \end{cases} \tag{1}$$

式中：$y(k)=y(t=kT)$表示第 k 个跳变时隙上的采样信号；$x(k)$表示被调制的符号；E 表示发射机的发射功率；$n_{\mathrm{A}}(k)$和$n_{\mathrm{I}}^{(i)}(k)$分别表示活跃频点和第 i 个静默频点上的加性高斯白噪声 (additive white Gaussian noise, AWGN)，$i=1,2,...,M-1$. 随后，利用能量最大似然 (energy maximum likelihood, EML) 检测器[8] 对 M 个收到的信号通过能量区分活跃频点和静默频点. 不失一般性，在某一接收时隙检测出的活跃频点可以表示为

$$\hat{y}_{\mathrm{A}}(k)=\arg\max\left\{|y_1(k)|^2,\ |y_2(k)|^2,\ ...,\ |y_M(k)|^2\right\} \tag{2}$$

式中，$y_i(k)$ 表示第 i 个可用频点的采样信号. 由于接收方具有相同的跳频图案，因此$\hat{y}_{\mathrm{A}}(k)$ 在跳频图案中的索引被用来恢复 m bit. 注意到，由于静默频点隐藏在大多数未使用的频点上，因此反应式干扰器无法追踪和干扰静默频点. 同时，反应式干扰信号在一般情况下很难清除活跃频点的能量，因此 IM-FHSS 中使用的 EML 检测器可以有效区分活跃频点和静默频点，IM-FHSS 可以抵御大部分的反应式干扰.

1.2　通信系统模型

图 2 给出了干扰场景下的通信系统模型. 其中，合法通信基站与合法接收方在合法链路上进行通信，而干扰方通过侦察链路获取通信信号的所在工作频点、调制方式等参数. 在干扰链路上，干扰方以提高 BER、中断合法通信为干扰目的，针对合法接收机使用的目标频段发送干扰信号.

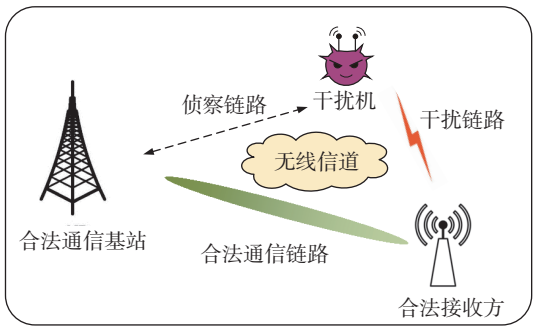

图 2　干扰场景下的通信系统模型

Fig. 2　Communication system model in jamming scenario

假设在第 k 个时刻，干扰方在特定的频点上发送干扰信号，表达式为

$$J(k)=\beta\exp(\mathrm{j}\Delta\theta)z(k) \tag{3}$$

式中：β和$\Delta\theta$分别表示干扰信号与合法通信信号在合法接收机处的幅度差异和相位差异；$z(k)$具有与$x(k)$相同的调制样式，例如当采用 BPSK 时有$x(k)=\pm1$, $z(k)=\pm1$. 当该干扰信号被调制至合法通信工作频段中的某一固定频点时，即形成定频干扰.

2　基于干扰认知的 IM-FHSS 策略

2.1　干扰认知

在传统的 IM-FHSS 中，未充分考虑如何认知并反制定频干扰，常规的手段是加大发射功率以及增加跳频带宽. 尽管跳频通信系统天然存在通过频点跳跃抗定频干扰的能力，但是仅通过扩大跳频带宽和增大功率的方式将付出较大的通信代价，抗干扰效能低. 并且，由于定频干扰只在某些时隙才能击中一部分通信信号的频点，认知发射机应该只在干扰信号攻击通信信号的时隙才需增强其发射功率. 可见，采用盲目的抗干扰策略将造成频谱和能量上的额外开销与浪费.

为了解决这一问题，一种有效的方式是利用基于“认知”的抗干扰策略. 对于干扰的认知，文献 [11] 提出利用数据驱动的方式训练干扰识别器，实现了对单音干扰、多音干扰、部分频带干扰等定频干扰的识别. 文献 [12] 详细论述了通信干扰的样式检测与参数估计. 其中，针对干扰参数的估计问题提出了功率谱滤波降噪法，对待估计的功率谱进行平滑处理，并通过门限设定等方式估计干扰的中心频率与带宽[12]. 此外，在实际干扰场景下通信信号与干扰信号混合，对干扰的样式识别与参数估计造成一定困难. 但由于合法通信方了解跳频信号在频点上的具体位置，因此可以通过一定预处理减少通信信号的影响. 综上所述，在实际干扰场景下对定频干扰的识别与参数估计是可行的.

在干扰认知环节，假设合法基站通过侦察链路获取了干扰样式，这里主要考虑定频干扰，并获取了干扰信号所在的频点. 由于认知了干扰信号的样式与干扰参数，可以获取的关键信息为下一个通信时隙干扰信号的所在频点. 活跃频点和静默频点是由信息比特和跳频图案共同决定的，这些待传输的信息比特和跳频图案是发射机已知的信息. 因此已经认知了定频干扰信号的发射机在传输前还拥有干扰信号将攻击活跃频点或静默频点的详细信息.

2.2　干扰反制策略

在本小节中，将讨论定频干扰下基于认知的 IM-FHSS 策略的两种情况：第一种情况比较特殊，干扰功率显著高于发射机的最高功率，从而完全破坏了被攻击的频点，因此两个合法用户都应该删除被攻击的频点以降低误码率；第二种更为普遍的情况是，定频干扰对目标频点仅使用有限的干扰功率，意味

着发射功率可以大于干扰功率,提供了高效抗干扰、利用干扰信号的机会,这也是本文研究的重点.

基于干扰认知的抗干扰策略可以分为以下三类情况进行讨论:

1) 干扰利用策略. 当活跃频点受到干扰信号的攻击时,干扰者可以被视为合作者. 在这里,IM-FHSS 发射机可以不发送任何信号,仅利用干扰信号来传输信息比特.

2) 干扰反制策略. 当静默频点受到持续的干扰信号攻击时,干扰者被视为非合作者. 合法的发射机需要提高活跃频点上的发射功率以抵抗干扰信号的影响.

3) 无需调整措施. 当前可用的频点在下个时隙不会被干扰攻击时,即干扰信号与通信信号正交,此时通信方无需采取任何措施.

具体来说,在第一类情况,即活跃频点被攻击时,此时发射机未在活跃频点上发射信号,而是利用干扰信号协助传输信号. 合法接收方在某一时隙接收的信号可以表示为

$$y(k)=\begin{cases} y_{\mathrm{A,D}}=J(k)+n_{\mathrm{A}}(k) \\ y_{\mathrm{I}}^{(i)}=n_{\mathrm{I}}^{(i)}(k) \end{cases} \tag{4}$$

式中,$y_{\mathrm{A,D}}$表示在活跃频点上的接收信号.

在第二类情况,即静默频点受到干扰攻击的情况下,不失一般性,假设第 j 个静默频点被攻击,接收的信号可以表示为

$$y(k)=\begin{cases} y_{\mathrm{A}}(k)=\sqrt{E_{\mathrm{a}}}x(k)+n_{\mathrm{A}}(k), \text{活跃频点} \\ y_{\mathrm{I,J}}^{(j)}(k)=J(k)+n_{\mathrm{I}}^{(j)}(k), \text{被攻击的空闲频点} \\ y_{\mathrm{I}}^{(i)}(k)=n_{\mathrm{I}}^{(i)}(k), \text{其他空闲频点} \end{cases} \tag{5}$$

式中,E_{a}表示发射机用于反制干扰信号的发射功率. 假设发射机允许的最大发射功率为$E_{\max}$,为了充分反制干扰,可以令$E_{\mathrm{a}}=E_{\max}$.

表 1 总结了基于认知的发射机策略实施的完整过程.

表 1 基于认知的 IM-FHSS 发射机策略

Tab. 1 Transmitter strategy of cognition-based IM-FHSS

输入: 当前的活跃频点f_{A},定频干扰存在的状态ϕ_{CJ},当前定频干扰的频点f_{J},允许的最大发射功率$E_{\max}$,初始发射信号$x(k)$
While $\phi_{\mathrm{CJ}}=1$ do
If $f_{\mathrm{J}}=f_{\mathrm{A}}$, then
$x'(k)=0$
End If
If $f_{\mathrm{J}}\in F_{\mathrm{I}}$, then
$E_{\mathrm{a}}=E_{\max}$
$x'(k)=\sqrt{E_{\mathrm{a}}}x(k)$
End If
End While
输出: 最终传输信号$x'(k)$

在此之前,假设当前静默频点的集合为 $F_{\mathrm{I}}=\{f_{\mathrm{I}}^{(1)},\ldots,f_{\mathrm{I}}^{(M-1)}\}$,其中$f_{\mathrm{I}}^{(i)}$表示第 i 个静默频点. ϕ_{CJ}表示定频干扰是否位于 M 个可用频点的逻辑状态,这是通过干扰认知后获取的信息. $\phi_{\mathrm{CJ}}=1$表示干扰位于可用频点上,即居于第一类与第二类情况.

3 性能分析

在本节中,给出基于干扰认知的 IM-FHSS 的 BER 性能分析. 在干扰信号的攻击下,存在三种情况: 1) 无可用频点被攻击; 2) 活跃频点被攻击; 3) 静默频点被攻击. P_{N}, P_{A}, P_{I}分别表示上述三种情况下的错误概率. 假设干扰落入了合法通信信号的目标频段,由干扰信号引入的错误比特可以用以下方式表示:

$$\varepsilon=\begin{cases} \rho_M P_{\mathrm{N}}, \text{发生概率为}\dfrac{K-M}{K} \\ \rho_M P_{\mathrm{A}}, \text{发生概率为}\dfrac{1}{K} \\ \rho_M P_{\mathrm{I}}, \text{发生概率为}\dfrac{M-1}{K} \end{cases} \tag{6}$$

式中,ρ_M 表示错误检测发生时的平均错误比特; K 表示跳频图案中所有频点的数量; M 表示每个跳频传输时隙的可用频点数量 (也即跳频图案数量). 则 BER 可表示为

$$P_{\mathrm{BER}}=\frac{\bar{\varepsilon}}{\log_2 M} \tag{7}$$

式中,$\bar{\varepsilon}$表示每个传输时隙的平均误比特数,

$$\bar{\varepsilon}=\frac{\rho_M}{K}(P_{\mathrm{A}}+P_{\mathrm{I}}(M-1)+P_{\mathrm{N}}(K-M)) \tag{8}$$

接下来,推导P_{N}、P_{A}与P_{I}的闭式表达式. 没有可用频点被攻击的情况下,AWGN 信道下的某一时隙接收信号可以表示为

$$y(k)=\begin{cases} y_{\mathrm{A}}=\sqrt{E}x(k)+n_{\mathrm{A}}(k), \text{活跃频点} \\ y_{\mathrm{I}}^{(i)}=n_{\mathrm{I}}^{(i)}(k), \text{空闲频点} \end{cases} \tag{9}$$

不失一般性,假设$x(k)=1$, 接收信号可以进一步表示为$\mathrm{Re}(y_{\mathrm{A}})$, 并且$\mathrm{Re}(y_{\mathrm{A}})\sim\mathcal{N}\left(\sqrt{E},\sigma^2/2\right)$. 根据文献[8]中的公式,可以构造出服从非中心 F 分布的随机变量:

$$T_{\mathrm{R}}=\left|\frac{\mathrm{Re}(y_{\mathrm{A}})}{\mathrm{Re}(y_{\mathrm{I}})}\right|^2\sim\mathrm{F}(n_1,n_2,\delta_{\mathrm{R}}) \tag{10}$$

式中: n_1和n_2表示分子、分母上随机变量的自由度,并且$n_1=1$、$n_2=1$; δ_{R}表示非中心 F 分布的非中心参数,

$$\delta_{\mathrm{R}}=\frac{n_1\times\mathbb{E}(\mathrm{Re}(y_{\mathrm{A}}))}{\mathrm{var}(\mathrm{Re}(y_{\mathrm{A}}))}=\frac{E}{\sigma^2/2} \tag{11}$$

式中,$\mathbb{E}(\cdot)$与$\mathrm{var}(\cdot)$分别表示求随机变量的均值和方差.

考虑 $M=2$, 此时错误检测概率可以表示为 $P_{\mathrm{r}}(T_{\mathrm{R}}<1)=\psi_1(\delta_{\mathrm{R}})$, 其中$\psi_1(\delta)$表示$\psi_1(1,1,1,\delta)$的简化

表示形式, $\psi(l,n_1,n_2,\delta)$表示自由度为n_1和n_2的非中心F分布的累计分布函数在l处的取值. 这里显然有$l=1$.

当$M\geqslant 2$时, 错误检测概率表示活跃频点信号能量小于$M-1$个静默频点信号能量事件的并集, 可以表示为

$$\begin{aligned}P_{\mathrm{N}}&=P_{\mathrm{r}}\left(\bigcup_{M-1}^{i=1}\left(\left|\frac{\mathrm{Re}(y_{\mathrm{A}})}{\mathrm{Re}(y_1^{(i)})}\right|^2<1\right)\right)\\&=1-P_{\mathrm{r}}\left(\bigcap_{M-1}^{i=1}\left(\left|\frac{\mathrm{Re}(y_{\mathrm{A}})}{\mathrm{Re}(y_1^{(i)})}\right|^2>1\right)\right)\\&\approx 1-(1-\psi_1(\delta_{\mathrm{R}}))^{(M-1)}\end{aligned}\tag{12}$$

式中: ∪和∩分别表示逻辑或、逻辑与操作; $\psi(l,n_1,n_2,\delta)$表达式为[13]

$$\psi(l,n_1,n_2,\delta)=\sum_{j=0}^{\infty}\frac{\left(\frac{\delta}{2}\right)^j}{j!}\exp\left(-\frac{1}{2}\delta\right)\mathrm{I}\left(\frac{n_1 l}{n_2+n_1 l}\middle|\frac{n_1}{2}+j,\frac{n_2}{2}\right)\tag{13}$$

$$\mathrm{I}(x|z,w)=\frac{1}{\mathrm{B}(z,w)}\int_0^x t^{z-1}(1-t)^{w-1}\mathrm{d}t\tag{14}$$

表示不完全贝塔函数, $\mathrm{B}(z,w)=\int_0^1 t^{z-1}(1-t)^{w-1}\mathrm{d}t$表示贝塔函数. 将$n_1=1$、$n_2=1$和$\delta=\delta_{\mathrm{R}}$代入上述式子, 可得

$$\mathrm{B}(z_1,w_1)=\frac{1}{j+\frac{1}{2}}\tag{15}$$

式中: $z_1=\frac{n_1}{2}+j$; $w_1=\frac{n_2}{2}$. 由于$\psi_1(\delta)$中$n_1=1$、$n_2=1$、$l=1$, 可以得到$x_1=\frac{n_1 l}{n_2+n_1 l}=\frac{1}{2}$. 将式 (15) 与$x_1=\frac{1}{2}$代入式 (14), 并通过必要的数学运算, $\psi_1(\delta)$中的不完全贝塔函数可以简化为

$$\mathrm{I}(x_1|z_1,w_1)=\left(\frac{1}{2}\right)^{j+\frac{1}{2}}\tag{16}$$

将式 (16) 代入式 (13), 可得

$$\psi_1(\delta_{\mathrm{R}})=\sum_{j=0}^{\infty}\frac{\left(\frac{\delta_{\mathrm{R}}}{2}\right)^j}{j!}\exp\left(-\frac{\delta_{\mathrm{R}}}{2}\right)\cdot\left(\frac{1}{2}\right)^{j+\frac{1}{2}}\tag{17}$$

再将式 (17) 代入式 (12), 即得到P_{N}的闭式表达式.

其次, 当活跃频点被干扰信号攻击时, 根据前述所采取的策略, 活跃频点上接收的信号可以表示为

$$y_{\mathrm{A,J}}(k)=J(k)+n_{\mathrm{A}}(k)\tag{18}$$

类似于式 (10)、(11) 和 (12) 中的操作过程, 可以得到

$$P_{\mathrm{A}}\approx 1-\left(1-\psi_1\left(\frac{(\beta\cos\Delta\theta)^2E}{\sigma^2/2}\right)\right)^{(M-1)}\tag{19}$$

最后一种情况下, 静默频点被定频干扰信号攻击, 若需要正确检测包含两个条件: 活跃频点比被干扰的静默频点具有更大的能量, 活跃频点比未被干扰的 $M-2$ 个静默频点具有更大的能量. 根据以上两个条件, 可以得出

$$P_{\mathrm{I}}=1-P_{\mathrm{C}}=1-P_{\mathrm{C_1}}\times P_{\mathrm{C_2}}\tag{20}$$

式中: P_{C}表示在静默频点被定频干扰信号碰撞的最后一种情况下的正确检测概率; $P_{\mathrm{C_1}}$表示被干扰的静默频点的能量比活跃频点小的概率; $P_{\mathrm{C_2}}$表示其余 $M-2$ 个未被干扰的静默频点的能量比活跃频点小的概率.

因此, $P_{\mathrm{C_1}}$可以表示为

$$P_{\mathrm{C_1}}=P_{\mathrm{r}}\left(\left|\frac{\mathrm{Re}(y_{\mathrm{I,J}})}{\mathrm{Re}(y_{\mathrm{A}}^*)}\right|^2<1\right)\tag{21}$$

式中: y_{A}^*与$y_{\mathrm{I,J}}$分别表示合法接收机采用所提算法后在活跃频点与被干扰的静默频点上接收到的信号. 随机变量$\left|\frac{\mathrm{Re}(y_{\mathrm{I,J}})}{\mathrm{Re}(y_{\mathrm{A}})}\right|^2$难以获得简单的概率密度函数表达式, 因此将式 (21) 近似为

$$\begin{aligned}&P_{\mathrm{r}}\left(\left|\frac{\mathrm{Re}(y_{\mathrm{I,J}})}{\mathrm{Re}(y_{\mathrm{A}}^*)}\right|^2<1\right)\approx P_{\mathrm{r}}(\mathrm{Re}(y_{\mathrm{I,J}})-\mathrm{Re}(y_{\mathrm{A}}^*)<0)\\&=Q\left(\frac{\beta\sqrt{E}\cos\Delta\theta-\sqrt{E_{\max}}}{\sigma}\right)\end{aligned}\tag{22}$$

式中, Q 函数所在的项可以通过$\mathrm{Re}(y_{\mathrm{I,J}})-\mathrm{Re}(y_{\mathrm{A}})\sim\mathcal{N}\left(\beta\sqrt{E}\cos\Delta\theta-\sqrt{E_{\max}},\sigma^2\right)$计算得到.

此外, $P_{\mathrm{C_2}}$可以表示为

$$P_{\mathrm{C_2}}\approx\left(1-\psi_1\left(\frac{E_{\max}}{\sigma^2/2}\right)\right)^{M-2}\tag{23}$$

将式 (22) 和 (23) 代入式 (20), 可以得到

$$P_{\mathrm{I}}\approx 1-Q\left(\frac{\beta\cos\Delta\theta\sqrt{E}-\sqrt{E_{\max}}}{\sigma}\right)\left(1-\psi_1\left(\frac{E_{\max}}{\sigma^2/2}\right)\right)^{M-2}\tag{24}$$

将式 (12)、(19) 与 (24) 带入到式 (6)、(7) 中, 可以得到最终的 BER 近似闭式表达式.

为了便于分析, 本文考虑了定频干扰信号攻击单一频点的情况, 当干扰方采取多音干扰或连续多频点干扰时, BER 的近似理论值通过计算并更新公式 (6) 中的攻击概率即可得到.

4　仿真分析

在本节中给出基于干扰认知的 IM-FHSS 与传统 IM-FHSS 的蒙特卡洛仿真结果. 其中每个 BER 仿

真值来源于10^6次蒙特卡洛仿真统计结果.

图 3 给出了基于干扰认知的 IM-FHSS 的 BER 仿真值与近似理论值在不同β、$\Delta\theta$与K下的比较. 其中, 跳频图案的数量为$M=2$, 发射机能达到的最大功率为$E_{\max}=10$. 由图 3 可见, 所提算法在不同β、$\Delta\theta$与K的仿真结果和理论分析结果相一致, 证明了理论分析结果的正确性. 此外, 当$\beta=2$时, 没有出现误码平层; 当$\beta=8$时, 发射机在活跃频点上注入最大功率也难以克服静默频点被攻击后的高能量, 因此出现了与跳频总频点数K成反比的误码平层.

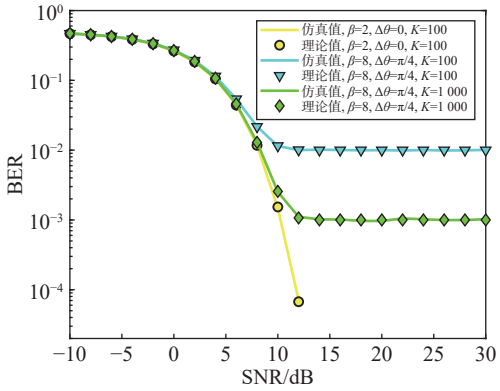

图 3 不同β, $\Delta\theta$与K下基于干扰认知的 IM-FHSS 的 BER 仿真值与近似理论值比较

Fig. 3 Comparison of simulated and approximate theoretical value of bit error rate based on cognition-based IM-FHSS at different β, $\Delta\theta$ and K

图 4 给出了基于干扰认知的 IM-FHSS 的 BER 仿真值与近似理论值在不同M与$E_{\max}$下的比较. 可以看出, 近似理论值与仿真值拟合较好. 注意到$M=4$、$E_{\max}=10$时具有比$M=4$、$E_{\max}=15$更大的近似误差, 这可以解释为式 (22) 中更小的$E_{\max}$将带来更大的近似误差. 此外, 当采用更大的$E_{\max}$时, 由于能够更有效地克服干扰信号, 因此在高 SNR 条件下能够取得更显著的 BER 性能增益.

图 5 给出了所提基于干扰认知的 IM-FHSS 与传统 IM-FHSS 在不同M和K下的 BER 性能比较. 其余参数设置为: $\beta=4$, $\Delta\theta=\pi/4$, $E_{\max}=10$. 可以看出, 传统的 IM-FHSS 仅使用跳频进行抗干扰, 因此 BER 曲线出现了与跳频点数相关的误码平层现象. 而所提基于干扰认知的 IM-FHSS 能够有效地调整发射机功率以适时地克服干扰信号的影响, 能够有效地改善误码平层现象. 特别是当 SNR 大于 10 dB, 所提方法的性能显著优于传统的 IM-FHSS. 这是由于此时背景噪声已经很小, 错误比特主要来源于干扰信号. 由于抗干扰策略能够有效克服干扰信号影响, 因此在该 SNR 区域所提方法能够有效改善 BER 性能.

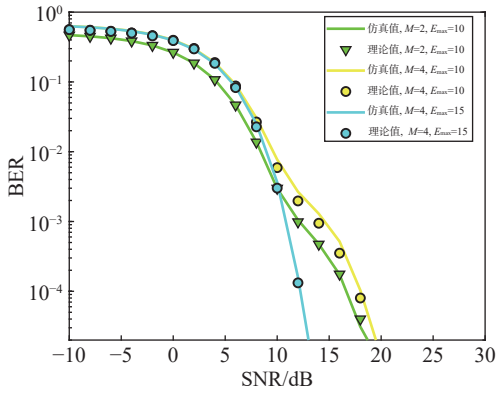

图 4 不同M与$E_{\max}$下基于干扰认知的 IM-FHSS 的 BER 仿真值与近似理论值比较 (β=4, $\Delta\theta$=π/4)

Fig. 4 Comparison of simulated and approximate theoretical value of bit error rate based on cognition-based IM-FHSS at different M and $E_{\max}$ (β=4, $\Delta\theta$=π/4)

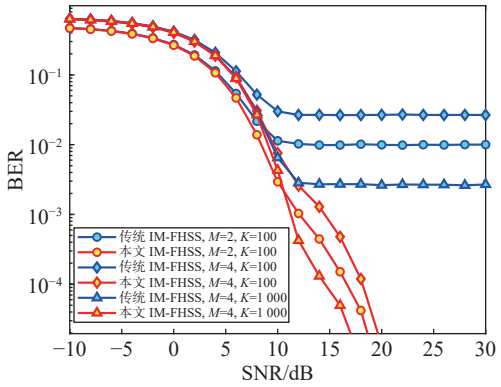

图 5 不同M和K下基于干扰认知的 IM-FHSS 与传统 IM-FHSS 的 BER 性能比较

Fig. 5 Comparison of bit error rate performance between cognition-based IM-FHSS and traditional IM-FHSS under different M and K

在现实条件下, 干扰认知结果可能出现错误, 这将影响基于干扰认知的 IM-FHSS 方法的实际性能. 为了衡量错误认知结果对所提方法 BER 性能的影响, 在无干扰条件下, 分别设定所提方法在理想认知水平下的虚警概率 (false probability) 为$p_{\mathrm{FA}}=0$、非理想认知水平下$p_{\mathrm{FA}}=0.01$进行比较. 由图 6 可见, 在非理想认知水平下, 在较高 SNR 区域 BER 仍能低于10^{-4}, 这表明所提方法在实际系统中是可行的. 并且, 随着跳频点数 K 增加到 1 000 时, BER 还将进一步降低. 具体的, 非理想干扰认知水平下的错误比特来源于所提方法误认为干扰信号会击中活跃频点, 因此不传输能量, 造成接收端的错误译码. 然而, 即使虚警概率高达 1%, 错误识别结果为击中活跃频点的概率也仅为 $1/K$, 造成的 BER 水平仅为$(1/K)$%, 对系统的影响很小.

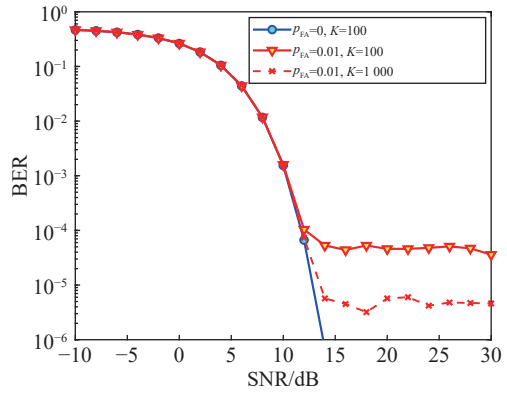

图 6　在不同认知水平下基于干扰认知的 IM-FHSS 的 BER 性能比较

Fig. 6　Comparison of cognition-based IM-FHSS BER performance under different cognition levels

5　结　论

本文提出了一种基于干扰认知的 IM-FHSS 方法，以高效应对干扰攻击. 通过利用认知干扰信号所在的频点信息并分析其作用于活跃频点、静默频点或者无干扰时所提算法的性能. 当干扰位于活跃频点时，所提算法可以利用干扰信号传输信息，而当干扰位于静默频点时，所提算法能够有效反制干扰信号. 仿真分析部分，理论分析的结果能够很好地拟合仿真结果，证明了理论分析结果的正确性；相比传统的 IM-FHSS 方法，基于认知的 IM-FHSS 方法能够在较高 SNR 条件下有效改善 BER，具备更好的抗干扰能力；在认知结果存在一定误差的情况下，仿真结果与理论分析表明其对 BER 性能的影响并不明显，证明了所提方法在实际系统中的可行性.

在后续的工作中，可以考虑在更加复杂的衰落信道中，以及获取了更加丰富的干扰认知信息时，设计更高效的索引调制跳频的功率控制方法，以进一步提升系统抗干扰性能.

参考文献

[1] 姚富强. 通信抗干扰工程与实践[M]. 北京: 电子工业出版社, 2012: 442.

[2] PELECHRINIS K, ILIOFOTOU M, KRISHNAMURTHY S V. Denial of service attacks in wireless networks: the case of jammers[J]. IEEE communications surveys & tutorials, 2011, 13(2): 245-257.

[3] GROVER K, LIM A, YANG Q. Jamming and anti-jamming techniques in wireless networks: a survey[J]. International journal of ad hoc and ubiquitous computing, 2014, 17(4): 197-215.

[4] WILHELM M, MARTINOVIC I, SCHMITT J B, et al. Short paper: reactive jamming in wireless networks-how realistic is the threat?[C]// The 4th ACM Conference on Wireless Network Security, 2011.

[5] WEN M W, ZHENG B X, JIN K K, et al. A survey on spatial modulation in emerging wireless systems: research progresses and applications[J]. IEEE journal on selected areas in communications, 2019, 37(9): 1949-1972.

[6] BASAR E, WEN M, MESLEH R, et al. Index modulation techniques for next-generation wireless networks[J]. IEEE access, 2017, 5: 16693-16746.

[7] BASAR E, AYGOLU U, PANAYIRCI E, et al. Orthogonal frequency division multiplexing with index modulation[J]. IEEE transactions on signal process, 2013, 61(22): 5536-5549.

[8] SHI Y, AN K, LI Y. Index modulation based frequency hopping: anti-jamming design and analysis[J]. IEEE transactions on vehicular technology, 2021, 70(7): 6930-6942.

[9] SHI Y, AN K, LU X, et al. Enhanced index modulation-based frequency hopping: resist power-correlated reactive jammer[J]. IEEE wireless communications letters, 2022, 11(4): 751-755.

[10] 鲁信金, 雷菁, 施育鑫. 基于旋转置乱的索引跳频抗干扰加密方法[J]. 通信学报, 2021, 42(12): 27-34.
LU X J, LEI J, SHI Y X. Index modulation aided frequency hopping anti-jamming and encryption method based on rotation scrambling[J]. Journal on communications, 2021, 42(12): 27-34. (in Chinese)

[11] SHI Y, LU X, NIU Y, et al. Efficient jamming identification in wireless communication: using small sample data driven naive Bayes classifier[J]. IEEE wireless communications letters, 2021, 10(7): 1375-1379.

[12] 李越. 通信干扰样式识别与参数估计算法研究[D]. 西安: 西安电子科技大学, 2019.
LI Y. Research on identification and parameter estimation of communication jamming signals[D]. Xi'an: Xidian University, 2019. (in Chinese)

[13] YEE T W. Univariate continuous distributions[M], 2015.

作者简介

施育鑫　(1995—)，男，福建泉州人，国防科技大学第六十三研究所博士研究生，研究方向为索引调制、抗干扰通信、物理层安全等. E-mail: shiyuxin13@nudt.edu.cn

(下转第 852 页)

2013, 24(4): 241-247.

[15] XIE H Y, LI G Z, NING B Q, et al. The possibility of using all-sky meteor radar to observe ionospheric E-region field-aligned irregularities[J]. Science China(technological sciences), 2019, 62(8): 1431-1437.

[16] VAUDRIN C V, PALO S E, CHAU J L. (2018). Complex plane specular meteor radar interferometry[J]. Radio science, 2017, 53(1): 112-128.

[17] YOUNGER J P, REID I M. Interferometer angle-of-arrival determination using precalculated phases[J]. Radio science, 2017, 52: 1058-1066.

作者简介

王思远 (1997—), 男, 内蒙古人, 哈尔滨工业大学(深圳)空间科学与应用技术研究院硕士研究生, 研究方向为流星雷达信号处理、流星雷达探测误差分析. E-mail: 283085454@qq.com

尹文杰 (1998—), 男, 安徽人, 武汉大学电子信息学院电离层实验室硕士研究生, 研究方向为流星雷达参数估计算法、VHF 雷达空间探测技术. E-mail: windsoryin@whu.edu.cn.

冯健 (1981—), 男, 山东人, 中国电波传播研究所研究员, 主要从事电离层物理及电波传播应用方面的研究. E-mail: fengjian428@163.com

赵正予 (1952—), 男, 吉林人, 哈尔滨工业大学(深圳)空间科学与应用技术研究院教授, 主要研究方向为电离层物理、电离层电波传播, 以及近地空间探测技术. E-mail: zhaozy@whu.edu.cn

(上接第 768 页)

李玉生 (1974—), 男, 国防科技大学第六十三研究所正高级工程师, 硕士生导师, 研究方向为通信抗干扰. E-mail: lys63s@163.com

安康 (1989—), 男, 国防科技大学第六十三研究所高级工程师, 研究方向为通信抗干扰、智能超表面、物理层安全、空天地一体化网络. E-mail: ankang89@nudt.edu.cn