



一种基于 PUE 恶意干扰的认知无线电态势感知方案^{*}

李方伟,冯德俊,朱 江

(重庆邮电大学移动通信技术重庆市重点实验室 重庆 400065)

摘 要:为了能及时、准确地掌握大范围内的仿冒主用户攻击情况及正确显示频谱态势图,提出一种基于仿冒主用户攻击检测的恶意用户干扰态势的研究方案,通过检测信道是否被恶意用户仿冒主用户攻击及对实施攻击的恶意用户的能量分布的检测与推理来构建干扰态势,并将其绘制成干扰态势图,从而方便决策者快速掌握大范围中的仿冒主用户攻击情况。仿真结果表明,该方案能够把主用户和恶意用户的能量及位置分离出来,从而充分发掘潜在的频谱空洞,提高频谱图的准确性,进而提高系统容量及安全性。

关键词:认知无线网络;仿冒主用户;干扰态势;频谱态势图;系统容量

doi: 10.3969/j.issn.1000-0801.2013.12.004

Situation Awareness Scheme Based on PUE Detecting for Cognitive Radio

Li Fangwei, Feng Dejun, Zhu Jiang

(Chongqing Key Lab of Mobile Communications Technology, Chongqing University of
Posts and Telecommunications, Chongqing 400065, China)

Abstract: To timely and accurately grasp the attack situation over a wide range when a malicious user emulates the primary user and attacks the channel, and to display correctly spectrum situation, a situation awareness scheme for the interference situation of malicious users was proposed. Decision-makers can know well the attack situation over a wide range, by detecting the primary user emulation attacker's energy and location to build the interference situation, and drew the interference into a situation map. The proposed approach can separate the energy and position of the primary users and malicious users, so as to fully exploit the potential of spectrum holes to improve the accuracy of the spectrum map, and improve safety and system capacity of the channels.

Key words: cognitive radio network, primary user emulation, interference situation, spectrum situation map, system capacity

1 引言

认知无线电(cognitive radio, CR)技术是提升频谱利用率的关键技术。如何系统、可靠地挖掘出网络中的可用频谱空洞,是实现认知无线电技术的关键之一。频谱态势图是指认知无线电中形象、直观地呈现频谱空洞的“频谱地

图”。一些参考文献^[1,2]研究了无攻击的态势图,在有攻击时,如仿冒主用户(primary user emulation, PUE)攻击,这种态势图就不能发现安全威胁,导致其系统容量和安全性较低。例如用参考文献[1]中的方法绘制的频谱态势图,便于CR网络的频谱分配中心对频谱进行宏观掌握,方便决策中心快速、正确地做出决策。但如果有PUE攻击,这种方

^{*} 国家自然科学基金资助项目(No.61271260, No.61071116, No.61102062)



法不能区分主用户(primary user, PU)和恶意用户(malicious user, MU)的能量,而使系统失去了对仿冒攻击的信道的支配权,同时降低了系统容量。一些研究只针对单个次用户(secondary user, SU)如何检测攻击,没有从大范围的角度分析攻击的影响及制定相应的应对方案。例如针对仿冒主用户攻击,参考文献[3~6]提出的抗攻击研究均是在首发端加入一些匹配算法(如散列函数、主用户能量指纹),避免仿冒攻击影响次用户正确判断信道是否空闲。这些方法基本上保证了对所有空闲信道的支配权,但是对于存在恶意用户的信道,如果信道分配中心对其干扰态势不加区分地分配给次用户,那么干扰范围内的次用户即使获得了该信道,仍然会因为干扰过大而不能安全地使用信道,从而降低了认知网络通信的安全性。因此,研究包含攻击的频谱态势图对安全、高效的无线电通信有重要意义。

本文针对仿冒主用户攻击的问题提出了一种基于PUE检测的恶意用户干扰态势研究方案。在该方案中,簇头从次用户发送的接收功率中挖掘出恶意用户,并估计恶意用户的位置和发射功率,从而将主用户能量和恶意用户能量分离,得到包含干扰态势的频谱态势图。恶意用户的干扰能量不同于主用户的能量,前者不具有排他性,也就是说如果能将两种能量分离,认知用户依然可以使用恶意用户施放干扰的信道,从而发掘更多的频谱空洞。所以,包含干扰态势的频谱态势图能提升系统容量。

2 系统模型

本方案基于 IEEE 802.22 协议,其网络模型如图 1 所示,网络中有 L 个主用户,每个主用户占用 1 个信道; M 个恶意用户任意分布在此区域; N 个次用户均匀地随机分布在特定范围内。

2.1 认知网络模型

认知网络采用协作频谱感知模型,即一定区域的次用户自动结合为簇,并推选一个簇头作为该簇的融合中心。各次用户将所检测到的能量值发送至簇头,由簇头进行统一处理。该网络中的主用户是移动的;次用户可以自由加入或离开该认知网络,但是在每个检测周期中不能移动。

每个次用户周期地执行频谱检测,每周期的时隙结构由感知时隙和数据时隙组成,如图 2 所示。本文所述方法在感知时隙执行。

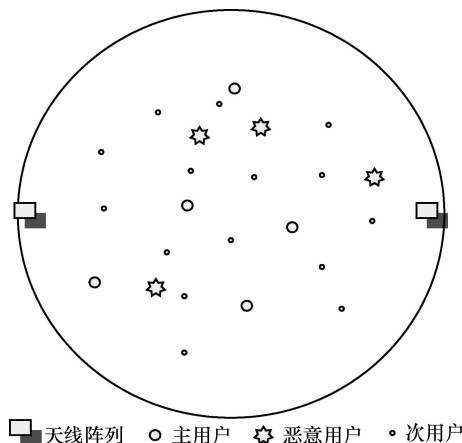


图 1 分布式认知无线网络模型

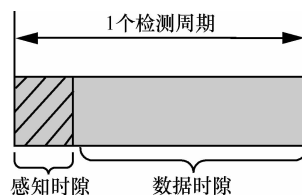


图 2 次用户检测周期的时隙结构

2.2 攻击模型

此文中讨论的攻击均为各 MU 独立进行的,即各 MU 之间不会互通消息,只根据自己的检测和推断结果发射仿冒信号。MU 的发射功率及位置不会改变,但可以自由加入或离开认知网络。

在无噪声干扰的环境下,接收信号场强服从自由空间传播模型,则次用户的接收功率为^[7]:

$$P_r = \frac{P_t G_t G_r \lambda^2}{(4\pi)^2 d^2 L} \quad (1)$$

其中, P_t 为发射功率, P_r 为接收功率, G_t 是发射天线增益, G_r 是接收天线增益, d 是主用户(或恶意用户)和次用户间的距离, L 是与传播无关的系统损耗因子, λ 为波长。

若 $|P_r^p - P_r^m| < \epsilon$, P_r^p 为 SU 检测到的主用户信号功率, P_r^m 为 SU 检测到的恶意用户信号功率,则恶意用户仿冒主用户攻击成功^[9]。

为方便表述,首先对网络模型进行以下假设。

- 如果 MU 感知到 PU 占用信道,则它不能攻击该信道,即 MU 不攻击 PU 占用的信道。
- 如果 MU 离 PU 足够远或恶意用户位于“频谱空洞”,从而感知不到信道上的 PU 信号,那么 MU 也可以在该信道发射仿冒信号,攻击该信道。
- MU 的位置及发射功率固定不变。

2.3 干扰态势图

本方案将从时间、空间和频率上建立三维的干扰态势图。时间上,每幅态势图体现当前检测周期中的干扰态势;频率上,每幅态势图体现一个信道中的干扰态势;空间上,每幅态势图展现一定区域中的干扰态势。

3 干扰态势感知方案

3.1 方案流程

由于主用户或者恶意用户占用或不占用信道的变化周期较长,只分析一个周期中的干扰态势。在一个检测周期中,对某一信道的检测流程如图 3 所示。

首先检测信道是否被占用(步骤 1)。若被占用,则检测该信道中的信号源有几个(步骤 2),若多于 1 个则说明该信道被攻击,因为正常信道中只存在一个主用户(即只有一个信号源);若只有一个则不能确定是主用户还是恶意用户,需要进行进一步检测(步骤 3)。当确定信道被仿冒攻击时,则对信道中的恶意用户进行定位和能量估计(步骤 4)。步骤 5 是对前面过程中出现的误差进行修正,以得到正确的干扰能量分布。至此可以得出较为准确的干扰态势图或者频谱态势图(步骤 6)。

3.2 被攻击信道挖掘算法

本节实现了对恶意用户存在于哪条信道的检测,是第 3.3 节对恶意用户定位的前提条件。

步骤 1 检测主用户信道是否被占用。

各 SU 先根据接收功率判断主用户是否使用信道。第 i 个用户 SU_i 的接收功率记为 P_{ri} ,若信道 f_i 上存在 P_{ri} -

$T_m > \sigma$ (T_m 为干扰温度门限),则暂定该信道为疑似主用户占用,标记为 f_k 。无论 SU_i 是否检测出主用户被占用,都将接收功率 P_{ri} 发送给簇头。

步骤 2 估计信号源个数。

盖氏圆盘估计 (GDE) 法是估计信号源个数的常用算法。用 GDE 算法估计疑似主用户占用的信道中信号源的个数 $n^{[8]}$ 。若信号源数 $n > 1$,则该信道处于仿冒主用户攻击中(因为一个信道中不可能存在两个主用户),则直接进入步骤 4;若信号源数 $n = 1$,则进入步骤 3。

步骤 3 判断疑似主用户占用是否为恶意用户占用。

当信道中只有一个用户时,不能确定是主用户还是恶意用户,需要进行 PUE 攻击检测。对于 PUE 检测,现有研究比较成熟,本方案采用参考文献[6]所述方法,其核心思想如下。

因为恶意用户的位置及发射功率是固定的,所以在任意两个周期 T_1 和 T_2 ,某点对其在两个不同信道发射信号的接收功率的差值只与频率有关,即:

$$\begin{aligned} \Delta P_r &= P_r^{T_1} - P_r^{T_2} \\ &= 26.16[\lg(f_1/f_2)] - [a_1(h_{re}) - a_2(h_{re})] \end{aligned} \quad (2)$$

其中, $a_1(h_{re})$ 、 $a_2(h_{re})$ 为移动天线修正因子, f_1 、 f_2 是这两个信道的中心频率。那么,若检测到各 SU 在 T_1 周期对信道 f_{D1} 的接收功率与在 T_1-1 周期对信道 f_{D2} 的接收功率的差值 $\Delta P_r' < \varepsilon$ (其中 $\varepsilon = 26.16[\lg(f_1/f_2)] - [a_1(h_{re}) - a_2(h_{re})] + x_n$, x_n 为平均系统噪声),则说明信道 f_{D1} 被攻击;否则,信道 f_{D1} 被主用户占用。

3.3 估计被攻击信道中的干扰能量分布

第 3.2 节中已检测出来哪些信道受到恶意用户的攻

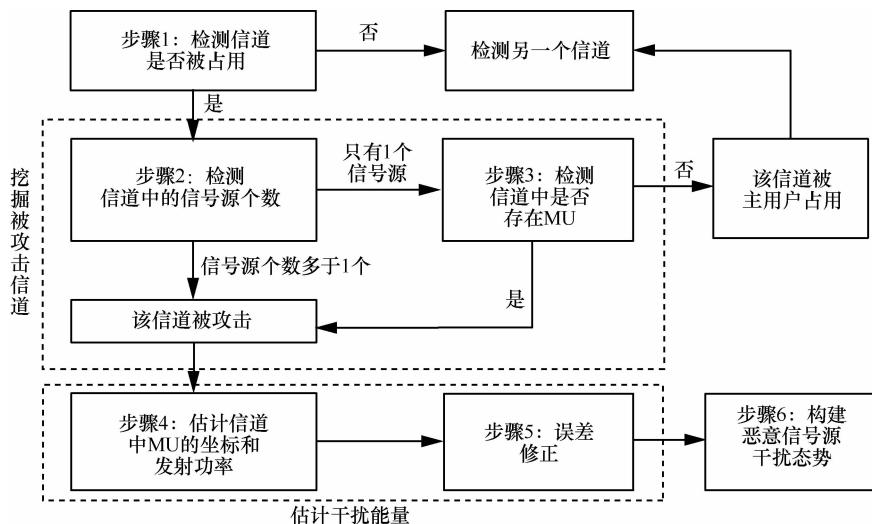


图 3 方案整体流程



击,但是这些信道中的恶意信号源的信息(位置、功率)并不知道,所以依然无法建立干扰态势,需要一一估计出这些信道中恶意信号源的位置及发射功率,为第3.4节构建干扰态势提供依据。

步骤4 估计信道中MU的坐标和发射功率。

首先进行粗估计。现有参考文献对信道中信号源的定位算法已有很多研究,本文采用参考文献[1]中的算法。现简要介绍如下。

首先利用 MUSIC 算法^[8]估计出各信号源的波达角 $\theta_1, \theta_2, \dots, \theta_m$ ^[7]。再根据波达角 θ_i 和阵列天线 1、2 的坐标 $(a_1, b_1), (a_2, b_2)$, 求出该信号源所在直线(即测向线)的方程。根据这些方程可求得包含恶意信号源的坐标的一系列交点(如图4所示)。在图4中一些交点不是信号源的坐标,此时可以根据 Dirichlet 原则和假设检验法挑选出正确的信号源坐标。因为信道中存在 n 个 MU, 所以选取 n 个 SU 并采用式(1)组成 n 元一次线性方程组求解这 n 个恶意信号源的发射功率 $P'_1 = P'_{T_1}, P'_{T_2}, \dots, P'_{T_n}$ 。

然后进行精确估计。

为了减小计算误差,本文提出以下两个措施。

措施1: 加设阵列天线3(如图4所示),减小波达角计算引起的误差。

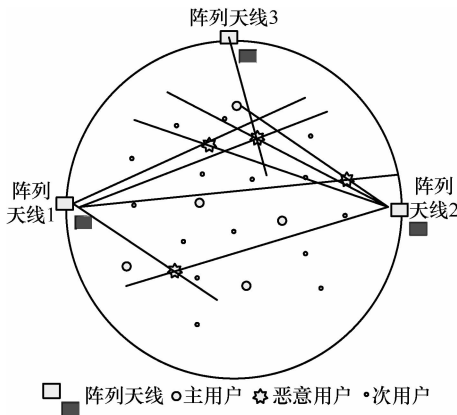


图4 阵列天线的测向线示意

因为当波达角 $\theta = (60^\circ, 90^\circ)$ 时,角度偏差一个小数值, $\tan \theta$ 就会产生较大误差,导致步骤4中交点计算的误差较大。加设一个阵列天线,采用三点定位法,即可减小此误差。

措施2: 计算 P'_1 的 M 个 SU, 由簇头选取离候选 MU 节点较近的 SU。

因为实际应用中,信号的传播衰落除了与空间距离有关,还与阴影衰落、环境噪声等因素有关,所以次用户的

实际接收功率为:

$$P_r = \Delta P_r + \frac{P_t G_t G_r \lambda^2}{(4\pi)^2 d^2 L} \quad (3)$$

那么用接收功率计算发射功率,则为:

$$P_t = (P_r - \Delta P_r) \frac{(4\pi)^2 d^2 L}{G_t G_r \lambda^2} \quad (4)$$

而步骤4粗估计中发射功率的计算式为:

$$P'_t = \frac{P_r (4\pi)^2 d^2 L}{G_t G_r \lambda^2} \quad (5)$$

则两者的误差为:

$$\begin{aligned} \Delta P_t &= P_t - P'_t = (P_r - \Delta P_r) \frac{(4\pi)^2 d^2 L}{G_t G_r \lambda^2} - \frac{P_r (4\pi)^2 d^2 L}{G_t G_r \lambda^2} \\ &= \Delta P_r \frac{(4\pi)^2 d^2 L}{G_t G_r \lambda^2} \end{aligned} \quad (6)$$

该误差随着 d 的增大而增大,所以要减小误差就要尽量选择较小的 d ,即选择与 MU 节点较近的 SU。

而作为数据融合中心簇头知道各 SU 的位置,也知道各组候选 MU 节点的位置,所以由簇头根据前面计算结果来选取这 n 个 SU。

3.4 构建干扰态势图

由于阴影衰落和环境噪声未知,虽然第3.3节估计出了 MU 的位置和发射功率,但这些计算所得的干扰能量分布仍存在一定的误差,不能较真实地还原干扰态势。所以,本节通过在考察区域均匀分布一些传感器,并采用插值方法,估计出该区域近似的阴影衰落和环境噪声,修正此误差。

步骤5 误差修正算法:当发射功率为 P'_1 时(见第3.3节)用式(1)计算只经过自由空间衰落后传感器的接收功率 P'_r ,将 P'_r 与传感器接收到的真实值 P_r 相减,其差 $\Delta P'_r$ 即该处的误差, $\Delta P'_r = P'_r - P_r$ 。再将每两个传感器的误差值之间插入 X 个值,即可得考察区域的误差修正值。

步骤6 由已求出的 MU 的位置和发射功率可以求得干扰能量分布的计算值,再加上误差修正值,则可以绘制出考察区域较为真实的干扰态势图。

本方案采用先定位,再插值求修正误差的方法可以减小干扰能量分布的计算误差。如果直接对传感器的接收功率做插值计算,所得干扰能量则误差较大。

4 基于干扰态势的认知用户容量

定义1 系统容量为考察区域中各信道平均容量的总和。各信道的平均容量为各次用户若接入该主用户信道

可以获得的信道容量的平均值。根据香农公式,各次用户若接入主用户信道,可以获得的最大信道容量为:

$$C(N_i) = B \lg \left(1 + \frac{S}{N_0 + N_i} \right) \quad (7)$$

其中, B 为信道带宽, S 为次用户发射功率, N_i 为次用户对恶意用户的接收功率(即干扰功率), N_0 为信道上的其他噪声干扰。

由式(7)可知,基于干扰态势图的第 i 个认知用户的容量为:

$$C(N_i) = \begin{cases} B \lg (1 + S/N_0), & \text{无恶意用户} \\ B \lg [1 + S/(N_i + N_0)], & \text{有恶意用户} \end{cases} \quad (8)$$

而不考虑干扰态势的第 i 个认知用户的容量为:

$$C(N_i) = \begin{cases} B \lg (1 + S/N_0), & \text{无恶意用户} \\ 0, & \text{有恶意用户} \end{cases} \quad (9)$$

由式(8)和式(9)对比可知,两种情况下的信道容量 C_i 差别在于有仿冒攻击时的容量不同。因为后者没有考虑攻击的情况,当有仿冒攻击时,后者会误认为是主用户使用而放弃对该信道的支配权,所以其信道容量为 0。

定义 2 第 i 个信道的容量 C_i 为系统中每个次用户对该信道的容量的平均。系统容量 C_s 是每个信道的容量之和,为:

$$C_s = \sum_{i=1}^L C_i = \sum_{i=1}^L \sum_{j=1}^N C(N_j) \quad (10)$$

对整个系统而言,考虑干扰态势的频谱态势图将会得到很多攻击时的信道容量,进而提高了系统的容量。当系统中的恶意用户只有 1 个时,两种方法下的系统容量差值为 $\Delta C_s = mB \lg [1 + S/(N_i + N_0)]$, 当有 m 个恶意用户时,系统的容量差值为 $\Delta C_s = mB \lg [1 + S/(N_i + N_0)]$, 所以恶意用户越多,系统容量差值越大。但这种趋势随着恶意用户数多于信道数而减小。因为当恶意用户数等于信道数后,每增加一个 MU, N_i 继续变大,由式(8)所得的 $C(N_i)$ 则继续减小,其系统容量也继续减小,也就是说,一个 MU 攻击一个信道还是两个攻击同一个信道,式(8)所得的容量是不同的;而对式(9)来说则不存在这种差别,所以当 MU 个数等于信道数后,其容量下降趋势明显变缓。

5 仿真及结果分析

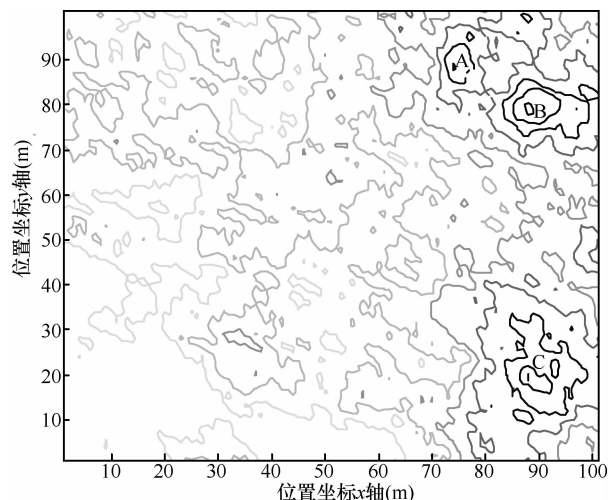
选择 $100 \text{ m} \times 100 \text{ m}$ 的正方形区域作为考察区域,主用户、次用户及恶意用户随机均匀分布在考察区域内。假设主用户信号传输系统采用 BPSK 调制系统,其干扰温度门

限为 $0.3002 \text{ W}^{[9]}$ 。

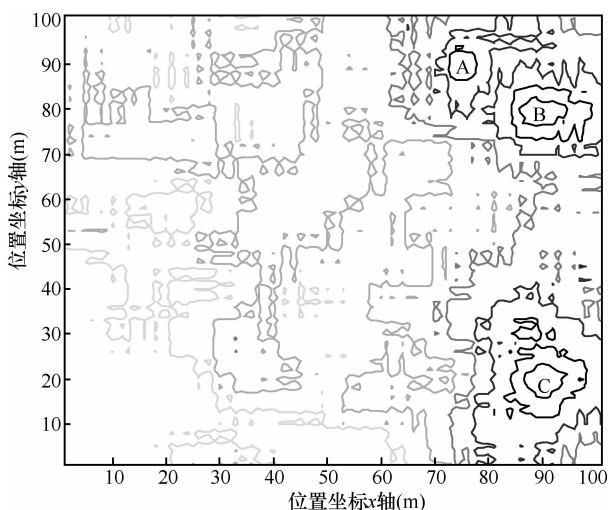
5.1 恶意用户的干扰态势的检测性能及误差

本节的仿真中设置 3 个恶意节点随机分布在考察区域,并在 $500 \sim 700 \text{ MHz}$ 频段随机选择信道进行仿冒主用户攻击。

图 5 是周期 T 、信道 i 中存在的恶意用户的干扰能量分布情况。图 5(a)是恶意用户的实际能量分布,图 5(b)是由本方案检测及估计所得的恶意用户能量分布。图中线圈的颜色由深至浅,表示接收功率由大变小。黑色表明此处 SU 接收到的干扰能量最大,如 A、B、C 处(这 3 处也正是恶意用户所在的位置);随着颜色逐渐变浅, SU 能接收到的干扰能量也逐渐变小,如图中左下角所示的空白区域表明此处几乎不受干扰。图中的干扰功率最高可达 20 dB ,



(a) 能量分布理论值二维图



(b) 能量分布估计值二维图

图 5 信道 i 中恶意用户能量分布的理论值与本文方法所得估计值的比较



最低只有-15 dB,如果某处的干扰功率小于接收机的信噪比门限,那么在知道该信道是被仿冒攻击的情况下,仍然可以使用此信道;但若干扰功率大于此处接收机的信噪比门限,就不适合使用此信道。对比图 5(a)和图 5(b)可知,簇头根据本方案所得出的恶意用户干扰能量分布图来给 SU 分配信道,可以使得通信成功概率大大提高,即提高了通信安全性。

图 6 是误差修正时采用不同的插值个数所得的系统均方误差分析。本方案的估计误差由图 5(a)中各点的功率值减去图 5(b)中的对应点的值求得的均方误差来体现。这些误差来源于对恶意用户进行坐标定位及发射功率估计时存在的些微误差和误差修正时造成的误差。前者的值很小,为 10^{-2} 级,可以忽略;整个方案中的误差主要是由修正误差造成的。由图 6 可以看出,随着两个传感器间距离的减小,误差不断减小。而且将图 5(a)与图 5(b)对比可知,这些误差并没有改变干扰能量分布的态势,也不会影响簇头对该信道的正确判断及使用,所以该方案的误差属于可接受范围。图 6 中两条曲线的对比说明本文方法可以更准确地描绘干扰态势。

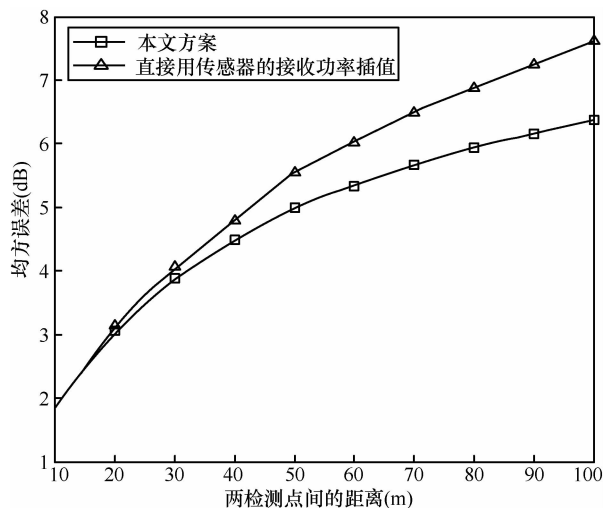


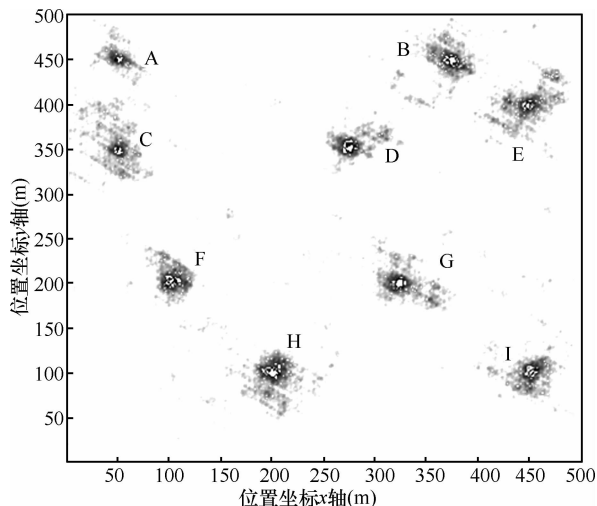
图 6 恶意用户干扰分布估计误差曲面

5.2 系统容量

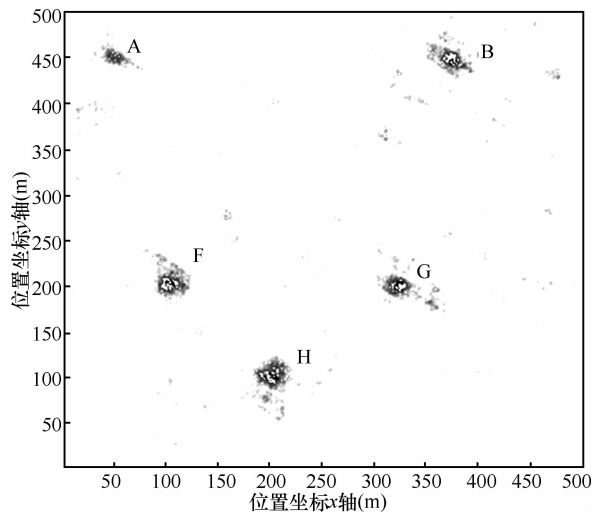
本节是将一认知簇由本方案所得的系统容量与参考文献[1]中方案所得的结果进行对比,如图 7 所示。

定义 3 频谱空洞是指对 PU 的接收能量很低而不可能存在主用户接收机的地方,本文定义为小于干扰温度门限的区域,即图 7 中的空白区域。

图 7(a)是由参考文献[1]所得的频谱态势。它表现某信道在一大范围区域中的频谱使用情况。图中各线圈表示



(a) 未进行 MU 检测的频谱态势



(b) 检测并去除 MU 的频谱态势

图 7 有无恶意用户检测的频谱态势图的比较

SU 接收到的 PU 或 MU 的信号功率,黑色区域是 PU 或 MU 存在的位置(标字母的地方),其接收功率较大。浅色线圈代表接收功率较小,空白区域表示“频谱空洞”。因为参考文献[1]不能检测仿冒攻击用户,所以其频谱态势图上存在 A 到 I 共 9 个“主用户”(包含主用户和仿冒攻击的恶意用户)，“频谱空洞”只有部分区域。图 7(b)是由本方案所得的同一考察区域的频谱态势,图中各线圈仅表示次用户接收到的 PU 的信号功率,黑色区域是 PU 的位置。因为能够检测仿冒攻击用户并准确估计其位置及发射功率,如图 7(b)所示的“频谱空洞”态势图上只存在 A、B、F、G、H 5 个真正的主用户,其频谱空洞也随之增多,即更多的认知用户可以得到信道使用机会,也就增大了系统容量。

现考察系统存在不同 MU 时,系统的信道容量总和的变化趋势。设考察区域中有 8 个信道,10 个 MU,各 MU 随机选择信道进行攻击,可两个或两个以上 MU 同时攻击同一个信道,在各信道均无主用户使用的情况下考察次用户接入时的信道容量。假设所有的信道带宽 $B=1$,接收信号功率 S 为 (0.000 1 W,30 W) 中的随机数, N_0 为高斯白噪声,本次仿真 5 000 次,取平均值,可得图 8。由图 8 可知,系统的信道容量之和随着恶意用户的增加而减少,但本方案的系统容量始终高于参考文献[1]的方案。图 8 中还可以看到当 MU 个数等于或者大于信道数之后,系统容量的下降趋势变缓。

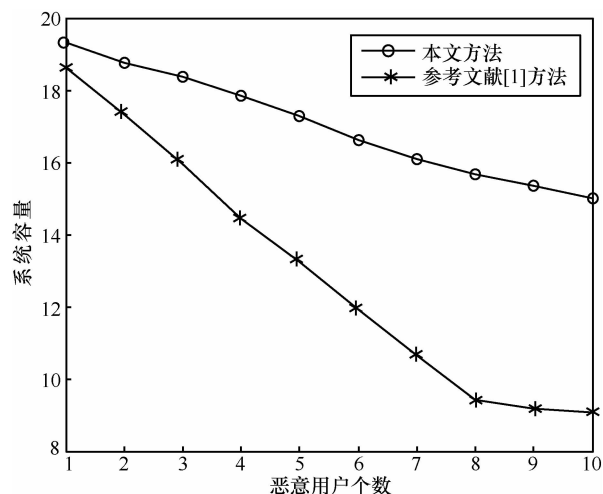


图8 两种方法下系统容量的对比

6 结束语

本文将态势感知的概念引入认知无线电安全研究领域,提出了一种基于 PUE 检测的恶意用户干扰态势研究方案。该方案可以准确地分离恶意用户和主用户的信号能量,从而构建恶意用户的干扰态势。仿真结果表明,该方案能够准确检测出信道中的干扰态势,并提高了敌对环境下频谱空洞检测的正确性,即有效地提高了系统的信道容量。

参考文献

- 张雯. 认知无线电中频谱检测的空域研究. 西安电子科技大学硕士学位论文, 2007
- 张晓明, 李思敏. 基于时域-空域联合的认知无线电频谱感知算法. 桂林电子科技大学学报, 2012, 32(5): 349~352
- Chen R, Park J M, Reed J H. Defense against primary user emulation attacks in cognitive radio networks. IEEE Journal on Selected Areas in Communications, 2008, 26(1): 25~37
- Chen Z, Cooklev T, Chen C, et al. Modeling primary user emulation attacks and defenses in cognitive radio networks. Proceedings of IEEE 28th International Performance Computing and Communications Conference (IPCCC), Phoenix, Arizona, USA, 2009: 208~215
- 薛楠, 周贤伟, 刘涛等. 基于簇的分布式认知无线网络安全体系结构. 电信科学, 2008, 24(11): 52~56
- 逢德明, 胡罡, 徐明. 基于能量指纹匹配的无线认知网络仿冒主用户攻击检测. 计算机科学, 2011, 38(3): 28~33
- Rappaport T S. Wireless Communications: Principles and Practice. New Jersey: Prentice Hall PTR, 1996
- 王永良, 陈辉, 彭应宁等. 空间谱估计理论与算法. 北京: 清华大学出版社, 2009
- 李妍琳, 康宁, 刁寅亮等. 认知无线电系统中频点门限的扩展讨论. 电波科学学报, 2010, 25(9): 169~171
- Mark B L, Nasif A O. Estimation of maximum interference-free power level for opportunistic spectrum access. IEEE Transactions on Wireless Communications, 2009, 8(5): 2505~2513
- Unnikrishnan J, Veeravalli V V. Cooperative sensing for primary detection in cognitive radio. IEEE Journal of Selected Topics in Signal Processing, 2008, 2(1): 18~27
- Yucek T, Arslan H. A survey of spectrum sensing algorithms for cognitive radio applications. IEEE Communications Surveys & Tutorials, 2009, 11(1): 116~130

[作者简介]



李方伟,男,博士,重庆邮电大学教授、博士生导师,主要研究方向为移动通信技术与理论、组网技术、信息安全技术、信号处理和智能天线技术。



冯德俊,女,重庆邮电大学硕士研究生,主要研究方向为移动通信安全技术、认知无线电安全技术。



朱江,男,博士,重庆邮电大学副教授、硕士生导师,主要研究方向为认知无线电安全技术、认知无线电感知技术、认知无线电频谱分配技术。

(收稿日期:2013-07-15)