可防御 SSDF 攻击的宽带压缩频谱感知

姚 刚 郑宝玉
(南京邮电大学信号处理与传输研究院，江苏南京 210003)

摘 要：SSDF(Spectrum Sensing Data Falsification)攻击是认知无线网络中对频谱感知性能危害最大的攻击方式之一。基于认知无线网络中信号频域的固有稀疏性，本文结合了压缩感知(CS)技术与平均一致(average consensus)算法，建立了可防御 SSDF 攻击的分布式宽带压缩频谱感知模型。本文建立了次用户的声望值指标，用以在分布式信息融合的过程中更加准确地排除潜在的恶意次用户影响。在感知阶段，各个 CR 节点对接收到的主用户信号进行压缩采样以减少对宽带信号采样的开销和复杂度，并做出本地频谱估计。在信息融合阶段，各 CR 节点的本地频谱估计结果以分布式的方式进行信息融合，排除潜在恶意次用户的影响，得到最终的频谱估计结果。仿真结果表明，本文提出的分布式频谱感知模型可以有效地抵御 SSDF 攻击，提高了频谱感知的性能。

关键词：认知无线电；宽带频谱感知；SSDF 攻击；压缩采样；平均一致算法
中图分类号：TN92 **文献标识码**：A **文章编号**：1003-0530(2013)02-0181-07

Compressed wideband spectrum sensing defensive against SSDF attacks

YAO Gang ZHENG Bao-yu
(Institute of Signal Processing and Transmission, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

Abstract: Spectrum Sensing Data Falsification (SSDF) attack is one of the most important threats to the spectrum sensing for wireless cognitive radio networks. On the basis that the wireless signal in cognitive radio network is inherently sparse in frequency domain, this paper develops a distributed compressed wideband spectrum sensing approach which combines compressed sensing and average consensus algorithm and defensive against SSDF attacks. To distinguish the potential malicious node more precisely, we evaluate reputation values for each of the CR nodes which will be used at the fusion stage. At sensing stage, compressed sensing is performed at each CR nodes to sample the received wideband signal at practical complexity and cost, and then locally reconstruct the frequency domain signal. At fusion stage, the local spectrum sensing results of each CRs are fused distributed and exclude the influence of potential malicious node at the same time without a fusion center. Simulation results show that spectrum sensing performance is enhanced using our proposed model and can defend against SSDF attacks.

Key words: cognitive radio; wideband spectrum sensing; Spectrum Sensing Data Falsification(SSDF); compressed sampling; average consensus

1 引言

认知无线电(CR)[1][2]的主要目的是通过允许未被授权的次用户接入被授权分配的频谱以改善频谱的利用率，次用户的接入需在频谱空洞即主用户空闲的频段范围。因此认知无线电首要的任务就是检测出那些暂时还没有被主用户占用的频谱空洞。

一种提高频谱感知性能的方式是多 CR 节点协作感知，通过协作，各节点可以交换信息并将信息融合，得到分集增益，结果比单个节点要更加准确[3]。很

收稿日期：2012-04-22；修回日期：2012-10-30
基金项目：国家自然科学基金项目(60972039)；江苏自然科学基金(BK2010077)

多协作频谱感知大都使用了集中式的信息融合方法[4][5],集中式的缺点是集中式处理方式要求所有CR节点将结果信息发往一个中心节点,这样会导致很大的通信开销,而且会导致整个网络对于中心节点的依赖性太强,一旦中心节点出现问题,网络将无法运行。

因为认知无线电网络中信号频域的固有稀疏性(正是这种固有的稀疏性才推动了动态频谱接入的思想),所以可将压缩采样技术[6][7][8]引入到认知无线电网络中来。一种AIC(analog to information converter)已经被提出[9]。[10]中,作者将压缩感知技术与平均一致算法相结合,建立了分布式宽带频谱感知模型,有效地解决了宽带频谱感知的若干问题。

安全问题作为认知无线网络中一个非常重要的问题,已经受到越来越多研究者的关注[11][12],SSDF攻击是其中一个主要的安全威胁。[10]中的模型没有考虑到CR节点中可能会有恶意节点的情况,一旦存在恶意节点,将对频谱感知性能产生很大的危害。[12]建立了可以防御SSDF攻击的分布式频谱感知模型,文中利用主用户估计能量偏离相邻单跳节点平均值的程度来衡量节点是否可能为恶意次用户,这样做的缺点是当CR网络中各CR节点信道状况都很差而只有少数个别CR节点信道状况较好时会将较好的节点误判为恶意次用户节点。

本文提出一种基于平均一致算法[13][14]的协作频谱感知模型以防御SSDF攻击。频谱感知分为两个阶段,即感知阶段和信息融合阶段。在感知阶段,每个CR节点处使用压缩采样技术进行频谱的估计以降低信号采样速率和开销[15][16]。在信息融合阶段,引入了CR节点的声望值(reputation value)[17]指标以帮助更加准确地排查出潜在的恶意次用户节点,并在使用平均一致算法融合信息的过程中筛除恶意次用户的数据,得到最终的频谱估计。

2 系统模型和问题描述

2.1 信号模型

考虑一个宽带频带范围同时包含主用户(Primary user)和次用户(Secondary user)。将这个宽带频谱范围分割成互不重叠的M个子信道,每个子信道以$\{f_m\}_{m=0}^{M-1}$为中心频率。这种信号模型在现实中是常见的,譬如OFDM信号,这些频率的划分是已知的,但是他们各自频率范围内的功率谱密度(PSD)是未知的并且随着时间而变化,当某个子信道空闲时,其功率谱密度处于较低水平,非空闲时,处于较高水平。子信道空闲时可以供次用户(SU)接入使用。

我们假设通过高层的协议控制,使主用户在发射信号的同时,所有次用户不发送任何信号,假设共有I个主用户在检测时隙里是活跃的(即可能会发射信号),并且主用户发射信号表示为$s_i(t)$,i=1,2,...,I。信号$s_i(t)$经过传输到达第j个CR接收机,我们假设第i个主用户到第j个CR接收机间为瑞利衰落信道,信道参数为$h_{ij}(t)$,则第j个CR接收机的接收信号为

$$r_j(t)=\sum_{i=1}^{I}h_{ij}(t)*s_i(t)+w_j(t) \tag{1}$$

其中$w_j(t)$是加性高斯白噪声,其均值为0,功率谱密度为σ_w^2。在整个信号频率范围内信道为频率选择性衰落信道,但是在每个子信道上为慢衰落信道。

为了反映出M个子信道上的离散信号响应,我们对CR接收机的接收信号$r_j(t)$作M点DFT,将频域响应值组合成一个M×1的向量$r_f^{(j)}$,可以得到

$$r_f^{(j)}=\sum_{i=1}^{I}D_h^{(ij)}s_f^{(i)}+w^{(j)} \tag{2}$$

其中$D_h^{(ij)}=diag(h_f^{(ij)})$是一个M×M的对角信道矩阵,$h_f^{(ij)}$,$s_f^{(i)}$和$w^{(j)}$分别是$h_{ij}(t)$,$s_i(t)$和$w_j(t)$的频域离散表达形式。这个信号模型可以重写为

$$r_f^{(j)}=H_f^{(j)}\bar{s}_f^{(j)}+w^{(j)} \tag{3}$$

当信道信息(CSI)未知时,有

$$H_f^{(j)}=H_f:=I_M;\ \bar{s}_f^{(j)}:=\sum_{i=1}^{I}D_h^{(ij)}s_f^{(i)} \tag{4}$$

当每个CR节点知道信道状态$h_f^{(ij)}$时,有

$$H_f^{(j)}:=\left[D_h^{(1j)},\ldots,D_h^{(Ij)}\right];$$

$$\bar{s}_f^{(j)}=\bar{s}_f:=\left[\left(s_f^{(1)}\right)^{\mathrm{T}},\ldots,\left(s_f^{(I)}\right)^{\mathrm{T}}\right]^{\mathrm{T}},\ \forall j \tag{5}$$

在每个CR节点,频谱感知就相当于通过估计(2)式中的$r_j(t)$来估计$\bar{s}_f^{(j)}$。当缺少信道状态CSI时,估算出的$\bar{s}_f^{(j)}$包含了未知的信道增益影响。当事先已知CSI时,就有可能通过(4)式中的$\bar{s}_f^{(j)}$估算出$\{s_f^{(i)}\}_{i=1}^{I}$。在大多数情况下,CR节点只想知道M个子信道中有哪些没有被占用,而不关心具体的信号频谱值$\bar{s}_f^{(j)}$。所有的次用户(SU)在被占用频段不发送信号并且所有的次用户之间通过某种机制共享空闲信道。这时就变成一个频谱检测问题,只想要得出一个表示M个子

信道是否被占用的二元状态向量 $d \in \{0,1\}^{M\times 1}$,$d[m]=1$,如果 $\exists i: s_f^{(i)}[m] \neq 0$;$d[m]=0$,如果所有的主用户在 f_m 频率处静默。在未知 CSI 的情况下频谱检测问题仍然可以解决,因为 $\bar{s}_f^{(j)}$ 和 $r_f^{(j)}$ 在相同的位置处非零,从而可以通过在 $r_f^{(j)}$ 找非零点来检测频谱。

2.2　CR 节点网络模型与平均一致(average consensus)算法

在我们的频谱感知模型中,次用户和它们的相邻节点建立通信链接并交换信息。这种网络可以表示为一个图 $\varsigma=(\varepsilon,\nu)$,我们为 CR 网络节点设定一个索引集 $\mathfrak{N}=\{1,2,\ldots,n\}$,其中有限点集 $\nu=\{\nu_i \mid i\in\mathfrak{N}\}$。边集 $\varepsilon=\{e_{ij} \mid i,j\in\mathfrak{N}\}$。节点 i 的邻集表示为 $\mathbb{N}_i=\{j: e_{ij}\in\varepsilon\}$,$\mathbb{N}_i$ 中元素的数目表示为 $|\mathbb{N}_i|$,其中的每一条边 e_{ij} 是在单跳通信范围内的无向边。图的通路包含一组节点 $\nu_1,\nu_2,\ldots,\nu_l, l\geq 2$,且满足 $(e_m,e_{m+1})\in\varepsilon$, $\forall 1\leq m\leq l-1$。如果图中两个不同的节点被一条通路相连,则称这两个节点是连通的。如果从一个图中的任意一个节点处出发可以到达任意一个其他节点,则称这个图是强连通的。在使用平均一致算法进行频谱感知时,对于建模为图 ς 的 n 个 CR 节点,为第 i 个节点分配一个状态变量 x_i,当算法收敛时,每个 x_i 异步收敛于一个共同的值 x^*。即 $x_i(k)\to x^*, k\to\infty$,其中 $k=0,1,2,\ldots$,是离散时间。基于平均一致算法的迭代式为

$$x_i(k+1)=x_i(k)+\varepsilon\sum_{j\in\mathbb{N}_i}(x_j(k)-x_i(k)),\quad i=1,2,\ldots,J \tag{6}$$

在我们的频谱感知模型下,使用分布式的平均一致算法可以在不需要汇聚节点(Fusion Center)的情况下,求出收敛值 x^* 且 $x^*=\left.\sum_i x_i\right/J$,其中 J 表示次用户节点的个数。

2.3　协作频谱感知中的 SSDF 攻击模型

在协作频谱感知中,一组次用户(SU)通过互相交换各自的本地信息来进行协作。恶意次用户可能会向其他 CR 节点发送错误的本地频谱感知结果,以此利用协作频谱感知来进行 SSDF 攻击。以下列出三种攻击模型。

在第一种攻击模型中,一个恶意次用户通过在攻击频段持续报告较高的功率谱密度以此来让其他次用户误认为该频段被主用户占用,从而放弃使用当前频段。这种恶意次用户的目的是想独占攻击频段的使用权,我们称这种攻击方式为自私 SSDF 攻击(Selfish SSDF)。在第二种攻击模型中,恶意次用户在攻击频段报告较低的功率谱密度以此让其他次用户误以为该频段未被主用户占用而试图使用该频段。这种恶意次用户既可以造成对主用户的干扰也可以妨碍其他次用户的通信。我们称这种攻击方式为干扰 SSDF 攻击(Interference SSDF)。在第三种攻击模型中,一个恶意次用户在攻击频段随机地报告正确的或者错误的主用户功率谱密度。这意味着有时该恶意次用户发送正确的主用户功率谱密度,有时发送错误的主用户功率谱密度。这种恶意次用户的目的是混淆其他次用户对其真实身份的判断。我们称这种攻击为混淆 SSDF(Confusing SSDF)。

3　协作压缩频谱感知

这一部分建立了可以防御 SSDF 攻击的分布式压缩频谱感知模型,为了找出潜在的恶意次用户,为每个 CR 节点建立了声望值指标,为了降低在 CR 节点处的数据采样率,使其控制在可实现的速率之内,我们采用压缩感知技术对数据进行采样。

3.1　单个 CR 节点的压缩频谱感知

对每个 CR 节点 j, j=1,2, ...,J。每个 CR 节点需要估计出 $\bar{s}_f$,为了达到这个目的,我们采用压缩感知技术来降低采样的代价。压缩感知的第一步是在 CR 节点处采集时域信号。为了达到这个目的,我们在每个 CR 节点处采用压缩采样矩阵 S_c,从接收信号 $r_j(t)$ 采集 K×1 的向量,K<=M。故有

$$x_t^{(j)}=S_c^{\mathrm{T}} r_t^{(j)} \tag{7}$$

其中,K×1 的向量 $x_t^{(j)}$ 表示以奈奎斯特速率采样 $r_j(t)$ 以后的离散表示形式,且 K<<M。需要指出的是,上式不是实际的采样过程,实际中并不需要先对 $r_j(t)$ 进行奈奎斯特速率的采样再进行压缩,事实上,AIC[9]可以有效的实现压缩采样。

在得到 K 个样本值 $x_t^{(j)}$ 后,现在要进行频谱感知。已知 $r_t^{(j)}=F_M^{-1}r_f^{(j)}$,其中 F_M^{-1} 是傅立叶反变换矩阵。我们有

$$x_t^{(j)}=S_c^{\mathrm{T}}F_M^{-1}r_f^{(j)}+S_c^{\mathrm{T}}F_M^{-1}w_f^{(j)}=S_c^{\mathrm{T}}F_M^{-1}H_f^{(j)}\bar{s}_f^{(j)}+S_c^{\mathrm{T}}F_M^{-1}w_f^{(j)} \tag{8}$$

因为主用户网络的频谱利用率很低,所以 $\bar{s}_f^{(j)}$ 是稀疏的。我们以 s=CS(x,A)来表示一个信号重建算

法(e.g.,BP,OMP,LASSO...)来重建信号 x=As+w,其中 w 是高斯白噪声。所以在 CR 节点 j 上的本地频谱感知结果可以表示为

$$\hat{\bar{s}}_f^{(j)} = CS(x_t^{(j)}; S_c^{\mathrm{T}} F_M^{-1} H_f^{(j)}) \tag{9}$$

3.2 CR 节点的声望值

为了防御 SSDF 攻击,我们必须找出在 CR 节点网络中哪些节点可能是恶意次用户,如果能在信息融合的过程中排除这些潜在的恶意次用户将对最终的频谱感知性能有很大的提升。为了达到这个目的,我们对每个 CR 节点建立声望值指标,以此来衡量 CR 节点为恶意次用户的潜在可能性。我们将每个 CR 节点声望值的初始值设定为 1,当第 j 个 CR 节点的频谱检测结果 $d^{(j)}(m)$ 与真实信道占用情况 $d(m)$ 相同时,声望值增加 1. 将第 j 个 CR 节点的声望值表示为 ν_j,ν_j 的更新式为

$$\begin{aligned} &\text{如果 } \nu_j>0,\text{则 } \nu_j \leftarrow \nu_j + \sum_m (-1)^{d^{(j)}(m)+d(m)};\\ &\text{如果 } \nu_j \leqslant 0,\text{则 } \nu_j \leftarrow 0 \end{aligned} \tag{10}$$

其中 m 表示第 m 个子信道。

3.3 数据筛选进程

为了更加准确地排除潜在的恶意次用户的影响,本文提出了一个数据筛选进程,该进程将在信息融合过程中判断出潜在的恶意次用户并排除其影响。考虑 $k \geqslant 1$ 的情况,我们假设 $|\mathbb{N}_i|>2$。对每个 CR 节点都执行以下进程:

第一步:CR 节点 i 收到时刻 k-1 的本地加权平均值

$$\mu_i(k-1) = \frac{\nu_i * x_i(k-1) + \sum_{j\in\mathbb{N}_i} \nu_j * x_j(k-1)}{\nu_i + \sum_{j\in\mathbb{N}_i} \nu_j} \tag{11}$$

由(11)式可以看出,声望值较高的节点将对加权平均值做出相对更多的贡献,使得加权平均值更能体现实际情况。

第二步:CR 节点 i 从相邻节点中找出偏离 $\mu_i(k-1)$ 最多的那个节点

$$\hat{j} = \arg\max_{j\in\mathbb{N}_i} |x_j(k) - \mu_i(k-1)| \tag{12}$$

第三步:CR 节点 i 创建一个表示正常节点的集合 $\hat{\mathbb{N}}_i(k)$

$$\hat{\mathbb{N}}_i(k) = \mathbb{N}_i \setminus \{\hat{j}\} \tag{13}$$

当 k=0 或者 $|\mathbb{N}_i| \leqslant 2$ 时,我们设置 $\hat{\mathbb{N}}_i(k) = \mathbb{N}_i$。

由上述进程可以看出,当一个相邻节点子集内多数 CR 节点信道状况较差时,采用声望值加权平均的方法可以避免将少数信道状况较好的 CR 节点误判为恶意次用户节点的可能性。

3.4 防御 SSDF 攻击的频谱感知模型

我们假设 CR 节点网络中相邻节点间已经建立好了双工通信链接,并且这些链接在平均一致算法收敛之前保持稳定。这样,CR 节点网络就是一个固定拓扑图。需要注意的是,恶意次用户也被包含在这个图中并且它将与相邻节点交换信息。基于这样的假设,我们提出可以防御 SSDF 攻击的协作频谱感知方案。

第一步:每个 CR 节点运用压缩采样技术收集时域样本 $x_t^{(j)}$,重构出其频域信号 $\bar{s}_f^{(j)} = CS\left(x_t^{(j)}; (S_c^{(j)})^{\mathrm{T}} F_M^{-1} H_f^{(j)}\right)$,根据 $\bar{s}_f^{(j)}$ 做出本地判决向量 $d^{(j)}$,$d^{(j)}[m] = (|\bar{s}_f^{(j)}[m]| \geqslant \eta)$,其中 m 代表第 m 个子信道,$\eta$ 是预设判决门限。然后根据(10)式更新各 CR 节点的声望值 ν_j。

第二步:每个 CR 节点与相邻节点建立链接,并且在时刻 $k \in Z_+$ 开始交换各自的频谱估计结果 $\bar{s}_f^{(j)}$。我们将 i 节点的频谱估计结果 $\bar{s}_f^{(i)}$ 表示为 $x_i(k)$。在每个时隙 k,k=0,1,2,3…,从相邻节点接收到 $x_j(k)$ 的同时,该 CR 节点执行数据筛选进程以此来排除一个潜在的恶意节点。这个进程会创建一个相邻节点子集并且该数据将会用于节点 i 的状态更新。

第三步:经过本地信息更新,每个节点 i 向相邻节点发送频谱估计结果 $x_i(k+1)$。然后上一步中的数据筛选进程和状态更新过程将被重复执行知道最后所有的频谱估计结果 $x_i(k)$ 都收敛至一个最终值 x^*,即 $\hat{\bar{s}}_f$。迭代式为

$$\begin{aligned} &x_i(k+1) = x_i(k) + \varepsilon \sum_{j\in\hat{\mathbb{N}}_i(k)} (x_j(k) - x_i(k)),\\ &i = 1,2,\ldots,J \end{aligned} \tag{14}$$

最后,根据收敛后的 x^* 即 $\hat{\bar{s}}_f$ 进行信道占用情况判决,$\hat{d}[m] = (|\hat{\bar{s}}_f[m]| \geqslant \eta_{th})$。

上述算法中,有可能出现 CR 节点 A 接收 CR 节点 B 为其相邻节点而 B 不接受 A 为其相邻节点的情况,此时无向图 ς 将变成有向图 ς_t,算法的收敛无法得到保证[12]。但是,如果有一个足够长的时刻窗[k, k+T],当各时刻的有向图的并集 $\bigcup_k^{k+T} \varsigma_t$ 是强连通的,则

算法可以收敛[18]。

4　仿真结果及分析

考虑一个划分成 M = 20 个子信道的宽带频带范围,每个子信道带宽相同。信道经历频率选择性衰落,其中每个子信道经历独立同分布的瑞利衰落。每个 CR 节点的信噪比(SNR)根据各 CR 节点状况而不同。压缩比率 K/M 定义为压缩采样后的样本数 K 和用奈奎斯特速率采样后的样本数 M 的比值。我们使用 mean square error(MSE)来衡量频谱估计的精度,$MSE = E\left\{ \| \hat{\bar{s}}_f - \bar{s}_f \|_2^2 \right\} \Big/ \| \bar{s}_f \|_2^2$。我们使用检测概率 $P_d = E\left\{ \frac{d^{\mathrm{T}}(d=\hat{d})}{1^{\mathrm{T}}d} \right\}$ 和虚警概率 $P_f = E\left\{ \frac{(1-d)^{\mathrm{T}}(d\neq\hat{d})}{M-1^{\mathrm{T}}d} \right\}$ 来衡量频谱空洞检测的性能,其中 $d = \{0,1\}^{M\times 1}$ 是真实频谱占用情况向量,1 表示全 1 向量。一个高的检测概率会导致高的虚警概率,从而对主用户形成更强的干扰。从另一方面说,一个低的虚警概率会导致低的检测概率,从而使得频谱利用率随之降低。为了便于直观比较,将各节点的威望值归一化,使得 $\sum_j \nu_j = 1$。平均信噪比 SNR 反映了 CR 节点的信道状况,为了体现出引入声望值指标的意义,我们设定了一个除少数节点以外信道状况普遍较差(即各 CR 节点 SNR 较低)的 CR 网络。

如图 1,11 个 CR 节点形成一个固定的可以互相通信的节点拓扑,其中有一个节点为恶意次用户节点,该节点发起 SSDF 攻击。恶意次用户节点首先利用压缩采样技术重构出对主用户的本地频谱估计 $\bar{s}_f$,并以概率 P_a 发起攻击,当重构出的 $\bar{s}_f$ 在第 m 个子信道上的功率谱密度 $\bar{s}_f(m) \geqslant \eta$ 时,恶意节点发送 $\bar{s}_f(m) - \Delta$;当重构出的 $\bar{s}_f$ 在第 m 个子信道上的功率谱密度 $\bar{s}_f(m) < \eta$ 时,恶意节点发送 $\hat{\bar{s}}_f(m) + \Delta$。图 2 展示了当一个没有防御体系的 CR 节点网络受到 SSDF 攻击时平均一致算法的收敛过程,可以看到,最后所有 CR 节点将收敛至恶意次用户发送的信号,增大了对主用户的估计误差(MSE),从而恶化了频谱感知的性能。图 3 展示了当引入了本文所提出的防御机制以后 CR 节点网络受到 SSDF 攻击时平均一致算法的收敛过程,可以看到,CR 节点网络在分布式信息融合的过程当中成功的分辨出了恶意次用户节点并排除了其消极影响。图 4 展示了在本文提出的防御机制下各 CR 节点(包括恶意次用户节点)的归一化声望值走势。其中实线表示正常 CR 节点,星点表示恶意次用户节点,可以看出,CR 节点网络中正常节点的声望值均大幅高出恶意次用户节点的声望值,且在 20 步检测轮数以内即可有效分辨出恶意次用户节点,达到了检测恶意次用户节点的目的。图 5 展示了各情况下的频谱感知性能(ROC),可以看出,当无防御机制的 CR 节点网络受到 SSDF 攻击时频谱感知性能恶化相当严重。引入了声望值指标的防御方案 2 比未引入声望值指标的防御方案 1 有着更好的频谱感知性能,这是因为当在大多数 CR 节点信道状况较差的情况下,未引入声望值指标的方案在信息融合过程中很容易将信道状况较好的 CR 节点误判为恶意次用户节点,从而导致最终频谱感知性能的恶化。根据主用户信号频域的稀疏性,我们引入了压缩感知技术,但同时压缩采样也会引起频谱检测性能的恶化,图 5 中可以看出,某些情况下压缩采样会抵消掉方案 2 比方案 1 的性能优势。

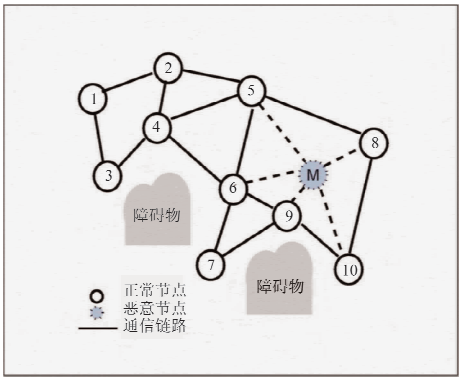


图 1　CR 节点网络拓扑

Fig. 1　Topology Of CR Network

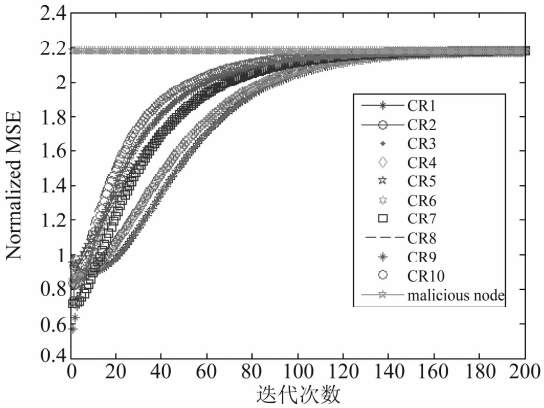


图 2　无防御时各节点信号的 MSE

Fig. 2　MSE of each CRs without defense against SSDF attacks

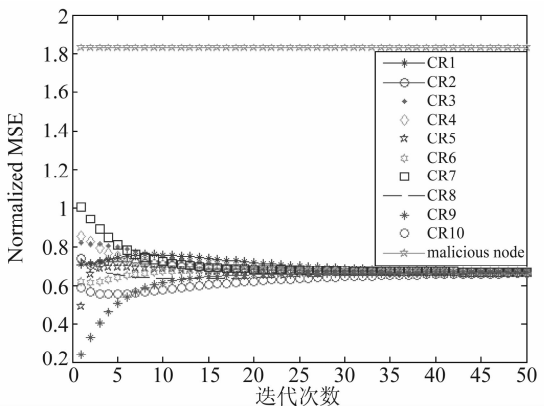


图 3 有防御时各节点信号的 MSE

Fig. 3 MSE of each CRs with proposed defense scheme

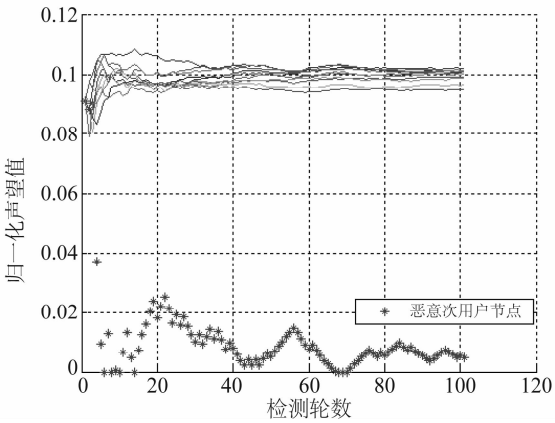


图 4 各节点声望值走势

Fig. 4 Trend of each CR's reputation value

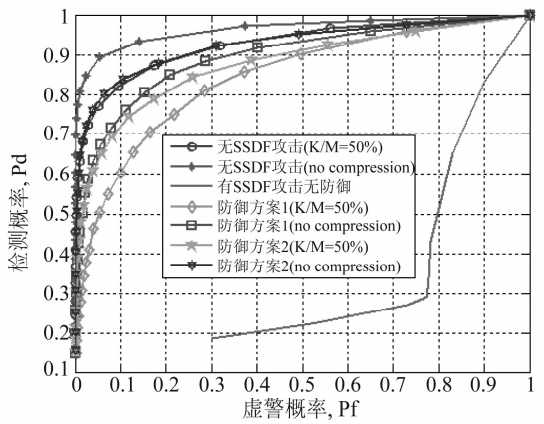


图 5 频谱感知性能对比

Fig. 5 ROC comparisons for different situations

5 总结

本文结合压缩感知技术与平均一致算法,为各 CR 节点建立了声望值指标。首先利用压缩感知技术使各 CR 节点的采样速率及开销大大降低,然后结合平均一致的分布式信息融合算法排除了潜在恶意次用户的消极影响并最终得出对主用户频段的频谱估计。仿真结果显示,结合压缩感知与平均一致算法以及引入了声望值指标的频谱感知模型可以有效增强 CR 节点网络在低信噪比信道情况下抵御 SSDF 攻击的能力,增强了频谱感知性能。

参考文献

[1] J. Mitola. An integrated agent architecture for software defined radio [D]. The Royal Institute of Technology, KTH, 2000.

[2] S. Haykin. Cognitive radio: Brain-empowered wireless communications[J]. IEEE J. Selected Areas in Communications, 2005. Vol. 23(2).

[3] I. F. Akyildiz, B. F. Lo, and R. Balakrishnan. Cooperative spectrum sensing in cognitive radio networks: A survey[J]. Physical Communication, 2011. 4(1):40-62.

[4] K. Ben Letaief and W. Zhang. Cooperative communications for cognitive radio networks[J]. Proceedings of the IEEE, May 2009. vol. 97:878-893.

[5] Z. Quan, S. Cui, and A. H. Sayed. Optimal linear cooperation for spectrum sensing in cognitive radio networks[J]. IEEE J. Sel. Topics Signal Process., Jan. 2008, 2(1): 28-40.

[6] R. G. Baraniuk. Compressive sensing[J]. IEEE Signal Process. Mag., 2007, 24(4):118-120, 124.

[7] E. J. Candès, J. Romberg, and T. Tao. Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information[J]. IEEE Trans. Inf. Theory, Feb. 2006, 52(2):489-509.

[8] D. L. Donoho. Compressed sensing[J]. IEEE Trans. Inf. Theory, Apr. 2006, 52(4):1289-1306.

[9] S. Kirolos, T. Ragheb, J. Laska, M. Duarte, Y. Massoud, and R. Baraniuk. Practical issues in implementing analog-to-information converters[J]. in Proc. Int. Workshop System-on-Chip for Real-Time Applicat., Dec. 2006, pp. 141-146.

[10] Zhi Tian. Compressed Wideband Sensing in Cooperative Cognitive Radio Networks[C]. IEEE "GLOBECOM" 2008 proceedings.

[11] R. Chen, J. M. Park, Y. T. Hou, and J. H. Reed. Toward secure distributed spectrum sensing in cognitive radio networks[J]. IEEE Communications Magazine Special Issue on Cognitive Radio Communications, 2008.

[12] F. Richard Yu, Helen Tang, Minyi Huang, Zhiqiang Li and Peter C. Mason. Defense against Spectrum Sensing Data Falsification Attacks in Mobile Ad Hoc Networks

with Cognitive Radios[C]. Military Communications Conference, 2009. MILCOM 2009. IEEE.

[13] W. Ren, R. Beard, and E. Atkins. A survey of consensus problems in multi-a gent coordination [C]. in Proc. American Control Conference '05, (Portl and, OR), June 2005.

[14] R. Olfati-Saber, J. Fax, and R. Murray. Consensus and cooperation in networked multi-agent systems[J]. Proceedings of the IEEE, Jan. 2007, vol. 95:215-233.

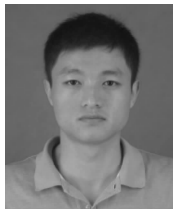
[15] Z. Tian and G. Giannakis. Compressed sensing for wideband cognitive radios[C]. in Proc. IEEE Int. Conf. Acoust., Speech, Signal Process. (ICASSP), Apr. 2007, vol. 4, pp. IV-1357-IV-1360.

[16] Y. Polo, Y. Wang, A. Pandharipande, and G. Leus. Compressive wideband spectrum sensing[C]. in Proc. IEEE Int. Conf. Acoust., Speech, Signal Process. (ICASSP), Apr. 2009, pp. 2337-2340.

[17] Xi Zhang, Xiaoyan Zhu. Distributed Secure Compressive Spectrum Sensing in Wireless Cognitive Radio Networks [C]. Military Communications Conference, 2010. MILCOM 2010. IEEE.

[18] W. Ren and R. W Beard. Consensus seeking in multiagent systems under dynamically chang ing interaction topologies[J]. IEEE Trans. Auto. Control, May 2005, vol. 50:655-661.

作者简介



姚　刚(1987-),男,江苏盐城人。本科毕业于南京邮电大学通信与信息工程学院电子信息工程专业获学士学位,现为南京邮电大学通信与信息工程学院信号与信息处理专业硕士研究生;主要研究方向为无线通信与信号处理技术。

E-mail:yao. gang. 1987@ gmail. com

郑宝玉(1945-),男,出生于福建省闽侯县。南京邮电大学教授、博士生导师,上海交通大学兼职教授、博士生导师,中国通信学会通信理论与信号处理专业委员会主任委员,IEEE 南京分会主席。主要研究方向为智能信号处理、通信信号处理和量子信号处理等。E-mail:zby@ njupt. edu. cn