基于能量指纹匹配的无线认知网络仿冒主用户攻击检测

逄德明 胡 罡 徐 明
(国防科技大学计算机学院 长沙 410073)

摘 要 频谱感知是无线认知网络有效工作的基础,现有研究主要集中在提高频谱检测的效率,对于如何保证在不可信的网络环境中实现安全可靠的频谱感知还没有理想的解决方案。针对频谱感知过程中存在的一种典型攻击行为——仿冒主用户攻击,提出了一种基于能量指纹匹配的检测方案。认知用户利用自身的位置分布特征,使用能量检测生成主用户的能量指纹,以此作为节点的身份标识,分析不同用户对频谱资源的使用方式,最终实现对仿冒行为的检测。理论分析以及模拟测试表明,该方案在误检概率较低的前提下,可以有效地检测仿冒攻击行为,提高频谱感知的准确率。

关键词 无线认知网络,无线网络安全,主用户仿冒攻击,能量指纹匹配
中图法分类号 TP309.2 **文献标识码** A

Detecting Primary Emulation Attacks Based on Energy Fingerprint Matching in Cognitive Radio Networks

PANG De-ming HU Gang XU Ming
(Computer School of National University of Defense Technology, Changsha 410073, China)

Abstract Spectrum sensing is an essential mechanism in cognitive radio networks. While so many works have been done or being carried on upon improving the efficiency of the sensing process, there is no appropriate scheme to realize security sensing in untrustworthy environments. We proposed a mechanism based on Energy Fingerprint(EF) matching to address a typical attack in CR networks, the Primary User Emulation Attack(PUEA). Based on the distribution of their positions and through energy detection, the secondary users can create PU's EF which is used as an identification of node to analyze the spectrum accessing mode of different users, and finally detect the PUEA. Through analysis and simulation, it can be demonstrated that while keeping the probability of missing the return of the primary low, it is possible to detect the emulation attack effectively.

Keywords Cognitive radio networks, Wireless network security, Primary user emulation attack, Energy fingerprint matching

1 引言

随着无线通信技术的发展与移动应用业务的急剧扩充,无线电频谱资源分配几乎殆尽,而频谱的实际利用率极低(平均低于10%)且严重不均[1,2],由此可见现有的静态频谱管理与使用方式严重束缚了无线通信网络的发展。在这种情况下,动态频谱接入的思想应运而生:在不对原有网络中的授权用户造成干扰的前提下,非授权用户伺机使用空闲频段,以增加时域、空域及频域上的频谱复用。

认知无线电(Cognitive radios, CR)是实现动态频谱接入的主要平台。CR的概念由软件无线电的发明人Mitola博士提出,即在软件无线电的基础上,依靠人工智能的支持,将无线电系统从预置程序的被动执行者转变成为无线电领域的智能Agent[3]。美国联邦通信委员会(FCC)出于提高频谱利用率与通信可靠性的目的提出了一种简化的定义[1]:认知无线电要感知周边环境的频谱使用状况以检测出频谱空洞(在特定时间和空间未被使用的授权频段),能在一定宽度的空域、时域和频域对相应授权用户频谱使用规律进行分析,并及时改变传输参数(如调制方式、功率、使用频段等)来充分利用频谱空洞。基于CR技术的无线认知网络在保证对授权频段内主用户(即授权用户)透明接入的前提下可以显著地提高频谱资源的使用效率。次用户(即非授权用户)通过对频谱环境的实时感知来完成对主用户信号的检测,并及时切换到空闲频段,避免对主用户的干扰。安全高效的频谱感知技术是无线认知网络广泛应用的基础,文献[4,5]对现有的一些感知技术与认知协议进行了详细介绍。

频谱感知的关键问题是如何准确地检测区分主用户(Primary User, PU)与次用户(Second User, SU)信号。由于开放的体系结构、无线通信覆盖范围、广泛存在的干扰因素以及频谱环境动态变化等原因,频谱感知协议的设计面临着诸

到稿日期:2010-04-27 返修日期:2010-08-10 本文受国家自然科学基金项目(60773017)资助。
逄德明(1984—),男,硕士生,主要研究方向为无线认知网络、网络安全,E-mail:pang3724@yahoo.com.cn;胡 罡(1980—),男,博士生,主要研究方向为无线认知网络;徐 明(1964—),男,教授,博士生导师,主要研究方向为移动计算技术、无线网络、无线网络安全。

多挑战[6-8]。在不可信的网络环境中，恶意用户（Malicious User，MU）可以基于软件控制 CR 空中接口，模仿主用户发射信号。次用户在频谱感知的过程中将该节点误判为主用户，并依据无线电礼仪进行退避。MU 根据两类用户对资源使用的优先级不同而进行的仿冒主用户攻击（Primary User Emulation Attacks，PUEA）可以显著地降低 CR 网络的可用空闲频谱资源，产生拒绝服务攻击。由于认知无线电接口的高度可配置性，使得这种仿冒行为极易发生。

PUEA 由 Park 等人首次提出，并基于无线定位技术提出了一种检测方案[9,10]。次用户检测到可疑主用户信号时，首先对信号源进行位置验证，与本地已知的主用户位置进行比较，若不符合则判断为仿冒者。使用的定位技术包括传统的距离比测试、距离差测试或者专用的无线传感器定位网络。利用接收信号强度与距离的关系，在无信号衰减环境下可以对单个仿冒节点进行较为有效的定位。检测过程中需要每个次用户事先掌握工作频段及所处位置范围内所有主用户的物理位置等信息，这样的条件限制使其无法工作在主用户移动或者位置信息不可知的授权网络（如无线麦克风、对讲机频段）。为了实现准确定位，检测过程中需要辅助专用的传感定位网络，这带来了较大的硬件开销。此外，恶意节点通过调整发射功率仍然可以实现基于位置的仿冒攻击。

文献[11]给出了基于能量检测的 PUEA 分析模型。将次用户检测的主用户信号看作对数正态分布随机变量，利用马尔科夫不等式可以得到仿冒成功概率的下界，在理论上证明了 PUEA 的可行性。在此基础上，文献[12]利用主用户与仿冒节点信号概率密度函数的差别，使用加权序列概率比测试进行仿冒攻击检测。与文献[9]相比，该方案考虑了信号衰退的影响，并且可以有效检测多个仿冒节点同时存在的情况。不足之处是增加了过多的预知条件限制，包括仿冒节点的分布及发射功率、次用户与仿冒节点的最小距离、主用户的位置信息与发射功率等。

国内对于认知无线电的研究主要集中在频谱感知与资源分配方面，对于认知网络中存在的安全问题涉及较少。在解决仿冒主用户攻击的问题上，只有北京科技大学的周贤伟等人提出的一种基于 HASH 匹配技术的检测方案[13,14]。首先要求主用户网络的基站在传输的数据上附加用于 HASH 计算的原始数据。次用户对接收到的数据做 HASH 计算，将结果同预先保留的 HASH 值相比较。如果匹配成功，则证明有主用户出现，否则认为存在仿冒攻击。该方案的实现依赖于主用户的通信协作，然而认知协议设计的首要条件是不能对授权网络进行任何形式的调整[15]，且授权网络与认知网络是独立的两个系统，次用户一般无法对主用户发送的信息进行正常解码，也就无法完成对接收到的主用户数据进行 HASH 计算。

本文针对 PUEA 设计了一种基于能量指纹匹配的检测方案。根据信号接收能量与位置的对应关系，每个信源在不同的接收端存在唯一的接收能量集合——能量指纹，将其作为该节点的身份标识。由于仿冒节点与正常主用户对频谱资源的使用方式不同，通过分析不同用户信道接入的特点，实现对仿冒行为的检测。

将该检测算法与频谱感知协议相结合，可以有效提高认知节点频谱检测的准确性，降低对主用户的漏检概率和误检概率。与现有的 PUEA 检测方案相比，没有对授权网络进行修改，且次用户不需要预知授权网络及仿冒节点的任何信息（如位置，分布，发射功率等），使得认知网络的实际应用与部署可以具有更好的灵活性。

本文第 2 节对检测方案的系统模型与所需的假设条件进行了介绍；第 3 节具体讨论了基于能量指纹匹配的仿冒攻击检测算法，并对该方案的安全性进行了分析；第 4 节给出了模拟测试的结果；最后对全文进行总结，并简要介绍了下一步的研究工作。

2 系统模型

2.1 目标认知网络模型

我们以认知 Mesh 为模型构建目标网络，并基于簇（cluster）的结构进行组网[16]。如图 1 所示，SU 根据位置分布及频谱空洞的可用性构建或加入某个簇，每个簇内存在本地控制信道。簇间通信由簇首完成，本文仅研究单个簇内的仿冒攻击检测。SU 基于认知无线电技术实现对频谱资源的动态接入与共享。通过能量感知与特征匹配相结合的方式进行频谱检测，寻找空闲频谱空洞，并通过本地控制信道实现 SU 之间的合作，将本地感知报告发送给簇首，簇首的选取过程参考文献[16]。

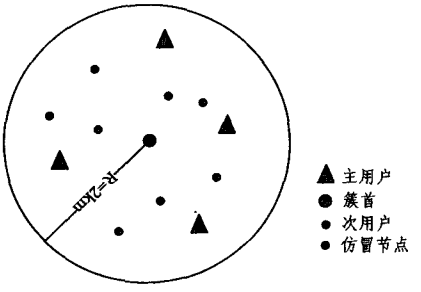

图 1 目标认知网络拓扑

通常使用能量检测的过程如下[4]：SU 检测接收信号能量，并与预设阈值 λ 比较。如果检测能量大于 λ，判断存在主用户，否则信道空闲。这种过于简单的单阈值检测使得 PUEA 极易发生，只要恶意节点的发射功率足够大便可以实现成功的仿冒攻击。本文中我们使用一种经过调整的检测方案，SU 将检测的能量值 P 与预设的两个阈值 λ_1 和 λ_2 进行比较，若 $\lambda_1<P<\lambda_2$，则判断相应信道存在主用户，否则信道空闲。这种方式与上面讨论的单阈值能量检测相比，可以提高频谱感知的准确性，对仿冒攻击行为有一定的限制作用[11]。仿冒节点不仅需要使其信号特征符合主用户，还应调整发射功率，使得接收端信号强度满足上述条件。

2.2 仿冒攻击模型

在无信号衰减的环境下，次用户的接收功率为：

$$P_r=P_tG_t^2G_r^2\frac{h_t^2h_r^2}{d_t^4L} \tag{1}$$

式中，P_t 为信源发射功率，G_t 与 G_r 分别为发送方与接收方的天线增益，h_t 与 h_r 分别为信源与信宿的天线高度，d_t 为信源与信宿的距离，L 为信号衰退因子。

根据次用户的能量检测机制，我们可以得到恶意用户 MU 的仿冒成功条件：

$$|P_p-P_m|<\delta \tag{2}$$

式中，P_p 与 P_m 分别为 SU 检测到的 PU 及 MU 的信号功率，分别由式(1)得出。这样，MU 为完成仿冒攻击，需要掌握自身与 SU 的距离、PU 与 SU 的距离及 PU 的发射功率。

由于认知无线电技术使得 SU 在理论上可以工作在任何频段，包括授权频带和非授权频带，这种动态频谱接入特性使其面临频谱干扰攻击时具有一定的抵抗力。在上述条件下，MU 为阻止 SU 接入空闲频谱空洞，需要在各个频段部署较多的攻击节点，从而增加了攻击成本。因此，在实际的仿冒模型中，MU 会采取一定的攻击策略，在使用较少攻击开销的情况下，降低 SU 的频谱接入概率。

基于认知无线电技术的仿冒节点可以实现对频谱环境的感知，并动态调整空中接口。这种能力使其在进行仿冒攻击时具有一定智能性，即通过感知 PU 与 SU 对频谱资源的使用状况，动态地在各个频段发射仿冒信号。此外，在现有的感知协议设计中，SU 在感知周期内通常采用频谱预测模型生成信道感知序列，以提高对频谱环境的检测效率。MU 获取了信道感知序列，或者检测到 SU 对信道的扫描规律后，通过在相应的信道内以跳频的方式有针对性地进行仿冒攻击，便可显著地提高攻击效率。

针对上述仿冒攻击模型，本文设计了一种能量指纹匹配技术，以有效地提高频谱感知的准确率。

首先对网络模型进行以下假设：

· 认知网络中存在多个主用户、次用户及仿冒节点(如图 1 所示)。

· 次用户与仿冒节点位置固定，可以动态加入或离开网络，簇内的次用户以同步的方式进行合作频谱感知(考虑到在实际的仿冒攻击中以自私仿冒节点居多[6]，这样在 mesh 网络模型中固定 SU 与 MU 的位置是合理的)。

· 仿冒攻击检测算法不需要预知主用户与仿冒节点的物理位置及发射功率等信息。

· 仿冒节点之间不存在合作关系，即每个节点根据自身掌握的信息及本地生成的攻击序列在各个频段进行仿冒攻击。多个仿冒节点在同一个次用户处的信号累积无法进行全局控制。

3 基于能量指纹匹配的仿冒攻击检测

3.1 检测依据

MU 在授权频段发射仿冒信号，前提是自身不会对 PU 产生干扰(对 PU 的干扰会被现有的授权频段保护策略检测)，即只能在频谱空洞内进行仿冒攻击。因此 MU 必须具备检测主用户的能力，当 PU 出现时，MU 应调整到其他信道。此外，为了提高仿冒攻击的成本收益比，MU 会采用前面讨论的跳频攻击模式。这种行为使得同一个仿冒者在不同信道内出现；当网络中存在多个仿冒节点时，由于不同节点在选择干扰信道时的随机性，同一个信道内也可能出现不同的 MU。由于物理位置及发射功率的差别，SU 会在同一个信道内检测到不同的主用户，然而这种情况在授权网络中是不可能出现的。以上讨论的两种异常行为为本文的检测方案提供了基础。

由上述分析可知，MU 在不同信道发射仿冒信号，SU 如果能够探知信号来源的位置，那么会发现在不同信道内的“授权用户”来自同一点。然而正常主用户使用信道的方式是静态的，同一个用户不会出现在不同频段，由此可以判断该可疑位置处的节点为仿冒攻击者。同理，如果在相同信道中检测的主用户信号来自不同位置，也能证明这种攻击行为的存在。这里将物理位置作为攻击者的身份标识，在实际网络条件下，我们可使用 MU 的能量标识代替物理位置，从而将多个不同位置的 SU 对同一仿冒节点检测的能量值作为其指纹信息。基于三角定位原理，只要存在至少 3 个不同位置的 SU 记录对信源的接收能量，便可唯一确定该节点，并将其作为身份标识，用于统计分析该节点的频谱使用模式。

由于不同位置的 SU 接收到的同一主用户信号能量不同，多个 SU 利用自身位置相对主用户的唯一性得到的信号能量指纹是不可复制的，指纹相同的信号必然来自同一个节点。MU 只能实现对单个 SU 的成功仿冒，但无法在全网范围内产生与正常主用户相同的能量指纹。只有当 MU 的位置及功率与主用户同时保持一致时才能实现成功的仿冒攻击，然而在实际网络环境下这种情况不可能出现。

PU 及 MU 能量指纹的唯一性是保证有效检测的关键。由于 PU 的位置及发射功率不变，其能量指纹只受传输环境的影响。然而 MU 的发射功率是可以调整的，其能量指纹可能发生变化。为了解决这个问题，我们使用文献[11]中的检测方式，设置两个约束阈值，只有 SU 检测到的信号功率满足给定阈值条件时才会将信源判定为主用户。若 MU 的发射功率变化，则无法满足式(2)的条件，本文只考虑发射功率不变的情况。

SU 检测的“主用户”信号可能来自一个或多个 MU。当信号来自单个 MU 时，SU 可以准确地通过下文介绍的能量指纹匹配检测仿冒行为。下面我们考虑多个 MU 存在的情况：MU 一般以随机的方式在各个信道中发射仿冒信号，在有效干扰区域内，多个仿冒节点(两个以上)在同一时刻出现在相同信道中的概率为：

$$\Phi=\frac{C_m^2 \cdot C_n^1 \cdot n^{m-2}}{n^m} \tag{3}$$

式中，m 为有效干扰距离内的 MU 数量，n 为认知网络工作的目标频段信道数。一般情况下 Φ 值较小(例如当 SU 与 MU 的比例为 1∶3，目标信道数为 50，同一信道中出现两个以上仿冒节点的概率 Φ 为 6%)，即通常每个 SU 检测到的信号来自单个 MU。即使多个 MU 在同一信道中出现，由于接收端的能量累积使得 P_m 远大于 P_p，这样 SU 的初次检测即可判断仿冒行为。

3.2 检测算法

如图 2 所示，SU 在感知周期内使用特征匹配及能量检测相结合的方式对目标频段进行扫描。当检测到主用户时，记录所在信道及能量值，并将其作为本地感知报告通过控制信道发送给簇首。簇首在得到簇内节点的感知报告后生成主用户能量指纹，得到临时指纹表，将其与已有的指纹库进行比较。

SU 进行能量感知，首先根据以下公式进行初步判断：

$$|P_{i,j}^n - P_{i,j-1}^n| < \delta$$

式中，$P_{i,j}^n$ 为第 i 个次用户在第 j 个感知周期内对信道 n 的感知能量值，$P_{i,j-1}^n$ 是上一个感知周期内信道 n 的能量值。δ 是不考虑仿冒攻击情况下正常使用能量检测的阈值，该值的选取与分析可参考现有研究方案，本文不做讨论。若检测到的

能量满足上述条件，则进行下一步检测—能量指纹匹配。在匹配相同信道内的信号时，若指纹相同，说明信号来自同一个节点，信道的使用方式符合授权网络规则，此时进行指纹更新；若在相同的信道内检测的信号指纹不同或在不同信道内的指纹相同，证明了相同的频段出现不同的主用户，或者不同的频段中出现了相同的主用户，这样就可以判定存在仿冒攻击行为。在某些应用场景中，不同的主用户也可能工作在同一个信道，此时可以只匹配不同频段信号，本文暂不考虑这种情况。

对于主用户移动模型下的授权网络（如无线麦克风、对讲机等），通过调整上述检测算法，同样可以实现对仿冒行为的检测。主用户移动过程中在接收端 SU 的能量指纹会发生变化，但由于工作频率固定，每个信道只可能存在一个主用户。此时只需要针对不同信道进行指纹匹配而不考虑相同信道的情况，即可完成判断。

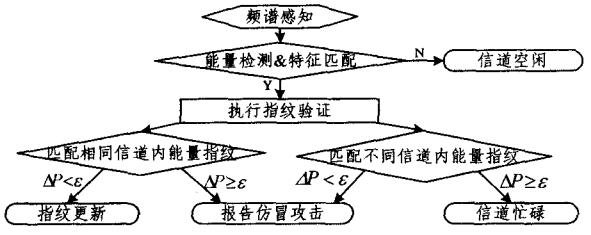

图 2　仿冒攻击检测流程图

3.2.1　主用户指纹采集

在部署认知网络过程中，由于对原有授权网络不能进行任何改变[15]，SU 与 PU 无法通信，同样也无法对 PU 的信号进行正常的解码。为了完成对 PU 的指纹采集，我们使用基于信号能量的方式。在不同感知周期由不同位置的 SU 对各个信道进行扫描，检测并收集主用户信息，将表 1 的内容作为本地报告发送给簇首，由其生成各个信道的能量指纹，如表 2 所列，其中 $P_{i,j}^{n}$ 为 SU 检测的信号能量值，当检测到主用户信号时 $k_n=1$，否则 $k_n=0$。

表 1　第 i 个认知节点在第 j 个感知周期得到的各个信道的主用户信号能量值

	信道 1	信道 2	…	信道 n
能量值	$P_{i,j}^{1}$	$P_{i,j}^{2}$	…	$P_{i,j}^{n}$

表 2　簇首节点各个信道内主用户能量指纹库

	节点 1	节点 2	…	节点 i	是否存在 PU
信道 1	$P_{1,j}^{1}$	$P_{2,j}^{1}$	…	$P_{i,j}^{1}$	k1
信道 2	$P_{1,j}^{2}$	$P_{2,j}^{2}$	…	$P_{i,j}^{2}$	k2
…	…	…	…	…	…
信道 n	$P_{1,j}^{n}$	$P_{2,j}^{n}$	…	$P_{i,j}^{n}$	kn

向量 $M_j^n=(P_{1,j}^n,P_{2,j}^n,\cdots,P_{i,j}^n)$ 即为第 j 个感知周期在信道 n 内检测到的主用户能量指纹。在一般情况下，由于主用户的发射功率不变，在不同感知周期内同一节点的能量指纹应该是相似的；主用户对信道的静态使用方式又使得不同信道内节点的能量指纹不同。

指纹库的更新：当认知节点在第 j 个感知周期内检测到信道 n 存在主用户时，首先将其记录在临时指纹库，并与该信道内记录的主用户的能量指纹进行匹配。若匹配结果不同，则判定存在仿冒攻击，否则进行指纹更新，更新规则如下：

$$M_j^n=[k_n(P_{1,j}^n\quad P_{2,j}^n\quad P_{3,j}^n\quad\cdots)+k_n'(P_{1,j-1}^n\quad P_{2,j-2}^n\quad P_{3,j-3}^n\quad\cdots)]\cdot 2^{-k_n\cdot k_n'}\tag{4}$$

式中，k_n' 取自临时指纹库，与 k_n 取值方式相同。

通过多个感知周期对能量指纹库进行更新，可以提高节点指纹信息的准确性，降低信号传输环境的影响或偶然因素引起的指纹偏差。

3.2.2　指纹匹配

在完成频谱感知，得到临时指纹信息后，簇首将存在主用户的信道对应的能量指纹与原有指纹库进行匹配。比较任意两个信道 α 和 β 内检测到的主用户能量指纹过程如下：

$$\Delta P=|M_j^{\alpha}-M_{j-1}^{\beta}|=||P_{1,j}^{\alpha}-P_{1,j-1}^{\beta}|+|P_{2,j}^{\alpha}-P_{2,j-1}^{\beta}|+\cdots+|P_{i,j}^{\alpha}-P_{i,j-1}^{\beta}||/i\tag{5}$$

$\Delta P<\varepsilon$：指纹吻合，信号来自同一个主用户

$\Delta P\geqslant\varepsilon$：两个信道内有不同的主用户

式中，i 为簇内节点总数，SU 可以动态加入或离开网络，不会影响正常的检测过程。

如果信道 α 和 β 内主用户信号来自同一个节点，那么 ΔP 的理论值接近于 0，但由于无线信号受环境的影响，ΔP 与理论值会产生偏差。根据式(2)可以得到以下条件：

$$P_p-\delta<P_{i,j}^{\alpha},P_{i,j-1}^{\beta}<P_p+\delta$$
$$|P_{i,j}^{\alpha}-P_{i,j-1}^{\beta}|<2\delta\tag{6}$$
$$\Delta P<2\delta$$

只有认知节点的接收功率 $P_{i,j}^{\alpha}$ 满足式(2)时才会将检测到的节点判定为授权用户，这样有 $\varepsilon<2\delta$。簇首节点检测算法的具体流程如图 3 所示。

```
for each j do                          //在每个感知周期 j 执行一次能量指纹匹配
  for each i∈S do                      // S 为簇内认知节点集合
    mesh_header[i,n] = node_i(n);
  end                                  //簇首收集节点 i 的感知报告，生成指纹库
  for each n∈C do                      // C 为工作频段内所有信道的集合
    P1 = |M_j^n − M_{j-1}^n|           //在相同信道内执行指纹匹配
    if( P1 < ε )
      M_j^n = fingerprint_update( M_j^n , M_{j-1}^n )      //指纹更新
    else
      Report the PUEA;
    end if
    for each m∈C−n do
      P2 = |M_j^n − M_{j-1}^n|         //在不同信道执行指纹匹配
      if( P2 > ε )
        Dectect the normal primary user;
      else
        Report the PUEA;
      end if
    end
  end
end
```

图 3　簇首节点能量指纹匹配算法

3.3　主用户信息已知情况下的仿冒行为检测

对于一些特定的授权网络（如 TV 网络），主用户（TV 信号发射器）信息如物理位置、发射功率以及信号的传输模型等可以通过一定方式获取。在这种网络模型中，可以使用简化的指纹匹配方案进行仿冒攻击检测。SU 根据已知信息计算 PU 在本地的接收功率并发送到簇首，这样可以得到该主用户理论上的能量指纹。在实际的频谱感知过程中，簇首根据 SU 对相应频段的实测结果生成主用户的能量指纹测试值，并与理论值进行匹配，判断是否为仿冒者。

已知主用户 k 的能量指纹：

$$M^k=(P_1^k,P_2^k,\cdots,P_j^k)$$

为减小传输环境对接收功率的影响，将多个周期内对 PU 信号的实际测试值与理论值相结合，可以得到更准确的指纹信息。簇首在每个感知周期内对各个信道检测的主用户与已有数据进行匹配，通过将 ΔP 与阈值进行比较，判断检测的节点指纹信息与该信道内已知的主用户指纹是否相同：

$$\Delta P=|M_j^k-M_j^n|=(|P_1^k-P_{1,j}^n|+|P_2^k-P_{2,j}^n|+\cdots+|P_i^k-P_{i,j}^n|)/i \tag{7}$$

与之前讨论的算法相比，简化的指纹匹配方案在检测仿冒行为时所需的时间更短，不需要等待 MU 出现跳频行为即可完成检测；降低了计算开销，只对相同信道内的能量指纹进行匹配，不必考虑不同信道内的情况；此外，对于 MU 移动的网络模型也可以准确检测，不会对算法产生影响。第一种检测方案的优点是不需要预知主用户的任何信息，包括发射功率、位置信息、环境因素（如信号衰退、多径效应）等，实际上这种检测方式与主用户没有直接关联，可以适用于不同类型的授权网络，检测过程中使用的所有数据是由 SU 对认知网络的实时检测得到的。但存在的不足是对仿冒者的跳频行为的判断需要多个感知周期，完成攻击检测所需的时间相对较长。

3.4 性能分析

对两种错误概率，即误检率与漏检率（见表 3）进行分析，首先定义以下两个事件：

事件 A：信号来源为主用户，但判断为仿冒节点。

事件 B：信号来源为仿冒节点，但判断为主用户。

表 3 两种错误概率分析

	检测为 PU	检测为 MU
信号源为 PU	正确	P(A)
信号源为 MU	P(B)	正确

误检率 $P(A)$：事件 A 发生的概率。

事件 A 只可能在以下两种情况发生：

Ⅰ. 不同信道中的主用户能量指纹在簇首内的匹配结果相同。由于主用户静态接入信道，同一个主用户不会在不同的频段内出现。不同频段的各个主用户能量指纹匹配相同的概率受匹配阈值的 ε 影响，通过对 ε 的适当选取可以减小该事件的发生概率。

Ⅱ. 同一个信道中，正常主用户的信号在不同的感知周期内到达接收端的能量不同。由于主用户的发射功率及位置不变，接收功率只受外部传输环境影响，环境的变化可能会导致事件 A 发生。我们使用多个分布在不同位置的次用户生成能量指纹，并且通过在多个感知周期内对接收的信号进行平滑处理来降低环境的影响，进而减小误检概率。

漏检率 $P(B)$：事件 B 发生的概率，即仿冒成功且未被检测的概率。

仿冒攻击检测的正确率为：

$$P_s=1-(P(A)+P(B)) \tag{8}$$

事件 A 可以通过对 ε 的适当选取来降低发生概率，那么影响对仿冒攻击检测正确率的主要因素是漏检概率 $P(B)$。在两种情况下事件 B 可能发生：首先，当仿冒节点只在单个频段内发射仿冒信号时，第一种检测方案无法区分主用户与仿冒节点，但第二种方案仍然可以正常检测。从另一个角度讲，如果仿冒节点以静态信道接入的方式进行恶意攻击，那么对认知网络的整体性能影响十分有限（考虑到认知网络较宽的可用频段）；其次，同一个仿冒节点在不同的频段内发射仿冒信号，但次用户在匹配不同信道内的能量指纹时并没有吻合，匹配阈值 ε 及检测阈值 δ 是影响该事件的主要因素。

考虑以下情况：当信道 α,β 内检测到的信号功率 $P_{i,j}^{\alpha}$ 与 $P_{i,j-1}^{\beta}$ 来自相同的仿冒节点时存在以下关系：

$$P(|P_p-P_{i,j}^{\alpha}|<\delta)=P(|P_p-P_{i,j-1}^{\beta}|<\delta)=q$$

即未使用指纹匹配检测时 MU 仿冒成功的概率为 q

$$P(|P_{i,j}^{\alpha}-P_{i,j-1}^{\beta}|<2\delta)=q$$

$$P(\Delta P<2\delta)=q$$

因此，当设定 $\varepsilon<2\delta$ 时，δ 的取值直接影响仿冒成功率与检测成功率。当 δ 增大时，MU 仿冒成功的概率增加，对攻击的检测成功率 P_s 也同时增加，但过大的匹配阈值 ε 也可能导致 $P(A)$ 的增加；当 δ 减小时，仿冒成功率下降，同时匹配阈值 ε 的减小使得漏检概率 $P(B)$ 增加，导致仿冒攻击检测的正确率下降。通过选取合适的能量检测阈值 δ 及匹配阈值 ε，可以在保证 $P(A)$ 值较低的前提下减小 $P(B)$，最终提高检测成功概率 P_s。

4 模拟测试

本节将介绍使用能量指纹进行仿冒主用户攻击检测的仿真测试，主要考察匹配阈值 ε 及信号传输环境的变化对检测概率与误检概率的影响。

4.1 实验环境

如图 1 所示，在一个半径为 2km 的认知网络中随机分布着若干（2～10 个）认知节点，并基于簇的结构组成 mesh 网络。仿冒攻击节点作为认知网络的一部分，通过在各个信道发射主用户信号来增加自己的可用频谱资源，阻止其他节点对频谱空洞的接入。测试中设置 3 个仿冒节点随机分布在认知网络模型中，并分别在 300MHz～500MHz 频段随机选择仿冒信道。

信号在传播过程中的路径损耗根据对数正态阴影路径衰减模型计算[17]：

$$PL(d)=\overline{PL}(d)+X_{\sigma} \tag{9}$$

式中，d 为信号发送方与接收方的距离，$\overline{PL}(d)$ 为路径损耗的均值，X_{σ} 是以 0 为均值、以 σ 为标准差的高斯分布随机变量，代表信号传输过程中阴影效应的影响。$\overline{PL}(d)$ 的计算使用 IEEE 802.22 工作组推荐的 HATA 模型[17]：

$$\overline{PL}(d)=29.67-8.29(\log 1.54)^2-13.82\log h_{te}+7.38\log f_c-4.78(\log f_c)^2+(44.9-6.55\log h_{te})\log d \tag{10}$$

式中，h_{te} 与 h_{re} 为发送方和接收方天线高度，f_c 为工作频率。

信号的接收功率为：

$$P_r=P_t-PL(d) \tag{11}$$

式中，P_t 为发射功率。式(9)－式(11)使用的数值单位均为 dBm。根据上述传输模型，对本文的仿冒检测算法进行模拟测试，得到的结果如下。

4.2 测试结果

实验中首先对仿冒行为的检出率进行测试：同一仿冒节点在不同信道内发射主用户信号，由簇内的认知节点记录接收信号能量，并发送给簇首，生成该仿冒节点的能量指纹，若匹配成功即完成了一次仿冒攻击检测。实验过程中的匹配阈值 ε 由 0dBm 增加到 30dBm，步长为 1，σ 取值为 8dBm。针对每次选取的阈值进行 100 次测试，得到了对仿冒行为的检出率 P。图 4 所示为匹配阈值 ε 与概率 P 的关系曲线，3 条曲线分别对应的检测节点数为 2，5，10。从图中可以看到，检出率 P 随着匹配阈值 ε 增加而递增。当认知节点增加时，可以减

小信号传输过程中的随机性对指纹匹配的影响，从而提高检测的成功率。在实际测试中，信号在衰退环境中的不稳定传输使得检测概率曲线出现较大波动，图 4 的曲线是经过 20 次重复实验，对得到的 20 组测试数据进行平滑处理后的结果。从图中可以看出，10 个节点的测试曲线相对另外两组测试更加稳定，表明了检测节点的增加可以提高攻击检测的稳定性与可靠性。

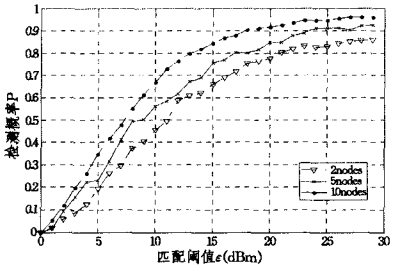

图 4　匹配阈值 ε 与检测概率 P 的测试结果

信号在传播过程中由于阴影效应（即多径效应）的影响，接收功率是随机可变的。不同的环境会对基于能量的检测算法产生较大影响，当环境复杂多变时（如城市环境），对仿冒行为的检测会出现不稳定性。在路径损耗模型(9)中的 σ 称为阴影方差（shadowing debiation），描述了阴影效应对接收功率的影响程度。σ 的取值通过对实际测试的数据使用线性回归得到，通常在室外环境下 σ 介于 4～12dBm[18]。实验中，我们分别将 σ 设为 4，8，11.8，并设置 5 个检测节点对不同传输环境下的检测概率进行测试。实验结果表明了（见图 5）信号传输环境对检测算法存在较大影响，当 σ 取 11.8 时（对应的环境变化快，地形复杂），有效检测概率只有 60%左右（匹配阈值 ε 为 15～20dBm）。而对于简单的传输环境中，该算法可以有较好的检测性能。

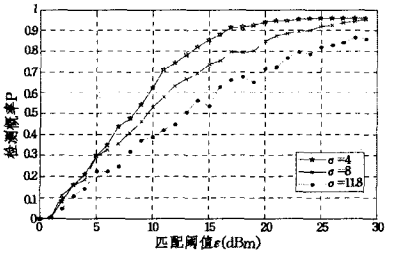

图 5　不同阴影效应下检测概率 P 的测试结果

实验的最后对检测算法的误检概率 $P(A)$ 进行了测试，考察了匹配阈值 ε 对误检概率的影响。在图 1 所示的网络模型中选取两个主用户，分别工作在 300MHz 与 350MHz，对其进行能量检测，得到图 6 所示的测试结果。当匹配阈值 ε 小于 20dBm 时，误检概率 $P(A)$ 大约在 2%以下，此时检测成功率 P 为 85%（5 个检测节点的情况），当 ε 超过 20dBm，$P(A)$ 迅速增加，导致了更多的误检事件发生。

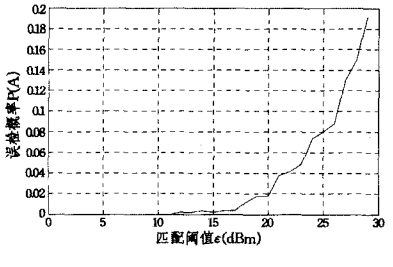

图 6　匹配阈值 ε 与误检概率 $P(A)$ 的测试结果

结束语　本文针对无线认知网络中仿冒主用户攻击行为提出了一种新的检测方案，该方案与现有的频谱感知协议相结合，能够提高频谱感知的准确性。认知节点通过采集主用户与仿冒节点的能量指纹信息，比较不同用户的频谱使用模式，完成对仿冒节点的检测。理论分析及模拟测试结果表明，在保持较低的误检概率前提下可以有效地完成对仿冒节点的检测。

该方案不需要预知授权网络及仿冒节点的相关信息，便于认知网络的实际部署应用，不足之处是认知节点使用的能量检测在实际网络环境中会存在不稳定性。接下来的工作重点是通过认知节点采集主用户更多的工作参数信息（如射频指纹）来完成指纹匹配，并解决移动网络模型中的仿冒攻击检测。

参 考 文 献

[1] ET Docket No 03-222 Notice of proposed rule making and order [S]. Washington: Federal Communications Commission, December 2003

[2] McHenry M. Spectrum white space measurements[C] // Presented to New America Foundation BroadBand Forum. June 2003

[3] Mitola J. Cognitive radio: an integrated agent architecture for software defined radio [D]. Royal Institute of Technology (KTH). Stockholm, Sweden, June 2000

[4] Akyildiz I F, Lee W, Vuran M C, et al. Next generation/dynamic spectrum access/cognitive radio: A survey[J]. Elsevier Journal on Computer Networks, 2006, 50: 2127-2158

[5] Visotsky E, Kuffner S, Peterson R. On collaborative detection of tv transmission in support of dynamic spectrum sharing [C]// Proceedings IEEE Symposium of New Frontiers in Dynamic Spectrum Access Networks (DySPAN). Nov. 2005: 338-345

[6] Brown T X, Sethi A. Potential Cognitive Radio Denial-of-Service Vulnerabilities and Protection Countermeasures: A Multi-dimensional Analysis and Assessment[J]. Mobile Networks and Applications, 2008, 13(5): 516-532

[7] Chen R, Park J, Hou Y, et al. Toward Secure Distributed Spectrum Sensing in Cognitive Radio: Networks[J]. IEEE Communications Magazine, 2008, 46: 50-55

[8] Burbank J L. Security in Cognitive Radio Networks: The Required Evolution in Approaches to Wireless Network Security [C] // CrownCom 2008. 3rd international Conference on. May 2008: 1-7

[9] Chen R, Park J M. Ensuring trustworthy spectrum sensing in cognitive radio networks[C]// Proceedings, IEEE Workshop on Networking Technol for Software Defined Radio Networks (SDR). Sep. 2006: 110-119

[10] Chen R, Park J M, Reed J H. Defense against primary user emulation attacks in cognitive radio networks[J]. IEEE Journal on Selected Areas in Communications: Special Issue on Cognitive Radio Theory and Applications, 2008, 26(1): 25-37

[11] Anand S, Jin Z, Subbalakshmi K P. An Analytical Model for Primary User Emulation Attacks in Cognitive Radio Networks[C]// Proc. of 3rd IEEE Symp. on New Frontiers in Dynamic Spectrum Access Networks (DySPAN'08). 2008: 1-6

（下转第 69 页）

这也进一步证明了 MDPTS 网络具有更好的系统性能。

在此基础上，为了对 MDPTS 网络中的系统性能进行进一步的优化，本文以系统的误帧率最小为目标，采用蒙特卡罗方法对系统的功率分配方案进行仿真。在发射端已知统计信道信息的情况下，以信噪比 SNR 在 30dB～90dB 范围内，$R=2,8$ 为仿真条件，得图 5、图 6。

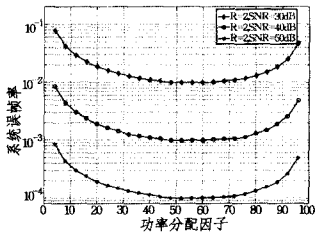

图 5 $R=2$ 时基于发射端已知统计信道信息的系统功率分配

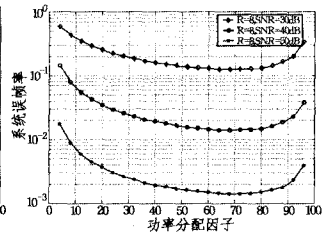

图 6 $R=2$ 时基于发射端已知统计信道信息的系统功率分配

分析图 5、图 6 中横坐标即功率分配因子的百分比 k，可以看出，当 $R=2,8$ 时，再生中继网络中选择 $k=\frac{1}{2}$，$k=\frac{2}{3}$ 时系统的功率分配达到最优。这一仿真结果也与本文推导出的系统最优功率分配方案吻合，证明了式(18)中最优解的准确性。

结束语 本文将协作通信技术引入到无线再生中继网络中，设计了一种基于 MDP 协议的信号传输方案 MDPTS，对系统的中断事件进行了定义，进而推导出系统的中断概率与误帧率，并结合系统的传输速率利用分集增益与复用增益的权衡对系统的性能进行了细致的分析。在此基础上提出了在发射端和中继器间的功率分配方案，运用拉格朗日法求得最优解。仿真结果表明，与采用传统传输方案的网络相比，采用 MDPTS 的网络具有更高的分集增益和复用增益，因此具有更高的系统性能。最后，本文采用蒙特卡罗方法对系统的功率分配方案进行了仿真，仿真实验结果也与文中的功率分配方案最优化结果相吻合，证明了文中推导的准确性。

参 考 文 献

[1] Nabar R U, Kneubuhler F W, BAolcskei H. Performance limits of amplify-and-forward based fading relay channels[C]// Proc. IEEE Int. Conf. Acoustics, Speech and Signal Processing. Canada, Montreal, May 2004, 4: 565-568

[2] Nabar R U, BAolcskei H, Kneubuhler F W. Fading relay channels: Performance limits and space-time signal design[J]. IEEE J. Sel. Areas Commun., 2004, 22: 1099-1109

[3] Azarian K, El-Gamal H, Schniter P. On the achievable diversity-multiplexing tradeoff in half-duplexing cooperative channels[J]. IEEE Trans. Inf. Theory, 2005, 51: 4152-4172

[4] Lee I, Kim D. BER analysis for decode-and-forward relaying in dissimilar Rayleigh fading channels[J]. IEEE Commun. Lett., 2007, 11: 52-54

[5] Beaulieu N C, Hu J. A closed-form expression for the outage probability of decode-and-forward relaying in dissimilar Rayleigh fading channels[J]. IEEE Commun. Lett, 2006, 10: 813-815

[6] Laneman J N, Wornell G W. Distributed space-time-coded protocols for exploiting cooperative diversity in wireless networks [J]. IEEE Trans. Inf. Theory, 2003, 49: 2415-2425

[7] Laneman N, Tse D N C, Wornell G W. Cooperative diversity in wireless networks: Efficient protocols and outage behavior[J]. IEEE Trans. Inf. Theory, 2004, 51: 3062-3080

[8] Nabar R U, Kneubuhler F W, BAolcskei H. Performance limits of amplify-and-forward based fading relay channels[C]// Proc. IEEE Int. Conf. Acoustics, Speech and Signal Processing. Montreal, QC, Canada, May 2004, 4: 565-568

[9] Nabar R U, BAolcskei H, Kneubuhler F W. Fading relay channels: Performance limits and space-time signal design[J]. IEEE J. Sel. Areas Commun., 2004, 22: 1099-1109

[10] Wang T, Giannakis G B. High-throughput cooperative communications with complex field network coding[C]// Proc. 41st Annual Conference on Information Sciences and Systems (CISS 2007). Mar 2007, 12: 253-258

[11] Zheng L, Tse D N C. Diversity and multiplexing: A fundamental tradeoff in multiple antenna channels[J]. IEEE Trans. Inf. Theory, 2003, 49: 1073-1096

[12] Li Jun, Chen Wen, Zhao Cheng, et al. On the Throughput-Reliability Tradeoff Analysis in Amplify-and-Forward Cooperative Channels[C]// IEEE International Conference on Communications(ICC). Beijing, May 2008, 3: 1034-1038

[13] Tarokh V, Seshadri N, Calderbank A R. Space-Time Codes for High Data Rate Wireless Communications: Performance Criterion and Code Construction[J]. IEEE Trans. Inf. Theory, 1999, 44: 744-765

[14] Tarokh V, Seshadri N, Calderbank R. Space-time block codes from orthogonal designs[J]. IEEE Trans. Inf. Theory, 1999, 45: 1456-1467

[15] Hunter T E, Nosratinia A. Diversity through coded cooperation [J]. IEEE Trans. Wireless Commun, 2006, 5: 283-289

[16] Hunter T E, Sanayei S, Nosratinia A. Outage analysis of coded cooperation[J]. IEEE Trans. Inf. Theory, 2006, 52: 375-391

(上接第 33 页)

[12] Jin Z, Anand S, Subbalakshmi K P. Detecting Primary User Emulation Attacks in Dynamic Spectrum Access Networks[C]// IEEE International Conference on Communications(ICC). Dresden, Germany, June 2009

[13] 薛楠，周贤伟，辛晓，等. 一种解决认知无线电网络模仿主用户攻击问题的方案[J]. 计算机科学，2009，36(8)

[14] 薛楠，周贤伟，刘涛，等. 基于簇的分布式认知无线电网络安全体系结构[J]. 电信科学，2008(11)

[15] Federal Communication Commission, Notice for Proposed Rule-making(NPRM 03-322): Facilitating Opportunities for Flexible, Efficient, and Reliable Spectrum Use Employing Cognitive Radio Technologies[S]. No. 03-108. ET Docket, Dec. 2003

[16] Chen Tao, Zhang Hong-gang, Zhou Xia-fei, et al. CogMesh: A Cluster Based Cognitive Radio Mesh Network[C]// 2nd IEEE International Symposium on. New Frontiers in Dynamic Spectrum Access Networks(DySPAN 2007). 2007: 168-178

[17] Rappaport T S. Wireless communications: principles and practice [M]. Prentice Hall, 1996

[18] Seidel S Y, Rappaport T S, Jain S, et al. Path loss, scattering and multipath delay statistics in four European cities for digital cellular and microcellular radiotelephone[J]. IEEE Trans. Vehicular Technology, 1991, 40(4): 721-730