doi:10.3969/j.issn.1000-436x.2013.01.017

认知无线电网络安全综述

裴庆祺[1]，李红宁[2]，赵弘洋[1]，李男[1]，闵莹[1]
(1. 西安电子科技大学 综合业务网理论及关键技术国家重点实验室，陕西 西安 710071；
2. 西安电子科技大学 计算机学院，陕西 西安 710071)

摘 要：认知无线电网络通过认知用户对无线环境的感知，获得频谱空洞信息，在不干扰主用户的前提下，伺机接入空闲频谱，从而满足更多用户的频谱需求，提高频谱资源的利用率，然而，也带来了前所未有的安全挑战。依托认知环，从数据信道、控制信道和终端设备三方面介绍其安全性所面临的问题，以及现有的解决方案，最后给出认知无线电网络的安全建议。

关键词：认知环；控制信道；数据信道；融合中心
中图分类号：TN 929 **文献标识码**：A **文章编号**：1000-436X(2013)01-0144-15

Security in cognitive radio networks

PEI Qing-qi[1], LI Hong-ning[2], ZHAO Hong-yang[1], LI Nan[1], MIN Ying[1]
(1.National Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China;
2. School of Computer Science and Technology, Xidian University, Xi'an 710071, China)

Abstract: Cognitive radio can obtain and access spectrum white holes without interfering primary users by sensing wireless environment to meet with the more spectrum requirement of users and improve spectrum utilization. However, it also brings new secure challenges that different from traditional wireless networks. Relying cognition cycle, the security issues in cognitive radio networks are presented from data channel, control channel and terminal equipment, then the existing defensive measures and propose the secure recommendations of cognitive radio networks are introduced.

Key words: cognition cycle; control channel; data channel; fusion center

1 引言

由于无线通信的快速发展，固定的频谱分配已不能满足越来越多的用户需求。FCC 考虑在不干扰授权用户(主用户)的前提下开放一部分授权频谱供非授权用户使用，认知无线电网络（CRN, cognitive radio network）应运而生。认知无线电的概念首先在 1999 年由 MITOLA J 提出[1]，他指出认知无线电是软件无线电的智能化，是软件无线电的特殊扩展，比软件无线电更具灵活性。MITOLA J 在其博士论文中给出了认知环模型，详细分析了计划阶段、决策阶段、执行阶段和学习阶段的功能特点，开创了认知无线电的研究方向。随着认知无线电的发展，延伸到网络层面，认知无线电网络可以在不影响主用户的前提下，利用空闲的授权频段，从而提高频谱资源的利用率，满足更多无线用户的频谱需求[2]，是近年来解决无线频谱资源稀缺的一项重要技术。

认知无线电网络，其本质是具有认知特性的无线通信网络。该网络能够观察周围的无线网络环境，利用环境认知获取频谱使用信息，对获取的信息经过处理与学习，进行智能的分析与决策，并动态接入可用频谱[3]，最终自适应并重构网络，以适应动态变化的认知无线电网络环境，从而达到最优

收稿日期：2012-06-25；**修回日期**：2012-12-28
基金项目：国家自然科学基金资助项目(61172068，61003300)；新世纪优秀人才支持计划基金资助项目(NCET-11-0691)；中央高校基本科研业务费专项基金资助项目(K50511010003)
Foundation Items: The National Natural Science Foundation of China(61172068，61003300); The Program for New Century Excellent Talents in University (NCET-11-0691) ;The Fundamental Research Funds for the Central Universities (K50511010003)

的网络性能[4]。认知无线电网络中的用户称为认知用户，与之对应的是主用户。认知用户在主用户不使用信道时接入进行通信，一旦主用户信号返回，认知用户立即撤离正在通信的信道，寻找其他可用的空闲信道进行通信。因此，认知用户首先应具有频谱感知的功能，即从无线环境中进行信号检测，确定频谱空洞，经过分析和调整，在不影响主用户的前提下利用频谱空洞进行通信。

综上所述，认知无线电网络应该具备以下功能：1）感知功能，认知无线电网络必须能够精确地感知无线频谱，并在相应的频段内进行频谱检测，获得空闲可用频段；2）分析决策功能，即认知无线电网络能够根据外界环境的变化，参考本身的需求，进行相关的分析决策；3）重配置功能，通过与外部环境的交互，考虑到本身需求，进行参数的调配。

本文首先对认知无线电网络关键技术及流程进行了概述，接着分类介绍了认知无线电网络中的安全问题，并分析了现有的安全解决方案，最后给出认知无线电网络的安全建议。

2　认知无线电网络关键技术及流程

2.1　关键技术介绍

认知无线电网络中的关键技术有频谱检测技术、动态频谱管理技术、自适应频谱分配技术等。在可用频谱实时变化的环境中，认知用户需要对外部环境进行感知，借助历史使用状况的学习和经验积累，对动态可用频谱信息进行分析；充分考虑认知用户需求，自适应调节各种参数，合理分配资源，以便更好地适应环境，达到最优化配置。

频谱检测技术，即频谱感知技术[5]，是认知无线电网络运行的前提条件，是指认知用户通过各种信号检测和处理手段来获取无线网络中的频谱使用信息，寻找频谱空洞。现有的频谱感知技术主要有以下几种：能量检测算法[6~8]，根据接收信号能量或功率的大小，与设定的门限值进行对比，若大于门限值，则认为是主用户的活动，否则是认知用户的活动；匹配滤波器检测算法[9,10]，通过采样对每个信号进行分析，首先需要为每一类主用户设置专门的接收机，并已知主用户的信号信息，通过匹配来判定信号源；协方差矩阵检测算法[11~13]，通过计算接收信号样本的协方差矩阵来检测主用户信号是否出现。由于主用户出现时接收信号的样本协方差矩阵行列式和噪声的样本协方差矩阵行列式通常是不同的，由此就可以通过接收信号的样本协方差矩阵判决出主用户是否出现。循环平稳特征检测算法[10, 14, 15]，通过分析已调信号的频谱自相关函数探测出信号特征，将噪声和信号区分开来，但此方法复杂度较高。目前，频谱感知方式以合作感知最为普遍，多种合作频谱感知算法被提出[16~21]。与单节点感知相比，合作感知的优点是能够提高感知的准确度，减少隐藏终端等问题造成的影响。

动态频谱管理技术，是一种时变的优化问题。由于认知无线电网络可用频谱的实时动态性，传统的频谱管理技术不再适用。即除了用户需求的实时变化，可用频谱资源也在随着主用户的使用情况而变化。因此，认知无线电网络中的动态频谱管理技术需要考虑到可用资源与用户需求 2 个方面，通过对可用频谱资源的分析管理，按照用户的需求，制定相应的策略。动态频谱管理的主要问题就是如何设计一种高效的频谱利用自适应策略，以达到认知无线电网络容量的最大化和对主用户干扰的最小化。文献[22]针对次级用户在使用空闲频谱而主用户出现时如何分配频谱的问题，提出了一种频谱空洞重分配的动态算法。该算法以最小化认知用户传输中断和增加认知用户成功传输的数量为目标，通过频谱空洞多配置、高性能频谱空洞再分配、频谱空洞借用 3 个过程实现了动态频谱管理。文献[23]从服务提供商、制造商以及政策制造者的角度来对认知无线电动态频谱管理政策做了研究。分别从技术、政策、商业这 3 个角度讨论了基于认知无线电的动态频谱使用的可行性，并推导出动态频谱管理政策为无线通信产业带来了积极影响。文献[24]提出了一种新颖的自组织动态频谱管理机制，该机制用一种分散方式解决了动态频谱管理问题，其优点是网络性能的分散性和可扩展性，计算简单性，成本效益，带宽保护等。文献[25]研究了在不完善的信道感知的情况下认知无线电网络中不同服务的动态资源分配问题。把功率和信道重分配问题建模为混合整数规划问题，另外，为减少计算复杂度将问题分两步解决并使用优化算法以追踪无线电环境的改变来动态地分配资源。

自适应频谱分配技术，即根据无线电系统的实际业务量，动态地分配资源，以避免或减少业务的

拒绝和频谱资源的浪费，达到网络资源的自适应配置，从而实现复杂通信系统中满足用户需求的灵活可靠通信以及资源的有效利用。文献[26]主要是通过使用隐藏马尔科夫模型（HMM）来预测主用户对频谱的占用情况，相比于传统的 CSMA 算法，基于马尔科夫链的信道预测算法（MCPA），能够更有效地减小认知用户对主用户的信号干扰，实现网络的动态频谱分配。文献[27]主要在传统的图论着色频谱分配算法的基础上，考虑了节点的优先级，包括用户的优先级和信道的优先级，提出一种改进的基于节点优先级的图论着色分配算法，更好地满足了用户需求，提高了频谱利用效率，且兼顾了频谱分配的公平性。文献[28]使用博弈论来分析认知无线电网络中频谱分配的问题。为了处理基于频谱共享的非合作式博弈的多种纳什均衡问题，用认知用户利用率的变化来判断迭代的稳定性，提出一种改进的非合作式频谱分配算法，在分布式网络中，可以在特定消耗的限制下稳定地收敛。

2.2 认知环及其工作流程

认知无线电网络从对无线环境的频谱感知，经过智能分析，做出最优决策进行重配置，认知用户根据决策结果进行资源的使用，整个过程称为认知循环，简称认知环。1999 年，MITOLA J 博士首次提出了认知无线电以及认知循环[1]，其中认知循环由观察、面向建立优先级、计划、决策和行动五部分组成。认知无线电通过对外界激励的提取，通过内外部分析，来调整参数以适应无线环境，达到最佳配置，优化网络性能[29]。

本文中使用的认知环结构由 4 部分组成，如图 1 所示，分别是感知、分析、决策和通信。中心式认知无线电网络中，认知用户通过对无线环境的感知，经过控制信道上传感知数据，融合中心根据收到的感知数据进行分析，得出可用信道列表。认知用户基站根据认知用户的申请信道请求，按照一定规则进行决策，即信道分配，并通过控制信道发放分配信息。认知用户分配到信道后，使用这些信道进行数据通信，称认知用户用于通信的信道为数据信道。分布式认知无线电网络中，认知用户通过对无线环境的感知，经过控制信道交互感知信息，分析达成统一的可用频谱列表，并按照一定的竞争机制对信道进行分配，最后跳转至数据信道进行通信。

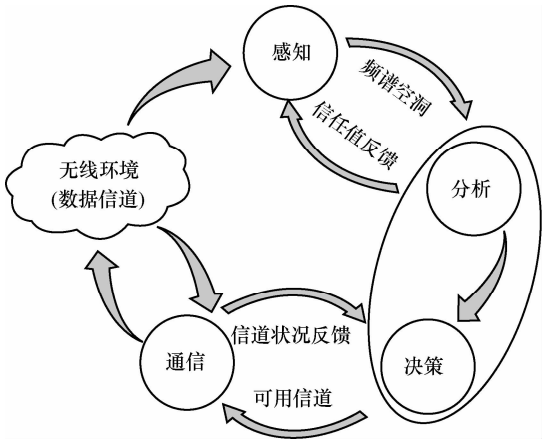

图 1 认知环

认知环是认知无线电网络工作的基本单元，所有环节由终端设备、控制信道和数据信道来完成。根据认知环各个环节的行为，把感知—分析—决策—通信 4 阶段分别对应于不同实体，即终端设备(认知用户)感知、控制信道上传感知数据、终端设备(融合中心)分析决策、控制信道发放决策信息、终端设备(认知用户)信道跳转、数据信道通信并作用于无线环境，从而进行一次完整的认知环流程。其中，终端设备是指认知用户、融合中心以及认知用户基站等设备；数据信道是指用户分配到信道后，在空闲信道上通信过程中使用的信道，认知用户感知行为和通信过程在数据信道上进行；控制信道是指频谱感知数据上传与下达以及频谱分配信息发放时所使用的信道，认知无线电网络的控制信息都在控制信道上进行。终端设备独立于控制信道和数据信道的行为称为终端用户自身行为。

本文对中心式(分布式)网络，分别从终端、信道等实体出发，将认知环的工作流程划分为以下几个步骤。

1) 认知用户在数据信道上侦听外部无线环境获得感知数据。

2) 认知用户整理感知数据。

3) 认知用户通过控制信道上传感知数据至融合中心(认知用户通过控制信道交互感知信息)。

4) 融合中心根据融合算法分析计算频谱感知结果，并由感知结果反馈相关信息(如信誉值等)于认知用户，感知结果信息与基站同步共享(经过协商分析得出统一的频谱感知结果)。

5) 基站通过控制信道发放可用信道列表(可用信道列表扩散)。

6) 认知用户通过控制信道进行申请信道请求(认知用户通过控制信道进行频谱使用的竞争)。

7) 基站通过控制信道发放分配信息(认知用户协商频谱分配)。

8) 认知用户跳转至数据信道进行通信。

9) 认知用户的通信作用于外部无线环境，并通过控制信道反馈于分析决策阶段。

认知环流程如图 2 所示。

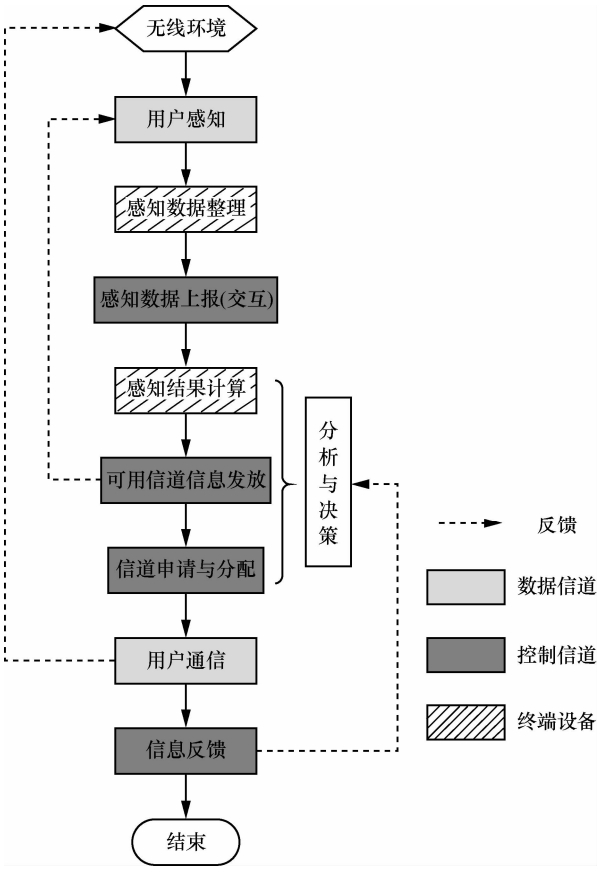

图 2　认知环工作流程

认知无线电网络的发展能够缓解无线频谱资源短缺的危机，充分利用空闲频谱以满足更多用户的需求。然而，智能性和认知特性也带来了新的挑战，如频谱感知过程中，恶意用户发出模仿主用户的信号，使认知用户误认为信道被主用户占用等；分析决策过程中，恶意用户通过篡改阻止网络的自适应调节等。因此，认知环的每一个环节都需要安全机制作保障，才能达到动态频谱接入的可行性。从感知到通信，过程中的终端设备行为、控制信道和数据信道的信息传递都需要严格的安全保障。如何保证频谱感知的准确性和实时性，通过学习机制实现自适应频谱分配而不造成对主用户的影响，达到通信性能的安全可靠，是认知无线电网络需要解决的重要问题。

3　认知无线电网络安全威胁

频谱感知技术是认知无线电网络中的关键技术之一，如何有效精确地获得可用频谱信息是认知无线电网络工作的前提。本文从感知阶段出发，依托认知环操作流程，分别从数据信道、终端设备和控制信道 3 个攻击点介绍现有的安全威胁。

3.1　数据信道攻击

3.1.1　模仿主用户（PUE, primary user emulation）

基于不干扰主用户的前提，认知用户可以伺机接入授权频段进行通信，这就需要认知用户连续地进行感知来检测主用户的出现。因此认知无线电网络的关键问题之一是频谱感知算法。当认知用户感知到主用户信号返回，必须撤离此信道并寻找其他空闲信道进行通信[30, 31]；当认知用户感知到信道正在被其他认知用户使用，需要启动频谱共享机制以达到频谱使用的公平性。因此，认知用户在数据信道上侦听信号并判断主用户是否占用信道是认知环中的首要步骤。攻击者在信道上发送模仿主用户特征的信号，导致其他行为规则的认知用户误认为主用户存在，认知用户对此数据信道的信号判定结果为繁忙，从而空出此信道，这样的攻击称为模仿主用户攻击[32]，如图 3 所示。模仿主用户攻击分为两类：自私攻击和恶意攻击。自私攻击一般由一对用户同时发起，以模仿主用户特征的信号进行相互通信；恶意攻击是攻击者发送模仿主用户特征的信号在信道上连续发送数据分组，以阻止其他认知用户的接入[20, 33, 34]。因此认知无线电网络面临的一个主要技术挑战是如何精确地区分主用户信号和认知用户信号[35]，以保证感知信号的准确性。

3.1.2　阻塞

认知环中继感知、分析、决策之后，认知用户接入可用信道开始通信，即进入认知环的最后一个环节数据通信。由于可用信道信息的公开性，攻击者可以随机或有针对性地选择某些可用信道进行阻塞，从而中断认知用户之间的正常通信。此时，尽管认知用户分配到空闲的可用信道，也不能进行正常通信。此过程中，攻击者亦可模仿主用户的信号，赶走正在使用信道的认知用户，迫使认知用户进行信道切换。多个认知用户在此信道上通信都被攻击者阻塞而跳转，认知用户对此信道使用的反馈结果会造成信道质量差的经验积累，从而减少此信道的分配，因此，恶意用户可以使用此信道进行通信。

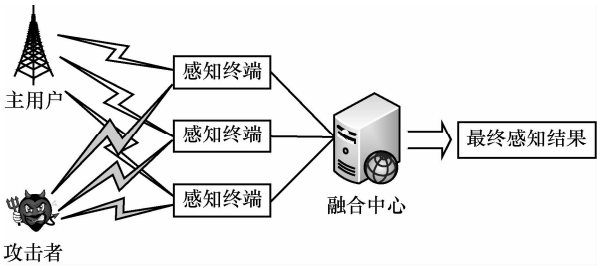

图 3 模仿主用户攻击

3.2 终端设备攻击

3.2.1 终端—频谱感知数据篡改(T-SSDF, terminal-spectrum sensing data falsification)

频谱感知数据篡改(SSDF, spectrum sensing data falsification)攻击，又称拜占庭攻击，是指攻击者向邻居节点或融合中心发送错误的本地频谱感知信息，引起接收者做出错误的频谱感知判决结果[36, 37]。SSDF 攻击[38]有 2 种形式，中心式认知无线电网络中，攻击者发送错误的本地频谱感知信息至融合中心，即 T-SSDF；攻击者在控制信道上截获并篡改认知用户上传的频谱感知信息后进行上传，即控制信道频谱感知数据篡改(C-SSDF, cortrol channel-spectrum sensing data falsification)，如图 4 所示。分布式认知无线电网络中，攻击者发送错误的本地频谱感知信息至邻居节点，或攻击者在控制信道上截获并篡改认知用户交互的频谱感知信息后进行发送。篡改结果有 2 种：主用户不使用信道时，攻击者声称该信道被主用户占用；主用户使用信道时，攻击者声称该信道空闲。SSDF 攻击将造成虚警或漏检，导致融合中心做出错误的频谱感知结果，从而影响后续的可用频谱分配过程，最终影响主用户通信或造成资源的浪费。

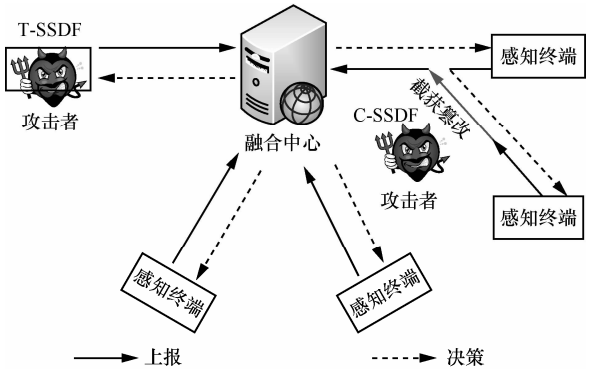

图 4 SSDF 攻击

3.2.2 目标函数攻击(OFA, objective function attack)

灵活性使得认知无线电网络能够感知外部环境，对其进行学习并智能决策以适应变化的环境。在认知无线电网络中，大量参数的自适应调节可以通过优化算法(如遗传算法、粒子群算法等)来最大化多目标函数。一旦选择好最优结果，认知无线电网络就会分配参数调节每一个子目标函数，系统就能达到最优状态。攻击者可以通过改变可控参数(如发送速率)等多种方式改变一个或多个子目标函数[39, 40]，从而阻止认知无线电网络的自适应调节，使系统无法适应于变化的无线环境，最终无法实现最优性能，如图 5 所示。如何做到有目的地可控参数调节是认知无线电网络中的重要研究问题。

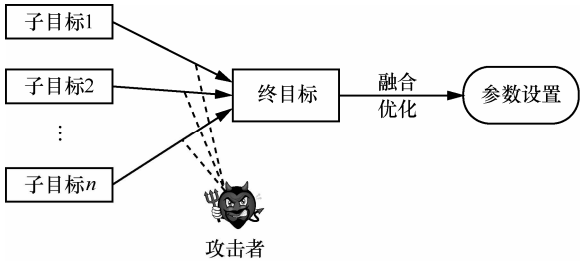

图 5 目标函数攻击

3.2.3 虚假申请

恶意认知用户通过对信道的申请，获得可用信道使用权后，并不使用此信道，如图 6 所示。此行为不但加重了网络负载，且造成资源的浪费，使得其他认知用户的需求得不到满足，降低频谱利用率，称此攻击为虚假申请。攻击者不需要花费太多能量，且由于采用静默期感知机制，认知无线电网络无法检测出虚假申请者。如果网络中存在多个虚假申请攻击者，将会导致网络资源的不可用性。

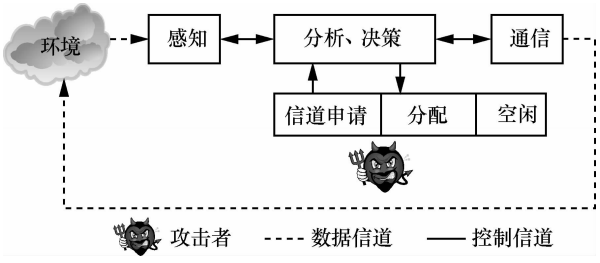

图 6 虚假申请

3.2.4 学习攻击

认知无线电网络的智能性和认知特性是其区别于传统无线网络的本质特性。终端设备在频谱感知、分析、决策以及通信过程中，都会参考历史学习内容，根据当前网络状态来反馈和调节参数。认知用户、融合中心以及认知用户基站在认知环工作

流程中，借鉴历史知识，对网络环境进行最优化处理，分别从感知、分析和决策阶段智能地收集整理可用信息，对网络进行预估。攻击者利用认知无线电网络的认知特性，修改以往的数据或者改变/伪装当前的条件，认知用户在没有任何判断标准的情况下，误把篡改后的数据当成实际输入的数据，从而进行学习推理，影响终端设备的自适应调节和学习经验积累与预测结果，并恶意教唆认知终端设备，使其渐变性恶化，对后续的操作造成长期影响，无法保证网络与实际环境的最佳适应。

3.3　控制信道攻击

3.3.1　控制信道污染

中心式认知无线电网络中，用户对无线环境进行感知之后，需要通过控制信道把感知数据发给融合中心。作为认知无线电网络中控制信息的传输通道，控制信道的信道质量是认知无线电网络的重要问题之一。由于可用信道的不稳定性和间断性，需要专门划拨出连续的信道为控制信息传输作保障。中心式认知无线电网络中，控制信道用来传输感知信息和认知用户信道分配信息，并负责控制信息的反馈；攻击者通过发出大量无用信息阻塞控制信道，以达到扰乱该信道数据传输的目的，影响正常认知用户感知信息的汇总与交互，甚至造成 DoS 攻击[41, 42]，从而阻碍控制信道的信息传输和共享，使得融合中心或认知用户无法收到感知数据，而不能进行最终的可用频谱判决，如图 7 所示。

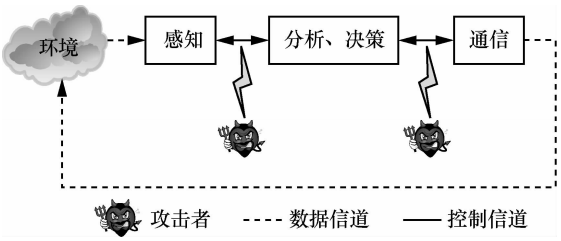

图 7　控制信道污染

3.3.2　窃听控制信道

认知无线电网络中，所有的控制信息都在控制信道上传输，攻击者隐藏在认知用户、融合中心或基站附近，窃听控制信道，可以获得个别认知用户甚至全网的可用信道信息，并根据网络中的信道选择算法计算出认知用户可以切换的信道，从而进行有针对性的攻击，如图 8 所示。窃听控制信道行为本身不会给网络带来影响，但是它是其他攻击形式的基础，作为辅助手段达到攻击者的目的。

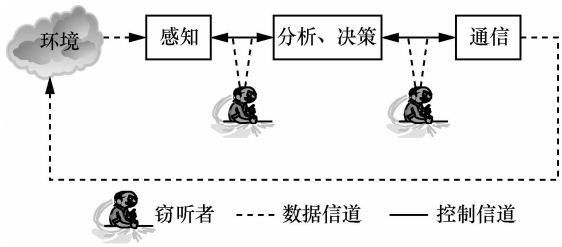

图 8　窃听控制信道

3.3.3　C-SSDF

中心式认知无线电网络中，C-SSDF 攻击即攻击者在控制信道上截获并篡改认知用户上传的频谱感知信息后进行上传，如图 4 所示；分布式认知无线电网络中，C-SSDF 攻击即攻击者在控制信道上截获并篡改认知用户交互的频谱感知信息后进行发送，这种由于信道的不安全造成的频谱感知数据篡改可以导致和 T-SSDF 同样的攻击效果。

3.4　联合攻击

以上分析的各种攻击可以从数据信道、终端设备和控制信道来分别说明，而攻击者针对多个攻击点同时发起的攻击，如 LEON O 等在文献[43,44]中提出的狮子攻击，称之为联合攻击，它是一种跨层攻击，在认知环中跨越多个环节。攻击者在认知用户使用的信道上发射模仿主用户的信号，迫使认知用户改变自己的传输信道，以此来破坏该用户的 TCP 连接，如图 9 所示。由于传输层并没意识到干扰，继续发送排队等候中的数据段，因此，未接收的 TCP 数据段在频率切换的过程中会推迟到达甚至丢失，造成 TCP 吞吐量的的降低。频率切换持续的时间越长，吞吐量降低的幅度越大。智能的狮子攻击中，攻击者可以阻止特定的认知用户接入网络。首先，攻击者需要窃听控制信道，获取最新的

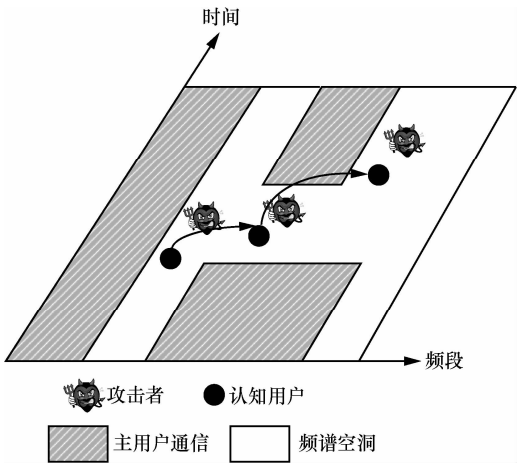

图 9　狮子攻击

可用频谱信息，并利用认知无线电网络中信道选择算法计算出认知用户要切换的信道，在切换的数据信道上发起模仿主用户攻击，迫使认知用户进行信道切换。狮子攻击大大降低了认知无线电网络的吞吐量，迫使认知用户不断地进行信道申请与切换，不能进行连续通信，很大程度上降低了认知用户的满意度。

按照数据信道、终端设备和控制信道把上述各种攻击及特点进行了整理，如表 1 所示。

4 认知无线电网络安全研究现状

根据攻击点的不同，分别从数据信道、终端设备和控制信道 3 方面分析现有的安全方案。

4.1 数据信道攻击安全方案

模仿主用户攻击是针对数据信道攻击的典型代表，是认知无线电网络中研究最早且最多的安全问题之一，文献[19, 32, 35, 45~52]针对模仿主用户攻击分别提出了解决方案和分析模型。JIN Z 等提出了一个分析模型作为检测 DoS 的使用机制。特别针对 PUE 攻击提出了分析方法，使用 Fenton 的近似法和 Wald 的连续概率比检测(WSPRT)[32]。文中提出用来描绘接收到功率特征的分析模型，得到在较小范围内 PUE 攻击成功的概率。在一个衰落无线电环境中利用 Fenton 的近似法推导出 PUE 攻击成功概率的表达式；利用马尔可夫不等式产生一个 PUE 攻击成功概率的更小范围；最后用 Wald 的连续概率比检测(WSPRT)来检测 PUE 攻击。但是此方法对主用户有严格要求，要求主用户与认知用户距离比较远，而且位置固定。

CHEN S 等提出一种针对移动主用户的 PUE 检测方案[46]，其中主用户是移动手机，每个次级认知用户装备一个声音传感器，通过这个传感器得到 RF 信号和声音信息之间的相互关系，进而证实无线手机用户的真实性。假设攻击者在模仿主用户信号时不发送声音波，因为攻击者的声音波和主用户的声音波不同，如果发送声音波就会很容易被检测到。因此文中通过对比 RF 信号和声音信息之间的相互关系来检测 PUE 攻击。如果信号不能通过相关性检测，就视为 PUE 攻击。该方法不需要复杂的硬件设备，但是声音和 RF 信号相关性检测对 AM 调制信号比较简单，对 FM 调制信号就比较难；时间限制也是一个问题，IEEE 802.22 要求在一个 200kHz 的频带检测无线手机信号需在 2s 之内，且误检和漏检概率小于 0.1。因此，快速检测 PUE 攻击是一个很高的要求。

CHEN R L 提出的发射机定位方案[45]、距离比(DRT)测验、距离差(DDT)测验[35]，可以通过估计信号源的位置，观察信号的特性来认证该信号是否是主用户发射机发射出来的信号。为了确定信号发射机的位置，利用一种非交互的基于 RSS 的定位方案。利用信号源的位置信息和信号特征来识别信号是否由主用户发出。该文章提出的模型假设主用户信号为电视塔信号，即主用户信号发射机是固定的，因此只适合于主用户位置固定的网络，对主用户具有移动性、小功率的认知无线电网络并不适用。

ZHAO C D 等提出了利用发射机指纹识别模仿主用户攻击[47]，利用振荡器的相位噪声这一唯一特征来识别主用户和攻击者，能够有效检测出模仿主用户攻击。

表 1 认知环中的各种攻击及影响

攻击点	攻击名称	攻击结果	攻击的影响
数据信道	PUE	认知用户感知结果出错	可用频谱预测错误，干扰主用户或资源浪费
	阻塞	中断通信且导致错误的反馈信息	攻击者有效使用空闲信道
终端设备	T-SSDF	融合中心接收到篡改的感知数据	可用频谱预测错误，干扰主用户或资源浪费
	OFA	控制参数调节	破坏自适应性
	虚假申请	已分配的空闲信道未被使用	资源浪费，降低认知用户需求满意度
	学习攻击	破坏认知性能	无法使网络适应于环境
控制信道	控制信道污染	拒绝服务	感知信息无法汇总，可用信道无法分配
	窃听	获取感知和分配信息	预测用户将要跳转的信道进行下一步攻击
	C-SSDF	融合中心接收到篡改的感知数据	可用频谱预测错误，干扰主用户或资源浪费
联合攻击	狮子攻击	降低网络吞吐量	用户无法进行连续通信

HAO D 提出一种利用攻击者和次级用户博弈的方法来减小模仿主用户攻击的影响[48]。将 PUE 攻击者和合法的次级用户之间的相互作用过程建模为一个常数和的微分博弈，称为 PUE 攻击博弈。合法的次级用户希望找到最优的感知策略，达到最大化信道利用率同时最小化 PUE 攻击的信道数目；而 PUE 攻击者希望最大化自己攻击的信道数目，最小化自己的功率消耗达到最小化次级用户的总体信道利用率。通过微分博弈过程(①哈密尔顿函数和解集的确立；②边缘约束；③关键的切换时间(critical switching time))，得到 PUE 攻击的纳什均衡，在存在 PUE 攻击者的情况下，使合法次级用户最大化整个认知无线电网络的频谱利用率。针对攻击者在长时间持续不断地对网络进行 PUE 攻击，同时能够智能地调节攻击参数的情况下，此方案可以有效降低 PUE 攻击的影响，但是在系统建模的时候假设只有一个攻击者，没有考虑存在多个攻击者联合篡改欺骗的情况。

PU D 等提出一种在认知无线电网络中检测 PUE 攻击的方法[52]，是由能量检测发起的定位频带上存在用户的方法。该方法使用循环平稳估计来代表用户信号的特征值，这个特征值会注入到一个人工神经网络来进行分类。现存的系统可以很容易的使用这个方法，而不需要做大量的架构或功能修改。此方法已经经过计算机仿真和实验硬件设备(USRP2 平台)的验证。硬件实验表明在真实的无线电环境中正确检测的概率达到 98%左右，且此方法的优点是不需要任何特殊的硬件或时间同步算法；不用对主用户做任何假设。

针对数据信道攻击提出的以上方案，其适用场景与优缺点如表 2 所示。

数据信道的阻塞也是认知无线电网络中的一种常见问题，但并不是特有的，可以采取传统无线网络信道阻塞方案来解决，文中不再详述。

4.2　终端设备攻击安全方案

通过攻击终端设备而达到目的的攻击形式有 T-SSDF、OFA、虚假申请和学习攻击。频谱感知数据篡改的 2 种形式，T-SSDF，攻击者本身发出错误的本地频谱感知信息，属于终端设备攻击范畴；C-SSDF，攻击者截获并篡改频谱感知信息，属于控制信道攻击，可以通过传统的加密方法解决。研究学者已经提出了多种数据融合技术来抵抗 T-SSDF 攻击[53~62]。合作感知可以利用多个认知用户的感知结果来计算并检测 T-SSDF 攻击，PANG D M 提出

表 2　　**数据信道攻击安全方案对比**

方案类型	适用场景	假设条件	优缺点
Wald 连续概率比检测(WSPRT)[32]	主用户固定的网络，且主次用户分区明显	主用户位置固定，认知用户距离主用户较远	优点：不需要认知用户之间合作，根据算法认知用户可以独自检测 PUE 攻击 缺点：要求主用户距认知用户较远且位置固定
声音检测(hearing is believing)[46]	主用户具有移动性且发射功率较低的网络	攻击者可以模仿主用户的功率、调制类型、带宽占用以及信号的其他特征；攻击者不发出声波	优点：可以快速减少积极和消极的错误概率至 0.1 以下，且不需要复杂的硬件设备 缺点：声音和 RF 信号相关性检测对 FM 调制信号比较难；单个设备解调不同制造商的无线产生器很难
发射机定位方案(LocDef)[45]	中心式网络，主用户信号发射机位置固定，如电视塔信号	主用户发射机位置固定；每个认知用户可移动、配备 CR 设备且能够自我定位；攻击者配备 CR 设备且能够改变调制类型、频率和输出功率	优点：在频谱感知过程中同时检测 PUE 攻击 缺点：不适用于主用户具有移动性、小功率的认知无线电网络
指纹识别[47]	分布式网络，如 ad hoc 网络	无	优点：能比较准确的区分主用户和攻击者的信号 缺点：产生噪声的因素不稳定，噪声相位提取及可靠性很难保证
博弈建模方法[48]	只有一个攻击者的多信道认知无线电网络	只存在一个攻击者	优点：可以在 PUE 攻击存在的情况下优化次级用户的资源使用率 缺点：系统建模假设只有一个攻击者，对多个攻击者存在的情况并不适用
人工神经网络[52]	多种形式的认知无线电网络	所有的用户都在相同频段的覆盖范围内；每一时间周期内，一个信道上只有一个用户传输且传输功率高于其他噪声；主用户的调制方案已知，且不同于其他用户	优点：顽健性；可用于核实未知坐标的移动发射机；不需要任何特殊的硬件或时间同步算法 缺点：不适用于智能的 PUE 攻击

一种基于信任模型的合作感知算法[53]，算法假设控制信道状况良好，每个认知用户都是感知终端，负责本地频谱感知。融合中心根据感知结果计算认知用户的信誉值，参考信誉值快速追踪或删除上报虚假感知数据的恶意认知用户，在攻击者数目较多的情况下能起到很好的效果。但是此方案中融合中心计算时需要大量的先验知识，是对安全合作感知技术的限制。

WANG W K 等提出一种恶意用户检测算法[54]，利用认知用户的历史感知结果计算其信誉值，针对单个恶意用户的 T-SSDF 攻击，此方法可以有效地区分诚实认知用户和恶意认知用户。

ZENG K 等提出 2 种基于信任机制的架构[55]，第一种是普通的信任架构，每个节点分配初始信任值（皆大于信任门限），信任值作为权重影响汇聚结果。汇聚结果与认知用户的判决结果影响信任值的增减。第二种架构中，文中指出“现有的安全合作频谱感知算法对全局判决的正确性非常敏感”，因而网络初始运行时的全局判决结果正确性非常重要。如果恶意用户在网络初始运行时进行攻击，则影响会很大。文章主要针对网络初始运行阶段恶意用户的 T-SSDF 攻击。把认知用户分为三类，信誉值过低的摒弃类、信誉值较高的可靠类以及居于两者中间的不确定类。在网络初始运行时，全局判决仅根据可靠类中的认知用户上报的结果产生。不确定类中的认知用户上报的结果虽不参加全局判决过程，但会影响相应用户的信誉值增减。网络初始运行时，只有接入点（AP, access point）、基站（BS, base station）、簇头等高级节点在可靠类中。过了初始运行阶段后，不确定类中的认知用户上报的结果如何使用，文章并没有提及。另外，方案中并不能保证簇头就是可信用户，这与簇头的选举依据有关。AP、BS 也不一定有感知功能，且感知范围、准确性有限。

针对合伙 T-SSDF 攻击，文献[61]中提出一种分段感知的方案，认知用户入网后按照模数规则被分配到不同的频段进行感知，合伙攻击者无法被分配到同一频段，因此不能对特定的频段进行欺骗，最终无法达成合伙攻击的结果；针对单个用户的 T-SSDF 攻击，采用信任值升降的方法，增加上报正确感知数据认知用户的信任值，减少上报错误感知数据认知用户的信誉值，本方法能有效阻止单个用户的 T-SSDF 攻击和合伙 T-SSDF 攻击。

CHEN R L 等提出利用抽样数为变量的权重序贯概率比融合算法[62]，分 2 个步骤来实施：一是信誉维护，二是实际假设检验测试，并分别对“与”、“或”和“多数原则”的融合技术进行了仿真，本方案达到了数据收集量和数据融合的健壮性的平衡，随着本地感知数据的增加，权重序贯概率比融合算法能够有效地控制融合开销。

目标函数攻击是另一种终端设备攻击形式，作用于认知无线电网络的自适应调整阶段，目前对于此攻击的研究还不成熟，大都侧重于参数的门限设定方面。文献[63]针对目标函数攻击，提出了一种多目标规划模型。首先通过约束条件，检查总目标函数的浮动范围，通过门限比较，检测出可能被篡改的参数。计算子目标浮动半径对总目标函数的影响，与自适应调节的子目标浮动范围相比较，来确定参数是否被攻击者篡改。检测到被篡改的参数后，通过粒子群算法[64]调整此参数为最优值。此方案能够检测到目标函数攻击的具体对象，即被篡改的子目标，并进行合理的调节，即使攻击者获得了用户的各个参数，也不能随意篡改，阻止认知无线电网络的自适应配置，此方案能够有效抵抗目标函数攻击。

针对以上提出的终端设备攻击的方案适用场景及优缺点对比如表 3 所示。学习攻击是针对终端设备认知功能的一种特殊攻击方式，通过多种途径恶意教唆终端设备做出不符合优化原则的调整。认知无线电网络中认知功能的研究还处于初始阶段，并没有完善的方案能够有效抵抗学习攻击。

4.3 控制信道攻击安全方案

针对控制信道的攻击有 C-SSDF 攻击、控制信道污染、窃听等。对于前者，可通过签密手段来阻止，以达到数据的完整性、不可伪造性，并能够验证发送数据源的身份，传统的密码学手段即可解决。由于认知无线电网络中控制信道的特殊性，感知信息和控制信息以及网络反馈都通过控制信道进行，因此，控制信道成为了认知无线电网络的瓶颈。针对控制信道污染、阻塞等，TAGUE P 等提出了一种利用随机密钥分配在时间或频段上隐藏控制信道位置的方法[66]。文中假设其中控制信道的接入以时隙划分，各个用户在模数相同的时候接入控制信道；攻击者可以合伙阻塞控制信道，造成 DoS 攻击；网络外部的攻击者可以伪装成合法用户。方案中把网络内部的攻击者和网络外部伪装身份的

攻击者统称为妥协用户，建立了控制信道的接入和安全信道通信之间的映射，利用随机控制信道密钥分配来还原被阻塞的控制信道，并把控制信道的性能恢复时间归结为一个关于妥协用户数量的函数。仿真数据表明，随着妥协用户数量的增多，被阻塞的控制信道恢复的时延就越长。

认知无线电网络中控制信道的重要性，使得其安全问题也随着控制信道的形式而变化。由于专门划拨出控制信道会有额外的开销，因此文献[67]中提出利用群体智能的方法来动态地寻找和管理控制信道。考虑了认知无线电网络中实际信道的特性，利用群体智能，移动用户和邻居的互传和扩散性达到信息传播的目的。此方法不需要时钟同步，且开销小，可以动态地使用短时间可用的碎片信道进行邻居节点的互传，在认知无线电网络中比较可行。HTIKE Z 等提出一种利用多个控制信道保证连通性的方法[65]，对可用信道进行分组，每一组选择一个信道为控制信道，当用户需要在控制信道传播信息时，首先要选择一个控制信道，感知信道是否空闲，并确认接收者也跳转至此信道。如果此控制信道繁忙，则选择其他控制信道进行同样的操作。此方案可以缓解控制信道饱和的问题，对主用户行为的容忍度更高。方案的对比分析如表 4 所示。

针对控制信道的窃听，攻击者获得有效信息从而进行相关的攻击。因此，可以通过加密隐藏控制信道信息来阻止攻击者提取有效的信息。如信道分配过程中，对某个认知用户发送分配的信道信息时，可以采用加密数字序号来达到目的。其中每个认知用户都和基站共享自己的偏好使用信道集合(有序集合)，即集合中的元素与其在集合中的位置序号一一对应。偏好使用信道集合通过特定的方式进行更新。即使攻击者获得了信道分配信息并解密得到序号，也无法找到序号对应的具体信道。这种加密隐藏方案依赖于密码体制和同步更新机制，可以大幅增加攻击者进行攻击行为的难度。

目前，控制信道的研究仍然是认知无线电网络中的关键问题之一。实际可操作性和可用频谱的动态性，使得控制信道的可靠性很难得到保障。

4.4　联合攻击安全方案

狮子攻击从控制信道、终端设备和数据信道三方面入手发起联合攻击，是一种跨越认知环多个阶段的攻击形式，严重降低了认知无线电网络的 TCP 吞吐量。传统无线网络中的增强 TCP 性能的方案只能减少狮子攻击的影响，并不能消除狮子攻击[36,68,69]。LEON O 等详细描述了狮子攻击并提出了潜在的对策[43, 44]，首先针对控制信道信息的泄露，攻击者可以获取认知用户下一跳要跳转的最佳信道这一问题，提出使用控制信息共享密钥或组密钥方式，通过对控制信息的加解密以及认知用户身份的认证，来减少恶意用户的窃听，但此方法只适用于网络外部攻击者，对攻击者是合法认知用户的情况并没有起到作用。文中也提出利用入侵检测系统来检测跨层攻击，通过监测来探测违背协议的可疑设备。作者建议为了改进认知无线网络中的入侵检测机制，

表 3　　**终端设备攻击安全方案对比**

方案类型	适用场景	假设条件	优缺点
基于信任模型的合作感知[53]	具有融合中心的认知网络	控制信道状况良好，融合中心有较多先验知识	优点：攻击者数目较多时效果良好 缺点：融合中心计算时需要大量的先验知识
恶意用户检测算法[54]	采用合作式感知的认知网络	最多只有一个恶意用户	优点：能够有效地区分诚实认知用户和恶意认知用户 缺点：只针对存在单个恶意用户的网络，不适用于多个恶意用户共存的环境
2 种基于信任机制的架构[55]	有 AP、BS 和簇头等高级节点的网络	AP、BS 和簇头等高级节点一直是可信的	优点：即使网络中存在大量攻击者，方案性能并不减弱 缺点：簇头的可靠性不能保证；AP、BS 也不一定具有感知性能，且感知范围，准确性有限
分段感知[61]	具有融合中心的分层分簇认知网络	根据地理位置分簇，簇内认知用户数目相同，且簇头可信	优点：能有效阻止单个用户的 T-SSDF 和合伙 T-SSDF 攻击 缺点：频谱分段和用户分组要花费一定的时间
权重序贯概率比融合算法[65]	ad hoc 认知网络	针对数据融合中的拜占庭错误	优点：达到了数据收集量和数据融合的健壮性的平衡，有效地控制融合开销 缺点：不能阻止除了拜占庭错误之外的 SSDF 攻击
多目标规划模型[63]	中心式或分布式认知无线电网络	用户能够自行检测自己的参数	优点：有效检测到被攻击的子目标；即使用户的参数泄漏，攻击者也不能随意篡改 缺点：每一轮检测之前计算浮动半径需要一定的时间

应该执行以下内容：1)必须以分布式合作的方法检测数据分组；2)通过不同层之间的交互来保证跨层攻击的检测。如狮子攻击可以通过物理层和传输层联合检测来发现攻击者，但并没有给出详细的检测方法。

WANG W K 等针对包含物理层上报错误感知信息和 MAC 层小退避窗口攻击的跨层攻击，提出一种基于信任的跨层抵御方法[70]。跨层攻击实施中，攻击者可以降低被检测到的概率，以较小的代价实现单层攻击不能达到的攻击目的。文中提出的抵抗跨层攻击的方案包括：单层监测和信任计算、信任融合以及异常检测。首先通过网络协议收集观察的信息，并计算各层的信任值；以单层信任值为输入，信任融合可以看作多路径信任传播模型，对每一个节点计算总的信任值；基于总的信任值识别恶意节点。仿真结果表明，相对于单层抵御方法，跨层防御能够明显降低跨层攻击带来的影响。联合攻击方案的特点如表 5 所示。

5 认知无线电网络安全建议

目前，认知无线电网络中认知环的各个阶段都存在相应的安全威胁，抵抗各种攻击的方案也相继出现。为保障认知无线电网络的安全有效运行，提出以下建议。

5.1 入网出网可控机制

为了保证网络对用户的可控性操作，首先需要政策支持，规定用户之间的优先级，即主用户>认知用户>其他用户。因此，攻击者若想获得与认知用户同样的优先级，必须加入认知无线电网络。而认知无线电网络中的用户加入和删除具有一定的规则，当认知用户不满足条件时，网络管理者会强行剔除认知用户，这样就保证了可控性操作，一旦发现了攻击者，便可采取相应的措施。不论在何种架构下的认知无线电网络，合理的入网出网机制都是保证网络用户正常行为的必要条件之一。中心式认知无线电网络中，管理者可以根据入网出网机制对异常行为的用户进行管制；分布式结构中，可以通过多点合作对异常行为用户进行隔离或强制出网，因此，入网出网机制是对网络中的用户进行可控操作的有效方法。

5.2 奖惩机制

认知无线电网络中，认知用户需要感知可用频

表 4 控制信道攻击安全方案对比

方案类型	适用场景	假设条件	优缺点
隐藏控制信道位置[66]	无线网络	控制信道的接入以时隙划分，各个用户在模数相同的时候接入控制信道	优点：不需要门限(妥协用户的数目)，增大设计的灵活性；不需要妥协用户的先验知识 缺点：没有考虑敌手的智能性，智能敌手可以选择性的阻塞以避免被发现
动态寻找和管理控制信道[67]	认知无线电网络	认知节点要有观察它周围环境（邻居节点的行动或状态等）的能力	优点：不需要时间同步，开销小，不需要交换谈判信息，实现简单 缺点：对认知节点的能力要求较高
多个控制信道的连通性[65]	ad hoc 认知无线网络	单跳网络； 多条控制信道，如果主用户出现而导致当前控制信道不能用，可以选择其他空闲的控制信道 认知用户可独立地在不同的控制信道上谈判	优点：可以缓解控制信道饱和问题，对主用户容忍度高 缺点：不适合多跳网络

表 5 联合攻击安全方案对比

方案类型	适用场景	假设条件	优缺点
控制信息共享密钥或组密钥[44]	认知无线网络	攻击者来自网络外部	优点：可以有效地减缓外部攻击者带来的影响 缺点：只适用网络外部攻击者，对攻击者是合法认知用户的情况并不起作用
利用入侵检测系统来检测跨层攻击[43, 44]	认知无线网络	用户必须以分布式合作的方法检测数据分组，且通过不同层之间的交互来保证跨层攻击的检测	优点：可以有效地检测跨层攻击 缺点：有损网络的性能，且文中并未给出详细的检测方法
基于信任的跨层抵御方法[69]	认知无线网络	攻击者在物理层实施上报错误感知数据攻击，在 MAC 层实施小退避窗口攻击	优点：能够明显降低跨层攻击带来的影响 缺点：用户彼此之间信息交互量大

谱信息，从而进行伺机接入。为了提高频谱感知的积极性，对感知数据上报次数多且感知结果准确的用户加以奖励，如设置感知信誉值。感知信誉值越高的用户，在感知结果融合中权值越大。在信道分配阶段的用户申请时，同等条件的用户，感知信誉值高的具有优先接入权。对恶意认知用户(如发起SSDF 攻击的用户)，通过感知结果的对比来减少感知信誉值。分配之后的通信过程中，设置礼节信誉，若认知用户不遵守法则占用信道，则会影响到礼节信誉值，感知信誉值和礼节信誉值的结合，称为认知用户的信誉值。当信誉值下降到固有的门限，认知用户就会被剔除出网络。另外，礼节信誉的合理设置可以用来检测和惩罚虚假申请攻击。合适的奖惩机制可以激励认知用户的正确频谱感知行为，并约束认知用户的通信礼节，可以增强认知无线电网络的健壮性。现有方案中有通过感知结果的正确度作为参考，来计算用户信誉值的高低，在分配过程中，若相同条件用户的竞争，则信誉值高的认知用户会有更高的接入优先级。奖惩机制可以用来规范网络中用户的行为，是对入网后的用户在出网之前这一过程中行为的约束；可以用于频谱感知和频谱分析中，以提高网内用户正常行为的积极性，降低恶意行为的概率；用于频谱分配，可以使用户为了得到更高的资源使用权限而严格遵守网络行为规则，从而更好地维持网络的运行。

5.3　修正机制

认知无线电网络的认知特性和学习功能是其区别于其他无线网络的明显特征，然而也带来了诸多的安全问题。为了防止学习攻击带来的影响，需要做到以下几点：设置合理的衰减因子，对历史学习积累的知识加以限制，时间越长的记忆影响越小，保证适应网络的变化；对历史学习进行修正，一旦检测到历史学习的错误，就要从学习数据库中进行修正，以免网络遭受长期的影响。学习攻击是认知无线电网络中特有的攻击之一，由于学习攻击潜藏在潜在的数据库中，只作为决策的参考，因此传统的异常检测无法发现学习攻击，也无法修复和降低学习攻击造成的深远影响。修正机制主要针对认知无线电网络中的学习特性，在当前行为决策时对历史学习积累进行修正，在线修正数据库，可以有效降低学习攻击造成的影响。

5.4　行为策略

认知无线电网络的行为策略分为积极型和保守型。频谱感知结果有 3 种状态：空闲、繁忙和不确定状态。对于不确定状态的处理，采用积极型或保守型，应该视认知无线电网络和主用户网络的环境而定。通过对主用户行为的分析建模，预测不确定状态被主用户占用的概率，并参考认知用户的数量来进行策略的选取。在频谱感知算法和频谱分配算法的设计中，都需要考虑行为策略，积极型策略可以为认知用户争取到更多的可用资源，保守型策略可以更好地保证主用户的活动不受干扰。在不同场景的需求下，考虑两者的权衡，制定更合适的感知与分配算法，最终使得认知用户最大限度地使用资源，且对主用户的干扰在限定的范围之内。

5.5　加密认证机制

认知用户入网时，需要注册获得唯一的身份信息。认知环的初始阶段，各个认知用户上传或互换感知信息时加入签名，防止恶意用户篡改数据，并对感知数据的来源进行追溯确认；可用信道列表与公共反馈信息采用签名机制发布；信道分配阶段，加密后分配信息分别发送至申请信道的认知用户；通信阶段，认知用户根据需要采用相应的加密认证机制。加密认证机制除了具备与传统无线网络相同的功能以外，可以有效抵抗 C-SSDF 攻击；对控制信道上信息的发放，以及认知无线电网络中的跨层攻击都有显著的抑制作用。

认知无线电网络采用智能的频谱共享技术，如图 10 所示，在整个网络运行过程中，首先要保证频谱感知数据的实时性和准确性，融合算法要考虑适应性和历史经验的参考价值，通过网络状况调整至最佳。总体来说，在整个认知环的操作流程和学习过程中，要达到智能性和安全性。

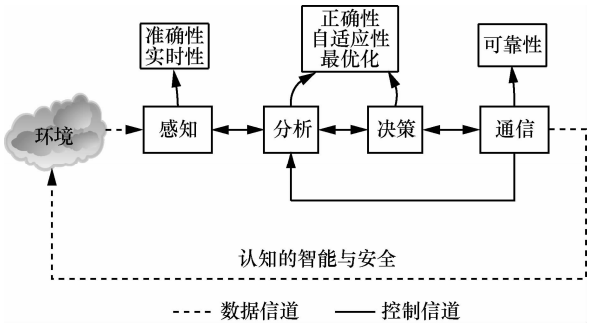

图 10　认知无线电网络安全

6　结束语

本文介绍了认知无线电网络中几种重要的安

全隐患，依托认知环，分别从数据信道、控制信道和终端设备三方面详细分析了各种安全问题，介绍了现有的解决方案，并从文章的分析中提出认知无线电网络的安全建议。目前，认知无线电网络的安全研究正处于起步阶段，从频谱感知到用户的可靠通信，认知环的各个阶段都需要安全保障。其中，以下几点将是认知无线电网络发展过程中需要解决的安全问题。安全的频谱感知数据融合算法，现有的频谱感知算法，在感知效率上固然有所提高，但对于恶意用户的欺骗行为以及合伙攻击，没有得到很好的控制，因此，需要从控制信道和终端设备以及算法本身来考虑频谱感知数据的准确性。在频谱感知信息确定的基础上，安全合理地分配资源。跨层攻击对认知用户资源的分配有很大的影响，不仅大幅度降低网络吞吐量，甚至可以永久阻止个别用户的网络接入，因此需要设计安全的接入算法以减少信道分配过程中被攻击的概率。安全路由的发现与选择，认知无线电网络中可用频谱资源的动态性，使得路由发现和选择更为困难，如何根据可达路径选择安全路由，也是需要考虑的问题。学习功能的安全有效实施，学习功能是认知无线电网络中特有的功能之一，而这种主观的学习本身就具有很多问题，如何建立一种安全的学习机制，让主观学习不受恶意或异常行为的影响，达到真正的安全智能，是认知无线电网络发展的重要步骤。跨层设计的安全管理，认知无线电网络的多种功能不可能在某个层中单独完成，需要各层的合作，因此，跨层设计是发展趋势，而动态资源的跨层管理既要考虑到安全问题，又要考虑隐私保护，也是进一步需要研究的重点。认知无线电网络的安全问题不仅仅是技术问题，还需要从管理机制、标准化等方面一起努力。

参考文献：

[1] MITOLA J, MAGUIRE G Q. Cognitive radio: making software radios more personal[J]. Personal Communications, IEEE, 1999, 6:13-18.

[2] SINGHAL D, SHARMA M K, GARIMELLA R M. Energy efficient localization of primary users for avoiding interference in cognitive networks[A]. Computer Communication and Informatics (ICCCI), 2012 International Conference on[C]. 2012. 1-5.

[3] QING Z, SWAMI A. A survey of dynamic spectrum access: signal processing and networking perspectives[A]. Acoustics, Speech and Signal Processing, ICASSP 2007, IEEE International Conference on[C]. 2007. 1349-1352.

[4] YUAN Z, GAO C X, XIAO Z G. Security threats in cognitive radio networks[A]. High Performance Computing and Communications, HPCC '08, 10th IEEE International Conference on[C]. 2008. 1036-1041.

[5] LEE W Y, AKYILDIZ I F. Optimal spectrum sensing framework for cognitive radio networks[J]. Wireless Communications, IEEE Transactions on, 2008, 7:3845-3857.

[6] PENG X, CHIN F, WONG S H, *et al*. A RAKE combining scheme for an energy detection based noncoherent OOK receiver in UWB impulse radio systems[A]. Ultra-Wideband, the 2006 IEEE International Conference on[C]. 2006. 73-78.

[7] LI G Y, FANG J, TAN H F, *et al*. The impact of time-bandwidth product on the energy detection in the cognitive radio[A]. Broadband Network and Multimedia Technology (IC-BNMT), 2010 3rd IEEE International Conference on[C]. 2010. 634-638.

[8] ZHANG L L, HUANG J G, TANG C K. Novel energy detection scheme in cognitive radio[A]. Signal Processing, Communications and Computing (ICSPCC), 2011 IEEE International Conference on[C]. 2011. 1-4.

[9] BRAUN M, ELSNER J P, JONDRAL F K. Signal detection for cognitive radios with smashed filtering[A]. Vehicular Technology Conference, VTC Spring 2009, IEEE 69th[C]. 2009. 1-5.

[10] BHARGAVI D, MURTHY C R. Performance comparison of energy, matched-filter and cyclostationarity-based spectrum sensing[A]. Signal Processing Advances in Wireless Communications (SPAWC), 2010 IEEE Eleventh International Workshop on[C]. 2010. 1-5.

[11] LEI K J, YANG X, PENG S L, *et al*. Determinant of the sample covariance matrix based spectrum sensing algorithm for cognitive radio[A]. Wireless Communications, Networking and Mobile Computing (WiCOM), 2011 7th International Conference on[C]. 2011. 1-4.

[12] MATE A, LEE K H, LU I T. Spectrum sensing based on time covariance matrix using GNU radio and USRP for cognitive radio[A]. Systems, Applications and Technology Conference (LISAT)[C]. Long Island, USA, 2011. 1-6.

[13] YANG X, LEI K J, PENG S L, *et al*. Blind detection for primary user based on the sample covariance matrix in cognitive radio[J]. Communications Letters, 2011, 15:40-42.

[14] DEEPA B, IYER A P, MURTHY C R. Cyclostationary-based architectures for spectrum sensing in IEEE 802.22 WRAN[A]. Global Telecommunications Conference (GLOBECOM 2010)[C]. 2010. 1-5.

[15] ZHANG T Y, YU G D, SUN C. Performance of cyclostationary features based spectrum sensing method in a multiple antenna cognitive radio system[A]. Wireless Communications and Networking Conference, WCNC 2009[C]. 2009. 1-5.

[16] VELEMPINI M, MOYO V, DLODLO M E. Improving local and collaborative spectrum sensing in cognitive networks through the implementation of cognitive collaborators[A]. Electrotechnical Conference (MELECON), 2012 16th IEEE Mediterranean[C]. 2012. 1045-1048.

[17] ZOU Y L, YAO Y D, ZHENG B Y. Cooperative relay techniques for cognitive radio systems: spectrum sensing and secondary user transmissions[J]. Communications Magazine, 2012, 50:98-103.

[18] CACCIAPUOTI A S, AKYILDIZ I F, PAURA L. Correlation-aware user selection for cooperative spectrum sensing in cognitive radio ad hoc networks[J]. Selected Areas in Communications, IEEE Journal on, 2012, 30:297-306.

[19] CHEN C, CHENG H B, YAO Y D. Cooperative spectrum sensing in cognitive radio networks in the presence of the primary user emulation attack[J]. Wireless Communications, IEEE Transactions on, 2011, 10:2135-2141.

[20] KALIGINEEDI P, KHABBAZIAN M, BHARGAVA V K. Secure cooperative sensing techniques for cognitive radio systems[A]. Communications, ICC '08, IEEE International Conference on[C]. 2008. 3406-3410.

[21] SUN X X, CHEN L, TSANG D H K. Energy-efficient cooperative sensing scheduling for heterogeneous channel access in cognitive radio[A]. Computer Communications Workshops (INFOCOM WKSHPS), 2012 IEEE Conference on[C]. 2012. 145-150.

[22] AISSA I, FRIKHA M, TABBANE S. Dynamic spectrum hole management in cognitive radio[A]. New Technologies, Mobility and Security (NTMS), 2011 4th IFIP International Conference on[C]. 2011. 1-4.

[23] JUNSEOK H, HYENYOUNG Y. Dynamic spectrum management policy for cognitive radio: an analysis of implementation feasibility issues[A]. New Frontiers in Dynamic Spectrum Access Networks, DySPAN 2008, 3rd IEEE Symposium on[C]. 2008. 1-9.

[24] KHOZEIMEH F, HAYKIN S. Self-organizing dynamic spectrum management for cognitive radio networks[A]. Communication Networks and Services Research Conference (CNSR), 2010 Eighth Annual[C]. 2010. 1-7.

[25] XIE R C, YU F R, JI H. Dynamic resource allocation for heterogeneous services in cognitive radio networks with imperfect channel sensing[J]. Vehicular Technology, IEEE Transactions on, 2012, 61:770-780.

[26] AKBAR I A, TRANTER W H. Dynamic spectrum allocation in cognitive radio using hidden Markov models: poisson distributed case[A]. SoutheastCon, Proceedings, IEEE[C]. 2007. 196-201.

[27] XIA D Y, QIU R H. An advanced dynamic spectrum allocation algorithm in cognitive radio based on priority of nodes[A]. Wireless Mobile and Computing (CCWMC 2011), IET International Communication Conference on[C]. 2011. 221-226.

[28] LI Y B, YANG R, YE F. Non-cooperative spectrum allocation based on game theory in cognitive radio networks[A]. Bio-Inspired Computing: Theories and Applications (BIC-TA), 2010 IEEE Fifth International Conference on[C]. 2010. 1134-1137.

[29] GUHA A, GANAPATHY V. Power allocation schemes for cognitive radios[A]. Communication Systems Software and Middleware and Workshops, COMSWARE 2008. 3rd International Conference on[C]. 2008. 51-56.

[30] LIU Q, ZHOU Z, YANG C, *et al*. The coverage analysis of cognitive radio network[A]. Wireless Communications, Networking and Mobile Computing, WiCOM '08, 4th International Conference on[C]. 2008. 1-4.

[31] MODY A N, REDDY R, KIERNAN T, *et al*. Security in cognitive radio networks: an example using the commercial IEEE 802.22 standard[A]. Military Communications Conference, MILCOM 2009[C]. 2009. 1-7.

[32] JIN Z, ANAND S, SUBBALAKSHMI K P. Detecting primary user emulation attacks in dynamic spectrum access networks[A]. Communications, ICC '09, IEEE International Conference on[C]. 2009. 1-5.

[33] SETHI A, BROWN T X. Hammer model threat assessment of cognitive radio denial of service attacks[A]. New Frontiers in Dynamic Spectrum Access Networks, DySPAN 2008, 3rd IEEE Symposium on[C]. 2008. 1-12.

[34] LI X H, CHEN J Y, FAN N. Secure transmission power of cognitive radios for dynamic spectrum access applications[A]. Information Sciences and Systems, CISS 2008, 42nd Annual Conference on[C]. 2008. 213-218.

[35] CHEN R I, PARK J M. Ensuring trustworthy spectrum sensing in cognitive radio networks[A]. Networking Technologies for Software Defined Radio Networks, SDR '06, 1st IEEE Workshop on[C]. 2006. 110-119.

[36] HANBALI A, ALTMAN E, NAIN P. A survey of TCP over ad hoc networks[J]. Communications Surveys & Tutorials, 2005, 7:22-36.

[37] KARLOF C, WAGNER D. Secure routing in wireless sensor networks: attacks and countermeasures[A]. Sensor Network Protocols and Applications, Proceedings of the First IEEE, 2003 IEEE International Workshop on[C]. 2003. 113-127.

[38] CHEN R L,, PARK J M, HOU Y T, *et al*. Toward secure distributed spectrum sensing in cognitive radio networks[J]. Communications Magazine, 2008, 46:50-55.

[39] RONDEAU T, RIESER C, LE B, *et al*. Cognitive radios with genetic algorithms: intelligent control of software defined radios[A]. Software Defined Radio Forum Technical Conference[C]. 2004.

[40] CLANCY T C, GOERGEN N. Security in cognitive radio networks: threats and mitigation[A]. Cognitive Radio Oriented Wireless Networks and Communications, CrownCom 2008, 3rd International Conference on[C]. 2008. 1-8.

[41] ZHU L, ZHOU H B. Two types of attacks against cognitive radio network MAC Protocols[A]. Computer Science and Software Engineering, 2008 International Conference on[C]. 2008. 1110-1113.

[42] THOPPIAN M, VENKATESAN S, PRAKASH R, *et al*. MAC-layer scheduling in cognitive radio based multi-hop wireless networks[A]. World of Wireless, Mobile and Multimedia Networks, WoWMoM 2006, International Symposium on[C]. 2006. 10-202.

[43] LEON O, HERN J, *et al.* Securing cognitive radio networks[J]. Int J Commun Syst, 2010, 23:633-652.

[44] LEON O, HERNANDEZ S J, SORIANO M. A new cross-layer attack to TCP in cognitive radio networks[A]. Cross Layer Design, IWCLD '09, Second International Workshop on[C]. 2009. 1-5.

[45] CHEN R L, PARK J M, REED J H. Defense against primary user emulation attacks in cognitive radio networks[J]. Selected Areas in Communications, IEEE Journal on, 2008, 26:25-37.

[46] CHEN S, ZENG K, MOHAPATRA P. Hearing is believing: Detecting mobile primary user emulation attack in white space[A]. INFOCOM, 2011 Proceedings IEEE[C]. 2011. 36-40.

[47] ZHAO C D, WANG W M, HUANG L F, *et al*. Anti-PUE attack base on the transmitter fingerprint identification in cognitive radio[A]. Wireless Communications, Networking and Mobile Computing, WiCom '09, 5th International Conference on[C]. 2009. 1-5.

[48] HAO D, SAKURAI K. A differential game approach to mitigating primary user emulation attacks in cognitive radio networks[A]. Advanced Information Networking and Applications (AINA), 2012 IEEE 26th International Conference on[C]. 2012. 495-502.

[49] JIN Z, ANAND S, SUBBALAKSHMI K P. Robust spectrum decision protocol against primary user emulation attacks in dynamic spectrum access networks[A]. Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE[C]. 2010. 1-5.

[50] ZESHENG C, COOKLEV T, CHAO C, *et al*. Modeling primary user emulation attacks and defenses in cognitive radio networks[A]. Performance Computing and Communications Conference (IPCCC), 2009 IEEE 28th International[C]. 2009. 208-215.

[51] ANAND S, JIN Z, SUBBALAKSHMI K P. An analytical model for primary user emulation attacks in cognitive radio networks[A]. New Frontiers in Dynamic Spectrum Access Networks, DySPAN 2008, 3rd IEEE Symposium on[C]. 2008. 1-6.

[52] PU D, SHI Y, ILYASHENKO A V, *et al*. Detecting primary user emulation attack in cognitive radio networks[A]. Global Telecommunications Conference (GLOBECOM 2011)[C]. 2011. 1-5.

[53] PANG D M, HU G, XU M. Trust model-based secure cooperative sensing techniques for cognitive radio networks[A]. The Tenth International Conference on Networks[C]. 2011. 1-6.

[54] WANG W K, LI H S, SUN Y, *et al*. Attack-proof collaborative spectrum sensing in cognitive radio networks[A]. Information Sciences and Systems, CISS 2009, 43rd Annual Conference on[C]. 2009. 130-134.

[55] ZENG K, PAWECZAK P, CABRIC D. Reputation-based cooperative spectrum sensing with trusted nodes assistance[J]. Communications Letters, 2010, 14:226-228.

[56] LIU S Y, LIU Q, GAO J, *et al*. Attacker-exclusion scheme for cooperative spectrum sensing against SSDF attacks based on accumulated suspicious level[A]. Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), 2011 IEEE International Conference on[C]. 2011. 239-243.

[57] FARMANI F, JANNAT A M A, BERANGI R. Detection of SSDF attack using SVDD algorithm in cognitive radio networks[A]. Computational Intelligence, Communication Systems and Networks (CICSyN), 2011 Third International Conference on[C]. 2011. 201-204.

[58] AKBARI M, FALAHATI A. SSDF protection in cooperative spectrum sensing employing a computational trust evaluation algorithm[A]. Telecommunications (IST), 2010 5th International Symposium on[C]. 2010. 23-28.

[59] ABDELHAKIM M, ZHANG L, REN J, *et al*. Cooperative sensing in cognitive networks under malicious attack[A]. Acoustics, Speech and Signal Processing (ICASSP), 2011 IEEE International Conference on[C]. 2011. 3004-3007.

[60] YU F R, TANG H, HUANG M Y, *et al*. Defense against spectrum sensing data falsification attacks in mobile ad hoc networks with cognitive radios[A]. Military Communications Conference, MILCOM 2009[C]. 2009. 1-7.

[61] LI H N, REI Q Q, JIANG X H, *et al.* A sub-spectrum sensing scheme based on reputation in cognitive radio networks[A]. Computational Intelligence and Security (CIS), 2010 International Conference on[C]. 2010. 478-482.

[62] CHEN R L, PARK J M, BIAN K G. Robust distributed spectrum sensing in cognitive radio networks[A]. 2008 IEEE INFOCOM[C]. Piscataway, NJ, USA, 2008. 31-35.

[63] PEI Q Q, LI H N, MA J F, *et al*. Defense against objective function attacks in cognitive radio networks[J]. Chin J Electron, 2011, 20:138-142.

[64] SUPRATID I M. A multi-subpopulation particle swarm optimization: a hybrid intelligent computing for function optimization[A]. Natural Computation, ICNC 2007, Third International Conference on[C]. 2007. 679-684.

[65] HTIKE Z, JUN L, CHOONG SEON H. A MAC protocol for cognitive radio networks with reliable control channels assignment[A]. Information Networking (ICOIN), 2012 International Conference on[C]. 2012. 81-85.

[66] TAGUE P, LI M Y, POOVENDRAN R. Probabilistic mitigation of control channel jamming via random key distribution[A]. Personal, Indoor and Mobile Radio Communications, PIMRC 2007, IEEE 18th International Symposium on[C]. 2007. 1-5.

[67] DOERR C, SICKER D C, GRUNWALD D. Dynamic control channel assignment in cognitive radio networks using swarm intelligence[A]. Global Telecommunications Conference, IEEE GLOBECOM 2008[C]. 2008. 1-6.

[68] GOFF T, MORONSKI J, PHATAK D S, *et al*. Freeze-TCP: a true end-to-end TCP enhancement mechanism for mobile environments[A]. INFOCOM 2000, Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies [C]. 2000. 1537-1545.

[69] HERNANDEZ-SERRANO J, LEON O, SORIANO M. Modeling the lion attack in cognitive radio networks[J]. Eurasip Journal on Wireless Communications and Networking, 2011,2011:1-10.

[70] WANG W K, SUN Y, LI H S, *et al*. Cross-layer attack and defense in cognitive radio networks[A]. Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE[C]. 2010. 1-6.

作者简介：

裴庆祺（1975-），男，广西玉林人，西安电子科技大学副教授，主要研究方向为无线通信网络及其安全、数字内容保护等。

李红宁（1984-），女，河南开封人，西安电子科技大学博士生，主要研究方向为认知无线电网络安全。

赵弘洋（1988-），男，内蒙古包头人，西安电子科技大学硕士生，主要研究方向为认知无线电网络安全。

李男（1986-），女，河北秦皇岛人，西安电子科技大学硕士生，主要研究方向为无线电网络安全。

闵莹（1988-），女，陕西西安人，西安电子科技大学硕士生，主要研究方向为认知无线电网络安全。