认知无线网络的认知能力保障方法研究综述

冯光升[1] 郑 晨[1] 王慧强[1] 赵 倩[2] 吕宏武[1]
(哈尔滨工程大学计算机科学与技术学院 哈尔滨 150001)[1]
(哈尔滨商业大学计算机与信息工程学院 哈尔滨 150028)[2]

摘 要 认知无线网络通过对无线环境的感知获得频谱空洞信息,并以动态频谱接入为关键技术,机会地使用空闲频谱,与传统的无线网络相比,具有更高的网络通信资源利用率。认知能力作为认知无线网络的本质属性,其安全保障直接关系到认知无线网络的实用化进程。由于网络结构的复杂性、节点的移动性等问题,认知能力在各个认知环节中均面临不同程度的安全威胁。首先从认知循环:认知通信、资源感知、推理决策和服务适配4个环节分析认知能力保障所面临的安全问题以及相应的解决方案,然后总结现有方法的不足和缺陷,提出认知能力保障策略基于信任机制的发展趋势;最后指出未来认知能力保障领域所面临的挑战,并对该领域的研究方向进行了展望。

关键词 认知无线网络,认知能力,认知通信,资源感知,服务适配
中图法分类号 TP393 **文献标识码** A

Survey towards Cognitive Ability Guarantee in Cognitive Radio Networks

FENG Guang-sheng[1] ZHENG Chen[1] WANG Hui-qiang[1] ZHAO Qian[2] LV Hong-wu[1]
(College of Computer Science and Technology, Harbin Engineering University, Harbin 150001, China)[1]
(College of Computer and Information Engineering, Harbin University of Commerce, Harbin 150028, China)[2]

Abstract Cognitive radio network can sense wireless environment and then uses spectrum white holes in an opportunistic manner through dynamic spectrum access technology. Cognitive ability is an essential attribute of cognitive radio network, therefore the safety guarantee of cognitive ability is directly related to the practical process in cognitive radio networks. Cognitive ability is faced various security threats due to the complexity of cognitive radio network architecture and node mobility issues. Cognitive ability security issues and corresponding solutions were introduced from the aspects of cognitive communication, resources sensing, inference decision, and services fit, and then the shortages and weaknesses of the existing solutions were summarized. Development tendencies on cognitive ability guarantee were proposed afterwards based on trust mechanism. Problems and challenges faced by cognitive ability guarantee as well as a discussion on the future research topics were referred to at last.

Keywords Cognitive radio network, Cognitive ability, Cognitive communication, Resources sensing, Services fit

1 引言

认知无线网络是一种以动态频谱接入为关键技术的无线网络,是认知网络、Ad hoc网络、Mesh网络等接入技术融合发展的结果,以认知无线电为主要技术,根据当前网络状态进行分析、决策和响应,即能够基于认知过程,从历史数据中学习并将其应用于未来的决策。其中,认知能力作为认知无线网络的本质属性,是实现认知过程的基本前提,同时也是实现认知无线网络端到端通信目标的根本保障,其核心内容是合作感知与机会传输。合作感知可使认知节点(Secondary Users, SUs)获得相对准确的可用传输资源信息,机会传输保证认知节点充分利用频谱空洞资源,而这两者容易成为恶意节点的利用手段和攻击目标。导致此类安全隐患的原因主要有:(1)为了获得准确的感知结果,认知节点间需要相互合作与协同感知,因此产生了不可预知的安全隐患,如SSDF(Spectrum Sensing Data Falsification);(2)为抵御各种安全隐患并保障认知能力的鲁棒性,认知节点间需要协作检测各种威胁和攻击,如PUEA(Primary User Emulation Attack),但这需要合作节点之间的互信与共享,进一步加剧了安全风险;(3)机会接入与传输的认知本质也给网络中的恶意节点带来可乘之机。可以看出,认知无线网络的应用环境具有复杂性、动态性和未知性的特点,如果存在恶意节点的干扰和攻击,则会对认知决策产生颠覆性的影响[1-5]。因此,如何在不安全的环境中实现网络认知能力的保障已经引起了学术界的高度关

到稿日期:2013-06-19 返修日期:2013-10-14 本文受教育部博士点基金优先发展领域项目(20122304130002),中央高校基本科研业务费(HEUCF100601),黑龙江省博士后基金(LBH-210204),黑龙江省自然科学基金(F201037,ZD201102)资助。
冯光升(1980—),男,博士,讲师,主要研究方向为认知网络、信息安全,E-mail:fengguangsheng@hrbeu.edu.cn;**郑 晨**(1988—),女,硕士生,主要研究方向为认知网络;**王慧强**(1960—),男,博士,教授,主要研究方向为网络技术与信息安全;**赵 倩**(1980—),女,博士,讲师,主要研究方向为可信计算;**吕宏武**(1983—),男,博士,讲师,主要研究方向为可信软件。

注。

目前对于认知无线网络安全的研究综述一般有以下两种思路:1)从彼此隔离的网络层次角度出发,分析不同层次面临的安全威胁,并总结其防御方案;2)依托认知环,从通信过程展开安全威胁的讨论。第一种分析手段沿用了传统无线网络的研究模式,忽略了认知网络的认知循环特性;第二种分析手段虽然强调了认知无线网络的认知特点,但缺乏对网络认知能力水平的整体考量。本文则以认知能力的保障策略为主线,首先概要介绍认知无线网络的认知能力保障所面临的威胁;其次,结合当前国内外的研究现状,针对不同的安全威胁介绍了认知能力的保障策略;然后,基于信任机制,提出了认知能力保障策略的发展趋势;最后,指出未来认知能力保障领域面临的挑战并展望了研究方向。

2 认知能力保障面临的威胁

2.1 认知能力保障的威胁概述

认知无线网络环境下,认知节点首先根据感知环节得到周围无线网络的有关信息,比如通过对信道的感知得到主用户(Primary Users,PUs)对信道的使用情况,通过对邻居节点的感知得到其信道使用情况等;然后通过对感知信息进行分析,自适应地调整网络参数,做出相应决策,比如用户接入方案的选择;最后通过认知通信完成决策执行,其结果会直接影响无线网络环境。这个环路称为认知循环,简称认知环,而维系该循环过程正确进行的能力就是无线网络的认知能力[6]。有效的认知能力是确保整个认知过程按照预期行为模式进行工作的基础。认知能力可以通过对认知通信、资源感知、推理决策和服务适配 4 个部分的服务状况来进行描述。

频谱资源作为认知无线网络中的重要资源,是异常节点最容易围绕执行异常操作的目标。认知节点机会使用频谱资源而不是永久性占用频谱资源,因此认知节点的机会接入方式并不能阻止其他节点特别是异常节点对频谱资源的侵占。如果采用 IEEE802.22 标准,其信道分片、聚合和绑定机制易遭受异常节点的侵入并引发认知服务崩溃,而且随着认知节点对频谱资源利用的适应性和智能性增强,恶意节点同样也可利用智能技术制造出更为隐蔽的攻击。由此看来,信道资源容易遭受异常节点的感知和接入,进而认知过程的各个部分都存在受攻击的可能[7,8]。表 1 给出了认知过程的 4 个部分可能遭受的主要攻击威胁,以及对认知能力可能造成的影响。可以看出,认知过程的各个阶段都面临着各种攻击的威胁。因此,认知能力的保障方法的研究工作亟需开展。

表 1 认知过程的潜在威胁

服务类别	威胁类别	威胁后果
认知通信	干扰阻塞通信,如 Jamming、Sybil	影响认知过程的通信,扰乱或中断认知无线网络的认知循环;干扰主用户,减少主用户频谱资源,或对某一信道进行阻塞使其不能被主用户和正常认知用户使用
资源感知	干扰资源感知,如 PUEA、SSDF	影响认知节点对内部状态和外部资源的感知,特别是频谱资源的探测;阻止认知节点使用空闲频谱资源,降低信道性能
推理决策	干扰认知引擎,如 OFA	影响认知无线网络运行参数的决策结果,使其偏离优化值;通过修改参与推理决策的交互数据,以获得不当利益
服务适配	跨层联合攻击,如狮子攻击	底层多种攻击传播到高层,影响服务执行过程;注入虚假数据,导致网络运行故障甚至是按照攻击者的指令运行,影响整个认知循环

2.2 认知能力保障的威胁分析

(1)认知通信

认知通信是认知无线网络通信过程的底层支持,其影响贯穿于整个认知过程。认知通信过程易受链路攻击和路由攻击两种威胁,对认知能力有重要影响,严重情况下能终止认知过程。

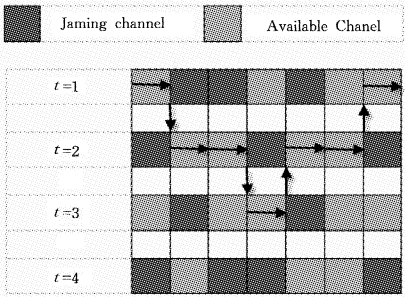

图 1 信道干扰示意图

由于认知无线网络本质上还是无线网络,认知通信所面临的链路威胁主要来自无线网络原发性底层攻击,通过干扰信道或阻塞链路直接终止通信过程。干扰攻击(Jamming)则是其中的典型代表,攻击位置位于网络物理层。实现链路/信道攻击的方式一般有:(1)干扰受攻击对象,降低其信噪比(Signal to Noise,SNR);(2)持续性发送报文,使频谱资源得不到释放。而第一种方式是认知无线网最容易遭受的攻击。如图 1 所示,在每一个时隙 t,PU 释放一些信道资源,如果没有信道攻击,SU 便可充分利用每个可用信道进行传输;但是当信道遭受攻击时,从 SU 的角度感知,一些在当前时隙下原本可用的信道就变得不可用,从而导致 SU 不得不等待下一个时隙的到来,这大大增加了传输时延,甚至导致传输中断而丢包。

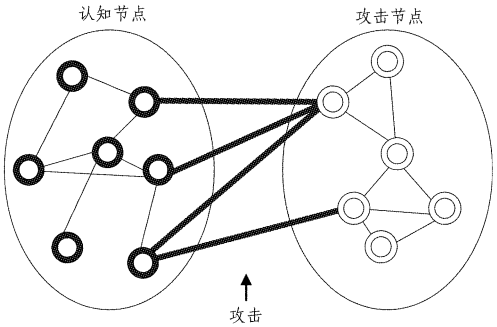

图 2 常见的路由攻击逻辑结构图

链路攻击主要是阻止认知用户使用信道资源,而路由攻击则有可能导致网络通信的中断,直接影响到认知循环的任何一个环节,女巫攻击(Sybil Attack)、虫洞攻击(Sinkhole Attack)均是典型的路由攻击。通常用无向图结构表示路由攻击,其中点表示认知节点或者攻击节点,边表示正常连接或者攻击连接[9],安全路由的问题可归结于节点间的信任问题,逻

辑结构如图 2 所示。因此，路由攻击检测就可以通过检测节点之间的关系来判断攻击边是否存在。在没有任何可信中心实体的情况下，抵御路由攻击非常困难，因为这些攻击既可以从网络内部发起，也可以从网外的僵尸网络发起。

(2)资源感知

在资源感知阶段，认知用户通过对其周围无线环境的资源感知，获得频谱空洞的信息，而这个过程可能会引入恶意节点或自私节点的干扰，使面向资源感知的认知能力面临安全威胁，主要威胁有资源阻止和资源欺骗两种。所谓资源阻止威胁，就是恶意节点通过阻止手段使其他节点无法使用空闲的频谱资源，导致资源的浪费。这一类攻击的代表为 PUEA，该攻击行为是恶意节点模仿主用户使用频谱资源，造成其他认知节点误认为是主用户正占用该频谱资源，从而放弃对该频谱资源的接入与使用。在认知无线网络中，单节点的资源感知结果受无线环境的影响比较大，因此资源感知主要采用合作感知的手段。合作感知是认知节点通过合作的方式对主用户占用频谱资源的情况进行探测，每个认知节点独立感知信道，然后共享感知结果，从而更准确地获得频谱资源信息，但同时也引来了安全威胁：恶意节点共享错误的感知结果，或截获并篡改正常节点的感知结果；自私节点为了节约能耗，只是把其他节点的检测结果据为己用或者花费少量能耗产生干扰信息来影响其他节点的判断，从而造成资源欺骗威胁。资源欺骗威胁的主要代表是 SSDF 攻击。

(3)推理决策

认知过程的一个关键步骤是通过感知外部环境来调整自身的运行参数，以提升网络性能，这是推理决策阶段，也是需要安全保障的重要阶段。然而有一类网络威胁，通过适当方式干扰网络底层通信资源，致使网络高层的服务能力发生变化，这对于有推理学习能力的认知无线网络来说，会引发认知引擎调整自身的工作参数，致使网络性能并不能总处于一个最优的水平上。目标方程攻击(Object Function Attack，OFA)是影响认知引擎的推理学习能力的主要威胁。攻击者可以通过干扰信道等手段，迫使认知网络通过优化算法调整自身的运行参数，使目标函数偏离最优值，从而达到操控网络运行的目的[10]。

(4)服务适配

根据认知循环的决策结果，认知无线网络可通过相应地调整两种类型的服务参数来展开其服务适配阶段：一类是底层运行参数，如频率、带宽、功率、制式、帧长等；另一类为高层服务参数，如传输层的传输速率、拥塞窗口等。其中，底层运行参数的调整容易遭受 OFA 攻击，而高层服务参数则易受跨层攻击的影响，导致高层服务适配能力下降。通常来讲，影响服务适配能力的跨层攻击一般有两种：一种攻击通过使用闭环流来恶意降低传输层的吞吐量，依靠端到端的控制协议，基于反馈测量推断网络状态，进一步对反馈测量信息实施干扰，致使传输层的吞吐量不断衰减，导致传输层功能紊乱[11]，如 Jellyfish；另一种通过在物理层和链路层精心设计 Jamming 或者 PUEA 攻击，迫使网络频繁发生频带切换，导致传输性能下降，如 Lion 攻击。

3 认知能力保障策略的分类及比较分析

从第 2 节可以看出，认知能力在认知通信、资源感知、推理决策和服务适配 4 个环节均面临着严峻的安全威胁，现有的保障策略研究均是从上述 4 个方面展开的。

3.1 面向认知通信的认知能力保障策略

认知通信贯穿于认知循环的整个过程中，如果认知通信能力得不到保障，则认知循环过程在链路层面和路由层面均可能受到攻击。

3.1.1 链路攻击的应对策略

防御链路攻击主要有两种方案：基于博弈论的方案和基于优化理论与密码学的方案，具体的分类及解决方案见表 2。

表 2 链路攻击威胁及其应对策略分类

方案类型	适用场景	假设条件	优点	缺点
基于博弈论的方案[12,13]	认知无线网络	主用户和认知用户发射的信号能明显区别开来	每一阶段都逼近最优策略	假设条件过于理想
基于优化理论与密码学的方案[14]	认知无线网络	认知无线网络不需要严格的时间同步	适合多种无线网络	较高的计算代价和处理时延

(1)基于博弈论的方案

基于博弈论的方案是根据 SUs 对频谱或攻击者的观察结果，采用博弈模型对信道切换、选择以及数据传输进行决策。文献[12]将 SUs 的安全机制与 Jamming 攻击行为建模为随机博弈模型；在每一博弈阶段，SUs 观察频谱可用性、信道质量以及攻击者的攻击策略；据此决策信道切换方案，以及预留命令传输和数据传输所需的信道数量；然后通过 MINIMAX-Q 学习，逼近最优策略。文献[13]通过分析 SUs 与攻击者的交互过程，将信道选择和信道跳跃建模为一个 Jamming 容忍博弈模型，在此基础上提出了一个基于 MDP(Markov Decision Process)的信道跳跃技术来降低 Jamming 攻击带来的影响。然而上述博弈观点解决信道抗干扰问题多需要严格的条件假设，如完美信息博弈，这与实际情况不符。采用机器学习方法可以弥补对手策略信息的不足，但是会带来较高的处理时延。

(2)基于优化理论与密码学的方案

基于优化理论与密码学的方案分别通过对邻居发现算法的优化和数据信道加密的方法，来防止信道干扰和应对信道攻击。文献[14]针对认知网络的邻居发现过程有可能被干扰攻击中断的情况，提出了一种 Jamming 攻击容忍算法，但其存在较高的计算代价和处理时延的问题。文献[15]提出了一个基于“Zero Pre-shared Secret Key”的抗信道干扰方案，该方案对控制信道和数据信道分别提出了应对策略；控制信道方案可以精确计算内外部攻击者的数量，保证了在控制信息交付过程中能够应对各种攻击者联盟；数据信道方案采用加密 PN 序列进行报文传输，在弹性应对干扰攻击和计算负载两方面取得平衡，但是该方案不符合 FCC 的规定。

3.1.2 路由攻击的应对策略

常见的路由攻击采用对称密码体制就可以防范，然而对认知无线网络环境中由网络内部恶意节点发起的攻击，如女巫攻击(Sybil)、选择转发、虫洞攻击(Sinkhole)等收效甚微；特别是认知特征促使 SUs 之间易于建立合作感知机制，SUs 可以在这种开放的网络域按需加入和退出，因而认知无线网络面临更为严重的路由安全威胁。应用第三方信任机制(Third Trusted Party，TTP)虽可以解决认知无线网络下的路由安全问题，但在动态开放的网络环境下，很难找到一个可信

的第三方实体；即便将 PUBS 作为第三方可信实体，也面临单点失效的问题，还违反了 FCC 的准则。目前路由攻击的解决方案主要有两种：基于认证与信号强度的方案和基于信任机制的方案，详见表 3。

表 3　路由攻击威胁及其应对策略分类

方案类型	适用场景	假设条件	优点	缺点
基于认证与信号强度的方案[17]	分布式网络	基站的能量对于用户来说是足够的甚至是有源的	网络能耗较小	检测的准确度有限
基于信任机制的方案[18]	车载Ad-hoc网络	大部分节点是可信的，且每辆车都装有GPS	不需要特殊的定位装置就可以检测 Sybil 攻击	需要部署子系统，如噪声评估系统

(1)基于认证与信号强度的方案

基于认证与信号强度的方案分别通过引入受信节点和信号强度阈值来进行节点的认证和攻击的检测，从而防御路由攻击。文献[16]为克服 Sybil 攻击中的敌手作弊，引入受信节点构成分布式认证系统，由受信节点对新加入节点进行认证，保证节点签名和 ID 不能伪造；同时引入记录洗牌加入过程的票据来判定节点合法性，杜绝了敌手积累过期。文献[17]针对 LEACH 协议存在的路由安全隐患问题，提出了一种改进 LEACH-S 机制；采用接收信号强度值(RSSI)的 Sybil 攻击入侵检测策略，设定合理的阈值来启动该机制，即只有在判定可能遭遇 Sybil 攻击时才启动。上述方案大都采用测量信号强度的概率分布来分析攻击是否存在，为提高检测准确度，虽然有方案通过邻居节点的合作探测来测量可疑节点的信号强度分布，并验证其物理位置，但是对于不稳定的无线信道，其能够达到的检测准确度有限，而且可能面临由恶意节点杜撰信号强度测量的问题。

(2)基于信任机制的方案

基于信任机制的方案通过分布式信任机制对网络单个节点或实体的信任评估，得出相应的信任度，据此进行攻击检测或防御。文献[18]设计了一个现场证据系统 PES(Presence Evidence System)来测量节点的信任度，在节点移动模型可知的情况下，采用概率统计的方法能够较为准确地检测到攻击节点。Kumar 等人[19]认为：为提高分布式网络的安全性能，有必要对网络中各参与实体进行信任估计，因而提出了一个降低 Sybil 攻击影响的 DAS 协议。EI Zoghby 等人[20]采用基于数据融合的方法检测 VANET 环境下的 Sybil 攻击，该方法在信任机制基础上建立了整个网络背景下的分布式信任。上述方案都是针对车载网络基于信任机制来检测 Sybil 攻击的，但都需要部署额外的子系统，结构复杂。

3.2　面向资源感知的认知能力保障策略

资源感知是认知循环的关键环节，是认知能力保障的核心，其面对的主要威胁是资源阻止和资源欺骗威胁。

3.2.1　资源阻止威胁的应对策略

对于资源阻止威胁，目前的研究一般通过验证主用户信号的真实性来进行防御，采取的防御手段主要有：基于地理位置信息与接收信号强度(Received Signal Strength，RSS)的验证方案[21]、基于概率模型的验证方案[22,23]和基于签名技术的验证方案[24]。具体的方案类型及其特点参见表 4。

表 4　资源阻止威胁及应对策略分类

方案类型	适用场景	假设条件	优点	缺点
基于地理位置信息与接收信号强度的验证方案[21]	节点移动性较低的认知网络	攻击者知道所有节点之间的距离	对网络负载没有影响	需要主用户的地理位置、认知节点的地理位置、RSS 的采集设备等，增加了部署和维护成本
基于概率模型的验证方案[22,23]	主用户固定的认知无线网络	主用户位置固定，认知用户距离主用户较远，且恶意节点在攻击过程中传输功率恒定	不需要地理位置先验知识，所有认知节点均可以根据算法独立检测 PUEA	要求认知节点和恶意节点服从均匀分布，且主用户距认知用户较远且位置固定
基于签名技术的验证方案[24]	攻击者距离主用户较远的认知无线网络	攻击者有较高的传输功率且不能攻击“辅助节点”	不需要学习训练过程	需要在每一个主用户附近部署一个“辅助节点”，增加了部署和维护开销

基于地理位置信息与接收信号强度的验证方案一般包括 3 个关键环节：校验信号特征、信号能量估计、传输者定位。然而这类方案适用于节点移动性较低的网络，并且需要假设攻击者知道所有节点之间的距离，也需要主用户的地理位置、认知节点的地理位置、RSS 的采集设备等，虽然对网络负载没有影响，但是增加了部署和维护成本；同时，攻击者可以采用估计技术从接受信号中获得环境信息，从而调整策略以获得最大收益，比如攻击者在 PUBS 附近实施 PUEA 就很难被发现。

基于概率模型的验证方案的基本思想是通过信号采样和概率模型进行拟合，根据拟合程度来判断威胁的存在与否，如文献[22]提出的 Wald 序贯概率检验方案(Wald's sequential probability ratio test，WSPRT)。该类方案适用于主用户固定且主次用户分区明显的网络。所有认知节点均可以根据算法独立检测 PUEA 攻击，并且不需要地理位置先验知识，但是要求认知节点和恶意节点服从均匀分布，且主用户与认知用户距离较远且位置固定，并假设恶意节点在攻击过程中传输功率恒定。

基于签名技术的验证方案，其最简单的方式是在主用户信号中嵌入签名，或者在主用户和认知节点之间采用认证机制，但这违反了 FCC 规定，所以通常采用折中的物理层鉴别方案：在主用户附近部署一个“辅助节点”[24]，该节点作为认知节点和主用户沟通的桥梁，认知节点可以验证“辅助节点”的密码签名信号，然后通过获取“辅助节点”的链路签名来验证主用户的信号。这类方案要求攻击者有较高的传输功率且距离主用户较远，并假设攻击者有较高的传输功率且不能攻击“辅助节点”。该类方案虽然不需要节点的学习训练过程，但是需要在每一个主用户附近部署一个“辅助节点”，增加了部署和维护开销。

3.2.2　资源欺骗威胁的应对策略

资源欺骗威胁的主要防御手段可分为集中式和分布式两种。在集中式的合作感知中，认知节点需要将感知结果共享或者发送给融合中心(Fusion Center，FC)，这个过程无法保证各个感知结果的正确性。为了避免错误的感知结果参与融

合决策，通常采取融合中心对各个认知节点的行为进行判断的方案，以确定该认知节点的感知结果是否可用于融合决策。其中，判断认知节点的典型方法是基于历史报告的信誉计算方案[25]，此外还有基于随机观察的方案[26]、基于RSS相似度检验的方案[27]、基于认知节点与融合中心输出比较的方案[28-32]。

基于历史报告的信誉计算方案通过恶意用户监测算法计算认知用户的可信程度，从而区分诚实用户和恶意用户，有效地提高频谱合作感知的安全性，但是要求信道状态的使用情况相互独立，并且只能检测单个攻击，此外，信誉计算需要大数据量采样，在高度动态的环境中容易发生死锁；基于随机观察的方案虽然能避免采样死锁，并可以解决SSDF多个攻击问题，但是要求认知节点在网络中分布均匀，而且若缺乏足够的观察数据，认知节点信誉值波动就会比较大；基于相似度检验的方案可以对抗智能的攻击者，即在没有融合中心决策的情况下也能知道主用户的信号是否存在攻击者，但是需要部署传感器节点以收集RSS，通过检验RSS的相似度来判断节点行为，并且假设传感器组成的簇在认知无线网络中分布均匀，超过2/3的传感器可以很好地工作，因此RSS检验也面临稳定性差的问题；基于认知节点与融合中心输出比较的方案，通过感知输出与FC输出的结果进行比较，来区别攻击者与诚实的用户，但是却面临着融合策略、融合中心故障或入侵等多方面的影响，稳定性较差。具体各类型的特点参见表5。

表5　集中式资源欺骗威胁及应对策略分类

方案类型	适用场景	假设条件	优点	缺点
基于历史报告的信誉计算方案[25]	信道使用情况相互独立的认知无线网络	只有一个恶意用户，且信道状态在不同的时隙是相互独立的	对于表现突然或偶尔变差的认知用户的感知信息也能充分利用	只能检测单个攻击，并且需要大数据量采样，在高度动态的环境中容易发生死锁
基于随机观察的方案[26]	节点分布均匀的认知无线网络	认知节点等概率地分布在区域的不同位置中	能避免采样死锁，并且可以解决SSDF多个攻击问题	如果缺乏足够的观察数据，认知节点信誉值波动会较大
基于RSS相似度检验的方案[27]	有传感器的动态频谱接入网路	基站或融合中心不会遭到攻击，并且超过2/3的传感器工作状态良好	可以对抗智能的攻击者，即在没有融合中心决策的情况下也能知道主用户的信号是否存在	需要部署辅助传感器网络，增大了网络的部署正本
基于认知节点与融合中心输出比较的方案[28-32]	认知无线网络	攻击者之间不进行通信，并且各自的攻击决策是相互独立的	可以对抗多个攻击	面临着融合策略、融合中心故障或入侵等多方面的影响，稳定性较差

分布式的资源欺骗威胁应对策略是共享各个节点独立感知信道的数据，然后由各个节点独立决策最终的感知结果。主要的检测手段是认知节点基于能量信息，探测主用户的传输状况，并通过邻居节点的共享信息来更新自身的探测结果，每个认知节点通过计算邻居节点共享信息与均值的偏差来过滤潜在的攻击者，以有效地避免单点失效问题。但是由于缺少融合中心的检测，这种方案很难抵御共谋攻击，因此依然面临着严重的感知欺骗问题。针对此问题，文献[33]提出了一种基于生物启发的分布式检测方案，即利用生物群体的自组织行为，使网络系统具备自配置和自维护的能力。

3.3　面向推理决策的认知能力保障策略

OFA问题通常可建模为多目标规划模型MOP(Multi-objective Programming Model)[35]，其造成的后果取决于所采用的在线学习算法的鲁棒性。目前有3种应对OFA攻击的方案：一是通过可调参数的门限值来鉴别OFA，如果参数调整偏离了约束范围，认知引擎的调整过程就终止[10]，但是在任何情形下都只能转变OFA攻击，并不能阻止它，而且阈值范围内的参数调整也可能导致目标函数偏离优化值；第二种方案采用IDS(Intrusion Detection System)的手段检验可疑或恶意的节点，并将这些信息提供给节点运行的其他协议(比如路由协议和聚合协议)，如文献[34]中，每个节点都参与入侵的检测和回应，并且配备自己的IDS代理，代理独立执行，监视本地活动并与邻居IDS代理共享检测信号，这些代理共同组成了IDS，为无线Ad hoc网络工作，该方案适合于小规模无线网络，对于规模稍大的网络而言缺乏可实施性；第三种方案，通过粒子群优化算法调节子目标的参数，使其适应新的环境，即使在篡改的数目较大的情况下也可以检测出所有被篡改的参数[35]，但是屡次使用该方案会带来较大的计算负载和通信负载。其具体的分类及相应的应对策略见表6。

表6　推理决策威胁及应对策略的分类

方案类型	适用场景	假设条件	优点	缺点
基于可调参数的门限值的验证方案[10]	认知无线网络	无	当参数超过阈值时可以及时制止通信	只能转变OFA攻击，并不能阻止，并且阈值范围内的参数调整也可能导致目标函数偏离优化值
基于IDS的验证方案[34]	无线Ad hoc网络	各IDS代理独立工作	多数据融合模块可以为多层综合入侵检测提供数据流的融合计算	不适合在大规模的认知无线网络部署
基于粒子群优化算法[35]	资源充分且计算能力较强的认知无线网络	无	可以检测出所有被篡改的参数	导致较大的计算负载和通信负载

3.4　面向服务适配的认知能力保障策略

认知无线网络可以根据认知循环的决策结果相应地调整底层运行参数和高层服务参数。其中底层参数的调整过程容易遭受OFA攻击，其防御方案详见上节；高层服务参数调整过程容易受跨层攻击的影响，导致高层服务适配能力下降，其典型的攻击代表是Jellyfish和Lion攻击。

针对Jellyfish攻击，目前的研究一般采用Freeze-TCP及EMUNE(Effective Mobile Usage of Heterogeneous Networks)的方案，使高层协议感知到网络底层发生的各种安全事件，并调整自身行为以适应网络状态的变化，但在本质上并没有消除威胁[36]。Lion攻击的防御手段主要是通过改进Freeze-TCP，使之能够定位威胁位置并跨层传导威胁信息，由

传输方主动预测连接中断，实施传输参数冻结方案，降低频繁切换信道对 TCP 性能的影响，并在切换频谱后重新连接并适应新的网络[37]。跨层攻击应对策略的分类详见表 7。

表 7　跨层攻击以应对策略分类

方案类型	适用场景	假设条件	优点	缺点
基于 Freeze-TCP 及 EMUNE 的检测方案[36]	认知无线网络或移动无线网络	移动节点总是能够回应 TCP 连接	及时地保证数据流传输的暂停和开启，保证在时间和空间上更有效地利用网络	在本质上并没有消除威胁
基于改进 Freeze-TCP 的检测方案[37]	认知无线网络	TCP 连接的往返时间总小于重传时间超时的最小值	有效地减小了频谱频繁切换对 TCP 性能下降带来的影响	不能对抗智能攻击，需要进一步引入入侵检测系统来检测智能的跨层攻击

3.5　认知能力保障策略的发展趋势

认知无线网络的认知能力保障问题已经引起了国内外学者的高度关注。认知能力的保障依赖于认知循环过程中信息处理与通信各环节的安全支持，开放共享的通信资源环境和未知节点的相互合作是威胁认知能力的首要原因。当前，对认知能力保障的研究主要集中在协作探测安全威胁和鲁棒性的频谱感知方面，如异常节点的定位、过滤，这类方案依赖于特定的网络拓扑结构，对认知能力的保障程度有限，而且现有的一些防御方案均是针对某一类具体的威胁，无法处理威胁演化、联合跨层攻击等情况，严格来讲，均是具体安全隐患或者攻击检测手段的升级演化。而且由于计算资源、通信资源、网络结构、FCC 规定等方面的限制，在不安全的环境中实现认知能力的保障还没有理想的解决方案。

鉴于上述存在的弊端，学术界逐渐意识到，认知能力的保障需要的是信任机制，而不是纯粹的安全机制：认知节点感知频谱空洞或者机会、动态地利用频谱空洞进行传输需要主用户的信任；认知节点利用无线节点进行通信、合作感知或者合作检测，需要合作节点的信任；利用主用户基站(Primary Users Base Station，PUBS)将报文转发到另外一个交换网络，需要主用户基站的信任。因此，无论是协作感知、协作检测还是机会接入都需要对认知域的合作节点进行评估，亟需一种信任机制使节点间彼此协同工作。

本章节基于信任机制，面向认知能力的保障提出以下 4 点建议：(1)针对认知能力保障的形式化问题，需要提出一种建模方法来建立相应的信任模型并探讨认知节点的行为决策；(2)结合节点的认知性、自私性等行为属性，需要提出一种节点信任度的测量方法；(3)需要一种信任的传播方案来保证在不安全的环境下实现可靠的全局信任计算；(4)需要设计一套适用于认知无线网络的测评工具集，来实现认知能力保障方法的评测验证。以上 4 点建议从认知无线网络的认知特征出发，分别从节点信任计算、信任传播和全局信任模型的层次角度解决认知能力保障的安全问题，这将为突破认知能力保障问题提供一种新思路，有助于丰富和完善认知无线网络的技术方法体系，对促进其实用化提供有力的支撑。

结束语　随着纷繁复杂的无线网络应用的不断推广，频谱资源的合理利用越来越值得重视，认知无线网络将会成为未来无线网络的研究重点，进而认知能力保障问题也将会成为国内外学者的研究热点。本文详细介绍了认知能力保障面临的安全威胁以及相应的应对方法，并提出了认知能力保障策略基于信任机制的发展趋势。目前，认知能力保障的研究正处于起步阶段，还存在以下问题没有得到解决：(1)由于认知无线网络的干扰限制，需要准确判断认知节点是由于自私性不参与合作，还是出于干扰控制而不进行合作。这是两个相互矛盾的指标，如果判断失误，对网络系统的服务适配决策将产生颠覆性的影响。(2)认知无线网络的异步通信和时效性特征，使得传统的信任评估、激励机制、时效性等均发生了本质的变化，传统的信任体制在应对不诚实推荐、协同作弊及一些复杂策略性攻击方面能力有限，不足以保障认知能力不受损害。(3)认知无线网络存在异构性，存储能力、计算能力、通信能力均有限，现存的复杂的协议或计算模型一般缺乏工程可行性，而且无法在上述因素间取得动态平衡。这些问题为认知能力的保障提供了进一步的研究方向，但同时也为研究带来了新的挑战。

参 考 文 献

[1] 薛楠，周贤伟，周健. 认知无线电网络诱骗攻击问题及安全解决方案[J]. 电信科学，2009，25(5)：81-87

[2] 黑永强，李晓辉，李文涛. 认知网络中的多用户 MIMO 线性协作频谱感知问题研究[J]. 通信学报，2012，33(3)：45-52

[3] 刘全，高俊，郭云玮，等. 抗 SSDF 攻击的一致性协作频谱感知方案[J]. 电子学报，2011，39(11)：2643-2648

[4] 曾昆，彭启航，唐友喜. 基于信任节点辅助的安全协同频谱感知策略[J]. 信号处理，2011，27(4)：486-491

[5] 贺倩，冯志勇，张平. 基于人工智能技术的认知无线网络重构决策算法[J]. 通信学报，2012，33(7)：96-102

[6] Fragkiadakis A G，Tragos E Z，Askoxylakis I G. A Survey on Security Threats and Detection Techniques in Cognitive Radio Networks[J]. Communications Surveys & Tutorials，IEEE，2013，15(1)：428-445

[7] Vien Q T，Stewart B G，Tianfield H，et al. Efficient cooperative spectrum sensing for three-hop cognitive wireless relay networks[J]. Communications，IET，2013，7(2)：199-127

[8] Zhang Xing，Xing Jia，Yan Z，et al. Outage performance study of cognitive relay networks with imperfect channel knowledge[J]. IEEE Communications Letters，2013，17(1)：27-30

[9] Kumar R N，Bapuji V，Govardhan A，et al. An Improvement to Trust Based Cross-Layer Security Protocol against Sybil Attacks (DAS)[J]. Computer Engineering and Intelligent Systems，2012，3(7)：62-70

[10] León O，Hernández-Serrano J，Soriano M. Securing cognitive radio networks[J]. International Journal of Communication Systems，2010，23(5)：633-652

[11] Reddy K G，Thilagam P S. Intrusion Detection technique for wormhole and following jellyfish and byzantine attacks in wireless mesh network[J]. Advanced Computing，Networking and Security，2012，7135：631-637

[12] Wang B，Wu Y，Liu K R，et al. An anti-jamming stochastic game for cognitive radio networks[J]. IEEE Journal on Selected Areas in Communications，2011，29(4)：877-889

[13] Wu Y，Wang B，Liu K，et al. Anti-jamming games in multi-channel cognitive radio networks[J]. IEEE Journal on Selected Areas in Communications，2012，30(1)：4-15

(下转第 19 页)

[8] Hare J S, Samangooei S, Dupplaw D P. OpenIMAJ and ImageTerrier: Java libraries and tools for scalable multimedia analysis and indexing of images, 2011 [C]// Proceedings of the 19th ACM international conference on Multimedia. Scottsdale, Arizona, USA, 2011: 691-694

[9] Chu Bin, Jiang Da-lin. Panoramic Image Stitching Using ASIFT, 2012 [C]// Fourth International Conference on Multimedia Information Networking and Security. 2010: 216-219

[10] Yin Chun-xia, Li Cheng-rong, Liu Hong-lin, et al. Experimental Contrast of Several Typical Algorithms for Local Features Detection, 2012 [C]// International Conference on Mechanical Engineering and Automation Advances in Biomedical Engineering. 2012: 65-71

[11] Panga Yan-wei, Lia Wei, Yuan Yuan, et al. Fully affine invariant SURF for image matching[J]. Neurocomputing, 2012, 85: 6-10

[12] 卢风顺，宋君强，银福康，等. CPU/GPU 协同并行计算研究综述[J]. 计算机科学，2011，38(3)：5-9

[13] 王永明，王贵锦. 图像局部不变性特征与描述[M]. 北京：国防工业出版社，2010：79-87

[14] Morel J-M, Yu Guo-shen. ASIFT: online demo[OL]. http://www. cmap. polytechnique. fr/～ yu/research/ASIFT/demo. html

(上接第 13 页)

[14] Asterjadhi A, Zorzi M. JENNA: a jamming evasive network-coding neighbor-discovery algorithm for cognitive radio networks [Dynamic Spectrum Management] [J]. Wireless Communications, IEEE, 2010, 17(4): 24-32

[15] Zhang Lu, Pei Qing-qi, Li Hong-ning. Anti-jamming Scheme Based on Zero Pre-shared Secret in Cognitive Radio Network [C]// Proceedings of Computational Intelligence and Security (CIS), 2012 Eighth International Conference on. Guangzhou, China, 2012: 670-673

[16] 聂晓文，卢显良，唐晖，等. 基于洗牌策略的 Sybil 攻击防御[J]. 电子学报，2008(11)：2144-2149

[17] 陈珊珊，杨庚，陈生寿. 基于 LEACH 协议的 Sybil 攻击入侵检测机制[J]. 通信学报，2011，32(8)：143-149

[18] Yu Bo, Xu Cheng-zhong, Xiao Bin. Detecting Sybil attacks in VANETs[J]. Journal of Parallel and Distributed Computing, 2013, 73(6): 746-756

[19] Kumar R N, Bapuji V, Govardhan A, et al. An Improvement to Trust Based Cross-Layer Security Protocol against Sybil Attacks (DAS) [J]. Computer Engineering and Intelligent Systems, 2012, 3(7): 62-70

[20] El Zoghby N, Cherfaoui V, Ducourthial B, et al. Distributed Data Fusion for Detecting Sybil Attacks in VANETs [M]// Belief Functions: Theory and Applications. Springer Berlin Heidelberg, 2012: 351-358

[21] Chen Ze-sheng, Todor C, Chen Chao, et al. Modeling primary user emulation attacks and defenses in cognitive radio networks [C]// Proceedings of 2009 IEEE 28th International Performance Computing and Communications Conference (IPCCC). Scottsdale, AZ, 2009: 208-215

[22] Jin Z, Anand S, Subbalakshmi K. Detecting primary user emulation attacks in dynamic spectrum access networks[C]// Proceedings of 2009 IEEE International Conference on Communications(ICC'09). Dresden, German, 2009: 1-5

[23] Jin Z, Anand S, Subbalakshmi K. Mitigating primary user emulation attacks in dynamic spectrum access networks using hypothesis testing[J]. ACM SIGMOBILE Mobile Computing and Communications Review, 2009, 13(2): 74-85

[24] Liu Y, Ning P, Dai H. Authenticating primary users' signals in cognitive radio networks via integrated cryptographic and wireless link signatures[C]// Proceedings of 2010 IEEE Symposium on Security and Privacy (SP). Oakland, CA, USA, 2010: 286-301

[25] Wang Wen-kai, Li Hu-sheng, Sun Y L, et al. Attack-proof collaborative spectrum sensing in cognitive radio networks[C]// Proceedings of the 43rd Annual Conference on Information Sciences and Systems(CISS 2009). Baltimore, MD, 2009: 130-134

[26] Zhu F, Seo S-W. Enhanced robust cooperative spectrum sensing in cognitive radio[J]. Journal of Communications and Networks, 2009, 11(2): 122-133

[27] Min A W, Shin K G, Hu Xin. Attack-tolerant distributed sensing for dynamic spectrum access networks[C]// Proceedings of 17th IEEE International Conference on Network Protocols (ICNP 2009). Princeton, NJ, 2009: 294-303

[28] Chen Rui-liang, Park Jung-min, Bian Kai-gui. Robust distributed spectrum sensing in cognitive radio networks[C]// Proceedings of the 27th IEEE Conference on Computer Communications(INFOCOM 2008). Phoenix, AZ, 2008: 1876-1884

[29] Chen R, Park J-M J, Bian K. Robustness against byzantine failures in distributed spectrum sensing[J]. Computer Communications, 2012, 35(17): 2115-2124

[30] Rawat A S, Anand P, Chen Hao, et al. Countering byzantine attacks in cognitive radio networks [C]// Proceedings of 2010 IEEE International Conference on Acoustics Speech and Signal Processing (ICASSP). Dallas, TX, 2010: 3098-3101

[31] Nguyen-Thanh N, Koo I. An enhanced cooperative spectrum sensing scheme based on evidence theory and reliability source evaluation in cognitive radio context[J]. Communications Letters, IEEE, 2009, 13(7): 492-494

[32] Li Hu-sheng, Han Zhu. Catching attacker (s) for collaborative spectrum sensing in cognitive radio systems: An abnormality detection approach[C]// Proceedings of 2010 IEEE Symposium on New Frontiers in Dynamic Spectrum. Singapore, 2010: 1-12

[33] Tang H, Yu F R, Huang M, et al. Distributed consensus-based security mechanisms in cognitive radio mobile ad hoc networks [J]. IET Communications, 2012, 6(8): 974-983

[34] Zhang Yong-guang, Lee Wen-ke. Intrusion detection in wireless ad-hoc networks[C]// Proceedings of the 6th annual international conference on Mobile computing and networking. ACM. New York, NY, USA, 2000: 275-283

[35] Pei Q, Li H, Ma J, et al. Defense against objective function attacks in cognitive radio networks[J]. Chinese Journal of Electronics, 2011, 20(4): 138-142

[36] Rathnayake U, Petander H, Ott M, et al. EMUNE: architecture for mobile data transfer scheduling with network availability predictions[J]. Mob. Netw. Appl., 2012, 17(2): 216-233

[37] Hernandez-Serrano J, León O, Soriano M. Modeling the lion attack in cognitive radio networks[J]. EURASIP Journal on Wireless Communications and Networking, 2011, 2011: 1-10