基于多角度多层次的认知无线电网络安全研究①

孙丽艳[1], 周森鑫[1], 周 健[1,2]

[1](安徽财经大学 管理科学与工程学院, 蚌埠 233041)
[2](北京邮电大学 计算机学院, 北京 100083)

摘 要: 认知无线电(Cognitive Radio)技术是为了解决无线网络中频谱资源短缺问题而提出来的新兴技术, 它的提出有效的缓解了频谱资源短缺问题, 但同时也引入了特有的安全威胁, 针对认知无线的特点, 从整体架构、协议栈和认知行为的多个角度和层次,研究其在无线网络中引入的安全隐患和已有的解决方案, 并对认知无线电安全问题做进一步的展望.

关键词: 认知无线电; 安全架构; 协议栈; 认知引擎; 安全

Security of Cognitive Radio Network Based on Multi-Perspective

SUN Li-Yan[1], ZHOU Sen-Xing[1], ZHOU Jian[1,2]

[1](School of Management Science and Engineering, Anhui University of Finance and Economics, Bengbu 233041, China)
[2](Department of Computer, Beijing University of Posts and Telecommunications, Beijing 100083, China)

Abstract: Cognitive radio network is a kind of wireless network in order to solve the problem of shortage of spectrum resources, and puts a new technology that can allocate shortage of spectrum resources efficiently, while brings the new questions about security because of characteristics, such as dynamic, distribute, openness. The paper introduces the security of cognitive radio and existing solutions from multi-perspective, including protocol stack and cognitive behavior. Finally, we discuss the development of cognitive wireless security in the future.

Key words: cognitive radio; security framework; protocol stack; cognitive engineer

随着无线通信业务需求的快速增长, 可用频谱资源变得越来越稀缺, 链路自适应、多天线等技术提高频谱效率的同时, 却增加了成本和干扰,限制了通信系统的容量和灵活性. 美国联邦通信委员会的大量研究报告说明频谱的利用情况极不平衡, 一些非授权频段占用拥挤, 而有些授权频段则经常空闲. 因此近几年来, 能够对不可再生的频谱资源实现再利用的频谱共享技术受到了人们的广泛关注. 虽然工业、科学和医用频段开放接入, 但是也存在干扰大、容量小、灵活性差等问题. 认知无线电(Cognitive Radio, CR)作为一种更智能的动态频谱共享技术, 能够依靠人工智能的支持, 感知无线通信环境, 根据学习和决策算法, 实时自适应地改变系统工作参数, 动态地检测和有效地利用空闲频谱, 在时间、频率以及空间上进行多维的频谱复用, 大大降低频谱和带宽限制对无线技术发展的束缚. 因此这一技术被预言为未来最热门的无线技术.

由于认知无线电是无线通信的一种, 因此也具有传统无线网络的安全隐患, 引入认知行为和动态频谱后, 也带来了新的安全隐患, 如对主用户的冒充、信道分配、自私行为等等. 传统计算机网络在设计之初, 没有考虑到安全问题, 使得计算机网络在大规模应用中面临诸多安全问题的挑战, 不仅协议设计具有脆弱性, 增加了设计成本, 降低效率; 而且不断增加的安全协议补丁, 破坏了计算机网络的体系结构. 因此作为下一代网络的关键技术--认知无线电网络, 应该在网络协议设计中综合考虑安全问题, 为将来的大规模应用做好基础准备.

① 基金项目:国家自然科学基金(61402001);安徽省高等学校自然科学研究项目(KJ2013B001);安徽财经大学 2015 年度校级科研课题(ACKY1517ZDB)
收稿时间:2015-03-17;收到修改稿时间:2015-05-07

1　无线网络的安全对CR网络的影响

ISO 于 1989 年制定出了 OSI 安全体系结构标准 ISO7498-2, 所定义的安全系统是一个多层次的安全体系结构. OSI 安全体系结构模型中定义了五组安全服务: 认证服务、保密服务、数据完整性服务、访问控制服务、抗抵赖服务. 通过认证和加密、防火墙及入侵检测系统技术建立网络安全的三道防线. 认知无线电网络[1]本质上还是一种无线网络. 当前对无线网络的攻击方式主要分成两类: 被动攻击(监听网络上传递的信息流, 破坏信息的保密性来实现的)和主动攻击(中断、篡改、伪造). 威胁主要表现在[2]: 非法授权访问、冒充合法用户、破坏数据完整性、干扰系统正常运行、利用网络传播病毒、线路侦听等. 传统的安全威胁, 主要集中于对协议缺陷的攻击和数据的获取, 短时间内破坏网络的运行效率. 其解决的主旨在于, 提高协议的安全性, 保证数据加密体制, 快速检测攻击行为, 提供早期的预警等. 传统网络的安全问题和解决方案仍是未来认知无线电安全的基础, 其传统安全特性中的保密性、完整性、可用性、不可否认性、可控性仍是认知无线电安全的主要追求目标[3,4].

2　认知无线电协议栈安全

认知无线电的独特工作结构, 如图 1 所示, 有别于传统网络工作原理, 认知无线电网络不仅仅依赖于协议栈, 其认知无线电引擎、无线电政策引擎和软件无线电组件也处于认知无线电网络的关键位置, 各个模块相互交织合作完成任务. 因此认知无线电网络的频谱开放性, 认知行为的灵活性使其面临独特的安全问题. 由于频谱处于网络的较低层, 影响协议栈每个层次的性能, 因此认知无线电的安全主要在物理层和 MAC 层展开; 针对认知行为带来的安全问题也处于初级阶段, 自主管理和自律行为将为认知无线电网络带来一些新的安全挑战; 同时不同的无线电政策法规也回带来新的不容忽视的安全问题. 由于政策法规的不确定性, 及认知无线电的政策引擎设计到更为广泛的政治、经济环境, 因此对它的安全性研究更为复杂和多变[5], 由于其混合了非技术因素, 不再讨论范围内. 下文主要从协议栈和认知行为的角度探讨认知无线电的安全问题.

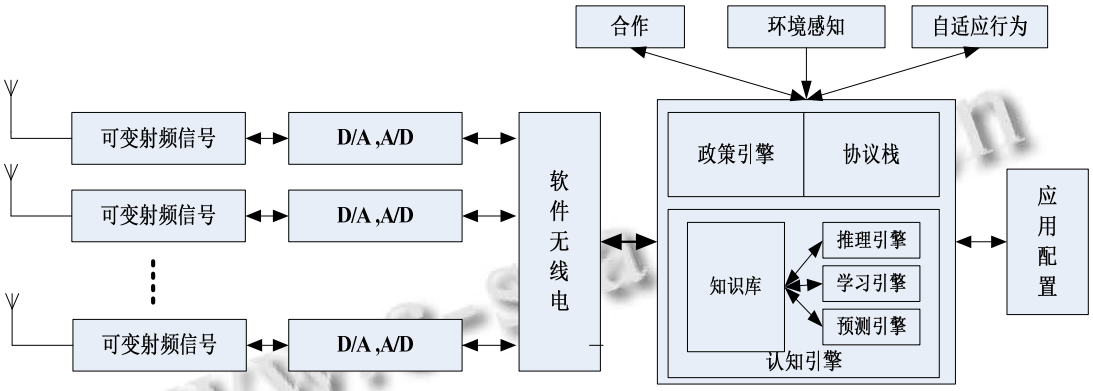

图 1　认知无线电工作结构

2.1 基于协议栈角度的安全分析

层次的协议栈设计虽然使得设计简单, 下层对上层透明, 但是过度的屏蔽物理层的特性, 使得认知无线电上层难于控制网络资源, 尤其当频谱处于开放状态下, 频谱环境的变化可能直接的影响更高层的协议, 这一点在频谱切换造成的延迟上尤为明显, 拥塞控制和可靠传输都会与固定频谱策略的网络不同. 由于频谱选择处于物理层, 是协议栈的最底层, 因此频谱选择是认知无线电安全协议设计的核心. 各层的主要安全攻击如图 2 所示.

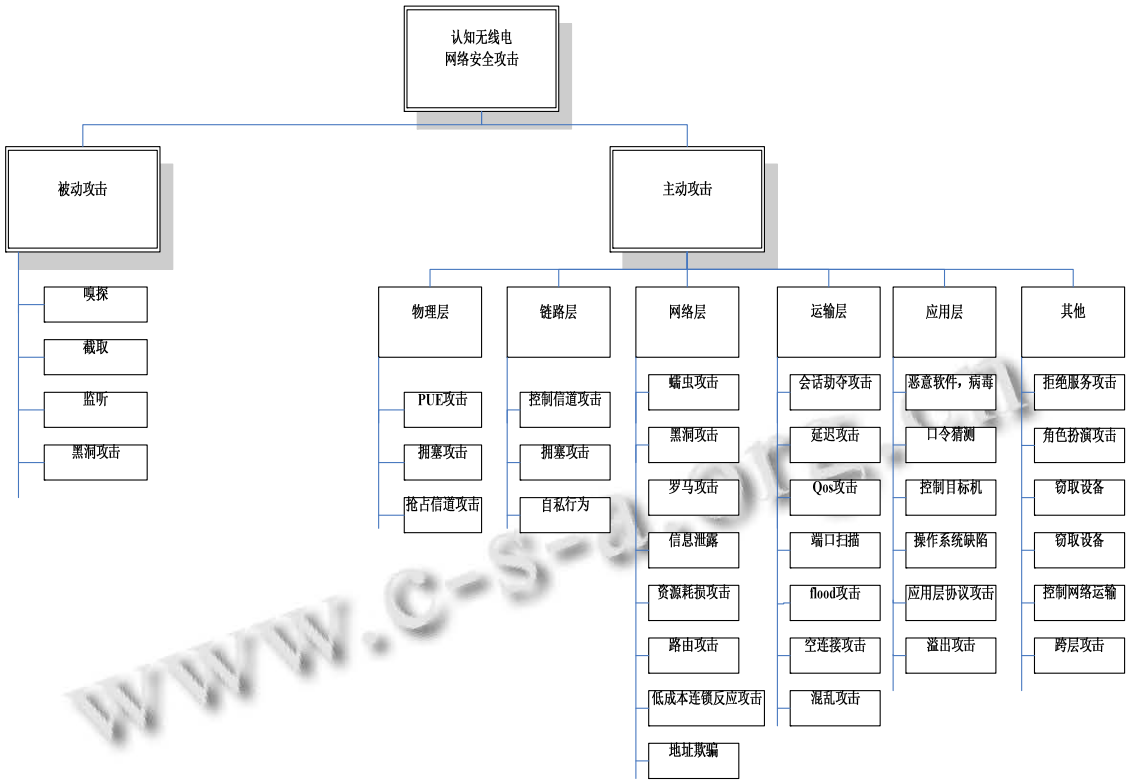

图 2 认知无线电典型攻击种类

2.1.1 物理层

认知无线电网络中物理层有能力在大多数频带上以各种频率进行传送，同时一个频谱转换到其它频谱时，转换过程会造成延迟. ①模仿主用户攻击(PUE, primary user emulation)是认知无线电独有的一种安全问题，对物理层特有的功能之一频谱感知造成极大威胁[6]. 攻击者模仿主用户信号特征发送 CR 信号，从攻击目的和手段来看，PUE 攻击可分为自私攻击和恶意攻击. 自私攻击主要是通过检测空闲频谱，模仿主用户特征信号，阻止其它认知用户竞争此频段，进而使其拥有的资源最大化，或者通过欺骗隐瞒机制不公平的占有频谱资源. 恶意攻击不一定是为个人的通信目的而获取空闲频谱，而是很可能在同一时间在多个频段上阻止机会频谱共享(Opportunity Spectrum share, OSS)， 这种攻击通过使用两个机会频谱共享机制来完成，通过在多频段以迂回循环方式发动 PUE 攻击，攻击者能够实现有效限制合法认知用户识别和使用空闲频谱；②拒绝服务攻击是物理层面临的另一种安全问题，它通过在相应信道的频带上发送干扰信号来达到攻击目的[7,8].

2.1.2 链路层

认知无线电链路层也存在严重的安全问题. ①自私行为节点的自私行为包括两种：一种自私行为为丢弃数据包，在网络中较为普遍. 另一种为自私信道协商，用户执行自私错误行为是为了在最大信道利用率和减小能量损耗方面获得不公平的优势[9]. 自私用户可能在设法提高自身性能的同时降低网络整体性能，例如吞吐量，端到端延迟等，恶化了网络性能和网络公平性. ②公开信道攻击，在传输数据前，节点使用分布式频谱感知方式确定空闲频带并将确定的空闲频带通过公共控制信道协商信道. 在多跳 CR 网络中，为了实现分布式频谱感知和信道分配，认知用户间需要相互交换本地频谱感知和信道分配信息. 对于大多数已有的 CR 网络 MAC 协议[10,11]，公共控制信道在节点交换本地信息时起到关键作用，然而最近研究表明公共信道非常容易遭到拒绝服务攻击. ③拒绝服务攻击，由于分布式 CR 网络中 MAC 协议有以下弱点：缺少 MAC 层认证、控制信道的饱和问题、可预测的控制信道忙碌序列. 同时现有的链路协议的缺点也造成了上述安全问题，因此对链路层发动 DOS 攻击将严重影响网络可用性.

2.1.3 路由层

路由层的安全问题主要集中于自组织认知无线电网络, 认知无线电不仅具有 Ad Hoc 网络的一些安全威胁,也具一些特有的安全问题. ①一般无线路由攻击: 路由安全问题表现为当路径具有恶意节点, 通过广播错误的路由信息给它的相邻节点, 或者使数据包复位向到错误方向, 使得路由中断. Ad Hoc 网络中已经发现了几种路由攻击, 分为两类: 路由中断攻击和资源消耗攻击, 表现形式为利用频谱接入的机会发动黑洞攻击[12], 灰洞攻击[13], 蠕虫洞攻击[14,15]. 目前主要使用密码机制保证路由信息的完整性和节点身份的真实性, 该方法也被认知无线电网络路由层采用解决安全问题. ②寄生虫攻击[16], 分为内部寄生虫攻击和信道外部寄生虫攻击, 前者通过内部节点获取高优先权信道, 同时并不把该信道通知给它的相邻节点, 而包含该节点的其它路由无法使用该链路, 导致高负载信道的隐藏使用, 后者是通过将它的所有接口切换到正在被使用的高优先权链路信道上; ③低成本连锁反应攻击[16], 恶意节点选择正常的负载信道而不是高负载信道, 同时将频谱分配的错误信息被发送给所有的相邻节点, 影响到路由树结构的稳定, 这种攻击具有更大的危害性和隐藏性, 同时这种信道错误分配也影响到路由树结构的稳定; ④跨层攻击: 一个层上的恶意操作会引起另外一个层的安全危害, 如 Jellyfish 攻击[17], 在网络层发起 Jellyfish 攻击, 传输层受到攻击影响. 通过三种攻击: 混乱, 丢弃和延迟变化使得运输层出现重传、吞吐量降低、定时器失效, 出现拥塞. 另外攻击者通过频繁的频谱切换, 引起网络层和传输层相当大的延迟[18], 吞吐量剧烈降低, 而且这种攻击网络层难于检测, 却使运输层出现拒绝服务攻击.

2.2 基于认知行为的安全分析

认知无线电有别于传统通信被动适应环境, 能够主动感知周围环境变化, 动态的调整行为模式, 为用户提供了一种灵活、可感知、可配置的智能通信方式, 如图 3 所示. 将智能学和认知学结合到无线电通信中. 认知用户不仅通过感知过程动态的调整通信方式, 同时保存通信中获取的知识, 以便于通信场景的分析, 主动应对多变的环境. 在认知行为中通过感知数据, 经过内在推理、学习、预测和外在感知、合作等环节建立的知识库, 是认知无线电引擎的核心, 应对知识库的攻击也是其主要安全问题.

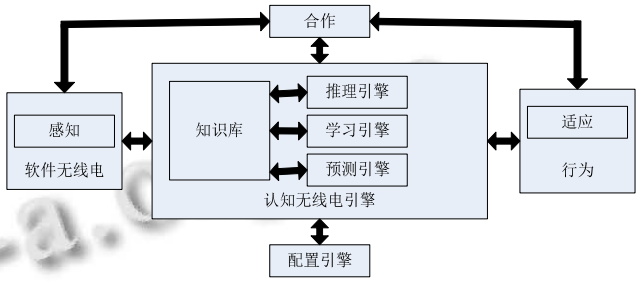

图 3 认知无线电引擎

认知无线电网络与被动适应环境的通信网络不同, 网络工作模式可以组织成一个认知环[19], 具有七种行为模式和一种特殊属性(感知、适应、推理、学习、计算、预测、合作、可配置), 将智能学和认知学结合到无线电通信中, 能够主动感知周围环境变化, 动态的调整行为模式, 在无可信第三方支持的情况和保证不泄露频谱私有信息的前提下提供可信的频谱计算方式, 为用户提供了一种灵活可配置的通信方式, 如图 3 所示. 认知引擎产生随之对应的安全问题. 通过认知行为的攻击, 具有区别一般网络通信安全问题: (1)潜在攻击的深远影响力和持久性质; (2)通过简单的频谱操纵, 就可以严重影响网络性能和行为; (3)攻击更具有潜伏性质; (4)攻击者需要更高的技术门槛, 不仅包括协议栈, 而且需要了解认知无线电引擎中的整体架构和各种算法设计, 如表 1 所示. 使用智能推理的方式: 分层结构虽然简化了设计, 但是认知无线网络中多种参数的变化间接影响到上层协议的运行.

表 1 认知行为下的攻击

行为	功能	攻击对象	恶意行为	解决方法	门槛
感知	获取频谱信息和环境参数	伪造环境, 欺骗用户	创造一个虚假的环境	提高频谱识别能力,提高灵敏性, 区别噪音和攻击	受害者具有感知行为和有能力创造理想的外部环境
适应	根据环境调整行为	改变认知行为模式	创造一个虚假的环境	提高可控制性	必须了解内部管理适应功能的方法/算法和目标
计算	计算频谱数据	窥探用户信息	泄露频谱信息	可信计算	支持公开加密解密算法

推理	推出特殊性结论	影响认知用户的行为功能	创造一个虚假的环境	在决策过程引入允许偏差机制	需要精确布置攻击策略和理想的行为. 需要了解推理算法和需要了解不断变化的目标.
学习	通过经验获取知识,改进认知行为	长期影响认知用户的行为	创造一个虚假的环境	在决策过程引入允许偏差机制，在学习中进行反馈	攻击必须是长期的，攻击过程中需要积累一定的知识，需要了解学习算法，有能力进行长期的欺骗.
预测	根据适应、学习、推理的知识预测将来的情况	错误的预测能够产生长期影响	创造一个虚假的环境	严格控制感知过程	能建立长期的欺骗环境，能够保持长期的攻击，需要知道预测模式.
合作	认知用户分享信息,共同完成任务	通过网络进行攻击	多个网络节点创造一个虚假的环境	保护外部环境免于攻击	建立邻居之间的欺骗环境，有能力观察邻居的行为模式，建立评估效益，做出合适的攻击.
可配置性	动态适应用户需求和环境需求，具有可编程性，可移植性	阻碍配置需求，提供虚假配置请求，混乱无线电政策	创造一个虚假的环境或者提供给用户虚假配置	保护外部环境免于攻击，提供多种渠道提供配置	需要了解配置环境和配置方案，以及传送方式.

3 解决方案

认知无线电网络除了使用现有的无线网络安全协议和安全方法，还从以下两个方面保证网络的安全性.

从协议栈角度解决安全问题的方法: ①从物理角度上，提高频谱感知技术，准确区分主用户信号和认知用户信号，现有的基于能量检测[20,21]、特征旋转检测[22]、滤波器匹配等都不足以识别主用户信号，设计新的诸如电波指纹技术、或者利用多种技术结合，如位置和能量检测相互结合，可以有效识别主用户. 为防止恶意用户，构建准确的频谱态势图，利用物理坐标检测攻击行为[23]; ②从密钥学角度上，在MAC层加入认证方案，如通过认证控制帧可能阻止生成伪造控制帧并且帮助查找发送错误控制帧的节点. 设计可信任第三方，在分布式认知无线电网络中节点间地位平等，管理较为困难，虽可通过多节点合作，或使用簇结构建立可信任的第三方，然而这些技术仍是不充分的，并且增加网络负载，攻击者利用频谱切换的延时伪造身份，进行中间人攻击，以及如何在分布式认知无线电网络中提高密钥协商的效率，因此研究将身份和频谱进行绑定[24]和多种路径下的密钥协商机制[25,26]. 提高加密技术，包括使用加密原语和发展模拟加密原语，前者是指大部分链路层攻击为恶意用户伪装成主用户，因此无论集中式还是分布式环境中，主用户身份认证都是很重要的，基于数字签名的主用户认证机制,使认知用户从主用户中识别恶意用户; 后者为现有大部分密码协议作用于数字域，将它们用于模拟信号是不可能的. 因此需研究模拟信号的密码协议，支持在模拟信号中进行加密和认证. ③从协议设计上，需要进一步研究用于检测认知网络中恶意行为的反应式安全机制. 例如有的机制能够检测非正常的较高的频谱切换，这种机制有助于防止干扰和频谱切换攻击; 结合信誉机制的检测能够使认知用户识别并阻止网络中的恶意用户. 跨层技术设计，虽然提高频谱感知技术改善频谱移动性和延迟，但这是不够的，跨层技术通过将频谱信息与高层协议的状态信息进行共享，虽然这种方法增加了层间的依赖，但使得整个通信协议对频谱是可知的，能更好防止对网络上层协议的攻击. 健壮安全模型，包括协议和协议栈整体安全模型的设计，前者提供可靠合作式协议，并且进一步研究健壮模型. 后者是基于现有协议栈不能很好的适用于认知无线电网络，从而设计比现有协议栈更为安全的架构，使用更为可靠的安全模型提供分布式计算的容错能力，提高网络的可靠性. 使用低开销的安全协议和原语: 认知用户的移动设备具有有限的处理功率和资源，提供融合认知能力和密钥管理的安全保护将会是一个挑战.

从人工智能角度解决网络安全问题的方法: ①智能推理，分层虽然简化了设计，但是认知无线网络中多种参数的变化间接影响到上层协议的运行，使用认知逻辑的推理帮助设计和分析安全协议. 如由Burrows等人设计的BAN逻辑被广泛应用于安全协议的推理分析[27]. ②机器学习，现有安全问题主要针对各层的安全设计，没有从整体上进行设计，然而整体的设计势必影响效率的执行. 因此在出现安全隐患的

早期, 利用较少的数据进行防御. Barreno 等人利用机器学习提出了针对安全的解决方案[28]. ③从社会学, 生物学角度研究认知无线电的通讯特征, 社会行为和人的行为、心里活动将会对无线电的使用产生影响, 将人类社会的安全模型, 如小世界理论应用于认知无线电网络. 人体的组织器官对于认知网络的协议栈设计具有启发意. ④构建自治、自主和自律性的认知引擎, 将频谱资源的管理扩展到其它网络资源, 从认知无线电网络延展到认知网络, 需要进一步研究认知引擎的架构[29].

从资源分配的角度解决网络安全问题的方法: ①为阻止 MAC 层自私能行为, 主要通过提高检测机制, 如 Kyasanur 提出接收方在 CTS 和 ACK 帧中向发送方分配并发送退出值, 然后用这些值检测错误行为. 一种更为可行的技术是使用经济学的方法来防止自私行为, 如 Cagalj 等在链路层应用博弈论研究自私行为[30], 和基于统计理论针对特定攻击的检测. ②提高频谱感知、分析和切换进程的速度, 并对高层协议透明, 将频谱移动性信息与高层协议的状态信息进行合并. ③合作竞争, 利用频谱感知结果进行分布式信道协商, 竞争节点间的合作保证了信道分配公平性. 在多跳网络中进行节点间合作并不容易. 在分布式信道协商方案中, 自私节点能轻易向其它节点隐藏可用数据信道, 并且为了留给自己使用, 它拒绝转发上一个节点发送来的数据包. 同时需要注意的是当自私节点在网络中不用位置危害也不相同, 自私节点放在网络周围对网络公平性影响很小. ④在无可信第三方支持的情况和保证不泄露频谱私有信息的前提下提供可信的频谱计算方式[31,32],但是可信计算的协议计算开销限制了认知无线电网络的应用场景. ⑤配置额外辅助设备, 例如通过 GPS 获取地理位置、通过基站或者传感器网络增强识别主用户的能力, 提供统一的频谱服务数据库对频谱资源分配进行统一管理, 通过 PKI 提供频谱的准入机会[33].

4 总结

本文从两个方面讨论了认知无线电网络特有的安全问题. 首先从协议栈角度论述了频谱开放性给协议栈带来的不同安全问题. 然后, 从认知行为的角度, 研究了利用认知行为的可能攻击方式机其影响, 这种攻击不但具有持久性和隐藏性, 带来的破坏性也比传统攻击方式严重, 攻击的技术门槛也较高. 通过这些攻击揭示了认知无线电网络潜在的基本思想还没有被实现: 提供弹性服务和通过认知把入侵者排除在网络之外的有自我意识的自主、自治和自律性网络还需要进一步的研究. 认知无线电是下一代网络发展的关键技术, 能否使得认知无线电网络大规模使用关键在于它的安全问题. 因此深入研究认知无线电安全关技术, 对安全问题提出合理、有效的解决方案, 增强了网络的安全性和强壮性, 为未来认知无线电的普及作充分的准备.

参考文献

1 Prasad R, Mohr W, Konhauser W. Third generation mob1e communication system: London, Boston: Artech House, 2000.

2 周贤伟,辛晓瑜,王丽娜,薛楠.认知无线电安全关键技术研究.电信科学,2008, 2:72–77.

3 Mitola J, Maquire GJ. Cognitive radios: making software radios more personal. IEEE Personal Communications, 1999, 6 (4): 13 – 18.

4 Haykin S. Cognitive radio: brain–empowered wireless communications. IEEE JSAC, 2005,23 (2):201–220.

5 Clancy TC, Goergen N. Security in cognitive radio networks: threats and mitigation. Cognitive Radio Oriented Wireless Networks and Communications, 2008. CrownCom 2008. 3rd International Conference on, Singapore, 15-17 May 2008: 1–8.

6 周贤伟,王义江,王丽娜.认知无线电物理层安全研究.电讯技术,2008,48(6):1–5.

7 徐谖钦,徐以涛,罗康,王阵,马云峰.认知无线电频谱感知安全的威胁与防御,军事通信技术,2014,35(2):26–31.

8 Ruiliang C, Jung-Min P, Reed JH. Defense against primary user emulation attacks in cognitive radio networks. IEEE Journal on Selected Areas in Communications, 2008, 26(1): 25–37.

9 Kyasanur P, Vaidya DN. Selfish MAC layer misbehavior in wireless networks. IEEE Trans. on Mobile Computing, 2005, 4(5):502–516.

10 Ma LP, Han XF, Shen CC. Dynamic open spectrum sharing MAC protocol for wireless ad hoc networks. Proc. DySPAN, 2005:203– 213.

11 Pawelczak P, Prasad RV, Liang X, Niemegeers IGMM.

Cognitive radio emergency networks - requirements and design. Proc. DySPAN, 2005: 601– 606.

12 Jakobsson M, Wetzel S, Yener B. Stealth attacks on ad hoc wireless networks. Proc. of the VTC. 2003.

13 Aad I, Hubaux JP, Knightly EW. Denial of service resilience in ad hoc networks. Proc. of the 10th Annual International Conference on Mobile Computing and Networking (MobiCom'04). 2004: 202–217.

14 Hu YC, Perrig A, Johnson DB. Ariadne: a secure on-demand routing protocol for ad hoc networks. MOBICOM, 2002: 12–23.

15 Awerbuch B, Holmer D, Nita-Rotaru C, Rubens H. An on-demand secure routing protocol resilient to byzantine failures. ACM Workshop on Wireless Security (WiSe), September, 2002.

16 Haq A, Naveed A, Kanhere SS. Securing channel assignment in multi-radio multi-channel wireless mesh networks. Wireless Communications and Networking Conference, 2007. WCNC 2007. IEEE, March 2007: 3111–3116.

17 Aad I, Hubaux JP, Edward WK. Denial of service resilience in ad hoc networks. Proc. of the 10th Annual International Conference on Mobile Computing and Networking. New York, USA, 2004: 202–215.

18 薛楠,周贤伟,林琳,周健.基于最短时延的认知无线电网络安全路由算法.计算机科学,2010,37(1):68–71.

19 裴庆祺,李红宁,赵弘洋,李男,闵莹.认知无线电网络安全综述.通信学报,2013,34(1):144–156.

20 Mangold S, Zhun Z, Challapali K, Chou CT. Spectrum agile radio: Detecting spectrum opportunities. 6th Annual International Symposium on Advanced Radio Technologies. GLOBECOM apos, 6(29), March 2004: 3467–3471.

21 Federal Communications Commission. Unlicensed operation in the TV broadcast bands and additional spectrum for unlicensed devices below 900 MHz in the 3GHz band. USA, Federal Communications Commission, May 2004.

22 Cabric DMSM, Brodersen RW. Implementation issues in spectrum sensing for cognitive radios. Conference Record of the Thirty- Eighth Asilomar Conference on Signals, Systems and Computers 2004. Beijing: Elsevier B.V, 15(3), Sept 2008: 1–7.

23 李方伟,刘帆,朱江,聂益芳.认知网络中一种基于频谱安全态势感知的路由方案.电讯技术,2014,54(9):1292–1297.

24 周健,周贤伟,孙丽艳.基于自认证的认知无线电密钥交换协议研究.计算机科学,2010, 37(6): 94–96.

25 孙丽艳,周健.基于认知无线电的容迟网络非交互密钥协商.计算机应用,2010,30(9):2404–2408.

26 周健,周贤伟,孙丽艳.大规模认知无线电网络多方密钥交换协议.计算机应用研究,2010,27(2):730–732.

27 Burrows M, Abadi M, Needham R. A logic of authentication. ACM Trans. on Computer Systems (TOCS). New York NY USA, Feb 1990,8(1):18–36.

28 Marco B, Blaine N, Russell S, Anthony D. Can Machine Learning Be Secure. Proce. of the 10th Annual International Conference on Mobile Computing and Networking. Philadelphia PA USA, March 2004, 202–215.

29 王慧强,徐俊波,冯光升,王振东,陈晓明.认知网络体系结构研究新进展.计算机科学,2011,38(8):9–24.

30 Cagalj M, Ganeriwal S, Aad I, Hubaux JP. On selfish behavior in CSMA/CA networks. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Switzerland: Proc. IEEE,4, March 2005: 2513 – 2524.

31 孙丽艳,张海,周健.非诚实环境下认知无线电共享信道安全协商.计算机系统应用,2012,21(3):67–71.

32 孙丽艳,周健.一种 Ad Hoc 认知无线电安全频谱管理方案.计算机系统应用,2011,20(3):60–63.

33 于雍,雷凤宇,秦玉化,张沙沙.一种适用于多跳认知无线电网络的高效 IBE 方案.计算机科学,2013,40(2):71–77.