Research on security issues of cognitive radio networks

Li Zhu, Huaqing Mao

Department of information science& technology, Oujiang College, Wenzhou University , Wenzhou, China, 325027

yeah_1397118@hotmail.com, mr.maohuaqing@yahoo.com

Abstract: Cognitive radio (CR), cognitive radio networks (CRN) lead to rapid development of communications industry, and bring the great convenience to people's lives, however, security becomes the key concern issue. CRN is built on the existing network infrastructure; and the future CRN will also face the security problems that exist in current wireless network. In addition, spectrum can be dynamically programmed and used in CRN, so, security of spectrum becomes the key issue that will restrict development of CRN. Therefore, spectrum access security of CRN and authentication of core network have extraordinary significance. In this paper, security issues of CRN are analyzed in detailed and the latest research is discussed clearly, finally, future development trend for CRN security mechanisms is given.

Keywords: cognitive radio networks; security of spectrum; authentication

认知无线网络安全问题研究

朱　丽，毛华庆

温州大学瓯江学院信息系，温州，中国，325027

yeah_1397118@hotmail.com,mr.maohuaqing@yahoo.com,

摘　要：认知无线电、认知无线网络技术促进了通信产业的快速发展，为人们的生活带来了极大的便利，但通信安全始终是值得关注的重点。认知无线网络构建于现有无线网络基础上，因此现有无线网络面临的安全问题在未来认知无线网络中同样会面临。此外，认知无线网络中频谱能够动态规划和使用，因此，频谱安全在未来将成为制约认知无线网络发展的一个关键因素。研究未来认知无线网络的频谱接入安全以及核心网络的身份认证安全具有重要的研究意义。本文对未来认知无线网络面临的安全问题进行了详细的分析，介绍了最新的研究成果，并在此基础上探讨了认知无线网络安全机制的未来发展方向。

关键字：认知无线网络；频谱安全；身份认证

1 引言

基于认知无线电构建的认知无线网络是未来网络的发展趋势，它能够融合现有的各种无线网络，包括GSM/WCDMA/WLAN 等。在网络接入层，由于其基于认知无线电技术构建，因此能够利用各种空白频段，提高频谱利用效率；在核心网络层，能够兼容现有的各种标准，降低了系统的部署成本，提高了传输速率。目前已经得到了广泛的关注与研究。认知无线网络的发展与成熟将极大的推进无线通信技术的发展。但同时，也面临着更大的困难与挑战，网络安全便是其中一个需要重点解决的问题。认知无线网络除了传统网络所面临的安全入侵问题，还具有许多其特有的安全隐患，主要包括以下几个方面：

- 认知无线网络中由于任意节点都能够使用其周围的空白频段，因此工作于现有授权频段下的主用户面临被监听的风险，同时面临攻击节点在工作频段上的干扰问题。
- 认知无线网络能够融合现有的各种无线网络，但现有的网络安全机制并不完全相同。

978-1-935068-18-1

GSM/WCDMA 等安全机制及身份认证极其严密，但 WLAN 等安全等级较低，因此可能因为某种网络标准的安全缺陷带来全网的安全隐患。

- 认知无线网络中任意节点都可以根据其周围环境自适应的改变其传输参数，与现有网络中节点只能工作于单一网络环境存在巨大的区别，任意节点都可以被利用作为攻击节点。如何保证所有节点的合法性以及身份鉴别是未来网络中的一个重要问题。

本文将首先描述现有无线网络所共有的安全问题，再重点对认知无线网络的安全问题展开讨论，最后对认知无线网络安全机制提出相应的解决思路和规划。

2 无线网络安全研究现状

现有无线网络的安全问题主要表现在以下几个方面：

2.1. 无线窃听

在无线通信过程中，所有的通信信息均由无线信道进行传输，攻击者只需要相应的设备即可截获传输信息。在商用无线通信系统中，传输的信息可能包括用户身份信息、计费信息、密钥信息、位置信息以及信令信息等。这些信息的泄露会给用户带来经济上、名誉上的损失，同时还可能会泄露用户隐私。针对无线窃听，目前解决办法是对传输信息进行加密，视传输信息的重要性采用不同强度的加密。采用该方法能够对传输信息进行有效的保护。但随着计算机硬件技术的快速发展，采用单一密钥加密传输存在被暴力破解的可能。因此需要提高加密算法强度、对密钥采取及时更新等措施来防范风险。

2.2. 假冒攻击

在无线通信中，基站与终端之间的身份信息交换均需要通过无线信道来进行，这些身份信息关系到网络控制以及网络服务、网络接入等。而由于无线信道存在窃听的可能，攻击者可能通过窃听无线信道来获得身份信息，当攻击者获得一个合法用户的身份后，就可以利用该身份信息假冒合法用户欺骗基站，从而接入网络，获得网络服务或从事网络攻击。在不同的无线通信系统中，假冒攻击的目的各异。通过截获身份信息假冒合法用户使用通信服务，逃避网络服务费，利用截获身份欺骗基站设备，甚至可以假冒基站设备欺骗终端用户，获得更多用户身份信息。

2.3. 信息篡改

信息篡改是指攻击者窃听到相关信息并进行修改后再传递给原本信息的接收者，包括对信息的删除、替换、修改等。信息篡改多发生在“存储-转发”型网络中，而在无线通信中，两个无线终端之间的信息也可能通过其他无线终端或者网络中心进行转发，这些“中转站”就可能篡改转发信息。信息篡改会严重威胁网络通信的完整性以及有效性，给用户造成不必要的损失。

2.4. 服务抵赖

服务抵赖是指用户在使用通信后，对通信服务或者通信过程中传输的数据进行否认。包括两方面内容：1）通信服务的抵赖。在商用网络中，用户否认曾使用网络，从而拒绝支付相关网络费用。2）通信内容的抵赖。用户对自己发起的传输内容进行否认。比如在电子商务或电子支付中，用户否认曾发生的交易而拒绝支付。服务抵赖影响到网络的信誉，同时会给运营商以及商家造成不必要的损失。现阶段主要采取身份认证的方式以及使用非对称加密算法来避免此类安全隐患。

2.5. 重放攻击

重放攻击是指攻击者将窃听到的有效信息经过一段时间间隔后再传送给接收者。其目的是利用有效信息在时间改变的情况下取得接收者的信任，达到获取更多有用信息的目的，比如获得用户口令，从而控制网络授权以及网络资源的访问等。

2.6. 拒绝服务与信息干扰

无线通信的载体为电磁波，随着硬件技术的快速发展，攻击者可以通过大功率的发射器来阻碍正常通信，即通过在工作频谱上制造噪音来淹没正常通信信号，从而达到干扰通信，造成基站设备无线资源不够用，达到拒绝用户接入的目的。信息干扰会产生严重的社会影响。

3 认知无线网络新的安全问题

认知无线网络的特点表现在两个方面：物理层的频谱移动性以及网络层的融合性。正是由于这两个特点给认知无线网络带来了一些新的安全问题。

3.1 认知无线网络的安全问题

认知无线网络属于无线网络范畴，因此也存在无线网络所固有的安全问题：窃听、篡改、抵赖、干扰等。

同时也存在新的安全问题。概括来讲包括以下两个大的方面：

1. 物理层频谱不确定性导致的安全问题。由于认知无线网络终端及基站设备可以工作于任何未被使用的空白频段，因此，存在两个方面的安全隐患：1） 现有的无认知功能的终端若身份被泄露，可以被攻击者利用，攻击者通过一直占用该频段进行发送，干扰认知终端的正常频谱检测以及通信使用。2 具有认知功能的终端若身份被泄露，可以被攻击者利用，通过强行占用主用户的频段，干扰主用户的正常使用，同时使得其他用户无空白频段使用，造成频段不足的问题。

2. 网络融合造成的安全问题。现有的无线通信标准其安全策略并不兼容。对于无线局域网、个人局域网等非商用无线网络，通过身份认证即可接入。而对于 GSM、WCDMA、CDMA2000 等商用网络，具有严格的终端认证以及用户身份认证，并且将终端认证与用户身份认证区分开来。通过基站端的严格认证来控制终端的合法性，通过 SIM 卡认证来对用户身份、用户接入进行控制。在未来网络中，需要将这些安全标准不同的无线网络融合在一起，因此网络的安全将成为一个隐患。

3.1.1 频谱安全问题

频谱安全问题主要表现在以下几方面：

频谱感知和频谱共享

频谱感知和频谱共享上的攻击最明显的表现为 DoS 攻击。在参考文献[1]中，Jakimoski 等介绍了在动态频谱管理策略中，无法为主用户以及认知用户提供必要的最小带宽的情况下，针对有中心节点和分布式的认知无线网络展开了讨论。在有中心节点的网络中，通过频谱池技术来检测空闲频段并将其分配给认知用户。攻击者通常能够欺骗认知用户使用非空闲的频段，从而干扰主用户的正常通信。

不管针对有中心节点的网络抑或是分布式网络，由于用户数的增多，攻击会产生极其严重的后果，研究者针对这些潜在的攻击行为提出了对应的防范策略：

- 改变调制方法：通过扩频技术比如跳频或者 DSSS 方法，使得攻击者难以开展有效的 DoS 攻击[2]。
- 阻止攻击者使用主动的方式获得主用户的位置信息以及传输信号。
- 使用授权和信任模型。在文献[3]中，wang 等给出了一种基于过去检测报告的信任模型。通过对用户过去检测报告的评估，来推断该用户当前检测报告的可信度，将可信度高的用户报告赋予较高的权重因子，从而避免了潜在的攻击。

频谱移动性

频谱移动性是指用户从一个信道移动到另外一个信道时候，能够无缝进行通信。通常情况，频谱移动性发生在用户从一个地方移动到另外一个地方，或者用户当前频段因为主用户的出现导致不可用的情况。为了维持通信过程，用户需要选择新的可用频段，并迅速转到可用频段上，频段接力过程从用户让出当前频段到新频段上连接建立为止[3]。

失败的频率切换会导致需要较长的恢复时间，并且能导致上层协议的失效。导致频率切换失败的情况有以下几种：

- 攻击者通过模拟主用户的出现，让认知用户退出当前频段。具体做法就是攻击者在频谱感知时隙内发送与主用户类似的干扰信号，从而迷惑认知用户。为了抵抗这类攻击，认知用户可以通过在多个信道上的随机跳动来解决[4]。这种认知用户和攻击者之间的影响称为频谱混战，主要是由于追求动态频谱以及逃避攻击造成的。在文献[5]中，Li 通过数据仿真，给出了多个阶段的攻击过程给认知用户造成的影响，通过仿真可以发现：当可用的频段数增加或者固定的频段减小时，认知用户的性能会得到很大的提高。
- 攻击者欺骗网络需要更多的时间来选择可用的新频段，或者报告网络无法建立新的连接，这样导致其他的认知用户需要消耗更多的能量以及代价来满足网络的平衡性。
- 如果攻击者获得了公共控制信道的控制权，则它能够通过改变关键量来影响合法用户，比如改变可用的信道数，或者干扰主用户。这种攻击能够阻止认知用户的合法频率切换。解决这种潜在攻击的方式是通过增设安全子层来保证控制信道的安全，包括使用 3A 手段来控制公共信道的接入。

频谱管理

认知用户通过频谱感知来检测空闲频段，并使用频谱管理单元来选择最好的频段分配给用户使用，以满足用户的 QoS 需求。在文献[4]中，频谱管理单元对感知到的频谱进行分析、分类并决定频谱如何分配。频谱分析对每个频段的传输特征进行分析，然后根据用户的 QoS 需求选择最合适的频段分配给用户。频谱感知数据的伪

978-1-935068-18-1 © 2010 SciRes.

造攻击是频谱管理中的一个最严重的安全隐患，它能够造成频谱分析过程产生偏差，并且导致频谱决策不正确，从而造成网络整体性能的下降。在这种攻击中，攻击者通过发送错误的频谱感知结果给频谱管理单元，从而造成频谱管理决策的错误。

这类攻击将会给系统和基站造成极其严重的影响。比如在 IEEE802.22 中，攻击者可以通过模拟一个 TV 信号的出现，当基站收到这个信号后，会给所有的认知终端下发指令，使得认知终端快速避让该频段[7]。在文献[8]中，Frangoudis 等给出了一种可信机制的频谱感知和汇报方法，来避免这类攻击者的出现。他们通过设置有效的过滤机制和投票机制来保证有用信号能够从多个观测结果中过滤出来，而对于错误的观测结果则予以舍弃。结果证明，该方法能够很容易的检测出异常的频谱测量结果，但该文献没有考虑到隐藏节点带来的影响。

MAC 层频谱共享

在认知无线电中，需要在 MAC 层设立频谱共享的方式，让多个用户共享频谱空洞，现有的解决方式包括随机的和按规则的。由于认知用户的终端设备是移动的，并且具有优先的资源和计算能力，因此，提供安全的服务成为挑战。MAC 层的频谱共享主要包括攻击者的恶意接入、隐藏信息等。这些潜在的威胁导致了上层协议以及应用的脆弱性。

3.1.2 网络融合安全问题

在认知无线网络中，网络融合造成的安全问题主要是由于网络结构不同造成的。在未来的认知无线网络中，有两种典型的网络结构：中心型网络和对等型网络。中心型网络指存在中心节点，而对等型网络则没有中心节点，所有用户处于平等状态。在中心型网络中，认知节点通过认知基站或者现有基站设备接入现有网络，认知基站与现有核心网络设备可以通过有线连接的方式进行连接。认知基站负责协调所有认知终端，认知终端通过合作或者非合作的方式进行频谱感知。在对等型网络中，认知节点与现有节点组成 MESH 网络，由现有节点或者终端节点对相关信息进行路由。未来认知无线网络需要解决中心型网络和对等型网络的融合问题，由于这两种结构采用的安全策略不同，简单宽泛的融合会造成安全策略不一致，从而导致安全隐患的出现。

3.1.3 接入安全

认知无线网络除了具有上述特有的频谱安全问题之外，还面临有现有网络接入的安全问题。当核心网络具备重配置能力后，现有终端的接入由于安全机制的不一致可能会导致接入被拒绝，或者由于终端的多次尝试接入导致基站拒绝服务。攻击者可以利用现有的终端设备，攻击网络。

3.1.4 传输安全

现有无线网络中，对于核心网络的安全建立在核心网络独立的情况，若攻击者尝试从核心网络发起攻击，可能会取得某些机密信息，造成网络危害。未来网络由于兼容现有的无线标准，虽然对于核心网络中传输信息进行了加密，但由于需要与现有网络标准保持兼容，可能会导致核心网络出现安全隐患。因此，保障核心网络的安全非常重要。

3.1.5 学习引擎

认知用户建立在对环境的感知之上，因此需要采用人工智能技术来进行决策。攻击者可以通过提供错误信息给学习引擎最终影响其决策结果。对于多数学习引擎而言，其决策结果多依赖于历史以及当前的信息。如果攻击者具有相当的耐心，则可通过提供错误结果来影响历史判断。此类攻击一旦发生，则恢复时间会更长。因为学习引擎需要更长的时间来更新其决策方法。

对于此种潜在危险，目前仍没有有效的解决方法。文献[1]给出了一种尝试方法，通过设立更严格的接收信息标准以及降低每个节点的可信时间，来给攻击者的潜伏增加难度。

3.2 认知无线网络安全对策研究现状

对于认知无线网络的安全机制，现有的研究主要从 802.16 PKMv2 延伸而来。802.16 的安全机制对解决未来认知网络的安全具有较好的参考作用。

在未来网络体系中，不仅有商用通信网络，包括 GSM/WCDMA，也会有无线局域网（WLAN）和无线城域网（WiMAX）等，这些无线通信标准面向的服务对象不一样，因此对身份认证以及安全认证的要求等级也不完全一样。无线局域网对于身份认证的要求较为简单，基于 WEP 的加密即可，而 GSM 的身份认证较为复杂，采用 SIM 认证的方式。未来网络需要融合这两种无线标准，则需要将不同的身份认证方法都包括进来。此外，对于数据传输的安全性，在 Internet 上也有不同的要求，因此其安全认证的方法也非唯一。

从国内外的研究现状来看，主要包括以下几个方面：

3.2.1 关于安全机制方面的研究

802.16 中的安全机制主要采用的是 EAP 机制[9]。文献[11]重点介绍了 WiMAX 中的安全机制，重点对密钥管理协议进行了详细分析，介绍了 MS 和 BS 之间的 RSA 认证、EAP 认证以及 RSA+EAP，EAP+EAP 的双认证、SA-TEK 三次握手过程和 TEK 的交换过程。指出了存在的安全风险及相应的解决方法。此外，文献[9]也对这些机制进行了探讨和分析。

国际上对 802.16 机制的研究主要侧重于身份认证部分，并且现有的 PKMv2 也存在一些缺点，如何克服这些缺点，是研究的一个热点[9]。文献[11] 针对现有 802.16 的身份认证缺点进行了阐述，并提出了相对应的解决方案。

文献[12, 13]指出了 802.11（WLAN）中的安全问题，针对无线局域网中的媒体控制访问层机制的不足、Ethernet MAC 层地址访问列表的缺点、公共共享密钥流等方面的问题进行了详细的论述。文章指出 WLAN 目前的安全体系结构是不够安全的，不能对用户的隐私、网络访问控制等提供有效的安全保障。并提出了改进的方法：针对 AP（Access Point）需要从 MAC 层进行加密，并且需要对整体的安全体系进行强化。

3.2.2 密钥产生方法以及密钥分发管理的研究

密钥产生和管理是整个安全体系的基石。现有的较高强度的加密算法主要有 RSA 和 ECC，其中后者由于其计算简便性得到了越来越广泛的关注，ECC 在非对称加密方法中起到了越来越重要的作用，是目前研究的热点与趋势。文献[16]给定了一个改进的椭圆曲线参数选取算法，同时也提出了一个椭圆曲线安全基点的选取算法，还提出了一个基于椭圆曲线密码的分布式密钥生成协议 ECC-DKG（Elliptic Curve Cryptography Distributed Key Generation Protocol）。此外，文献[14, 15]也对 ECC 算法进行了详细的分析与探讨。

对于对称加密算法，主要采用的是 DES 算法。文献[6]给出了 DES 加密算法的基本原理以及加密步骤，从理论上说明了 DES 算法的严密性。同时文献[17]对 DES 算法的改进也做了大量的工作。改进后的 DES 算法能适合计算能力有限的移动终端进行处理。

文献[18]对 WiMAX 中密钥管理协议，包括密钥管理的发展情况，密钥管理协议中使用的消息及消息参数进行了分析和总结，同时详细分析了 PKMv2 版本中包括密钥体系、认证方式下的密钥交换过程、对密钥的管理和使用方法，针对密钥管理协议版本中仍然存在的安全漏洞，给出了可行的解决方案。

3.2.3 身份认证机制的研究

文献[19]给出了一种 3A 认证（Authentication, Authorization, Accounting）的框架，AAA 服务器端提供一组接口，应用程序通过调用接口函数来实现认证。其目的是要建立一种统一的符合 3A 认证的安全认证体系结构。

身份认证机制是网络通信的一个重点，文献[20]阐述了现今常采用的三种身份认证机制：基于 DCE/Kerberos 的认证机制、基于公共密钥的认证机制和基于挑战/应答的认证机制。并对其安全性进行了分析和阐述，为设计网络安全系统时采用何种认证机制提供了详细的参考依据。

认知无线网络由于其特点，面临与现有网络的不同问题。文献[21]针对认知无线网络中存在的模仿主用户攻击和自私行为攻击问题，提出了一种基于簇的分布式认知无线电网络安全体系结构。这种安全体系结构通过采用数据加密和认证等安全技术解决无线网络中原有的安全问题，通过在主用户基站和认知用户间使用 Hash 匹配技术可解决模仿主用户攻击问题，通过簇头向目的节点发送转发节点的可用频谱信息可解决自私行为攻击问题。文献[22]给出了一种基于 EAP-SIM 身份认证机制的设计方案，分析了当前用户接入网络所经历的 4 个步骤（Identity，Start，Challenge，Success），并在 WANC（Wireless Access Network Control 网络接入控制器）上实现了相关认证功能用于支持 EAP-SIM 认证机制，使其充当 RADIUS 客户端的角色，通过 RADIUS 协议与存放有用户认证信息的 AAA 服务器交换数据。文献[10]给出了一种 EAP-CRP 方法来支持认知无线网络中终端节点的重认证，为高速切换提供了一个参考解决思路。通过仿真结果，证明该方法比其他基于 AAA 的认证方法更适合在切换过程中使用。文献[23]重点介绍了基于认知无线网络的扩展安全协议问题，提出了一种 EAP-CRP 方法来支持基于 EAP 的安全传输，同时使用用户位置信息来确保在重新分配密钥过程中确认用户信息，该文献还给出了一种基于移动用户位置记录信息的认证和加密密钥产生方法，在 EAP 密钥管理系统中，所有密钥随着用户位置的更新而更新，确保了密钥的安全性。

4 认知无线网络安全对策发展方向

针对认知无线网络的安全问题，本文认为未来认知

978-1-935068-18-1 © 2010 SciRes.

无线网络的安全问题应该从以下几个方面来进行探讨：

- 针对物理层安全，应该有一种新的物理层安全子层，负责频谱的感知、管理及监测的安全。从而解决物理层频谱可能存在的安全隐患，消除隐终端、恶意终端等造成的威胁。
- 针对接入安全，可以通过身份认证体系，对用户和终端进行分开认证与授权。通过给终端配备唯一识别号码，来保证接入终端的合法性；对于用户认证，通过 EAP-SIM 认证的方式，保证用户身份的安全，同时对用户所能使用的服务与权限进行授权。
- 针对传输网络安全：采用严密的安全体系来对网络传输进行保障。其安全体系结构能够兼容现有的各种无线网络以及未来可能出现的网络标准。

References (参考文献)

[1] Jakimoski G., Subbalakshmi K. P., Denial-of-service attacks on dynamic spectrum access networks, IEEE International Conference on Communications Workshops 2008, pp.524～528.

[2] DoC N., Manual of Regulations and Procedures for Federal Radio Frequency Management. In NTIA.

[3] Wang W., Li H., Sun Y., et al., Attack-proof collaborative spectrum sensing in cognitive radio networks, IEEE 43rd Annual Conference on Information Sciences and Systems 2009.

[4] Akyildiz I. F., Lee W. Y., Vuran M. C., et al., NeXt generation/dynamic spectrum access/cognitive radio wireless networks: a survey, Computer Networks, 2006, 50(13), pp.2127～2159.

[5] Chen R., Park J. M., Reed J. H., Defense against primary user emulation attacks in cognitive radio networks, IEEE Journal on Selected Areas in Communications, 2008, 26(1), pp. 25～37.

[6] Hammond P. H., Conference report of DES 84, Computer-Aided Engineering Journal, 1984, 1(6), pp. 206～207.

[7] Clancy T. C., Goergen N., Security in cognitive radio networks: threats and mitigation, 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications, 2008, pp.1～8.

[8] Frangoudis P. A., Arkoulis S., Marias G. F., et al., Incentives and Security Considerations in Distributed Spectrum Sensing, Proc. 1st Euro-NF Socioeconomics Workshop, Athens, Greece, 2008.

[9] Shon T., Choi W., An analysis of mobile WiMAX security: vulnerabilities and solutions, Network-Based Information Systems, pp. 88～97.

[10] Nomura R., Evaluation of EAP based Re-authentication Protocol for High-speed Vehicular Handover in Cognitive Radio Networks.

[11] ZHAO Yue-hua， Security Mechanism Analysis of PKMv2 in IEEE802.16e, Communication technology, 2009, pp. 177～179.

[12] William A., Arbaugh N. S., Your 802.11 Wireless Network has No Clothes, IEEE Wireless Communications, 2002, 9(6), pp. 44～54.

[13] Park J. S., Dicoi D., WLAN security: current and future, IEEE Internet Computing, 2003, 7(5), pp. 60～65.

[14] Seroussi G., Elliptic curve cryptography, Information Theory and Networking Workshop, 1999.

[15] Cheng Song, Yanfei Liu, Introduction of Elliptic curve cryptography, Shanxi Electronic Technology, 2007, (2), pp.23-27.

[16] Xiaoying Wang, research distributed Key generation protocols and application on Elliptic Curve Cryptography, West China University University, dissertation, 2007.

[17] Qiaoxia Chang, Tieliang Cheng, Analysis and research on S-box of DES Encryption algorithm, Fujian Computer, 2009, (9), pp.12-15.

[18] Hailing Wang, WiMAX security research, Beijing University of Posts and Telecommunications, Dissertation, 2007.

[19] de Laat C, et al., RFC2903:Generic AAA Architecture, RFC Editor United States, 2000.

[20] LI Jin-ku， ZHANG De-yun， ZHANG Yong, Research of User Authentication Mechanism and Its Security Analysis, Application research of computers, 2001, 18(2), pp.87-91.

[21] Xue Nan, Cluster-based Security Architecture for Distributed Cognitive Radio Networks, Telecommunications Science，2008，24(11), pp. 52-56.

[22] Fang Wang，Research on Security Architecture and Authentication Methods for Wireless Metropolitan Area Network，Journal of Jiangsu University of Science and Technology 2007, 21(5), pp.24-27.

[23] Nomura R., Evaluation of EAP based Re-authentication Protocol for High-speed Vehicular Handover in Cognitive Radio Networks.