认知无线电网络安全路由问题研究

林 琳,周贤伟,薛 楠,刘臻臻
(北京科技大学 信息工程学院 通信工程系,北京 100083)

摘 要:认知无线电是一种智能频谱共享技术,可显著提高频谱的利用率。根据认知无线电在国内外的研究现状以及该技术的应用发展趋势,给出了认知无线电网络中安全路由的一个研究体系。该体系以一种混合式的网络结构为基础,将身份认证,密钥分配,组播树的创建,对当前空闲频谱信息进行合理定价,递减式组播模式以及跨层设计路由等问题结合在一起,形成了一个较为完备的认知无线电网络安全路由问题体系,为未来认知无线电安全路由的研究开拓了一条新路。

关键词:认知无线电;安全路由;递减式组播;定价;跨层设计
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2010)01-0159-04

Study on Problems of Security Routing in Cognitive Radio Networks

LIN Lin, ZHOU Xian-wei, XUE Nan, LIU Zhen-zhen
(Department of Communication Engineering, School of Information Engineering, Beijing University of Science and Technology, Beijing 100083, China)

Abstract: Cognitive radio is a smart spectrum sharing technology which can effectively improve the utilization of radio resources. In this paper, proposes a research framework of security routing in cognitive radio networks according to the research status and the development trend of cognitive radio. Based on a composite network configuration, combine some interesting problems to form a relatively complete framework of security routing in cognitive radio networks, the problems includes identity authentication, key management, multicast tree and reasonable pricing of idle spectrum information, decreasing multicast model and cross-layer routing design. The framework exploits a new way of study on security routing in cognitive radio networks in the future.

Key words: cognitive radio; security routing; decreasing multicast; pricing; cross-layer design

0 引 言

无线通信的迅猛发展逐渐暴露了频谱分配体制的缺点,人们在采用先进的无线通信理论和技术来提高频谱利用率的同时,却发现全球授权频段的频谱利用率极低。如果在不影响首要用户的前提下,采用频谱共享技术,可以极大地缓解目前频谱资源紧张造成的压力。自从1999年美国的Joseph Mitola提出了认知无线电(CR,cognitive radio[1,2])的概念之后,国内外就开始了对认知无线电的研究。

在对认知无线电近十年的研究中,人们的研究重点先是集中在认知无线电的频谱感知特性上,之后是将频谱感知和频谱接入进行跨层设计。近年来,有一些研究人员把研究兴趣转到路由的跨层设计上,但是他们的研究只是针对路由设计算法[3~8],研究的前提条件中有很多难以实现的假设。究其原因在于,相对于其它的无线网络,认知无线电网络更强调整体性,因此,即使是为了设计一个路由算法,也要从网络本身的构成开始,从应用角度出发,将路由设计的前提条件整合清楚,这样得到的不是单独的某个研究点,而是一个具有应用前景的问题体系。文中就是基于以上的指导思想,结合现有的网络环境,设计了一个较为完备的认知无线电网络安全路由问题体系,为未来对认知无线电网络安全路由的研究提供了参考。

收稿日期:2009-05-07;**修回日期**:2009-08-02
基金项目:国家863计划(2009AA01Z209);国家自然科学基金(60773074)
作者简介:林 琳(1983-),女,博士研究生,研究方向为自组织网络组播路由、认知无线电网络以及微分博弈理论;周贤伟,教授,研究领域为自组织网络、移动通信、宽带通信网与安全技术、认知无线电和通信中的调度理论。

1 认知无线电网络安全路由研究

2004年成立的IEEE802.22工作组提出了以认知无线电为核心技术的无线区域网[9],标志着对于集中式认知无线电网络架构及其通信和安全协议的研究有了很好的依据。但对于分布式的研究,由于各标准组织尚未制定标准,研究大部分是基于一定的假设,比如

为了研究的方便，一般假定认知用户之间有一个预先设定的公共控制信道。另外，认知无线电的频谱感知技术尚不成熟，对于空闲频谱的获取在理论上，尤其是实际应用上还有待研究。在这种情况下，为了达到让认知用户使用空闲授权频段来提高频谱利用率的最初的目的，结合我国现存的网络架构，提出一种混合式的认知无线电网络架构。所谓混合式，是指将主用户基站作为认知无线电网络的一部分，向认知用户有偿提供空闲频谱信息，只要在认知用户加入网络时对其进行身份认证，认知无线电网络中一切通信过程不仅不会影响到主用户网络的安全性，而且由于认知用户通过主用户基站及时掌握了空闲频谱信息以及主用户的其它特征信息，比如信号类型与天线参数等，在提高频谱利用率的同时，还提高了对主用户退避的及时性和准确度，进一步降低了对主用户的干扰。主用户基站和认知用户交易使用的控制信道是主用户基站预留的，不会因为某个主用户出现而变得不可用。同时，利用主用户基站有偿地对认知用户提供信息，不但给网络运营商增加了收益，而且可以通过定价管理和监督认知用户对授权频谱的使用。基于以上的分析，在这种混合式的认知无线电网络架构下提出了一个安全路由的问题体系，如图 1 所示。

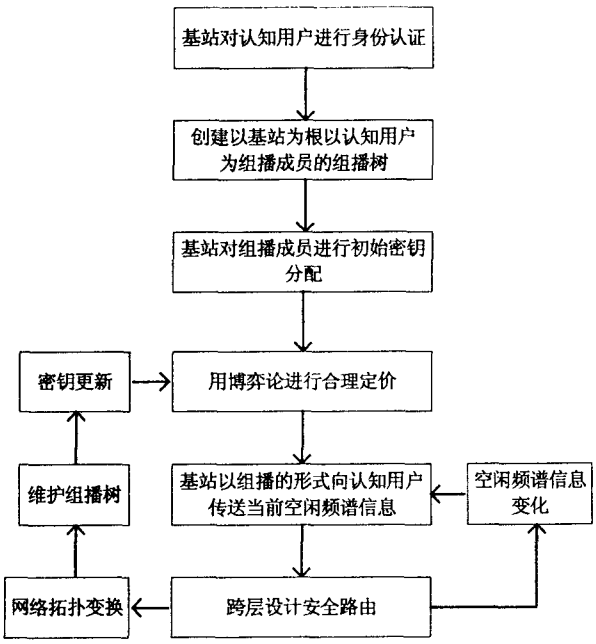

图 1 认知无线电网络安全路由问题体系

从图 1 中可以看出，问题体系中包含的研究内容有以下几个方面。

1.1 基站对认知用户进行身份认证

这里假设认知用户本身应具有可以验证的身份。在现实生活中，这个假设是可以成立的，因为每个认知用户都应该是国家已注册的单位，都有唯一的标示，基站可以通过对认知用户的标示对其进行身份认证。

1.2 创建组播树

我们的目的是利用主用户的基站向认知用户提供当前空闲频谱信息，认知无线电网络频谱资源的动态性使得空闲频谱信息动态变化，为了节省带宽资源，采用组播的形式传送空闲频谱信息，组播的转发结构是一棵有源树，树根是主用户基站，组播成员是认知用户，在分布式多跳无线网络中，由于无线传输的广播特性，最小化带宽消耗的组播树并不总是 Steiner 树，而是要最小化数据传输的次数，也即具有最少承担转发节点任务的树[10,11]。这个问题用数学语言描述就是：在一个给定的网络 G 中，有源节点 s，目的节点集 D，求一棵以 s 为根的有向树 T，使得 $D \subseteq V(T)$ 且 $|\{v \in V(T) \setminus \{s\} | d(v) \geqslant 2\}|$ 最小。通过将其特殊情况转化为一个已知的 NP－完备问题——连通控制集问题，可证明它的 NP－完备性，未来要设计这个问题的近似算法或启发式算法。

1.3 初始密钥分配

主用户基站对各认知用户分配的密钥采用非对称密钥，有两方面的作用：一是为了传送空闲频谱信息的保密性，也便于主用户基站向不同的认知用户传送不同的空闲频谱信息；二是为了在设计路由协议时，增强通信过程中的信息安全性。

1.4 合理定价

在我们设计的体系结构中，主用户基站有偿地向认知用户提供空闲频谱信息是我们的主导思想。毫无疑问，基站如何合理定价需要用博弈理论来研究，但与已有定价模型[12~15]的不同之处在于：其一，由于主用户分布的区域不同，主用户基站出售给不同认知用户的空闲频谱信息也可能不同；其二，认知用户到主用户基站有可能需要多跳才可到达；其三，认知用户和主用户基站之间承担转发任务的有可能是主用户，它是纯粹的中间商，也有可能是认知用户，它有客户和中间商两种身份。以上三条使得认知无线电网络中的定价策略比以往难度更大，但更符合实际情况。

1.5 以递减式组播模式传送信息

由于主用户基站向每个认知用户传送的空闲频谱信息不同，而为了节省带宽，采用递减式组播模式传送信息。所谓递减式组播，它与传统组播在组播转发结构上没有什么区别，只是前者在组播树中的每个节点上复制的信息是不同的，组播树上每条链路的下游转发节点所转发的信息都是其上游转发节点所转发信息的子集，这里的子集选择是通过私钥解密实现的。举一个简单的例子，设组播树如图 2 所示，s 为主用户基站，s_1, s_4, s_5, s_6, s_7 是认知用户，s_2, s_3 是主用户，s_i 的公

钥为 k_i,需要得到的信息记为 $M_i, i = 1,2,\cdots,7$。则 s 向 s_1, s_2 发送的数据内容为 $M = (k_1(M_1), k_7(M_7), k_4(M_4), k_5(M_5), k_6(M_6))$,$s_1$ 收到后用私钥解密得到 M_1,并将解密得到的$(k_5(M_5), k_6(M_6))$传送给 s_3,s_4, s_4 解密得到 M_4, s_3 将$(k_5(M_5), k_6(M_6))$ 传送给 s_7, s_7 解密得到 M_7。同理,s_5, s_6 分别得到 M_5 和 M_6。从上面的例子可以看出,递减式组播保留了传统组播模式节省带宽的特性,加之在组播树中传送的信息是逐步减少的,进一步节省了带宽资源。由于各认知用户分布区域内主用户情况不同,认知用户想得到的信息也不同,况且除了自己需要的信息以及需要给自己下游节点转发的信息之外,别的信息对自己是没有用的,递减式组播刚好能满足各认知用户的需要又不浪费资源,非常适用于认知无线电网络。

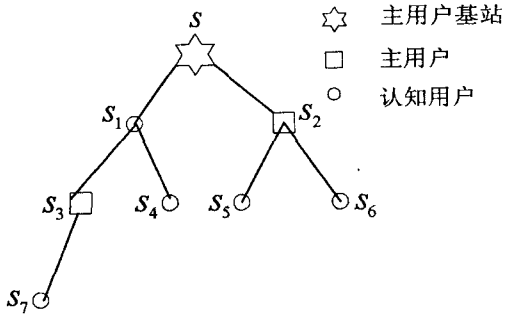

图 2　组播树

1.6　跨层设计安全路由

由于认知无线电网络中可用频谱的动态性,路由的跨层设计是一个热门的研究方向,也是一个研究难点,到目前为止,还未有评价认知无线电网络路由的标准。现有的文献主要是从以下两个方面来研究路由策略的:一是假设知道全局的频谱分布信息,采用集中式来进行路由选择和信道分配;二是采用按需路由,在需要发送数据时才寻找路由和频谱分配。前者的假设在分布式网络中很不容易实现,后者虽然不需要全局的频谱信息,但由于认知用户的感知能力有限,不能及时得到准确的可用频谱信息,很有可能造成频谱的频繁切换以及时延过长等后果,甚至会干扰主用户。文中所设计的认知无线电网络安全路由体系通过一种混合式的网络结构,以及频谱信息定价方式,使得每个认知用户通过主用户基站准确地知道自己的可用频谱资源,以及其它一些主用户特征信息,这样在路由选择和信道分配过程中,不需要知道全局的信息,也避免了频谱的不必要切换和对主用户的干扰,可以实现多维的干扰回避跨层设计来优化路由。

总结以上的分析,在文中的研究体系下来跨层设计路由有以下优势:

(1)路由的成功率较高。在可用频谱动态变化的多跳网络中,路由成功的首要条件是源和目的节点之间的中间节点有可用的信道,而这些依赖于节点是否掌握了准确的可用频谱信息,如果靠节点自己感知,少数节点的错误信息就会导致路由失败。如果是从主用户基站那里买准确的信息,路由的成功率会高很多。

(2)保证信息安全性。由于主用户基站已经给各认知用户分发了非对称密钥,采用一些加密算法可以保证通信过程中的信息安全。

(3)避免模仿主用户攻击。所谓主用户攻击是认知无线电网络特有的一种攻击形式,是指一些恶意节点模仿主用户的信号类型以及特征,达到使认知用户退避的目的。在我们的研究体系中,由于认知用户是从主用户基站得到的准确的空闲频谱信息,按照这样的信息选择信道,只会对真正的主用户退避,而置那些假冒的主用户于不顾。

(4)便于对自私节点进行监督和惩罚。所谓自私节点,就是在频谱接入时只顾自己的接入方便而不按照竞争规则接入的节点,以及在分组转发过程中不积极为其它节点转发分组的节点。在我们的研究体系中,认知用户是从主用户基站得到的空闲频谱信息,如果发现自私节点,可通知主用户基站通过提高价格或中断交易来对自私节点进行惩罚。

(5)避免频谱的不必要切换。相对于认知用户自己感知得到的空闲频谱信息,从主用户基站那里得到的信息更准确,且对未来主用户的动态预测得更为可靠,这样便于认知用户选择相对空闲时间较长的信道来接入,避免了由于选择不当而产生的不必要的信道切换。

(6)有效地回避干扰。认知用户在路由过程中,可以根据主用户基站传递的有关信息相对准确地判断干扰情况,改被动退避为主动回避,在避免对主用户及其他用户产生干扰的前提下,增强了当前路由存活的概率。

2　结束语

设计了认知无线电网络安全路由的问题体系,相比现有的研究方向更具有整体性,更有应用前景。研究体系中涉及到的几个重要的问题,比如密钥管理,合理定价,组播树的创建与维护,路由的跨层设计等都是认知无线电网络中的研究重点,在文中的研究体系下进行跨层设计路由有明显的优势。时至今日,经过了对认知无线电仁者见仁、智者见智的探索和分析之后,已有的文献还缺乏对未来研究体系的展望,文中对认知无线电网络安全路由的研究提供了一个实际而有价值的参考。

参考文献:

[1] Mitola J, Maguire G Q. Cognitive radio: making software radios more personal[J]. IEEE Pers Commun, 1999, 6(4): 13 - 18.

[2] Mitola J. Cognitive radio: An integrated agent architecture for software defined radio[D]. Stockholm, Sweden: Dept. of Teleinformatics, Royal Institute of Technology(KTH), 2000.

[3] Pradeep K, Vaidya N H. Protocol design challenges for multi - hop dynamic spectrum access networks[C]//IEEE DySPAN' 05. Baltimore: [s. n.], 2005: 645 - 648.

[4] Mansoor A, Randeep B, Li Li. Joint channel assignment and routing for throughput optimization in multi - radio wireless mesh networks[C]//ACM Mobicom'05. Cologne, Germany: [s. n.], 2005: 58 - 72.

[5] So Junming, Vaidya N H. A routing protocol for utilizing multiple channels in multi - hop wireless networks with a single transceiver[R]. US: University of Illinois at Urbana - Champaign, 2004.

[6] Krishnamurthy S, Thoppian M, Venkatesan S, et al. Control channel based MAC - layer configuration, routing and situation awareness for cognitive radio networks[C]//IEEE MILCOM'05. Atlantic City, USA: [s. n.], 2005: 455 - 460.

[7] Gong Michelle X, Midkiff Scott F. Distributed channel assignment protocols: A cross - layer approach[C]//IEEE WCNC'05. New Orleans, USA: [s. n.], 2005: 2195 - 2200.

[8] Xin Chunsheng, Xie Bo, Shen Chien - Chung. A novel layered graph model for topology formation and routing in dynamic spectrum access networks[C]//IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks. Baltimore, MD, USA. Piscataway, NJ, USA: IEEE, 2005: 308 - 317.

[9] Cordeiro C, Challapali K, Birru D, et al. IEEE 802.22: the first worldwide wireless standard based on cognitive radios [C]//IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks. Baltimore, MD, USA. Piscataway, NJ, USA: IEEE, 2005: 328 - 337.

[10] Xu Chen - guang, Xu Yin - long, Wu Jun - min. On the minimization of the number of forwarding nodes for multicast in wireless ad hoc networks[C]//ICCNMC. Berlin, Germany: Springer - Verlag, 2005: 286 - 294.

[11] Ruiz P M, Gomez - SKarmeta A F. Heuristic algorithms for minimum bandwith consumption multicast routing in wireless mesh networks[C]//ADHOC - NOW. Berlin Heidelberg: Springer - Verlag, 2005: 258 - 270.

[12] Lam P K, Chiu Dah - Ming, Liu J C S. On the access pricing and network scaling issues of wireless mesh networks[J]. IEEE Transactions on Computers, 2007, 56(11): 1456 - 1469.

[13] Anderegg L, Eidenbenz S. Ad hoc - VCG: A truthful and cost - efficient routing protocol for mobile ad hoc networks with selfish agents[C]//Ninth Annual International Conference on Mobile Computing and Networking. San Diego, CA, United States: Association for Computing Machinery, 2003: 245 - 259.

[14] Zhong S, Li L E, Liu Y G, et al. On designing incentive - compatible routing and forwarding protocols in wireless ad - hoc networks - an integrated approach using game theoretical and cryptographic techniques[C]//MobiCom' 05. Cologne, Germany: Association for Computing Machinery, 2005: 117 - 131.

[15] Wang W, Li X - Y, Wang Y. Truthful multicast routing in selfish wireless networks[C]//MobiCom' 04. Philadelphia, PA, United States: Association for Computing Machinery, 2004: 245 - 259.

(上接第 154 页)

性能成为粘合 J2EE 各层开发的粘合剂。这三者的结合使得它们的性能更加优越,成为软件开发最为经典的轻量级开发架构。

参考文献:

[1] 胡峰松,熊建新. 基于 J2EE 技术的办公自动化系统研究[J]. 江西科学,2008,26(2):300 - 301.

[2] 杜 威,邹先霞,常会友. 基于 MVC 模式的 OA 系统结构设计[J]. 福建电脑,2007(1):15 - 16.

[3] 李 刚. 整合 Struts + Hibernate + Spring 应用开发详解[M]. 北京:清华大学出版社,2007.

[4] 王国辉,王 毅,伊相群. Java Web 开发技术方案宝典[M]. 北京:人民邮电出版社,2008.

[5] Hibernate Reference Documentation[EB/OL]. 2005 - 04. http://www. hibernate. org/hib - docs/v3/reference/en/html/.

[6] 田秀彦. 论 J2EE 中 Hibernate + Spring 架构及其在 OA 系统开发中的应用[J]. 科技信息,2008(1):78 - 79.

[7] 龚雪冰,何 彪. 基于 Tapestry + Spring + Hibernate 框架的 Web 应用[J]. 计算机技术与发展,2007,17(4):131 - 135.

[8] Walls C, Breidenbach R. Spring in Action[M]. [s. l.]: Manning Publications Co, 2005.

[9] Johnson R. Spring Framework reference documentation[EB/OL]. 2004. http://www. springframework. org/documentation.

[10] 刘中兵. 开发者突击:Java Web 主流框架整合开发:J2EE + Struts + Hibernate + Spring[M]. 北京:电子工业出版社,2008.

[11] 贾 昆,甘仞初,高慧颖. 数据访问对象模式在企业应用集成中的应用[J]. 计算机工程与设计,2006,27(3):373 - 375.