doi:10.11959/j.issn.1000-436x.2016253

认知 ad hoc 网络中的多信道路由安全威胁及其对策研究

冯景瑜[1,2,3]，杜续[1]，王宏刚[1,2]，黄文华[1]

（1. 西安邮电大学通信与信息工程学院，陕西 西安 710121；
2. 西安邮电大学陕西省信息通信网络及安全重点实验室，陕西 西安 710121；
3. 中国科学院信息安全国家重点实验室，北京 100093）

摘 要：在日趋紧张的频谱资源环境中，不依赖固定基础设施和固定频谱分配策略的认知 ad hoc 网络相关技术已经获得了十分迅速的发展。但是，认知 ad hoc 网络的多信道路由特点使其收益与风险并存，面临着严重的安全威胁困扰。为深入理解多信道路由安全威胁，掌握其防御对策的研究现状及发展趋势，从节点路由和多信道选择这 2 个层面细化出具体的威胁类型，归纳目前的典型防御对策，总结出保障认知 ad hoc 网络安全的首要前提是在认知节点之间建立信任关系，而信任管理正是解决多信道路由安全威胁的基础。最后，针对目前多信道路由及其防御对策研究中存在的亟待解决问题，明确了一些有待继续研究的方向。

关键词：多信道路由；认知无线电；ad hoc；信任管理; 协作频谱感知

中图分类号：TN911.23 **文献标识码**：A

Research on multi-channel routing threats and defense for cognitive ad hoc network

FENG Jing-yu[1,2,3], DU Xu[1], WANG Hong-gang[1,2], HUANG Wen-hua[1]

(1. Department of Communication Engineering, Xi'an University of Posts and Telecommunications, Xi'an 710121, China;
2. Shaanxi Key Laboratory of Information Communication Network and Security,
Xi'an University of Posts and Telecommunications, Xi'an 710121, China;
3. State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China)

Abstract: In the environment of scarce spectrum resources, cognitive ad hoc network which is independent with infrastructure and fixed spectrum allocation policy，has been also developed quickly. Due to the characteristic of multi-channel routing, cognitive ad hoc network is commonly perceived as an environment offering both opportunities and threats. To further understand the multi-channel routing threats, the current research situation and development trend, the types of threats were analyzed in terms of the node routing and the multi-channel selection, and several typical security methods were concluded. Meanwhile, the most important solution to keep the security of cognitive radio network was found to build trust relationship among cognitive users. Trust management was just the basic technology to solve the security problems of multi-channel routing. Finally, the current problems of related works and research trends in this area were discussed.

Key words: multi-channel routing, cognitive radio, ad hoc, trust management, cooperative spectrum sensing

收稿日期：2016-09-15

基金项目：国家自然科学基金资助项目（No.61301091）；中科院信息安全国家重点实验室开放课题基金资助项目（No.2015-MS-14）；陕西省工业公关计划基金资助项目（No.2014K05-09）；陕西省教育厅专项科研计划基金资助项目（No. 14JK1660）；西安邮电大学“西邮新星”团队支持计划基金资助项目

Foundation Items: The National Natural Science Foundation of China (No.61301091), The Open Foundation of State Key Laboratory of Information Security (No.2015-MS-14), The Industrial Public Relation Project of Shaanxi Province (No.2014K05-09), The Natural Science Foundation of Education Department of Shaanxi Province (No.14JK1660), The New Star Team of Xi'an University of Posts and Telecommunications

1　引言

近年来，无线通信、移动互联网技术的迅速发展，使无线自组织 ad hoc 网络技术的应用越来越广泛，已在军事战场、抗震救灾、重大活动、应急系统、商业会议和个人通信等环境中得到了广泛应用。在这些环境中，ad hoc 网络一般具有较高的节点密度，需要实时传输大量数据。然而，ad hoc 网络通常都工作在无需授权的ISM(industrial scientific medical)频段(如 2.4 GHz 频段)[1]。伴随着同样使用这些公用频段的无线通信技术(如 Wi-Fi、蓝牙等)的快速发展，ISM 频段日益拥挤。对于采用固定分配频谱资源策略的 ad hoc 网络节点来说，ad hoc 网络将很难在这些节点密度高、频谱资源使用紧张的环境中正常工作。在这种情况下，不依赖固定频谱资源分配的认知 ad hoc 网络应运而生[2]。

认知 ad hoc 网络是认知无线电技术与 ad hoc 网络的结合，通过赋予未授权用户（认知节点）频谱感知功能来寻找可用的频谱资源，并在授权用户（主用户）的可用频谱资源空闲时进行动态接入，以限制和避免冲突的发生。由于主用户的可用频谱资源存在空闲随机性的特点，认知节点在多跳路由通信过程中需要随时进行多信道切换，形成了一种基于多信道选择的认知 ad hoc 多跳通信过程[3, 4]。

认知 ad hoc 网络的出现可以说是 ad hoc 网络发展史上的一次重大技术革新，不但能够缓解 ad hoc 网络节点公用频谱资源的拥挤情况，还因为其多信道选择的特点，有效避免了通信过程中的同信道干扰。但是从安全角度来看，ad hoc 网络路由协议中的安全隐患不仅依然存在于认知 ad hoc 网络中，而且由于认知 ad hoc 网络在节点路由过程中具有多信道选择的特点，又产生了新的安全威胁。

在认知 ad hoc 网络中，协作频谱感知是实现多信道选择的关键技术基础。所谓协作频谱感知，就是融合多个认知节点的感知信息来消除单个认知节点感知的不确定性、多径衰落和“终端隐藏”问题，共同协商确定主用户空闲频谱资源的使用情况，达到最佳感知性能[5]。但是，协作频谱感知的这种特点使其收益与风险并存，恶意节点凭借伪造、注入、篡改、合谋等方式扰乱认知无线电系统对主用户可用频谱资源的空闲判断，发动频谱感知数据伪造(SSDF, spectrum sensing data falsification)攻击[6]。一旦输入的感知数据是错误的，认知无线电系统就难以如实按照外界环境进行动态频谱切换，认知节点的多信道选择过程就会被恶意节点操控利用。因此，SSDF 攻击的有效防御是确保可靠多信道选择的关键基础和核心。

国内外目前对认知 ad hoc 网络中多信道路由安全威胁的研究已经出现，涉及节点路由和多信道选择 2 个层面，信任管理机制则是设计其防御对策最有效的方案。本文在此基础上进一步归纳和细化多信道路由安全威胁的类型，从信任管理角度对典型的防御对策进行总结分析，针对当前相关研究中存在的问题，明确了一些亟待继续研究的方向。

2　多信道路由安全威胁细化

根据认知 ad hoc 网络的多信道路由特点，从节点路由和多信道选择这 2 个层面，进行威胁类型的归纳和细化。

2.1　节点路由层面的威胁类型

路由协议的作用是在网络节点中建立正确和有效的路径，并及时传递各种信息。由于在认知 ad hoc 网络中依然需要路由协议引导节点转发信息，因而有关传统 ad hoc 网络路由协议的安全隐患依然在认知 ad hoc 网络中存在，相关威胁类型如下所示[7,8]。

1) 自私行为。电池能量有限性，一些“聪明”的节点不愿意帮助其他节点转发信息。这种节点的大量存在，会严重破坏网络的路由功能。

2) 信息篡改。恶意节点在网络中随意更改路由信息、插入虚假数据、错误的路由推荐信息，将导致路由路径的误定向，甚至使整个网络瘫痪。

3) 伪装欺骗。恶意节点冒充某合法节点发出伪造的数据分组，用来非法更新路由表，导致路由表被破坏，网络信息被错误传递或者丢失。

4) 黑洞问题。恶意节点谎称自己拥有通向某一节点的最近路由，以致数据分组会不断流入该恶意节点中，形成一个信息流“黑洞”，造成大量网络数据分组的丢失，甚至使整个网络瘫痪。

5) 信息泄露。恶意节点网络向未授权的节点泄露机密信息，如位置或者关键路由信息等，使未授权节点能够获知目标路由路径上的所有节点信息，容易引来各类恶意攻击。

2.2　多信道选择层面的威胁类型

SSDF 攻击的特征是恶意节点在协作频谱感知中注入虚假感知数据，使认知无线电系统在数据融合时难以得出主用户可用空闲频谱资源的正确判

断，进而达到某些攻击意图。从协作频谱感知中恶意节点的内在攻击动机、感知数据的伪造行为特点等方面进行深入分析，并融入已有 SSDF 攻击类型，可细化出具体的 SSDF 攻击类型。

1) 静态性 SSDF 攻击。恶意节点始终提交虚假的频谱感知数据，自私地长期占用某个空闲频谱，或干扰主用户对自身频谱的使用[9]。

2) 动态性 SSDF 攻击。恶意节点执行交替式策略，轮流提交真实或虚假的感知数据，进行动态的感知数据伪造策略[9]。

3) 规避性 SSDF 攻击。由于协作频谱感知缺乏激励机制，以及对追求低系统开销的考虑，导致认知节点没有直接的动机提交感知信息[10]。

4) 合谋性 SSDF 攻击。多个恶意节点相互合作形成合谋攻击组，有组织、有预谋地发起 SSDF 攻击[11]。相比单个恶意节点发起的感知数据伪造攻击，合谋形式的攻击危害性会更大，更难以抑制，会造成更严重的安全威胁。

5) 复合性 SSDF 攻击。恶意节点在一个周期内，分阶段交替式地发起多种类型 SSDF 攻击。

3 基于信任管理的典型防御对策

信任管理源于人际关系领域，在网络方面最早由 Blaze 等[12]为了解决 Internet 服务的安全策略而提出，已在 P2P 网络[13]、ad hoc 网络[14]、无线传感器网络[15]、在线社交网络[16]、物联网[17]等开放式网络环境中得到了广泛应用，成为网络行为安全领域的一个研究热点。同时，信任管理受到广泛关注的很大原因还来自于诸如淘宝、京东、当当等在线网购和电子商务活动的急剧活跃。

由于认知 ad hoc 网络与人际关系网络具有同构性[18]，同时由于避免单点失效的考虑，认知 ad hoc 网络往往会有一种分布式的倾向。因而该领域信任管理研究偏向以证据、推荐为主，也就是以声誉为主，并且大多数主流信任管理模型都是基于声誉的。

为应对多信道路由安全的威胁，国内外目前对认知 ad hoc 网络信任管理的研究可归结为 2 个方面：节点路由和多信道选择，如图 1 所示。

3.1 节点路由层面的信任管理

节点路由层面的信任管理研究主要是目前 ad hoc 网络中关于路由协议的信任管理研究内容，主要任务是寻找信任值高的邻居节点建立可信路由。

文献[19]提出了一种称为 watchdog 的监视方法，运行于每个节点上，实施对邻居节点的不良行为监视。在这种方法中，实现信任管理的关键步骤是行为监视，借助节点之间的相互监视来得到邻居节点的直接经验资料，这也是后续推荐信息的产生基础。文献[20]提出了基于加权的声誉评价措施，加权平均来自不同推荐路径的路由推荐信息。文献[13]通过一种分布式的方法来处理 ad hoc 网络中自适应信任计算和有效声誉评估的问题。文献[21]设计出综合基于直接经验信息、间接推荐信息和 Beta 分布的声誉评估模型，同时引入信任论中熵的有关概念用于声誉评价。此外，文献[22]提出一种基于信任评估的路由协议（TDSR）以激励节点协作并参与数据转发，低转发率的节点将被信任机制排除出网络，并被屏蔽一定时间后才能复活。

随着研究的深入，节点路由层面的信任管理研究内容逐渐趋于成熟，在很大程度上增强了路由协议的安全性。

3.2 多信道选择层面的信任管理

多信道选择层面信任管理的主要任务是防御恶意节点的 SSDF 攻击，为认知节点以协作频谱感知的方式寻找空闲信道提供安全保障。

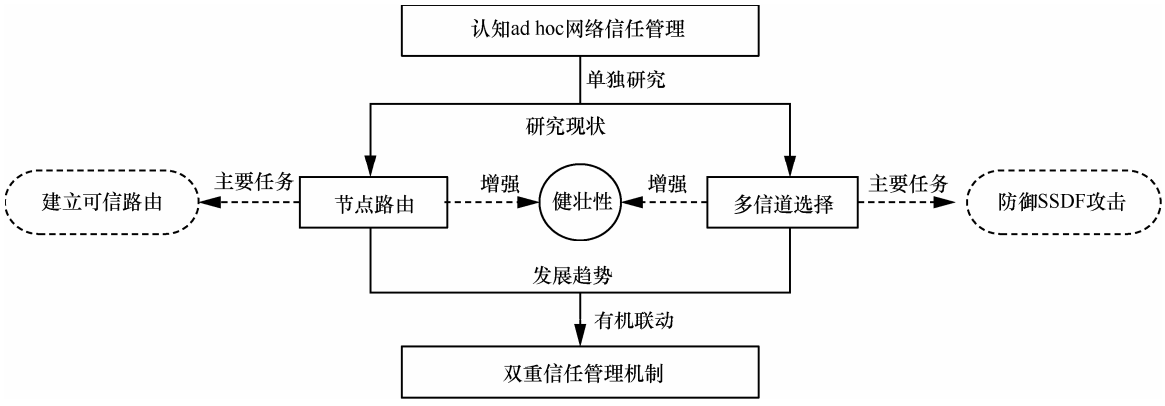

图 1 认知 ad hoc 网络信任管理的研究现状和发展趋势

对此，文献[23]使用 Beta 系统提出了一个在集中式协作频谱感知环境下的信任管理模型，解决恶意节点检测和虚假感知数据的过滤问题。文献[24]借助网络中可信节点的感知结果，在用户域和时间域这 2 个维度上消除恶意节点的影响，提出了一种基于可信节点辅助的安全协同感知模型。文献[25]将信任值作为每个认知节点的加权因子，进行加权融合及判决，并根据每个认知节点的历史行为更新其信任值。文献[26]提出一种基于社会关系度的信任管理机制，激励认知节点的感知数据贡献行为，并给出了该机制在无中心网络环境下的具体实现策略。文献[27]分析恶意节点的历史感知数据，提取出加性惩罚因子和乘性衰减因子实现对其信任值的动态衰减，从而抑制恶意节点的动态性 SSDF 攻击。文献[28]发现认知 ad hoc 网络在进行中继式协作频谱感知时，恶意用户可对转发过程中的感知数据进行篡改，其攻击成本更低于 SSDF 攻击。对此，从基于身份的密码机制和邻居监控的角度出发，提出了针对感知数据篡改攻击的抑制对策。

4　存在的问题与展望

4.1　当前存在亟待解决的问题

对当前国内外研究情况进行分析，可以看出，在认知 ad hoc 网络中基于信任管理实现对多信道路由安全威胁的防御对策设计，已得到了学术界的逐渐关注，但仍存在一些亟待解决的问题。

1) 虽然节点路由层面的信任管理研究内容已经成熟，但是其声誉式的信任管理完全依赖于推荐信息的特点，会致使信任管理自身潜伏着一些影响其应用安全性的威胁隐患。信任管理自身的安全性异常重要，安全性如果不能得到及时保障和有效增强，恶意节点就会利用信任管理的缺陷提升信任值，从而能躲避检测，并使正常节点丧失防范能力，最终会使信任管理的可靠性受到质疑。

2) 对于多信道选择方面信任管理的研究，不能局限在某 1 种或 2 种类型 SSDF 攻击的防御上，需要融合多种 SSDF 攻击类型的防御方法，来得出系统的防御体系，实现防御复合性 SSDF 攻击的功能，从而达到协作频谱感知的整体安全性提升。

3) 节点路由和多信道选择方面之间的信任管理缺乏有机的衔接性，不能使之很好地有机融合，共同解决认知 ad hoc 网络中的多信道路由安全威胁。

4) 在集中式认知无线网络中，通常会有一个中心节点管理主用户空闲频谱资源的动态使用，但是认知 ad hoc 网络的无中心特性，使空闲频谱资源难以管理，因而也会造成新的多信道路由安全威胁。此外，认知节点在路由过程中每转发一次信息都需要进行多信道选择，会极大地增加网络负载。

4.2　展望

SSDF 攻击的防御将是保障多信道路由的关键，在其防御对策的研究中，可在以下几个方面展开进一步研究。

1) 信任管理的健壮性取决于信任的有效度量，因此，要增强节点路由层信任管理的健壮性，就要从信任的度量因素分析、信任推荐信息的安全传输、错误信任推荐信息的过滤，以及信任值的有效更新和存储上进行多方面的综合研究。

2) 在多信道选择方面中引入信任管理理论，研究不同类型的 SSDF 攻击的防御对策，今后需要不断完善和优化已有 SSDF 攻击类型的防御方法，研究多维的 SSDF 攻击防御体系，使信任管理模型能有效防御复合性 SSDF 攻击。同时，积极探索和研究潜在的 SSDF 攻击类型及其防御方法。

3) 虽然在认知 ad hoc 网络的节点路由和多信道选择方面涌现了大量的有关信任管理的研究成果，但大家都从某一角度来解决问题，对于认知 ad hoc 网络中所存在的一个不可忽视的问题如“节点在其充当路由器角色时是可信的，但在其扮演认知节点角色时是否会提交真实的感知数据”还没有给出很好的解决方案。因此，必须在研究这 2 个方面信任管理的基础上，抽取出共性，注重个性，构建一个系统的双重信任管理机制，从而既可以为节点路由创建可信路由协议提供支撑，也可以为多信道选择方面融合各种类型 SSDF 攻击的防御方法提供有力帮助，从而实现 2 个方面信任管理的相互协作与有机联动。

4) 可利用信任管理在认知 ad hoc 网络中进行选举算法的研究，让网络中最可信的部分认知节点组成裁判委员会，管理主用户空闲频谱资源的动态使用。裁判委员同时负责监视路由发起节点通过协作频谱感知找出的空闲频谱是否在路由路径中一直可用。若主用户在路由过程中回归，则要求相关路由节点退出该频谱，并重新寻找新的可用空闲频谱，从而会减少路由过程中的多信道选择次数。

5 结束语

认知 ad hoc 网络中的多信道路由安全威胁已得到国内外学术界的广泛关注。本文在分析当前多信道路由安全威胁的研究进展基础上，从节点路由和多信道选择这 2 个层面进行了主要威胁类型细化，从信任管理角度归纳总结了一些典型的防御对策。最后，探讨了多信道路由安全威胁的防御对策方面值得进一步研究的方向。到目前为止，随着认知无线传感器网络、认知物联网、认知车载网等认知 ad hoc 网络类型的出现，多信道路由安全威胁及其对策的研究会逐渐变得活跃，具有潜在的研究空间。

参考文献：

[1] SHAH M A, ZHANG S. A novel multi-fold security framework for cognitive radio wireless ad-hoc networks [C]//The IEEE 18th International Conference on Automation and Computing. 2012: 1-6.

[2] AKYILDIZ I F, LEE W Y, CHOWDHURY K R. CRAHNs: cognitive radio ad hoc networks[J]. Ad Hoc Networks, 2009, 7(5): 810-836.

[3] JEON W S, HAN J A, JEONG D G. A novel MAC scheme for multichannel cognitive radio ad hoc networks[J]. IEEE Transactions on Mobile Computing, 2012, 11(6): 922-934.

[4] CACCIAPUOTIA A S, CALEFFIA M, PAURA L. Reactive routing for mobile cognitive radio ad hoc networks[J]. Ad Hoc Networks, 2012, 10(5): 803-815.

[5] AKYILDIZ I F, LO B F, BALAKRISHNAN R. Cooperative spectrum sensing in cognitive radio networks: a survey[J]. Physical Communication, 2011, 4(1): 40-62.

[6] CHEN R L, PARK J M, HOU Y T. Toward secure distributed spectrum sensing in cognitive radio networks[J]. IEEE Communications Magazine, 2008, 46(4):50-55.

[7] CARVALHO M. Security in mobile ad hoc networks[J]. IEEE Security & Privacy, 2008, 6: 72-75.

[8] 王梅, 吴蒙. MANET 中常见的路由安全威胁及相应解决方案[J]. 通信学报, 2005, 26(5):106-112.
WANG M, WU M. Dominating security threats in MANET and their corresponding solutions[J]. Journal on Communications, 2005, 26(5):106-112.

[9] RICHARD F, HUANG M Y, TANG H. Biologically inspired consensus-based spectrum sensing in mobile ad hoc networks with cognitive radios[J]. IEEE Network, 2010, 24(3): 26-30.

[10] LI S, ZHU H J, YANG B, et al. Towards a game theoretical modeling of rational collaborative spectrum sensing in cognitive radio networks[C]//The IEEE International Conference on Communication. 2012: 1-5.

[11] 冯景瑜. 协作频谱感知中的SSDF攻击及其对策研究[J]. 电信科学, 2014, 30(1): 67-72.
FENG J Y. Research on SSDF attack and defense for cooperative spectrum sensing[J]. Telecommunications Science, 2014, 30(1): 67-72.

[12] BLAZE M, FEIGENBANM J, STRAUSS M. Compliance checking in the PolicyMaker trust management system[C]//The International Conference on Financial Cryptography Springer-Verlag. 1998: 254-274.

[13] LI X Y, ZHOU F, YANG X D. Scalable feedback aggregating (SFA) overlay for large-scale P2P trust management[J]. IEEE Transactions on Parallel and Distributed Systems, 2012, 23(10): 1944-1957.

[14] BOUKERCHE A, REN Y, PAZZI R W. An adaptive computational trust model for mobile ad hoc networks[C]//2009 International Conference on Wireless Communications and Mobile Computing. 2009:191-195.

[15] GANERIWAL S, BALZANO L K, SRIVASTAVA M B. Reputation-based framework for high integrity sensor networks[J]. ACM Transactions on Sensor Networks, 2008, (4): 1-37.

[16] 乔秀全, 杨春, 李晓峰, 等. 社交网络服务中一种基于用户上下文的信任度计算方法[J]. 计算机学报, 2011, 34(12): 2406-2413.
QIAO X Q, YANG C, LI X F, et al. A trust calculating algorithm based on social networking service users' context[J]. Chinese Journal of Computers, 2011, 34(12): 2406-2413.

[17] 刘文懋, 殷丽华, 方滨兴, 等. 物联网环境下的信任机制研究[J]. 计算机学报, 2012, 35(5): 846-855.
LIU W M, YIN L H, FANG B X, et al. A hierarchical trust model for the Internet of things[J]. Chinese Journal of Computers, 2012, 35(5): 846-855.

[18] YU F R, TANG H, HUANG M, et al. Distributed cooperative spectrum sensing in mobile ad hoc networks with cognitive radios [J]. Mathematics, 2011, 24(3): 26-30.

[19] MARTI S, GIULI T J, LAI K, et al. Mitigating routing misbehavior in mobile ad hoc networks[C]//The Proceedings of the 6th Annual International Conference on Mobile Computing and Networking. 2000: 255-265.

[20] GUHA R, KUMAR R, RAGHAVAN P, et al. Propagation of trust and distrust[C]//The 13th International Conference on World Wide Web. 2004: 403-412.

[21] BUCHEGGER S, BOUDEC J Y. A robust reputation system for P2P and mobile ad hoc networks[C]//2nd Workshop on Economics of Peer-to-Peer Systems. 2004: 1-6.

[22] 许智君, 胡琪, 张玉军, 等. MANET网络激励节点协作的信任评估路由协议[J]. 通信学报, 2012, 7(9): 27-35.
XU Z J, HU Q, ZHANG Y J, et al. Trust evaluation routing protocol to enforce cooperation in mobile ad hoc networks[J]. Journal on Communications, 2012, 7(9): 27-35.

[23] QIN T, YU H, LEUNG C, et al. Towards a trust aware cognitive radio architecture[J]. ACM Sigmobile Mobile Computing and Communications Review, 2009: 13(2): 86-95.

[24] ZENG K, PAWELCZAK P, CABRIC D. Reputation-based cooperative spectrum sensing with trusted nodes assistance[J]. IEEE Communication Letters, 2010, 14(03): 226-228.

[25] 闫琦, 杨家玮, 张雯. 认知无线电网络中安全的合作频谱感知[J]. 北京邮电大学学报, 2011, 34(2): 71-75.