



协作频谱感知中的 SSDF 攻击及其对策研究 *

冯景瑜^{1,2}

(1. 西安邮电大学通信与信息工程学院 西安 710121;

2. 中国科学院大学计算机与控制学院 北京 100190)

摘要: 协作频谱感知是认知无线电中实现频谱有效利用的关键环节,但协作频谱感知由于其聚集感知数据的特点,为恶意用户提供了可乘之机。恶意用户可以通过实施频谱感知数据伪造 (spectrum sensing data falsification, SSDF) 攻击的方式,使认知无线电系统不能如实地根据外界环境进行动态的频谱切换。为深入理解 SSDF 攻击,掌握其防御对策的研究现状及发展趋势,从攻击手段、攻击形式和攻击策略 3 个角度细化出具体的 SSDF 攻击类型,总结了目前 SSDF 攻击的典型防御对策。同时,针对目前相关研究中所存在的问题,明确了一些有待继续研究的方向。

关键词: 认知无线电;协作频谱感知;无线通信;SSDF 攻击

doi: 10.3969/j.issn.1000-0801.2014.01.011

Research on SSDF Attack and Defense for Cooperative Spectrum Sensing

Feng Jingyu^{1,2}

(1. Institute of Communication Engineering, Xi'an University of Posts and Telecommunications, Xi'an 710121, China;

2. Institute of Computer and Control, University of Chinese Academy of Sciences, Beijing 100190, China)

Abstract: Cooperative spectrum sensing is the core of cognitive radio technologies to utilize spectrum resources effectively. However, cooperative spectrum sensing schemes are vulnerable to abuses by false sensing data, and thus offering opportunities for malicious users. By launching the spectrum sensing data falsification attack, some of them can make a well cognitive radio system useless. To further understand the SSDF attack and its current research situation and development trend, the types of SSDF attack were analyzed in the form of three aspects, and several typical security methods were concluded. Meanwhile, the current problems of SSDF attack and research trends in this area were discussed.

Key words: cognitive radio, cooperative spectrum sensing, wireless communication, spectrum sensing data falsification attack

1 引言

微电子、计算机通信和无线电技术的迅速发展以及物联网、移动互联网的广泛应用,不断消耗着日益紧缺的频

谱资源。认知无线电^[1]的出现,有效地缓解了频谱资源稀缺与日益增长的无线接入需求之间的矛盾,因而得到了频谱资源管理部门、标准化组织、研究机构及行业联盟的广泛关注,成为下一代无线通信发展的关键技术之一。

* 国家自然科学基金资助项目(No.61301091),中国博士后科学基金资助项目(No.2013M541013),陕西省国际科技合作重点项目(No.2013KW01-03),西安邮电大学青年教师科研基金资助项目(No.ZL2012-06)



频谱感知是认知无线电技术的首要环节,感知性能的好坏会影响到整个认知无线电系统的性能。所谓频谱感知,就是在时域、频域和空域多维空间,对分配给授权用户(也称主用户)的频谱不断进行感知,发现“频谱空洞”。认知用户可以临时使用频谱空洞,但不能对主用户形成干扰,主用户具有频谱空洞使用的优先权。由于阴影效应和多径衰落等因素的存在,单个认知用户得出的频谱感知结果往往不可靠,并可能导致所谓的“终端隐藏问题”^[2]。于是,一些研究者提出了协作频谱感知技术^[3-5],通过多个认知用户感知数据的融合来消除单个用户感知的不确定性,实现更好的频谱感知性能。

协作频谱感知的特点是多个认知用户共同协商确定频谱的使用情况,数据融合中心通过对多个认知用户感知数据的协同处理来提高频谱感知的精确性。但是,这种特点使协作频谱感知技术收益与风险并存,面临严重的安全问题。一般来说,恶意用户可以通过伪造、欺骗、泛洪和团伙合作等方式影响频谱感知过程,使数据融合中心得到错误的感知数据和指令^[6]。一旦输入的感知数据是伪造的,认知无线电系统就不能如实地根据外界环境进行动态的频谱切换,信道分配就会被攻击者控制利用。这种将伪造的感知数据发送给数据融合中心以干扰数据融合中心正常工作的攻击方式就是频谱感知数据伪造(spectrum sensing data falsification, SSDF)攻击。

防御 SSDF 攻击,确保协作频谱感知的顽健性,是认知无线电技术健康稳定发展的关键。目前,国内外对 SSDF 攻击的研究虽然还处于起步阶段,但已有不少文献分析了 SSDF 攻击的类型并提出了有关 SSDF 攻击的防御对策。本文在此基础上进一步细化归纳 SSDF 攻击类型,对目前 SSDF 攻击的典型防御对策进行总结,并针对目前相关研究中存在的问题,明确了一些有待继续研究的方向。

2 SSDF 攻击类型细化

SSDF 攻击的特征是恶意用户在协作频谱感知中伪造虚假的感知信息,使认知无线电系统得出主用户可用频谱资源的错误判断,从而达到某些恶意用户的攻击意图。通过总结已有 SSDF 攻击类型^[7-10],并对协作频谱感知的技术特点、恶意用户频谱感知数据伪造行为的内在动机进行深入分析,从攻击手段、攻击形式和攻击策略 3 个角度细化出具体的 SSDF 攻击类型,如图 1 所示,具体介绍如下。

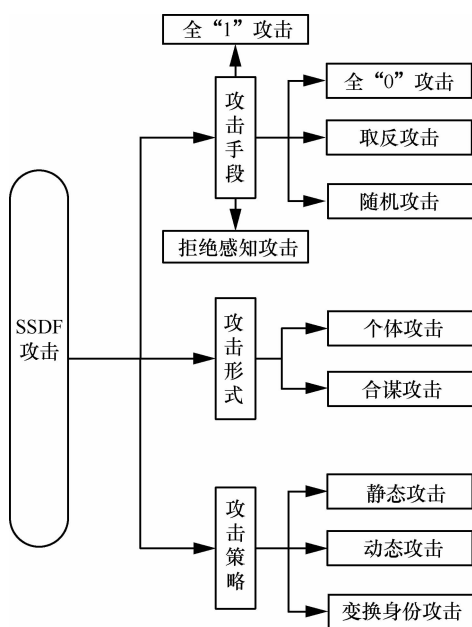


图 1 SSDF 攻击类型

(1) 攻击手段

恶意用户伪造感知数据的具体操作和手段,包括以下 5 种。

- 全“1”攻击:在协作频谱感知中,“1”表示感知数据中的主用户信号存在,“0”表示主用户信号不存在。恶意用户伪造全“1”形式的感知数据,使认知无线电系统认为主用户一直处于“繁忙”状态。
- 全“0”攻击:恶意用户伪造全“0”形式的感知数据,使认知无线电系统认为主用户一直处于“空闲”状态。
- 取反攻击:恶意用户伪造与主用户实际频谱使用状态相反的感知数据。
- 随机攻击:恶意用户不经过对主用户频谱使用状态的感知,随机伪造一个感知数据提交给数据融合中心。
- 拒绝感知攻击:恶意用户煽动参与协作感知的认知用户拒绝提交感知数据。

(2) 攻击形式

恶意用户从事 SSDF 攻击的形式和方法,包括以下两种。

- 个体攻击:单个恶意用户为了某种目的,独自实施 SSDF 攻击。
- 合谋攻击:多个恶意用户合谋形成攻击组,共同发起 SSDF 攻击。

(3) 攻击策略

恶意用户从事 SSDF 攻击的策略和方针,包括以下 3 种。

- 静态攻击:恶意用户一直提交虚假的频谱感知数据策略。
- 动态攻击:恶意用户交替式地提交真实或虚假的频谱感知数据,进行动态的频谱感知数据伪造策略。
- 变换身份攻击:恶意用户被发现后,需要一个新的身份实现漂白,从而继续从事危害行为。

可以说,攻击手段是进行 SSDF 攻击的操作方式和基本原则。全“1”攻击是一种自私性攻击,目的是使恶意用户长期占有主用户的空闲频谱;全“0”攻击是一种干扰性攻击,目的是使某些认知用户误认为主用户处于空闲状态,从而造成对主用户的干扰;取反攻击和随机攻击是混淆性攻击,目的是混淆参与协作感知的认知用户,使他们无法实现一致性。此外,出现拒绝感知攻击的原因在于,协作频谱感知的建立依赖于多个认知用户提交的感知信息,但是频谱感知缺乏激励机制,导致认知用户没有直接的动机提交感知信息。这种攻击的目的是通过减少协作频谱感知的参与用户,使数据融合中心无法得到精确的感知结果。

在其余两个角度的划分中,攻击形式是恶意用户在实施 SSDF 攻击手段过程中的内在表现形式。相比个体攻击,合谋形式的攻击危害性更大,也更难以抵制,造成的安全威胁更严重。攻击策略则是恶意用户为规避发现,提高 SSDF 攻击的成功率,在实施 SSDF 攻击手段过程中采取的策略方针。相比静态攻击,从事动态攻击策略的恶意用户具有更好的隐蔽性,更难以被发现和识别。

3 SSDF 攻击的防御对策

目前,国内外研究学者倾向于引入信任机制识别恶意用户,并确保频谱感知数据的可信性。

3.1 信任机制与协作频谱感知安全

信任机制最早由 Blaze 等人^[11]为解决网络服务安全问题而提出,并在 P2P 网络^[12]、Ad Hoc 网络^[13]、无线传感器网络^[14]、社交网络^[15]和物联网^[16]等开放式环境中得到广泛应用,如今已成为网络安全领域的一个研究热点。同时,信任机制受到广泛关注的很大原因还来自诸如 Amazon、eBay 和淘宝网等在线交易方式和电子商务活动在近年的急剧增长。这样无论从学术界还是产业界都对信任机制提出了强有力的需求,使得信任机制成为解决用户行为安全问题的一个极为重要的措施。

信任机制适用于协作频谱感知的主要原因在于:只要是涉及分布式协作的行为活动,都会存在信任问题,频谱

协作感知正是一种典型的分布式协作活动。引入信任机制后,认知用户的信任值形成于其在协作感知活动中的表现,恶意用户会因为虚假的感知数据,得到较低信任值,从而被识别加以防范,削弱其提交的频谱感知数据在数据融合过程中的影响或直接被丢弃。

信任机制在协作频谱感知中是一个新颖的研究课题,该领域的研究基于传统信任机制研究的部分成果,同时结合协作频谱感知的特点,形成了适合在协作频谱感知中应用的一系列研究成果,主要任务是防御恶意用户的 SSDF 攻击,帮助认知用户通过协作频谱感知准确寻找出可用的主用户空闲频谱资源,并避免对主用户形成干扰。协作频谱感知中的信任机制研究现状和发展趋势如图 2 所示。

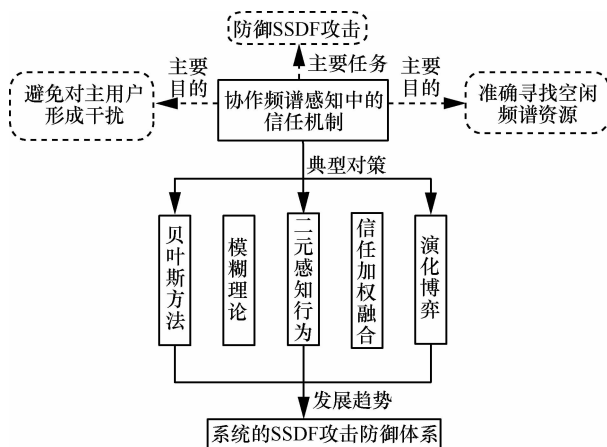


图2 协作频谱感知中的信任机制研究现状和发展趋势

3.2 基于信任机制的典型防御对策

国内外对于信任机制领域的 SSDF 攻击防御对策的研究,虽处于起步阶段,但已产生不少研究成果。对此进行总结,归纳出基于信任机制的 SSDF 攻击典型防御对策主要集中在贝叶斯方法、模糊理论、二元感知行为、信任加权融合以及演化博弈 5 个方面。

(1) 贝叶斯方法

信任就是相信对方,是一种建立在已有知识基础上的主观判断,是主体对客体能力、诚实度和可靠性的可信程度。信任不同于人们对客观事物的“相信”,而是一种主观判断,所有的信任本质上都是主观的,信任本身并不是事实或者证据,而是关于所观察到的事实的知识^[17]。通常信任的度量区间是 $[0, 1]$,任何超出这个范围的取值都要归一化^[18]。在协作频谱感知中,每个认知用户的信任值分布呈现出主观性、随机性特征,可以发现信任值的概率分布函数符合贝叶斯分布。对此,参考文献[19]通过贝叶斯方法



量化认知用户的可信程度,规避恶意用户对协作频谱感知的负面影响,根据对认知用户的历史行为分析,使用贝叶斯概率密度函数^[20]的数学期望,计算每个认知用户的信任值,并且引入遗忘因子动态衰减信任值,一旦认知用户出现不好的感知行为,遗忘因子会加速其信任值的衰减。在进行协作感知数据融合时,利用信任值权重每个认知用户的感知数据,并对权重结果与认知用户基站(SUBS)持有的感知结果进行综合考虑,从而得出更可靠的感知决策。

(2)模糊理论

信任本身就是一个模糊的概念,参考文献[21]引入模糊逻辑理论进行恶意用户过滤,以确保协作频谱感知数据融合的可信性。在模糊逻辑理论中,隶属度可以看成主体隶属于可信任集合的程度。模糊化感知数据以后,信任机制利用模糊逻辑规则对这些模糊数据进行分析,推测主体的可信任程度。依据信任的不确定性和模糊性,参考文献[21]划分出两种隶属度:模糊信任度(fuzzy trust level, FTL)和模糊怀疑度(fuzzy suspicious level, FSL)。FTL表示认知用户的可信程度,一个认知用户的FTL值越高,其所提供的感知数据就越值得信任,在协作式能量检测判决中,FTL权重每个认知用户的能量检测值,并得出最终的可靠感知决策;FSL表示对恶意用户的怀疑程度,一个恶意用户的FSL值越高,说明该用户在协作频谱感知中提交虚假感知数据越频繁。为确保协作频谱感知数据融合的可信性,需要在协作式能量检测判决中过滤掉恶意用户提供的感知数据。

(3)二元感知行为

参考文献[22]研究发现协作频谱感知中,每个认知用户的信任值度量与其以往提供感知数据的行为表现相关,过去经常提供正确的感知数据使信任值升高,错误的感知数据使信任值降低。认知用户表现出的这种二元感知行为,影响着信任值度量。因此,每个认知用户的信任值可以看成其正确感知总次数与感知总数(正确感知总次数+错误感知总次数)之比。在此基础上,参考文献[22]深入分析SSDF攻击的合谋特点,发现一种策略性的合谋攻击,在这种攻击方式下,只有当少量感兴趣的主用户出现时,合谋攻击者才实施频谱感知数据的篡改行为,以达到占用该主用户频谱的目的,并能时刻保持较好的信任值。对此,认知用户对于不同主用户的信任值度量要区别对待,以此为理论依据研究差异性信任机制,得到了这种类型SSDF攻击

的防御策略。

(4)信任加权融合

参考文献[23]提出了一种基于信任节点辅助的安全协作感知策略,该策略通过借助网络中信任节点的感知结果,形成信任加权因子,在用户域和时间域两个维度上消除恶意用户对软判决融合算法^[24]的影响,确保软判决融合算法在存在较多恶意用户的环境中仍能保持较好的感知决策性能。

参考文献[25]分析了存在SSDF攻击时协作频谱感知硬判决融合算法的性能,提出了一种基于信任加权的协作频谱感知算法。该算法首先根据每个认知用户的历史行为更新其信任值,再利用信任值为每个认知用户分配加权因子,最后进行加权硬判决融合及判决,以此衰弱恶意用户参与软判决数据融合的权重,更准确地进行数据融合,从而提高了“or”、“and”、“majority”^[26]等硬判决融合算法的安全性能。

可以看出,信任加权融合的实质就是在感知数据融合过程中,优先选取高信任值认知用户提供的感知数据,较少考虑甚至排除恶意用户的感知数据。

(5)演化博弈

参考文献[27]将协作频谱感知建模为一种演化博弈模型,主要研究自私认知用户为了最大限度地提高自己的吞吐量的协作与非协作行为,一定程度上起到抑制拒绝感知攻击的目的。在非协作频谱感知博弈中,认知用户可以选择一个行为集合{C, D},其中C代表认知用户参与协作频谱检测的行为,D代表认知用户拒绝参与协作感知的行为。一方面,认知用户可以通过消耗自身传输时间和设备电池能量,参与协作感知,从而获得一个相对稳定的吞吐量;另一方面,认知用户也可以选择参与协作频谱感知,以避免过多消耗自身传输时间和设备电池能量。如果所有认知用户都出于这种保守考虑,不参与协作频谱感知,那么就可能不会获得任何吞吐量。这是因为认知用户一旦都不参与协作频谱感知,认知无线电系统就无法判断出主用户的可用空闲频谱,也就寻找不出可供信息传递的无线信道。因此,参考文献[27]通过使用演化博弈理论的基本动态概念——“模仿者动态”,认知用户间可以相互作用和调整以决定是否参与协作频谱感知。

3.3 典型防御对策比较

根据具体的SSDF攻击类型,对所描述的典型防御对策进行比较,见表1。

表 1 典型防御对策比较

防御对策	贝叶斯方法	模糊理论	二元感知行为	信任加权融合	博弈论
全“1”攻击	是	是	是	是	否
全“0”攻击	是	是	是	是	否
取反攻击	是	是	是	是	否
随机攻击	是	是	是	是	否
拒绝感知攻击	否	否	否	否	是
个体攻击	是	是	是	是	是
合谋攻击	是	是	是	是	否
静态攻击	是	是	是	是	是
动态攻击	是	否	是	否	否
变换身份攻击	否	否	否	否	否

4 存在的问题与展望

4.1 当前存在的问题

综合国内外研究现状，基于信任机制的 SSDF 攻击防御对策研究已经受到一些关注，但仍存在一些问题，具体介绍如下。

- 在基于信任机制的 SSDF 攻击防御对策中，恶意用户进行全“1”攻击、全“0”攻击、取反攻击、随机攻击时，不论采取个体攻击还是合谋攻击，都会出现信任值的衰减，因而能达到有效抑制恶意行为的目的。然而，这些防御对策只考虑到松散的合谋攻击形式，缺少对严谨性合谋攻击形式的考虑。个体恶意用户或松散合谋用户执行的 SSDF 攻击手段所造成的威胁毕竟有限，攻击形式也相对容易识别。如果多个恶意用户合谋形成攻击组，有组织、有预谋地发起攻击，危害性更大，也更难以抵制，所造成的安全威胁要严重得多。此外，这些防御对策也没有考虑当合谋的恶意用户在协作感知中成为大多数的感知数据提供者时，该如何应对这种威胁。
- 基于信任机制的防御对策尚无法抑制恶意用户的变换身份攻击行为。虽然可以要求认知无线电系统将每个认知用户的 ID 与其手机号或 IP 地址绑定，但是恶意用户若使用新的手机号或 IP 地址重新进入系统，就能获得新的 ID，达到变换身份的目的。
- 引入演化博弈论激励认知用户提交感知信息，虽能在一定程度上有效防御拒绝感知攻击，但在协作频谱感知过程中进行博弈论建模时，所涉及的数学运算过于复杂、计算复杂度太高，对于无中心环境中

的认知用户设备是无法承受的。

- 当前针对 SSDF 攻击防御对策的研究，大多局限在对某一种或两种攻击类型的防御进行分析和解决。然而，在复杂的真实认知无线网络环境中，恶意认知用户能运用多种攻击手段对频谱协作感知技术及认知无线电系统造成威胁，片面地应对无法提升协作频谱感知技术的顽健性。

4.2 展望

在 SSDF 攻击的防御对策研究中，可在以下几个方面进一步展开研究。

- 认知无线电系统具有 3 种不同形式的实现环境：集中式、中继式和分布式^[28]。有关 SSDF 攻击防御对策的研究，目前偏向于集中式环境下的安全问题解决，缺少分布式和中继式环境下的研究。中继式和分布式环境下的认知无线电技术应用越来越广泛，在这两种应用环境中，协作频谱感知的安全保障以及 SSDF 攻击防御对策亟待拓展和深入研究。
- 由于无线传感器网络、无线 mesh 网络、移动 Ad Hoc 网络、车载网络以及物联网等无线网络对频谱资源有着极大的需求性，认知无线电技术已逐渐应用于这些无线网络。相应的，SSDF 攻击在不同类型的无线网络应用环境下可能会体现出有差异的攻击手段、策略和形式，因此有必要针对具体的无线网络应用环境，展开对应的 SSDF 攻击防御对策研究。
- 注重效率与成本的统一。协作频谱感知中的认知用户通常是一些低能量和低计算能力的便携式移动设备。在无中心环境中，由于没有中心基站可以依



赖, 认知用户自己要承担起融合感知数据和识别恶意用户的功能。因此, 在尽可能降低计算成本的前提下, 设计轻量级的 SSDF 攻击防御机制用于保障协作频谱感知的安全性。

- 需要研究一个多维的 SSDF 攻击防御体系, 以便融合多种攻击的防御对策, 实现各种类型 SSDF 攻击的相互协作与联动。

5 结束语

认知无线电中的协作频谱感知安全得到了国内外研究学者的广泛关注。在当前有关 SSDF 攻击的研究进展的基础上, 详细分析了 SSDF 攻击的主要类型, 总结了一些典型的防御对策。同时, 探讨了有关 SSDF 攻击防御对策的进一步研究方向。协作频谱感知安全以及 SSDF 攻击防御对策的研究是一个非常活跃的方向, 目前尚处于研究的起始阶段, 还具有潜在的研究空间。

参考文献

- Mitola J, Maguire G. Cognitive radio: making software radios more personal. *IEEE Personal Communications*, 1999, 6 (4)
- Ghasemi A, Sousa E S. Collaborative spectrum sensing for opportunistic access in fading environments. *Proceedings of the First IEEE Symposium on DySPAN*, Baltimore, USA, 2005
- Mishra S M, Sahai A, Broderick R W. Cooperative sensing among cognitive radios. *Proceedings of the 2006 IEEE International Conference on Communications*, Istanbul, Turkey, 2006
- Tevfik Y, Huseyin A. A survey of spectrum algorithms for cognitive radio applications. *IEEE Communications Surveys & Tutorials*, 2009, 11(1)
- Lu G Y, Wang Y X, Xie K, *et al.* Novel spectrum sensing method based on the spatial spectrum for cognitive radio systems. *Journal of Electronics (China)*, 2010, 27(5)
- 李红宁. 认知无线电安全性研究. 西安电子科技大学硕士学位论文, 2010
- Chen R, Park J M, Hou Y T. Toward secure distributed spectrum sensing in cognitive radio networks. *IEEE Communications Magazine*, 2008, 46(4)
- Chen R, Park J M. Robust distributed spectrum sensing in cognitive radio networks. *Proceedings of the 2008 IEEE INFOCOM Conference*, Phoenix, USA, 2008
- 韩勇, 陈强, 王建新. 合作频谱感知安全技术研究. *通信技术*, 2011, 6(44)
- 周贤伟, 辛晓瑜, 王丽娜等. 认知无线电安全关键技术研究. *电信科学*, 2008, 24(2)
- Blaze M, Feigenbaum J, Strauss M. Compliance checking in the policymaker trust management system. *Proceedings of the 1998 International Conference on Financial Cryptography*, Anguilla, British West Indies, 1998
- Li X Y, Zhou F, Yang X D. Scalable feedback aggregating (SFA) overlay for large-scale P2P trust management. *IEEE Transactions on Parallel and Distributed Systems*, 2012, 23(10)
- Boukerche A, Ren Y, Pazzi R. An adaptive computational trust model for mobile Ad Hoc networks. *Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing*, Leipzig, Germany, 2009
- Ganerwal S, Balzano L K, Srivastava M B. Reputation-based framework for high integrity sensor networks. *ACM Transactions on Sensor Networks*, 2008 (4)
- 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值计算方法. *计算机学报*, 2011, 34(12)
- 刘文懋, 殷丽华, 方滨兴等. 物联网环境下的信任机制研究. *计算机学报*, 2012, 35(5)
- 李小勇, 桂小林. 大规模分布式环境下动态信任模型研究. *软件学报*, 2007, 18(6)
- Sepandar D K, Mario T S, Hector G M. The EigenTrust algorithm for reputation management in P2P networks. *Proceedings of the 2003 International Conference on World Wide Web*, Budapest, Hungary, 2003
- Qin T, Yu H, Leung C, *et al.* Towards a trust aware cognitive radio architecture. *ACM SIGMOBILE Mobile Computing and Communications Review*, 2009, 13(2)
- Jsang A, Ismail R. The beta reputation system. *Proceedings of the 2002 International Conference on Electronic Commerce Conference*, Bled, Slovenia, June 2002
- Ehsan M T, Bahman A. A fuzzy secure spectrum sensing (F3S) scheme for cognitive radios in adversarial environment. *Proceedings of the 2002 International Conference on Computer Communication and Management*, Singapore, 2011
- Feng J Y, Zhang Y Q, Lu G Y, *et al.* Defend against collusive SSDF attack using trust in cooperative spectrum sensing environment. *Proceedings of the 2013 IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, Melbourne, Australia, 2013
- Zeng K, Pawelczak P, Cabric D. Reputation-based cooperative spectrum sensing with trusted nodes assistance. *IEEE Communication Letters*, 2010, 14(3)
- Liu Y, Li X R. Operating characteristic and average sample number functions of truncated sequential probability ratio test. *Proceedings of the 2013 IEEE International Conference on Information Fusion*, Singapore, 2012
- 闫琦, 杨家玮, 张雯. 认知无线网络中安全的合作频谱感知. *北京邮电大学学报*, 2011, 34(2)

(下转第 82 页)

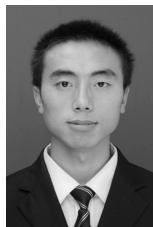


- 8 3GPP Tdoc R2-131055.Alternative Speed Estimation Solutions for Improving MSE. Alcatel-Lucent Shanghai Bell, 2013
- 9 3GPP Tdoc R2-131197. MSE-based Mobility Enhancement. Institute for Infocomm Research (I2R),2013
- 10 3GPP TR 36.932 V12.1.0. Technical Specification Group Radio Access Network; Scenarios and Requirements For Small Cell Enhancements for E-UTRA and E-UTRAN (Release 12), 2013
- 11 3GPP Tdoc R2-131315.Improving HO Performance in HetNet. Samsung,2013
- 12 3GPP Tdoc R2-130957.HO Performance Improvement in Hetnet. ZTE Corporation,2013
- 13 3GPP Tdoc R2-130963.Mobility Performance Improvement of High Speed UE.CATT,2013
- 14 3GPP Tdoc R2-131053.Views on How to Down Select Solutions for Improving Overall HO Performance. Fujitsu,2013
- 15 3GPP Tdoc R2-130961.Evaluation on Adjusting Parameters for the Handover Type. CATT,2013
- 16 3GPP Tdoc R2-131057. Discussion on UE Based Speed Estimation for Improving the Mobility Performance in HetNets. Alcatel-Lucent Shanghai Bell,2013
- 17 3GPP Tdoc R2-130933.RLF Recovery Enhancements. Qualcomm Incorporated,2013
- 18 3GPP Tdoc R2-131396.Fast Handover Using RSRQ/RSRP with SToS/Ping-Pong Avoidance. Intel Corporation,2013
- 19 3GPP Tdoc R2-131002.Mobility Performance Enhancement

Based on UE speed in HetNet.New Postcom,2013

- 20 3GPP Tdoc R2-131371.Improving HO Performance by Multicasting HO Command. Research In Motion UK Limited, 2013

[作者简介]



王东军,男,重庆邮电大学硕士研究生,主要研究方向为 LTE-Advanced 异构小蜂窝网络下的移动性管理研究。

符媛柯,女,重庆邮电大学硕士研究生,主要研究方向为 LTE-Advanced 异构小蜂窝网络下的移动性管理研究。

唐伦,男,博士,重庆邮电大学副教授、硕士生导师,主要研究方向为新一代无线通信、LTE-Advanced 异构小蜂窝网络。

陈前斌,男,博士,重庆邮电大学教授、博士生导师、通信与信息工程学院院长,主要研究方向为个人通信、多媒体信息处理与传输、下一代网络、LTE-Advanced 异构小蜂窝网络等。

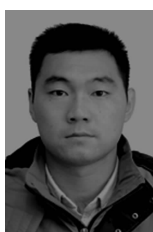
(收稿日期:2013-07-12)

(上接第 66 页)

[作者简介]



吴大中,男,南京信息工程大学副教授,主要研究方向为智能测控技术。



吴海东,男,南京信息工程大学硕士研究生,主要研究方向为信道编码技术。

(收稿时间:2013-09-27)

(上接第 72 页)

- 26 Shen J, Liu S, Zeng L, *et al.* Optimisation of cooperative spectrum sensing in cognitive radio network. IET Communications, 2009, 3(7)
- 27 Wang B, Liu K, Clancy T C. Evolutionary cooperative spectrum sensing game: how to collaborate. IEEE Transactions on Communications, 2010, 58(3)
- 28 Ian F A, Brandon F L, Ravikumar B. Cooperative spectrum sensing in cognitive radio networks: a survey. Physical Communication, 2010(4)

[作者简介]



冯景瑜,男,西安邮电大学讲师,中国科学院大学在站博士后,主要研究方向为无线通信安全、认知无线电、协作频谱感知。

(收稿日期:2013-10-30)