协作频谱感知及SSDF攻击研究

曹 龙[1,2] 赵杭生[2] 鲍丽娜[3] 赵小龙[1,2]
(解放军理工大学通信工程学院 南京 210007)[1] (总参第六十三研究所 南京 210007)[2]
(南京邮电大学通信与信息工程学院 南京 210003)[3]

摘 要 认知无线电网络中,协作频谱感知技术利用多个认知用户的本地感知,克服了多径效应、阴影效应等问题的制约,提高了系统的检测性能。介绍了典型的协作感知系统模型,对本地感知和融合判决这两个关键要素进行了分析,给出了单节点检测与协作感知时的ROC曲线及性能比较。介绍了频谱感知数据篡改攻击、分类以及目前对该攻击的研究现状,针对可能出现的攻击情况,进行了理论分析和仿真,仿真结果表明遭受SSDF攻击后系统性能明显下降。最后总结了全文。

关键词 认知无线电,协作频谱感知,SSDF攻击,检测性能
中图法分类号 TN915.01 **文献标识码** A

Research on Cooperative Spectrum Sensing and SSDF Attacks

CAO Long[1,2] ZHAO Hang-sheng[2] BAO Li-na[3] ZHAO Xiao-long[1,2]
(Institute of Communication Engineering, PLA University of Science and Technology, Nanjing 210007, China)[1]
(The 63rd Institute of General Staff, Nanjing 210007, China)[2]
(College of Communication and Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)[3]

Abstract In cognitive radio network, cooperative spectrum sensing technology overcomes the problems of multipath effects, shadow effects and such constraints by using local sensing results of cognitive users, hence improves the detection performance. This paper introduces the normal model of cooperative spectrum sensing, analyzes the local spectrum sensing and fusion decision these two key elements, shows the differences of ROC between local spectrum sensing and cooperative sensing. Then presents the concept, classification and state-of-the-art of research of spectrum sensing data falsification attack, we also analyzes and simulates for the possible case, simulation results show that the detection performance decline since be attacked. Finally, we summarize this paper.

Keywords Cognitive radio, Cooperative spectrum sensing, SSDF attack, Detection performance

1 引言

随着无线通信的发展,有限的频谱资源中的大部分已经分配完毕,可供新业务使用的频谱资源越来越稀缺,而已分配频谱的利用率却不高[1]。认知无线电(Cognitive Radio,CR)技术使非授权用户能够感知、识别、智能地接入当前空闲的频段,在不干扰授权用户的情况下满足通信需求,在提高频谱利用率、解决频谱稀缺问题上具有广阔的应用前景[2]。

根据CR的定义,CR通信的一个重要前提是具有频谱感知能力,要求能够在某时、某地准确感知是否存在空闲频段,以供CR用户使用;同时还应随时监测是否有新的授权用户需要接入该频段,使CR用户及时腾出该频段或调整工作方式,避免对授权用户造成影响。因此研究人员认为频谱感知是CR最核心的关键技术之一。

频谱感知技术可以分为单节点频谱感知(Local Spectrum Sensing,LSS)技术和协作频谱感知(Cooperative Spectrum Sensing,CSS)技术。单节点感知是指单个认知节点根据本地的无线环境进行频谱特性标识,在实际中,单节点频谱感知的性能常常受到诸如多径衰落、阴影效应和接收机不确定性问题的影响。而协作感知则是通过数据融合,将多个节点的感知结果进行综合判决,克服了单节点感知的缺陷,整个检测性能大大提高。

无论认知无线电网络(Cognitive Radio Network,CRN)中采用何种频谱感知技术,都存在单个节点对频谱资源情况进行检测,所以可以认为单节点频谱感知是频谱感知技术的基础。单节点频谱感知可以分为主用户(Primary User,PU)接收端检测和PU发射端检测,PU接收端检测包括能量检测、匹配滤波器检测和循环平稳特征检测[3]。根据协作认知用户在网络中共享感知数据的方式不同,可以将协作频谱感知方法分为集中式、分布式和中继辅助式[3]。

本文受国家自然科学基金项目(61072077),解放军理工大学预研基金重点项目(20110601)资助。

曹 龙(1988—),男,硕士生,主要研究方向为频谱管理、认知无线电网络等,E-mail:caolong460@sohu.com;赵杭生(1962—),男,博士后,研究员,主要研究方向为频谱管理;鲍丽娜(1987—),女,硕士生,主要研究方向为认知无线电网络;赵小龙(1989—),男,硕士生,主要研究方向为频谱管理、认知无线电网络等。

与传统网络相比，CRN 的认知能力在改善系统性能、提高频谱利用率的同时带来了很多新的安全问题。频谱感知作为实现认知无线的前提和基础，其感知结果对系统的可靠性起着重要作用。本文针对具有代表性的频谱感知数据篡改(Spectrum Sensing Data Falsification，SSDF)[4]攻击，介绍了该攻击的分类及研究现状，对系统遭到攻击时的性能情况进行了分析和仿真。

2 系统模型

在 CRN 中，采用集中式协作频谱感知方法，如图 1 所示，系统中存在单个 PU 及若干 CR 用户，CR_0 作为融合中心(Fusion Center，FC)控制协作感知过程。首先，FC 选择一个信道并控制所有 CR 用户各自对本地频谱资源使用情况进行检测；其次，所有的 CR 用户通过报告信道向 FC 发送本地感知结果(硬判决)；最后 FC 根据综合所有感知数据，决策 PU 是否存在，并将结果发送给所有 CR 用户。

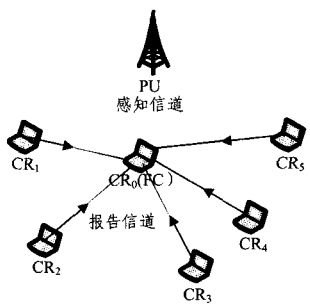

图 1 CRN 协作频谱感知系统模型

2.1 本地感知

如前文所述，目前本地频谱检测的方法很多，能量检测(Energy Detector)是最基本的频谱检测方法，其优点在于不需要知道信号的先验信息，因此实现简单。它通过测量一段观测空间(频域或时域)内的接收信号总能量来判决是否有 PU 用户信号出现[6]。

简单的能量检测器将输入信号通过一个带通滤波器进行 A/D 转换后，对其平方求和构建判决统计量如下：

$$T(x)=\sum_{i=1}^{N}|x(n)|^2 \underset{<}{\overset{\geqslant}{}} \gamma \tag{1}$$

γ 是能量检测的判决门限，则 CR 用户在第 n 次采样中接收的信号符合以下二元假设检验[7]：

$$\begin{cases} H_0: y(n)=v(n) \\ H_1: y(n)=x(n)+v(n) \end{cases} \tag{2}$$

式中，$v(n)$ 是均值为 0、方差为 σ_n^2 的加性高斯白噪声，$x(n)$ 表示 PU 发射的方差为 σ_s^2 的信号，$y(n)$ 表示 CR 用户接收到的信号，H_0 表示该频段内只存在噪声，H_1 表示该频段内存在 PU 信号。

记 $x=(x(1),x(2),\cdots,x(N))^{\mathrm{T}}$，则 $T(x)$ 服从自由度为 N 的 χ^2 分布[8]，根据中心极限定理，当 N 足够大时，χ^2 分布 $T(x)$ 近似服从高斯分布，此时可知：

$$T(x)\sim\begin{cases} H_0: Normal(N\sigma_n^2, 2N\sigma_n^4) \\ H_1: Normal(N\sigma^2, 2N\sigma^4) \end{cases} \tag{3}$$

式中，$\sigma^2=\sigma_n^2+\sigma_s^2$，于是检测概率 P_d 和虚警概率 P_f 分别为[7]：

$$P_d=P\{T(x)>\gamma|H_1\}=Q\left(\frac{\gamma-N\sigma^2}{\sigma^2\sqrt{2N}}\right) \tag{4}$$

$$P_f=P\{T(x)>\gamma|H_0\}=Q\left(\frac{\gamma-N\sigma_n^2}{\sigma_n^2\sqrt{2N}}\right) \tag{5}$$

式中，$Q(x)=\frac{1}{\sqrt{2\pi}}\int_x^{\infty}\mathrm{e}^{-u^2/2}\mathrm{d}u$，$x\geqslant 0$，表示正态高斯互补累积函数。将式(4)和式(5)联立并消去参数 γ，可以得到为了达到目标(P_d,P_f)水平，需要的采样次数是信噪比 $SNR=\sigma_s^2/\sigma_n^2$ 的函数：

$$N=2[Q^{-1}(P_f)-Q^{-1}(P_d)\sqrt{1+2SNR^2}]^2SNR^{-2} \tag{6}$$

从由上式可看出，在低信噪比 $SNR<<1$ 的情况下，满足检测概率和虚警概率所需的最少的采样点数，也即感知时间的数量级为 $O(1/SNR^2)$。

2.2 融合判决

CR 用户进行本地感知后，FC 将这些感知信息进行融合从而判决 PU 是否存在，感知信息的融合方式称为融合判决算法，最常用的融合判决算法有：软判决算法[9]和硬判决算法[9]。本节选取硬判决算法中最常见的“或”判决算法、“与”判决算法和“K-out-of-N”判决算法进行分析和比较。

在硬判决算法中，各个 CR 用户根据本地感知信息做出判决，并将判决结果 H_0/H_1 发送给 FC，最后 FC 根据这些结果做出最终判决并将结果告知 CR 用户。

(1)“或”判决算法(OR 准则)

N 个 CR 用户参与协作的 CRN 网络中，只要有一个用户报告的感知结果为 H_1，FC 就做出 H_1 的判决，否则判为 H_0。其优点在于可最大化保护 PU 免受 CR 用户由于漏检而造成的有害干扰。

假定有 N 个 CR 用户参与协作，其中第 i 个 CR 用户的虚警概率为 $P_{f,i}$，检测概率为 $P_{d,i}$，则采用该算法进行融合后，系统的 P_F 和 P_D 分别为：

$$P_F=1-\prod_{i=1}^{N}(1-P_{f,i}) \tag{7}$$

$$P_D=1-\prod_{i=1}^{N}(1-P_{d,i}) \tag{8}$$

(2)“与”判决算法(AND 准则)

N 个 CR 用户参与协作的 CRN 网络中，只有所有用户报告的感知结果都为 H_1，FC 才做出 H_1 的判决，否则判为 H_0。与“或”判决算法相反，其注重资源利用率的最大化，也就是虚警概率的最小化。

采用该算法进行融合后，系统的 P_F 和 P_D 分别为：

$$P_F=\prod_{i=1}^{N}P_{f,i} \tag{9}$$

$$P_D=\prod_{i=1}^{N}P_{d,i} \tag{10}$$

(3)“K-out-of-N”判决算法(KN 准则)

N 个 CR 用户参与协作的 CRN 网络中，任意大于等于 K 个 CR 用户报告的感知结果都为 H_1，FC 才做出 H_1 的判决，否则判为 H_0。可以理解为将 N 个 CR 用户的感知结果累加起来的值与 K 相比较，若大于等于 K，则做出 H_1 的判决，否则判为 H_0[10]。由此可以得到当每个 CR 用户的虚警概率和检测概率都分别为 P_f 和 P_d 时，系统的 P_F 和 P_D 分别为：

$$P_F=\sum_{i=k}^{N}C_N^i(P_f)^i(1-P_f)^{N-i} \tag{11}$$

$$P_D=\sum_{i=k}^{N}C_N^i(P_d)^i(1-P_d)^{N-i} \tag{12}$$

2.3 仿真结果及分析

仿真场景：采用类似 ATSC[11]的信号作为主用户信号，

噪声条件为 AWGN，采用能量检测法进行检测，采样点数 N 为 2048，检测平均次数为 20000 次。

图 2 给出了 P_f 分别为 0.01，0.02，0.05 和 0.1 时，单节点能量检测下的 SNR 与 P_d 的关系。可以看出相同 P_f 情况下，P_d 随着 SNR 的提高而增大；相同 SNR 情况下，P_d 随着 P_f 的增大而增大。

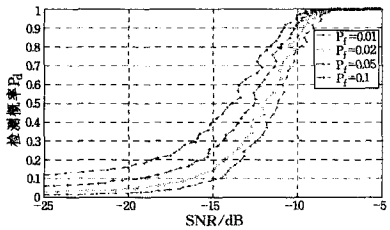

图 2 不同 P_f 下，单节点能量检测 SNR 与 P_d 的关系

图 3 给出了参与协作的 3 个 CR 用户的 SNR 分别为 −14dB，−16dB，−18dB 时，分别采用“OR 准则”、“AND 准则”和“KN 准则”进行融合的 ROC(Receiver Operating Chara-cteristic)曲线，并与单节点检测作比较。可以看出采用协作频谱感知方法后，相同 P_f 下的检测性能得到了明显提高，例如 P_f=0.1 时，单节点能量检测的 P_d 为 0.34，而采用“OR 准则”、“AND 准则”和“KN 准则”的协作频谱感知后 P_d 分别为 0.4、0.43 和 0.48，相对于本地检测性能分别提高了 18%、26%和 41%。

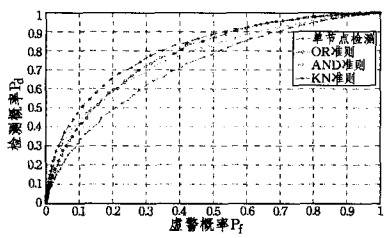

图 3 对 3 个 SNR 不同的用户感知结果进行融合

3 SSDF 攻击

如上节所述，集中式 CRN 网络中所有的 CR 用户必须通过报告信道向 FC 发送本地感知结果，而分布式中 CR 用户向其他用户发送本地感知结果。当系统遭受 SSDF 攻击时，CR 用户则向 FC 或者其他 CR 用户发送不可靠的数据。图 4 举例说明了 SSDF 攻击。

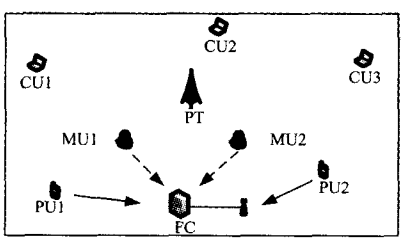

图 4 SSDF 攻击示例

3.1 攻击分类

该攻击发起的目的可以分为以下 3 类[12]：

• 恶意用户　误导 FC 或其他节点发送错误观测结果，这样 FC 或其他节点对频谱的占用情况就会产生误判；

• 贪婪用户　持续报告某一频谱被 PU 信号占用，这些用户迫使其他 CR 用户腾出该频段，从而达到长期占有的目的；

• 无意识用户　由于硬件故障或软件配置错误而报告错误的信息。

3.2 研究现状

文献[13-15]等对 SSDF 攻击的研究主要集中在集中式协作频谱框架下，也就是图 1 所示的系统模型。假设初始参与协作的 CR 用户不可信，引入“信誉度”来检测并孤立攻击者。一般来说，本地感知结果与 FC 最终决策一致的 CR 用户，系统就会提高其“信誉度”，否则降低其“信誉度”；当攻击者被孤立后，FC 利用其余 CR 用户的感知结果进行融合。

3.3 攻击仿真及分析

在上节所述的系统模型下，恶意用户为了实现其攻击目的，可能随机地发送 0 或 1(0 代表 PU 不存在，1 代表 PU 存在)、一直发送 0 或 1 以及发送与实际感知结果相反的数据；贪婪用户为了实现其攻击目的，必须向 FC 或其他 CR 用户报告该频段内一直存在 PU，也就是一直发送 1；最后无意识用户有可能是以上任何一种情况。

对单节点而言，如果它一直发送 1，其物理意义为不管 PU 信号实际是否存在，都判定其存在，此时 P_d=1，P_f=1；如果它一直发送 0，其物理意义为不管 PU 信号实际是否存在，都判定其不存在，此时 P_d=0，P_f=0。

在采用传统的“OR 准则”融合判决算法时，根据算法定义或式(7)和式(8)容易得到当存在单个用户一直发送 1 时，系统的 P_D=1，P_F=1；图 5 给出了此时单个用户发起 SSDF 攻击，即一直发送 0 时系统的 ROC 曲线。可以看出系统的性能明显下降，在 P_f=0.1 时，检测概率下降了 25%。

同样在采用传统的“AND 准则”融合判决算法时，根据算法定义或式(9)和式(10)容易得到当存在单个用户一直发送 0 时，系统的 P_D=0，P_F=0；图 5 同样给出了此时单个用户发起 SSDF 攻击，即一直发送 1 时系统的 ROC 曲线。可以看出系统的性能明显下降，在 P_f=0.1 时，检测概率下降了 28%。

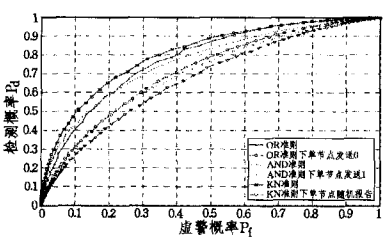

图 5 SSDF 攻击对感知性能的影响

图 5 给出了在采用“KN 准则”融合判决算法，单个用户发起 SSDF 攻击时系统的 ROC 曲线，在仿真中该节点随机发送 0 和 1，并且发送的先验概率相同。可以看出系统的性能明显下降，在 P_f=0.1 时，检测概率下降的幅度甚至达到了 45%。

在采用传统的“OR 准则”和“AND 准则”时，攻击甚至会导致系统失效(P_D=1，P_F=1 或 P_D=0，P_F=0)。综合仿真结果可以看出，系统在遭受 SSDF 攻击时，检测性能明显下降，攻击对采用“KN 准则”融合判决算法的影响最大。

结束语　介绍了典型的协作感知系统模型，对本地感知和融合判决这两个关键要素进行了分析，给出了单节点检测

与协作感知时的 ROC 曲线及性能比较。介绍了频谱感知数据篡改攻击、分类以及目前对该攻击的研究现状，针对可能发送的攻击信号的情况进行了理论分析和仿真。仿真结果表明遭受 SSDF 攻击后系统检测性能明显下降。

参 考 文 献

[1] Spectrum policy task force report [R]. Technical Report 022 135. Federal Communications Commision, Nov. 2002

[2] Akyildiz I F, Lee W-Y. NeXt generation/dynamic spectrum access/cognitive radio wireless networks: A survey[J]. Computer Networks, 2006, 50(13): 2127-2159

[3] 温志刚. 认知无线电频谱检测理论与实践[M]. 北京：北京邮电大学出版社，2011

[4] 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

[5] Kaligineedi P, Khabbazian M, Bhargava V. Secure cooperative sensing techniques for cognitive radio systems[C]// IEEE International Conference on Communications. 2008: 3406-3410

[6] Cabric D, Brodersen R W. Physical layer design issues unique to cognitive radio system[C]// IEEE International Symposium on Personal, Indoor and Mobile Radio Communications. 2005: 759-763

[7] 周来秀. 感知无线网络中频频检测与动态接入技术研究[D]. 长沙：中南大学，2007

[8] Edward P, Liang Ying-chang. Optimization for cooperative sensing in cognitive radio networks[C]// IEEE Wireless Communications and Networking Conference. 2007: 27-32

[9] Quan Zhi, Cui Shu-guang, Vincent Poor H, et al. Collaborative Wideband Sensing for Cognitive Radios[J]. IEEE Signal Processing Magazine, 2008, 25(6): 60-73

[10] Barkat M. Signal detection and estimation(2nd ed)[M]. Artech House Inc, 2005

[11] Advanced Television Systems Committee[Z]. ATSC Standard: Digital television standard(A/53), Revision D, Including amendment, 2005

[12] Fragkiadakis A G, Tragos E Z, Askoxylakis I G. A survey on security threats and detection techniques in cognitive radio networks[J]. IEEE Communications Surveys & Tutorials, 2013, 15(1): 428-445

[13] Chen Y. Collaborative spectrum sensing in the presence of secondary user interferences for lognormal shadowing[J]. Wireless Communications and Mobile Computing, 2012, 12(5): 463-472

[14] Shen B, Kwak K, Bai Z. Optimal linear soft fusion schemes for cooperative sensing in cognitive radio networks [C] // IEEE Global Telecommunications Conference. 2009: 1-6

[15] Meng J, Yin W, Li H, et al. Collaborative spectrum sensing from sparse observations using matrix completion for cognitive radio networks[C] // IEEE International Conference on Acoustics Speech and Signal Processing. 2010: 3114-3117

(上接第 301 页)

提升更加显著。

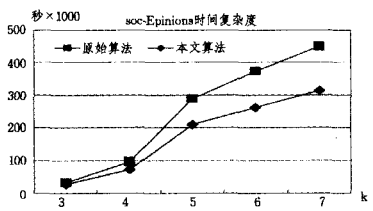

图 4 soc-Epinions 时间复杂度

实验表明本文提出的改进算法能较好地适应各种网络，并对于大、中型网络均能取得较好的运行效率提升。

结束语 针对 K-Reach 索引的创建算法中存在的重复访问路径和顶点的问题，本文提出一种改进算法，其充分利用了已计算顶点的路径信息，避免了顶点的重复访问，提高了算法效率。实验表明，针对中、大网络，改进算法均能明显地降低运行时间，并能更好地适应大型网络的索引创建。

参 考 文 献

[1] Cheng J, Shang Ze-chao, Cheng Hong, et al. K-Reach: Who is in Your Small World [C]// Proceedings' of the 38th International Conference on Very Large Databases. 2012: 1292-1303

[2] Cheng J, Ke Yi-ping, Chu Shu-mo, et al. Efficient processing of distance queries in large graphs: a vertex cover approach [C]// Proceedings of the ACM SIGMOD International Conference on Management of Data. 2012: 457-468

[3] Jin Ruo-ming, Yang Xiang, Ruan Ning, et al. Path-Tree: An Efficient Reachability Indexing Scheme for Large Directed Graphs [J]. ACM Transactions on Database Systems, 2011(36): 1-7

[4] Jin Ruo-ming, Yang Xiang, Ruan Ning, et al. 3-HOP: a high compression indexing scheme for reachability query [C]// Proceedings of the ACM SIGMOD International Conference on Management of Data. SIGMOD 2009: 813-826

[5] Stanford Large Network Dataset Collection[OL]. http://snap.stanford.edu/data/index.html

[6] Chen Yang-jun. An Efficient Algorithm for Answering Graph Rechability Queries [C]// Proceedings of the IEEE 24th International Conference on Data(ICDE). 2008: 893-902

[7] Cheng J, Ke Yi-ping, Fu A W-C, et al. Graph Query Processing with a Low-cost Index [J]. VLDB Journal, 2011, 20(4): 521-539

[8] Nutanonong S, Jacox E H, Samet J H. Distance-constraint Reachability Computation in Uncertain Graphs [C]// Proceedings of the 37th International Conference on Very Large Databases. 2011, 4: 506-517

[9] van Schaik S, de Moor O. A Memory Efficient Reachability Data Structure Through Bit Vector Compression [C]// Proceedings of the ACM SIGMOD International Conference on Management of Data. 2011: 913-924

[10] Jin Ruo-ming, Ruan Ning, Dey S, et al. SCARAB: Scaling Reachability Computation on Large Graphs [C]// Proceedings of the ACM SIGMOD International Conference on Management of Data. 2012: 169-180