doi:10.3969/j.issn.1001-893x.2014.09.022
引用格式:李方伟,刘帆,朱江,等.认知网络中一种基于频谱安全态势感知的路由方案[J].电讯技术,2014,54(9):1292-1297.[LI Fang-wei, LIU Fan, ZHU Jiang, et al. Spectrum Security Situational Awareness for Routing in Cognitive Radio Networks[J]. Telecommunication Engineering, 2014, 54(9): 1292-1297.]

认知网络中一种基于频谱安全态势感知的路由方案*

李方伟,刘 帆**,朱 江,聂益芳

(重庆邮电大学 重庆市移动通信技术重点实验室,重庆 400065)

摘 要:从构建准确的频谱态势图,实现频率资源充分利用的角度出发,针对目前在构建频谱态势图时没有考虑恶意用户(Malicious User,MU)存在的情况,结合克里金(Kriging)插值法估计空域内频谱干扰态势,通过地理位置检测方案识别 MU,从而构建更准确、更安全的频谱态势图,并将其用于端到端的路由协议中。仿真结果表明,该方案能构建完整的频谱态势图,平均误差仅为0.106 dBm,能准确识别恶意用户,识别率高于80%;并且通过识别 MU,在基于频谱态势图的路由过程中,可以减少路由跳数,增加可用频谱空间。

关键词:认知无线电;频谱态势感知;干扰态势;恶意用户;Kriging 插值;路由
中图分类号:TN915.08 **文献标志码**:A **文章编号**:1001-893X(2014)09-1292-06

Spectrum Security Situational Awareness for Routing in Cognitive Radio Networks

LI Fang-wei, LIU Fan, ZHU Jiang, NIE Yi-fang

(Chongqing Key Laboratory of Mobile Communications Technology, Chongqing University of Posts and Telecommunications, Chongqing 400065, China)

Abstract: This paper concerns the construction of accurate spectral situation map, which can help to achieve frequency resource reuse. The traditional methods of constructing spectrum space situation map do not take the influence of malicious users(MUs) into consideration, but the scheme proposed in this paper makes use of Kriging interpolation to estimate the interference situation over a finite geographical area, and identifies malicious user by location detection method, then constructs a more accurate and more secure spectrum situation map. Finally, the spectrum situation map is applied in the end-to-end route protocols. Simulation results demonstrate that the proposed scheme can construct a complete spectrum situation map and the average error is only 0.106 dBm; it can accurately identify malicious users and the detection rate is higher than 80%; it can reduce the routing hops and increase the available spectrum space in the process of routing based on spectrum situation map after identifying MUs.

Key words: cognitive radio; spectrum situational awareness; interference situation; malicious users; Kriging interpolation; route

1 引 言

认知无线网络中,次用户(Secondary Users, SUs)通过检测频谱空洞,在不影响主用户(Primary Users, PUs)正常通信的情况下,利用空闲频段接入

* **收稿日期**:2014-03-31;**修回日期**:2014-05-28 Received date:2014-03-31;Revised date:2014-05-28
基金项目:国家自然科学基金资助项目(61271260)
Foundation Item: The National Natural Science Foundation of China(No. 61271260)
** **通讯作者**:liufancqupt@163.com **Corresponding author**: liufancqupt@163.com

网络,实现频谱资源的充分利用。感知频谱空洞是认知无线电实现的前提。当前频谱空洞的检测和利用主要集中在时间和频率两个维度上,空间维度的利用非常有限,这种传统的空洞利用方式并没有充分地利用频谱资源[1]。

获取 PU 在空间上的位置和干扰分布,即频谱态势图,将有助于 SU 在空间维度上机会式地接入信道,而不对 PU 造成干扰。文献[2]根据 PU 位置在空间上分布的稀疏性,利用随机场理论建模,通过压缩感知方案来重构频谱干扰强度的空间分布图。文献[3]则基于空间插值的方法,根据区域内已知采样点的干扰强度,插值生成连续的表面,用该表面代表区域内干扰态势,构建的频谱态势图主要用于功率控制[4]、资源分配[5]和路由[6]领域。但现有文献在构建和利用频谱态势图时均没有考虑存在 MU 的情况:MU 检测到没有 PU 激活时,便在空域发起仿冒主用户(Primary User Emulation,PUE)[7]攻击,占用该频谱空间;基于不干扰主用户的原则,处于 MU 干扰区域内的 SU 不再使用该频段,由此便浪费了大量频谱可用空间。

针对上述情况,本文利用 Kriging 空间插值法[8]构建频谱态势图,并在恶意用户存在的情况下,通过发射机地理位置检测方案[9]识别恶意用户,从而构建更准确、更安全的频谱态势图。最后将频谱态势图利用于认知网络的路由协议中,通过对恶意用户识别可以提高频谱空间利用率,减少路由跳数。

2　系统模型

2.1　认知网络模型

本文采用具有态势融合中心的网络模型,SU 节点以网格形式均匀分布在区域内,并且可以在类似于 GPS 系统的辅助下确定自身所处位置。为了节省通信开销,仅一部分 SU 通过控制信道将感知到的 PU(MU)信号强度与所处位置发送至融合中心,中心节点采用 Kriging 插值法恢复区域内任意一点的干扰强度,从而构建频谱态势图。

令$\{\boldsymbol{x}_i=(x_i,y_i),i=1,2,\cdots,N\}$表示 SU 节点 i 的坐标,$Z(\boldsymbol{x}_i)$表示第 i 个 SU 在路径损耗和阴影衰落影响下接收到的 K 个 PU 及 MU 信号强度的积累,即

$$Z(\boldsymbol{x}_i)=10^{\frac{W}{10}}\sum_{j=1}^{K}P_j d_{ij}^{-\alpha} \tag{1}$$

其中,P_j 为第 j 个 PU(MU)发射功率,α 为路径损耗因子,d_{ij}为第 i 个 SU 到第 j 个 PU(MU)的距离,$W\sim N(0,\sigma^2)$表示阴影衰落,为服从零均值的高斯随机变量。

图 1 为在路径损耗和阴影衰落影响下的频谱态势图,其中所有 PU 发射功率均设定为1.5 W,路径损耗因子 α 为 2,阴影衰落的标准差 σ 为5 dB;PU 的坐标依次为 $A(40,30)$、$B(40,140)$、$C(80,95)$、$E(130,190)$、$f(140,120)$、$G(155,50)$、$H(180,120)$。

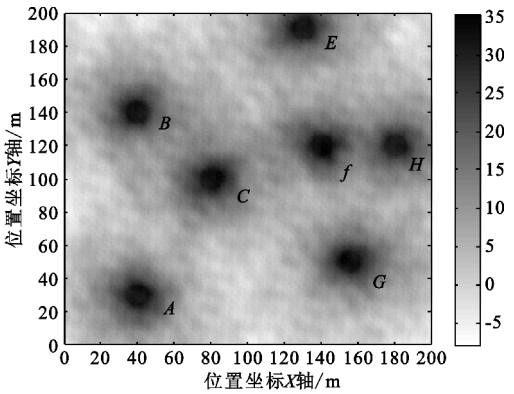

图 1　频谱态势图

Fig. 1 Spectrum situation map

图中颜色由深至浅,表示干扰强度由大变小。黑色区域表明 SU 接收到的干扰强度较大即 PU 的通信范围;颜色逐渐变浅表明 SU 接收到的干扰强度逐渐变小,如图中所示的灰色及白色区域表明此处干扰很小或几乎不受干扰。

2.2　MU 攻击模型

本文所指的攻击是 MU 在空间维度上发起的 PUE 攻击,即 MU 检测到某一频谱空间没有被占用时,便仿冒 PU 占用该空间,而处于 MU 通信区域内的 SU 不再使用该频段,由此浪费大量频谱可用空间,区别于一些文献中所讨论的在频率维上的仿冒攻击[10]。

为方便表述,对网络模型作以下假设:

(1)本文只考虑某一确定信道上频谱态势图的构建及 PUE 攻击;

(2)如果 MU 感知到 PU 已占用某一空间范围,则它不能再占用该区域,即 MU 不占用 PU 已占用的空间;

(3)PU 位置不变,且 SU 网络通过一段时间的感知后存储有 PU 位置信息;

(4)在构建频谱态势图阶段,PU 对频谱的占用

情况不变[6]。

3 空间插值及 MU 识别

3.1 Kriging 数学模型

Kriging 数学模型建立在变异函数理论及结构分析基础上,可以对有限区域内的区域化变量取值进行无偏最优估计。

设研究区域空间为 Ω_0,Z 为空间中某一变量的值(例如 SU 检测到的干扰强度),记为$\{Z(\boldsymbol{x})\in\Omega_0\}$,$\boldsymbol{x}$ 表示空间位置,Kriging 模型的估计公式为

$$Z^*(\boldsymbol{x}_0)=\sum_{i=1}^{N}\lambda_i Z(\boldsymbol{x}_i) \tag{2}$$

其中,$Z(\boldsymbol{x}_i)$ 是$\boldsymbol{x}_i$ 处的测量值;λ_i 为待定系数,表示分配给 $Z(\boldsymbol{x}_i)$的权重;$Z^*(\boldsymbol{x}_0)$ 是在$\boldsymbol{x}_0$ 位置的估计值;N 是用于估计的测量值个数。此处的权系数不是一般方案中由距离决定的,而是在满足无偏性和最小方差性的条件下,依赖变异函数而确定的。由此可见,Kriging 插值法的关键是计算变异函数。其中,第一步是获取实验半方差图,然后选择合适的半方差模型对其拟合得到理论半方差图。半方差图是半方差关于滞后距离的函数,可以通过下式计算:

$$\gamma^*(h)=\frac{1}{2N_n}\sum_{i=1}^{N_n}[Z(x_i+h)-Z(x_i)]^2 \tag{3}$$

其中,N_n 为距离相隔为 h 的点对个数。

3.2 基于地理位置方案识别 MU

3.1 节介绍的空间插值方案能构建 PU 信号强度在空间上的分布情况,但是当存在 MU 在空域上发起 PUE 攻击时,SU 基于不干扰 PU 的原则会浪费大量的频谱空间,故本文采用基于发射机地理位置检测方案对 MU 进行识别。在完成频谱感知后,SU 系统对检测到的干扰区域内信号源进行定位,并将该位置与已知 PU 位置进行比较。当信号源位置与各 PU 发射机位置均不匹配时,即判定该信号源为仿冒攻击者。SU 网络将干扰区域中干扰强度最大值点所处的位置作为 PU(MU)发射机位置。由于空间插值法在定位方面存在一定的误差,所以设定一个误差门限值 ξ,当 $d(p_{\mathrm{PU}},p_{\mathrm{PU}'})>\xi$ 时,即判定检测到的干扰为仿冒主用户攻击者引起的,其中 p_{PU}为 PU 位置,$p_{\mathrm{PU}'}$为检测到的干扰源位置,d 为两者之间的距离。

故基于 Kriging 插值法构建频谱态势图及识别 MU 的流程如图 2 所示。

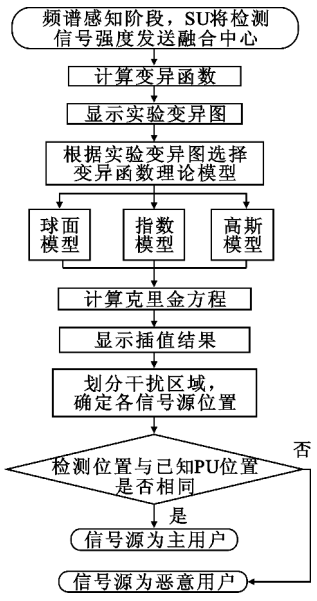

图 2 构建频谱态势图及识别 MU 流程图

Fig. 2 Flowchart of building spectrum situation map and identifying MU

4 基于频谱态势图的路由

在 SU 与 PU 共存的网络中,SU 利用频谱空洞的前提是发射机控制功率以免对 PU 造成干扰,因而上述构建的频谱态势图可用于量化 SU 的发射功率。在 SU 系统无法获知 PU 接收机所处具体位置时,SU 发射功率的设定应满足不能干扰整个 PU 的通信范围,故离 SU 发射机最近的干扰区域处接收到的 SU 信号强度应小于阈值,即

$$d_{\min}^{-\alpha}P_{\mathrm{SU\_Tx}}\leqslant\eta_{\mathrm{PR}} \tag{4}$$

采用基于地理位置的 GPSR 路由协议[11]来说明频谱态势图在路由中的作用。SU 发射机发送数据前通过查询频谱态势图来确定发射功率及选择下一跳路由节点,避免对 PU 产生干扰。频谱态势图可以显示每个 SU 节点处的干扰值,在仅有一个 SU 发射机并且只考虑路径损耗的情况下,SU 接收机处的信噪比为

$$SINR_{\mathrm{SU}_j}=\frac{P_{\mathrm{SU-Tx}}d_{R_j}^{-\alpha}}{I_j+N_0} \tag{5}$$

其中,d_{R_j}为 SU 接收机 j 到发射机的距离,I_j 是第 j 个 SU 处的干扰值,N_0 为噪声。由公式(4)确定 SU 发射功率后,路由转发节点(SU 接收机)的选择还应满足

$$\Gamma=\{R_j\mid SINR_{\mathrm{SU}_j}\geqslant\eta_{\mathrm{SINR}},j=1,2,\cdots,N\} \tag{6}$$

式中,η_{SINR}是 SU 接收机成功接收的信噪比门限。

最后 SU 发射机选择满足公式(6)的节点中离目的节点最近的作为下一跳节点,即

$$R_{i+1}=\arg\max_{R_j}\{\overrightarrow{SD}\cdot\overrightarrow{R_iR_j},R_j\in\Gamma\} \qquad (7)$$

式中,S 和 D 为源节点与目的节点,$\overrightarrow{SD}$和$\overrightarrow{R_iR_j}$分别为路由源节点到目的节点的向量以及上一跳节点 i 到下一跳节点 j 的向量,·表示内积运算,内积值最大者即为离目的节点最近的转发节点。

综上,基于频谱态势图的路由算法描述:

初始化 $i=1$,R_i=路由源节点
while $i>0$ 执行
　R_i 确定附近区域干扰分布
　R_i 由公式(4)确定 P_{SU_Tx}
　if 目的节点在传输范围内
　　if $SINR_{Dest}\geq\eta_{SINR}$
　　　break
　else
　　R_i 由公式(6)确定转发节点集合
　　R_i 由公式(7)选择下一跳节点
　　$i=i+1$

由上述分析可知,SU 路由路径会绕过 PU 通信范围,但当存在恶意用户发起 PUE 攻击时,若不将其识别,SU 基于不干扰 PU 的原则也会控制发射功率,绕开 MU 的干扰区域,增加了路由长度。通过 3.2 节介绍的方案识别恶意用户,若 MU 为次用户系统内节点,则将其剔除;若 MU 是系统外节点,无法关停或剔除时,存在于 MU 干扰区域周围的 SU 发射机可以适当提高发射功率,只需接收机处的信噪比满足公式(6)即可,不用考虑会对 MU 接收机造成干扰,由此便可增加频谱空间可用机会,减少路由跳数。

5　仿真及结果分析

设置一个 200 m×200 m 的正方形区域作为考察区域,SU 节点均匀放置于区域内,用于感知周围信号强度,一定数量的主用户和恶意用户也随机分布在区域内。

5.1　频谱干扰态势图的构建

图 3 为态势融合中心节点采用球面变异函数模型对接收到的 100 个 SU 信号强度的实验半方差图进行拟合,然后利用 Kriging 方法构建的图 1 所示的频谱态势图,可以看出,Kriging 插值法能准确地恢复出区域内干扰分布。交叉检验发现,平均误差仅为0.106 dBm,误差标准差为 1.33。

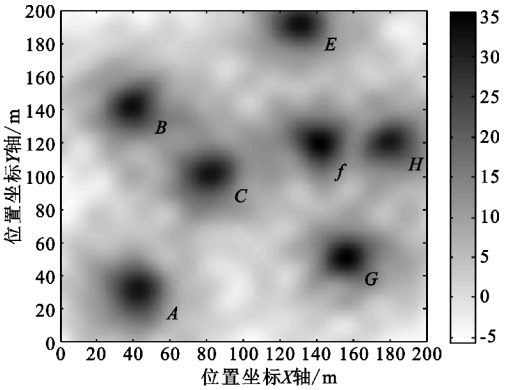

图 3　基于 Kriging 方法构建的频谱态势图
Fig. 3 Spectrum situation map based on Kriging

5.2　恶意用户的检测性能分析

本小节的仿真中设置6 个 PU 和 1 ~2 个 MU 随机分布在区域内,位置固定。SU 系统采用地理位置方案识别 MU,将干扰区域内干扰值最大的点作为信号源的位置,当检测出来的干扰源位置与已知的主用户位置间距离大于阈值时,判定该节点为 MU。其中根据具体仿真环境及文献[12]中 Kriging 插值法的定位性能将阈值 ξ 设置为5 m。

进行10 000次仿真对 MU 的平均检测性能进行分析,如图 4 所示。仿真结果表明,随着阴影衰落标准差的增加,采样次用户数目的减少和 MU 个数的增加,MU 的检测性能逐渐下降,但总体来说 MU 的检测率均能保持在 80% 以上,说明 Kriging 插值法构建的频谱态势图有较高的定位精度,能准确识别 MU,保证系统安全性。

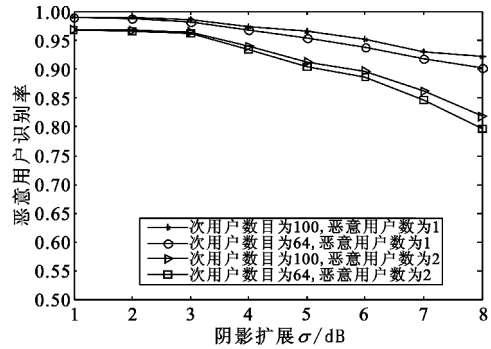

图 4　不同条件下 MU 识别率比较
Fig. 4 Comparison of MU recognition rate under different conditions

5.3　路由性能分析

设定图 1 所示的频谱态势图中,A、B、C、E、G、H 为合法的 PU,f 为 MU。图 5 为不识别恶意用户、识别恶意用户为系统内节点将其剔除以及识别恶意用户为系统外节点无法将其关停或剔除 3 种情况下的

路由路径。

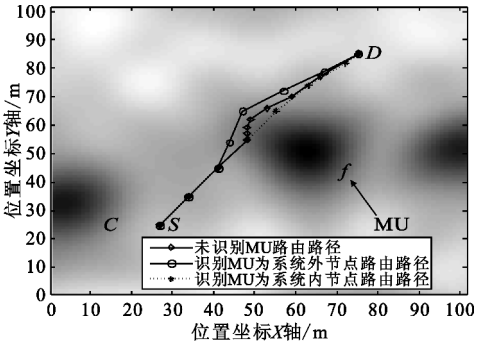

图 5 三种情况下路由路径

Fig. 5 Routing path in three cases

三种情况下的路由路径在绕过正常主用户时相同,故不再比较。但在绕过 MU 的干扰区域时,若未识别 MU,SU 基于不干扰 PU 的原则会控制发射功率且需满足 SU 接收机处的信噪比大于阈值,因而增加了路由跳数;若识别 MU 为系统外节点,且下一跳路由节点存在于 MU 干扰范围附近时,SU 发射机可以提高发射功率,只需满足接收机处信噪比大于阈值,数据便可传送至该节点;同时,若识别 f 为系统内的 MU 时,则将其剔除,路由路径可直接传过该区域。图 5 中,未识别 MU 时的路由跳数为 10 跳,识别 MU 为系统外节点和系统内节点后,路由跳数均减少至 7 跳,并且识别恶意用户后的路由路径仅可能会干扰到 MU 的接收机,对次用户和正常主用户网络不会造成影响。

图 6 为公式(6)中所设置的信噪比阈值对路由跳数的影响,其中,源节点和目的节点坐标分别为 $S(10,10)$、$D(160,160)$。可以看出,随着所设信噪比阈值的增加,三种情况下的路由跳数均有所增加,原因在于信噪比阈值增大时,路由路径需绕到离干扰区域更远的地方,因而增加了路由跳数,但是通过识别 MU 并作相应处理可以减少路由跳数。

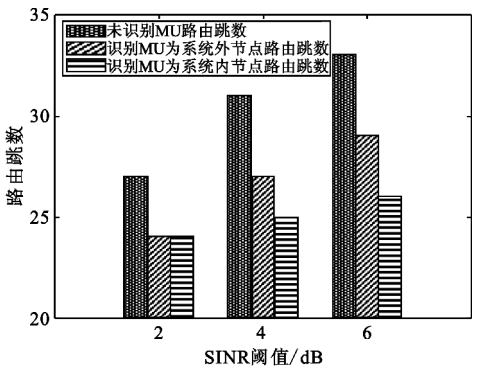

图 6 不同信噪比下路由跳数比较

Fig. 6 Comparison of routing hops under different SINR

6 结 论

本文将恶意用户存在的情况引入到频谱态势图的构建过程中。在利用 Kriging 空间插值法构建频谱态势图的基础上,通过地理位置检测方案识别恶意用户,并进行相应处理。该方案可以较准确地区分主用户和恶意用户的干扰分布,从而可以在基于频谱态势图的路由过程中减少路由跳数,增加频谱空间可用范围。在未来的工作中,作者将对频谱态势图构建过程中 PU 占用频谱的动态性变化,以及更准确地识别 MU 的方法进行进一步研究。

参考文献:

[1] 马志垚. 认知无线电中基于时—频—空三维空洞的机会接入研究[D]. 北京:清华大学,2009.
MA Zhi-yao. Studies on Temporal-Frequency -Spatial Three-Dimensional Spectrum Hole Based Opportunistic Access in Cognitive Radio Networks[D]. Beijing:Tsinghua University,2009. (in Chinese)

[2] Jayawickrama B A,Dutkiewicz E,Oppermann I,et al. Improved performance of spectrum cartography based on compressive sensing in cognitive radio networks[C]// Proceeding of 2013 IEEE International Conference on Communications. Budapest,Hungary:IEEE,2013:5657-5661.

[3] Boccolini G,Hernandez-Penaloza G,Beferull-Lozano B. Wireless Sensor Network for Spectrum Cartography based on Kriging Interpolation[C]// Proceeding of 2012 IEEE 23rd International Symposium on Personal Indoor and Mobile Radio Communications. Sydney, Australia: IEEE, 2012:1565-1570.

[4] Dall'Anese E,Kim S J,Giannakis G B,et al. Power control for cognitive radio networks under channel uncertainty [J]. IEEE Transactions on Wireless Communications, 2011,10(10):3541-3551.

[5] Mahapatra R,Strinati E C. Interference-aware dynamic spectrum access in cognitive radio network[C]// Proceeding of IEEE 22nd International Symposium on Personal Indoor and Mobile Radio Communications. Toronto, Canada: IEEE,2011:396-400.

[6] Shih S Y,Chen K C. Compressed sensing construction of spectrum map for routing in cognitive radio networks[J]. Wireless Communications and Mobile Computing,2012, 12(18):1592-1607.

[7] Chen Z,Cooklev T,Chen C,et al. Modeling primary user emulation attacks and defenses in cognitive radio networks [C]// Proceeding of IEEE 28th International Performance Computing and Communications Conference. Arizona,USA:IEEE,2009:208-215.

[8] 冯文江,李俊. 认知无线电中基于 Kriging 方法的干扰

温度空域分布估计[J]. 重庆大学学报,2011,34(2):58-63.
FENG Wen-jiang, LI Jun. The spatial distribution estimation of Interference temperature based on kriging method in cognitive radio[J]. Journal of Chongqing University,2011,34(2):58-63. (in Chinese)

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

[10] 逄德明,胡罡,徐明. 基于能量指纹匹配的无线认知网络仿冒主用户攻击检测[J]. 计算机科学,2011,38(3):28-33.
PANG De-ming, HU Gang, XU Ming. Detecting Primary Emulation Attacks Based on Energy Fingerprint Matching in Cognitive Radio Networks[J]. Computer Science,2011,38(3):28-33. (in Chinese)

[11] 张鹏明,李洪烈,林成浴. 基于地理定位信息的移动自组网路由协议综述[J]. 电讯技术,2012,52(9):1552-1560.
ZHANG Peng-ming, LI Hong-lie, LIN Cheng-yu. Survey on Position-based Routing Protocols for Mobile Ad Hoc Networks[J]. Telecommunication Engineering, 2012,52(9):1552-1560. (in Chinese)

[12] Ureten S, Yongacoglu A, Petriu E. A comparison of interference cartography generation techniques in cognitive radio networks[C]//Proceedings of 2012 IEEE International Conference on Communications. Ottawa, Canada: IEEE,2012:1879-1883.

作者简介:

李方伟(1960—),男,重庆人,教授、博士生导师,主要研究方向为移动通信理论与技术、信息安全技术;

LI Fang-wei was born in Chongqing, in 1960. He is now a professor and also the Ph. D. supervisor. His research concerns mobile communication theory and technology, information security technology.

刘　帆(1988—),男,湖北人,硕士研究生,主要研究方向为认知无线电和网络安全;

LIU Fan was born in Hubei Province, in 1988. He is now a graduate student. His research concerns cognitive radio and network security.

Email:liufancqupt@163.com

朱　江(1977—),男,湖北人,2009 年于电子科技大学获博士学位,现为副教授,主要研究方向为认知无线电;

ZHU Jiang was born in Hubei Province, in 1977. He received the Ph. D. degree from University of Electronic Science and Technology of China in 2009. He is now an associate professor. His research direction is cognitive radio.

聂益芳(1990—),女,重庆人,硕士研究生,主要研究方向为移动通信网络安全。

NIE Yi-fang was born in Chongqing, in 1990. She is now a graduate student. Her research direction is mobile communication network security.