

动态频谱访问无线网络的连通性分析

侯孟书 李玉军 卢显良 屈 鸿 任立勇

(电子科技大学计算机科学与工程学院 成都 611731)

摘 要 与传统无线网络不同,在动态频谱访问无线网络中,授权用户对分配的频段具有优先使用权,非授权用户网络的连通性受授权用户的分布和授权用户对频段的使用行为的影响。基于连续渗流理论,证明当授权用户较为稀疏或者负载较轻时,非授权用户可以构成部分连通的网络;反之,当授权用户较为密集并且负载较重时,无法部署部分连通的非授权用户网络。此外,在授权用户和非授权用户共享 1 个信道的情况下,给出了非授权用户网络存在部分连通的必要条件。仿真实验数据验证了理论分析的正确性。

关键词 动态频谱访问,连通性,连续渗流

中图法分类号 TP393 **文献标识码** A

On the Connectivity Analysis over Dynamic Spectrum Access Networks

HOU Meng-shu LI Yu-jun LU Xian-liang QU Hong REN Li-yong

(School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China)

Abstract Different from traditional wireless networks, in dynamic spectrum access networks, primary users have privilege to use the spectrum and hence the connectivity of secondary user network is affected by the distribution and activity of the primary users. Based on continuum percolation theory, this paper proved that secondary users can form the percolated network when there were less primary users or the load of primary users was light. On the other hand, secondary user network couldnot be percolated when there were many primary users and the load was heavy. The necessary condition of the existence of percolated secondary user network was derived when the primary users and secondary users shared one channel. All above conclusions are examined by extensive simulations.

Keywords Dynamic spectrum access, Connectivity, Continuum percolation

1 引言

无线电频谱是一种珍贵、有限的自然资源,其使用方式受各国政府的严格管制。现有频谱使用策略大多采用静态分配原则,即把频谱资源条状分割成若干个子频段,每个子频段通常只分配给一种授权用户使用。随着无线通信产业的快速发展,对频谱资源的需求越来越多,使有限的频谱资源变得越来越稀缺;而另一方面,美国联邦通信委员会的调查显示,随着地域和时域的不同,已分配频段的利用率从 15%~85% 不等,除了少数频段超负荷以外,绝大部分频段利用率低下^[1]。近年来,业界广泛认识到现有的静态频谱分配政策是造成频谱稀缺、利用率低下的主要原因。

在这种情况下,动态频谱访问(Dynamic Spectrum Access, DSA)的思想应运而生:在不影响授权用户正常通信的前提下,非授权用户伺机使用已分配的授权频段,以增加时域、空域以及频域上的频谱复用^[2,3]。动态频谱访问技术不仅能缓解频谱稀缺问题,降低信道干扰,提高无线网络容量,而且还望在日益拥挤的无线传播环境中实现各种通信系统的

共存、兼容和互用。因此,动态频谱访问技术在无线网络通信领域备受关注。

迄今为止,在频谱政策、标准化组织及国内外研究机构的推动下,动态频谱访问无线网络的研究取得了重大进展。但这些研究大都集中在频谱感知、频谱分析、频谱决策等物理层和 Mac 层的功能上^[4-9],对于网络层、传输层和应用层的研究相对较少^[3,10,11]。同时,在动态频谱访问无线网络中,由于授权用户对于分配的频段具有优先使用权,因而非授权用户网络的功能、性能等特性受授权用户的分布及授权用户对频段使用行为的影响。然而,这种影响目前还没有引起研究人员的足够重视,对于非授权用户网络的连通性这一基本特性的研究几乎处于空白状态^[12]。

在动态频谱访问无线网络中,对于任意两个非授权用户而言,它们之间无线链路的存在情况不仅依赖于它们之间的物理距离,而且还与它们周围授权用户的分布和这些授权用户对频段的使用情况密切相关。基于这一特性,本文采用连续渗流理论,证明了当授权用户较为稀疏或者负载较轻时,非授权用户可以构成部分连通的网络;与之相反,当授权用户较

到稿日期:2009-08-21 返修日期:2009-11-05 本文受国家自然科学基金项目(无线自组织网络的极限性能分析,60903156),电子科技大学博士后基金(无线传感网络的信任研究),电子科技大学青年重点基金(带宽密集型大规模 P2P 分发网络流量优化技术研究)资助。

侯孟书(1971—),男,博士后,副教授,主要研究方向为计算机网络、P2P 计算、无线传感网络等,E-mail:mshou@uestc.edu.cn;李玉军(1975—),男,博士生,主要研究方向为无线网络路由算法、P2P 计算;卢显良(1943—),男,教授,博士生导师,主要研究方向为操作系统、分布式计算。

为密集并且负载较重时,无法部署部分连通的非授权用户网络。进而,在授权用户和非授权用户共享1个信道的情况下,给出了非授权用户网络存在部分连通性的必要条件。

2 系统模型

系统模型包括网络模型和通信模型两个部分。网络模型主要描述授权用户、非授权用户的分布特性,以及授权用户对分配频段的使用情况;通信模型主要讨论非授权用户节点之间无线链路的存在条件,以及非授权用户网络部分连通性的定义。

2.1 网络模型

假设授权用户、非授权用户分别以参数为 λ_p, λ_s 的泊松点过程分布在二维平面上。所有授权用户、非授权用户分别具有相同的通信半径 r_p, r_s 。共计分配了 N 个不同的信道供授权用户使用,并且每个授权用户从 N 个信道中随机选取1个信道作为自己的工作信道。同时,将时间均匀地划分为若干个时间间隙,在每个时间间隙内,每个授权用户使用工作信道进行通信的概率为 p_a 。概率 p_a 描述了授权用户对工作信道的占用情况,称为授权用户的负载。

2.2 通信模型

在动态频谱访问无线网络中,授权用户对分配的频段具有优先使用权。为了避免非授权用户之间的信号传输对授权用户的正常通信造成干扰,假设每个授权用户 P_i 都有1个通信保护范围 $PR(P_i)$ 。若非授权用户 S_j 希望伺机使用 P_i 的工作信道,并且 P_i 正在通信,则 S_j 必须位于 P_i 的通信保护范围 $PR(P_i)$ 之外,以保证 P_i 的正常通信不受干扰。

定义1 (P_i 的通信保护范围 $PR(P_i)$) 授权用户 P_i 的通信保护范围 $PR(P_i)$ 是以 P_i 为中心、以 $(1+\alpha)r_p$ 为半径的圆形区域,其中 $\alpha>0$ 为保护系数。

进一步假设所有授权用户具有相同数值的保护系数 α ,因此所有授权用户具有相同尺寸的保护范围。

定义2 (通信保护半径 R_p) 所有授权用户具有相同数值的通信保护半径 $R_p = (1+\alpha)r_p$ 。

假设非授权用户能够伺机使用这些分配给授权用户的 N 个信道。然而,为了避免对授权用户的正常通信造成干扰,每个非授权用户在某一时间间隙内也许只能伺机使用 N 个信道中的某些子集。为此,我们引入了可用信道的概念,具体描述如下。

定义3 (可用信道 $ACH(S_j)$) 在某一时间间隙内,非授权用户 S_j 的可用信道 $ACH(S_j)$ 是指非授权用户 S_j 能够伺机使用的信道集合。即 $ACH(S_j) = \{k | 1 \leq k \leq N, \text{并且} \forall P_i \in D(S_j, R_p) \cap AP \text{ 有 } CH(P_i) \neq k\}$,其中 AP 是该时间间隙内正在通信的授权用户的集合, $CH(P_i)$ 为授权用户 P_i 的工作信道。

可用信道的概念反映了在动态频谱访问无线网络中信道的访问方式与传统的无线网络存在着本质的不同。在传统的无线网络中,所有节点对分配的信道具有对等的访问权限,以公平竞争的方式获得信道的使用权。在这些网络中,若两个节点位于彼此的通信范围之内,则它们之间必然存在着无线链路连接。然而在动态频谱访问无线网络中,即使两个非授权用户 S_i 和 S_j 之间的距离小于它们的通信半径 r_s ,在某一时间间隙内,若这两个非授权用户可用信道的交集为空,即

$ACH(S_i) \cap ACH(S_j) = \emptyset$,则在该时间间隙内 S_i 和 S_j 之间也因无伺机使用的信道而无链路连接。我们引入下述定义来具体描述非授权用户之间的链路存在情况。

定义4 (可用链路) 若两个非授权用户 S_i, S_j 之间的距离小于或等于它们的通信半径 r_s ,即 $\|S_i, S_j\|_2 \leq r_s$,并且至少存在一个可以伺机使用的公共信道,即 $ACH(S_i) \cap ACH(S_j) \neq \emptyset$,则称 S_i, S_j 之间存在一条可用链路。

同时,我们拓宽了传统网络部分连通性的概念,给出非授权用户网络部分连通性的定义,具体描述如下。

定义5 (非授权用户网络的部分连通性) 任意给定一个时间间隙 t_m ,若非授权用户网络在 t_m 内处于渗流状态,则称非授权用户网络处于部分连通状态。即在 t_m 内,当动态频谱访问无线网络趋于无穷大时,非授权用户之间能够通过可用链路构成一个大连通分支,该连通分支内包含的无穷数量的非授权用户的概率为1。

3 非授权用户网络的部分连通性

本节首先证明当授权用户较为稀疏或者负载较轻时,在非授权用户密度足够大的前提下,非授权用户可以构成部分连通的网络。在此情况下,可依靠非授权用户网络实现长距离多跳通信。反之,当授权用户较为密集并且负载较重时,可供非授权用户伺机使用的信道很少。在此情况下,即使部署的非授权用户非常密集,它们也无法构成部分连通网络,因此无法利用非授权用户网络进行长距离多跳通信。

在讨论非授权用户网络的部分连通性之前,首先介绍正方格上的边渗流现象。将一个平面划分为若干个大小相同的正方格,这些正方格构成了一个无穷大的网格 L ,如图1所示。若每个正方格的每条边以概率 p_e 处于开启状态,且每条边是否处于开启状态仅依赖于与它相邻的六条边,而非相邻的边无关。为叙述方便,将处于开启状态的边称作有效边,将相互连通的有效边构成的集合称为边连通簇,即对于一个边连通簇内的任意两个边之间至少存在一条由有效边组成的路连接。若网格 L 中最大的边连通簇内仅包含有限数目的有效边,则称网格 L 处于非渗流状态。反之,若网格 L 中存在唯一一个包含有无穷多个有效边的边连通簇,则称网格 L 处于边渗流状态。对于这一渗流现象,存在下述引理。

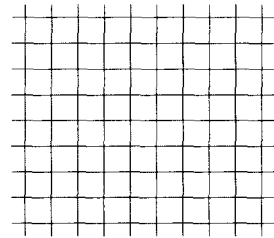


图1 网格 L

引理1 当 $p_e > 14/15$ 时,网格 L 以概率1处于边渗流状态;当 $p_e < 1/9$ 时,网格 L 不会发生边渗流现象的概率为 $1^{[13]}$ 。

基于引理1,关于非授权用户网络的部分连通性,我们推导出了下列定理。

定理1 当授权用户较为稀疏或者负载较轻时,在非授权用户密度足够大的前提下,非授权用户可以构成部分连通的网络;反之,当授权用户较为密集并且负载较重时,即使非

授权用户密度再大,也无法构成部分连通的网络。

证明:采用构造法,即将非授权用户网络的连通性影射为网格 L 的边渗流现象。

假设动态频谱访问无线网络部署在一个无穷大的二维平面上。我们将该平面划分为若干个大小相同的正方格,其中每个正方格的边长为 $d=2R_p$,这些正方格构成了一个无穷大的网格 L ,如图 1 所示。

通过定义网格 L 中每条边的关联矩形,首先建立网格 L 中的有效边与非授权用户网络的连通性二者之间的关联关系。对于网格 L 中的每条水平边 ab ,定义其关联矩形 $RB_{ab} = [x_a - d/4, x_b + d/4] \times [y_a - d/4, y_b + d/4]$,其中 (x_a, y_a) , (x_b, y_b) 分别为 a, b 两点的坐标。如图 2 所示, RB_{ab} 由 3 个小正方形组成,分别命名为 RB_{ab}^L, RB_{ab}^M 和 RB_{ab}^R 。

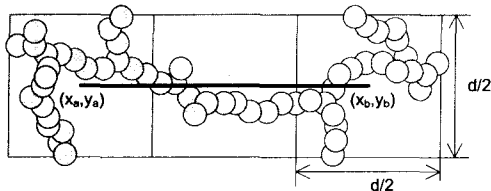


图 2 水平边 ab 的关联矩阵 RB_{ab}

任意给定一个时间间隔 t_m ,若位于矩形区域 RB_{ab} 内的非授权用户在 t_m 内满足以下 3 个条件:

i) 存在一条横穿矩形 RB_{ab} 的路 $S_{m1}S_{m2}S_{m3}\dots S_{mi}$,即 S_{mi} 到矩形 RB_{ab} 左边界的距离小于 r_s ,并且 S_{mi} 到矩形 RB_{ab} 右边界的距离小于 r_s ;

ii) 存在一条竖穿正方形 RB_{ab}^L 的路 $S_{n1}S_{n2}S_{n3}\dots S_{nj}$,即 S_{n1} 到正方形 RB_{ab}^L 上边界的距离小于 r_s ,并且 S_{nj} 到正方形 RB_{ab}^L 下边界的距离小于 r_s ;

iii) 存在一条竖穿正方形 RB_{ab}^R 的路 $S_{l1}S_{l2}S_{l3}\dots S_{lk}$,即 S_{l1} 到正方形 RB_{ab}^R 上边界的距离小于 r_s ,并且 S_{lk} 到正方形 RB_{ab}^R 下边界的距离小于 r_s ;

则边 ab 为一条有效边,如图 2 所示。

对于网格 L 中的垂直边,可以通过类似的方法定义有效边(等价于把水平边 ab 和矩形 RB_{ab} 同时旋转 90°)。

根据有效边与非授权用户网络连通性之间的关联关系,可以证明:在时间间隔 t_m 内,非授权用户是否处于部分连通状态等价于网格 L 是否发生了边渗流现象。其证明方法与文献[13]中引理 1 的证明方法类似,不再赘述。

在时间间隔 t_m 内,若授权用户较为稀疏或者负载较轻,使得矩形区域 RB_{ab} 内存在 1 个可供所有非授权用户伺机使用的信道的概率大于 $14/15$,则在足够大的非授权用户密度下,可以保证边 ab 为有效边的概率 $p_e > 14/15$ 。根据引理 1 可知,此时网格 L 发生边渗流现象的概率为 1。因此,非授权用户处于部分连通状态。

与之相反,若授权用户较为密集并且负载较重,使得正方形 RB_{ab}^M 内存在一块宽度为 r_s 的条形区域,如图 3 中的阴影部分所示。该条形区域不存在可供非授权用户伺机使用的信道的概率大于 $8/9$,则即使非授权用户密度再大,边 ab 为有效边的概率也不可能超过 $1/9$,即 $p_e < 1/9$ 。根据引理 1 可知,此时网格 L 不会发生边渗流现象的概率为 1。因此,非授权用户无法构成部分连通网络。

定理得证。

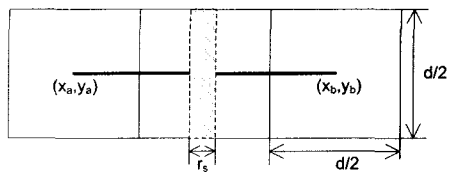


图 3 RB_{ab}^M 不存在竖穿路

当 $N=1$ 时,即授权用户和非授权用户共享 1 个信道,我们进一步给出了非授权用户网络存在部分连通性的必要条件。

定理 2 在授权用户和非授权用户共享 1 个信道(即 $N=1$)的前提下,非授权用户可以构成部分连通网络的必要条件为 $\lambda_p \leq \lambda_p^*$,其中 $\lambda_p^* = 4\lambda_c^* / ((4R_p^2 - r_s^2) p_a)$ 称为授权用户密度上界, λ_c^* 为泊松布尔模型(Poisson Boolean Model) $B(X, 1, \lambda)$ 的临界密度。

证明:采用反证法,其证明过程与文献[12]中定理 2 的证明方法类似。假设在时间间隔 t_m 内非授权用户处于部分连通状态。根据非授权用户网络的部分连通性的定义可知,在时间间隔 t_m 内,以概率 1 存在一个包含有无穷多个非授权用户的大连分支 C_{max} 。

假设 $Path_\infty = S_1 S_2 S_3 \dots$ 为大连分支 C_{max} 内的一条无穷大路径。即在时间间隔 t_m 内,对于任意一个非授权用户 $S_i \in Path_\infty$, S_i 和 S_{i+1} 之间存在一条可用链路; S_i 在 $Path_\infty$ 中仅出现一次。

由于授权用户和非授权用户共享 1 个信道,并且授权用户对信道具有优先使用权,因此对于任意的非授权用户 $S_i \in Path_\infty$,在时间间隔 t_m 内,以 S_i, S_{i+1} 为中心,以 R_p 为半径的两个圆形区域内均不能存在正在通信的授权用户。

定义时间间隔 t_m 内正在通信的授权用户的集合为 $AP(t_m)$ 。对于无穷大路径 $Path_\infty$ 中的每条可用链路 $S_i S_{i+1}$ ($1 \leq i$),定义一个对应的关联矩形区域 $RB_i = [-d_i/2, d_i/2] \times [-\epsilon, \epsilon]$,其中 d_i 为 S_i 与 S_{i+1} 之间的距离,这些矩形如图 4 中的虚线所示。定义 l_i 为时间间隔 t_m 内正在通信的授权用户到矩形区域 RB_i 的最短距离,即 $l_i = \inf\{|P_j, Y| | P_j \in AP(t_m), Y \in RB_i\}$ 。

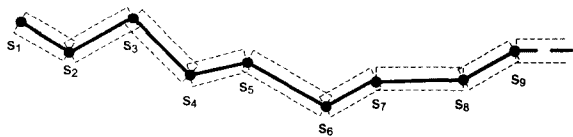


图 4 无穷大路径 $Path_\infty$ 及其关联矩形

根据上述定义及非授权用户之间可用链路的存在条件,通过简单的几何计算可知:

$$l_i \geq l_{\min} \quad (1)$$

式中, $i=1, 2, 3, \dots$

$$l_{\min} = \sqrt{R_p^2 - \frac{r_s^2}{4}} - \frac{\epsilon}{2} \quad (2)$$

根据泊松点过程的抽样定理(Thinning Theorem)[14]可知 $AP(t_m)$ 是一个参数为 $\lambda_p p_a$ 的泊松点过程。我们通过反正法证明若在时间间隔 t_m 内存在无穷大路径 $Path_\infty$,那么泊松布尔模型 $B(X_p, l_{\min}, \lambda_p p_a)$ 必然未发生渗流现象。

泊松布尔模型 $B(X_p, l_{\min}, \lambda_p p_a)$ 是指 X_p 是二维平面上参数为 $\lambda_p p_a$ 的泊松点过程, X_p 中的每个点占据一个以该点

坐标为中心、以 l_{min} 为半径的圆形区域。对于某块连续区域 A , 若对于任意一点 $a \in A$ 、任意一点 $c \in X_p$, 点 a, c 之间的距离大于 l_{min} , 则称区域 A 为一块连续空白区域; 反之, 对于某块连续区域 B , 若对于任意一点 $b \in B$, 存在点 $c' \in X_p$, 使得点 b, c' 之间的距离小于或等于 l_{min} , 则称区域 B 为一块连续非空白区域。若泊松布尔模型 $B(X_p, l_{min}, \lambda_p p_a)$ 发生了渗流现象, 则根据连续渗流理论可知, 平面中不存在一个无穷大的连续空白区域, 整个平面的空白区域由若干个面积有限的连续空白区域组成。

假设泊松布尔模型 $B(X_p, l_{min}, \lambda_p p_a)$ 发生了渗流现象, 则在时间间隔 t_m 内, 无穷大路径 $Path_\infty$ 必然经过某些连续非空白区域。假设无线链路 $S_i S_j$ 经过了连续非空白区域 B , 则至少存在一个正在通信的授权用户 $P_k \in B$ 使得 P_k 到线段 $S_i S_j$ 的距离小于或等于 l^* , 与式(1)矛盾。

因此, 在时间间隔 t_m 内, 若非授权用户之间存在一条无穷大路径 $Path_\infty$, 则泊松布尔模型 $B(X_p, l_{min}, \lambda_p p_a)$ 必然未发生渗流现象。由渗流理论的伸缩率(Scaling Law)^[15]可知, 泊松布尔模型 $B(X_p, l_{min}, \lambda_p p_a)$ 未发生渗流现象的充要条件为:

$$\lambda_p \leq \frac{\lambda_c^*}{p_a l_{min}^2} \quad (3)$$

根据式(2)和式(3), 使 $\epsilon \rightarrow 0$, 得:

$$\lambda_p \leq \frac{4\lambda_c^*}{(4R_p^2 - r_s^2) p_a} \quad (4)$$

因此, 可以部署部分连通的非授权用户网络的必要条件为:

$$\lambda_p \leq \frac{4\lambda_c^*}{(4R_p^2 - r_s^2) p_a} \quad (5)$$

定理得证。

4 仿真实验

在本节中, 我们对定理 2 的正确性予以检验。即在授权用户和非授权用户共享 1 个信道($N=1$)的前提下, 当授权用户密度大于一定程度时, 非授权用户无法构成部分连通的网络。仿真实验参数设置为 $r_s=0.1, r_p=0.2, \alpha=0.1, p_a=0.1$ 和 $\lambda_s=150$ 。

与传统网络的连通性分析类似, 我们用非授权用户网络中大连通分支的相对尺寸来评价网络的连通状况, 其定义为非授权用户网络中最大的连通分支内非授权用户数目与网络内非授权用户总数目的比值。在不同的授权用户密度下, 非授权用户网络中大连通分支的相对尺寸如图 5 中的实线所示。我们用虚线表示授权用户密度理论上界 λ_p^c 。

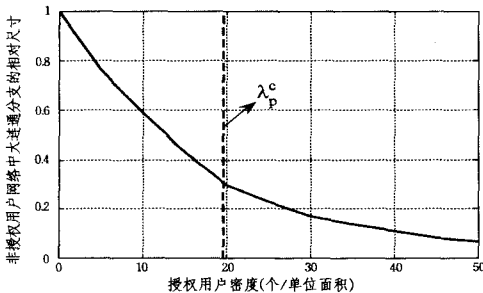


图 5 非授权用户网络连通状况的变化过程与授权用户密度的关系

实验数据分析总结如下: 第一, 当授权用户密度大于 λ_p^c 时, 非授权用户网络中最大连通分支的相对尺寸小于 40%,

非授权用户无法构成部分连通的网络, 验证了理论分析的正确性。

第二, 与传统无线网络的连通性不同, 非授权用户网络从非连通状态到部分连通状态的转变不是一个骤变过程。即非授权用户网络从非连通到部分连通状态的转变过程中, 授权用户的密度变化范围较大。因此, 我们需要分别界定非授权用户构成部分连通网络时需要的授权用户密度下界 λ_p^l (即当授权用户密度小于 λ_p^l 时, 可以部署部分连通的非授权用户网络)、非授权用户不存在部分连通网络时需要的授权用户密度上界 λ_p^u (即当授权用户密度大于 λ_p^u 时, 授权用户无法构成部分连通的网络)。本文仅给出了 λ_p^u 的理论上界 λ_p^c , 关于 λ_p^l 的研究还在进行之中。

结束语 本文主要分析动态频谱访问无线网络中非授权用户网络的部分连通性问题。在动态频谱访问无线网络中存在授权用户和非授权用户两种截然不同的节点类型。其中, 授权用户对分配的频段具有优先使用权, 而非授权用户只能在不影响授权用户正常通信的前提下伺机使用这些分配给授权用户的频段。基于连续渗流理论, 证明当授权用户较为稀疏或者负载较轻时, 非授权用户可以构建部分连通网络; 反之, 当授权用户较为密集并且负载较重时, 我们无法部署部分连通的非授权用户网络。进而, 在授权用户和非授权用户共享 1 个信道的情况下, 给出了非授权用户网络存在部分连通性的必要条件。仿真实验数据验证了理论分析的正确性。这些分析结论为部署动态频谱访问无线网络提供了技术依据。

参考文献

- [1] FCC Spectrum Policy Task Force. Report of the spectrum efficiency working group[R]. Nov. 2002
- [2] Haykin S. Cognitive radio; brain-empowered wireless communications[J]. Selected Areas in Communications, IEEE Journal on, 2005, 23: 201-220
- [3] Akyildiz I F, Lee W-Y, Vuran M C, et al. NeXt generation/dynamic spectrum access/cognitive radio wireless networks: a survey[J]. Comput. Netw., 2006, 50: 2127-2159
- [4] Cabric D, Tkachenko A, Brodersen R W. Experimental study of spectrum sensing based on energy detection and network cooperation[C]// Proceedings of the First International Workshop on Technology and Policy for Accessing Spectrum Boston, Massachusetts, ACM, 2006
- [5] Shen J, Jiang T, Liu S, et al. Maximum channel throughput via cooperative spectrum sensing in cognitive radio networks[J]. Trans. Wireless. Comm., 2009, 8: 5166-5175
- [6] Yucek T, Arslan H. A survey of spectrum sensing algorithms for cognitive radio applications[J]. Communications Surveys & Tutorials, IEEE, 2009, 11: 116-130
- [7] Etkin R, Parekh A, Tse D. Spectrum sharing for unlicensed bands[J]. Selected Areas in Communications, IEEE Journal on, 2007, 25: 517-528
- [8] Zhao Q, Swami A. A Survey of Dynamic Spectrum Access; Signal Processing and Networking Perspectives[C]// Acoustics, Speech and Signal Processing, 2007. ICASSP 2007. IEEE International Conference, 2007: IV-1349-IV-1352

(下转第 104 页)

中,

$$A = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}, b = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}。密码算法簇的新$$

S盒映射设定为 $f_1(g(f_2(x)))$, 逆S盒映射为 $f_2^{-1}(g(f_1^{-1}(x)))$, 其中 g 为有限域上的逆映射, f_1, f_2 为仿射变换。

为方便讨论, 取定 $f_1 = f, f_2: x \rightarrow y = x \oplus b$, 其中 b 由密钥 K_f 唯一指定, 这里设定每轮的 f 相同, 显然 $|K_f| = 2^{128}$, 当 b 取全零时, 密码算法簇中的该映射即为 AES 算法。

4.2 安全性分析

新S盒的非线性度由有限域上的乘法求逆变换决定, 增加一次仿射变换只会掩盖乘法求逆变换的代数结构, 而不会改变其非线性度。新S盒的代数次数在取定 f_2 变换的情况下, 可以通过 lagrange 插值公式求得。通过选取合适的仿射变换, 可以使得合成后的S盒有较高的代数次数。

仿照 AES 算法, 遵循宽轨迹策略, 可以得到算法的最大差分特征概率和最大线性特征概率, 从而可以分析算法簇抵抗差分密码分析和线性密码分析的能力。

4.3 实现效率分析

该算法簇的设计是, 在密钥不同的情况下, S盒的运算不同, 如果采用 LUT 方式实现S盒, 可采用分解运算的方式, 构造一个有限域乘法求逆运算的查找表, 其余的矩阵乘法和异或运算采用逻辑门实现, 其电路规模与基于 LUT 方式实现的 AES 算法相比, 只增加了少许基本门运算; 如果基于有限域运算实现S盒, 不同的 f_2 在变换相似的情况下, 电路规模与同样方法实现的 AES 算法几乎相同, 而新增的线性变化带来的电路时延也不大。

该实例除了S盒部件外, 其他部件的硬件实现都可参照

AES 算法, 根据上面的分析, 整个算法簇的硬件实现资源消耗和电路性能大致与 AES 算法相当。

结束语 密码设计一直是工程多于科学^[10]的一项工作, 从算法的应用中发现问题, 进而改进密码算法设计是密码学者必须进行的研究工作。我们给出可重构密码算法簇的概念, 提供了密码算法一种新的设计思路, 相关研究包括密码算法整体框架研究、算法模块的密码参数研究、密码算法的硬件实现效率等多方面内容, 涉及密码算法设计的各个方面, 通过对其进行深入探讨, 可加深对密码算法设计的认识。

参考文献

- [1] 高娜娜. 密码算法可重构性分析及高速可重构密码芯片研究[D]. 北京: 北京科技大学, 2005, 12
- [2] 姜晶菲. 可重构密码处理结构的研究与设计[D]. 长沙: 国防科技大学, 2004
- [3] 曲英杰. 可重组密码逻辑的研究与设计[D]. 北京: 北京科技大学, 2001
- [4] Schneier B. 应用密码学[M]. 吴世忠, 等译. 北京: 机械工业出版社, 2000
- [5] Menezes A J, van Oorschot P C, Vanstone S A. 应用密码学手册[M]. 胡磊, 等译. 北京: 电子工业出版社, 2005
- [6] Charney C, O'Connor L, Pieprzyk J, et al. Comments on Soviet encryption algorithm[C] // Advances in Cryptology-EUROCRYPT'94 (LNCS 950). 1995: 433-438
- [7] 张文涛. 分组密码的分析与设计[D]. 北京: 中国科学院, 2004
- [8] Hong S, Lee S, Lim J, et al. Provable Security against Differential and Linear Cryptanalysis for the SPN Structure[C] // Bruce Schneier, ed. Fast Software Encryption' 2000, LNCS 1978. Springer-Verlag, 2000: 273-283
- [9] Kang J S, Hong S, Lee S. Practical and provable security against differential and linear cryptanalysis for substitution-permutation networks[J]. ETRI journal, 2001, 23(4): 158-167
- [10] Daemen J, Rijmen V. 高级加密标准(AES)算法-Rijndael 的设计[M]. 谷大武, 等译. 北京: 清华大学出版社, 2003
- [11] Cordeiro C, Challapali K, Ghosh M. Cognitive PHY and MAC layers for dynamic spectrum access and sharing of TV bands[C] // Proceedings of the First International Workshop on Technology and Policy for Accessing Spectrum. Boston, Massachusetts: ACM, 2006
- [12] Cheng G, Liu W, Li Y, et al. Spectrum Aware On-Demand Routing in Cognitive Radio Networks[C] // New Frontiers in Dynamic Spectrum Access Networks, 2007. DySPAN 2007. 2nd IEEE International Symposium. 2007: 571-574
- [13] Feng Z, Yang Y. Joint transport, routing and spectrum sharing optimization for wireless networks with frequency-agile radios[C] // INFOCOM 2009. The 28th Conference on Computer Communications. IEEE, 2009
- [14] Ren W, Zhao Q, Swami A. Connectivity of cognitive radio networks: proximity vs. opportunity[C] // Proceedings of the 2009 ACM Workshop on Cognitive Radio Networks. Beijing, China: ACM, 2009
- [15] Xing F, Wang W. On the critical phase transition time of wireless multi-hop networks with random failures[C] // Proceedings of the 14th ACM International Conference on Mobile Computing and Networking. San Francisco, California, USA: ACM, 2008
- [16] Penrose M. Random Geometric Graphs[M]. Oxford University Press, 2003
- [17] Meester R, Roy R. Continuum percolation[M]. Cambridge University Press, 1996