基于分层编码的物理层安全多播算法

陈　雷*

(中国刑事警察学院公安情报学系　沈阳　110035)

【摘要】多播系统的保密容量受限于系统中最差用户的信道质量，并且传统的添加人工噪声的物理层安全单播技术不能直接应用于多播传输中。为了解决以上问题，该文提出一种基于分层编码的物理层安全多播算法。该算法在保障用户不同的保密 QoS 需求的前提下，最大化系统保密容量。从仿真分析看，本文的次优化算法的系统性能十分接近最优化算法，并且计算复杂度明显降低；与此同时，算法功效超出了传统安全多播算法。

关　键　词　人工噪声；　分层编码；　多播；　物理层安全

中图分类号　TN929.53　　**文献标志码**　A　　doi:10.12178/1001-0548.2018109

Layered Coding Based Physical Layer Secure Multicast Algorithm

CHEN Lei*

(Department of Public Security Intelligence, Criminal Investigation Police University of China　Shenyang　110035)

Abstract　The total security throughput of multicast group is limited by the users with the worst channel quality. Moreover, traditional the artificial noise of physical layer security techniques for unicast transmission, do not apply well to multicast transmission. To solve this problem, we consider a layered coding based physical layer secure multicast algorithm. The algorithm can max security throughput of the entire multicast group, while ensuring the security of all users' quality of service (QoS) requirements. The simulation results show that the performance gap between the optimal algorithm and the suboptimal algorithm is very small. Moreover, the computational complexity of suboptimal algorithm is obviously reduced. The proposed algorithm is much better than the conventional multicast security scheme (CMSS). In addition, it achieves more throughput than another algorithm.

Key words　artificial noise;　layered coding;　multicast;　physical layer security

基于正交频分多址 (orthogonal frequency division multiple access, OFDMA) 的多媒体广播/多播 (multimedia broadcast multicast service, MBMS) 技术[1] 是采用相同的时频资源为多个用户提供相同的服务。在现有的多播传输技术中，多播组的速率是以多播组中信道质量最差的用户所能正确接收数据的速率而发送的[2-3]。传统的多播传输技术的传输速率受限于组内最差的用户，严重影响整个多播系统的吞吐量。针对该问题，国内外学者提出了各种类型的资源分配方案来提升多播系统的性能，如：机会多播传输方案[4-5]、基于有限反馈多播资源分配方案[6-7]、基于分层编码的多播资源分配方案[8-9] 等。但这些分配方案，都没有考虑数据安全传输的问题。

近年来，无线物理层安全技术逐渐被人们所研究和利用，关于物理层安全传输技术的研究多集中在安全单播传输，主要采用添加人工噪声的技术[10-11]。如果安全单播传输技术被直接应用于多播传输中，它将不能在合法用户信道向量的正交空间中添加有效的人工噪声，从而不能保证数据的安全传输。针对该问题，文献 [12] 根据多播用户信道条件的不同，将子载波分配给不同的用户，以保证合法用户信道矢量的正交空间存在有效的人工噪声。文献 [13] 将 2 维波束赋形的 Alamouti 编码应用于安全多播中。文献 [14] 将多播用户分为多个多播簇，在每个簇中多播用户的信道矢量的正交空间中产生人工噪声，从而实现物理层安全多播传输。但这些研究都没有考虑如何在采用物理层安全传输的同时提升系统的保密容量的问题。

综上，本文将多播物理层安全传输技术与多播资源分配技术相结合。在单组多播系统中，结合分

收稿日期：2018－04－24；修回日期：2019－06－19
基金项目：辽宁省博士科研启动金 (201601083)；辽宁省自然科学基金 (20180550046)
作者简介：陈雷 (1981－)，男，博士后，主要从事无线资源分配、物理层安全及协作通信方面的研究. E-mail：chenleikb@bupt.edu.cn

层编码的特点，利用子载波分配算法构造合法用户的信道零空间，并将人工噪声技术引入零空间，保证多播系统的物理层安全传输。

1 系统模型

图1为本文研究的系统模型，在多播组中有K个多播用户和1个窃听者。在下行OFDMA单组多播系统中，以精细可伸缩视频编码(fine granular scalable, FGS)用于基站端。首先，原始多播数据被编码成一个基本层和多个增强层数据。基本层数据要求每个用户正确接收，增强层数据可以根据不同用户的不同信道条件进行接收。定义R^s_{base}表示系统要求的保密基本层速率，$R^{s-\text{req}}_k$表示满足用户k的保密QoS需求时所需要的保密速率，要求$R^{s-\text{req}}_k > R^s_{\text{base}}$。基站配置多根天线发送多播数据给多播组内的每个用户，每个用户采用单天线接收并且每个用户的保密QoS需求不同。假设发送基站配置的天线总数为M_t，多播组中窃听者的天线数目为M_e，并要求$M_e < M_t$。系统中基站端与接收用户间的通信链路都是慢时变块衰落信道，并且基站通过发送导频训练序列可准确地估计用户的信道状态信息(channel state information, CSI)。主信道定义为多播组内合法用户与基站间的无线链路，窃听信道定义为窃听者与基站间的无线链路。整个多播系统的带宽B被划分为N个子载波。假设每个用户反馈瞬时CSI和保密QoS需求给基站。定义P_T表示基站总的发射功率，p_n表示每个子载波所加载的功率。当M_t大于每次接收数据的用户数时，基站端在合法用户主信道的零空间产生人工噪声，然后将其与多播数据混叠后传输该信号。当信号通过主信道传输时，人工噪声由于处于主信道的零空间，因此不会干扰合法用户正确解码数据。但对于窃听信道而言，由于人工噪声一般不会处于窃听信道的零空间内，因此会对窃听者产生干扰，进而使窃听者的接收信噪比(signal noise ratio, SNR)恶化，无法正确解码数据，进而实现数据的安全传输。可见，基于人工噪声的物理层安全方法受限于M_t；当M_t小于每次接收数据的用户数时，信道增益矩阵$\boldsymbol{H}(\boldsymbol{H} \in \Re^{K\times M_t})$不存在零空间，就无法通过引入人工噪声的方法来提高保密速率。

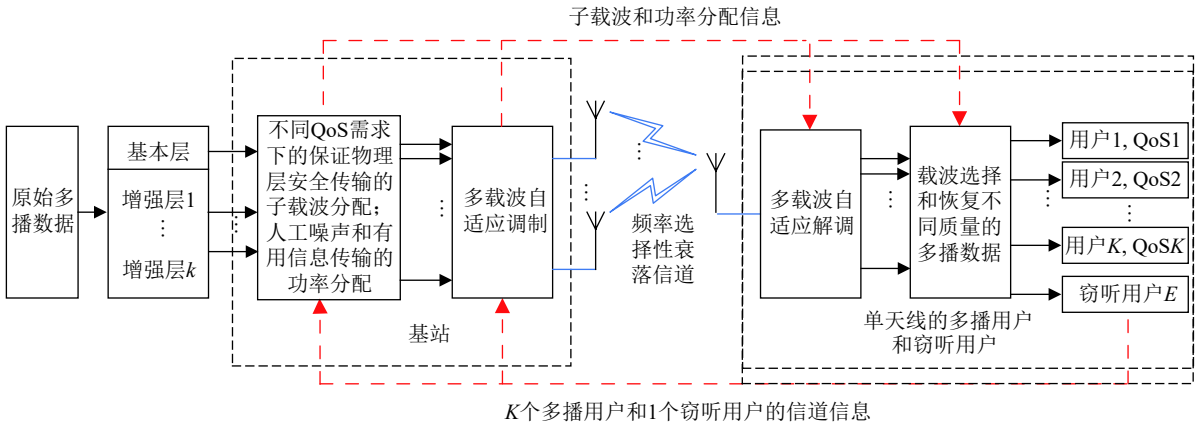

图1 采用分层编码的物理层安全多播系统模型

2 人工噪声分析及最优化问题式

2.1 添加人工噪声分析

定义用户k在子载波n上所对应的主信道与窃听信道增益矩阵分别为$H_{k,n}$和$H_{e,n}$；发送方在主信道的零空间内随机产生均值为0、方差为δ_v^2的人工噪声A_n，且满足$H_{k,n}A_n = 0$。为了在安全多播传输中使用人工噪声技术，首先需要保证在每次传输中基站发送天线数量多于合法多播用户的接收天线数量(每个载波能够服务的用户数为$L_n(L_n \leqslant M_t - 1)$个)，目的是确保传输所用子载波$n$上存在合法用户信道的零空间。其次，根据这$L_n$个合法用户反馈的瞬时CSI，在其信道零空间内引入人工噪声。因此，当使用子载波n时，定义多播组中的主信道与窃听信道的信道增益表示为：

$$\alpha_n = \min_{k\in L_n}\left\{\left|\boldsymbol{\omega}_n^{\mathrm{H}}\boldsymbol{H}_{k,n}\right|^2 \Big/ \delta_{b,n}^2\right\} \tag{1}$$

$$\beta_n = \left|\boldsymbol{\omega}_n^{\mathrm{H}}\boldsymbol{H}_{e,n}\right|^2 \Big/ (\delta_{e,n}^2 + \delta_v^2) \tag{2}$$

式中，$\left|\boldsymbol{\omega}_n^{\mathrm{H}}\boldsymbol{H}_{k,n}\right|^2$表示用户$k$与基站间在子载波$n$上的信道增益；$\boldsymbol{\omega}_n$为子载波$n$的波束赋形矢量；$\boldsymbol{H}_{k,n} = [h_{k,n,1} \quad h_{k,n,2} \quad \cdots \quad h_{k,n,M_t}]^{\mathrm{T}}$表示多播组中的第$k$

个用户在第 n 个子载波上的信道矢量，其中$h_{k,n,j}$表示用户 k 与基站端天线 j 之间在子载波 n 上的瞬时信道增益；$\delta_{b,n}^2$表示主信道中的加性高斯白噪声的方差；$\delta_{e,n}^2$表示窃听信道中的加性高斯白噪声的方差。

依据香农式计算子载波 n 的传输速率为：

$$R_n = \frac{B}{N}\log_2(1+p_n\alpha_n) \tag{3}$$

当系统中存在窃听者时，子载波 n 的保密容量表示为主信道传输速率与窃听信道传输速率之差：

$$R_n^s = \frac{B}{N}[\log_2(1+p_n\alpha_n)-\log_2(1+p_n\beta_n)]^+ \tag{4}$$

式中，符号R_n^s表示子载波 n 上的保密容量；$[x]^+=\max(0,x)$，$\alpha_n>\beta_n$。式 (4) 表示只有主信道的信道增益高于窃听信道时，才存在保密容量。

定义用户 k 在子载波 n 上的保密速率为：

$$R_{k,n}^s = \frac{B}{N}\left[\log_2\left(1+p_n\frac{\left|\omega_n^{\mathrm{H}}\boldsymbol{H}_{k,n}\right|^2}{\delta_{b,n}^2}\right)-\log_2(1+p_n\beta_n)\right]^+ \tag{5}$$

2.2　最优化问题式

本文提出的基于分层编码的物理层安全多播问题，是在基站端总的发射功率有限、多播合法用户信道条件优于窃听者信道条件，并保障每个合法用户保密 QoS 需求时保密容量最大化的最优化问题。因此，最优化问题式为：

$$\max_{p_n,w_{k,n}}\sum_{n=1}^{N}\sum_{k=1}^{K}R_{k,n}^s w_{k,n} \tag{6}$$

满足：

$$\alpha_n>\beta_n \tag{7}$$

$$\sum_{n=1}^{N}p_n\leqslant P_T \quad p_n\geqslant 0 \tag{8}$$

$$\sum_{n=1}^{N}\sum_{k=1}^{K}R_{k,n}^s w_{k,n}\geqslant R_k^{s-\mathrm{req}} \quad \forall k \tag{9}$$

$$w_{k,n}=\{0,1\} \quad \forall k,\forall n \tag{10}$$

$$1\leqslant\sum_{k=1}^{K}w_{k,n}\leqslant K \quad \forall n \tag{11}$$

如果用户 k 使用子载波 n，则 $w_{k,n}$ 为 1，否则为 0。式 (7) 表示合法用户信道条件优于窃听者信道条件；式 (8) 表示系统总功率受限；式 (9) 表示保证用户的保密 QoS 需求；式 (10) 表示子载波能够分配给哪些多播用户；式 (11) 表示子载波数量的限制。可知该最优化问题是一个非凸混合整数规划问题。

3　FGS 编码下保障安全多播的子载波及功率分配

3.1　最优子载波分配算法

本文提出一个保障物理层安全的最优子载波分配算法 (optimal subcarrier allocation with security scheme, OSASS)。因为计算线性整数规划问题的计算量要远小于与非凸混合整数规划问题[15]，所以为了将最优化问题中的目标函数即式 (6) 和限制条件式 (7)～(11)，转化为线性整数规划问题。将限定式 (5) 的结果向下取整数值，对于子载波的分配将采用遍历搜索的方法。这里对子载波的遍历搜索将有2^{2KN}种可能的分配方式。根据多播传输的特点可知，某些子载波的分配方式是不必要的，因此，将$R_{k,n}^s(k=1,2,\cdots,K)$ 递减排列，即$R_{l_1,n}^s\geqslant R_{l_2,n}^s\geqslant\cdots\geqslant R_{l_K,n}^s$。如果子载波 n 被分配给用户 l_k，这时对于用户索引号 $l_i>l_k$ 的用户也能以$R_{k,n}^s$的保密速率接收到该数据。在满足$L_n(L_n\leqslant M_t-1)$条件下，需要确定给哪些用户分配哪些子载波时，能够使系统的保密容量达到最大，所以，为了确定最优的子载波分配方式，就需要计算K^{2N}种分配方式。虽然该策略较穷举搜索法减少了计算量，但计算量仍然较大。

3.2　次优子载波分配算法

为了减少计算量，采用一种保障物理层安全的次优化子载波分配算法 (suboptimal subcarrier allocation with security scheme, SSASS)，该算法分为保密基本层算法和保障 QoS 需求的保密增强层算法。在次优化子载波分配阶段，为每个子载波设置相等的功率。因此最优化问题的式 (6)～(11) 可重新表示为：

$$\max_{w_{k,n}}\sum_{n=1}^{N}\sum_{k=1}^{K}R_{k,n}^s w_{k,n} \tag{12}$$

满足：

$$\sum_{n=1}^{N}p_n\leqslant P_T \quad p_n\geqslant 0 \tag{13}$$

$$\alpha_n>\beta_n \tag{14}$$

$$\sum_{n=1}^{N}\sum_{k=1}^{K}R_{k,n}^s w_{k,n}\geqslant R_k^{s-\mathrm{req}} \quad \forall k \tag{15}$$

$$w_{k,n}=\{0,1\}\quad \forall k,\forall n \tag{16}$$

$$1\leqslant\sum_{k=1}^{K}w_{k,n}\leqslant K\quad \forall n \tag{17}$$

1) 保密基本层算法

基于分层编码的特点，保密基本层数据将在保证安全传输的条件下，使用尽量少的子载波分配给所有的用户。

①初始化设置：$B=\{1,2,\cdots,K\}$，$A=\{1,2,\cdots,N\}$。$B_n=\min\limits_{k\in B}R_{k,n}^s$，$n\in A$，若$R_{\text{base}}^s\leqslant\sum\limits_{n=1}^{N}B_n$则转到步骤②，否则退出。

②当$A\neq\emptyset$时，由于传输采用时分的方式，因此，在T_1时隙，找到一个子载波n^*满足$n^*=\arg\max\limits_{n\in A}B_n$，将子载波$n^*$分配给信道质量较好的前$L_n(L_n\leqslant M_t-1)$个用户，如果有未被分配该子载波的用户，则在$T_2$时隙继续分配该子载波给剩余的用户，并要满足信道质量较好的前$L_n(L_n\leqslant M_t-1)$个用户，直到所有用户都被分配完毕；更新$R_{\text{base}}^s=R_{\text{base}}^s-B_{n^*}$，$A=A-\{n^*\}$；如果$R_{\text{base}}^s<0$，则计算剩余子载波的集合为$A^*=\{1,2,\cdots\}$；否则，返回到步骤②。

③K个用户都被分配完，并且任意用户满足$R_k^s\geqslant R_{\text{base}}^s$。

2) 保障QoS需求的保密增强层算法

在该算法中，根据每个用户的不同QoS需求和信道差异来传输增强层数据，通过子载波分配使得系统的保密容量最大化。用k_n表示子载波n传输数据的用户中信道质量最差的用户，$T_{k_n,n}^s$表示子载波n的保密吞吐量(即保密容量之和)。

①初始化设置：对$R_k^{s-\text{req}}$按递减排序，选取$R_k^{s-\text{req}}$最大的用户k，进行增强层子载波分配，对用户k上可用的子载波的保密速率$R_{k,1}^s,R_{k,2}^s,\cdots,R_{k,N}^s$ ($k\in B$，$n\in A^*$) 按递减次序排列。

②当$A^*\neq\emptyset$时，计算$T_{k_n,n}^s=\sum\limits_{k=1}^{K}R_{k_n,n}^s1(R_{k,n}^s\geqslant R_{k_n,n}^s)$。$1(A)$表示当满足条件$A$时，$1(A)$值为1，否则为0。找到一个用户满足$k^*=\arg\max\limits_{k_n\in B}T_{k_n,n}^s$，设置$w_{k,n}=\begin{cases}1 & R_{k,n}^s\geqslant R_{k_n^*,n}^s\\ 0 & \text{其他}\end{cases}$，并判断子载波$n$能被分配的用户数$L_n$是否满足$L_n(L_n\leqslant M_t-1)$，如果满足则进行分配，更新$R_k^{s-\text{req}}=R_k^{s-\text{req}}-R_{k^*,n}^s$，返回步骤①；否则将排除被分配的用户中保密速率最小的用户，并重新进行判断条件$L_n(L_n\leqslant M_t-1)$，直到满足条件。

③N个子载波都被分配完毕。

3.3 加入人工噪声的功率分配算法

在次优化子载波分配阶段，假设每个子载波等功率，这种功率分配方式并不能最优地利用有限的功率，因此在功率分配阶段，研究了加入人工噪声时的功率分配算法 (power allocation base on artificial noise, PAAN)。这时最优化问题的式(12)～(17)又可以重新表示为：

$$\max_{p_n}\sum_{n=1}^{N}\sum_{k=1}^{K}R_{k,n}^s \tag{18}$$

满足：

$$\sum_{n=1}^{N}p_n\leqslant P_T\quad p_n\geqslant 0 \tag{19}$$

功率分配问题可采用拉格朗日方法求解，构造式(18)的拉格朗日算子函数：

$$L(p_n,\lambda)=\sum_{n=1}^{N}\sum_{k=1}^{K}R_{k,n}^s-\lambda\left(\sum_{n=1}^{N}p_n-P_T\right) \tag{20}$$

式中，λ为拉格朗日算子。对式(20)中的L求偏导，即：

$$\frac{\partial L}{\partial p_n}=\frac{\alpha_n}{1+p_n\alpha_n}-\frac{\beta_n}{1+p_n\beta_n}-\lambda=0 \tag{21}$$

每个子载波上可分配的功率表示为：

$$p_n=\frac{\sqrt{(\alpha_n-\beta_n)^2+4\alpha_n\beta_n\left(\frac{\alpha_n-\beta_n}{\lambda}\right)}-\alpha_n-\beta_n}{2\alpha_n\beta_n} \tag{22}$$

可将式(22)代入式$\sum\limits_{n=1}^{N}p_n=P_T$来求解$\lambda$。

1) 初始化设置：

初始化λ，根据多播用户反馈的CSI计算载波的信道增益，如果$\alpha_n>\beta_n$，则执行步骤2)，否则结束PAAN功率分配过程；

2) 根据式(22)计算分配给各载波的功率，若满足式$\sum\limits_{n=1}^{N}p_n=P_T$，则执行步骤3)，否则重新选取拉格朗日算子$\lambda$，重复步骤1)；若每个载波加载的功率$p_n\geqslant 0$，则PAAN算法结束；否则重新回到步骤2)。

3) 所有的p_n都大于等于0。

4 仿真结果与分析

将本文算法、文献[15]中的算法、传统安全多播传输算法 (conventional multicast with security scheme, CMSS) 进行仿真对比。文献[15]的算法

中，在子载波等功率分配时，采用 3 步次优化算法进行子载波的分配。采用图 1 所示的仿真场景。合法用户的平均 SNR 表示为 SNRB，窃听者的平均 SNR 表示为 SNRE。根据 3GPP 标准规定的城市部署场景[16]，表 1 列出了仿真实验的仿真参数。

表 1　仿真参数

参数	参数值
小区半径/km	1
路损指数	3
总的子载波数目	64
基站发射功率/W	10
载波频率/GHz	2
加性高斯白噪声单边功率谱密度/dBW·Hz^{-1}	−90
子载波带宽/MHz	0.2
多播组总用户数	30
基站天线数	8

在仿真过程中，信道模型采用复合信道衰落模型，信道模型由大、中、小尺度衰落组成。设置大尺度衰落的路径损耗指数为 3、中等尺度的阴影衰落指数为 8，小尺度衰落指数为均值为 0 和方差为 1 的复高斯随机变量，其幅度服从瑞利分布。用户随机分布在小区覆盖的范围内。

图 2 比较了本文的 OSASS-PAAN 算法、SSASS-PAAN 算法、SSASS 算法、文献 [15] 的算法、CMSS 算法在窃听方的 SNRE=3 dB、合法用户 SNRB 增大的情况下，系统总的保密容量的变化情况。仿真显示，在合法用户的 SNRB 增大的情况下，OSASS-PAAN 算法与 SSASS-PAAN 算法之间的差距逐渐减少。这说明 SSASS-PAAN 算法是合理可行的。CMSS 算法实现的保密容量远低于本文算法，这是因为本文算法通过 FGS 分层编码，能够获得来自不同信道条件的多用户的分集增益，通过仿真还可以看到添加功率分配算法的保密容量要高于没有功率分配算法的保密容量。而 CMSS 算法系统保密容量受限于多播组中信道质量最差的用户，并且 CMSS 算法中每个子载波采用的是等功率的分配方式，没有根据不同用户的信道条件有效的利用好有限的功率。

图 3 仿真了当多播用户数目增多时，5 种算法的系统保密容量的变化情况。在窃听方的 SNRE=3 dB、合法用户 SNRB=15 dB 时，除 CMSS 算法以外其余 4 种算法，都随着用户数的增加系统保密容量也在不断增加。但采用 CMSS 算法时系统保密容量将达到饱和。这是因为 OSASS-PAAN/SSASS-PAAN 算法与 SSASS 算法均使用了 FGS 分层编码，克服了系统性能受限于多播组中信道质量最差用户的情况，因此获得了编码增益。从仿真分析还可以看出本文算法与 CMSS 算法相比，更适合多播组用户数较多的场景。另外，在系统保密容量上，SSASS-PAAN 算法、SSASS 算法的系统性能都高于文献 [15] 的算法，原因是这两种算法不限制子载波的保密速率必须取整数值，然而文献 [15] 的算法限定了子载波的保密速率的取值范围，因此损失掉了一部分系统性能。

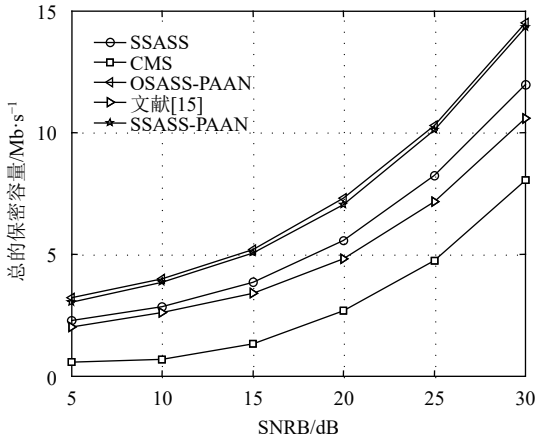

图 2　合法用户平均信噪比 (SNRB) 与系统总保密容量的关系 (N=16，K=6)

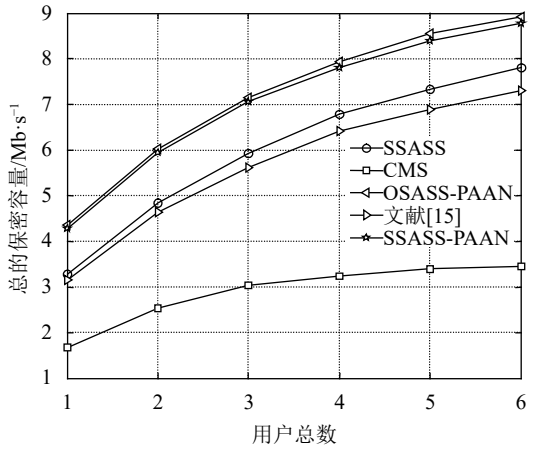

图 3　用户数与系统总保密容量的关系 (N=8)

图 4 比较了用户总数目增加时，有不同保密 QoS 需求的 3 个合法多播用户的保密速率的变化情况。在窃听方的 SNRE=3 dB、合法用户 SNRB=15 dB 时，假设用户 1、用户 2 和用户 3 有不同的保密 QoS 需求。用户 1 到用户 3 的保密 QoS 需求$R_1^{s-\mathrm{req}}$、$R_2^{s-\mathrm{req}}$和 $R_3^{s-\mathrm{req}}$分别是 0.31 Mb·s^{-1}、0.27 Mb·s^{-1} 和 0.18 Mb·s^{-1}。而其他用户有相同的保密 QoS 需求即 $R_k^{s-\mathrm{req}}$=0.15 Mb·s^{-1} ($k \neq 1,2,3$)。规定所有多播用户的

R^s_{base}是 0.09 Mb·s^{-1}。通过仿真可知当用户数目增多时，3 个用户的保密速率依次降低到 0.31 Mb·s^{-1}、0.27 Mb·s^{-1} 和 0.18 Mb·s^{-1}。当用户数继续增加时，这 3 个用户的保密速率继续降低到 0.09 Mb·s^{-1}。从仿真可以看到本文算法的可行性，当用户增多时，用户的保密速率首先降低到各自的保密 QoS 需求的速率，之后再降低到保密基本层速率，这与本文采用的 FGS 分层编码的特点相一致。

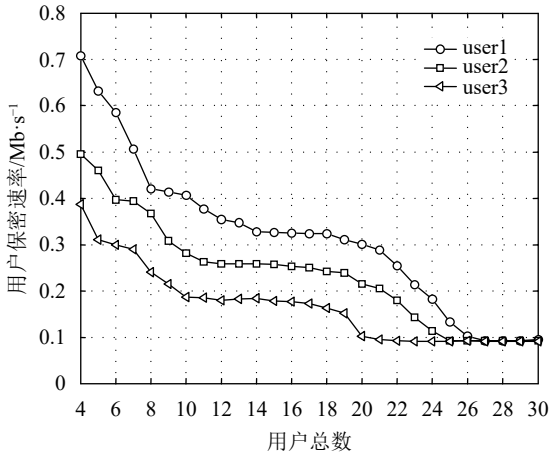

图 4 用户数与用户保密速率的关系 (N=64，K=6)

图 5 给出了 K=4、窃听方的 SNRE=25 dB 时，SSASS-PAAN 算法下的系统保密速率与子载波数目变化的关系。N=1 时表示单播传输模式，系统中只有一个子载波可以使用，在该子载波上如果合法用户的信道质量低于窃听者的信道质量，根据式 (4) 的分析可知，此时不能采用物理层安全传输技术，所以系统保密速率为零。当系统中可以利用的子载波有越多时，合法用户的信道质量高于窃听者的信道质量的概率也会越来越大，此时将人工噪声技术添加到合法用户的信道零空间来降低窃听者接收信号的信噪比，从而确保安全多播系统的保密传输速率。

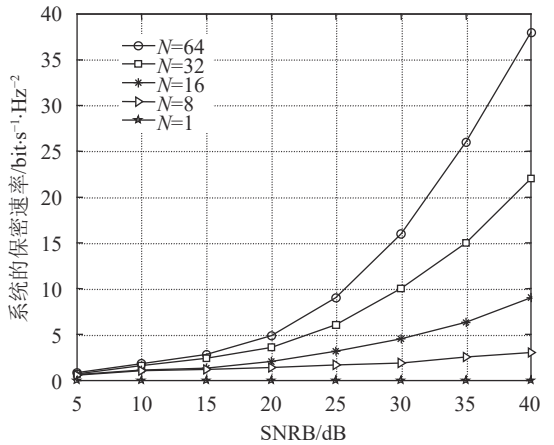

图 5 载波数与保密速率的关系

表 2 比较了 CMSS 和 SSASS-PAAN 所需的平均计算时间占最优化算法 OSASS-PAAN 所需的平均计算时间的比例。可以看到 OSASS-PAAN 算法复杂度高，计算时间长。SSASS-PAAN 算法的复杂度低，计算时间短，仅为 OSASS-PAAN 算法的 61%～84%。

表 2 CMSS 算法、SSASS-PAAN 算法与 OSASS-PAAN 算法平均计算时间对比

P_T(W)	平均计算时间占比/%	
	CMSS	SSASS-PAAN
2	58.67	60.47
6	69.41	71.98
10	80.13	83.23

5 结 束 语

本文提出了一个基于分层编码的物理层安全多播资源分配算法。该算法采用 FGS 分层编码来提升多播系统保密容量，并在多播传输中添加人工噪声作为物理层传输技术。针对最优化求解计算复杂度高的问题，提出了一种低复杂度的两阶段次优化算法，分为保障安全多播的子载波分配阶段和加入人工噪声的功率分配阶段。仿真可知，虽然所提出的最优化算法比次优化算法的系统性能略高，但次优化算法的计算时间要远低于最优化算法，而且所提出的算法所达到的系统性能要远远超过传统安全多播算法，也比文献 [15] 的算法有更好的系统功效。

本文研究工作还得到中国刑事警察学院 2019 年重大项目培育计划 (D201902001) 的资助，在此表示感谢。

参 考 文 献

[1] JEAN-MARIE V, SAVIOUR Z. A survey of multicasting over wireless access networks[J]. IEEE Communications Surveys & Tutorials, 2013, 15(2): 718-753.

[2] VARSHNEY U. Multicast over wireless networks[J]. IEEE Communications of the ACM, 2012, 45(12): 31-37.

[3] ZHANG H, WANG X, LI F., et al. Channel-aware adaptive resource allocation for multicast and unicast services in orthogonal frequency division multiplexing systems[J]. IEEE IET Communications, 2012, 6(17): 3006-3014.

[4] MA Y, LETAIEF K, WANG Z. Multiple description coding-based optimal resource allocation for OFDMA multicast service[C]//IEEE Global Telecommunications Conference. [S.1.]: IEEE, 2010: 1-5.

[5] SUH C, MO J. Resource allocation for multicast services in multicarrier wireless communications[J]. IEEE

Transactions on Wireless Communications, 2008, 7(1): 27-31.

[6] LEI C, WANG X, HE G. Dynamic resource allocation with precoding and joint coding scheme for limited feedback-based multi-antenna wireless multicast systems[J]. IET Communications, 2013, 7(5): 397-407.

[7] JEON J, SON K, LEE H, et al. Feedback reduction for multiuser OFDM systems[J]. IEEE Transactions on Vehicular Technology, 2010, 59(1): 160-169.

[8] 陈雷, 王洪玉. 应用分层编码保障组播系统 QoS 的高效资源分配[J]. 北京邮电大学学报, 2014, 37(4): 64-68.
CHEN Lei, WANG Hong-yu. Efficient resource allocation based on layered coding in multicast systems with QoS guarantee[J]. Journal of Beijing University of Posts and Telecommunications, 2014, 37(4): 64-68.

[9] CARLA L, CHITI F, FANTACCI R, et al. Power efficient resource allocation strategies for layered video delivery over eMBMS network[C]//IEEE International Conference on Communication. [S.1.]: IEEE, 2014: 3505-3510.

[10] 洪涛, 李志鹏. 人工噪声辅助物理层安全通信系统峰均比[J]. 系统工程与电子技术, 2016, 38(11): 2653-2659.
HONG Tao, LI Zhi-peng. Research of the peak to average power ratio problem for physical layer security communication system aided by artificial noise[J]. Systems Engineering and Electronics, 2016, 38(11): 2653-2659.

[11] WEI D, LILI L, MENG Z. A polarization state modulation based physical layer security scheme for wireless communications[C]//IEEE Military Communications Conference. [S.1.]: IEEE, 2016: 1195-1201.

[12] 林通, 黄开枝, 罗文宇. 一种基于多载波的多播系统物理层安全方案[J]. 电子与信息学报, 2013, 35(6): 1338-1343.
LIN Tong, HUANG Kai-zhi, LUO Wen-yu. A multicarrier based physical layer security scheme for the multicast systems[J]. Journal of Electronics & Information Technology, 2013, 35(6): 1338-1343.

[13] ZHU B, GE J, HUANG Y. Rank-two beamformed secure multicasting for wireless information and power transfer[J]. IEEE Signal Process Letter, 2014, 21(2): 199-203.

[14] 陈雷. 基于用户分簇的物理层增强安全多播算法[J]. 工程科学与技术, 2017, 49(6): 1-7.
CHEN Lei. A physical layer enhanced secure multicast algorithm based on user clustering[J]. Advanced Engineering Sciences, 2017, 49(6): 1-7.

[15] LIN T, DI P, YUBO Y. Subcarrier allocation for multicast services in multicarrier wireless systems with QoS guarantees[C]//IEEE Wireless Communications and Networking Conference.[S.1.]: IEEE, 2010: 1-6.

编　辑　叶　芳