Hans Journal of Wireless Communications 无线通信, 2016, 6(2), 61-71
Published Online April 2016 in Hans. http://www.hanspub.org/journal/hjwc
http://dx.doi.org/10.12677/hjwc.2016.62009

Hans汉斯

A New SFBC Combined Physical Layer Transmission Scheme for LPI and High Throughput in the Cooperative SC-FDMA System

Chao Wu[1,2], Dashuang Chen[1], Yali Shang[1], Haiyue Li[1], Yingshan Li[1]

[1]Department of Communication Engineering, College of Electronic Information and Optical Engineering, Nankai University, Tianjin
[2]Department of Mechanical and Electrical Engineering, Shijiazhuang Vocational College of Scientific and Technical Engineering, Shijiazhuang Hebei
Email: yingsl1122@nankai.edu.cn

Received: Apr. 3rd, 2016; accepted: Apr. 24th, 2016; published: Apr. 27th, 2016

Abstract

In recent days, cooperative diversity and communication security become important research issues for wireless communications. In this paper, to achieve LPI (low probability of interception) and high throughput in the cooperative SC-FDMA (Single-Carrier Frequency Division Multiple Access) system, a new SFBC combined physical layer transmission scheme is proposed, where, a new SFBC combined encryption algorithm is applied, adaptive modulation based on CSI (channel state information) is further considered. By doing so, neither relay node nor eavesdropper intercepts the information signals transmitted from UT (user terminal). Simulation results show above new SFBC combined physical layer transmission scheme can bring in higher transmission safety and secrecy rate, further derive better transmission performance and transmission throughput.

Keywords

LPI, Cooperative Transmission, SFBC, SC-FDMA, Encryption

上行SC-FDMA协作通信系统中联合SFBC编码的物理层加密传输方案

文章引用: 吴超, 陈大爽, 商亚莉, 李海月, 李英善. 上行 SC-FDMA 协作通信系统中联合 SFBC 编码的物理层加密传输方案[J]. 无线通信, 2016, 6(2): 61-71. http://dx.doi.org/10.12677/hjwc.2016.62009

吴　超[1,2]，陈大爽[1]，商亚莉[1]，李海月[1]，李英善[1]

[1]南开大学电子信息与光学工程学院通信工程系，天津
[2]石家庄科技工程职业学院机电工程系，河北 石家庄
Email: yingsl1122@nankai.edu.cn

收稿日期：2016年4月3日；录用日期：2016年4月24日；发布日期：2016年4月27日

摘　要

当前协作通信的多样性和安全性已成为越来越重要的问题。在本论文中，为了在上行SC-FDMA (单载波频分多址)协作通信系统中达到低截获概率(LPI)，低误比特率和高吞吐量的目的，我们提出了一种新的联合SFBC编码的物理层加密传输方案，将SFBC编码联合用于物理层加密算法，并接着与自适应编码调制相结合。运用我们新提出的联合SFBC编码的物理层加密传输方案，无论是RN还是窃听者都不能从发射机(UT)获取任何有用信息。实验结果表明，联合SFBC编码的物理层加密传输方案可以进一步提高信息传输的安全性，得到很好的保密速率，并且进一步提高系统的传输性能和吞吐量。

关键词

LPI，协作通信，SFBC，SC-FDMA，加密

1. 介绍

SC-FDMA (单载波频分多址)技术被 3GPP 组织采用为 LTE (Long Term Evolution，长期演进)上行链路空中接口技术标准。SC-FDMA 可以有效的降低移动终端的 PAPR (峰值平均功率比)，提高移动终端的电池效率。

协作分集作为无线通信的新技术已经获得了社会的广泛关注。协作通信技术利用空间协作分集增益，可以在不添加额外天线的情况下提供与先前通信系统相同的可靠性。因此在 SC-FDMA 上行链路传输系统中，协作分集可以看作是一个高效的 QoS (服务质量)传输方案。但是必须考虑中继节点(RN)和窃听者窃听的风险性，并保证信号传输的可靠性和安全性[1]。

信号传输安全性是当前无线通信研究的热点之一，由于无线信道的开放特性和广播特性，信息安全问题变得越来越重要。利用无线信道的物理特性进行加密，保证信号传输安全最近备受关注。

与有线通信系统不同，在无线通信系统中，任何信号传输广播范围内的接收机或者窃听者都能够接收、监听或者分析信号，使得无线通信的保密安全性极其脆弱。高层加密数据是一种较为有效的加密方式，但由于高层加密算法本身存在的缺陷，所以很容易被破解，物理层加密算法可以克服高层加密的诸多缺点，目前得到了广泛的应用和研究。

在文献[2]中，Wyner 指出在 wire-tap 信道中，信源和信宿可以进行完全安全的信息传输，而窃听者检测不到任何有用信息。在文献[3] [4]中，Wyner 的结论分别延伸到高斯(Gaussian) wire-tap 信道和广播信道当中。在文献[5] [6]中，Li.H. Wu 和 Ratazzi 解决了在 MIMO 无线通信系统中无需对高层协议数据加密而实现 LPI 的问题。他们通过在物理层随机化发送信号，来达到防止窃听的目的。在文献[7] [8]中，Zheng Li 和 Xiang-Gen Xia 设计了一个物理层传输方案，在协作通信系统中实现 LPI。他们提出了一种有效的信号随机方法，对于窃听者接收到的信号实现随机化，但授权的接收器可通过算法解密接收到的信号。即窃听者

不能检测到所接收的符号，而授权的接收器可以在不知道信道状态信息的情况下正确解码，接收传输信号。

在本文中，为了实现协作 SC-FDMA 通信系统的 LPI 和高吞吐量，我们提出了一种新的联合 SFBC 编码的物理层加密传输方案，将 SFBC 编码联合用于物理层加密算法，并接着与自适应编码调制相结合。首先从授权的接收终端发送已知的训练序列至发射机，从而发射机通过计算得知信道状态信息(CSI)，而接收机并不知道任何有关的 CSI。发射机先对发送数据进行 SFBC 编码，接着根据 CSI 设计区分不同用户的随机加权系数，还据此进行自适应编码调制以提高系统的吞吐量。

本章组织如下：在第 2 节描述 SFBC 编码上行 SC-FDMA 协作通信物理层加密系统的模型。在第 3 节，论述联合 SFBC 编码的物理层加密算法。在第 4 节给出相应的性能仿真结果。最后在第 5 节给出相应结论。

2. 系统模型

2.1. SC-FDMA 系统

SC-FDMA 是一种能够在未来的蜂窝系统中进行高数据速率传输且很有前途的技术。它显示了良好的频谱效率，良好的对频率选择性衰落的鲁棒性。特别是，与先前的 OFDM 相比，SC-FDMA 具有低的 PAPR 特性。在频域中，多个用户变换的时域符号分别通过 DFT 处理块，以得到频域的子载波。然后将每个用户的子载波映射到一个预先分配的系统的频谱部分，像在普通的 OFDM 系统一样进行 IFFT 变换和 CP 插入。SC-FDMA 传输方案相比 OFDM 系统明显降低 PAPR，从而降低移动设备的功耗。

2.2. 联合 SFBC 编码的物理层加密算法用于上行链路 SC-FDMA 协作系统的方案

如图 1 所示为 SFBC 编码上行链路 SC-FDMA 物理层加密协作通信系统，假设只有一个信源和一个中继节点。基站(BS)为授权的接收机，发射机(UT)附近存在一个窃听者。h_1 是“直连信道”，其信道状态信息为 CSI_1，h_2 是“中继信道”，其信道状态信息为 CSI_2，h_3 是“用户间信道”，其信道状态信息为 CSI_3，h_4 是“窃听者信道”，其信息状态信息为 CSI_4。

假定在通信过程中采用半双工传输模式，并将时隙分为三个阶段。如表 1 所示。

时隙 1 分成两个子时隙。在时隙 1 的子时隙 1，BS 发送训练序列到 UT 和 RN。假设信道状态在信道估计后的短暂时间内不变，则 UT 获得精确的 CSI_1，RN 获得精确的 CSI_3。然后在时隙 1 的子时隙 2，RN 发送训练序列和 CSI_3 到 UT，UT 获得精确的 CSI_2 和 CSI_3。至此，UT 获取了所有三个信道状态信息 CSI_1，CSI_2，CSI_3。

在时隙 2 和时隙 3 期间，UT 根据状态信息 CSI_i (i = 1, 2, 3)获知各个信道的信道质量，并根据最差的信道质量采用集中式自适应编码方式，将传输信息编码为 QPSK，16QAM 或者 64QAM 中的一种。之后根据“直连信道”和“中继信道”的 CSI，对两条传输信道分别进行联合 SFBC 编码的物理层加密并传输。

在时隙 3，将 RN 接收到的 UT 信号转发到 BS。最后在 BS 端，将从 UT 和 RN 接收到的信号根据联合 SFBC 编码的物理层解密算法进行解密。

图 2 为采用联合 SFBC 编码的物理层加密算法的 SC-FDMA 系统方框图。

3. 联合 SFBC 编码的物理层加密传输方案

联合 SFBC 编码的物理层加密传输方案如下：

UT 端首先对发送数据进行 SFBC 编码，该方案如表 2 所示，s_0 作为参考信号，$s_k\,(k=1,2,3,\cdots N-1)$ 作为有用信息。只是在时隙 2 中，子载波 0 发送的是有用信号 s_1，而子载波 1 传输的是参考信号 s_0^*；而

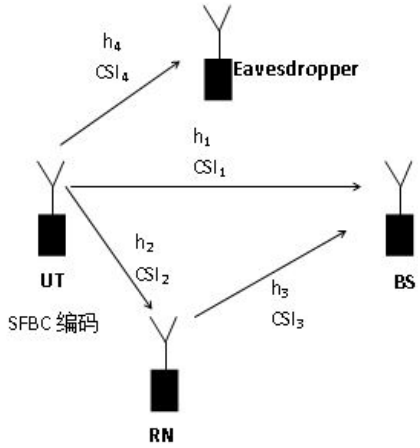

Figure 1. Model of the SFBC combined physical layer encryption algorithm in the cooperative SC-FDMA system
图 1. 联合 SFBC 编码的物理层加密算法用于上行链路 SC-FDMA 协作系统的模型

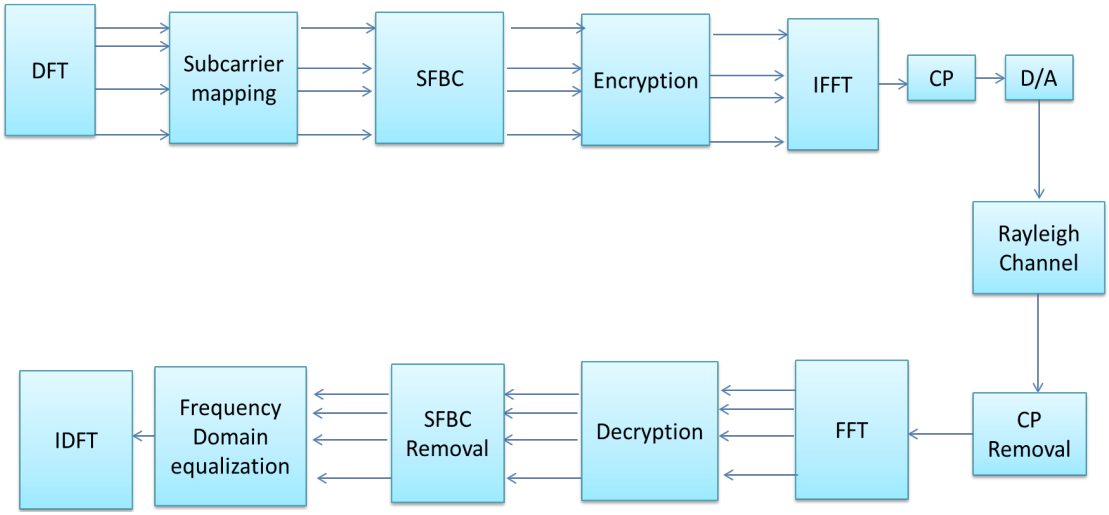

Figure 2. SFBC combined physical layer encryption algorithm in the cooperative SC-FDMA system
图 2. 采用联合 SFBC 编码的物理层加密算法的 SC-FDMA 系统

Table 1. The slot of cooperative communication system
表 1. 协作通信系统时隙

时隙 1		时隙 2	时隙 3
子时隙 1	子时隙 2		
获取 CSI_1	获取 CSI_2 和 CSI_3	联合 SFBC 编码的物理层加密、自适应调制，发送到 RN	联合 SFBC 编码的物理层加密、自适应调制，发送到 BS
取 CSI_3	送训练序列和 CSI_3 到 UT	从 UT 接收信号	转发信号到 BS
送训练序列到 UT 和 RN			从 UT、RN 接收信号

Table 2. SFBC encoder transmission slot
表 2. SFBC 编码传输时隙

	时隙 2							时隙 3						
子载波索引	0	1	2	3	…	$N-2$	$N-1$	0	1	2	3	…	$N-2$	$N-1$
UT→BS								s_0	$-s_1^*$	s_2	$-s_3^*$	…	s_{N-2}	$-s_{N-1}^*$
UT→Relay	s_1	s_0^*	s_3	s_2^*	…	s_{N-1}	s_{N-2}^*							

在时隙 3 中，子载波 0 发送的是参考信号 s_0，而子载波 1 传输的是有用信号 $-s_1^*$。

本小节，为了在上行 SC-FDMA 协作通信系统中达到 LPI，我们提出了一个新的基于 CSI 的联合 SFBC 编码的物理层加密算法。通过设计“随机”的加密权重系数使得接收机 BS 能正确解码，而 RN 和窃听者不能得到任何有用信息。

文献[7] [8]论述了在 OFDM 系统中，假定所有的 RN 是可信任的，通过多个 RN 构成 STBC 阵列传输的物理层加密算法，但这样有一半的传输符号被用作参考符号，降低了信号传输的效率，同时对于 RN 来说，信号是可知的，如果 RN 是不安全的，容易造成信息被窃听和盗取。

与之前的文献相比，本论文假设 RN 是不可信的，同时为了提高信号传输效率，我们只采用一个子载波来传输参考符号。因此无论是窃听者还是 RN 都不能获取 UT 发来的任何有用信息。

3.1. SFBC 物理层加密具体过程

1) 如表 2 所示，对 UT 信息进行 SFBC 编码。

2) 在时隙 2 期间，UT 发送的信息通过随机权重系数 λ_i 加密，并发送到 RN。

3) 在时隙 3 期间，UT 发送的信息通过随机权重系数 ω_i 加密，并发送到 BS。

即发送到 RN 和 BS 的信息在时隙 2 和时隙 3 的两个子时隙被分别有序的加密。

在 UT 端的加密算法如下所示：

1) 在经过时隙 1 的信道估计之后，UT 获取了状态信息 CSI_1，CSI_2 和 CSI_3，而 RN 不知道 CSI_2，BS 不知道任何 CSI_i ($i=1$，2，3)。

2) UT 发送信号的 N 个子载波($i=0,1,2,\cdots,N-1$)被分为两组。参考符号组(子载波 $i=0$)和信息符号组(其他子载波 $i=1,2,3,\cdots,N-1$)。

3) 随机权重加密系数 ω_i 和 λ_i 定义如下：

$$|\omega_i||h_{1,i}| = |\omega_0||h_{1,0}| = C; (1 \le i \le N-1) \tag{1}$$

$$|\lambda_i||h_{2,i}||h_{3,i}| = |\lambda_1||h_{2,1}||h_{3,1}| = D; (0 \le i \le N-1, i \ne 1) \tag{2}$$

ω_i 是直连信道的随机权重加密系数，λ_i 是中继信道的随机权重加密系数。$h_{m,i}$ 表示信道 $m(m=1,2,3)$ 的子载波 $i(i=0,1,\cdots,N-1)$上的复数瑞利平坦衰落信道。C 和 D 是正数。

可以根据实际的传输信号功率以及直连信道和中继信道功率分配比率来设计 C 和 D 的数值，为了简化，我们假定 $C=D$。

为了限制总功率，随机权重加密系数设计如下：

$$\begin{aligned} &|\omega_i||h_{1,i}| = |\lambda_i||h_{2,i}||h_{3,i}| = C, \ (0 \le i \le N-1) \\ &|\omega_i|^2 + |\lambda_i|^2 = 2 \end{aligned} \tag{3}$$

再根据式(1)，(2)计算可得：

$$\begin{aligned} |\omega_i| &= \frac{C}{|h_{1,i}|} \\ |\lambda_i| &= \frac{C}{|h_{2,i}||h_{3,i}|} \\ C &= \frac{\sqrt{2}|h_{1,i}||h_{2,i}||h_{3,i}|}{\sqrt{|h_{1,i}|^2 + |h_{2,i}|^2|h_{3,i}|^2}} \end{aligned} \tag{4}$$

随机权重加密系数 ω_i 和 λ_i 的相位可以认为是均匀分布，可以如下设计：

$$\begin{aligned}&\omega_i h_{1,i} = \omega_0 h_{1,0} = C\mathrm{e}^{j\varphi_1};\left(\varphi_1 \in (0,2\pi)\right)\\&\theta_{\omega_i} = \varphi_1 - \theta_{h_{1,i}}\left(0 \le i \le N-1\right)\end{aligned} \tag{5}$$

$$\begin{aligned}&\lambda_i h_{2,i} h_{3,i} = \lambda_0 h_{2,1} h_{3,1} = D\mathrm{e}^{j\phi_2};\left(\phi_2 \in (0,2\pi)\right)\\&\theta_{\lambda_i} = \phi_2 - \theta_{h_{2,i}} - \theta_{h_{3,i}}\left(0 \le i \le N-1\right)\end{aligned} \tag{6}$$

如上述分析推导，物理层加密算法的随机权重加密系数 ω_i 和 λ_i 设计完成。

3.2. 联合 SFBC 编码的物理层解密算法具体过程

首先，让我们考虑直连信道。在 BS 端的接收信号偶数子载波的接收信号可写为：

$$y_{1,2k} = h_{1,2k}\omega_{2k}s_{2k} + n_{1,2k},\left(k = 0,1,2,\cdots,(N-2)/2\right), \tag{7}$$

BS 上接收的奇数子载波的接收信号可写为：

$$y_{1,2k+1} = -h_{1,2k+1}\omega_{2k+1}s_{2k+1}^{*} + n_{1,2k+1}\left(k = 0,1,2,\cdots,(N-2)/2\right), \tag{8}$$

特别要指出 BS 上接收的第 0 位偶数子载波(即 $k=0$)传输的为参考信号 s_0，接收信号可写为：

$$y_{1,0} = h_{1,0}\omega_0 s_0 + n_{1,0}, \tag{9}$$

当 $h_{1,0}\omega_0 = h_{1,2k}\omega_{2k}$ 的时候，在 BS 端接收偶数子载波信号为：

$$y_{1,2k} = \frac{s_{2k}}{s_0}y_{1,0} + \left(n_{1,2k} - \frac{s_{2k}}{s_0}n_{1,0}\right),\left(k = 1,2,\cdots,(N-2)/2\right) \tag{10}$$

我们可以用最大似然法(ML)解码符号：

$$\widehat{s_{2k}} = \arg\min_{s_{2k}}\left\|y_{1,2k} - \frac{\widehat{s_{2k}}}{s_0}y_{1,0}\right\|_F^2,\left(k = 0,1,2,\cdots,(N-2)/2\right) \tag{11}$$

当 $h_{1,0}\omega_0 = h_{1,2k+1}\omega_{2k+1}$ 的时候，在 BS 端接收奇数子载波信号为：

$$y_{1,2k+1} = -\frac{s_{2k+1}^{*}}{s_0}y_{1,0} + \left(n_{1,2k+1} - \frac{-s_{2k+1}^{*}}{s_0}n_{1,0}\right),\left(k = 0,1,2,\cdots,(N-2)/2\right) \tag{12}$$

我们可以用最大似然法(ML)解码符号：

$$-\widehat{s_{2k+1}^{*}} = \arg\min_{s_{2k+1}}\left\|y_{1,2k+1} - \frac{-\widehat{s_{2k+1}^{*}}}{s_0}y_{1,0}\right\|_F^2,\left(k = 0,1,2,\cdots,(N-2)/2\right) \tag{13}$$

其次，我们讨论中继信道和用户间信道。

RN 上接收的偶数子载波的接收信号可写为：

$$y_{2,2k} = h_{2,2k}\lambda_{2k}s_{2k+1} + n_{2,2k},\left(k = 0,1,2,\cdots,(N-2)/2\right) \tag{14}$$

RN 上接收的奇数子载波的接收信号可写为：

$$y_{2,2k+1} = h_{2,2k+1}\lambda_{2k+1}s_{2k}^{*} + n_{2,2k+1},\left(k = 0,1,2,\cdots,(N-2)/2\right) \tag{15}$$

特别要指出 RN 上接收的第 1 位奇数子载波(即 k = 0)传输的为参考信号，接收信号可写为：

$$y_{2,1} = h_{2,1}\lambda_1 s_0^* + n_{2,1}, \tag{16}$$

假设 RN 采用 AF(放大前传)协议，中继节点 RN 将接收到的信号进行放大，然后重新发送该信息到 BS。

BS 接收到从 RN 发来的偶数子载波上的信号可写为：

$$\begin{aligned} y_{3,2k} &= \theta h_{3,2k}\left(h_{2,2k}\lambda_{2k}s_{2k+1} + n_{2,2k}\right) + n_{3,2k} \\ &= \theta h_{3,2k}h_{2,2k}\lambda_{2k}s_{2k+1} + \theta h_{3,2k}n_{2,2k} + n_{3,2k} \\ &= \theta h_{3,2k}h_{2,2k}\lambda_{2k}s_{2k+1} + N_{2k},\ \left(k = 0,1,2,\cdots,(N-2)/2\right) \end{aligned} \tag{17}$$

BS 接收到从 RN 发来的奇数子载波上的信号可写为：

$$\begin{aligned} y_{3,2k+1} &= \theta h_{3,2k+1}\left(h_{2,2k+1}\lambda_{2k+1}s_{2k}^* + n_{2,2k+1}\right) + n_{3,2k+1} \\ &= \theta h_{3,2k+1}h_{2,2k+1}\lambda_{2k+1}s_{2k}^* + \theta h_{3,2k+1}n_{2,2k+1} + n_{3,2k+1} \\ &= \theta h_{3,2k+1}h_{2,2k+1}\lambda_{2k+1}s_{2k}^* + N_{2k+1},\ \left(k = 0,1,2,\cdots,(N-2)/2\right) \end{aligned} \tag{18}$$

特别要指出 BS 接收到从 RN 发来的第 1 位奇数子载波上的参考信号可写为：

$$\begin{aligned} y_{3,1} &= \theta h_{3,1}\left(h_{2,1}\lambda_1 s_0^* + n_{2,1}\right) + n_{3,1} \\ &= \theta h_{3,1}h_{2,1}\lambda_1 s_0^* + \theta h_{3,1}n_{2,1} + n_{3,1} \\ &= \theta h_{3,1}h_{2,1}\lambda_1 s_0^* + N_1 \end{aligned} \tag{19}$$

其中 s_0^* 是第 1 个子载波对应的并且为 BS 已知的参考符号。s_{2k}^* 和 s_{2k+1} 是发送端的信息符号，$h_{2,k}$ 和 $h_{3,k}$ 表示信道 2，3 上的复数瑞利平坦衰落信道。N_{2k} 等于 $\theta h_{3,2k}n_{2,2k} + n_{3,2k}$，$N_{2k+1}$ 等于 $\theta h_{3,2k+1}n_{2,2k+1} + n_{3,2k+1}$。$N_1$ 等于 $\theta h_{3,1}n_{2,1} + n_{3,1}$。$\theta$ 是放大系数常量因子，这里为了方便讨论，我们假定 θ 为 1。

同样的，当 $\lambda_{2k}h_{2,2k}h_{3,2k} = \lambda_1 h_{2,1}h_{3,1}$ 时，

在 BS 端接收偶数子载波信号为：

$$y_{3,2k} = \frac{s_{2k+1}}{s_0^*}y_{3,1} + \left(N_{2k} - \frac{s_{2k+1}}{s_0^*}N_1\right),\ \left(k = 0,1,2,\cdots,(N-2)/2\right) \tag{20}$$

我们可以用最大似然法(ML)解码符号：

$$\widehat{s_{2k+1}} = \arg\min_{s_{2k+1}}\left\| y_{3,2k} - \frac{\widehat{s_{2k+1}}}{s_0^*}y_{3,1}\right\|_F^2,\ \left(k = 0,1,2,\cdots,(N-2)/2\right) \tag{21}$$

同样的，当 $\lambda_{2k+1}h_{2,2k+1}h_{3,2k+1} = \lambda_1 h_{2,1}h_{3,1}$ 时，

在 BS 端接收奇数子载波(除了第 1 位参考信号子载波外)信号为：

$$y_{3,2k+1} = \frac{s_{2k}^*}{s_0^*}y_{3,1} + \left(N_{2k+1} - \frac{s_{2k}^*}{s_0^*}N_1\right),\left(k = 0,1,2,\cdots,(N-2)/2\right) \tag{22}$$

我们可以用最大似然法(ML)解码符号：

$$\widehat{s_{2k}^*} = \arg\min_{s_{2k}}\left\| y_{3,2k+1} - \frac{\widehat{s_{2k}^*}}{s_0^*}y_{3,1}\right\|_F^2,\ \left(k = 1,2,\cdots,(N-2)/2\right) \tag{23}$$

接着，在 BS 端，将从 UT 和 RN 接收到的信号进行 SFBC 解码，可得到有用信号如下：

$$\widetilde{s_{2k+1}} = \frac{\widehat{s_{2k+1}} - \widehat{\left(-s_{2k+1}^{*}\right)^{*}}}{2}, \left(k = 0,1,2,\cdots,(N-2)/2\right)$$
$$\widetilde{s_{2k}} = \frac{\widehat{s_{2k}} + \widehat{\left(s_{2k}^{*}\right)^{*}}}{2}, \left(k = 1,2,3,\cdots,(N-2)/2\right) \quad (24)$$

值得一提的是，在 RN 和窃听者端，他们接收到的各子载波信号是随机变化的，并且不知道随机权重加密系数 ω_i 和 λ_i，同时因为信道之间的差异，在 RN 端 $\lambda_i h_{2,i} \neq \lambda_1 h_{2,1}$，而窃听者端 $\omega_i h_{4,i} \neq \omega_0 h_{4,0}$，$\lambda_i h_{4,i} \neq \lambda_1 h_{4,1}$。因此，RN 和窃听者没有办法获取有用的信息符号。详细的说，因为 $h_{1,i}, h_{2,i}, h_{3,i}$ 是不断变化的，且 ω_i 和 λ_i 都随着信道状态 $h_{1,i}, h_{2,i}, h_{3,i}$ 不断变化，而不是永恒不变的，所以哪怕 RN 或者窃听者得知某一个特定时间的 ω_i 和 λ_i，如果它不能同时知道当时的 $h_{1,i}, h_{2,i}, h_{3,i}$，一样无法解密，除非 RN 或者窃听者能够同时知道 ω_i 和 λ_i 还有 $h_{1,i}, h_{2,i}, h_{3,i}$，并能精确跟踪这些参数的不断变化，而实际情况中无线信道状态是瞬息万变的，所以这是不现实的。

3.3. 集中式自适应调制和编码(AMC)

基于 CSI，UT 可以很好的采用自适应调制编码技术来提高系统的吞吐量、数据速率和频谱利用率。这里我们采用基于 CSI 门限值的集中式调制编码方案(MCS)。

根据 CSI_i(i = 1, 2, 3)对三条信道(直连信道、中继信道、用户间信道)采用相同的调制编码方式。在时隙 1，UT 获取 CSI_i(i = 1, 2, 3)的所有信息，定义这三个 CSI_i 中最小值为 ref_CSI，此外，定义两个门限值 CSI，名为|H1|和|H2| (|H1| < |H2|)。当 ref_CSI < |H1|时，采用 QPSK 调制方式，当|H1| < ref_CSI < |H2|时，采用 16QAM 调制方式，当 ref_CSI > |H2|时，采用 64QAM 调制方式。

系统吞吐量的表达式如下所示：

$$throughput = M^n \cdot R^n \cdot \left[\left(1 - f\left(\gamma_{S,R}^n\right)\right) \cdot \left(1 - f\left(\gamma_{S,D}^n, \gamma_{R,D}^n\right)\right) + f\left(\gamma_{S,R}^n\right) \cdot \left(1 - f\left(\gamma_{S,D}^n\right)\right)\right] \quad (25)$$

系统传输的误块率表达式可以表达为下式：

$$P_e^n = \left(1 - f\left(\gamma_{S,R}^n\right)\right) \cdot f\left(\gamma_{S,D}^n, \gamma_{R,D}^n\right) + f\left(\gamma_{S,R}^n\right) \cdot f\left(\gamma_{S,D}^n\right) \quad (26)$$

M^n 对应于第 n 种 MCS 方式的调制阶数，比如，MCS 为 16QAM 时，M^n = 4，MCS 为 64QAM 时，M^n = 6。R^n 对应第 n 种 MCS 方式的编码速率。$f\left(\gamma_{S,R}^n\right)$ 表示当信噪比 SNR 为 $\gamma_{S,R}^n$ 时，对应的协作信道传输错误概率。S 代表信源(UT)，R 代表中继(RN)，D 代表终端(BS)。

本论文中我们采用了 QPSK，16QAM 和 64QAM 三种调制方式，另外在传输到 BS 端的训练序列中携带编码调制方式信息，00 代表 QPSK，01 代表 16QAM，10 代表 64QAM，所以 BS 端可以在不知道信道信息的情况下根据这两位二进制符号采用相应的解调方式进行解调。

4. 性能仿真结果分析

为了对采用联合 SFBC 编码的物理层加密算法并接着采用 AMC 的上行 SC-FDMA 协作系统进行性能评估，我们考虑一个典型的无线通信模型。系统中并行传输信道子载波数量是 128 个，FFT 长度为 256，符号率是 250,000 bit/s，采用 QPSK，16QAM，64QAM 调制方式。

为了与传统调制方式以及没有联合 SFBC 编码的物理层加密方案进行性能比较，我们在相同的信道质量下评估了传输性能。我们为每个信道链路定义了不同的信噪比(SNRs)，其中 SNR_1 为 UT 和 BS 之间信道的信噪比，SNR_2 为 UT 和 RN 之间信道的信噪比，RN 和 BS 之间信道的信噪比为 SNR_3。BER 为 E_b/N_0

的函数，其中 E_b 是 BS 接收到的每比特的能量，$N_0/2$ 是双边的噪声功率谱密度。

首先，我们假设三条传输信道的 SNRs 相同($SNR_1 = SNR_2 = SNR_3$)，在相同信道条件下比较了 BER 性能。之后，我们给出了吞吐量和保密速率的性能分析。吞吐量的理论公式由(25)式给出。其中可以实现的保密速率定义为信息从信源安全地传输到信宿的传输速率。特殊情况下，当只有一个窃听者时，可以实现的保密速率是 $R_s = \max\{R_d - R_e\}$。其中 R_d 是可实现的信源至信宿的直连链路的传输速率，而 R_e 是可达到的信源至窃听者链路的传输速率。

图 3 显示了在相同信道质量条件下 QPSK，16QAM 和 64QAM 以及 SFBC_QPSK，SFBC_16QAM 和 SFBC_64QAM 协作方案的性能。即考虑所有的链路 SNR1 = SNR2 = SNR3。正如图中所示，RN 和窃听者的 BER 约为 0.5，这意味着 RN 和窃听者很难实施正确解码。此外，各种调制模式的 BER 性能依 SFBC_QPSK > QPSK > SFBC_16QAM > 16QAM > SFBC_64QAM > 64QAM 的顺序降低。总体而言联合 SFBC 编码的物理层加密算法并接着采用 AMC 的传输方式相对没有联合 SFBC 编码的方案显著提高了 BER 性能。另外从图中可见，SFBC_QPSK 的 BER 性能最优，而 64QAM 的 BER 性能最差。可知，联合 SFBC 编码的物理层加密传输方案可以进一步提高信息传输的 BER 性能。

1) BER 性能分析

2) 吞吐量性能分析

图 4 所示为归一化吞吐量的性能仿真结果。基于 AMC 方法，我们可以充分使用 CSI，当 ref_CSI 在门限值附近时，我们采取适当的冒险(通过高码率的映射方法调制信号)以换取更高的吞吐量。正如图中所示，当 SNR 在 0 dB 到 8 dB 之间时，各种调制方式的性能依 SFBC_AMC > AMC > SFBC_QPSK > QPSK > SFBC_16QAM > 16QAM > SFBC_64QAM > 64QAM 顺序下降。当 SNR 在 8 dB 至 13 dB 时，各种调制方式的性能依 SFBC_AMC > AMC > SFBC_16QAM > 16QAM > SFBC_QPSK > QPSK > SFBC_64QAM > 64QAM 顺序递减。然后，当 SNR 在 13 dB 到 16 dB 之间时，各种调制方式的性能下降的顺序为 SFBC_AMC > AMC > SFBC_16QAM > 16QAM > SFBC_64QAM > 64QAM > SFBC_QPSK > QPSK。最后，当 SNR 在 16 dB 到 35 dB 之间时，各种调制方式的性能下降顺序为 SFBC_AMC > AMC > SFBC_64QAM > 64QAM > SFBC_16QAM > 16QAM > SFBC_QPSK > QPSK。总体而言，在任何信噪比情况下 SFBC_AMC 相对于以往的 AMC 显著增加了系统吞吐量。虽然不同 SNR 区间，不同调制方式的归一化吞吐量变化不一，但是可以看出无论 SNR 在哪个区间，SFBC_AMC 和 AMC 比其他调制方式具有更好的吞吐量性能，而 SFBC_AMC 比 AMC 具有更好的性能。可知联合 SFBC 编码的物理层加密传输方案可进一步提高吞吐量。

图 5 所示为误块率的性能分析。如图所示，各种调制模式的误块率性能依 SFBC_QPSK > QPSK > SFBC_16QAM > 16QAM > SFBC_64QAM > 64QAM 顺序下降。总体而言增加 SFBC 编码后的调制方式相对没有 SFBC 编码方案显著提高了 BER 性能。另外从图中可见，SFBC_QPSK 的误块率性能最优，而 64QAM 的误块率性能最差。可知，联合 SFBC 编码的物理层加密传输方案可进一步提高信息传输的误块率性能。

3) 误块率性能分析

4) 保密速率性能分析

图 6 所示为归一化保密速率的性能。如图所示，性能的下降趋势为 SFBC_AMC > SFBC_QPSK > AMC > QPSK > SFBC_16QAM > 16QAM > SFBC_64QAM > 64QAM。根据文献[1]，当窃听者无法解码时，其 BER 约为 0.5，保密速率与 BER 成反比，它随着 ebn0 的增加趋近于信道容量，这意味着系统可以保证信号传输的安全性。同时，如图 4 所示，当 ebn0 大于 10 dB 时，SFBC_AMC 的归一化保密速率趋近于 1。可知，联合 SFBC 编码的物理层加密传输方案可以进一步提高信息传输的归一化保密速率。

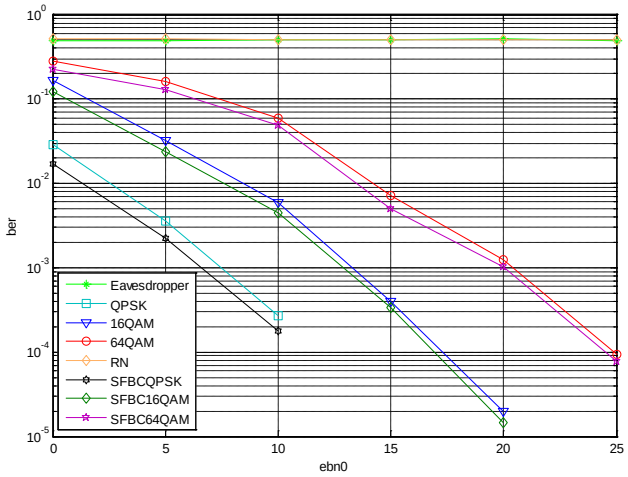

Figure 3. BER performance when SNR1 = SNR2 = SNR3
图 3. 当 SNR1 = SNR2 = SNR3 时的 BER 性能比较

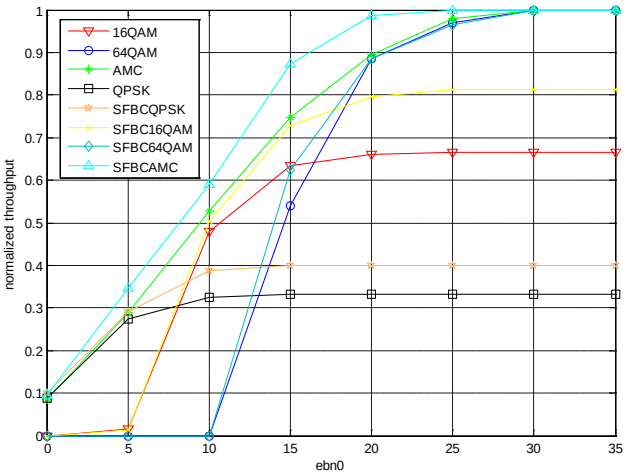

Figure 4. Normalized throughput
图 4. 归一化吞吐量

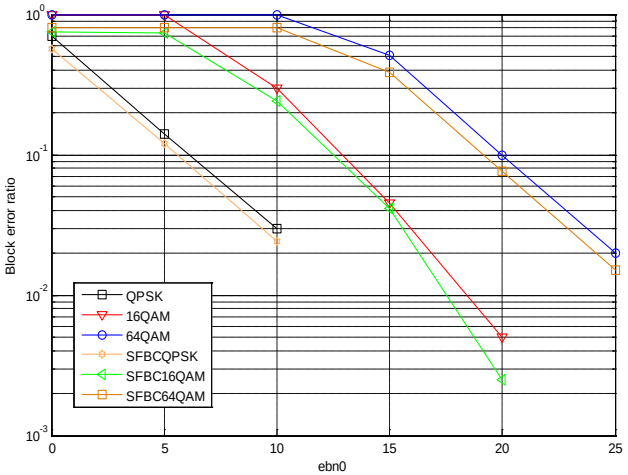

Figure 5. Block error performance when SNR1 = SNR2 = SNR3
图 5. 当 SNR1 = SNR2 = SNR3 时的误块率性能比较

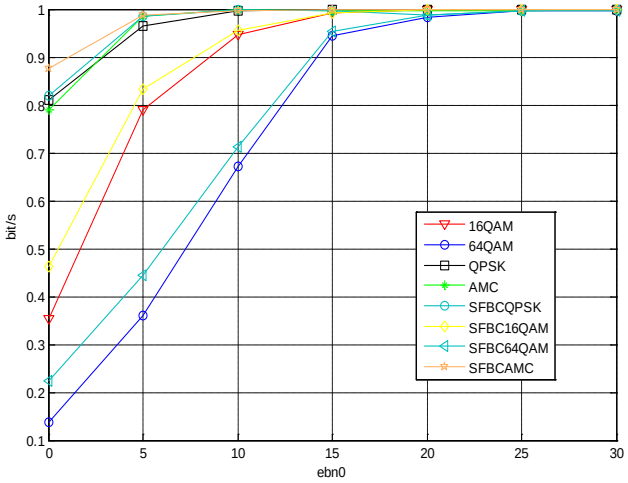

Figure 6. Normalized secrecy rate
图 6. 归一化保密速率

5. 结论

在文中，为了实现 SC-FDMA 协作通信系统的 LPI、高吞吐量以及高保密速率，我们提出了一个新的联合 SFBC 编码的物理层加密传输方案，将 SFBC 编码联合用于物理层加密算法，并接着与自适应编码调制相结合。首先从授权的接收终端发送已知的训练序列至发射机，从而发射机通过计算得知信道状态信息(CSI)，而接收机并不知道任何有关的 CSI。发射机先对发送数据进行 SFBC 编码，接着根据 CSI 设计区分不同用户的随机加权系数，达到防止 RN 和窃听者窃听的效果，还据此进行自适应编码调制，以达到提高系统的吞吐量的效果。与之前文献认为 RN 可信相比，我们认为 RN 是不可信赖的，需要防止 RN 窃听，同时为了减少信息速率损失，我们优化了物理层加密算法，只采用 1 个子载波来传输参考符号。运用我们新提出的联合 SFBC 编码的物理层加密传输方案，无论是 RN 还是窃听者都不能从发射机(UT)获取任何有用信息。实验结果表明，联合 SFBC 编码的物理层加密传输方案可以进一步提高信息传输的安全性，得到很好的保密速率，并且进一步提高系统的传输性能和吞吐量。

参考文献 (References)

[1] Zheng, K., Peng, Y.-X., Long, H. and Liu, G.Y. (2010) Cooperative Communication and Its Application in the LTE-Advanced. 127-146.

[2] Wyner, A.D. (1975) The Wire-Tap Channel. *The Bell System Technical Journal*, **54**, 1355-1387. http://dx.doi.org/10.1002/j.1538-7305.1975.tb02040.x

[3] Leung-Yan-Cheong, S.K. and Hellman, M.E. (1978) The Gaussian Wire Tap Channel. *IEEE Transactions on Information Theory*, **24**, 451-456. http://dx.doi.org/10.1109/TIT.1978.1055917

[4] Csiszár, I. and Körner, J. (1978) Broadcast Channels with Confidential Messages. *IEEE Transactions on Information Theory*, **24**, 339-348. http://dx.doi.org/10.1109/TIT.1978.1055892

[5] Li, X., Wu, J.H. and Ratazzi, E.P. (2006) Array Redundancy and Diversity for Wireless Transmissions with Low Probability of Interception. *Proceedings IEEE ICASSP*, **4**.

[6] Li, X., Wu, J.H. and Ratazzi, E.P. (2007) Using Antenna Array Redundancy and Channel Diversity for Secure Wireless Transmissions. *Journal of Communications*, **2**, 24-32.

[7] Li, Z. and Xia, X.-G. (2009) A Distributed Differentially Encoded OFDM Scheme for Asynchronous Cooperative Systems with Low Probability of Interception. *IEEE Transactions on Wireless Communications*, **8**, 3372-3379.

[8] Li, Z. and Xia, X.-G. (2008) A Distributed Differentially Space-Time-Frequency Coded OFDM for Asynchronous Cooperative Systems with Low Probability of Interception. *IEEE GLOBECOM Global Telecommunications Conference*, 1-5. http://dx.doi.org/10.1109/GLOCOM.2008.ECP.232