مجله علمی - پژوهشی "پدافند الکترونیکی و سایبری"
سال سوم، شماره ۲، تابستان ۱۳۹۴، ص ۶۰- ۴۹

افزایش امنیت در ارتباطات شبکه‌های مخابرات سلولی با به‌کارگیری روش همراستاسازی تداخل

علی گلستانی[1*]، کمال محامدپور[2]، علی حبیبی بسطامی[3]

۱- دانشجوی کارشناسی ارشد، دانشگاه صنعتی خواجه نصیرالدین طوسی، دانشکده مهندسی برق و کامپیوتر
۲- استاد، دانشگاه صنعتی خواجه نصیرالدین طوسی، دانشکده مهندسی برق و کامپیوتر
۳- استادیار، دانشگاه صنعتی خواجه نصیرالدین طوسی، دانشکده مهندسی برق و کامپیوتر

(دریافت: ۹۳/۱۱/۲۶؛ پذیرش: ۹۴/۰۶/۱۰)

چکیده

یکی از چالش‌های معمول در شبکه‌های مخابرات بی‌سیم، شنود شدن سیگنال‌های پخش‌شده از ایستگاه‌های رادیویی توسط استراق‌سمع‌کننده‌ها می‌باشد. در این مقاله نشان داده می‌شود که در یک شبکه مخابرات سلولی با وجود تخصیص فرکانس یکسان به تک‌تک کاربران، تکنیک همراستاسازی تداخل (IA)، افزون بر این‌که می‌تواند تداخل‌های درون و بین سلولی را به‌طور کامل حذف کند؛ همچنین قادر است حداکثر درجات آزادی (DoF) امن را برای شبکه فراهم کند و ارتباطات را در برابر شنود مقاوم سازد. تکنیک IA می‌تواند نرخ محرمانگی شبکه را در SNRهای بالا به ناحیه نرخ کانال پخش تداخلی (IFBC) نزدیک نماید. به‌منظور اثبات ریاضی و شهودی قابلیت تکنیک همراستاسازی تداخل در افزایش امنیت ارتباطات، از یک الگوریتم IA شکل‌بسته در لینک فروسو یک شبکه سلولیِ ناامن‌شده استفاده شده است. نتایج شبیه‌سازی‌ها نشان می‌دهد که به‌ازای محدوده‌ای معین برای تعداد آنتن‌های دریافتِ هر شنودگر، نرخ محرمانگی شبکه در SNRهای بالا به‌خوبی به ظرفیت مجموع شبکه نزدیک می‌گردد.

واژه‌های کلیدی: شبکه مخابرات سلولی، امنیت، همراستاسازی تداخل، درجات آزادی امن، نرخ محرمانگی، کانال تداخل MIMO

۱- مقدمه

در مخابرات بی‌سیم، از آنجایی‌که سیگنال‌های ارسالی در فضای سایبر پخش می‌شوند؛ به‌شدت در برابر شنود آسیب‌پذیرند. آسیب‌پذیری ارتباطات بی‌سیم در برابر استراق سمع، نقطه ضعفی اساسی در برقراری ارتباطات امن محسوب می‌شود. برای آن دسته از شبکه‌های ارتباطی که امنیت در آن‌ها از اولویت بالایی برخوردار است؛ مخابرات بی‌سیم تنها درصورتی می‌تواند کارآمد باشد که برای امن نمودن ارتباطات خود راه‌حلی مؤثر اتخاذ نموده باشد. یکی از راه‌حل‌های ممکن برای ایمن‌سازی ارتباطات در سیستم‌های چندکاربره[1] (MU)، به‌کارگیری تکنیک همراستاسازی تداخل[2] می‌باشد. در واقع تکنیک IA یکی از روش‌های مطمئن و امن در ارسال داده‌ها و اطلاعات با ارزش برای فرد مجاز در فضای سایبر می‌باشد که این موضوع IA را به نوعی راه‌کار پدافند سایبری تبدیل می‌کند. کاربرد اصلی تکنیک IA (همان‌طور که از نام‌گذاری آن مشخص است)؛کاهش تداخل به‌منظور برقراری ارتباطات همزمان و هم‌فرکانس در سیستم‌های چندکاربره می‌باشد. همراستاسازی تداخل یک تکنیک ارسال و یا دریافت مشارکتی[3] است که به‌صورت خطی (یا غیرخطی) سیگنال‌ها را روی چند بعد، نظیر شیارهای زمانی، بلوک‌های فرکانسی و آنتن‌ها کد می‌کند [۱]. به‌عبارت دیگر IA به‌دنبال حداکثرسازی ابعاد فضایی سیگنال مطلوب و در نتیجه حداقل‌سازی ابعاد فضایی سیگنال‌های تداخلی در فضای گیرنده مطلوب می‌باشد [۲]. بنابراین، به کمک تکنیک IA، هر کاربر می‌تواند سمبل‌های مستقل ارسالی از طرف ایستگاه رادیویی را بدون مواجهه با تداخل ناشی از سیگنال‌های سایر کاربران، دریافت نماید.

فرض کنید سیستمی چندکاربره وجود دارد که در آن ارسالات به‌صورت همزمان و هم‌فرکانس بر اساس تکنیک IA صورت می‌گیرد. در این سیستم، اگر شنودگر[4] یا شنودگرهایی قصد استراق‌سمع ارتباطات را داشته باشند؛ حتی با استفاده از هرگونه روش آشکارسازی و کدگشایی[5] نمی‌توانند سیگنال‌های ارسالی را تشخیص دهند. علت آن است که سیگنال‌های تداخلی

* رایانامه نویسنده مسئول: agolestani@ee.kntu.ac.ir

1- Multi-user
2- Interference alignment (IA)
3- Cooperative
4- Eavesdropper
5- Decoding

تمام ابعاد فضای دریافت آن‌ها را اشغال خواهد نمود و به‌دلیل همزمان و هم‌فرکانس بودن ارتباطات، سیگنال مطلوب (از دید شنودگر)، از سیگنال‌های تداخلی قابل جداسازی نخواهد بود [۳].

ایمن‌سازی ارتباطات به کمک تکنیک IA در مقالات محدودی بررسی گردیده است. در مقاله [۴]، از تکنیک IA برای ایجاد امنیت در کانال تداخل K کاربره با حضور یک شنودگر استفاده‌شده است. مرجع [۵]، سیستمی شامل یک زوج فرستنده و گیرنده چندآنتنه در نظر می‌گیرد که در آن تعداد آنتن‌های دریافت دو برابر تعداد آنتن‌های ارسال است. هر گیرنده دو جَمِر را از میان تعدادی جَمِر به‌صورت فرصت‌طلبانه طوری انتخاب می‌کند که اگر تعداد جَمِرها به بی‌نهایت میل کند؛ تعداد درجات آزادی امن به حداکثر مقدار خود برسد و اگر تعداد آنتن‌های شنودگر کوچک‌تر یا مساوی تعداد آنتن‌های گیرنده مطلوب باشد؛ شنودگر به‌هیچ عنوان قادر به آشکارسازی سیگنال مطلوب نخواهد بود. مقاله [۶] نیز با استفاده از تکنیک IA، ارتباطات امن را برای شبکه X فراهم نموده است.

ما در این مقاله از تکنیک IA به‌منظور تأمین امنیت در ارتباطات فروسو[1] (DL) یک شبکه مخابرات سلولی استفاده می‌کنیم. سیستمی متقارن شامل چند کاربر و چند سلول در نظر گرفته‌ایم. در مرکز هر سلول یک ایستگاه پایه[2] (BS) واقع شده است و در هر سلول علاوه‌بر K کاربر، یک شنودگر نیز وجود دارد. در این سیستم درجات آزادی امن[3] و نرخ محرمانگی[4] را پس از اعمال تکنیک هم‌راستاسازی فضایی تداخل[5] محاسبه و شبیه‌سازی خواهیم نمود. اجرای IA فضایی وابسته به وجود تعداد آنتن‌های کافی در ایستگاه‌های پایه و کاربران می‌باشد.

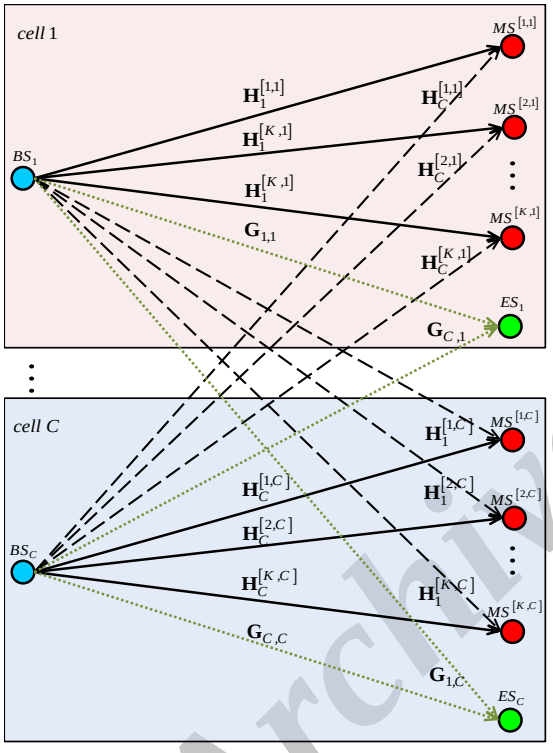
در ادامه، ابتدا در بخش ۲، مدل سیستم بررسی خواهد شد و در بخش ۳، تکنیک هم‌راستاسازی به‌کارگیری‌شده معرفی می‌شود. بخش ۴، به تعریف روابط نرخ محرمانگی و درجات آزادی امن اختصاص پیدا می‌کند و در بخش ۵، عملکرد سیستم سلولی مبتنی‌بر IA به‌وسیله این دو پارامتر مهم، ارزیابی خواهد شد. نتیجه‌گیری و جمع‌بندی مقاله در بخش ۶، صورت می‌گیرد.

در روابط ریاضی به‌کار گرفته‌شده، علائم $\mathbf{A}^T$، $\mathbf{A}^H$ و $\mathbf{a}_i$ به ترتیب نمایانگر ترانهاده، هرمیتین و ستون iام ماتریس $\mathbf{A}$ می‌باشند. نماد $\mathbf{a}_{N\times 1}$ معرف بردار $N\times 1$ به‌صورت $\mathbf{a}=\left[\{a_n\}_{n=1}^{N}\right]^T$ است. $\mathbf{I}_d$ و $\mathbf{0}_{N\times M}$ به‌ترتیب ماتریس‌های $d\times d$ همانی و $N\times M$ صفر را معرفی می‌کنند. $\mathrm{E}\{a\}$ بیان‌گر امید ریاضی متغیر تصادفی a است و نماد $\mathbb{C}$ مجموعه اعداد مختلط را نشان می‌دهد.

1- Downlink
2- Base station
3- Secure DoF
4- Secrecy Rate (SR)
5- Spatial IA

۲- مدل سیستم

یک شبکه سلولی متقارن در سناریوی DL به‌عنوان مدل سیستم انتخاب می‌شود. این شبکه دارای C سلول و در هر سلول افزون بر BS، K کاربر (MS) و یک ایستگاه شنود[6] (ES) وجود دارد. چنین شبکه‌ای را می‌توان همانند شکل (۱) به‌صورت MIMO IFBC[7] مدل نمود. در این شکل BS_c، ایستگاه پایه سلول cام، $MS^{[k,c]}$ کاربر kام درسلول cام و ES_c شنودگر سلول cام می‌باشد.



شکل (۱). نمایش سیستم سلولی شامل ایستگاه‌های پایه، کاربران و شنودگرها

ماتریس $\mathbf{H}_b^{[k,c]}$ معرف کانال MIMO مابین BS سلول bام و kامین کاربر سلول cام است. هر BS، دارای M_b آنتن ارسال و هر MS دارای N_m آنتن دریافت است؛ در نتیجه $\mathbf{H}_b^{[k,c]}\in\mathbb{C}^{N_m\times M_b}$. محوشدگی[8] کانال به‌صورت رایلی شبه‌ایستا در نظر گرفته شده است و هر زیرکانال به‌صورت i.i.d. طبق $h_{i,j}\sim\mathcal{CN}(0,1)$ انتخاب می‌شود.

ماتریس $\mathbf{G}_{b,c}\in\mathbb{C}^{N_e\times M_b}$ نیز معرف کانال MIMO مابین BS سلول bام و شنودگر سلول cام می‌باشد. تعداد آنتن‌های

6- Eavesdropping station
7- Multi input multi output interference broadcast channel
8- Fading

دریافت هر شنودگر (N_e) نامشخص است و به‌صورت پیش ماتریس $\mathbf{G}_{b,c}$ نیز به شکل $g_{i,j} \sim \mathcal{CN}(0,1)$ تولید می‌شود.

در سناریوی DL، BS سلول cام، در هر لحظه از زمان، $d^{[k,c]}$ رشته داده (سمبل) مستقل را برای کاربر $[k,c]$ ارسال می‌کند که $d^{[k,c]} \le \min\{M_b, N_m\}$. $d^{[k,c]}$ برای تمامی کاربران در تک‌تک سلول‌ها یکسان در نظر گرفته می‌شود:

$$d^{[k,c]} = d \quad \forall k \in \mathcal{K}; c \in \mathcal{C} \qquad (۱)$$

در این $\triangleq$ رابطه $\mathcal{C} \triangleq \{1,\ldots,C\}$ و $\mathcal{K} \triangleq \{1,\ldots,K\}$. در این صورت می‌توان پیکربندی[1] سیستم سلولی را به‌صورت $\left(M_b \times (N_m, d)^K\right)^C$ نمایش داد. بردار سمبل ارسالی برای کاربر $[k,c]$ توسط $\mathbf{s}^{[k,c]} \in \mathbb{C}^{d\times 1}$ تعریف می‌گردد که $\mathbf{s}^{[k,c]} = \left[s_1^{[k,c]} \;\; s_2^{[k,c]} \;\; \ldots \;\; s_d^{[k,c]}\right]^T$. این بردار دارای قید محدودیت توان $\mathrm{E}\left\{\mathbf{s}^{[k,c]}\mathbf{s}^{[k,c]H}\right\} \le P\mathbf{I}_d$ می‌باشد. هر بردار $\mathbf{s}^{[k,c]}$ توسط ماتریس $\mathbf{V}^{[k,c]} \in \mathbb{C}^{M_b \times d}$ پیش‌کد می‌گردد که $\mathbf{V}^{[k,c]} = \left[\mathbf{v}_1^{[k,c]} \;\; \mathbf{v}_2^{[k,c]} \;\; \ldots \;\; \mathbf{v}_d^{[k,c]}\right]$ ستون‌های این ماتریس مستقل‌اند ($\forall i \in \mathcal{D}; \mathcal{D} = \{1,\cdots,d\}$ که $\mathbf{v}_i^{[k,c]}$) و هر یک، سمبل ارسالی متناظر با خود را کد می‌کنند. پس از پیش‌کدگذاری[2]، بردار سیگنال ارسالی توسط هر BS، یک بردار $M_b \times 1$ خواهد بود:

$$\mathbf{x}^{[k,c]} = \sum_{i=1}^{d} \mathbf{v}_i^{[k,c]} s_i^{[k,c]} = \mathbf{V}^{[k,c]}\mathbf{s}^{[k,c]} \quad \forall k \in \mathcal{K}; c \in \mathcal{C} \qquad (۲)$$

بردار سیگنال دریافتی توسط کاربر $[k,c]$ عبارت است از:

$$\begin{aligned}\mathbf{y}^{[k,c]} &= \sum_{b=1}^{C}\mathbf{H}_b^{[k,c]}\sum_{u=1}^{K}\mathbf{x}^{[u,b]} + \mathbf{n}^{[k,c]} \\ &= \underbrace{\mathbf{H}_c^{[k,c]}\mathbf{V}^{[k,c]}\mathbf{s}^{[k,c]}}_{\text{the desired signal}} + \underbrace{\sum_{u=1,u\neq k}^{K}\mathbf{H}_c^{[k,c]}\mathbf{V}^{[u,c]}\mathbf{s}^{[u,c]}}_{\text{intra-cell interfering signals}} \\ &\quad + \underbrace{\sum_{b=1,b\neq c}^{C}\sum_{u=1}^{K}\mathbf{H}_b^{[k,c]}\mathbf{V}^{[u,b]}\mathbf{s}^{[u,b]}}_{\text{inter-cell interfering signals}} + \mathbf{n}^{[k,c]} \\ &\quad \forall k \in \mathcal{K}; c \in \mathcal{C}\end{aligned} \qquad (۳)$$

که $\mathbf{y}^{[k,c]} \in \mathbb{C}^{N_m\times 1}$ و $\mathbf{n}^{[k,c]}$ بردار $N_m \times 1$ نویز AWGN مختلط با میانگین صفر و واریانس σ_n^2 می‌باشد ($\mathbf{n}^{[k,c]} \sim \mathcal{CN}\left(\mathbf{0}_{N_m\times 1}, \sigma_n^2\mathbf{I}_{N_m}\right)$). پس از اعمال ماتریس پس‌کد[3] فرض $N_e = N_m$ منظور می‌گردد. هر المان $\mathbf{U}^{[k,c]}$ در گیرنده، سیگنال دریافتی توسط کاربر $[k,c]$ به شکل رابطه (۴) درمی‌آید [۷].

$$\begin{aligned}\hat{\mathbf{y}}^{[k,c]} &= \mathbf{U}^{[k,c]H}\mathbf{y}^{[k,c]} \\ &= \mathbf{U}^{[k,c]H}\mathbf{H}_c^{[k,c]}\mathbf{V}^{[k,c]}\mathbf{s}^{[k,c]} \\ &\quad + \mathbf{U}^{[k,c]H}\left(\sum_{u=1,u\neq k}^{K}\mathbf{H}_c^{[k,c]}\mathbf{V}^{[u,c]}\mathbf{s}^{[u,c]}\right. \\ &\quad \left. + \sum_{b=1,b\neq c}^{C}\sum_{u=1}^{K}\mathbf{H}_b^{[k,c]}\mathbf{V}^{[u,b]}\mathbf{s}^{[u,b]}\right) + \hat{\mathbf{n}}^{[k,c]} \\ &\quad \forall k \in \mathcal{K}; c \in \mathcal{C}\end{aligned} \qquad (۴)$$

که $\hat{\mathbf{y}}^{[k,c]} \in \mathbb{C}^{d\times 1}$ و $\mathbf{U}^{[k,c]} \in \mathbb{C}^{N_m\times d}$. $\mathbf{U}^{[k,c]}$ در راه‌حل IA طوری طراحی خواهد شد که ستون‌هایش مستقل شوند و نیز $\left\|\mathbf{U}^{[k,c]}\right\| = 1$ (که نماد $\|\cdot\|$ معرف نُرم ۲ می‌باشد)؛ در نتیجه نویز $\hat{\mathbf{n}}^{[k,c]}$ دارای توزیع $\mathcal{CN}\left(\mathbf{0}_{d\times 1}, \sigma_n^2\mathbf{I}_d\right)$ خواهد بود.

ماتریس پیش‌کد $\mathbf{V}^{[k,c]}$ نیز ماتریسی نرمالیزه شده است؛ بنابراین ماتریس‌های سیگنال و تداخل را برای سیستم سلولی MIMO IFBC می‌توان به‌صورت روابط (۵) و (۶) تشکیل داد.

$$\mathbf{S}^{[k,c]} = \sqrt{P}\mathbf{U}^{[k,c]H}\mathbf{H}_c^{[k,c]}\mathbf{V}^{[k,c]} \quad \forall k \in \mathcal{K}; c \in \mathcal{C} \qquad (۵)$$

$$\begin{aligned}\mathbf{J}^{[k,c]} = \sqrt{P}\mathbf{U}^{[k,c]}\Bigg[&\left\{\mathbf{H}_c^{[k,c]}\mathbf{V}^{[u,c]}\right\}_{u=1,u\neq k}^{K} \\ &\left\{\left\{\mathbf{H}_b^{[k,c]}\mathbf{V}^{[u,b]}\right\}_{u=1}^{K}\right\}_{b=1,b\neq c}^{C}\Bigg] \\ &\forall k \in \mathcal{K}; c \in \mathcal{C}\end{aligned} \qquad (۶)$$

$\mathbf{S}^{[k,c]}$ ماتریسی $d\times d$ است که معرف زیرفضای سیگنال مطلوب[4] دریافتی توسط کاربر $[k,c]$ می‌باشد و $\mathbf{J}^{[k,c]} \in \mathbb{C}^{d\times(KC-1)d}$ ماتریس زیرفضای تداخل برای این کاربر است که از کنار هم چیدن ماتریس‌های $d\times d$ فضای تداخل درون و بین سلولی (ICI[5] و IUI[6]) به وجود می‌آید. راه‌حل IA هنگامی به‌درستی ماتریس‌های پیش‌کد و پس‌کد $\mathbf{V}^{[k,c]}$ و $\mathbf{U}^{[k,c]}$ را برای کاربر $[k,c]$ طراحی خواهد نمود و به هم‌راستاسازی کامل تداخل[7] دست می‌یابد که:

$$\mathbf{J}^{[k,c]} = \mathbf{0}_{d\times(KC-1)d} \quad \forall k \in \mathcal{K}; c \in \mathcal{C} \qquad (۷)$$

$$\mathrm{rank}\left(\mathbf{S}^{[k,c]}\right) = d \quad \forall k \in \mathcal{K}; c \in \mathcal{C} \qquad (۸)$$

1- Configuration
2- Precoding
3- Post-coder matrix
4- Subspace of desired signal
5- Inter-cell interference
6- Inter user interference
7- Perfect IA

مقالات [۸] و [۹] شرایط امکان‌پذیری[1] همراستاسازی خطی تداخل را برای پیکربندی‌هایی دلخواه از سیستم‌های سلولی متقارن MIMO IFBC بررسی نموده‌اند. بر این اساس کران مناسبِ درجات آزادی[2] (DoF) برای سیستم $\left(M_b\times(N_m,d)^K\right)^C$ مطابق رابطه (۹) خواهد بود.

$$d\le\frac{M_b+N_m}{KC+1} \qquad (۹)$$

مشابه با رابطه (۴) سیگنال دریافتی توسط شنودگر سلول c ام پس از اعمال ماتریس پس‌کد به شکل رابطه (۱۰) در می‌آید.

$$\begin{aligned}\hat{\mathbf{y}}_c &= \mathbf{W}_c{}^H\mathbf{y}_c\\ &= \mathbf{W}_c{}^H\mathbf{G}_{c,c}\mathbf{V}^{[k,c]}\mathbf{s}^{[k,c]}\\ &+\mathbf{W}_c{}^H\left(\sum_{u=1,u\neq k}^{K}\mathbf{G}_{c,c}\mathbf{V}^{[u,c]}\mathbf{s}^{[u,c]}\right.\\ &\left.+\sum_{b=1,b\neq c}^{C}\sum_{u=1}^{K}\mathbf{G}_{b,c}\mathbf{V}^{[u,b]}\mathbf{s}^{[u,b]}\right)+\hat{\mathbf{n}}_c\\ &\forall k\in\mathcal{K};c\in\mathcal{C}\end{aligned} \qquad (۱۰)$$

در این رابطه $\mathbf{W}_c\in\mathbb{C}^{N_e\times d}$ ماتریس پس‌کد شنودگر سلول c ام می‌باشد و $\hat{\mathbf{y}}_c\in\mathbb{C}^{d\times1}$. فرض می‌شود؛ ماتریس پس‌کد مربوط به شنودگر سلول cام به‌منظور شنود سیگنال ارسال‌شده برای کاربر $[k,c]$، توسط یک فیلتر ZF[3] تولید شود:

$$\mathbf{W}_c=\left(\sum_{b=1u=1}^{C}\sum^{K}\mathbf{G}_{b,c}\mathbf{V}^{[u,b]}\mathbf{V}^{[u,b]H}\mathbf{G}_{b,c}{}^H\right)^{-1}\mathbf{G}_{c,c}\mathbf{V}^{[k,c]} \qquad (۱۱)$$
$$\forall k\in\mathcal{K};c\in\mathcal{C}$$

ماتریس‌های پس‌کد شنودگرها پس از تولید، نرمالیزه می‌شوند ($\|\mathbf{W}_c\|=1$)؛ در نتیجه نویز سفید $\hat{\mathbf{n}}_c$ دارای توزیع $\mathcal{CN}\left(\mathbf{0}_{d\times1},\sigma_n^2\mathbf{I}_d\right)$ خواهد بود.

اگر فرض شود شنودگر سلول cام به‌دنبال شنود سیگنال کاربر $[k,c]$ باشد؛ در این‌صورت ماتریس‌های سیگنال و تداخل مربوط به این شنودگر را می‌توان به‌صورت زیر تشکیل داد:

$$\mathbf{S}_c=\sqrt{P}\mathbf{W}_c{}^H\mathbf{G}_{c,c}\mathbf{V}^{[k,c]}\quad\forall k\in\mathcal{K};c\in\mathcal{C} \qquad (۱۲)$$

$$\begin{aligned}\mathbf{J}_c&=\sqrt{P}\mathbf{W}_c{}^H\left[\left\{\mathbf{G}_{c,c}\mathbf{V}^{[u,c]}\right\}_{u=1,u\neq k}^{K}\right.\\ &\left.\left\{\left\{\mathbf{G}_{b,c}\mathbf{V}^{[u,b]}\right\}_{u=1}^{K}\right\}_{b=1,b\neq c}^{C}\right]\\ &=\sqrt{P}\mathbf{W}_c{}^H\bar{\mathbf{J}}_c\quad\forall k\in\mathcal{K};c\in\mathcal{C}\end{aligned} \qquad (۱۳)$$

$\mathbf{S}_c$ ماتریسی $d\times d$ است که معرف زیرفضای سیگنال مطلوب دریافتی توسط ES_c می‌باشد و $\mathbf{J}_c\in\mathbb{C}^{d\times(KC-1)d}$ ماتریس زیرفضای تداخل برای این شنودگر است که از کنار هم چیدن ماتریس‌های $d\times d$ فضای تداخل درون و بین سلولی به‌وجود می‌آید. $\bar{\mathbf{J}}_c$ نیز ماتریسی $N_e\times(KC-1)d$ می‌باشد که در ادامه مباحث به‌کارگیری خواهد شد.

۳- راه‌حل IA فضایی شکل‌بسته

مقاله [۱۰]، راه‌حلی شکل‌بسته[4] برای همراستاسازی تداخل در یک سیستم MIMO IFBC دو سلوله پیشنهاد می‌دهد. در هر سلول این سیستم دو کاربر وجود دارد. تعداد آنتن‌های ارسال و دریافت طوری تعیین می‌شود که شرط امکان‌پذیری IA در حالت تساوی برقرار گردد؛ این موضوع معادل با تخصیص تعداد بهینه آنتن در شبکه سلولی می‌باشد. این مقاله نشان می‌دهد که الگوریتم پیشنهادی‌اش به بهینه درجات آزادی $2N_m$ در حالت $\lceil3/2N_m\rceil\le M_b<2N_m$ دست پیدا خواهد کرد (عملگر $\lceil\cdot\rceil$ مقدار عدد اعشاری را به نزدیک‌ترین عدد صحیح بزرگ‌تر گرد می‌کند).

مقاله [۷] راه‌حل مقاله [۱۰] را برای رسیدن به حالت کلی K کاربر و C سلول توسعه می‌دهد. این مرجع برای رسیدن به این هدف، از طرح گروه‌بندی[5] استفاده می‌کند. این الگوریتم برای دست یافتن به راه‌حلی کلی، قیدی را به شرط امکان‌پذیری IA اضافه می‌کند. این الگوریتم شکل‌بسته در تمامی نواحی SNR[6] با رعایت شدن قیود، حداکثر ابعاد بدون تداخل را برای زیرفضای سیگنال‌های مطلوب کاربران فراهم می‌کند؛ ولی تنها در SNRهای بالا مجموع نرخ[7] بهینه دارد. الگوریتم مقاله [۷] طی دو گام طراحی می‌شود:

- **گام اول:** پس از آن‌که کاربران هر سلول کانال DL را تخمین زدند؛ به‌صورت مشارکتی اطلاعات حالت کانال[8] (CSI) خود را بین یکدیگر به اشتراک می‌گذارند. با تکیه‌بر دانش کانال، این کاربران ماتریس‌های پس‌کد را طوری طراحی می‌کنند که بخشی از کانال‌های ICI همراستا گردند.
- **گام دوم:** پس از آن‌که هر یک از کاربران، کانال مؤثر ($\mathbf{U}^{[k,c]H}\mathbf{H}_c^{[1,c]}$) خود را فیدبک نمودند؛ هر BS قادر است بر اساس کانال‌های ICI همراستاشده، ماتریس‌های پیش‌کد را به‌صورت مناسب طراحی کند و تداخل‌های درون و بین‌سلولی را به‌طور کامل حذف نماید. برای این منظور هر BS باید ماتریس‌های پیش‌کد را به‌صورت متعامد با زیرفضای

1- Feasibility conditions
2- Degree of freedom
3- Zero-forcing

4- Closed-form solution
5- Grouping scheme
6- Signal to noise ratio
7- Sum-rate
8- Channel state information

گستردگی[1] ماتریس‌های کانال مؤثر[2] ICI و IUI طراحی کند.

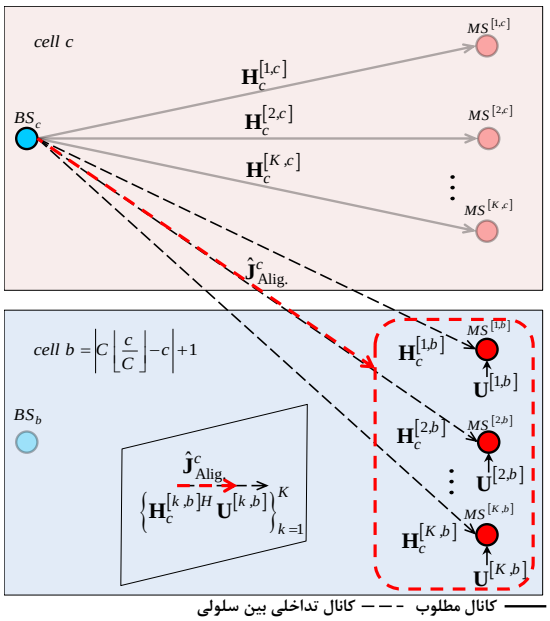
در ادامه دو گام فوق با جزئیات بیشتری بررسی می‌گردد.

۳-۱- طراحی ماتریس‌های پس‌کد

ابتدا بخشی از کانال‌های تداخلی بین سلولی که BS هر سلول برای دیگر سلول‌ها ایجاد می‌کند توسط ماتریس‌های پس‌کد هم‌راستا می‌گردد. برای این کار از طرح گروه‌بندی استفاده می‌شود. در این طرح، کانال‌های ICI ناشی از سلول c، توسط ماتریس‌های پس‌کد تمام کاربران سلول $b=\left|C\left\lfloor c/C\right\rfloor-c\right|+1$ هم‌راستا می‌گردند؛ یعنی

$$\begin{aligned}\hat{\mathbf{J}}^{c}_{\text{Alig.}}\left(\left\{\mathbf{U}^{[k,b]}\right\}_{k=1}^{K}\right)&=\text{span}\left(\mathbf{H}_{c}^{[1,b]H}\,\mathbf{U}^{[1,b]}\right)\\&=\text{span}\left(\mathbf{H}_{c}^{[2,b]H}\,\mathbf{U}^{[2,b]}\right)\\&=\cdots=\text{span}\left(\mathbf{H}_{c}^{[K,b]H}\,\mathbf{U}^{[K,b]}\right)\end{aligned}\qquad(۱۴)$$

که $\hat{\mathbf{J}}^{c}_{\text{Alig.}}$ مطابق شکل ۲، ماتریس $M_b\times d$ کانال‌های ICI مؤثر هم‌راستاشده از BS_c به کاربران سلول b می‌باشد و $\text{span}(\mathbf{A})$ بیان‌گر فضای گستردگی ماتریس $\mathbf{A}$ است. برای یافتن $\hat{\mathbf{J}}^{c}_{\text{Alig.}}$ و $\left\{\mathbf{U}^{[k,b]}\right\}_{k=1}^{K}$ از معادله ماتریسی (۱۵) کمک گرفته خواهد شد.



شکل (۲). تعیین ماتریس‌های پس‌کد به کمک طرح گروه‌بندی

در این معادله $\mathbf{A}_c\in\mathbb{C}^{KM_b\times(M_m+KN_m)}$، $\mathbf{X}_c\in\mathbb{C}^{(M_b+KN_m)\times d}$ و عملگر $\lfloor\cdot\rfloor$ مقدار عدد اعشاری را به نزدیک‌ترین عدد صحیح کوچک‌تر گرد می‌کند.

$$\begin{bmatrix}\mathbf{I}_{M_b} & -\mathbf{H}_c^{[1,b]H} & \mathbf{0}_{M_b\times N_m} & \cdots & \mathbf{0}_{M_b\times N_m}\\ \mathbf{I}_{M_b} & \mathbf{0}_{M_b\times N_m} & -\mathbf{H}_c^{[2,b]H} & \cdots & \mathbf{0}_{M_b\times N_m}\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ \mathbf{I}_{M_b} & \mathbf{0}_{M_b\times N_m} & \mathbf{0}_{M_b\times N_m} & \cdots & -\mathbf{H}_c^{[K,b]H}\end{bmatrix}\begin{bmatrix}\hat{\mathbf{J}}^{c}_{\text{Alig.}}\\ \mathbf{U}^{[1,b]}\\ \mathbf{U}^{[2,b]}\\ \vdots\\ \mathbf{U}^{[K,b]}\end{bmatrix}$$
$$=\mathbf{A}_c\mathbf{X}_c=\mathbf{0}_{KM_b\times d}\qquad\forall b=\left|C\left\lfloor c/C\right\rfloor-c\right|+1;c\in\mathcal{C}\qquad(۱۵)$$

برای یافتن ماتریس مجهولات $\mathbf{X}_c$ از معادله (۱۶) استفاده می‌گردد.

$$\mathbf{X}_c\subset\text{null}(\mathbf{A}_c)\qquad\forall c\in\mathcal{C}\qquad(۱۶)$$

$\text{null}(\mathbf{A}_c)$ بیان‌گر فضای نال ماتریس $\mathbf{A}_c$ می‌باشد. $\mathbf{A}_c$ ماتریسی تمام رتبه نیست و $M_b+KN_m>KM_b$. از طرفی ماتریس $\mathbf{X}_c$ ماتریسی $(M_b+KN_m)\times d$ است. در نتیجه برای محاسبه مستقیم ماتریس $\mathbf{X}_c$ بدون ترکیب نمودن (انتخاب نمودن بخشی از) پایه‌های اورتونرمال فضای نال $\mathbf{A}_c$، باید

$$\begin{aligned}&M_b+KN_m-KM_b=d\\&\rightarrow M_b(1-K)+KN_m=d\end{aligned}\qquad(۱۷)$$

۳-۲- طراحی ماتریس‌های پیش‌کد

پس از محاسبه ماتریس‌های پس‌کد و کانال‌های ICI هم‌راستا شده ($\left\{\hat{\mathbf{J}}^{c}_{\text{Alig.}}\right\}_{c=1}^{C}$) می‌توان ماتریس‌های پیش‌کد را طبق رابطه (۱۸) استخراج نمود.

$$\mathbf{V}^{[k,c]}\subset\text{null}\left(\mathbf{B}^{[k,c]}\right)\qquad\forall k\in\mathcal{K};c\in\mathcal{C}\qquad(۱۸)$$

برای این کار، نخست باید ماتریس $K(C-1)d\times M_b$، $\mathbf{B}^{[k,c]}$ را برای کاربر $[k,c]$ تشکیل داد. این ماتریس از کنار هم چیدن ماتریس‌های $M_b\times d$ کانال‌های مؤثر ICI هم‌راستاشده، کانال‌های مؤثر ICI هم‌راستا نشده و کانال‌های مؤثر IUI وابسته به BS_c همانند رابطه (۱۹) برای کاربر kام به‌وجود می‌آید.

$$\mathbf{B}^{[k,c]}=\Bigg[\underbrace{\hat{\mathbf{J}}^{c}_{\text{Alig.}}}_{\text{effective aligned ICI channels}}\quad\underbrace{\left\{\left\{\mathbf{H}_{c'}^{[k,c]H}\,\mathbf{U}^{[u,c']}\right\}_{u=1}^{K}\right\}_{c'=1,c'\neq c,b}^{C}}_{\text{effective non-aligned ICI channels}}$$
$$\underbrace{\left\{\mathbf{H}_{c}^{[k,c]H}\,\mathbf{U}^{[u,c]}\right\}_{u=1,u\neq k}^{K}}_{\text{effective IUI channels}}\Bigg]^{H}\qquad(۱۹)$$

$\mathbf{B}^{[k,c]}$ ماتریسی تمام رتبه نیست و $M_b>K(C-1)d$. از طرفی $\mathbf{V}^{[k,c]}$ ماتریسی $M_b\times d$ می‌باشد؛ بنابراین برای محاسبه

1- Span subspace
2- Effective channel

مستقیم ماتریس $\mathbf{V}^{[k,c]}$ باید

$$\begin{aligned} & M_b - K(C-1)d = d \\ \rightarrow & M_b = \left[K(C-1)+1\right]d \end{aligned} \quad (۲۰)$$

با جای‌گذاری رابطه (۲۰) در (۱۷) مقدار N_m نیز به‌دست می‌آید.

$$\begin{aligned} & \left[K(C-1)+1\right]d(1-K)+KN_m = d \\ \rightarrow & N_m = \frac{d+\left[K(C-1)+1\right](K-1)d}{K} \\ & = \left[(K-1)(C-1)+1\right]d \end{aligned} \quad (۲۱)$$

۳-۳- بررسی شرط امکان‌پذیری IA در الگوریتم [۷]

با جای‌گذاری مقادیر M_b و N_m از روابط (۲۰) و (۲۱) در رابطه (۹)، شرط امکان‌پذیری IA عبارت است از:

$$d \le \frac{\left[(2K-1)(C-1)+2\right]d}{KC+1} \quad (۲۲)$$

در این رابطه اگر $C \ge 2$ باشد؛ شرط امکان‌پذیری IA همواره برقرار خواهد بود.

$$C \ge 2 \rightarrow \begin{cases} \dfrac{M_b+N_m}{KC+1} = d & ;C=2 \\ \dfrac{M_b+N_m}{KC+1} > d & ;C>2 \end{cases} \quad (۲۳)$$

طبق رابطه (۲۳)، هنگامی‌که $C=2$ باشد؛ تعداد آنتن‌های M_b و N_m که از محدودیت ساختاری راه‌حل شکل‌بسته حاصل می‌شوند؛ بهینه هستند اما به ازای $C>2$، این تعداد از مقادیر بهینه دور می‌شوند.

۴- محاسبه درجات آزادی امن و نرخ محرمانگی

نرخ قابل‌دستیابی توسط کاربر $[k,c]$ عبارت است از

$$\begin{aligned} & R^{[k,c]}\left(\mathbf{U}^{[k,c]}, \left\{\left\{\mathbf{V}^{[u,b]}\right\}_{u=1}^{K}\right\}_{b=1}^{C}\right) \\ & = \mathrm{E}\left\{\log_2 \det\left[\mathbf{I}_d + \left(\sigma_n^2\mathbf{I}_d + \mathbf{J}^{[k,c]}\mathbf{J}^{[k,c]H}\right)^{-1}\mathbf{S}^{[k,c]}\mathbf{S}^{[k,c]H}\right]\right\} \\ & \forall k \in \mathcal{K}\ ; c \in \mathcal{C} \end{aligned} \quad (۲۴)$$

$\det(\mathbf{A})$ معرف دترمینان ماتریس $\mathbf{A}$ می‌باشد. به‌صورت مشابه نرخ قابل حصول برای شنودگر سلول cام باهدف استراق سمع نمودن سیگنال در حال ارسال به کاربر $[k,c]$ مطابق رابطه (۲۵) خواهد بود.

$$\begin{aligned} & R_c\left(\mathrm{W}_c, \left\{\left\{\mathbf{V}^{[u,b]}\right\}_{u=1}^{K}\right\}_{b=1}^{C}\right) \\ & = \mathrm{E}\left\{\log_2 \det\left[\mathbf{I}_d + \left(\sigma_n^2\mathbf{I}_d + \mathbf{J}_c\mathbf{J}_c{}^H\right)^{-1}\mathbf{S}_c\mathbf{S}_c{}^H\right]\right\} \\ & \forall c \in \mathcal{C} \end{aligned} \quad (۲۵)$$

بر اساس روابط (۲۴) و (۲۵) نرخ محرمانگی و درجات آزادی امن برای کاربر $[k,c]$ به ترتیب به‌صورت زیر تعریف می‌شود [۳ و ۵]:

$$SR^{[k,c]} = \left[R^{[k,c]} - R_c\right]^+ \quad (۲۶)$$

$$\hat{d}_{\text{Secure}}^{[k,c]} = \lim_{P\to\infty} \frac{\left[R^{[k,c]} - R_c\right]^+}{\log_2(P)} \quad (۲۷)$$

که $[\cdot]^+$ معرف $\max(0,\cdot)$ می‌باشد. مجموع نرخ محرمانگی و مجموع درجات آزادی به‌ترتیب برابر است با:

$$SR_\Sigma = \sum_{c=1}^{C}\sum_{k=1}^{K} SR^{[k,c]} \quad (۲۸)$$

$$\hat{d}_{\text{Secure}}^{\Sigma} = \sum_{c=1}^{C}\sum_{k=1}^{K} \hat{d}^{[k,c]} \quad (۲۹)$$

۴-۱- محاسبه درجات آزادی امن قابل‌حصول

بعد از اعمال راه‌حل همراستاسازی مرجع [۷]، شروط همراستاسازی کامل تداخل (۷) و (۸) محقق می‌شوند. در این صورت سیگنال‌های تداخل درون و بین سلولی در فضایی $N_m - d$ بُعدی محصور خواهند شد و همواره در هر کاربر d بُعد بدون تداخل برای دریافت d سمبل ارسالی مطلوب وجود خواهد داشت. به عبارتی؛

$$\begin{aligned} \hat{d}^{[k,c]} &= \lim_{P\to\infty} \frac{R^{[k,c]}}{\log_2(P)} \\ &= \lim_{P\to\infty} \frac{\mathrm{E}\left\{\log_2 \det\left[\mathbf{S}^{[k,c]}\mathbf{S}^{[k,c]H}\right]\right\}}{\log_2(P)} \\ &= \lim_{P\to\infty} \frac{\sum_{i=1}^{\mathrm{rank}\left(\mathbf{S}^{[k,c]}\right)} \mathrm{E}\left\{\log_2 \lambda_i\left(\mathbf{S}^{[k,c]}\mathbf{S}^{[k,c]H}\right)\right\}}{\log_2(P)} \\ &= \lim_{P\to\infty} \frac{\sum_{i=1}^{d}\log_2(P)}{\log_2(P)} = d \end{aligned} \quad (۳۰)$$

$\mathrm{rank}(\mathbf{A})$ همان رتبه ماتریس $\mathbf{A}$ و $\lambda_i(\mathbf{A})$ معرف iامین مقدار ویژه بزرگ ماتریس $\mathbf{A}$ می‌باشد.

اگر شنودگر، $N_e \le (KC-1)d$ آنتن دریافت داشته باشد؛ همواره تمام ابعاد فضای دریافتِ شنودگر توسط سیگنال‌های تداخل درون و بین سلولی اشغال خواهد بود. بدین ترتیب در فضای دریافتِ شنودگر سلول cام، زیرفضای بدون تداخل برای

شنود سیگنال کاربر $[k,c]$ وجود نخواهد داشت. اگر $N_e > (KC-1)d$ باشد؛ در این صورت $N_e-(KC-1)d$ بُعد بدون تداخل برای دریافت سمبل‌های کاربر $[k,c]$ آزاد می‌شود و درصورتی‌که $N_e = KCd$ باشد؛ شنودگر می‌تواند d سمبل ارسالی برای کاربر $[k,c]$ را دریافت کند. به‌طور مثال فرض کنید $d=3$، $C=2$ و $K=5$ باشد؛ در این صورت شنودگر سلول c ام باید دو برابر کاربر $[k,c]$ آنتن دریافت داشته باشد تا بتواند سیگنال این کاربر را به‌طور کامل شنود کند.

حرف‌های زده‌شده را می‌توان به‌صورت ریاضی نیز نشان داد. درجات آزادی در شنودگر سلول cام که سیگنال کاربر $[k,c]$ را استراق سمع می‌کند؛ به‌صورت زیر محاسبه می‌شود:

$$\begin{aligned}\hat{d}_c &= \lim_{P\to\infty}\frac{R_c}{\log_2(P)}\\ &= \left[\lim_{P\to\infty}\frac{\mathrm{E}\left\{\log_2\det\left[\left(\sigma_n^2\mathbf{I}_d+\mathbf{J}_c\mathbf{J}_c{}^H\right)^{-1}\mathbf{S}_c\mathbf{S}_c{}^H\right]\right\}}{\log_2(P)}\right]^+\\ &= \left[\lim_{P\to\infty}\frac{\mathrm{E}\left\{\log_2\det\left[\mathbf{S}_c\mathbf{S}_c{}^H\right]\right\}}{\log_2(P)}-\lim_{P\to\infty}\frac{\mathrm{E}\left\{\log_2\det\left[\sigma_n^2\mathbf{I}_d+\mathbf{J}_c\mathbf{J}_c{}^H\right]\right\}}{\log_2(P)}\right]^+\\ &= \left[\lim_{P\to\infty}\frac{\mathrm{E}\left\{\log_2\det\left[\mathbf{S}_c\mathbf{S}_c{}^H\right]\right\}}{\log_2(P)}-\lim_{P\to\infty}\frac{\mathrm{E}\left\{\log_2\det\left[\sigma_n^2\mathbf{I}_d+\mathbf{J}_c\mathbf{J}_c{}^H\right]\right\}}{\log_2(P)}\right]^+\end{aligned}$$

در فوق تعریف می‌کنیم؛

$$R_c^+ \triangleq \mathrm{E}\left\{\log_2\det\left[\mathbf{S}_c\mathbf{S}_c{}^H\right]\right\} \qquad (۳۱)$$

$$R_c^- \triangleq \mathrm{E}\left\{\log_2\det\left[\sigma_n^2\mathbf{I}_d+\mathbf{J}_c\mathbf{J}_c{}^H\right]\right\} \qquad (۳۲)$$

لم ۱: اگر $N_e \le (KC-1)d$ باشد؛ تعداد درجات آزادی قابل‌حصول در شنودگر سلول cام صفر خواهد بود.

اثبات: فرض شده است که ماتریس پس‌کد هر شنودگر متعامدسازی شده باشد ($\mathbf{W}_c{}^H\mathbf{W}_c=\mathbf{I}_d$) می‌توان نوشت:

$$\begin{aligned}R_c^+ &= \mathrm{E}\left\{\sum_{i=1}^{d}\log_2 P\lambda_i\left(\mathbf{G}_{c,c}\mathbf{V}^{[k,c]}\mathbf{V}^{[k,c]H}\mathbf{G}_{c,c}{}^H\right)\right\}\\ &= \mathrm{E}\left\{\sum_{i=1}^{d}\log_2(Pc_i)\right\}\end{aligned}$$

که c_i مقداری ثابت به‌صورت $0<c_i<<+\infty$ است. در نتیجه

$$\lim_{P\to\infty}\frac{R_c^+}{\log_2(P)} = d \qquad (۳۳)$$

از طرفی کران‌های بالا و پایین R_c^- عبارت‌اند از:

$$\begin{aligned}R_c^- &\ge \mathrm{E}\left\{\sum_{i=N_e-d+1}^{N_e}\log_2\left(\sigma_n^2+P\lambda_i\left(\bar{\mathbf{J}}_c\bar{\mathbf{J}}_c{}^H\right)\right)\right\}\\ &\ge d\,\mathrm{E}\left\{\log_2\left(\sigma_n^2+P\lambda_{N_e}\left(\bar{\mathbf{J}}_c\bar{\mathbf{J}}_c{}^H\right)\right)\right\}\end{aligned} \qquad (۳۴)$$

$$\begin{aligned}R_c^- &\le \mathrm{E}\left\{\sum_{i=1}^{d}\log_2\left(\sigma_n^2+P\lambda_i\left(\bar{\mathbf{J}}_c\bar{\mathbf{J}}_c{}^H\right)\right)\right\}\\ &\le d\,\mathrm{E}\left\{\log_2\left(\sigma_n^2+P\lambda_1\left(\bar{\mathbf{J}}_c\bar{\mathbf{J}}_c{}^H\right)\right)\right\}\end{aligned} \qquad (۳۵)$$

ماتریس $\bar{\mathbf{J}}_c\bar{\mathbf{J}}_c{}^H\in\mathbb{C}^{N_e\times N_e}$ دارای توزیع Wishart می‌باشد؛ بنابراین مقادیر ویژه[1] آن با احتمال یک، مقادیری غیر صفر و مثبت هستند [۵]. در نتیجه

$$\lim_{P\to\infty}\frac{(34)}{\log_2(P)} = \lim_{P\to\infty}\frac{R_c^-}{\log_2(P)} = \lim_{P\to\infty}\frac{(35)}{\log_2(P)} = d \qquad (۳۶)$$

پس اگر $N_e \le (KC-1)d$ باشد؛ داریم:

$$\hat{d}_c = \lim_{P\to\infty}\frac{R_c}{\log_2(P)} = \lim_{P\to\infty}\frac{\left[R_c^+-R_c^-\right]^+}{\log_2(P)} = 0 \qquad (۳۷)$$

$$\hat{d}_{\text{Secure}}^{[k,c]} = \lim_{P\to\infty}\frac{\left[R^{[k,c]}-R_c\right]^+}{\log_2(P)} = \lim_{P\to\infty}\frac{R^{[k,c]}}{\log_2(P)} = d \qquad (۳۸)$$

۵- نتایج عددی

در شبیه‌سازی‌ها، عملکرد نرخ محرمانگی و درجات آزادی امن برای سیستم متقارن دوسلولی $\left(M_b\times(N_m,d)^2\right)^2$ و به‌ازای $d=1,3,5$ بررسی شده است. پیش از تحلیل نمودن نتایج به‌دست‌آمده، فرضیات شبیه‌سازی بیان می‌شود.

۵-۱- فرضیات شبیه‌سازی

سطح توان نویز، واحد فرض شده است ($\sigma_n^2=1$) و نمودارهای مجموع نرخ به‌ازای SNRهای $dB[0:3:30]$ و $dB[0:10:150]$ رسم گردیده‌اند؛ در نتیجه تخصیص توان به هر سمبل ارسال به‌صورت $P(i)=10^{SNR(i)/10}/Kd$ در نظر گرفته می‌شود. نتایج عددی طبق روش شبیه‌سازی مونت‌کارلو از متوسط‌گیری روی ۳۰۰ تحقق کانال به‌دست آمده‌اند. هر المان ماتریس‌های کانال $\mathbf{G}_{b,c};\forall b,c\in\mathcal{C}$ و $\mathbf{H}_b^{[k,c]};\forall k\in\mathcal{K};b,c\in\mathcal{C}$ به‌صورت i.i.d. از توزیعی گوسی مختلط با متوسط صفر و واریانس یک تولید می‌گردد. ماتریس‌های پیش‌کد و پس‌کد بعد از تولید، نرمالیزه و متعامدسازی می‌شوند.

برای شبیه‌سازی درجات آزادی به ازای تعداد دلخواه آنتن در شنودگرها، رابطه (۲۹) طبق مرجع [۱۱]، به‌صورت (۳۹) بازنویسی می‌شود:

$$\hat{d}_{\text{Secure}}^{\Sigma} = \sum_{c=1}^{C}\sum_{k=1}^{K}\left[\left[\text{rank}\left(\mathbf{S}^{[k,c]}\right)-\text{rank}\left(\mathbf{J}^{[k,c]}\right)\right]^+ -\left[\text{rank}\left(\mathbf{S}_c\right)-\text{rank}\left(\mathbf{J}_c\right)\right]^+\right]^+ \qquad (۳۹)$$

1- Eigen values

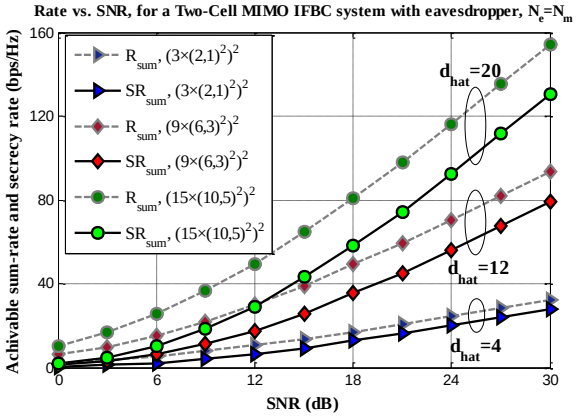
ازآنجایی‌که رتبه یک ماتریس به‌صورت تعداد مقادیر یکتا[1] بزرگ‌تر از صفر آن ماتریس تعریف می‌شود و مقادیر یکتای ماتریس‌های سیگنال و تداخل ممکن است بسیار نزدیک به صفر باشند ولی دقیقاً صفر نشوند؛ پارامتری به نام دقت DoF تعریف می‌گردد. مقدار این پارامتر 10^{-6} لحاظ شده است؛ در نتیجه مقادیر یکتای کوچک‌تر از 10^{-6} در محاسبه رتبه ماتریس، شمارش نخواهند شد.

۵-۲- نتایج نرخ محرمانگی و DoF امن بر حسب SNR

بر اساس مرجع [۱۲]، حداکثر مجموع درجات آزادی فضایی برای سیستم MIMO IFBC به‌ازای پیکربندی متقارن به شکل رابطه (۴۰) می‌باشد.

$$\hat{d}_{\Sigma} = \min\left\{CM_b, KCN_m, \max\left(M_b, KN_m\right)\right\} \qquad (۴۰)$$

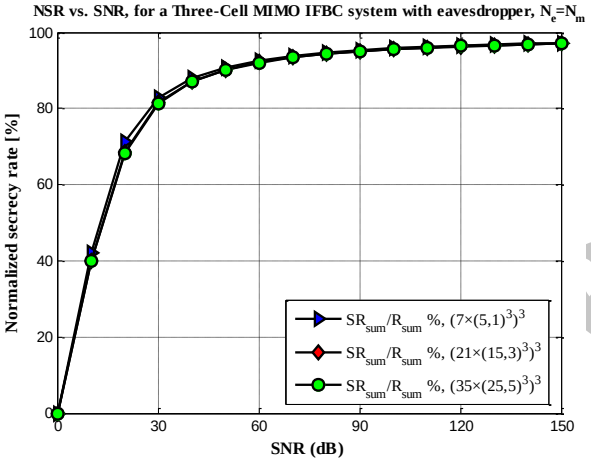
به‌ازای $C=2$ و $K=1,2$ مجموع درجات آزادی امن برای حالت $N_e \le (KC-1)d$ برابر با حداکثر DoF کانال تداخل خواهد بود. این نتیجه با توجه به شکل (۳) برای سیستمی با $C=2$، $K=2$ و $N_e=N_m$ کاملاً قابل تأیید است. به‌طور مثال، به ازای $d=5$، تعداد آنتن‌های ارسال و دریافت به ترتیب ۱۵ و ۱۰ خواهد بود؛



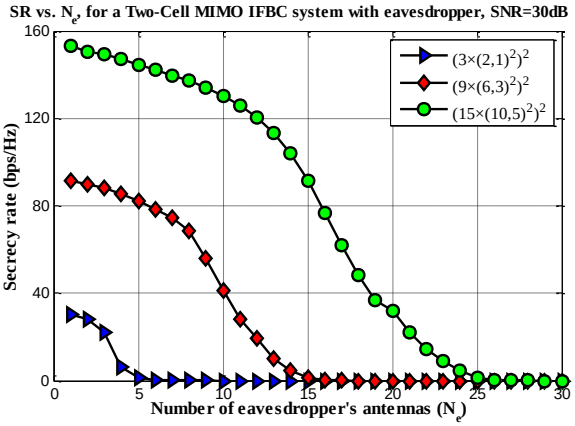
شکل (۳). عملکرد نرخ محرمانگی و DoF امن در سیستمی با $C=2$، $K=2$ و $N_e=N_m$ به ازای $d=1,3,5$

بنابراین تعداد حداکثر DoF کانال تداخل طبق رابطه (۴۰) به‌صورت $\hat{d}_{\Sigma}=KN_m=20$ می‌باشد. از طرفی طبق شکل ۳ و رابطه (۳۹) مجموع درجات آزادی امن نیز به همین مقدار می‌رسد ($\hat{d}^{\Sigma}_{\text{Secure}}=KCd=20$).

در شکل ۳ و شکل ۴ عملکرد نرخ محرمانگی در سیستمی دو سلوله که در هر سلول دو کاربر و یک شنودگر وجود دارد؛ بررسی‌شده است. تعداد آنتن‌های دریافت شنودگر برابر با تعداد آنتن‌های دریافت هر کاربر فرض شده و نتایج نرخ به ازای تعداد مختلف سمبل‌های ارسالی به‌دست‌آمده است. همان‌گونه که در شکل ۳ مشخص است؛ به ازای d سمبل ارسالی برای هر کاربر، نرخ محرمانگی به‌ازای افتی تقریباً ثابت، عملکرد ظرفیت مجموع[2] شبکه را با افزایش SNR تعقیب خواهد نمود. این موضوع سبب می‌شود که طبق شکل ۴، در SNRهای بالا نسبتِ نرخ محرمانگی به مجموع نرخ شبکه به یک میل کند. در نتیجه در رژیم SNR بالا نرخ محرمانگی به ناحیه ظرفیت[3] کانال پخش تداخلی نزدیک خواهد شد.



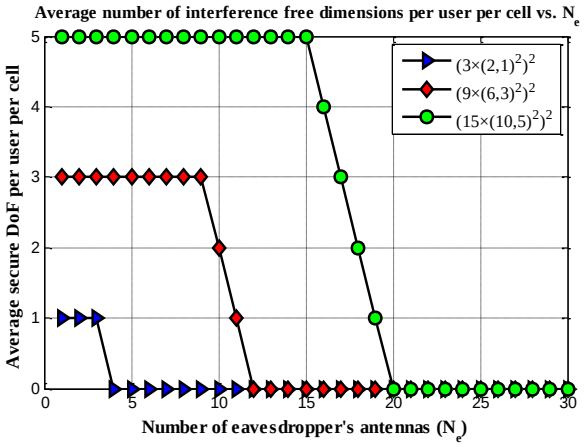
شکل (۴). عملکرد نرخ محرمانگی در سیستمی با $C=2$، $K=2$ و $N_e=N_m$ به ازای $d=1,3,5$



شکل (۵). عملکرد نرخ محرمانگی بر حسب N_e در سیستمی با $C=2$، $K=2$ به ازای $d=1,3,5$ و $SNR=30dB$

1- Singular values

2- Sum capacity
3- Capacity region

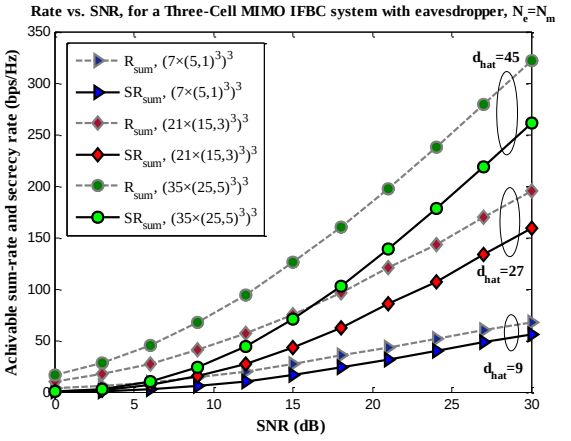


شکل (۶). عملکرد درجات آزادی امن بر حسب N_e در سیستمی با $K=2$ ،$C=2$ به ازای $d=1,3,5$ و $SNR=30\,dB$

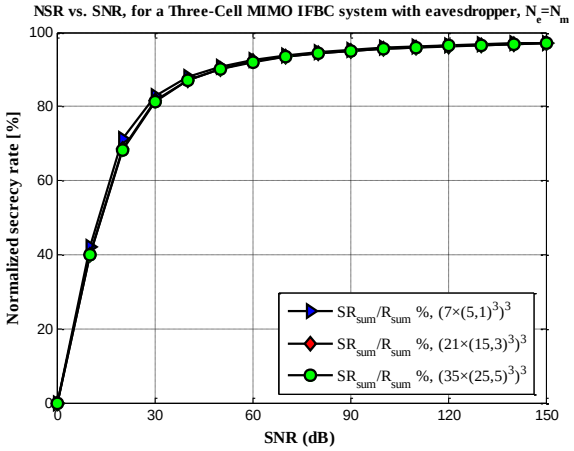
۵-۳- نتایج نرخ محرمانگی و DoF امن بر حسب N_e

در شکل های(۵ و ۶) به ترتیب عملکرد نرخ محرمانگی و درجات آزادی امن در سیستم دو سلولی بر حسب تعداد آنتن‌های دریافت شنودگر به نمایش در آمده است.

آن‌چنان‌که مشخص است؛ هر چه تعداد آنتن‌های دریافت در شنوگرها افزایش یابد؛ نرخ محرمانگی به‌ازای dهای مختلف کاهش خواهد یافت. با افزایش N_e سرانجام نرخ محرمانگی و میانگین درجات آزادی امن به صفر خواهد رسید. بنا به شکل ۶، اگر تعداد آنتن‌های دریافت هر شنودگر کوچک‌تر یا مساوی $(KC-1)d=3d$ باشد؛ شبکه به حداکثر درجات امن دست خواهد یافت. اما اگر $N_e>3d$ باشد؛ میانگین درجات آزادی امن در هر کاربر تا زمانی که N_e به $4d$ برسد به میزان N_e-3d افت خواهد کرد و به‌ازای $N_e\geq 4d$ درجات آزادی امن در شبکه دو سلوله برابر با صفر می‌گردد.



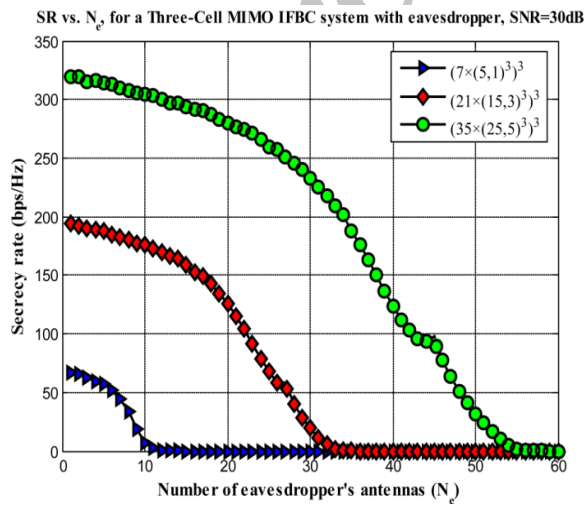
شکل (۷). عملکرد نرخ محرمانگی و DoF امن در سیستمی با $C=3$، $K=3$ و $N_e=N_m$ به‌ازای $d=1,3,5$



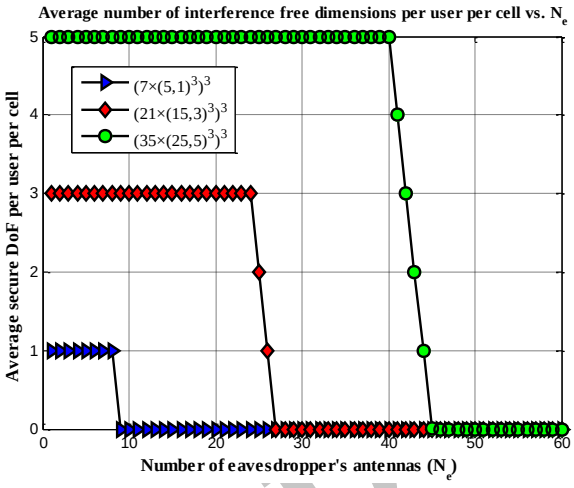
شکل(۸). عملکرد نرخ محرمانگی در سیستمی با $C=3$، $K=3$ و $N_e=N_m$ به ازای $d=1,3,5$

۵-۴- نتایج نرخ محرمانگی و DoF امن در سیستم سه سلوله

در این زیر بخش عملکرد نرخ محرمانگی و درجات آزادی امن برای سیستمی با $C=3$ و $K=3$ در شرایط حضور شنودگر در سلول‌ها بررسی‌شده است. همانطور که در شکل ۷ تا شکل ۱۰ مشهود است؛ نتایج شبیه‌سازی‌ها برای سیستم سه سلوله در حالت کلی (صرف نظر از تغییر مقیاس‌ها) به نتایج به دست آمده در سیستم دو سلولی نزدیک می‌باشد؛ در نتیجه از تحلیل شکل‌ها صرف نظر شده است.



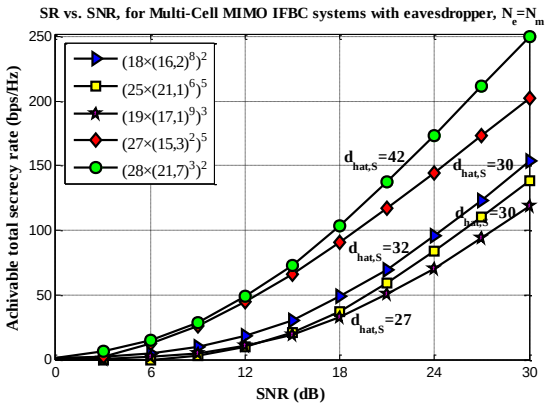
شکل (۹). عملکرد نرخ محرمانگی بر حسب N_e در سیستمی با $C=3$، $K=3$ به ازای $d=1,3,5$ و $SNR=30\,dB$



شکل (۱۰). عملکرد درجات آزادی امن بر حسب N_e در سیستمی با $C=3$، $K=3$ به‌ازای $d=1,3,5$ و $SNR=30\,dB$

۵-۵- نتایج نرخ محرمانگی و DoF امن به‌ازای پیکربندی‌های گوناگون

در شکل (۱۱) به‌منظور تأیید کارایی تکنیک IA شکل‌بسته در امن نمودن ارتباطات شبکه‌های سلولی شبیه‌سازی‌های متنوعی صورت گرفته است. در این شکل، نتایج نرخ محرمانگی و درجات آزادی مربوط به الگوریتم شکل‌بسته [۷] به ازای انواع متنوعی از پیکربندی‌های سیستم سلولی ارزیابی شده است. به عبارتی این شبیه‌سازی‌ها به‌ازای C، K و d مختلف و با فرض $N_e=N_m$ صورت گرفته است.

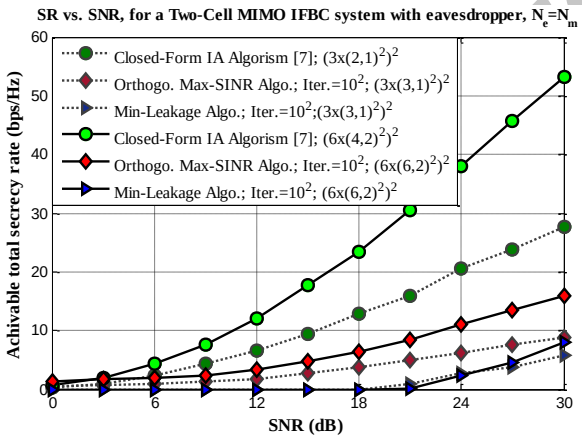


شکل (۱۱). عملکرد نرخ محرمانگی و درجات آزادی امن به‌ازای پیکربندی‌های مختلف سیستم سلولی

۵-۶- مقایسه نتایج نرخ محرمانگی انواع الگوریتم‌های IA

الگوریتم‌های همراستاسازی فضایی تداخل را می‌توان به دو دسته الگوریتم‌های شکل‌بسته و تکرارشونده تقسیم نمود. همان‌گونه که در این مقاله دیده شد؛ الگوریتم‌های شکل‌بسته معمولاً سریع می‌باشند و تنها به‌یک‌بار تکرار نیاز دارند. همچنین عملکرد آن‌ها به‌طور کامل قابل پیش‌بینی است و به‌ازای CSI دقیق هم‌ترازی کامل تداخل را تضمین می‌کنند. اگرچه الگوریتم‌های تکرارشونده به‌طور معمول به تعداد تکرار بالا برای رسیدن به همگرایی نیاز دارند اما این الگوریتم‌ها نسبت به راه‌حل‌های شکل‌بسته مقاومت بیشتری در شرایط CSI ناقص از خود نشان می‌دهند و در اکتساب CSI، هزینه سرزیر[1] کمتری می‌پردازند.

در شکل (۱۲)، عملکرد نرخ محرمانگی الگوریتم‌های IA شکل‌بسته و تکرارشونده در سیستمی دو سلوله به ازای $K=2$، $d=1,2$ و $N_e=N_m$ مقایسه شده است. ازآنجایی‌که دو الگوریتم تکرارشونده و مشهور Min-Leakage و Max-SINR (برگرفته از [۸ و ۱۳]) براساس خاصیت تقابلی بودن کانال[2] (TDD[3]بودن ارتباطات) عمل می‌نمایند؛ باید ضریب 1/2 را هنگام محاسبه نرخ در رابطه (۲۴) لحاظ نمود. این موضوع سبب می‌شود که نتایج نرخ محرمانگی این دو الگوریتم به‌رغم N_m بیشتر نسبت به الگوریتم شکل‌بسته [۷]، افت چشم‌گیری داشته باشد.



شکل (۱۲). مقایسه عملکرد نرخ محرمانگی الگوریتم IA شکل‌بسته [۷] با الگوریتم‌های IA تکرارشونده Min-Leakage و Max-SINR

۶- نتیجه‌گیری

محاسبات ریاضی و شبیه‌سازی‌های این مقاله به‌خوبی نشان دادند که تکنیک هم‌راستاسازی تداخل می‌تواند نقشی کلیدی در امن نمودن ارتباطاتِ سیستم‌های چندکاربره به‌خصوص شبکه‌های سلولی ایفا نماید. بنا به نتایج شبیه‌سازی و محاسبات

1- Overhead
2- Reciprocity property
3- Time division duplexing

ریاضی، اگر تعداد آنتن‌های دریافت در شنودگرها از شرط $N_e \le (KC-1)d$ پیروی کند؛ با به‌کارگیری تکنیک IA می‌توان به حداکثر درجات آزادی امن دست یافت و نرخ محرمانگی شبکه سلولی را در SNRهای بالا به ظرفیت مجموع شبکه نزدیک نمود.

۷- مراجع

[1] O. E. Ayach, S. W. Peters, and R. W. Heath, "The Practical Challenges of Interference Alignment," IEEE Wireless Commun. Mag., vol. 20, no. 1, pp. 35-42, Feb. 2013.

[2] L. Qian, R. Q. Hu, Q. Yi, and W. Geng, "Cooperative Wireless Communications for Wireless Networks: Techniques and Applications in LTE-Advanced Systems," IEEE Wireless Commun., vol. 19, no. 2, pp. 22–29, April 2012.

[3] S. Sasaki, et al., "Secure communications using Interference Alignment in MIMO interference channels," in Proc. Int. Symp. on Antennas and Propagation (ISAP), pp. 762-765, 29 Oct.-2 Nov. 2012.

[4] O. O. Koyluoglu, H. El Gamal, L. Lai, and H. V. Poor, "Interference Alignment for Secrecy," IEEE Trans. on Inf. Theory, vol. 57, no. 6, pp. 3323-3332, June 2011.

[5] J. H. Lee, S. H. Chae, and W. Choi, "Opportunistic jammer selection for secure degrees of freedom," in Proc. IEEE Global Commun. Conf. (GLOBECOM), pp. 4862-4867, 3-7 Dec. 2012.

[6] T. Gou and S. A. Jafar, "On the secure degrees of freedom of wireless X networks," in Proc. 46th Annual Allerton Conf. on Commun., Control and Computing, pp. 826-833, 23-26 Sep. 2008.

[7] J. Tang and S. Lambotharan, "Interference Alignment Techniques for MIMO Multi-Cell Interfering Broadcast Channels," *IEEE Trans. on Commun*., vol. 61, no. 1, pp. 164-175, Jan. 2013.

[8] B. Zhuang, R. A. Berry, and M. L. Honig, "Interference Alignment in MIMO Cellular Networks," in Proc. IEEE ICASSP, May 2011.

[9] T. Liu and C. Yang, "On the Feasibility of Linear Interference Alignment for MIMO Interference Broadcast Channels with Constant Coefficients," IEEE Trans. on Signal Process., vol. 61, no. 9, pp. 2178-2191, May 2013.

[10] W. Shin, N. Lee, J. Lim, C. Shin, and K. Jang, "On the Design of Interference Alignment Scheme for Two-Cell MIMO Interfering Broadcast Channels," IEEE Trans. on Wireless Commun. pp. 437-442, Feb. 2011.

[11] D. S. Papailiopoulos and A. G. Dimakis, "Interference Alignment as a Rank Constrained Rank Minimization," IEEE Trans on Signal Process., vol. 60, no. 8, pp. 4278-4288, August 2012.

[12] S. A. Jafar and M. J. Fakhereddin, "Degrees of Freedom for the MIMO Interference Channel," IEEE Trans. Inf. Theory, vol. 35, no. 7, pp. 2637-2642, July 2007.

[13] J. Schreck and G. Wunder, "Distributed Interference Alignment in Cellular Systems: Analysis and Algorithms," in Proc. Sustainable Wireless Technol. (European Wireless) Conf., pp. 1-8, 27-29 April 2011.

Journal Of Electronical & Cyber Defence
Vol. 3, No. 2, 2015, Serial No. 10

Enhancing Communication Security in Cellular Communications Networks by using Interference Alignment Technique

A. Golestani*, K. Mohamedpour, A. Habibi Bastami

K. N. Toosi University of Technology

(Received: 15/02/2015, Accepted: 01/09/2015)

ABSTRACT

One of the common challenges in wireless communications networks is wiretapping broadcast signals from radio stations by eavesdroppers. In this paper is shown that interference alignment (IA) technique can be completely eliminated intra and inter-cell interferences, in a cellular communications network with the same frequency allocation to all of the users. Also, this technique is able to provide maximum degrees of freedom (DoF) and securing the communication against eavesdropping. IA approximately can close the rate of network secrecy to rate region of the interfering broadcast channel (IFBC) in high SNR regime. In order to prove the mathematical and intuitive capability of the interference alignment technique in increasing communication security, a kind of IA algorithm closed-form is used in the downlink of an unsecured cellular network. Simulation results are demonstrated for a certain range from the number of eavesdropper's receive antennas, that secrecy rate well possible come close to the network sum-capacity in high SNRs.

Keywords: Cellular communications network, security, interference alignment, secure degrees of freedom, secrecy rate, MIMO interference channel.

* Corresponding Author Email: agolestani@ee.kntu.ac.ir