Journal of Electronical & Cyber Defence
Vol. 9, No. 2, 2021, Serial No. 34

Improving the Security in Cellular Communications Networks with Artificial Noise Addition by Non-Orthogonal Resource Allocation Techniques

M. A. Kamari, H. R. Khodadadi*
*Imam Hossein Comprehensive University
(Received: 20/09/2020, Accepted: 11/01/2021)

ABSTRACT

The non-orthogonal multiple access (NOMA) method is known as a bandwidth efficient access method for fifth generation wireless systems. Unlike the conventional orthogonal multiple access method, which uses only one subcarrier to send information simultaneously, the NOMA utilizes a number of subcarriers simultaneously to serve multiple users. In previous attempts, the superiority of the non-orthogonal multiple access method over the orthogonal access method from the viewpoint of security against eavesdropping, has been investigated and despite the dominance of the NOMA over the OMA by the secrecy sum rate (SSR) criterion, no substantial difference is noticed between them. This paper attempts to increase the secrecy sum rate by adding artificial noise along with the user's signal in the transmitter. In this way, legitimate users receive the artificial noise signal and they remove this signal from the received signal on arrival, but the eavesdroppers assume that it is the signal of a legitimate user and spend a lot of energy to decode it. This reduces the eavesdropper rate and thus the listening probability. The results obtained in this paper show that, for example, in a specific SNR such as 10 dB, the total secrecy sum rate (SSR) for the orthogonal multiple access method is about 0.1, for the common non-orthogonal multiple access method is about 0.25 and for the non-orthodontic multiple access method using the artificial noise is about 1 bit per second per hertz.

Keywords: Non-orthogonal multiple access (NOMA), Secrecy Sum Rate (SSR), Artificial Noise (AN), Security, Resource Allocation

* Corresponding Author Email: hkhdadi@ihu.ac.ir

نشریه علمی "پدافند الکترونیکی و سایبری"
سال نهم، شماره ۲، تابستان ۱۴۰۰، ص ۱۴۲-۱۳۵

علمی – پژوهشی

بهبود امنیت در شبکه‌های مخابرات سلولی با کمک اضافه کردن نویز مصنوعی به روش تخصیص منابع نامتعامد

محمدامین کمری[۱]، حمیدرضا خدادادی[۲*]

۱- دانشجوی کارشناسی ارشد، ۲- استادیار، دانشگاه جامع امام حسین(ع)، تهران، ایران
(دریافت: ۱۳۹۹/۰۶/۳۰، پذیرش: ۱۳۹۹/۱۰/۲۲)

چکیده

روش دسترسی چندگانه نامتعامد (NOMA) به‌عنوان یک روش دسترسی کارآمد ازلحاظ استفاده از باند، برای سامانه‌های بی‌سیم نسل پنجم شناخته می‌شود. برخلاف روش دسترسی چندگانه متعامد معمولی که به‌طور هم‌زمان فقط از یک زیر حامل برای ارسال اطلاعات استفاده می‌کند، NOMA حوزه توان را برای خدمت‌رسانی به کاربران چندگانه از تعدادی زیر حامل به‌طور هم‌زمان استفاده می‌کند. در تلاش‌های قبلی برتری روش دسترسی چندگانه نامتعامد بر روش دسترسی چندگانه متعامد از بعد امنیت در مقابل شنود، با معیار مجموع نرخ محرمانگی (SSR) بررسی شده است؛ اما باوجود برتری مجموع نرخ محرمانگیNOMA نسبت به OMA، تفاوت چشم‌گیری بین آنها ملاحظه نمی‌شود. در این مقاله سعی شده است با استفاده از اضافه کردن نویز مصنوعی به همراه سیگنال کاربران در فرستنده، مجموع نرخ محرمانگی افزایش یابد. در این روش کاربران حقیقی اطلاعات سیگنال نویز مصنوعی را دارند و به‌محض ورود، آن را از سیگنال دریافتی کم می‌کنند؛ ولی شنودگرها آن را سیگنال یک کاربر اصلی فرض کرده و انرژی زیادی برای رمزگشایی آن صرف می‌کنند. همین امر نرخ شنودگر را کاهش داده و منجر به کم شدن احتمال شنود خواهد شد. نتایج به‌دست آمده در این مقاله نشان می‌دهد که به‌عنوان مثال در یک SNR مشخص مانند۱۰dB ، مجموع نرخ محرمانگی برای روش دسترسی چندگانه متعامد در حدود ۰/۱ ، برای روش دسترسی چندگانه نامتعامد متداول در حدود ۰/۲۵ و برای روش دسترسی چندگانه نامتعامد با استفاده از نویز مصنوعی در حدود ۱ بیت بر ثانیه بر هرتز است.

کلیدواژه‌ها: دسترسی چندگانه نامتعامد (*NOMA*)، مجموع نرخ محرمانگی (*SSR*)، نویز مصنوعی (*AN*)، امنیت، تخصیص منابع

۱- مقدمه

امروزه، بهره‌وری طیفی به یکی از چالش‌های اساسی برای کنترل تقاضای فزاینده ترافیک داده تبدیل می‌شود. علاوه بر این، به دلیل ازدیاد استفاده از سرویس‌های نوظهور مانند اینترنت اشیا (IoT)[۱]، سامانه‌های ارتباطی تلفن همراه 5G برای پاسخگویی به تقاضای دستگاه‌ها با تأخیر کم و انواع خدمات متنوع، نیاز به پشتیبانی از اتصال گسترده دارند [۱]. به همین منظور، دسترسی چندگانه غیر متعامد (NOMA)[۲] به‌عنوان یک روش امیدوارکننده برای بهره‌برداری مؤثرتر از منابع محدود و به‌صورت غیرمتعامد پیشنهاد شده است [۲]. یک طرح NOMA معمولی حال حاضر به این صورت است که به‌طور هم‌زمان از طریق تسهیم چندگانه دامنه قدرت به چندین کاربر خدمت کند. در طرح دامنه قدرت NOMA سیگنال‌های حاوی اطلاعات چند کاربر برای انتقال سوار بر حامل می‌شوند و فن‌آوری کارآمد تشخیص چند کاربر در گیرنده از طریق لغو تداخل پی‌درپی (SIC)[۳] مورد استفاده قرار می‌گیرد. به‌طورکلی، چندین کاربر NOMA باید مطابق با شرایط کانال متفاوت آن‌ها، برای تسهیل روند مؤثر SIC به‌کارگیری شوند.

فناوری دسترسی چندگانه تقسیم فرکانس متعامد (OFDMA)[۴]، در لینک فروسوی شبکه‌های بی‌سیم نسل چهارم (4G) موجود است. در سامانه‌های OFDMA به کاربران مختلف منابع فرکانس متعامد اختصاص داده شده است که می‌تواند به‌طور مؤثر تداخل بین کاربر را کاهش دهد اما به‌نوبه خود کارایی طیف سیستم را محدود می‌کند. ازنظر تئوری اطلاعات برتری مجموع ظرفیت NOMA نسبت به (OMA)[۵] زمانی بیشتر

* رایانامه نویسنده مسئول: hkhdadi@ihu.ac.ir

[1] Internet of Things
[2] Non-Orthogonal Multiple Access
[3] Successive Interference Cancellation
[4] Orthogonal Frequency-Division Multiple Access
[5] Orthogonal Multiple Access

ناشر: دانشگاه جامع امام حسین (ع)

قابل‌توجه می‌شود که شرایط کانال کاربران هم‌زمان با سرویس‌دهی بهتر هم بشوند؛ بنابراین، NOMA برای کاربران با شرایط مختلف کانال مفید است. علاوه بر این، کاربران همچنین می‌توانند با توجه به الزامات مختلف کیفیت سرویس (QoS)[1] خود تفکیک شوند [۳]. برتری NOMA نسبت به‌دسترسی چندگانه متعامد متعارف OMA از دیدگاه بهره‌وری طیفی، بازده انرژی نیز مورد بررسی قرار گرفته است [۴].

در فناوری5G متفاوت از دسترسی چندگانه متعامد متعارف (OMA)، NOMA قادر است با بهره‌برداری از دامنه قدرت برای دسترسی چندگانه با استفاده از تجمیع طیف کاربران متعدد، به چندین کاربر خدمت کند و بنابراین، می‌تواند طیف سیستم را بیشتر بهبود بخشد. اشتراک طیف یکسان در بین کاربران منجر به تداخل متقابل بالا هنگام رمزگشایی اطلاعات می‌شود. بااین‌حال، با استفاده از لغو کننده تداخل پی‌درپی SIC در گیرنده، می‌توان اطلاعات را به‌درستی رمزگشایی کرد و درنتیجه توان سیستم را بهبود بخشید، درنتیجه NOMA با تخصیص منابع غیر متعامد و SIC ممکن است به کاهش تداخل قابل‌توجهی دست پیدا کند که همراه با تسهیل ارتباط گسترده، به ظرفیتی بالاتر خواهد رسید.به دلیل ماهیت پخش شوندگی ارتباطات بی‌سیم، پیام محرمانه در برابر شنودها آسیب‌پذیر است که این مسئله چالش امنیتی انتقال بی‌سیم را ایجاد می‌کند. امنیت لایه فیزیکی به‌عنوان یک فناوری اصلی مکمل برای حفاظت از امنیت ارتباطات با بهره‌گیری از ویژگی‌های تصادفی ذاتی کانال‌های لایه فیزیکی بی‌سیم در نظر گرفته شده است [۵]. امنیت لایه فیزیکی عمدتاً به تفاوت نسبت‌های دریافتی سیگنال به نویز (SNR)[2] بین کاربران قانونی و شنود کننده متکی است. بنابراین، ایجاد تداخل ممکن است برای افزایش محرمانگی مفید باشد. جالب است بدانید که سیاست تخصیص منابع غیر متعامد با تداخل اضافی بین کاربر، با توجه به اصل NOMA می‌تواند عملکرد امنیت لایه فیزیکی را به‌دلیل تخریب قابل‌توجه SNRدریافت‌کننده شنودگر بهبود بخشد. در این راستا، استفاده از فناوری NOMA نه‌تنها باعث افزایش کارایی طیفی می‌شود، بلکه عملکرد محرمانگی را نیز به‌صورت هم‌زمان افزایش می‌دهد. با توجه به مزایای ذکر شده، موضوع امنیت لایه فیزیکی در سامانه‌های NOMA اخیراً توجه فراوانی را به خود جلب کرده است. مسئله برای به حداکثر رساندن میزان جمع محرمانه قابل‌دست‌یابی (SSR)[3] در سیستم NOMA تک ورودی تک خروجی (SISO)[4] برای اولین بار در [۶] مورد مطالعه قرار گرفت.

از آن زمان چندین تجزیه‌وتحلیل و مشکلات بهینه‌سازی انتقال محرمانه در سامانه‌های SISO NOMA با لینک ثابت در [۷] مورد مطالعه قرار گرفته است. بعلاوه با استفاده از فناوری آنتن چندگانه، مشکلات بهینه‌سازی SSR در سامانه‌های NOMA چند ورودی تک خروجی (MISO)[5] و چند ورودی چند خروجی (MIMO)[6] با استفاده از فرم پرتو و تخصیص توان در [۸] مورد بررسی قرار گرفت. بااین‌وجود (CSI)[7] لحظه‌ای شنودگران برای طراحی و بهینه‌سازی در کارهای چند آنتن موردنیاز است، که به‌دست آوردن آن در عمل دشوار است.

از سوی دیگر، این فرض که CSI آماری شنودگران شنود در دسترس است، در مقالات فعلی به‌طور گسترده‌تری پذیرفته شده است و سناریوهای مختلف NOMA و طرح‌های انتقال از منظر امنیت لایه فیزیکی بررسی شده است [۹]، نویز مصنوعی (AN)[8] [۱۰] و شبکه‌های در مقیاس بزرگ [۱۱] همگی بررسی شده‌اند. بااین‌حال، همه کارهای فوق فقط بر روی تجزیه‌وتحلیل عملکرد محرمانگی بدون بهینه‌سازی تخصیص توان متمرکز هستند که با طراحی مناسب می‌تواند عملکرد محرمانگی را بیشتر بهبود بخشد. اخیراً، چن و همکاران [۱۲] میزان محرمانگی سامانه‌های عظیم NOMA چند آنتن را بررسی کرده و تخصیص نیرو را برای افزایش امنیت بهینه کرده است. بااین‌حال، نویسندگان فرض کردند که شنودگران توانایی تشخیص چند کاربر را ندارند، که ممکن است توانایی‌های شنود آن‌ها را دست‌کم گرفته و منجر به عملکرد محرمانگی بیش‌ازحد خوش‌بینانه شود. علاوه بر این نتیجه‌گیری در مرز پایین تقریبی SSR با بهره‌گیری از ویژگی‌های آنتن‌های با تعداد بالا است که این یک مورد خاص است و نمی‌تواند در مورد سناریوی کلی اعمال شود.

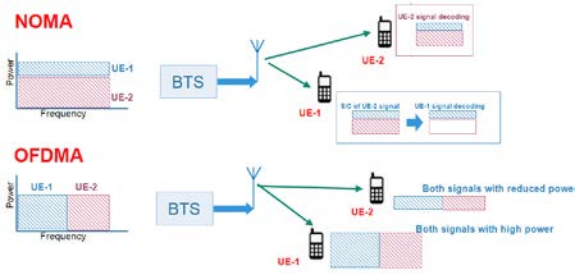
مقاله حاضر درنظر دارد با استفاده از اضافه کردن نویز مصنوعی به همراه سیگنال کاربران در فرستنده به روش تخصیص منابع نامتعامد، احتمال شنود سیگنال توسط شنودگر را کاهش دهد. در ادامه این مقاله به‌صورت زیر سازمان‌دهی شده است:
در بخش دوم مدل سیستم با در نظر گرفتن کاربران حقیقی و نویز مصنوعی ارائه شده و در بخش سوم شبیه‌سازی مورد بررسی قرار گرفته است. نتایج به‌دست‌آمده بیانگر رسیدن به نرخی بالاتر از مجموع نرخ محرمانگی در روش دسترسی چندگانه متعامد و همچنین بالاتر از مجموع نرخ محرمانگی در روش دسترسی چندگانه نامتعامد معمولی به مقدار قابل‌توجه می‌باشد. جمع‌بندی و بررسی نهائی طرح پیشنهادی در بخش آخر آورده شده است.

[1] Quality of Service
[2] Signal to Noise Ratio
[3] Secrecy Sum Rate
[4] Single-Input and Single-Output
[5] Multiple-Input and Single-Output
[6] Multiple-Input and Multiple-Output
[7] Channel State Information
[8] Artificial Noise

۲- مدل سیستم

در شکل (۱) ساختار مورد استفاده برای دو نوع مدولاسیون NOMA و OMA دو کاربر آورده شده است.

با فرض پهنای باند نرمالیزه یک هرتز در NOMA کل پهنای باند به‌طور مشترک برای دو کاربر استفاده شده است. به‌هرحال با OMA کاربر۱ از α هرتز استفاده می‌کند و باقی‌مانده $1-\alpha$ هرتز برای کاربر۲ در نظر گرفته می‌شود. در NOMA کاربر ۲ ابتدا SIC را برای رمزگشایی سیگنال کاربر۱ استفاده می‌کند تا زمانی که بهره کانال کاربر۲ بالاتر از کاربر۱ باشد. سیگنال رمزگشایی شده سپس از سیگنال دریافتی کاربر۲ کم می‌شود. سیگنال حاصل را برای رمزگشایی برای کاربر۲ استفاده می‌کند. برای کاربر۱، SIC موردنیاز نیست و سیگنال به‌صورت مستقیم رمزگشایی می‌شود؛ بنابراین، نرخ اطلاعات قابل‌دست‌یابی برای کاربر ۱ و کاربر ۲ توسط روابط (۱) و (۲) به‌دست می‌آید [۱۴].



شکل (۱): ساختار متداول **NOMA** و مقایسه با **OMA.**

$$R_1 = \log_2(1+\frac{P_1|h_1|^2}{P_2|h_1|^2+\sigma_n^2}) \quad (۱)$$

$$R_2 = \log_2(1+\frac{P_2|h_2|^2}{\sigma_n^2}) \quad (۲)$$

وقتی‌که P توان کاربرها، h بهره کانال هر کاربر و σ_n^2 توان نویز باشد.

برای OMA نرخ اطلاعات قابل‌دست‌یابی برای کاربر۱ و کاربر۲ توسط روابط (۳) و (۴) به‌دست می‌آید [۱۴].

$$R_1 = \alpha \log_2(1+\frac{P_1|h_1|^2}{\sigma_n^2}) \quad (۳)$$

$$R_2 = (1-\alpha)\log_2(1+\frac{P_2|h_2|^2}{\sigma_n^2}) \quad (۴)$$

از روابط (۱) و (۲) مشخص است که طرح NOMA بازدهی عملی را برای هر کاربر به‌وسیله تعدیل کردن نسبت اختصاص توان P_1/P_2 کنترل می‌کند. بنابراین، بازدهی کلی و دوستی با کاربر به‌طور نزدیکی با طرح اختصاص توان ارتباط دارد. برای کانال‌های نامتقارن وقتی‌که نسبت سیگنال به نویز SNR برای دو کاربر متفاوت باشد، می‌توان به‌صورت عددی نشان داد که مقدار R_1 و R_2 از روابط (۱) و (۲) به ترتیب قابل‌محاسبه است. که به مقدار زیادی بیشتر از مقدار R_1 و R_2 قابل‌محاسبه از روابط (۳) و (۴) است. مقایسه عددی به‌صورت پایه در ظرفیت کانال چندکاربره در [۴] آنالیز شده است. در حالت کلی بیشترین ظرفیت قابل دست‌یابی برای NOMA بیشتر از ظرفیت قابل دست‌یابی برای OMA است. بنابراین، NOMA زمانی که کانال‌های دو کاربر متفاوت باشد، بازدهی عملی سطح سیستم بالاتر و مؤثرتری دارد. بنابراین، NOMA یک طرح روش دسترسی قابل پیش‌بینی برای آینده ارتباطات رادیویی است. همچنین NOMA می‌تواند با همین شرایط برای طرح فراسو نیز مورداستفاده قرار بگیرد. در فراسو SIC در BS مورد استفاده قرار می‌گیرد.

در طرح پیشنهادی برای بالا رفتن امنیت حتی بیشتر از حالت‌های عادی در روش دسترسی نامتعامد که به‌صورت ذاتی امنیتی بیشتر از روش‌های دسترسی متعامد دارد و ازنظر نرخ محرمانگی در شرایط بهتری به سر می‌برد، از نویز مصنوعی استفاده شده است.

نویز مصنوعی یک پیام حاوی اطلاعات بی‌ارزش یا اطلاعات اشتباه است که سهمی از توان ارسالی را به خود اختصاص می‌دهد. درواقع تنها برای گمراه کردن شنودگرها و ایجاد کردن این فرض برای آن‌ها که این سهم از توان حاوی اطلاعات اصلی از یک کاربر است، فرستاده می‌شود. نویز مصنوعی به‌طورمعمول دارای انرژی بیشتری نسبت به بقیه کاربران است و همراه با سیگنال بقیه کاربران فرستاده می‌شود [۱۳].

به‌این‌علت که گیرنده اطلاعات این سهم از توان را دارد و از اساس می‌داند که این همان نویز مصنوعی است که توسط فرستنده و طور عمد تولید شده است، وقتی به کاربر حقیقی برسد کاربر در ابتدا آن را به‌سادگی حذف می‌کند و روش SIC را برای فهمیدن اطلاعات دیگر کاربران را بعد از حذف این سیگنال آغاز می‌کند. آن‌چنان‌که سهم توان بعد از آن را به‌عنوان کاربر اول محسوب کرده و به روش گفته‌شده در فصل قبل تک‌تک کاربران را شناسایی می‌کند.

نکته جالب این است که شنودگر به علت این‌که اطلاعات این سیگنال و اطلاعات حالت کانال را ندارد نمی‌تواند تشخیص دهد که سیگنال نویز مصنوعی حاوی اطلاعات صحیح نیست و چون غالباً این سیگنال بزرگ‌ترین سهم توان را دارد، آن را به‌عنوان یک سیگنال اصلی به‌حساب می‌آورد و سعی در شناسایی

آن خواهد داشت. ازاین‌رو، برای به‌دست آوردن نرخ شنودگر در مخرج کسر از این قسمت به‌عنوان تداخل در به‌دست آوردن SINR استفاده می‌شود.

در اینجا به بیان روابط از فرستنده تا گیرنده پرداخته می‌شود که مانند دیگر طرح‌های دسترسی چندگانه نامتعامد سیگنال‌های تولیدشده باید با یکدیگر جمع شده و بعد ارسال می‌شوند. در شبکه مدنظر، همان‌طور که گفته شد برای ارتقای امنیت اطلاعات، از نویز مصنوعی برای کمک به انتقال امن اطلاعات استفاده می‌شود.

در مدل اول برای ساده نشان دادن انتقال از دو کاربر استفاده شده است و با توجه به سیگنال نویز مصنوعی سه سهم از توان اصلی که دوتای آن برای کاربران و یکی برای نویز مصنوعی می‌باشد، با یکدیگر جمع می‌شوند. بنابراین، با توجه به SC سیگنال‌های ارسالی به‌صورت زیر خواهند بود [۶]:

$$S[n] = \sqrt{\alpha_1 P}x_1[n] + \sqrt{\alpha_2 P}x_2[n] + \sqrt{\alpha_3 P}x_a[n] \quad (۵)$$

که $x_1[n]$ و $x_2[n]$ سمبل‌های کاربران ۱ و ۲ در شیارهای زمانی nام و $x_a[n]$ نویز مصنوعی است که برای دفاع در مقابل شنودگر استفاده می‌شود و α_3 ضریب تخصیص توان برای نویز مصنوعی را نشان می‌دهد. ازآن‌جهت که α_1، α_2 و α_3 ضریب‌های تخصیص توان هستند؛ یعنی کل مقدار توان P را به نسبت‌هایی بین کاربران تقسیم می‌کنند باید مجموع آن‌ها یک شود. پس داریم [۶]:

$$\alpha_3 + \alpha_2 + \alpha_1 = 1 \quad (۶)$$

همچنین از فرضیات این طرح، این است که $\alpha_2 < \alpha_1$ باشد یعنی توان اختصاص‌یافته به کاربر اول بیشتر از توان اختصاص‌یافته به کاربر دوم است. دلیل آن هم واضح است، فرقی بین حالت عملی یا حالت آزمایشگاهی وجود ندارد، فاصله کاربرها یکسان نیست و حتی اگر هم باشد، واضح است که شرایط کانال دو کاربر هم فاصله از فرستنده با یکدیگر یکسان نیست. در روش دسترسی چندگانه نامتعامد برای برقراری عدالت بین کاربران به کاربر دورتر یا دارای شرایط کانال ضعیف‌تر توان بیشتری اختصاص داده می‌شود تا از قطع شدن ارتباط کاربران در لبه سلول جلوگیری شود.

در اینجا فرض می‌شود که نویز مصنوعی انتقالی که توسط فرستنده با یک دنباله شبه تصادفی تولید کرده است، ایجاد شده است که آن را گیرنده‌های حقیقی مانند D_1 و D_2 می‌دانند ولی برای شنودگرهای باقی‌مانده، ناشناخته است.

علاوه‌بر این بر اساس پروتکل گیرندگی در روش دسترسی چندگانه نامتعامد D_1 سمبل $x_1[n]$ مربوط به خود را با در نظر گرفتن سمبل $x_2[n]$ به‌عنوان نویز رمزگشایی می‌کند. به‌این‌علت که توان کاربر۱ از کاربر۲ و در صورت داشتن تعداد کاربران بیشتر از تمامی آن‌ها بیشتر است، کاربر۱ سیگنال کاربر۲ یا تمامی دیگر کاربران را به‌عنوان نویز شناسایی کرده و به رمزگشایی سیگنال خود می‌پردازد.

بنابراین، SINR دریافتی در D_1 که با $\gamma_{x_1}^d$ نمایش داده شده برای به‌دست آوردن سمبل $x_1[n]$ به‌صورت زیر است [۶]:

$$\gamma_{x_1}^d = \frac{\alpha_1 P \left|h_{s.D_1}\right|^2}{\alpha_2 P \left|h_{s.D_1}\right|^2 + \sigma_n^2} \quad (۷)$$

که در آن، $h_{s.D_1}$ بهره کانال از فرستنده به گیرنده کاربر اول است.

همچنین نرخ دریافتی برای گیرنده D_1 به‌صورت زیر خواهد بود [۱۴]:

$$R_b^1 = \log_2(1 + \frac{\alpha_1 P \left|h_{s.D_1}\right|^2}{\alpha_2 P \left|h_{s.D_1}\right|^2 + \sigma_n^2}) \quad (۸)$$

در سمت دیگر، با توجه به پروتکل گیرندگی دسترسی چندگانه نامتعامد، کاربر دیگر با شرایط کانال قوی‌تر (در اینجا D_2) ابتدا نیاز دارد تا اطلاعات کاربر با بهره کانال بیشتر از خود (در اینجا D_1) را رمزگشایی کند و از مقدار کل سیگنال دریافتی کم کند و سپس اطلاعات مربوط به خود را با توجه به SIC به‌دست آورد. بنابراین، SINR برای $x_1[n]$ و SNR برای $x_2[n]$ در گیرنده D_2 به‌صورت زیر به‌دست می‌آید [۶]:

$$\gamma_{x_1 \to x_2}^d = \frac{\alpha_1 P \left|h_{s.D_2}\right|^2}{\alpha_2 P \left|h_{s.D_2}\right|^2 + \sigma_n^2} \quad (۹)$$

که در آن، $x_1 \to x_2$، SINR موردنیاز در D_2 برای رمزگشایی سمبل $x_1[n]$، و $h_{s.D_2}$ بهره کانال از فرستنده به گیرنده کاربر دوم است.

بعد از رمزگشایی $x_1[n]$ و کم کردن آن از سیگنال اصلی نوبت به سیگنال باقیمانده مربوط به $x_2[n]$ و دیگر کاربران می‌شود که در اینجا چون مدل دو کاربر را داریم تمام سیگنال مربوط به $x_2[n]$ است و دیگر در محاسبه نسبت توان به نویز آن در قسمت نویز تداخلی از دیگر کاربران نداریم که SNR آن به‌صورت زیر خواهد بود [۶]:

$$\gamma_{x_2}^d = \frac{\alpha_2 P \left|h_{s.D_2}\right|^2}{\sigma_n^2} \quad (۱۰)$$

همچنین نرخ دریافتی برای گیرنده دوم به‌صورت زیر خواهد [۱۴]:

$$R_b^2 = \log_2(1 + (\frac{\alpha_1 P |h_{s.D_2}|^2}{\alpha_2 P |h_{s.D_2}|^2 + \sigma_n^2} + \frac{\alpha_2 P |h_{s.D_2}|^2}{\sigma_n^2})) \quad (۱۱)$$

باید در نظر گرفت که برای شنودگرها هم فرضیات مشابهی برقرار است. بدترین شرایط را در شبکه‌هایی با ابعاد بزرگ در نظر گرفته می‌شود که شنودگرها دارای قدرت تشخیص بالا برای فهمیدن داده‌های کاربران حقیقی هستند. بنابراین، SINR آن‌ها برای تشخیص اطلاعات حقیقی $x_1[n]$ و $x_2[n]$ در شنودگرها به‌صورت زیر بیان می‌شود:

$$\gamma_{E_L} = \max_{k=1,\dots,K} \frac{\alpha_L P |h_{s.E_K}|^2}{\alpha_3 P |h_{s.E_K}|^2 + \sigma_E^2} \quad (۱۲)$$

وقتی که $h_{s.E_K}$ بهره کانال از فرستنده به گیرنده شنودگر است. $L \in \{1.2\}$ که به این معنی است که احتمال نرخ شنود را برای کاربران ۱ و ۲ حساب کرده و بعداً برای به‌دست آوردن R_S، از نرخی که از SNR بالا به‌دست آمد، استفاده می‌شود، که رابطه نرخ شنودگر به‌صورت زیر است [۱۴]:

$$R_{E_L} = \log_2(1 + (\frac{\alpha_L P |h_{s.E_K}|^2}{\alpha_3 P |h_{s.E_K}|^2 + \sigma_E^2})) \quad (۱۳)$$

سپس با توجه به فرمول‌های نرخ محرمانگی که در زیر به آن‌ها اشاره می‌شود، نرخ محرمانگی هر کاربر و میانگین آن‌ها محاسبه می‌شود.

$$R_s^m = [R_b^m - R_e^m]^+ \quad (۱۴)$$

$$R_s = \sum_{m=1}^{M} R_s^m \quad (۱۵)$$

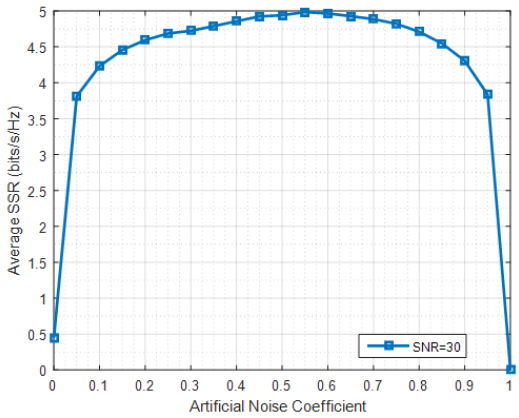
۳- شبیه‌سازی و بررسی نتایج

در این قسمت شبیه‌سازی SSR در مقابل مقدار سهم نویز مصنوعی نسبت به سهم بقیه کاربران در حالاتی که دو کاربر با یکدیگر سهم تقریباً برابر داشته باشند و برای حالاتی که شبکه دایره‌ای به دور یک سلول یا به‌فرم ایده‌آل دو کاربر که دارای فاصله یکسانی باشند، در نظر گرفته شده است.

در شکل (۲) که برای طرح دو کاربر با نسبت توان‌های تقریباً برابر شبیه‌سازی شده است، مشاهده می‌شود که با سهم ۰/۵۵ از توان کل بیشترین مقدار SSR به‌دست می‌آید و این به این یعنی است که در حالت بهینه باید این مقدار از توان کل را به نویز مصنوعی اختصاص داد و بقیه مقدار را بین دیگر کاربران تقسیم کرد. البته با توجه به اینکه در شرط ارسال نویز مصنوعی داریم که برای فریب شنودگر باید مقدار سهم نویز مصنوعی از توان کل، از بیشترین سهم یک کاربر حقیقی بیشتر باشد و در این طرح مقدار نسبت توان کاربران به هم، برابر است پس فقط کافی است مقدار سهم نویز مصنوعی از ۳۴ درصد توان کل بیشتر باشد در این صورت هر یک از دو کاربر دیگر سهمی کمتر از نویز مصنوعی دارند و شنودگر در صورت اعمال نویز مصنوعی قادر به شناسایی سیگنال نیست[۱۴].

در این قسمت مجموع نرخ محرمانگی کاربران در حالت‌های دو تا ۲۰ کاربر در سهم‌های نویز مصنوعی مختلف به نمایش گذاشته شده است. همان‌طور که در شکل (۳) مشخص است با اضافه شدن تعداد کاربران مقدار SSR کاهش می‌یابد و این کاهش در ابتدا شدید و در انتها حالت به‌آرامی اتفاق می‌افتد.

دلیل آن هم این است که در حالت ۲ کاربر تفاوت بین نرخ کاربر اول و دوم بسیار زیاد است و کاربران دوم سهم بسیار زیادی از توان را به خود اختصاص می‌دهد اما هرچه تعداد کاربران بیشتر می‌شود، مقدار توان کل بین آن‌ها تقسیم شده و هنگامی‌که از آن‌ها میانگین گرفته می‌شود، مقدار SSR کمتری از حالت‌های با کاربر کمتر به‌دست می‌دهند [۱۵].

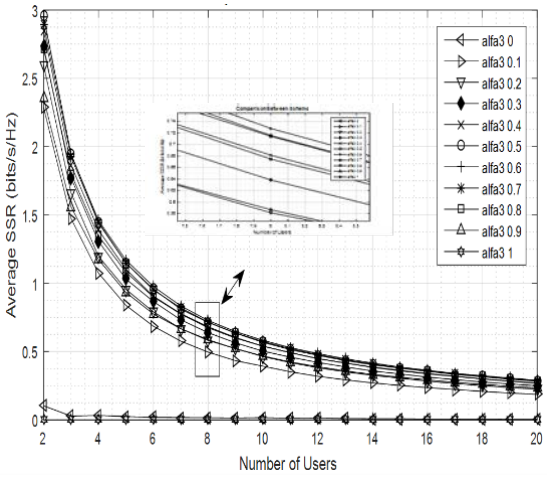


شکل (۲): محاسبه سهم بهینه نویز مصنوعی در طرح دو کاربر

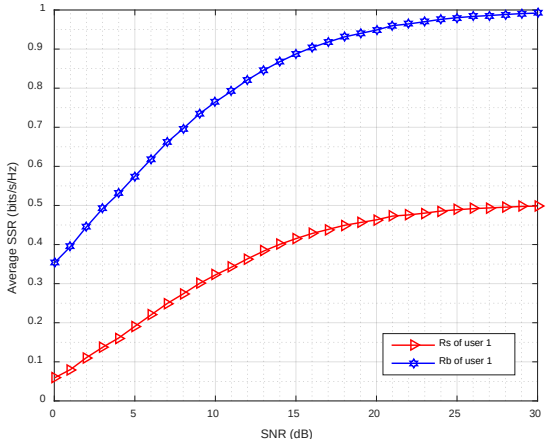
در این بخش مجموع نرخ محرمانگی طرح پیشنهادی که استفاده از NOMA به همراه نویز مصنوعی است، با روش دسترسی چندگانه نامتعامد متداول و روش دسترسی چندگانه متعامد در طرح دو کاربر با یکدیگر مقایسه شده است. در شکل (۳) مشاهده می‌شود که طرح NOMA متداول مجموع نرخ محرمانگی بیشتری نسبت به طرح OMA دارد. اما تفاوت چندانی درمجموع نرخ محرمانگی آن‌ها نیست. ولی طرح NOMA به همراه نویز مصنوعی ارائه شده در این مقاله اختلاف بسیار زیادی را در این نرخ نسبت به دو روش قبلی دارد. دو روش قبل در

مقاله بیشینه‌سازی مجموع نرخ محرمانگی نوشته آقای ژانگ و همکاران به‌دست آورده شده است [۱۶].

شکل (۴) نشان‌دهنده نرخ کاربر ۱ قبل و بعد از شنود در طرح روش دسترسی نامتعامد دو کاربرِ به کمک نویز مصنوعی که در حالتی نسبت توان کاربران حقیقی تقریباً برابر باشد را نشان می‌دهد. در این شکل نرخ کاربر قبل و بعد از شنود در توان‌های صفر dB ۰ تا dB ۳۰ نشان داده شده است. در این شکل مشاهده می‌شود که نرخ کاربر اول با توجه به اینکه بیشترین شنود را متحمل می‌شود در توان‌های پایین حدود یک‌ششم و در توان‌های بالا در حدود نصف آن شنود می‌شود. این بدان معنی است که تا توان dB ۲۰ که بعداً از نمودار به اشباع می‌رود، هرچه توان بیشتر شود احتمال شنود در طرح پیشنهادی کمتر می‌شود.



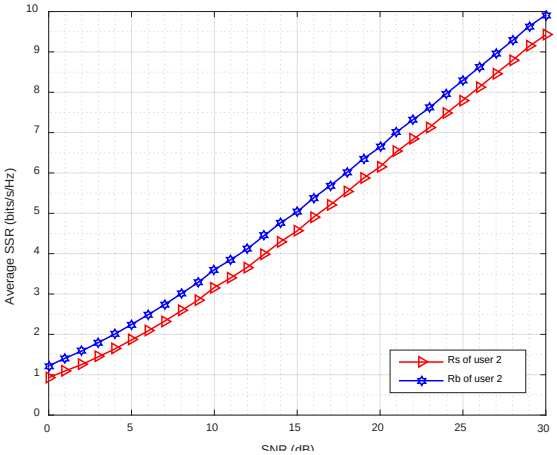
شکل (۳): مقایسه مجموع نرخ محرمانگی در حالت‌های تا ۲۰ کاربر



شکل (۴): نرخ کاربر ۱ قبل و بعد از شنود در طرح دو کاربر با نسبت توان‌های تقریباً برابر

در شکل (۵) نرخ کاربر دوم قبل و بعد از شنود مشاهده می‌شود. کاربر دوم به علت این‌که در روش دسترسی چندگانه نامتعامد دو کاربر، با توجه به روش گیرندگی SIC در مخرج SNR آن دیگر کاربری به‌عنوان نویز اضافه نمی‌شود و از مقدار نرخ چیزی کم نمی‌شود، SSR بهتری نسبت به کاربر اول دارد اما مقدار شنود از آن همان مقداری است که از کاربر اول کم می‌شد درصورتی‌که درصد شنود آن بسیار کمتر از کاربر اول و در حدود یک‌سوم در SNRهای پایین و تا یک بیستم در SNRهای بالا متغیر است.

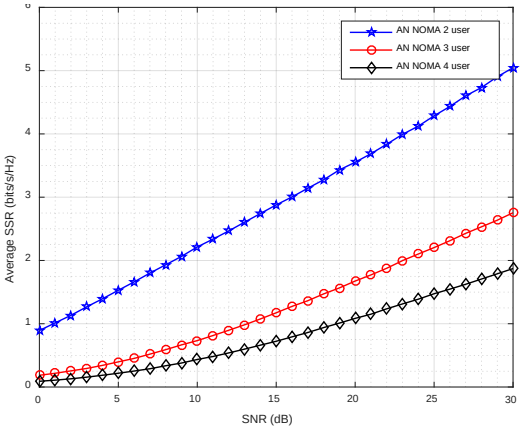
علت این تفاوت در رابطه نرخ مخصوصاً برای کاربران آخر است؛ جایی که در مخرج SNR رابطه نرخ شنودگر، نویز مصنوعی به‌عنوان نویز (کاربران قبلی) به‌حساب آمده و به علت بزرگ بودن آن نرخ شنودگر را کم و آسیب شنود را تا حد بالایی خنثی می‌کند.



شکل (۵): نرخ کاربر ۲ قبل و بعد از شنود در طرح دو کاربر با نسبت توان‌های تقریباً برابر

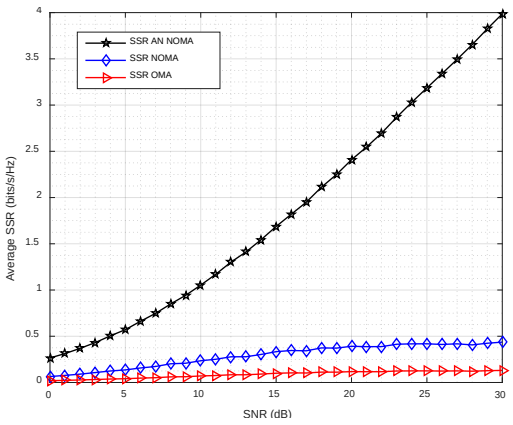
تا این قسمت نتایج شبیه‌سازی نرخ محرمانگی کاربران برای طرح دو کاربر ارائه شد، در شکل (۶) بخش مجموع نرخ محرمانگی در هر یک از طرح‌های دو، سه و چهار کاربر در یک نمودار به نمایش گذاشته می‌شود.

در این نمودار مشاهده می‌شود که در یک SNR مشخص مقدار مجموع نرخ محرمانگی طرح دو کاربر بیشتر از طرح سه کاربر و مجموع نرخ محرمانگی سه کاربر بیشتر از چهار کاربر است. علت این موضوع این است که در طرح دو کاربر، توان باقی‌مانده بعد از کم شدن سهم نویز مصنوعی بین دو کاربر تقسیم می‌شود و به‌این‌علت، مجموع نرخ محرمانگی از دو کاربر با نرخ بالاتر حساب می‌شود. اما در طرح سه و چهار کاربر این مقدار از توان بین تعداد بیشتری کاربر تقسیم و درنتیجه بعد از شنود مجموع نرخ محرمانگی کمتری دارند.



شکل (۶): مقایسه مجموع نرخ محرمانگی در طرح‌های دو، سه و چهار کاربر

در این بخش مجموع نرخ محرمانگی طرح پیشنهادی که استفاده از NOMA به همراه نویز مصنوعی است، با روش دسترسی چندگانه نامتعامد متداول و روش دسترسی چندگانه متعامد در طرح دو کاربر با یکدیگر مقایسه شده است. در شکل (۷) مشاهده می‌شود که طرح NOMA متداول مجموع نرخ محرمانگی بیشتری نسبت به طرح OMA دارد. اما تفاوت چندانی درمجموع نرخ محرمانگی آن‌ها نیست. ولی طرح NOMA به همراه نویز مصنوعی ارائه شده در این پایان‌نامه اختلاف بسیار زیادی را در این نرخ نسبت به دو روش قبلی دارد. دو روش قبل در مقاله بیشینه‌سازی مجموع نرخ محرمانگی نوشته آقای ژانگ و همکاران به‌دست آورده شده است. علت این تفاوت در رابطه نرخ مخصوصاً برای کاربران آخر است؛ جایی که در مخرج SNR رابطه نرخ شنودگر، نویز مصنوعی به‌عنوان نویز (کاربران قبلی) به‌حساب آمده و به علت بزرگ بودن آن نرخ شنودگر را کم و آسیب شنود را تا حد بالایی خنثی می‌کند.



شکل (۷): مقایسه طرح پیشنهادی با طرح‌های قبلی

۴- نتیجه‌گیری

استفاده از اضافه کردن نویز مصنوعی به همراه سیگنال کاربران در فرستنده می‌تواند مجموع نرخ محرمانگی افزایش را دهد. برای این منظور ابتدا نیاز است مقدار سهم نویز مصنوعی مناسب برای اثربخش بودن مقدار SSR به‌دست آورده شود. در این مقاله در شرایط مختلف و در سناریوهای ۲ تا ۲۰ کاربر این مقدار به‌دست آورده شده است. بعد از آن مقدار SSR در SNRهای مختلف برای طرح‌های ۲ کاربر دسترسی چندگانه متعامد، دسترسی چندگانه نامتعامد متداول و دسترسی چندگانه نامتعامد با اضافه کردن نویز مصنوعی بررسی شده و مشاهده گردید که طرح پیشنهادی عملکرد امنیتی بیشتری نسبت به دیگر طرح‌ها ایجاد می‌کند. نتایج به‌دست آمده نشان می‌دهد که، به‌عنوان‌مثال در یک SNR مشخص مانند ۱۰dB، مجموع نرخ محرمانگی برای روش دسترسی چندگانه متعامد در حدود ۰/۱، برای روش دسترسی چندگانه نامتعامد متداول در حدود ۰/۲۵ و برای روش دسترسی چندگانه نامتعامد با استفاده از نویز مصنوعی در حدود ۱ بیت بر ثانیه بر هرتز است. باید در نظر داشت که هزینه بالا رفتن امنیت با توجه به طرح پیشنهادی، از دست دادن مقداری از توان به‌عنوان توان نویز مصنوعی می‌باشد که طبیعتاً بالا رفتن هزینه و انرژی را به دنبال دارد. این طرح در کاربردهای نظامی و یا مواردی که اطمینان از امنیت در اولویت اول قرار دارد، توجیه‌پذیر بوده و مزیت بالا بردن امنیت بر این ضرر غلبه می‌کند.

تشکر و قدردانی

نویسندگان این مقاله از حمایت‌های مرکز علم و فناوری ارتباطات و شبکه دانشگاه جامع امام حسین(ع) کمال سپاسگزاری را دارند.

۵- مراجع

[1] L. Dai, B. Wang, Y. Yuan, S. Han, I. Chih-Lin, and Z. Wang, “Nonorthogonal multiple access for 5G: solutions, challenges, opportunities, and future research trends,” IEEE Commun. Mag., vol. 53, no. 9, pp. 74–81, September 2015.

[2] Y. Saito, Y. Kishiyama, A. Benjebbour, T. Nakamura, A. Li, and K. Higuchi, “Non-Orthogonal multiple access (NOMA) for cellular future radio access,” in Proc. IEEE Veh. Technol. Conf. (VTC), Dresden, Germany, pp. 1–5, Jun 2013.

[3] Z. Ding, H. Dai, and H. V. Poor, “Relay Selection for Cooperative NOMA,” IEEE Wireless Commun. Lett., vol. 5, no. 4, pp. 416–419, Aug. 2016, pp. 1393–1405, 2016.

[4] S. Timotheou and I. Krikidis, “Fairness for non-orthogonal multiple access in 5G systems,” IEEE Signal Process. Lett., vol. 22, no. 10, pp. 1647–1651, Oct. 2015.

[5] H.-M. Wang, T.-X. Zheng, J. Yuan, D. Towsley, and M. H. Lee, "Physical layer security in heterogeneous cellular networks," IEEE Trans. Commun., vol. 64, no. 3, pp. 1204–1219, Mar. 2016.

[6] Y. Zhang, H.-M. Wang, Q. Yang, and Z. Ding, "Secrecy sum rate maximization in non-orthogonal multiple access," IEEE Commun. Lett. vol. 20, no. 5, pp. 930–933, May 2016.

[7] M. Qin, S. Yang, H. Deng, and M. H. Lee, "Enhancing security of primary user in underlay cognitive radio networks with secondary user selection," IEEE Access, vol. 6, pp. 32624–32636, 2018.

[8] N. Nandan, S. Majhi, and H. C. Wu, "Secure beamforming for MIMO NOMA based cognitive radio network," IEEE Commun. Lett., vol. 22, no. 8, pp. 1708–1711, Aug. 2018.

[9] Z. Yang, J. A. Hussein, P. Xu, Z. Ding, and Y. Wu, "Power allocation study for non-orthogonal multiple access networks with multicastunicast transmission," IEEE Trans. Wireless Commun., vol. 17, no. 6, pp. 3588–3599, Jun. 2018.

[10] L. Lv, Z. Ding, Q. Ni, and J. Chen, "Secure MISO-NOMA transmission with artificial noise," IEEE Trans. Veh. Technol., vol. 67, no. 7, pp. 6700–6705, Jul. 2018.

[11] Y. Liu, Z. Qin, M. Elkashlan, Y. Gao, and L. Hanzo, "Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks," IEEE Trans. Wireless Commun., vol. 16, no. 3, pp. 1656– 1672, Mar. 2017.

[12] X. Chen, Z. Zhang, C. Zhong, D. W. K. Ng, and R. Jia, "Exploiting inter-user interference for secure massive non-orthogonal multiple access," IEEE J. Sel. Areas Commun., vol. 36, no. 4, pp. 788–801, Apr. 2018.

[13] M. F. Hanif, Z. Ding, T. Ratnarajah, and G. K. Karagiannidis, "A minorization-maximization method for optimizing sum rate in the downlink of non-orthogonal multiple access systems," IEEE Trans Signal Process, vol. 64(1), pp. 76-88, 2016.

[14] Y. Zhang, H.-M. Wang, T.-X. Zheng, and Q. Yang, "Energy-efficient transmission design in non-orthogonal multiple access. IEEE Trans Veh Technol," vol. 66(3), pp. 2852-2857, 2017.

[15] Ming Zeng, Man-Phong Nguyen, A. Dobre Octavia, H. Vincent Poor, "Securing Downlink Massive MIMO-NOMA Networks With Artificial Noise," IEEE Journal of Selected Topics in Signal Processing, vol. 13, Issue 3, June 2019.

[16] Pooja Singh and Aditya Trivedi, "NOMA and massive MIMO assisted physical layer security using artificial noise precoding," Physical Communication, vol. 39, April 2020.

[17] S. M. Riazul Islam, Nurilla Avazov, Octavia A. Dobre, and Kyung-Sup Kwak, "Power-Domain Non-Orthogonal Multiple Access (NOMA) in 5G Systems: Potentials and Challenges," IEEE Communications Surveys & Tutorials vol. 19, Issue 2, 2017.