مقاله پژوهشی

انتخاب کاربران و جمرهای با قابلیت برداشت انرژی در شبکه‌های چندبانده لینک بالای NOMA جهت بهبود عملکرد و امنیت شبکه

مریم نجیمی

چکیده: در این مقاله، ارسال امن لینک بالا در ارسال چندگانه غیر متعامد (NOMA) با انتخاب کاربرهای مناسب جهت ارسال به سمت ایستگاه پایه (BS) در هر کانال و جمرهایی با قابلیت برداشت انرژی بررسی می‌گردد. در واقع، هر فریم زمانی به دو فاز تقسیم می‌شود. در فاز اول، جمرها توان خود را از ایستگاه پایه برداشت می‌کنند و در فاز دوم، کاربران انتخاب‌شده، ارسال لینک بالا را به صورت NOMA به ایستگاه پایه انجام می‌دهند، در حالی که جمر انتخاب‌شده، نویز ساختگی خود را برای گمراه‌کردن کاربر استراق سمع‌کننده ارسال می‌کند. در واقع، مسئله مورد نظر، بهینه‌سازی قابلیت گذردهی محرمانه با انتخاب کاربرهای مناسب در هر کانال فرکانسی جهت ارسال داده به ایستگاه پایه و نیز انتخاب جمرهای مناسب است، البته با قیودی که روی احتمال قطعی محرمانه (SOP) و احتمال قطعی ارتباط (COP) در نظر گرفته می‌شود. مسئله مورد نظر با استفاده از روش‌های مبتنی بر بهینه‌سازی محدب و شرایط KKT برای انتخاب کاربران مناسب، مطرح و الگوریتمی برای حل آن پیشنهاد می‌گردد و عملکرد سیستم برای روش پیشنهادی ارزیابی می‌شود. نتایج شبیه‌سازی بیانگر آن است که روش پیشنهادی، عملکرد بهتری از نظر بهبود قابلیت گذردهی و ایجاد امنیت در شبکه در شرایط و سناریوهای متفاوت نسبت به الگوریتم‌های محک در نظر گرفته شده دارد.

کلیدواژه: **NOMA، قابلیت گذردهی، احتمال قطعی محرمانه، احتمال قطعی ارتباط.**

۱- مقدمه

اخیراً NOMA[1] یک تکنیک اساسی برای رفع مشکلات نسل بعدی شبکه‌های ارتباطی بی‌سیم مانند قابلیت اطمینان بالا و کاربری کارامد طیف می‌باشد. برخلاف تکنیک‌های مرسوم یا دسترسی چندگانه متعامد (OMA)[2]، در NOMA چندین کاربر می‌توانند به طور هم‌زمان از منابع یکسانی (مانند زمان، فرکانس و کد) استفاده کنند. در این مقاله، کدینگ در سمت فرستنده انجام می‌شود در حالی که لغو تداخل پشت سر هم (SIC) در سمت گیرنده انجام می‌پذیرد تا امکان استفاده از منابع یکسان با سطوح توان متفاوت امکان‌پذیر باشد [۱] و [۲].

به عبارت دیگر به واسطه طبیعت انتشار کانال‌های بی‌سیم و کاربردهای وسیع تکنولوژی ارتباطات، امنیت اطلاعات بی‌سیم با چالش‌های بزرگی روبه‌رو می‌شود. به عبارت دیگر، امنیت لایه فیزیکی (PLS)[3] منجر به نگرانی زیادی در شبکه‌های NOMA شده است. در واقع PLS از پارامترهای تصادفی کانال‌های بی‌سیم بهره‌برداری می‌کند تا سیگنال‌های ارسالی را که می‌توانند توسط استراق سمع‌کننده[4] دیکد شوند به دست آورد. در [۳]، امنیت لایه فیزیکی NOMA در شبکه‌های با مقیاس وسیع در سناریوهای ارسال تک‌آنتنه و چندآنتنه و احتمال قطعی امن برای هر دو سناریو در نظر گرفته می‌شود. در بخش بعد پیشینه تحقیق مربوط به مقاله بیان گردیده است.

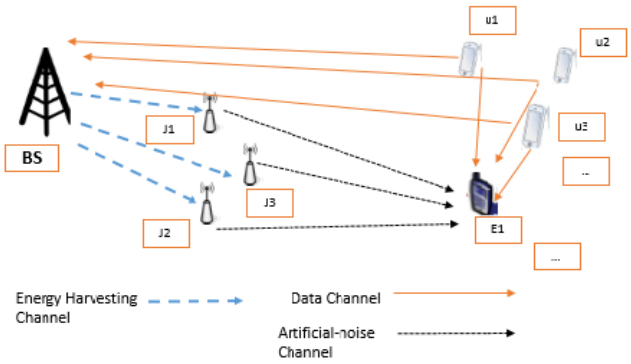
۲- پیشینه تحقیق

در [۴]، یک سیستم NOMA هماهنگ دوطرفه با دو کاربر پیشنهاد می‌گردد و SOP هر دو کاربر و مجموع ظرفیت ارگادیک بررسی می‌گردد. در [۵]، بهینه‌سازی توان ارسالی و نرخ اطلاعات با توجه به محدودیت‌های احتمال قطعی امن و کیفیت سرویس در نظر گرفته می‌شود. در [۶]، نویسندگان یک شبکه رادیویی هوشمند NOMA چندورودی تک‌خروجی را در حضور چندین استراق سمع‌کننده در نظر می‌گیرند و طرح جمینگ هماهنگ با نویز ساختگی را برای بهبود امنیت شبکه اولیه به کار می‌برند. در [۷]، یک طرح پرتوی با کمک نویز ساختگی به همراه تخصیص توان پیشنهاد می‌گردد تا عملکرد امن را برای ارسال لینک پایین NOMA بهبود دهد. در واقع، استفاده از جمرها برای ارسال نویز ساختگی، یک تکنیک مؤثر برای غلبه بر استراق سمع می‌باشد [۸]. در واقع، در حالت لینک پایین، ایستگاه پایه (BS)[5] به چندین آنتن مجهز می‌شود تا از تکنیک پرتوی به عنوان یک روش ارسال امن استفاده کند. با وجود این، به واسطه محدودیت‌های توان گره‌ها در شبکه‌های عملی و سختی امکان استفاده از چندین آنتن در ایستگاه پایه و نیز به دلیل آن که خیلی از گره‌ها توانایی صرف انرژی خود را برای تولید نویز ساختگی ندارند، توانایی برداشت انرژی[6] در جمرها در [۹] و [۱۰] بیان می‌گردد؛ به طوری که گره‌های با قابلیت برداشت انرژی به عنوان جمر استفاده می‌شوند تا سرویس‌های جمینگ را برای ارسال محرمانه انجام دهند. به عبارت دیگر، جمینگ هماهنگ به همراه برداشت انرژی یک روش مناسب برای ارسال امن در سناریوی NOMA لینک بالا[7] می‌باشد. در [۱۱]، یک شبکه بی‌سیم همکارانه در نظر گرفته می‌شود که در آن، یک منبع و چندین گره میانی وجود دارند که از میان آنها یک جفت رله انتخاب می‌شود، در حالی

این مقاله در تاریخ ۲۸ دی ماه ۱۳۹۹ دریافت و در تاریخ ۴ بهمن ماه ۱۴۰۰ بازنگری شد.

مریم نجیمی، (نویسنده مسئول)، دانشکده مهندسی برق و کامپیوتر، دانشگاه علم و فناوری مازندران، بهشهر، ایران، (email: maryam_najjimi1361@yahoo.com).

1. Non-Orthogonal Multiple Access
2. Orthogonal Multiple Access
3. Physical Layer Secrecy
4. Eavesdropper
5. Base Station
6. Energy Harvesting
7. Uplink



شکل ۱: دیاگرام شماتیک مدل سیستم.

که قابلیت برداشت انرژی را دارند. همچنین یک جمر برای ارسال سیگنال‌های امن به مقصد و سیگنال‌های جمینگ به استراق سمع‌کننده انتخاب می‌گردد. در [۱۲] از تکنیک NOMA چندکاربره جهت بهبود کارامدی انرژی و عملکرد سیستم استفاده می‌گردد، به طوری که کاربران مناسب به زیرکانال‌ها تخصیص داده می‌شوند. در [۱۳]، امنیت لایه فیزیکی در شبکه NOMA لینک بالا بررسی می‌گردد. در این حالت، دو کاربر برای NOMA انتخاب می‌گردند در حالی که یک کاربر به عنوان جمر دوستانه جهت گمراه‌کردن استراق سمع‌کننده انتخاب می‌شود. انتخاب جمر در دو حالت بررسی می‌گردد: حالت اول وقتی که اطلاعات حالت کانال استراق سمع‌کننده در دسترس نباشد و حالت دوم وقتی که این اطلاعات موجود باشد.

در این مقاله هدف، بهبود عملکرد سیستم NOMA امن لینک بالا در حالت چندکاربره با انتخاب جمرها و کاربرهای مناسب برای هر باند فرکانسی با توجه به قابلیت برداشت انرژی در جمرها می‌باشد. در واقع، مهم‌ترین اهداف این مقاله به صورت زیر بیان می‌گردد:

- مسئله انتخاب جمرهای با قابلیت برداشت انرژی و انتخاب کاربر مناسب در یک شبکه NOMA لینک بالا در هر کانال فرکانسی به منظور بهینه‌سازی عملکرد امن آن در حضور استراق سمع‌کننده بیان می‌گردد. همچنین اطلاعات کانال بین ایستگاه پایه و کاربران، جمرها و کاربران، کاربران و استراق سمع‌کننده و نیز جمرها و استراق سمع‌کننده دانسته فرض می‌گردد.
- پارامترهای مؤثر در تحلیل عملکرد شبکه، احتمال قطعی ارتباط (COP)[۱]، احتمال قطعی محرمانه (SOP)[۲] و قابلیت گذردهی محرمانه مؤثر (EST)[۳] می‌باشند.
- برای حل مسئله مورد نظر، با نگاشت اندیس‌های تخصیص[۴] از محدوده گسسته به پیوسته آن را ساده می‌نماییم و سپس از روش‌های بهینه‌سازی محدب[۵] برای به دست آوردن شرایط بهینه بر مبنای شرایط KKT[۶] استفاده می‌کنیم.
- شبیه‌سازی‌ها، کارامدبودن الگوریتم پیشنهادی را از نظر بهبود قابلیت گذردهی و پارامترهای COP و SOP بیان می‌کنند.

ساماندهی این مقاله به این ترتیب است که در بخش ۳ مدل سیستم بیان می‌گردد. بخش ۴ به توصیف پارامترهای مورد نظر برای تحلیل شبکه می‌پردازد، در حالی که در بخش ۵ به بیان مسئله مورد نظر با انتخاب کاربران و جمرهای مناسب در هر باند فرکانسی جهت بهینه‌سازی قابلیت گذردهی شبکه پرداخته می‌شود. بخش ۶ به الگوریتم پیشنهادی جهت حل مسئله اختصاص می‌یابد. بخش ۷ به نتایج شبیه‌سازی می‌پردازد و نتیجه نهایی مقاله در بخش ۸ بیان می‌گردد.

۳- مدل سیستم

یک شبکه بی‌سیم شامل یک ایستگاه پایه (BS)، یک استراق سمع‌کننده (E)، K کاربر NOMA و N جمر با قابلیت برداشت انرژی می‌باشد (شکل ۱). کاربران و ایستگاه پایه به صورت تک‌آنتنه هستند. با در نظر گرفتن طول هر فریم به اندازه T، دو فاز در هنگام برقراری ارتباط وجود دارد. فاز اول که به اندازه زمان αT می‌باشد، جهت ارسال انرژی RF بی‌سیم به جمرها جهت برداشت انرژی و فاز دوم که به اندازه زمان $(1-\alpha)T$ است، جهت ارسال به صورت NOMA و لینک بالا به ایستگاه پایه می‌باشد. به عبارت دیگر در این فاز، به منظور داشتن یک ارسال امن بین کاربران و ایستگاه پایه، جمرهایی با قابلیت برداشت انرژی در هر باند فرکانسی در نظر گرفته می‌شوند تا نویزهای ساختگی را برای گمراه‌کردن استراق سمع‌کننده ارسال نمایند.

در این مقاله، کانال‌های سیستم به فرم محوشدگی رایلی شبه‌ایستای مستقل[۷] در نظر گرفته می‌شوند و همه کانال‌های بین کاربران و ایستگاه پایه از رابطه $|h_{u_1,b}|^2 \le \ldots \le |h_{u_n,b}|^2 \le \ldots \le |h_{u_M,b}|^2$ تبعیت می‌کنند. به منظور کاهش تأخیر ناشی از انجام SIC، برای هر کانال فرکانسی یک جفت جهت انجام NOMA در نظر گفته می‌شود؛ بنابراین مطابق با اصول NOMA به صورت لینک بالا، ایستگاه پایه ابتدا سیگنال کاربر قوی‌تر u_n را دیکد می‌کند، به طوری که سیگنال ضعیف‌تر u_m را به صورت نویز در نظر می‌گیرد. سپس ایستگاه پایه با استفاده از تکنولوژی SIC، سیگنال u_n را حذف می‌کند و سپس سیگنال u_m را دیکد می‌کند. بنابراین SINR لحظه‌ای برای دیکدکردن سیگنال‌های u_n و u_m عبارت هستند از [۱۱]

$$\gamma_{n,b} = \frac{\rho_u |h_{n,b}|^2}{1+\rho_s |h_{m,b}|^2}, \quad (1)$$

$$\gamma_{m,b} = \rho_u |h_{m,b}|^2. \quad (2)$$

به طوری که $\rho_u = P_u/N$ و P_u توان ارسالی کاربران به ایستگاه پایه است. N واریانس نویز گوسی سفید جمع‌شونده می‌باشد، در حالی که $h_{n,b}$ و $h_{m,b}$ به ترتیب نشان‌دهنده کانال بین کاربر nام و کاربر mام با ایستگاه پایه هستند. به عبارت دیگر، به واسطه خاصیت انتشار کانال‌های بی‌سیم، استراق سمع‌کننده، تلاش برای رهگیری ارسال محرمانه بین کاربران و ایستگاه پایه را دارد. در مورد استراق سمع‌کننده فرض بر آن است که قابلیت آشکارسازی سیگنال u_n (u_m) بدون ایجاد تداخل با u_m (u_n) وجود دارد.

همان طور که بیان شد به منظور بهبود امنیت بین لینک‌های کاربران و BS در مقابل استراق سمع‌کننده، از میان کاربران، یک کاربر به عنوان جمر انتخاب می‌شود و از یک دنباله شبه‌تصادفی[۸] برای ارسال نویز

1. Connection Outage Probability
2. Secrecy Outage Probability
3. Effective Secrecy Throughput
4. Assignment Indices
5. Convex Optimization
6. Karush-Kuhn-Tucker
7. Independent Quasi-Static Raleigh Fading
8. Pseudo-Random Sequence

$$P_{c,n}=\Pr(C_{u_nb}<R_{n,t})=\begin{cases}\tilde{\Sigma}\left(\frac{1}{a+b}-\frac{e^{-a\bar{\gamma}_{n,t}}}{a\bar{\gamma}_{n,t}+b}\right)c & ,\ \bar{\gamma}_{n,t}\geq 1\\ \tilde{\Sigma}\left(\frac{e^{-\frac{(a+b)\bar{\gamma}_{n,t}}{1-\bar{\gamma}_{n,t}}}}{a\bar{\gamma}_{n,t}+b}+\frac{1}{a+b}-\frac{e^{-\frac{(a+b)\bar{\gamma}_{n,t}}{1-\bar{\gamma}_{n,t}}}}{a+b}-\frac{e^{-a\bar{\gamma}_{n,t}}}{a\bar{\gamma}_{n,t}+b}\right)c & ,\ 0<\bar{\gamma}_{n,t}<1\end{cases} \quad (7)$$

$$P_{c,m}=\Pr(C_{u_mb}<R_{m,t})=\begin{cases}1-\tilde{\Sigma}\frac{c}{a\bar{\gamma}_{n,t}+b}e^{-a\bar{\gamma}_{n,t}}e^{-(a\bar{\gamma}_{n,t}+b)\bar{\gamma}_{m,t}} & ,\ \bar{\gamma}_{n,t}\geq 1\\ 1-\tilde{\Sigma}\left(\frac{c}{a\bar{\gamma}_{n,t}+b}e^{-a\bar{\gamma}_{n,t}}\left(e^{-(a\bar{\gamma}_{n,t}+b)\bar{\gamma}_{m,t}}-e^{\frac{-(a\bar{\gamma}_{n,t}+b)\bar{\gamma}_{n,t}}{1-\bar{\gamma}_{n,t}}}\right)+\frac{c}{a+b}e^{\frac{-(a+b)\bar{\gamma}_{n,t}}{1-\bar{\gamma}_{n,t}}}\right) & ,\ 0<\bar{\gamma}_{n,t}<1\end{cases} \quad (8)$$

ساختگی استفاده می‌کند [۱۴]، به طوری که این دنباله برای BS و کاربران شناخته‌شده است در حالی که برای استراق سمع‌کننده ناشناخته می‌باشد و در نتیجه، منجر به گمراه‌شدن آن می‌گردد. با توجه به قابلیت برداشت انرژی در جمرهای منتخب، توان ارسالی جمر j ام که در فاز اول با توجه به برداشت انرژی دریافت نموده است عبارت است از

$$P_{r_j}=\frac{E_j}{(1-\alpha)T}=\frac{\alpha\eta P_b\left|h_{br_j}\right|^2}{1-\alpha} \quad (3)$$

به طوری که P_b توان ارسالی BS و h_{br_j} کانال بین ایستگاه پایه و جمر j ام می‌باشد. E_j مقدار انرژی برداشت‌شده در جمر مورد نظر می‌باشد در حالی که η بازده تبدیل انرژی است. در این حالت، SNR لحظه‌ای برای آشکارسازی سیگنال‌ها در استراق سمع‌کننده می‌تواند به صورت زیر بیان گردد

$$\gamma_{u_ke}=\frac{\rho_u\left|h_{u_ke}\right|^2}{\rho_t\left|h_{br_j}\right|^2\left|h_{r_je}\right|^2+1} \quad (4)$$

به طوری که $\rho_t=\alpha\eta\rho_b/(1-\alpha)$ و $\rho_b=P_b/N_0$ است. h_{u_ke} بیانگر کانال بین k امین کاربر و استراق سمع‌کننده می‌باشد و h_{r_je} بیانگر کانال بین جمر j ام و استراق سمع‌کننده است. در بخش بعد، پارامترهای مورد نظر برای مشخص‌کردن عملکرد شبکه بیان می‌گردد.

٤- پارامترهای مورد نظر جهت تحلیل عملکرد شبکه

در این بخش، پارامترهای COP، SOP و EST برای شبکه بیان می‌گردد.

قطعی ارتباط هنگامی اتفاق می‌افتد که ظرفیت کانال کمتر از یک نرخ آستانه ($R_{n,t}$ یا $R_{m,t}$) باشد. مطابق با ظرفیت کانال شانون، ظرفیت کانال برای کاربر u_n به صورت زیر بیان می‌گردد

$$C_{u_nb}=(1-\alpha)\log_2(1+\gamma_{n,b}) \quad (5)$$

در ارسال لینک بالای NOMA، ایستگاه پایه ابتدا سیگنال u_n را دیکد می‌کند و سپس آن را با استفاده از SIC حذف می‌نماید تا سیگنال u_m را دیکد کند. بنابراین ظرفیت کانال u_m به صورت زیر به دست می‌آید

$$C_{u_mb}=\begin{cases}(1-\alpha)\log_2(1+\gamma_{m,b}) & ,\ C_{u_nb}\geq R_{n,t}\\ 0 & ,\ \text{o.w}\end{cases} \quad (6)$$

بنابراین COP برای کاربران u_n و u_m می‌تواند به صورت (۷) و (۸) بیان شود [۱۱]. به طوری که

$$\tilde{\Sigma}=\Lambda\sum_{p=0}^{m-1}\sum_{q=0}^{n-m-1}(-1)^{p+n-m-q-1}\binom{m-1}{p}\binom{n-m-1}{q} \quad (9)$$

و

$$\Lambda=\frac{M!}{(m-1)!(n-m-1)!(M-n)!} \quad (10)$$

و

$$a=\frac{M-m-q}{\rho_u\lambda_{u_n}b} \quad (11)$$

و

$$b=\frac{p+q+1}{\rho_u\lambda_{u_m}b} \quad (12)$$

و

$$c=\frac{1}{(M-m-q)\rho_u\lambda_{u_m}} \quad (13)$$

در حالی که $\bar{\gamma}_{n,t}=2^{\frac{R_{n,t}}{1-\alpha}}-1$ و $\bar{\gamma}_{m,t}=2^{\frac{R_{m,t}}{1-\alpha}}$ به ترتیب آستانه‌های SNR از پیش تعریف شده برای کاربر n ام و کاربر m ام می‌باشند.

پارامتر مهم دیگر در برآورد عملکرد یک شبکه امن، احتمال قطعی محرمانه (SOP) است. به عبارت دیگر، قطعی محرمانه هنگامی اتفاق می‌افتد که ظرفیت کانال استراق سمع بزرگ‌تر از نرخ هزینه کد استراق سمع[1] باشد. بنابراین SOP برای کاربر k ام به نحوی که $k\in\{n,m\}$ است به صورت (۱۴) بیان می‌گردد [۱۱]

$$\begin{aligned}P_{s,k}&=\Pr(C_{u_ke}>R_{k,t}-R_{k,s})\\&=\frac{\pi^2}{4L\lambda_{u_ke}\rho_u}\sum_{\tau=1}^{L}\sqrt{1-w_\tau^2}\,e^{-\frac{\tan\nu_T+\bar{\gamma}_{k,e}}{\lambda_{u_ke}\rho_u}}\sec^2\nu_T\\&\times\prod_{j\in\Delta}\left(1-2\sqrt{\frac{\tan\nu_T}{\lambda_{br_j}\lambda_{r_je}\bar{\gamma}_{k,e}\rho_t}}K_1\left(2\sqrt{\frac{\tan\nu_T}{\lambda_{br_j}\lambda_{r_je}\bar{\gamma}_{k,e}\rho_t}}\right)\right)\end{aligned} \quad (14)$$

به طوری که $R_{k,s}$ نرخ محرمانگی مقصد[2] برای کاربر k ام است، در حالی که $R_{k,t}-R_{k,s}$ نرخ هزینه در مقابل استراق سمع‌کننده می‌باشد و $\bar{\gamma}_{k,e}=2^{\frac{R_{k,t}-R_{k,s}}{1-\alpha}}-1$ است. C_{u_ke} ظرفیت کانال بین کاربر k ام و استراق سمع‌کننده می‌باشد. لازم به ذکر است که اثبات (۸) و (۱۴) به دلیل

1. Cost Rate of Wiretap Code
2. Target Secrecy Rate

محدودیت مقاله و اثبات آنها در مقالات دیگر، در این مقاله ذکر نشده است [۱۱].

$\mathcal{R}_i$ بیانگر مجموعه غیر تهی iام است، در حالی که $\Delta = |\mathcal{R}_i|$ و Δ نشان‌دهنده تعداد جمرها می‌باشد. $w_T = \cos((2\tau-1)\pi/2L)$ و $\nu_T = \pi(w_T+1)/4$ است. L پارامتر دقت در مقابل پیچیدگی و $K_1(.)$ تابع بسل نوع دوم از مرتبه اول می‌باشد. توجه به این نکته ضروری است که COP و SOP در واقع، پارامترهای قابلیت اطمینان و امنیت هستند، اما این پارامترها جهت محاسبه عملکرد قابلیت اطمینان و امنیت کافی نیستند. به منظور مشخص‌کردن عملکرد سیستم، پارامتر EST در نظر گرفته می‌شود و مطابق با تعریف، EST برای کاربر kام عبارت است از

$$\begin{aligned} T_k &= R_{k,s}\Pr(C_{u_k b} > R_{k,t}, C_{u_k e} < R_{k,t} - R_{k,s}) \\ &= R_{k,s}(1-P_{s,k})(1-P_{c,k}) \end{aligned} \quad (۱۵)$$

۵- بیان مسئله مورد نظر جهت ماکسیمم‌سازی بهبود عملکرد سیستم با انتخاب کاربران و جمر مناسب با قابلیت برداشت انرژی

در این قسمت، هدف بیان مسئله است به طوری که با انتخاب مناسب یک جفت کاربر و جمر مناسب با قابلیت برداشت انرژی در هر کانال فرکانسی، عملکرد سیستم بهینه شود به گونه‌ای که امنیت سیستم بهبود یابد. به عبارت دیگر، جمر مناسب بهینه، SNR سیگنال دریافتی در استراق سمع‌کننده را مینیمم می‌کند. توجه به این نکته ضروری است که CSI[1] استراق سمع‌کننده دانسته فرض می‌گردد [۱۵]. در نتیجه، مسئله مورد نظر عبارت است از

$$\max_{\rho_m,\rho_n,j} T = \sum_{m=1}^{K}\rho_m T_m + \sum_{\substack{n=1\\n\neq m}}^{K}\rho_n T_n \quad (۱۶)$$

$$\text{s.t. } \rho_n P_{s,n} + \rho_m P_{s,m} \le \varepsilon \ , \ \forall m,n \in K \quad (۱-۱۶)$$

$$\rho_n P_{c,n} + \rho_m P_{c,m} \le \zeta \ , \ \forall m,n \in K \quad (۲-۱۶)$$

$$\rho_k \gamma_{u_k e} \le \vartheta \ , \ \forall k \in K \quad (۳-۱۶)$$

$$\begin{matrix}\rho_m \in \{0,1\} \\ \rho_n \in \{0,1\}\end{matrix} \ , \ \forall m,n \in K \quad (۴-۱۶)$$

به عبارت دیگر هدف، انتخاب جفت کاربرانی است که با توجه به جمر انتخابی به ماکسیمم‌کردن عملکرد سیستم و بهبود امنیت آن کمک کنند. ρ_m و ρ_n اندیس انتخاب هستند، بدین معنی که وقتی مقدار آن یک است، کاربر جهت ارسال داده انتخاب می‌شود و در غیر این صورت مقدار آن صفر می‌باشد. توجه به این نکته ضروری است که راه حل بهینه برای این مسئله، روش جستجوی فراگیر[2] می‌باشد که با توجه به پیچیدگی بالای این الگوریتم، به دنبال الگوریتم‌هایی با درجه پیچیدگی کمتر هستیم. بدین منظور برای سادگی حل مسئله (۱۶)، ابتدا پارامترهای ρ_m و ρ_n به صورت پیوسته در بازه $[0,1]$ در نظر گرفته می‌شوند و بعد از حل مسئله، این پارامترها دوباره به فضای گسسته نگاشت می‌شوند. از آنجایی که $\partial T/\partial\rho_m > 0$ و $\partial T/\partial\rho_n > 0$ و نیز قیود مسئله توابعی صعودی از ρ_m و ρ_n می‌باشند، برای حل مسئله می‌توان از روش‌های بهینه‌سازی محدب استفاده کرد [۱۴]. بنابراین تابع لاگرانژ و شرایط KKT برای مشخص‌کردن اولویت حسگرها برای انتخاب کاربران ارسال‌کننده داده در نظر گرفته می‌شود. در نتیجه داریم

$$\begin{aligned} L = &-\sum_{m=1}^{K}\rho_m T_m + \sum_{\substack{n=1\\n\neq m}}^{K}\rho_n T_n + \mu_{m,n}(\rho_n P_{s,n} + \rho_m P_{s,m} - \varepsilon) \\ &+ \upsilon_{m,n}(\rho_n P_{c,n} + \rho_m P_{c,m} - \zeta) + \chi_k(\rho_k \gamma_{u_k e} - \vartheta) \end{aligned} \quad (۱۷)$$

که $\mu_{m,n}$، $\upsilon_{m,n}$ و χ_k ضرایب لاگرانژ نامنفی هستند. این نکته را باید در نظر گرفت که با توجه به شرایط KKT می‌توان نوشت

$$\begin{aligned} &\frac{\partial L}{\partial \rho_m} = -T_m + \mu_{m,n}P_{s,m} + \upsilon_{m,n}P_{c,m} + \chi_m\rho_m\gamma_{u_m e} = 0 \\ &, \ \forall m \in K \end{aligned} \quad (۱۸)$$

مشابه با این روابط برای $\partial L/\partial\rho_n$ هم وجود دارد. در نتیجه، اولویت هر کاربر برای انتخاب جهت ارسال داده در کانال فرکانسی برابر است با

$$cost(m) = -T_m + \mu_{m,n}P_{s,m} + \upsilon_{m,n}P_{c,m} + \chi_m\gamma_{u_m e} \quad (۱۹)$$

به عبارت دیگر هر کاربر با T_m بیشتر و $P_{c,m}$، $P_{s,m}$ و $\gamma_{u_m e}$ کمتر، اولویت بیشتری را برای انتخاب جهت ارسال داده دارد. همچنین طبق شرایط مکمل زاید[3] داریم

$$\begin{aligned} &\mu_{m,n}(\rho_n P_{s,n} + \rho_m P_{s,m} - \varepsilon) = 0 \\ &\rightarrow \mu_{m,n} = 0 \ , \ \rho_n P_{s,n} + \rho_m P_{s,m} < \varepsilon \end{aligned} \quad (۲۰)$$

و

$$\begin{aligned} &\mu_{m,n} \neq 0 \\ &\rho_n P_{s,n} + \rho_m P_{s,m} = \varepsilon \end{aligned} \quad (۲۱)$$

و

$$\begin{aligned} &\upsilon_{m,n}(\rho_n P_{c,n} + \rho_m P_{c,m} - \zeta) = 0 \\ &\rightarrow \upsilon_{m,n} = 0 \ , \ \rho_n P_{c,n} + \rho_m P_{c,m} < \zeta \end{aligned} \quad (۲۲)$$

و

$$\begin{aligned} &\upsilon_{m,n} \neq 0 \\ &\rho_n P_{c,n} + \rho_m P_{c,m} = \zeta \end{aligned} \quad (۲۳)$$

و

$$\chi_k(\rho_k\gamma_{u_k e} - \vartheta) = 0 \rightarrow \chi_k = 0 \ , \ \rho_k\gamma_{u_k e} < \vartheta \quad (۲۴)$$

و

$$\begin{aligned} &\chi_k \neq 0 \\ &\rho_k\gamma_{u_k e} = \vartheta \end{aligned} \quad (۲۵)$$

با توجه به این که تابع هدف T و قیود، توابعی صعودی از ρ_m و ρ_n می‌باشند، بنابراین ρ_m و ρ_n را باید طوری افزایش داد که تابع هدف ماکسیمم گردد، در حالی که قیود (۲۱)، (۲۳) و (۲۵) برآورده شوند. در نتیجه منجر به جواب مطلوب می‌گردد. بنابراین $\mu_{m,n} \neq 0$، $\upsilon_{m,n} \neq 0$ و $\chi_k \neq 0$ شرایط بهینه می‌باشند.

٦- الگوریتم پیشنهادی جهت حل مسئله

در این بخش الگوریتم پیشنهادی برای بهینه‌سازی عملکرد سیستم در

1. Channel State Information
2. Exhaustive Search
3. Complimentary-Slackness

OEHJ & US Algorithm

$\mu_{m,n\min} = 0$

$\mu_{m,n\max} = \mu$ (a large enough number)

$\upsilon_{m,n\max} = \upsilon$ (a large enough number for each sensor)

$\upsilon_{m,n\min} = 0$

$\upsilon_{m,n} = \upsilon_{m,n\max}$

$\chi_{k_{\min}} = 0$

$\chi_{k_{\max}} = \chi$

$\chi_k = \chi_{k_{\max}}$

Iteration $= \alpha_{it}$ (a big number)

$\varepsilon_1 =$ small parameter

$\varepsilon_2 =$ small parameter

Select the jammer which minimizes (4)

While

$((\left|\mu_{(m,n)}^{(k+1)} - \mu_{(m,n)}^{k}\right| > \varepsilon_1 \;\&\&\; \left|\upsilon_{(m,n)}^{(k+1)} - \upsilon_{(m,n)}^{k}\right| > \varepsilon_2 \;\&\&\; \left|\chi_k^{(k+1)} - \chi_k^{k}\right|) > \varepsilon_3)$

Compute $P_{s,m}$ and $P_{c,m}$ for each user

Compute $cost(m) = -T_m + \mu_{m,n}P_{s,m} + \upsilon_{m,n}P_{c,m} + \chi_m\gamma_{u_m e}$ for each user

Compute T for the network

Update the Lagrangian multipliers as follows

$\mu_{m,n}^{(k+1)} = \mu_{m,n}^{k} + \Gamma_1^k(\rho_n P_{s,n} + \rho_m P_{s,m} - \varepsilon)$

$\upsilon_{m,n}^{(k+1)} = \upsilon_{m,n}^{k} + \Gamma_2^k(\rho_n P_{c,n} + \rho_m P_{c,m} - \zeta)$

$\chi_k^{(k+1)} = \chi_k^{k} + \Gamma_3^k(\rho_k \gamma_{u_k e} - \vartheta)$

End

شکل ۲: شبه‌کد الگوریتم پیشنهادی.

حالی که امنیت سیستم بهبود یابد، بیان می‌گردد. برای رسیدن به این منظور، کاربران و جمرهای با قابلیت انرژی مناسب جهت گمراه‌کردن استراق سمع‌کننده انتخاب می‌شوند. توجه به این نکته ضروری است که همه جفت کاربرها می‌توانند کاندیدای انتخاب باشند. در الگوریتم پیشنهادی، در هر تکرار جهت به روز رسانی $\mu_{m,n}$، $\upsilon_{m,n}$ و χ_k تابع هزینه مطابق با (۱۹) برای همه جفت کاربران محاسبه گردیده و کاربران با کمترین تابع هزینه جهت ارسال داده انتخاب می‌شوند. سپس عملکرد سیستم مطابق با (۱۶) برای جفت کاربران انتخاب‌شده به دست می‌آید. $\mu_{m,n}$، $\upsilon_{m,n}$ و χ_k با روش زیرگرادیان[1] به روز رسانی می‌گردند. زمان خاتمه الگوریتم وقتی است که قید همگرایی آن برآورده گردد. الگوریتم پیشنهادی به اختصار الگوریتم OEHJ & US[2] نامیده می‌شود. در واقع به منظور ماکسیمم‌کردن تابع هدف (۱۶)، می‌توان از روش زیرگرادیان استفاده کرد. بدین ترتیب که اگر اندازه گام $\Gamma_i^k, i = 1,2, (\Gamma_i^k > 0)$ از قانون غیر قابل جمع شدن[3] در kامین تکرار تبعیت کند، داریم

$$\lim_{k\to\infty} \Gamma_i^k = 0$$
$$\sum_{k=1}^{\infty} \Gamma_i^k = \infty \qquad (۲۶)$$

در نتیجه، روش زیرگرادیان منجر به جواب بهینه مسئله می‌گردد [۱۶] و [۱۷]. بدین ترتیب با استفاده از روش زیرگرادیان، ضرایب لاگرانژ در $k+1$امین تکرار به صورت زیر به روز رسانی می‌شوند

$$\mu_{m,n}^{k+1} = \mu_{m,n}^{k} + \Gamma_1^k(\rho_n P_{s,n} + \rho_m P_{s,m} - \varepsilon) \qquad (۲۷)$$

1. Subgradient
2. Optimal Energy Harvesting Jammer and User Selection
3. Non-Summable Diminishing Rule

جدول ۱: مقادیر پارامترهای مورد نظر در شبیه‌سازی.

پارامتر	مقدار
λ_{br_j}	۱
$\lambda_{r_j e}$	۱
$\lambda_{u_k e}$	۱
$\lambda_{u_{k,b}}$	۱
L	۲۰
$R_{k,t}$	۱٫۵ BPCU
$R_{k,s}$	۰٫۸ BPCU
α	۰٫۱ – ۰٫۵
η	۰٫۸

$$\upsilon_{m,n}^{k+1} = \upsilon_{m,n}^{k} + \Gamma_2^k(\rho_n P_{c,n} + \rho_m P_{c,m} - \zeta) \qquad (۲۸)$$

و

$$\chi_k^{k+1} = \chi_k^{k} + \Gamma_2^k(\rho_k \gamma_{u_k e} - \vartheta) \qquad (۲۹)$$

اندازه گام $\Gamma_i^k = w_i/\sqrt{k}, i = 1,2,3$ است به طوری که $w_i \gg 1$ می‌باشد. شبه‌کد برای الگوریتم پیشنهادی در شکل ۲ آمده است.

۷- شبیه‌سازی مسئله

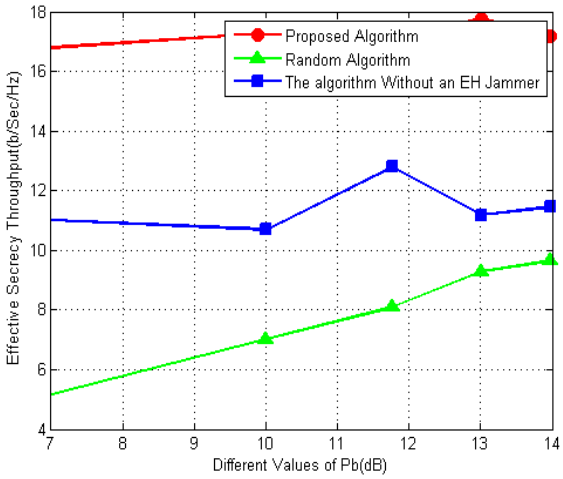
در این قسمت از نرم‌افزار متلب[4] جهت به دست آوردن نتایج شبیه‌سازی استفاده می‌گردد. در شبکه مورد نظر، کاربران و جمرها با توزیع یکنواخت در یک محیط مربعی‌شکل با ابعاد ۵۰۰ m پخش می‌شوند. بدون از دست دادن کلیت مسئله، تعداد کانال‌های فرکانسی ۳، تعداد کاربران ۱۲ و تعداد جمرها و تعداد کاربران استراق سمع‌کننده ۳ در نظر گرفته می‌شوند. ایستگاه پایه در مرکز محیط مربع‌شکل قرار می‌گیرد. مدل کانال در نظر گرفته شده بر اساس تأثیرات، افت مسیر، محوشدگی سریع رایلی و سایه‌انداختن نرمال لگاریتمی در مقیاس وسیع[5] است. مقادیر پارامترهای دیگر نیز در جدول ۱ بیان می‌گردند [۱۱].

نتایج شبیه‌سازی با متوسط‌گیری روی ۵۰۰ تکرار انجام شده است. الگوریتم پیشنهادی با الگوریتم‌های دیگر به عنوان الگوریتم‌های محک[6] در شبیه‌سازی مقایسه می‌گردد:

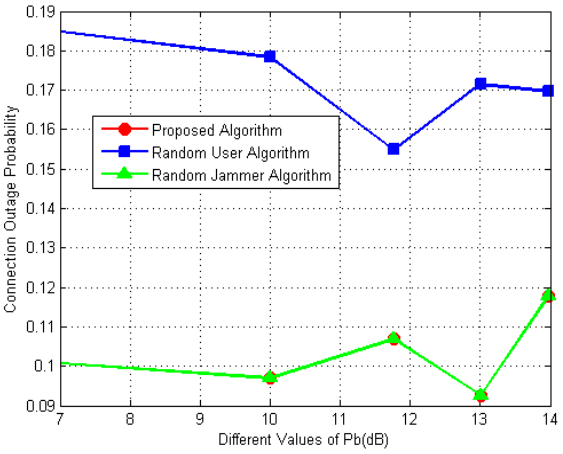
- الگوریتم انتخاب تصادفی جمر: در این الگوریتم جمر در هر باند فرکانسی به صورت تصادفی انتخاب می‌گردد. در واقع، این الگوریتم به منظور نشان‌دادن تأثیر انتخاب مناسب جمر در بهبود عملکرد، قابلیت گذردهی و امنیت شبکه انتخاب شده است.
- الگوریتم انتخاب تصادفی کاربران: در این الگوریتم، کاربران در هر کانال فرکانسی به صورت تصادفی انتخاب می‌شوند. این الگوریتم بیانگر تأثیر انتخاب مناسب کاربران در بهبود قابلیت گذردهی و امنیت شبکه است.

شکل ۳ بیانگر وضعیت قابلیت گذردهی محرمانه مؤثر (EST) به ازای مقادیر مختلف P_b می‌باشد. همان طور که در شکل مشخص می‌شود، الگوریتم پیشنهادی به دلیل انتخاب مناسب جمر و همچنین کاربران مناسب برای هر باند فرکانسی، عملکرد خوبی در مقابل الگوریتم اول محک دارد که در آن جمر به صورت تصادفی برای هر باند انتخاب

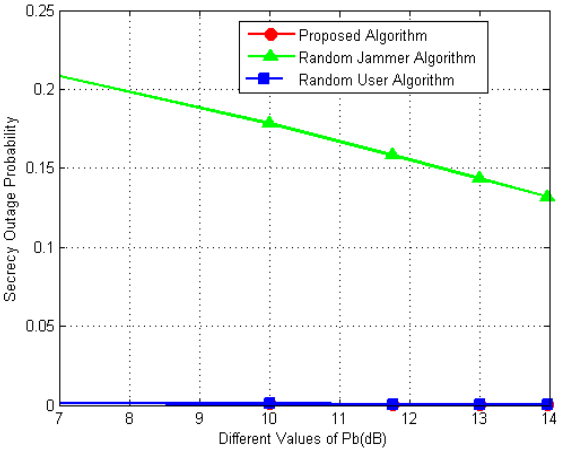
4. MATLAB
5. Raleigh Fast Fading and Large Scale Log-Normal Shadowing
6. Benchmark Algorithm



شکل ۳: قابلیت گذردهی محرمانه مؤثر به ازای مقادیر مختلف P_b.



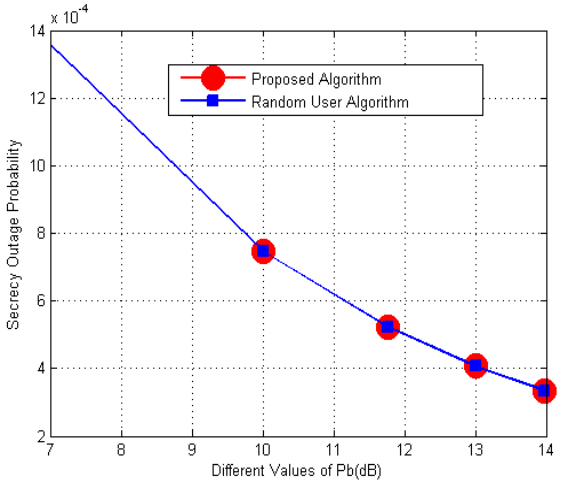
شکل ۴: احتمال قطعی ارتباط به ازای مقادیر مختلف P_b.



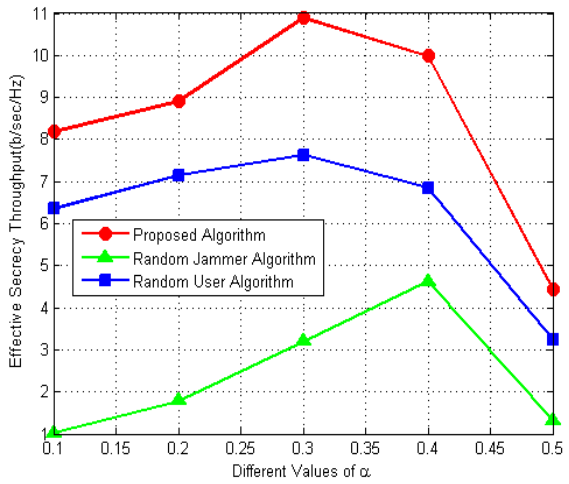
شکل ۵: احتمال قطعی محرمانه به ازای مقادیر مختلف P_b.

می‌گردد و نیز عملکرد بهتری نسبت به الگوریتم دوم محک دارد که در آن کاربران به صورت تصادفی جهت ارسال داده در هر باند فرکانسی انتخاب می‌گردند.

شکل‌های ۴ و ۵ به ترتیب نشان‌دهنده احتمال قطعی ارتباط و احتمال قطعی محرمانه به ازای مقادیر مختلف P_b می‌باشند. همان طور که در شکل مشخص است، الگوریتم پیشنهادی کمترین مقدار را به ترتیب در مقایسه با الگوریتم محک دوم و الگوریتم محک اول دارد. به عبارتی، انتخاب مناسب کاربران ارسال‌کننده داده و نیز جمر مناسب با قابلیت برداشت انرژی، تأثیر بسیار مهمی در بهبود امنیت شبکه دارد و این در



شکل ۶: احتمال قطعی محرمانه به ازای مقادیر مختلف P_b (با وضوح بیشتر نسبت به شکل ۵).



شکل ۷: قابلیت گذردهی محرمانه مؤثر به ازای مقادیر مختلف α.

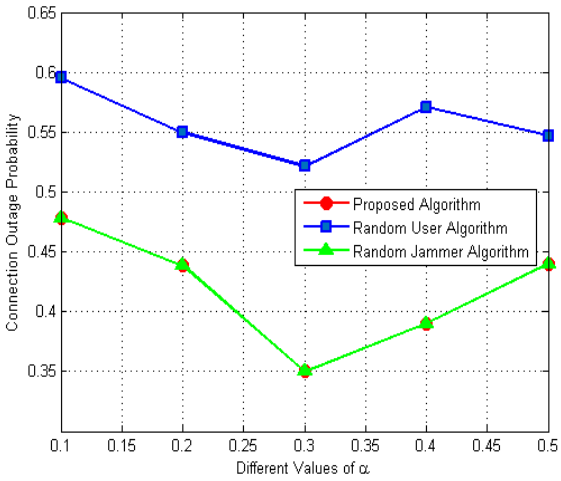
حالی است که الگوریتم دوم، بیشترین مقدار احتمال قطعی ارتباط و الگوریتم اول بیشترین مقدار احتمال قطعی محرمانه را دارد و این بدان معنی است که این الگوریتم‌ها امنیت شبکه را به خوبی تضمین نمی‌کنند.

شکل ۶ همان شکل ۵ با وضوح بیشتر است و کاهش احتمال قطعی محرمانه الگوریتم پیشنهادی را در مقایسه با الگوریتم انتخاب تصادفی کاربران نشان می‌دهد. توجه به این نکته ضروری است که با افزایش مقدار P_b، احتمال قطعی محرمانه کاهش می‌یابد زیرا افزایش P_b منجر به افزایش ρ_t و در نتیجه کاهش احتمال آشکارسازی توسط استراق سمع‌کننده می‌شود.

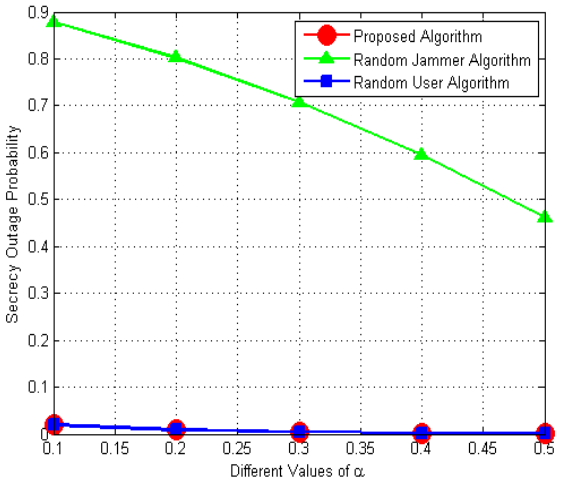
شکل ۷ بیانگر تأثیر فاکتور سوئیچینگ زمانی α روی قابلیت گذردهی محرمانه مؤثر است. با افزایش α، انرژی بیشتری باید به جمر انتخاب‌شده اختصاص یابد تا نویز ساختگی را برای استراق سمع‌کننده ارسال نماید. بنابراین زمان کمتری برای ارسال اطلاعات NOMA لینک بالا استفاده می‌شود و قابلیت گذردهی محرمانه مؤثر کاهش می‌یابد.

شکل‌های ۸ و ۹ بیانگر احتمال قطعی ارتباط و احتمال قطعی محرمانه به ازای مقادیر مختلف فاکتور سوئیچینگ زمانی α می‌باشند. همان طور که در شکل‌های ۷ تا ۹ مشخص است، تقریباً در $\alpha = ۰/۳$ می‌توان به مقدار بهینه برای الگوریتم پیشنهادی رسید. زیرا در این مقدار، قابلیت گذردهی محرمانه مؤثر بیشترین مقدار خود را دارد، در حالی که کمترین مقادیر احتمال‌های قطعی ارتباط و قطعی محرمانه را دارد.

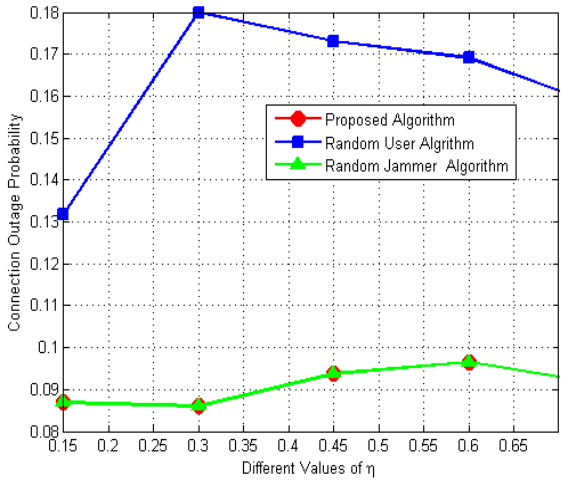
شکل‌های ۱۰ و ۱۱ بیانگر احتمال قطعی ارتباط و احتمال قطعی



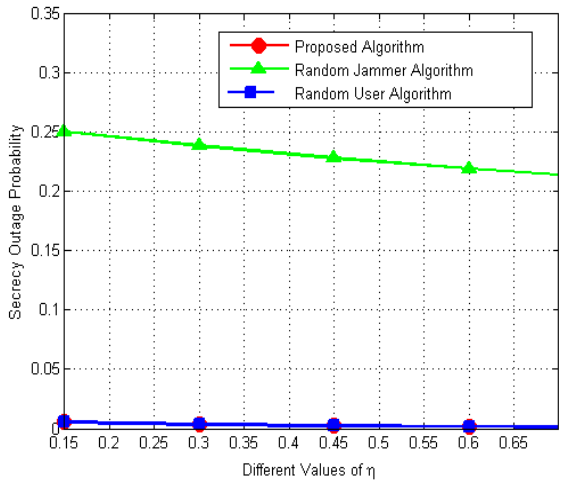
شکل ۸: احتمال قطعی ارتباط به ازای مقادیر مختلف α.



شکل ۹: احتمال قطعی محرمانه به ازای مقادیر مختلف α.



شکل ۱۰: احتمال قطعی ارتباط به ازای مقادیر مختلف η.



شکل ۱۱: احتمال قطعی محرمانه به ازای مقادیر مختلف η.

محرمانه به ازای مقادیر مختلف بازده تبدیل انرژی η هستند. همان طور که در شکل‌ها مشخص می‌گردد، الگوریتم انتخاب تصادفی جمر بیشترین مقدار احتمال قطعی ارتباط و احتمال قطعی محرمانه را دارد، در حالی که الگوریتم پیشنهادی و الگوریتم انتخاب کاربر تصادفی کمترین مقدار این پارامترها را دارند. در واقع با افزایش η، توان ارسالی جمر انتخاب‌شده در الگوریتم پیشنهادی افزایش می‌یابد و در نتیجه، احتمال قطعی محرمانه کاهش می‌یابد.

۸- نتیجه‌گیری

در این مقاله، یک ارسال لینک بالای NOMA با قابلیت انتخاب جمرها و کاربران در هر باند فرکانسی مطرح شد. بدین منظور، الگوریتمی پیشنهاد گردید و دو الگوریتم نیز به عنوان الگوریتم محک جهت برآورد عملکرد شبکه در نظر گرفته شد. در واقع مسئله مورد نظر، بهینه‌سازی قابلیت گذردهی محرمانه با انتخاب کاربرهای مناسب در هر کانال فرکانسی جهت ارسال داده به ایستگاه پایه و جمرهای مناسب جهت ایجاد نویز ساختگی برای کاربر استراق سمع‌کننده با در نظر گرفتن قیودی روی احتمال قطعی و احتمال قطعی ارتباط (COP) به منظور حفظ امنیت شبکه می‌باشد. برای حل مسئله از روش‌های بهینه‌سازی محدب استفاده می‌گردد. بدین ترتیب که با استفاده از روش‌های KKT و تابع هزینه در نظر گرفته شده، کاربران و جمرهای مناسب جهت ارسال داده و ایجاد مزاحمت برای استراق سمع‌کننده در هر باند فرکانسی انتخاب می‌شوند. نتایج شبیه‌سازی بیانگر مؤثربودن الگوریتم پیشنهادی در بهبود عملکرد و حفظ امنیت شبکه در مقایسه با الگوریتم‌های محک می‌باشند.

مراجع

[1] L. Dai, *et al*., "Non-orthogonal multiple access for 5G: solutions, challenges, opportunities, and future research trends," *IEEE Commun. Mag.*, vol. 53, no. 9, pp. 74-81, Sept. 2015.

[2] S. M. R. Islam, N. Avazov, O. A. Dobre, and K. S. Kwak, "Power domain non-orthogonal multiple access (NOMA) in 5G systems: potentials and challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 721-742, 2nd Quart., 2017.

[3] 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.

[4] C. Zhong and Z. Zhang, "Non-orthogonal multiple access with cooperative full-duplex relaying," *IEEE Commun. Lett.*, vol. 20, no. 12, pp. 2478-2481, Dec. 2016.

[5] B. He, A. Liu, N. Yang, and V. K. N. Lau, "On the design of secure non-orthogonal multiple access systems," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 10, pp. 2196-2206, Oct. 2017.

[6] F. Zhou, Z. Chu, H. Sun, R. Q. Hu, and L. Hanzo, "Artificial noise aided secure cognitive beamforming for cooperative MISO-NOMA using SWIPT," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 930-931, Apr. 2018.

[7] Y. Feng, S. Yan, Z. Yang, N. Yang, and J. Yuan, "Beamforming design and power allocation for secure transmission with NOMA," *IEEE Trans. Wireless Commun.*, vol. 18, no. 5, pp. 2639-2651, May 2019.

[8] F. Jameel, S. Wyne, G. Kaddoum, and T. Duong, "A comprehensive survey on cooperative relaying and jamming strategies for physical

layer security," *IEEE Commun. Surv. Tuts.*, vol. 21, no. 3, pp. 2734-2771, Jul. 2019.
[9] M. Liu and Y. Liu, "Power allocation for secure SWIPT systems with wireless-powered cooperative jamming," *IEEE Commun. Lett.*, vol. 21, no. 6, pp. 1353-1356, Jun. 2017.
[10] Y. Bi and A. Jamalipour, "Accumulate then transmit: towards secure wireless powered communication networks," *IEEE Trans. Vehicular Technology*, vol. 67, no. 7, pp. 6301-6310, Jul. 2018.
[11] K. Cao, *et al*., "Improving physical layer security of uplink NOMA via energy harvesting jammer," *IEEE Trans. on Information Forensics and Security*, vol. 16, pp. 786-799, 2020.
[12] B. Rashid, A. Ahmad, S. Saleem, and A. Khan, "Joint energy efficient power and sub-channel allocation for uplink MC-NOMA networks," *International J. of Communication Systems*, vol. 33, no. 17, Article ID: e4606, 25 Nov. 2020.
[13] K. Cao, *et al*., "On the security enhancement of uplink NOMA systems with jammer selection," *IEEE Trans. on Communications*, vol. 68, no. 9, pp. 5747 - 5763, Sept. 2020.
[14] Y. Zou, "Physical-layer security for spectrum sharing systems," *IEEE Trans. Wireless Commun.*, vol. 16, no. 2, pp. 1319-1329, Feb. 2017.
[15] K. Cao, B. Wang, H. Ding, T. Li, and F. Gong, "Optimal relay selection for secure NOMA systems under untrusted users," *IEEE Trans. Veh. Technol.*, vol. 69, no. 2, pp. 1942-1955, Feb. 2020.
[16] W. Yu and R. Lui, "Dual methods for nonconvex spectrum optimization of multicarrier systems," *IEEE Trans. on Commun*, vol. 54, no. 7, pp. 1310-1322, Jul. 2006.
[17] D. P. Bertsekas, A. Nedic, and A. E. Ozdaglar, *Convex Analysis and Optimization*. Belmont, MA: Athena Scientific, 2003.

مریم نجیمی در سال ۱۳۸۳ مدرک کارشناسی مهندسی برق گرایش الکترونیک خود را از دانشگاه دانشگاه سیستان و بلوچستان در سال ۱۳۸۷ مدرک کارشناسی ارشد مهندسی برق گرایش مخابرات سیستم خود را از دانشگاه صنعتی خواجه نصیرالدین طوسی و در سال ۱۳۹۳ مدرک دکتری مهندسی برق گرایش مخابرات خود را از دانشگاه صنعتی نوشیروانی دریافت نمود. دکتر نجیمی از سال ۱۳۹۳ در دانشکده مهندسی برق و کامپیوتر دانشگاه علم و فناوری مازندران در بهشهر مشغول به فعالیت گردید و اینک نیز عضو هیأت علمی این دانشکده می‌باشد. زمینه‌های علمی مورد علاقه نام‌برده متنوع بوده و شامل موضوعاتی مانند شبکه‌های حسگر بی‌سیم هوشمند، شبکه‌های NOMA، محاسبات نرم و روش‌های بهینه‌سازی در شبکه‌ها می‌باشد.