بهینه‌سازی گذردهی در شبکه پخش با حفظ محرمانگی اطلاعات اختصاصی هر گیرنده با استفاده از کدینگ، مدولاسیون و توان ارسالی وفقی

مهرداد تاکی

چکیده: در این مقاله روشی برای ارسال بهینه اطلاعات در شبکه پخش ارائه می‌شود که در آن ضمن حداکثرکردن بهره‌برداری از منابع شبکه، امنیت لایه فیزیکی برای اطلاعات هر کاربر تأمین می شود، یعنی سناریوی ارسال به گونه‌ای تدوین شده که اطلاعات ارسالی هر کاربر صرفاً در گیرنده متناظرش با احتمال خطای مناسب قابل آشکارسازی است و احتمال خطای آشکارسازی اطلاعات در گیرنده‌های غیر خودی تا حد قابل قبولی زیاد می‌باشد. در روش پیشنهادی از تنظیم نرخ گسسته با استفاده از کدبندی و مدوله‌سازی وفقی استفاده می‌شود و نرخ ارسال بر مبنای سیگنال به نویز لینک‌های مختلف تعیین می‌گردد. حل‌های دقیق و تقریبی برای حل مسأله بهینه‌سازی ارائه شده که حل تقریبی ضمن داشتن اختلاف اندک با حل دقیق، پیچیدگی قابل قبولی دارد. بررسی‌های عددی حاکی از آن است که اضافه‌شدن قید امنیت موجب کاهش جزئی نرخ‌های قابل دسترسی در شبکه در عوض حفظ محرمانگی اطلاعات خواهد شد.

کلید واژه: **امنیت لایه فیزیکی، شبکه پخش، کدینگ و مدولاسیون وفقی.**

۱- مقدمه

در شبکه‌های مخابراتی بی‌سیم به علت مشترک‌بودن محیط ارسال، حفظ محرمانگی اطلاعات یک چالش اساسی است. ایجاد امنیت در دو سطح قابل پیاده‌سازی است. در سطح لایه فیزیکی شبکه، سمبل‌های ارسالی باید به گونه‌ای باشند که ابهام آشکارسازی آنها در گیرنده غیر خودی تا حد قابل قبولی زیاد باشد [۱]. در سطح لایه کاربردی، سمبل‌های ارسالی می‌توانند به گونه‌ای رمزنگاری شده باشند که حتی در صورت آشکارسازی با ابهام قابل قبول در گیرنده به سختی قابل بازنگاشت به اطلاعات اصلی باشند. در این مقاله هدف ایجاد امنیت لایه فیزیکی در یک شبکه پخش با وجود کانال‌های متغیر با زمان و با استفاده از کدینگ و مدولاسیون وفقی می‌باشد.

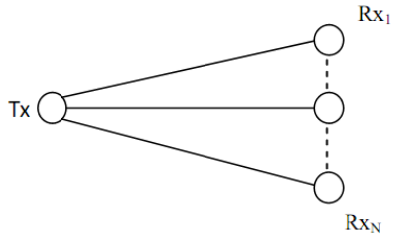
بحث ایجاد امنیت لایه فیزیکی از دیدگاه تئوری اطلاعات ابتدا توسط شانون مطرح شد [۱] و سپس در [۲] توسط وینر تعمیم داده شد و در [۳] و [۴] در شبکه‌های پیچیده‌تر به کار گرفته شده است. در این مقالات گین کانال‌ها ثابت است و گین کانال تا گیرنده غیر خودی نسبت به گین کانال تا گیرنده اصلی کمتر است. در مقالات یادشده از کدهای ظرفیت با احتمال خطای متمایل به صفر استفاده می‌شود و توزیع کلمات کد ارسالی به گونه‌ای بهینه‌سازی می‌شود که اطلاعات متقابل بین سمبل‌های ارسالی و سمبل‌های دریافتی در گیرنده خودی حداکثر شود و در عین حال اطلاعات متقابل بین سمبل‌های ارسالی و سمبل‌های دریافتی در گیرنده غیر خودی صفر (امنیت کامل) و یا تا حد قابل قبولی کم باشد (امنیت نسبی). نرخ‌های قابل دسترسی در شبکه‌ها با وجود کانال‌های متغیر با زمان و قید امنیت نسبی در [۵] و [۶] مورد بررسی قرار گرفته است. در این مقالات فرض شده که نرخ ارسال به طور پیوسته قابل تنظیم است و از کدهای ظرفیت با احتمال خطای میل‌کننده به صفر استفاده می‌شود.

تنظیم نرخ پیوسته و استفاده از کدهای ظرفیت هر چند دید خوبی می‌دهد، اما در عمل ممکن نیست. در سیستم‌های عملی حد کمی از احتمال خطا پذیرفته است و نرخ ارسال از یک مجموعه محدود از نرخ‌های گسسته انتخاب می‌شود [۷]. یک ایده مناسب برای اعمال امنیت نسبی در لایه فیزیکی در سیستم‌های عملی آنست که ارسال به گونه‌ای صورت پذیرد که احتمال خطای سمبل‌های دریافتی در گیرنده غیر خودی از یک حدی بیشتر باشد. کدهای مناسب برای این سیستم‌ها، آنهایی هستند که در منحنی عملکردشان یک تغییر اندک در سیگنال به نویز (SNR) کلمات دریافتی به تغییر قابل توجهی در احتمال خطای آشکارسازی منجر شود. همچنین در سیستم‌های عملی تنظیم نرخ پیوسته امکان‌پذیر نیست و نرخ ارسال از مجموعه‌ای از نرخ‌های گسسته انتخاب می‌شود که هر نرخ به کمک یک کدینگ و یک مدولاسیون خاص پیاده شده است (کدینگ و مدولاسیون وفقی [۷]). در سیستم‌های مخابراتی به طور گسترده از کدینگ و مدولاسیون وفقی به منظور حداکثرکردن گذردهی لینک‌ها (بدون در نظر گرفتن قید امنیت) استفاده شده است [۸] تا [۱۰]. در [۱۱] استفاده از کدینگ و مدولاسیون وفقی برای ایجاد امنیت در یک سیستم شامل یک فرستنده، یک گیرنده اصلی و یک گیرنده غیر خودی پیشنهاد شده که در آن متوسط اطلاعات ارسالی حداکثر می‌شود با این شرط که احتمال خطای آشکارسازی اطلاعات در گیرنده اصلی از حد مشخصی کمتر باشد ولی اطلاعات در گیرنده غیر خودی با احتمال خطای زیاد دریافت شوند.

در این مقاله یک شبکه پخش شامل یک فرستنده و چندین گیرنده با اهمیت و نیازمندی‌های مختلف در نظر گرفته شده است. فرض می‌شود که کانال‌های متناظر با گیرنده‌های مختلف متعامد هستند و متوسط توان ارسالی فرستنده محدود است. روشی جدید برای ارسال بر مبنای SNR کانال‌ها در این شبکه طراحی شده که با استفاده از آن مجموع وزن‌دار از متوسط نرخ لینک‌ها حداکثر شده و در عین حال قید امنیت مورد ملاحظه قرار می‌گیرد. در طرح پیشنهادی هر بخش از اطلاعات صرفاً در گیرنده متناظرش با احتمال خطای مناسب قابل آشکارسازی است و احتمال خطای آشکارسازی در سایر گیرندگان تا حد بالایی زیاد می‌باشد. اطلاعات نویسنده حاکی از آنست که این مقاله اولین کار در حوزه ایجاد امنیت لایه فیزیکی در شبکه پخش با استفاده از کدینگ و مدولاسیون وفقی می‌باشد.

این مقاله در تاریخ ۱۳ تیر ماه ۱۳۹۱ دریافت و در تاریخ ۲۷ مهر ماه ۱۳۹۲ بازنگری شد.

مهرداد تاکی، گروه مهندسی برق، دانشکده فنی مهندسی، دانشگاه اصفهان، اصفهان، (email: m.taki@eng.ui.ac.ir).



شکل ۱: ساختار شبکه بی‌سیم.

روش ارائه‌شده می‌تواند در بسیاری از لینک‌های فروسو در شبکه‌های ارتباطی بی‌سیم که در آنها امکان استفاده از بلوک‌های پیچیده رمزنگاری وجود ندارد، به کار گرفته شود تا ضمن تضمین قیود امنیت، حداکثر بازدهی طیفی را برای کاربران فراهم آورد. آن گونه که ارزیابی‌های عددی در بخش پنجم نشان می‌دهد در اثر اعمال قید امنیت نرخ‌های قابل دسترسی افت اندکی خواهند کرد ولی در عوض مسأله امنیت و حفظ محرمانگی در شبکه‌های پخش به خوبی مورد ملاحظه قرار خواهد گرفت. دو روش دقیق و تقریبی برای حل مسأله ارائه شده که روش تقریبی ضمن داشتن عملکردی بسیار نزدیک به روش دقیق، پیچیدگی اندکی دارد.

در ادامه در بخش دوم به بیان اصول و مفاهیم مورد نیاز از جمله ساختار شبکه، ویژگی لینک‌ها و نحوه کدینگ و مدولاسیون وفقی می‌پردازیم. بخش سوم، فرمول‌بندی مسأله و حل آن را بیان می‌دارد و در مورد بهینه‌بودن حل و پیچیدگی آن بحث خواهد کرد. در بخش چهارم به منظور ایجاد یک مبنای مقایسه برای بررسی تأثیر اعمال قید امنیت بر نرخ‌های قابل دسترسی، روش بهینه‌سازی شده ارسال در شبکه پخش بدون در نظر گرفتن قیود امنیت مورد بررسی قرار خواهد گرفت. بخش پنجم به بیان ارزیابی‌های عددی می‌پردازد و در بخش ششم نتیجه‌گیری ارائه می‌شود.

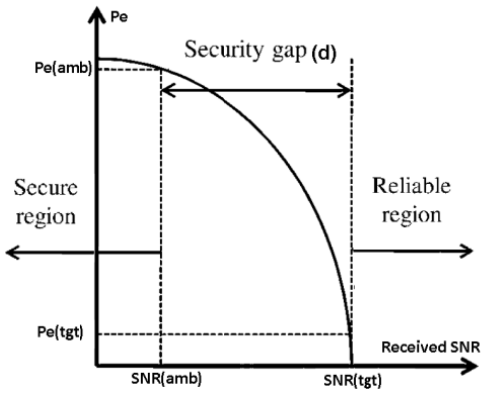
۲- اصول و مفاهیم اساسی

۲-۱ علایم و نشانه‌گذاری‌ها

در این مقاله متغیرها با حروف ایتالیک مثل z، ثابت‌ها با حروف بزرگ مثل N و تابع چگالی احتمال متغیر تصادفی x با $f_x(x)$ آمده است.

۲-۲ توصیف سیستم و مدل کانال‌ها

شکل ۱ شبکه بی‌سیم در نظر گرفته شده را نمایش می‌دهد و در حالت کلی N لینک بی‌سیم وجود دارد که از ۱ تا N شماره‌گذاری شده‌اند که هر لینک مسیر ارتباطی بین فرستنده Tx و گیرنده $1 \le i \le N, \mathrm{Rx}_i$ بوده و دارای کانال متغیر با زمان و دارای فیدینگ فرکانسی تخت هستند. مدل فیدینگ بلوکی در نظر گرفته شده که در آن بهره کانال در طول یک بلوک (چندین کلمه کد) ثابت می‌ماند و به طور مستقل از یک بلوک به بلوک دیگر تغییر می‌کند [۱۲] و لینک‌ها دارای باندهای فرکانسی متعامد با عرض باندهای یکسان هستند. فرض شده که عرض باند کلی سیستم به N بخش مساوی تقسیم می‌گردد و اطلاعات مربوط به گیرنده iام $(1 \le i \le N)$ در باند iام ارسال می‌شود. اگر h_i^j $(1 \le i, j \le N)$ گین کانال در باند iام تا گیرنده jام باشد، نسبت سیگنال به نویز دریافتی در باند فرکانسی iام و در گیرنده jام برابر $\gamma_i^j = p_i \left|h_i^j\right|^2 / \sigma_j^2$ خواهد بود که در آن σ_j^2 واریانس نویز گاوسی در گیرنده jام و p_i توان ارسالی در باند فرکانسی iام می‌باشد. در این مقاله $s_i^j = \left|h_i^j\right|^2 / \sigma_j^2$ سیگنال به نویز (SNR) نرمالیزه و یا به اختصار SNR در باند فرکانسی iام و در گیرنده jام نامیده می‌شوند.



شکل ۲: فاصله امنیتی برای تضمین امنیت لایه فیزیکی [۱۳].

۲-۳ نرخ ارسال و مدهای کدبندی و مدوله‌سازی وفقی

در سیستم‌های عملی $M+1$ حالت ارسال با استفاده از کدبندی و مدوله‌سازی وفقی وجود دارد که هر یک متناظر با یک روش کدبندی و مدوله‌سازی می‌باشند که در نهایت به نرخ ارسال R_m منجر می‌شود [۷]. حالت‌های ارسال بسته به نرخشان به صورت $0 = R_0 < R_1 < \ldots < R_M$ مرتب می‌شوند که حالت صفر بیانگر حالتی است که در آن هیچ اطلاعاتی ارسال نمی‌شود. برای هدفی که ما در این مقاله دنبال می‌کنیم، کدهای مناسب برای این سیستم‌ها آنهایی هستند که در منحنی عملکردشان یک تغییر اندک در SNR کلمات دریافتی به تغییر قابل توجهی در احتمال خطای آشکارسازی منجر شود و به عبارت دقیق‌تر فاصله امنیتی[1] در این کدها کم باشد [۱۳]. در شکل ۲ مفهوم فاصله امنیتی مشخص شده که در اثر کاهش SNR دریافتی به اندازه فاصله امنیتی d، احتمال خطا از سطح قابل قبول $\mathrm{Pe}_{(tgt)}$ به سطح نامناسب $\mathrm{Pe}_{(amb)}$ می‌رسد. برای داشتن کدهایی با فاصله امنیتی کم بایستی به سراغ کدهای LDPC رفت. با این روش اگر γ بیانگر نسبت سیگنال به نویز دریافتی در گیرنده باشد، در حالت ارسال mام احتمال خطا را شبیه آنچه در [۱۱] پیشنهاد شده است، می‌توان با تابع زیر تخمین زد

$$\mathrm{p_e}(\gamma, \mathrm{R}_m) = \begin{cases} 0.5\exp(-\mathrm{A}_{1,m}\gamma^{\mathrm{A}_{2,m}}) & , \ 0 \le \gamma \le \Gamma_m \\ \dfrac{\mathrm{A}_{3,m}}{(1+\exp(\mathrm{A}_{4,m}(\gamma - \mathrm{A}_{5,m})))^{\mathrm{A}_{6,m}}} & , \ \Gamma_m \le \gamma \end{cases} \quad (1)$$

به طوری که $\{\mathrm{A}_{1,m}, \mathrm{A}_{2,m}, \mathrm{A}_{3,m}, \mathrm{A}_{4,m}, \mathrm{A}_{5,m}, \mathrm{A}_{6,m}, \Gamma_m\}$ ثابت‌هایی تابع حالت ارسال می‌باشند و برای مدهای ارسال مورد استفاده در این مقاله در جدول ۱ آمده‌اند. در حالت ارسال mام حداقل SNR مورد نیاز برای تضمین حداکثر احتمال خطای لحظه‌ای B_0 با $\mathrm{g}_{\mathrm{B}_0}(\mathrm{R}_m)$ نمایش داده می‌شود که از روابط زیر به دست می‌آید

$$\mathrm{p_e}(\gamma, \mathrm{R}_m) \le \mathrm{B}_0 \Rightarrow \gamma \ge \mathrm{g}_{\mathrm{B}_0}(\mathrm{R}_m)$$

$$\mathrm{g}_{\mathrm{B}_0}(\mathrm{R}_m) = \begin{cases} \left(\dfrac{-1}{\mathrm{A}_{1,m}} \times \ln\dfrac{\mathrm{B}_0}{0.5}\right)^{\frac{1}{\mathrm{A}_{2,m}}} & , \ \mathrm{B}_0 \le \mathrm{p_e}(\Gamma_m, \mathrm{R}_m) \\ \dfrac{1}{\mathrm{A}_{4,m}} \times \ln\left(\left(\dfrac{\mathrm{A}_{3,m}}{\mathrm{B}_0}\right)^{\frac{1}{\mathrm{A}_{5,m}}} - 1\right) + \mathrm{A}_{6,m} & \\ \quad , \ \mathrm{B}_0 > \mathrm{p_e}(\Gamma_m, \mathrm{R}_m) & \end{cases} \quad (2)$$

1. Security Gap

۳- بهینه‌سازی بازدهی طیفی در شبکه پخش با در نظر گرفتن قید امنیت

شبکه پخش نشان داده شده در شکل ۱ یک الگوی ارسال اطلاعات متداول در انواع سیستم‌های مخابراتی می‌باشد که از آن جمله می‌توان به لینک فروسو در شبکه‌های مخابرات سلولی اشاره کرد. در چنین حالتی بهره‌برداری حداکثری از منابع شبکه با توجه به نیازمندی‌ها و اهمیت کاربران مختلف و در عین حال حفظ محرمانگی اطلاعات هر کاربر از اهمیت بالایی برخوردار است.

در ادامه مسأله مورد نظر را فرمول‌بندی کرده و سپس حل آن را ارائه می‌دهیم و در مورد بهینه‌بودن حل به لحاظ ریاضی صحبت خواهیم کرد، در نهایت پیچیدگی حل ارائه‌شده را مورد توجه قرار خواهیم داد.

۳-۱ فرمول‌بندی مسأله

در یک شبکه پخش شامل N لینک مختلف، هدف حداکثرکردن یک مجمع وزن‌دار از بازدهی طیفی (متوسط نرخ ارسال در واحد زمان و در واحد عرض باند) لینک‌ها است به طوری که وزن نسبت داده شده به لینک iام یا همان ω_i $(1 \le i \le N)$ بر اساس نیازمندی و اهمیت آن تعیین می‌شود. در شبکه مورد نظر متوسط توان ارسالی فرستنده محدود و حداکثر برابر P_{max} می‌باشد. برای آن که کاربر iام اطلاعات متناظر خود را آشکارسازی کند بایستی احتمال خطای بیت در آن حداکثر B_i^t باشد و برای این که اطلاعات در سایر گیرنده‌های غیر خودی قابل آشکارسازی نباشد بایستی احتمال خطای بیت در آنها حداقل برابر B_i^s باشد. اگر k_i نرخ لحظه‌ای ارسال در باند iام (نرخ ارسال اطلاعات اختصاصی کاربر iام) باشد مسأله به صورت ذیل فرمول‌بندی خواهد شد

$$\max_{k(i),p(i),1\le i\le N} \sum_{i=1}^{N} \omega_i E\{k(i)\} \quad \text{subject to :}$$

$$\begin{aligned}
&C(1): \sum_{i=1}^{N} E\{p(i)\} \le P_{max} \quad , \quad 1 \le i \le N \\
&C(2),\ldots,C(N+1): BER_i^i \le B_i^t \quad , \quad 1 \le i \le N \\
&C(N+2),\ldots,C(2N): BER_1^j \ge B_1^s \quad , \quad 2 \le j \le N \\
&\vdots \\
&C(i(N-1)+3),\ldots,C(i(N-1)+N+1): BER_i^j \ge B_i^s \\
&\quad , \quad 1 \le j \ne i \le N \\
&\vdots \\
&C(N^2-N+3),\ldots,C(N^2+1)): BER_N^j \ge B_N^s \\
&\quad , \quad 1 \le j \le N-1
\end{aligned} \tag{۳}$$

که BER_i^j احتمال خطای بیت در آشکارسازی اطلاعات باند iام در گیرنده jام است. در مسأله فوق قید $C1$ مربوط به متوسط توان ارسالی فرستنده، قیود $C2$ تا $C(N+1)$ مربوط به تضمین احتمال خطای مناسب برای آشکارسازی اطلاعات اختصاصی هر گیرنده و قیود $C(N+2)$ تا $C(N^2+1)$ تضمین‌کننده زیادبودن احتمال خطای آشکارسازی برای گیرنده‌های غیر خودی و به عبارتی حفظ محرمانگی اطلاعات است.

با ملاحظه (۳) می‌توان دریافت که مسأله تدوین‌شده، پیچیده است و به طور مستقیم قابل حل نمی‌باشد، لذا در ادامه ابتدا آن را به فرم ساده‌تر بازنویسی می‌کنیم و سپس آن را حل خواهیم کرد.

۳-۲ بازنویسی مسأله

برای بازنویسی مسأله ابتدا با در نظر گرفتن قیود احتمال خطا، توان ارسال لحظه‌ای مناسب تعیین می‌شود و شرط لازم برای ارسال محرمانه مشخص می‌گردد. سپس استراتژی مناسب برای تخصیص نرخ ارسال در لینک‌ها تعیین خواهد شد و در نهایت مسأله به فرم ساده‌تر بازنویسی می‌گردد.

جدول ۱: مدهای AMC مورد استفاده و ثابت‌های مربوط به تخمین احتمال خطای آنها.

شماره مد	۵	۴	۳	۲	۱
مدولاسیون	۱۶-QAM	۱۶-QAM	۴-QAM	۴-QAM	۴-QAM
نرخ کد	$\frac{5}{6}$	$\frac{1}{2}$	$\frac{5}{6}$	$\frac{2}{3}$	$\frac{1}{2}$
نرخ مد	$\frac{20}{6}$	۲	$\frac{10}{6}$	$\frac{4}{3}$	۱
$A_{1,m}$	۰/۵۳۷۶۵	۰/۴۷۱۲	۱/۱۵۸۹	۱/۱۲۴۱	۱/۰۷۴۰
$A_{2,m}$	۰/۶۰۰۸۱	۰/۵۸۹۸	۰/۶۴۳۵۸	۰/۶۱۸۶۸	۰/۵۹۲۲
$A_{3,m}$	۰/۰۷۰۸۵۹	۰/۱۴۶	۰/۰۵	۰/۰۹۳	۰/۱۴
$A_{4,m}$	۲/۸۵۴۹	۲۴/۶۲۷۱	۱۲/۷۰۴	۱۶/۲	۶۰/۱۵۸
$A_{5,m}$	۱۵/۳۸	۴/۷۴۷	۳/۶	۲/۱۱۵	۱/۳۸
$A_{6,m}$	۲۳۸	۲/۲۷۱۴	۳۶۷	۳۰/۷۷	۱۴۶
Γ_m	۸/۲	۵/۷	۴/۱	۲	-۰/۵

۳-۲-۱ در نظر گرفتن قیود احتمال خطا در تعیین توان ارسالی و شرط ارسال

همان طور که گفته شد با توجه به (۳) دو دسته قیود احتمال خطا داریم که دسته اول قیود $C(i+1)$ $(1 \le i \le N)$ که تضمین‌کننده آشکارسازی مناسب اطلاعات اختصاصی هر گیرنده هستند. با در نظر گرفتن این قیود در مورد توان ارسال لحظه‌ای می‌توان به شرط زیر رسید

$$\begin{aligned}
&C(i+1): BER_i^i \le B_i^t \overset{(2)}{\Leftrightarrow} \gamma_i^j = p_i s_i^i \ge g_{B_i^t}(k_i) \\
&\overset{(2)}{\Leftrightarrow} p_i \ge \frac{g_{B_i^t}(k_i)}{s_i^i} \quad , \quad 1 \le i \le N
\end{aligned} \tag{۴}$$

دسته دوم قیود $C(N+2)$ تا $C(N^2+1)$ که تضمین‌کننده محرمانه‌ماندن اطلاعات اختصاصی هر گیرنده در سایر گیرنده‌ها است. با در نظر گرفتن این قیود در مورد توان ارسالی لحظه‌ای می‌توان به شرط زیر رسید

$$\begin{aligned}
&C(i(N-1)+3),\ldots,C(i(N-1)+N+1): \\
&BER_i^j \ge B_i^s \overset{(2)}{\Leftrightarrow} p_i s_i^j \le g_{B_i^s}(k_i) \\
&\Leftrightarrow p_i \le \frac{g_{B_i^s}(k_i)}{s_i^j} \quad , \quad 1 \le j \le N, i \ne j
\end{aligned} \tag{۵}$$

از ترکیب دو شرط (۴) و (۵) داریم

$$\frac{g_{B_i^t}(k_i)}{s_i^i} \le p_i \le \frac{g_{B_i^s}(k_i)}{s_i^i} \quad , \quad 1 \le j \le N, i \ne j \tag{۶}$$

از آنجا که بر روی توان ارسالی محدودیت وجود دارد، حداقل توان ممکن را تخصیص می‌دهیم یعنی $p_i = g_{B_i^t}(k_i) / s_i^i$. اما زمانی توان ارسالی فوق قابل تخصیص است و به عبارت دیگر امکان ارسال اطلاعات اختصاصی لینک iام وجود دارد که داشته باشیم

$$\begin{aligned}
&\frac{g_{B_i^t}(k_i)}{s_i^i} \le \frac{g_{B_i^s}(k_i)}{s_i^j} \Leftrightarrow \frac{s_i^j}{s_i^i} \le \frac{g_{B_i^s}(k_i)}{g_{B_i^t}(k_i)} = G_i(k_i) \\
&, 1 \le \forall j \ne i \le N \Leftrightarrow \Sigma_i = \max_{1 \le j \le N, i \ne j} (s_i^j) \le G_i(k_i) s_i^i
\end{aligned} \tag{۷}$$

می‌توان گفت که برای حفظ محرمانگی اطلاعات باند iام، لازم است حداکثر SNR در سایر گیرنده‌ها در باند iام (Σ_i) از $G_i(k_i)s_i^i$ بیشتر نباشد.

۳-۲-۲ تخصیص نرخ ارسالی

برای تخصیص نرخ از رویکردی مشابه آنچه در [۷] در مورد یک لینک مجزا صورت پذیرفته استفاده می‌کنیم. برای SNR لینک iام در باند iام، $N+1$ آستانه به صورت $\tau_{0,i} \le \tau_{1,i} \cdots \tau_{N,i} \le \tau_{(N+1),i} = \infty$ در نظر می‌گیریم و با توجه به شرط (۵) برای حفظ محرمانگی اطلاعات باند iام تخصیص نرخ را به صورت زیر در نظر می‌گیریم

$$k_i = \begin{cases} R_m, \tau_{m,i} \le s_i^i < \tau_{m+1,i} \text{ and } \dfrac{\Sigma_i}{G_i(R_m)} \le s_i^i \\ 0 \quad , \quad \text{otherwise} \end{cases} \qquad (۸)$$

۳-۲-۳ تخصیص نرخ ارسالی

با توجه به استراتژی تخصیص نرخ در نظر گرفته شده متوسط توان ارسالی و متوسط نرخ ارسال در هر باند به صورت زیر به دست می‌آیند

$$E\{k_i\} = \omega_i \sum_{m=1}^{M} R_m \int_{\tau_{m,i}}^{\tau_{m+1,i}} \int_{0}^{G_i(R_m)s_i^i} f_{\Sigma_i}(\Sigma_i) f_{s_i^i}(s_i^i) d\Sigma_i ds_i^i$$

$$E\{p_i\} = \sum_{i=1}^{N} \sum_{m=1}^{M} g_{B_i^t}(R_m) \times \qquad (۹)$$

$$\int_{\tau_{m,i}}^{\tau_{m+1,i}} \int_{0}^{G_i(R_m)s_i^i} \frac{1}{s_i^i} f_{\Sigma_i}(\Sigma_i) f_{s_i^i}(s_i^i) d\Sigma_i ds_i^i$$

با توجه به متوسط نرخ و توان محاسبه‌شده مسأله (۳) به صورت زیر بازنویسی می‌شود

$$\max_{\tau_{m,i}, 1 \le i \le N, 1 \le m \le M} \sum_{i=1}^{N} \omega_i E\{k(i)\} \text{ subject to:}$$
$$C(1): \sum_{i=1}^{N} E\{p(i)\} \le P_{max} \quad , \quad 1 \le i \le N \qquad (۱۰)$$

قیود احتمال خطای $C(2)$ تا $C(N^2+1)$ در (۳) اکنون در تنظیم توان ارسالی (رابطه (۶)) و تخصیص نرخ (رابطه (۸)) در نظر گرفته شده‌اند.

۳-۲-۴ حل دقیق مسأله

رابطه (۱۰) یک مسأله بهینه‌سازی مقید است که به کمک روش ضرایب لاگرانژ قابل حل می‌باشد که در مورد روش ضرایب لاگرانژ چهار نکته وجود دارد:

نکته ۱: اگر لاگرانژین یک تابع، پیوسته مشتق‌پذیر باشد و قیود مسأله بهینه‌سازی به طور خطی از هم مستقل باشند، در این صورت اگر x^* یک نقطه بهینه محلی جواب باشد، داریم $\nabla \mathcal{L}(x^*) = 0$ به طوری که $\nabla \mathcal{L}$ بیانگر گرادیان لاگرانژین است [۱۴] (قضیه ۱۲-۶). در این حالت می‌توان نتیجه گرفت که مجموعه نقاط کاندیدای جواب مسأله شامل مجموعه نقاطی هستند که به ازای آنها $\nabla \mathcal{L}(x) = 0$ و یا مجموعه نقاطی که به ازای آنها گرادیان لاگرانژین تعریف نمی‌شود، مثل نقاط ابتدا و انتهای بازه قابل قبول برای هر متغیر.

نکته ۲: در صورتی که لاگرانژین، یک تابع مقعر (محدب) از x باشد جواب مسأله جایی است که به ازای آن $\nabla \mathcal{L}(x) = 0$ می‌شود [۱۴] (قضیه ۱۲-۶) در غیر این صورت بایستی تمام نقاط کاندیدا با توجه به نکته ۱ برای یافتن جواب بررسی شوند.

با توجه به نکات فوق ابتدا لاگرانژین مسأله را به صورت زیر تشکیل می‌دهیم

$$\mathcal{L}(\{\tau_{m,i}, 1 \le i \le N, 1 \le m \le M\}) = \sum_{i=1}^{N} \omega_i \sum_{m=1}^{M} R_m$$
$$\times \int_{\tau_{m,i}}^{\tau_{(m+1),i}} \int_{0}^{G_i(R_m)s_i^i} f_{\Sigma_i}(\Sigma_i) f_{s_i^i}(s_i^i) d\Sigma_i ds_i^i$$
$$- \lambda \sum_{i=1}^{N} \sum_{m=1}^{M} g_{B_i^t}(R_m) \qquad (۱۱)$$
$$\times \int_{\tau_{m,i}}^{\tau_{(m+1),i}} \int_{0}^{G_i(R_m)s_i^i} \frac{1}{s_i^i} f_{\Sigma_i}(\Sigma_i) f_{s_i^i}(s_i^i) d\Sigma_i ds_i^i$$

به طوری که $\lambda \ge 0$ ضریب لاگرانژ است. معادله $\nabla \mathcal{L}(.) = 0$ به دستگاه معادلات زیر برای $\tau_{m,i}$ها می‌انجامد

$$\frac{\partial \mathcal{L}}{\partial \tau_{m,i}} = 0 \Rightarrow -\omega_i R_m \int_{0}^{G_i(R_m)\tau_{m,i}} f_{\Sigma_i}(\Sigma_i) d\Sigma_i$$
$$+ \omega_i R_{m-1} \int_{0}^{G_i(R_{m-1})\tau_{m,i}} f_{\Sigma_i}(\Sigma_i) d\Sigma_i$$
$$+ \lambda \frac{g_{B_i^t}(R_m)}{\tau_{m,i}} \int_{0}^{G_i(R_m)\tau_{m,i}} f_{\Sigma_i}(\Sigma_i) d\Sigma_i \qquad (۱۲)$$
$$- \lambda \frac{g_{B_i^t}(R_{m-1})}{\tau_{m,i}} \int_{0}^{G_i(R_{m-1})\tau_{m,i}} f_{\Sigma_i}(\Sigma_i) d\Sigma_i = 0$$
$$1 \le i \le N \ , \ 1 \le m \le M$$

از آنجا که راجع به علامت $\partial^2 \mathcal{L} / \partial (\tau_{m,i})^2$ نمی‌توان اظهار نظر دقیقی کرد و در نتیجه نمی‌توان راجع به محدب‌بودن لاگرانژین ادعایی داشت لذا برای یافتن مقدار بهینه $\tau_{m,i}$ طبق نکته ۱ بایستی تمامی کاندیداهای جواب را بررسی کرد و جوابی که متوسط نرخ را حداکثر می‌کند، انتخاب کرد. کاندیداهای جواب حل معادله $\partial \mathcal{L} / \partial \tau_{m,i} = 0$ و ابتدا و انتهای بازه قابل قبول برای $\tau_{m,i}$ یعنی $\tau_{m-1,i}$ و $\tau_{m+1,i}$ می‌باشند.

نکته ۳: ضریب لاگرانژ λ بر طبق یک روش ریشه‌یابی معادله بایست به گونه‌ای تعیین شود که قید $C(1)$ با تساوی برقرار گردد [۱۴]. یک روش متداول و کارامد برای ریشه‌یابی، روش دوبخشی[1] است که با تقسیمات متوالی، بازه حضور ریشه مرتباً کوچک می‌شود تا با دقت مناسب به ریشه برسیم.

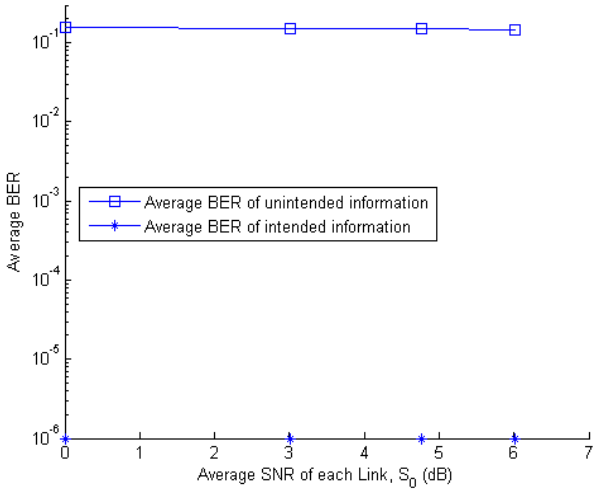
نکته ۴: برای حل (۱۰) می‌توان از روش مجموعه فعال[2] استفاده کرد. در این روش برای یافتن جواب، جستجوی خطی با روزامدکردن هسیان لاگرانژین صورت می‌پذیرد و در فرایند جستجو، قیود مسأله نیز ملاحظه می‌گردند [۱۴]. توابع مربوط به پیاده‌سازی این روش در نرم‌افزار MATLAB موجود است.

همان گونه که دیده می‌شود حل دقیق ارائه‌شده نسبتاً پیچیده است، لذا در بخش بعدی حل تقریبی با دقت بسیار بالا برای مسأله ارائه خواهیم کرد.

۳-۳ حل تقریبی مسأله

در صورتی که بتوان برای $m > 1$، $\int_{0}^{G_i(R_m)\tau_{m,i}} f_{\Sigma_i}(\Sigma_i) d\Sigma_i$ را برابر با

1. Bi-Section
2. Active-Set



شکل ۳: احتمال خطای آشکارسازی اطلاعات در گیرنده‌های اصلی و غیر اصلی وقتی لینک‌ها همگن هستند، $E\{s_i^j\}=S_0, 1\le i,j\le 2$ و $P_{max}=4$ و با وجود نیازمندی‌های یکسان برای کاربران $\omega_i=1, 1\le i\le 2$.

فرض کرد، مجموعه (۱۲) به فرم ساده‌شده زیر $\int_0^{G_i(R_{m-1})\tau_{m,i}} f_{\Sigma_i}(\Sigma_i)d\Sigma_i$ در می‌آید

$$\frac{\partial \mathcal{L}}{\partial \tau_{m,i}}=0 \Rightarrow \tau_{m,i}=\frac{\lambda}{\omega_i}\frac{g_{B_i^t}(R_m)-g_{B_i^t}(R_{m-1})}{R_m-R_{m-1}} \qquad (۱۳)$$
$$, 1\le i\le N, 1\le m\le M$$

در این حالت همچنین می‌توان گفت که $\partial^2\mathcal{L}/\partial(\tau_{m,i})^2<0$ و در نتیجه با توجه به محدب‌بودن لاگرانژین، مقادیر بهینه $\tau_{m,i}$ها از (۱۳) به دست می‌آید و ضریب لاگرانژ λ نیز بر اساس نکته ۳ تعیین می‌شود.

بررسی‌های عددی ما در بخش ۵ نشان می‌دهد از آنجا که مقدار $G_i(R_{m-1})$ تقریباً با $G_i(R_m)$ برابر است فرض یادشده با دقت زیادی برقرار خواهد بود. همچنین در بخش ۵ نرخ‌های قابل دسترسی با حل دقیق مسأله و حل تقریبی با همدیگر مقایسه شده‌اند که این مقایسه حاکی از بسیار اندک‌بودن اختلاف می‌باشد.

۴- بهینه‌سازی بازدهی طیفی در شبکه پخش بدون در نظر گرفتن قید امنیت

در این بخش برای ایجاد یک مبنای مقایسه و بررسی تأثیر اضافه‌شدن قیود محرمانگی، مسأله حداکثرکردن یک جمع وزن‌دار از متوسط نرخ کاربران در شبکه پخش را در نظر می‌گیریم و در این حالت فرض می‌کنیم که صرفاً قید مجموع متوسط توان ارسالی و قیود احتمال خطای بیت برای آشکارسازی اطلاعات اختصاصی وجود دارد. در این حالت مسأله کاملاً مشابه (۳) فرمول‌بندی می‌شود با این تفاوت که $B_i^s=0$ $(1\le i\le N)$ و یا به عبارتی قیود $C(N+2)$ تا $C(N^2+1)$ حذف می‌گردند. در حل این مسأله توان ارسالی لحظه‌ای مشابه (۴) تعیین می‌شود یعنی $p_i=g_{B_i^t}(k_i)/s_i^i$. برای تخصیص نرخ نیز مشابه بخش ۳-۲-۳ آستانه‌های $\{\tau''_{m,i}, 1\le i\le N, 1\le m\le M\}$ در نظر گرفته می‌شود و استراتژی تخصیص نرخ، مشابه (۸) است با این فرق که در این حالت $G_i(k_i)=\infty$ $(1\le i\le N)$ می‌باشد و به عبارتی تخصیص نرخ در باند iام ربطی به مقدار $\Sigma_i=\max_{1\le j\le N, i\ne j}(s_i^j)$ ندارد. مقدار دقیق و بهینه آستانه‌ها مشابه بخش ۳-۳ از رابطه‌ای مشابه (۱۳) به دست می‌آید و ضریب لاگرانژ λ نیز بر اساس نکته ۳ تعیین می‌شود.

۵- ارزیابی‌های عددی

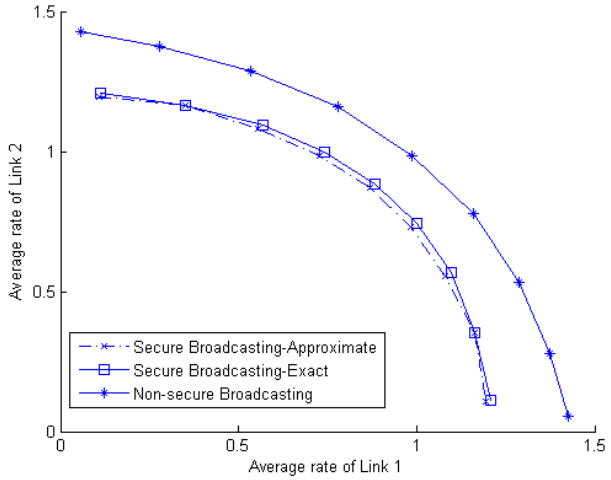
به منظور ارزیابی عملکرد روش پیشنهادی، مدهای AMC از استاندارد [DVB-S2] انتخاب شده‌اند و پارامترهای تخمین احتمال خطا در مدها طبق (۱) در جدول ۱ آمده‌اند. در این حالت ۷ مد ارسال وجود دارد که هر یک به کمک یک نوع کدبندی و یک نوع مدوله‌سازی خاص ساخته می‌شوند و در نهایت به نرخ‌های $R_i\in\{0, 0.5, 1, 1.5, 2, 3, 4\}$ منجر می‌شوند. برای ارزیابی عملکرد یک سیستم مطابق شکل ۱ با احتمال خطاهای مورد نیاز $B_i^t=10^{-6}$، $B_i^s=0.05$، $1\le i\le N$ و کانال‌های دارای فیدینگ رایلی را در نظر می‌گیریم و فرض می‌کنیم متوسط SNR های دریافتی در گیرنده jام، $1\le j\le N$ در تمامی باندهای فرکانسی یکسان باشد و به عبارت دیگر $E\{s_i^j\}=S^j$ و $(1\le i\le N)$.

در شکل ۳ به ارزیابی روش پیشنهادی در تضمین احتمال خطای مناسب برای آشکارسازی اطلاعات اصلی و حفظ محرمانگی اطلاعات در گیرنده‌های غیر خودی پرداخته شده است. در یک شبکه پخش دوکاربره همگن $E\{s_i^j\}=S_0$ $(1\le i,j\le 2)$ با وجود نیازمندی‌های یکسان برای کاربران $\omega_i=1$ $(1\le i\le 2)$ وقتی $P_{max}=4$ است، احتمال خطای آشکارسازی اطلاعات اصلی و احتمال خطای آشکارسازی اطلاعات غیر اصلی به ازای مقادیر مختلف S_0 رسم شده است. آن گونه که از نتایج شبیه‌سازی‌ها بر می‌آید، متوسط احتمال خطاها در محدوده قابل قبولی با توجه به طراحی انجام‌گرفته قرار دارند.

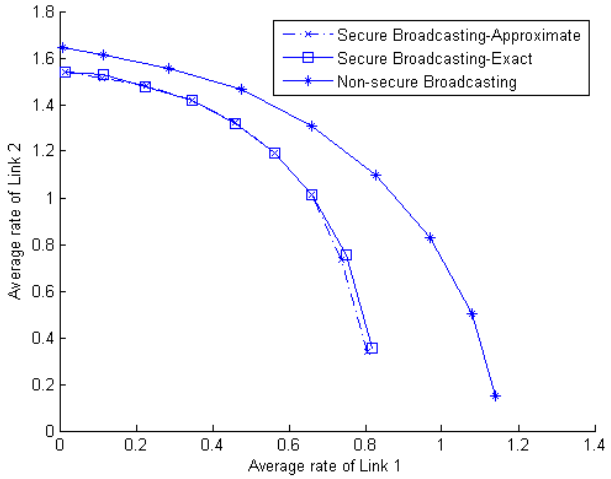
در شکل‌های ۴ و ۵ شبکه‌های پخش دوکاربره در نظر گرفته شده‌اند و نرخ‌های قابل دسترسی به ازای مقادیر مختلف ضرایب وزن‌دهی ω_1 و ω_2 رسم شده است. در شکل ۴ لینک‌ها همگن $(S^1=S^2=4.7\,dB)$ ولی در شکل ۵ لینک‌ها ناهمگن هستند $(S^1=3\,dB$ و $S^2=6\,dB)$ و در هر دو حالت فرض شده که $P_{max}=1$ باشد. در این شبکه‌ها نرخ‌های قابل دسترسی با وجود قیود امنیت و بدون وجود قیود امنیت رسم شده‌اند و همچنین نرخ‌های قابل دسترسی وقتی آستانه‌ها از روش دقیق به دست آمده‌اند و وقتی از روش تقریبی به دست آمده‌اند با همدیگر مقایسه شده‌اند. از بررسی نتایج می‌توان دریافت که اولاً جواب به دست آمده از روش تقریبی بسیار نزدیک به روش دقیق است در حالی که پیچیدگی روش تقریبی به مراتب کمتر می‌باشد و ثانیاً در نظر گرفتن قیود امنیت باعث کاهش نرخ‌های قابل دسترسی شده است، اما در عوض اطلاعات اختصاصی هر گیرنده برای گیرنده غیر خودی قابل آشکارسازی نیست.

در شکل ۶ یک شبکه پخش با لینک‌های همگن در نظر گرفته شده، یعنی $E\{s_i^j\}=3\,dB$ $(1\le i,j\le N)$ و در حالی که قید مجموع متوسط توان‌های ارسالی برابر $P_{max}=2$ است و کاربران دارای نیازمندی‌های یکسان هستند، $\omega_i=1$ $(1\le i\le N)$، متوسط نرخ قابل ارسال در هر لینک بر حسب تعداد کاربران رسم شده است. در این حالت نیز اضافه‌کردن قید امنیت موجب کاهش نرخ‌های قابل دسترسی می‌شود و همچنین به علت ثابت‌بودن مجموع متوسط توان‌های ارسالی با افزایش تعداد کاربران متوسط نرخ هر کاربر کاهش می‌یابد.

در شکل ۷ هم یک شبکه پخش با لینک‌های همگن در نظر گرفته شده، یعنی $E\{s_i^j\}=3\,dB$ $(1\le i,j\le N)$ و قید مجموع متوسط توان‌های ارسالی برابر $P_{max}=2$ است. دو دسته از کاربران با دو نوع مختلف نیازمندی در نظر گرفته شده‌اند. کاربران با شماره فرد دارای متوسط نرخ مورد نیاز کمتری نسبت به کاربران با شماره زوج هستند که این مسأله در ضرایب وزن‌دهی اختصاص داده شده به آنها به صورت زیر منعکس شده است



شکل ۴: نرخ‌های قابل دسترسی در یک شبکه پخش دو لینک به ازای ضرایب مختلف وزن‌دهی ω_1 و ω_2 (نیازمندی‌های مختلف برای لینک‌ها) وقتی لینک‌ها همگن هستند، $S^1 = S^2 = 4.8\,\text{dB}$ و $P_{max} = 1$.



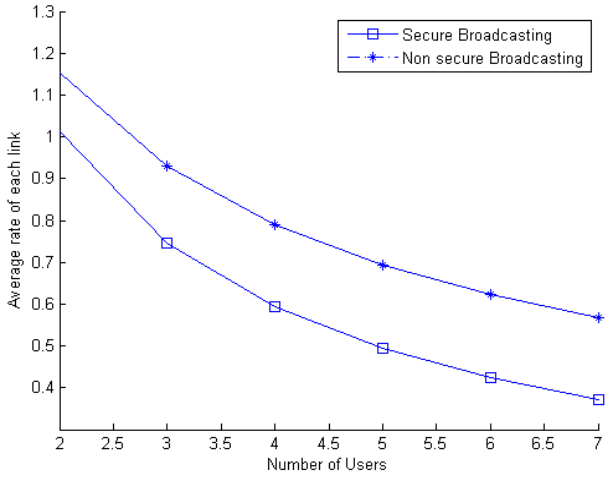
شکل ۵: نرخ‌های قابل دسترسی در یک شبکه پخش دو لینک به ازای ضرایب مختلف وزن‌دهی (نیازمندی‌های مختلف برای لینک‌ها) وقتی لینک‌ها ناهمگن هستند، $S^1 = 3\,\text{dB}$، $S^2 = 6\,\text{dB}$ و $P_{max} = 1$.

$$\begin{cases} \omega_i = 1 & , \quad i : odd \\ \omega_i = 1.5 & , \quad i : even \end{cases} \quad , \quad 1 \le i \le N \qquad (14)$$

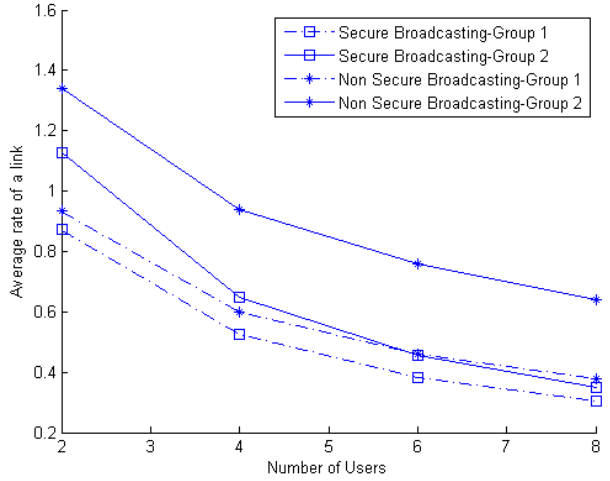
در شکل متوسط نرخ قابل ارسال در هر لینک از هر یک از دو گروه بر حسب تعداد کاربران رسم شده است.

۶- نتیجه‌گیری

در این مقاله مسأله حداکثرکردن یک جمع وزن‌دار از بازدهی طیفی لینک‌ها در شبکه پخش با وجود قیود متوسط توان ارسالی فرستنده، احتمال خطای مناسب آشکارسازی اطلاعات اختصاصی و امنیت لایه فیزیکی مورد بررسی قرار گرفت. با استفاده از کدینگ، مدولاسیون و توان ارسالی وفقی، نرخ ارسال لحظه‌ای در هر لینک به گونه‌ای تنظیم می‌شود که احتمال خطای آشکارسازی اطلاعات در گیرنده‌های غیر خودی بسیار زیاد باشد و در عین حال اطلاعات اختصاصی در گیرنده خودی با احتمال خطای مناسب آشکارسازی شوند. بررسی‌های عددی نشان می‌دهند که اضافه‌شدن قیود امنیت لایه فیزیکی موجب کاهش نرخ‌های قابل دسترسی می‌شود و با این وجود حفظ محرمانگی اطلاعات در شبکه پخش بی‌سیم از اهمیت بالایی برخوردار است.



شکل ۶: نرخ قابل دسترسی در هر لینک در یک شبکه پخش همگن $E\{s_i^j\} = 3\,\text{dB}$ $(1 \le i, j \le N)$ با N کاربر و با وجود نیازمندی‌های یکسان برای کاربران $\omega_i = 1$ $(1 \le i \le N)$ وقتی $P_{max} = 2$.



شکل ۷: نرخ قابل دسترسی در هر لینک در یک شبکه پخش همگن $E\{s_i^j\} = 3\,\text{dB}$ $(1 \le i, j \le N)$ با N کاربر و با وجود نیازمندی‌های مختلف برای کاربران طبق (۱۴) وقتی $P_{max} = 2$.

۷- سپاس‌گزاری

این مقاله با حمایت مالی معاونت پژوهشی دانشگاه اصفهان در قالب طرح پژوهشی شماره ۹۱/۹۲۱۳۶ انتشار یافته است.

مراجع

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 2, pp. 656-715, Oct. 1949.

[2] D. Wyner, "The wiretap channel," *Bell. Syst. Tech. J.*, vol. 54, no. 8, pp. 1355-1387, Oct. 1975.

[3] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 24, no. 3, pp. 339-348, May 1978.

[4] Y. Liang, A. Somekh - Baruch, H. V. Poor, and S. Shamai, "Capacity of cognitive interference channels with and without secrecy," *IEEE Trans. Inform. Theory*, vol. 55, no. 2, pp. 604-619, Feb. 2009.

[5] P. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inform. Theory*, vol. 54, no. 10, pp. 4687-4698, Oct. 2008.

[6] Y. Liang, H. V. Poor, and S. Shamai, "Secrecy capacity region of fading broadcast channels," in *Proc. IEEE Int. Symp. Information Theory*, pp. 1291-1295, Nice, France, 24-29 Jun 2007.

[7] S. T. Chung and A. J. Goldsmith, "Degrees of freedom in adaptive modulation: a unified view," *IEEE Trans. Commun.*, vol. 49, no. 9, pp. 1561-1571, Sep. 2001.

[8] K. J. Hole, H. Holm, and G. E. Oien, "Adaptive multidimensional coded modulation over flat fading channels," *IEEE J. Select. Areas Commun.*, vol. 18, no. 7, pp. 1153-1158, Jul. 2000.
[9] M. Taki and F. Lahouti, "Discrete rate interfering cognitive link adaptation design with primary link spectral efficiency provisioning," *IEEE Trans. Wireless Commun.*, vol. 10, no. 9, pp. 2929-2939, Sep. 2011.
[10] M. Taki and F. Lahouti, "A framework for integrated discrete - rate and power adaptation and user selection in heterogeneous wireless networks," in *Proc. IEEE Wireless Advanced Conf.*, pp. 252-257, London, UK, 20-22 Jun. 2011.
[11] H. Khodakarami and F. Lahouti, "Link adaptation for physical layer security overwireless fading channels," *IET Commun.*, vol. 6, no. 3, pp. 353-362,. 2012.
[12] L. H. Ozarow, S. Shamai, and A. D. Wyner, "Information theoretic considerations for cellular mobile radio," *IEEE Trans. Veh. Technol.*, vol. 43, no. 2, pp. 359-378, May 1994.
[13] D. Klinc, J. Ha, S. W. McLaughlin, J. Barros, and B. Kwak, "LDPC codes for physical layer security," in *Proc. IEEE Global Telecommunications Conf., GLOBECOM*, 6 pp., Honolulu, US, 30 Nov.-4 Dec. 2009.
[14] J. Nocedal and S. J. Wright, *Numerical Optimization*, Springer Verlag, Berlin, New York, 2nd ed., 2006.
[15] *ETSI EN: DVB-S2 Standard Specification*, 2005.

مهرداد تاکی تحصیلات خود را در مقاطع کارشناسی، کارشناسی ارشد و دکتری مهندسی برق- مخابرات به‌ترتیب در سال‌های ۱۳۸۲، ۱۳۸۴ و ۱۳۹۰ در دانشگاه‌های تهران، علم و صنعت ایران و تهران به پایان رسانده است و هم‌اکنون استادیار دانشگاه اصفهان می‌باشد. زمینه‌های تحقیقاتی مورد علاقه ایشان عبارتند از: طراحی و بهینه‌سازی بین لایه‌ای در شبکه‌های مخابراتی بی‌سیم، پردازش سیگنال‌های چندرسانه‌ای بی سیم، تئوری کدینگ، تئوری اطلاعات و رمزنگاری.