ارتباط رله‌کننده امن با گره مقصد کاملاً دوطرفه چند آنتنه

فاطمه جعفریان[۱]، دانشجوی کارشناسی ارشد؛ زهرا مبینی[۲]، استادیار

۱- دانشکده فنی و مهندسی - دانشگاه شهرکرد - شهرکرد - ایران – f.jafarian@stu.sku.ac.ir
۲- دانشکده فنی و مهندسی - دانشگاه شهرکرد - شهرکرد - ایران – z.mobini@eng.sku.ac.ir

چکیده: در این مقاله امنیت لایه فیزیکی یک سیستم بی‌سیم مشارکتی امن کاملاً دوطرفه (FD) [۱] چند آنتنه بررسی می‌شود. فرض می‌شود که گره مبدأ با گره مقصد به کمک یک گره رله درحضور یک گره استراق سمع‌کننده ارتباط برقرار می‌کند. با در نظرگرفتن حالت عملیاتی کاملاً دوطرفه برای گره مقصد، هم‌زمان با دریافت اطلاعات ارسالی در آن، یک سیگنال تداخل جهت تضعیف لینک گره رله-گره استراق سمع‌کننده از گره مقصد به‌طرف گره استراق سمع‌کننده ارسال می‌شود. طرح‌های پرتودهی مختلفی برای سیستم مورد نظر پیشنهاد داده می‌شود و برای آن‌ها نرخ‌های محرمانه لحظه‌ای و متوسط محاسبه می‌شود. همچنین تأثیر تعداد آنتن‌ها، موقعیت گره استراق سمع‌کننده و نیز تأثیر توان ارسالی گره مبدأ و مقصد بر روی نرخ محرمانه متوسط را مورد مطالعه قرار می‌گیرد. نشان داده می‌شود که روش‌های پرتودهی پیشنهادی، به همراه ارسال سیگنال تداخل از گره مقصد به‌میزان زیادی امنیت شبکه مشارکتی را بهبود می‌دهند. همچنین نتایج شبیه‌سازی نشان می‌دهد که انتخاب نوع پرتودهی نقش کلیدی در میزان بهره سیستم کاملاً دوطرفه پیشنهادی دارد.

واژه‌های کلیدی: امنیت لایه فیزیکی، کاملاً دوطرفه، چند ورودی-چند خروجی، ارتباطات بی‌سیم مشارکتی، استراق سمع‌کننده، نرخ محرمانه قابل حصول.

Secure Relaying Communication with Multi-Antenna Full-Duplex Destination

F. Jafarian[1], Master of Sience; Z. Mobini[2], Assistant professor

1- Faculty of Engineering, Shahrekord University, Shahrekord, Iran, Email: f.jafarian@stu.sku.ac.ir
2- Faculty of Engineering, Shahrekord University, Shahrekord, Iran, Email: z.mobini@eng.sku.ac.ir

Abstract: In this paper, the physical layer security of a full-duplex secure cooperative wireless system with multiple input multiple-output (MIMO) destination node is examined. We assume that a source node communicates with a destination node in the presence of an eavesdropper. In addition, a jamming signal is sent via destination to weaken the relay-eavesdropper thanks due to the full-duplex operation at the destination node. We propose different beamforming schemes and accordingly derive the instantaneous and average secrecy rates. We also study the effect of the number of antennas, the position of the eavesdropper, and the transmit power of the source and destination nodes on the average secrecy rate. Our results reveal that beamforming and friendly jamming increase the secrecy of cooperative communication. Moreover, simulation results demonstrate that the choice of the beamforming scheme plays a critical role in determining the FD cooperative communication gains.

Keywords: Physical layer security, full-duplex, multiple-input multiple-output (MIMO), cognitive wireless communication, eavesdropper, achievable secrecy rate.

تاریخ ارسال مقاله: ۱۳۹۶/۰۶/۰۱
تاریخ اصلاح مقاله: ۱۳۹۶/۰۸/۰۶
تاریخ پذیرش مقاله: ۱۳۹۶/۰۹/۰۳
نام نویسنده مسئول: زهرا مبینی
نشانی نویسنده مسئول: ایران - شهرکرد - بلوار رهبر - دانشگاه شهرکرد- دانشکده فنی و مهندسی-گروه الکترونیک و مخابرات.

۱ -معرفی

تکنولوژی ارتباطات بی‌سیم تقریباً در تمام جنبه‌های زندگی اجتماعی وارد شده است. شبکه‌های هوشمند، شبکه‌های حسگر، شبکه‌های تلفن همراه، شهرها و خانه‌های هوشمند فقط چند نمونه از سیستم‌های بی‌سیم است که مردم از آن‌ها اکنون و یا در آینده نزدیک استفاده می‌کنند. امنیت همیشه یک مسئله مهم در ارتباطات بی‌سیم است. با توجه به ماهیت پخش محیط بی‌سیم، سیگنال ارسالی می‌تواند هم توسط کاربرهای مشخص و هم توسط گره‌های استراق سمع‌کننده مخرب[۲] ره‌گیری شود. امنیت و ارتباط بی‌سیم محرمانه [۱] ارائه‌شده توسط تکنیک‌های رمزنگاری مرسوم با توسعه سریع دستگاه‌های محاسبات در معرض تهدید می‌باشد. از دیدگاه تئوری اطلاعات، یک ارتباط امن با بهره‌برداری از ویژگی‌های کانال به‌عنوان‌مثال محوشدن، نویز و تداخل می‌تواند محقق شود، حتی اگر گره استراق سمع‌کننده دارای قابلیت محاسبات قوی باشد.

نرخ محرمانه می‌تواند به‌صورت تفاضل نرخ ارسال لحظه‌ای کانال قانونی و کانال استراق سمع‌کننده تعریف شود. اگر نرخ محرمانه کم‌تر از صفر شود، گره استراق سمع‌کننده می‌تواند بخش زیادی از اطلاعات محرمانه را ره‌گیری کند. هدف امنیت لایه فیزیکی [۲] ماکزیمم‌کردن نرخ محرمانه است. برای دستیابی به این هدف انواع مختلف از تکنیک‌های لایه فیزیکی معرفی شده است. به‌عنوان‌مثال تکنیک آنتن‌های متعدد، تکنیک ارسال سیگنال تداخل (Jamming) به‌صورت مشارکتی و تکنیک نویز مصنوعی. نرخ محرمانه توسط شرایط کانال گره مبدأ-گره مقصد و کانال گره مبدأ-گره استراق سمع‌کننده تحت تأثیر قرار می‌گیرد. هنگامی‌که کانال گره مبدأ-گره مقصد (کانال قانونی) از کانال گره رله-گره استراق سمع‌کننده (کانال استراق سمع‌کننده) ضعیف‌تر باشد، نرخ محرمانه مثبت نمی‌تواند حاصل گردد مگر این‌که چندین آنتن فرستنده به‌کار گرفته شود. از آن‌جا که استفاده از چند آنتن در یک گره مستلزم هزینه سخت‌افزاری قابل توجهی است، بنابراین گره مشارکتی یک جایگزین کم‌هزینه می‌باشد که موجب بهره‌مندی گره‌های تک آنتنه از مزایای سیستم‌های دارای چند آنتن می‌شود.

چندین تکنیک ارسال مشارکتی وجود دارد که در میان آن‌ها رله بازگشایی و ارسال (DF)[۳] و رله تقویت و ارسال (AF)[۴] دو تکنیک مهم هستند. به‌طور خاص ارتباط گره‌ها از طریق گره رله می‌تواند نرخ محرمانه قابل حصول را افزایش دهد.

تکنیک رله دارای چند ورودی-چند خروجی به‌عنوان یک راه مؤثر بهبود عملکرد محرمانه می‌باشد که از یک طرف این تکنیک میزان قدرت سیگنال قانونی را با توجه به چندگانگی فضایی[۵] و فاصله انتشار کوتاه افزایش می‌دهد و از طرف دیگر احتمالاً میزان سیگنال ره‌گیری شده توسط گره استراق سمع‌کننده را از طریق پرتودهی فضایی[۶] تضعیف می‌کند.

در [۳، ۴] طرح‌های پرتودهی بهینه برای پروتکل‌های رله بازگشایی و ارسال و رله تقویت و ارسال در ارتباطات امن دومرحله‌ای ارائه شده است، که نرخ محرمانه را ماکزیمم می‌کند.

در مقاله [۵] تکنیک حذف و همسوسازی تداخل با استفاده از ارسال کد الموتی کاربران ثانویه برای شبکه‌های رادیو شناختگر مطرح و مورد بحث قرار گرفته است.

در [۶] یک طرح پرتودهی قوی با فرض اطلاعات وضعیت کانال ناقص درگره رله مطالعه شده است. علاوه بر این، با فرض عدم وجود اطلاعات وضعیت کانال گره استراق سمع‌کننده در [۷] یک طرح ارسال سیگنال تداخل و پرتودهی مشترک پیشنهاد شده است.

همان‌طورکه قبلاً هم گفته شد یک روش مؤثر برای افزایش نرخ محرمانه در سیستم‌های ارتباطی بی‌سیم، تضعیف قابلیت رمزگشایی گره‌های استراق سمع‌کننده است که با به‌کارگیری تداخل کنترل‌شده و یا نویز مصنوعی صورت می‌گیرد. زمانی‌که گره مبدأ به استفاده از یک آنتن محدود شده است، یک مجموعه از گره‌های رله خارجی برای ارسال مشارکتی سیگنال‌های تداخل می‌توانند به کار گرفته شوند، که کانال مربوط به گره استراق سمع‌کننده را تضعیف می‌کنند. این رویکرد به روش ارسال سیگنال تداخل مشارکتی [۱۵-۸] اشاره دارد. در[۱۵] نویسنده‌ها احتمال قطع محرمانه را با استفاده از روش ارسال سیگنال تداخل مشارکتی و برای سطوح مختلف اطلاعات وضعیت کانال مطالعه می‌کنند. طراحی بردار پرتوی ارسال بهینه همراه با طراحی نویز مصنوعی، برای مینیمم‌کردن احتمال قطع محرمانه در [۱۶، ۱۷] نشان داده شده است. ایده استفاده از گره مقصد و مبدأ به‌عنوان گره‌های ارسال‌کننده سیگنال تداخل در مرحله اول یک شبکه رله دومرحله‌ای در[۱۸] ارائه شده است. همچنین از یک طرح ارسال سیگنال تداخل به کمک گره مقصد در [۱۹] استفاده شده است.

بر اساس مطالعات موجود، روش ارسال سیگنال تداخل مشارکتی به‌طور عمده به گره‌های کمک کننده بیرونی مثلاً رله‌ها تکیه می‌کند، بنابراین از مسائل مربوط به تحرک گره کمک‌کننده، هماهنگ‌سازی و اعتماد رنج می‌برد. در برخی مطالعات جدید روش‌هایی پیشنهاد شده است که نیازی به گره‌های کمک‌کننده بیرونی برای ارسال سیگنال تداخل ندارند مانند طرح پیشنهادی در [۲۰] که در آن گیرنده به‌عنوان یک گره ارسال کننده سیگنال تداخل عمل می‌کند. در این طرح، گره مبدأ عمل ارسال سیگنال را تکرار می‌کند درحالی‌که گره مقصد به‌طور تصادفی یکی از سیگنال‌های ارسال‌شده در هر نمونه زمانی را مسدود می‌کند، از آن‌جا که گره استراق سمع‌کننده نمی‌داند که کدام نمونه سالم

است، بنابراین قادر به بازگشایی سیگنال‌های ارسالی از گره مبدأ نیست.

با این‌حال، طرح فوق نیاز به ارسال مجدد سیگنال از گره مبدأ دارد و بنابراین توان عملیاتی را کاهش می‌دهد. در اکثر طرح‌های مطالعاتی موجود، گره‌ها در حالت نیمه دوطرفه[۷] عمل می‌کنند، بنابراین قادر به دریافت و ارسال اطلاعات به‌طور هم‌زمان نیستند. با این‌حال پیشرفت‌های اخیر در الکترونیک، فناوری آنتن و پردازش سیگنال، حالت عملیاتی کاملاً دوطرفه را برای گره‌ها فراهم می‌سازد به‌طوری‌که گره‌ها می‌توانند اطلاعات را هم‌زمان و بر روی باند فرکانسی یکسان ارسال و دریافت کنند. عملکرد سیستم‌های کاملاً دوطرفه در [۲۱] مطالعه شده است.

در [۲۲] نویسنده‌ها تکنولوژی حالت عملیاتی کاملاً دوطرفه را در زمینه امنیت لایه فیزیکی به کار گرفته‌اند. یک سیستم شامل یک گره مقصد کاملاً دوطرفه تولیدکننده نویز مصنوعی برای تضعیف کانال گره استراق سمع‌کننده در [۲۳] ارائه شده است. عملکرد محرمانه این گیرنده بر اساس ناحیه قطع محرمانه، از یک دیدگاه هندسی ارزیابی می‌شود.

در این مقاله مزایای بالقوه گره مقصد کاملاً دوطرفه دارای چند ورودی-چند خروجی را در یک سیستم مشارکتی امن شامل یک گره مبدأ، یک گره رله بازگشایی و ارسال و یک گره استراق سمع‌کننده بررسی می‌شود که گره مقصد به‌طور هم‌زمان به‌عنوان یک گره ارسال‌کننده سیگنال تداخل و یک گیرنده عمل می‌کند و نرخ محرمانه را بهبود می‌دهد.

در سیستم پیشنهادی هم‌زمان با ارسال سیگنال تداخل از آنتن‌های خروجی گره مقصد به سمت گره استراق سمع‌کننده، این سیگنال در سمت آنتن‌های ورودی گره مقصد نیز دریافت می شود و باعث ایجاد یک حلقه خودتداخلی[۸] در گره مقصد می‌شود. با این‌حال در [۲۳] فرض بر این است که حلقه خودتداخلی در گره مقصد می‌تواند کاملاً حذف شود که یک فرض عملی نمی‌باشد. اگر وضعیت نامطلوب از یک گره مبدأ تک آنتنه را در نظر بگیریم، از آن‌جا که در این حالت درجه آزادی کافی (DoF)[۹] برای طراحی و ارسال سیگنال تداخل وجود ندارد، بنابراین مولد گره مبدأ نرخ محرمانه را بهبود نخواهد داد.

در ایده پیشنهادی ما، یک مکانیزم محافظت از سیگنال‌های اطلاعات دریافت‌شده در سمت گره مقصد فراهم می‌شود، بدون این‌که به ارسال مجدد داده‌ها از گره مبدأ و یا گره‌های کمکی خارجی برای ارسال سیگنال تداخل نیاز داشته باشد. در سیستم پیشنهادی به دلیل این‌که گره مقصد عملکرد کاملاً دوطرفه دارد، سیگنال تداخلی که گره مقصد به‌طرف گره استراق سمع‌کننده ارسال می‌کند بر روی مدارهای گیرنده گره مقصد هم اثر می‌گذارد که به آن خودتداخلی گفته می‌شود و برای مبارزه با این خودتداخلی، طرح‌های پرتودهی ارسال و دریافت مناسبی پیشنهاد می‌دهیم که با کمک روش‌های بهینه‌سازی، قابلیت حذف خودتداخلی در گره مقصد را کاملاً دارند و به‌این‌ترتیب سیستم ما دیگر تداخل محدود نمی‌باشد و همچنین هم‌زمان نرخ محرمانه سیستم افزایش می‌یابد. نتایج و تحلیل‌های مهمی را که در این مقاله انجام شده است، در چهار دسته زیر خلاصه می‌نماییم:

- در سیستم مورد نظر بردارهای پرتوی ارسال و دریافت برای طرح‌های پرتودهی TZF[۱۰] RZF[۱۱] و MRC/MRT[۱۲] طراحی می‌شود. در ضمن برای این طرح‌های پرتودهی، احتمال قطع در گره استراق سمع‌کننده و گره مقصد محاسبه می‌شود.
- عبارت‌های دقیقی برای نرخ‌های محرمانه قابل حصول متوسط و لحظه‌ای سیستم به‌دست آورده می‌شود که برای طرح‌های پرتودهی مختلف معتبر خواهند بود.
- مشاهده می‌کنیم که برای توان‌های ارسالی کم‌تر از توان بهینه، طرح MRC/MRT بهتر از طرح‌های TZF و RZF عمل می‌کند ولی بعد از نقطه توان ارسالی بهینه، بازدهی این طرح‌ها بهتر از MRC/MRT می‌شود. همچنین مشاهده می‌کنیم که در طرح‌های TZF و RZF نرخ محرمانه متوسط به‌ترتیب با افزایش تعداد آنتن‌های ارسالی (N_T) و تعداد آنتن‌های دریافتی (N_R) به‌طور قابل‌توجهی افزایش می‌یابد.
- با توجه به نتایج شبیه‌سازی مشاهده می‌کنیم تا زمانی‌که فاصله گره استراق سمع‌کننده از گره رله کم باشد عملکرد طرح MRC/MRT از طرح RZF بهتر می‌باشد ولی با افزایش این فاصله، طرح RZF دارای عملکرد بهتری می‌باشد.

نمادها: از حروف انگلیسی بزرگ و کوچک با فونت توپر (bold) به‌ترتیب برای نشان‌دادن ماتریس و بردار استفاده می‌کنیم. بالانویس $(.)^{\dagger}$، هرمیتین یک بردار یا ماتریس را نشان می‌دهد. عملگر $\|.\|$، برای نشان‌دادن اندازه بردار استفاده می‌شود. از نماد $X \sim CN(\mu,\sigma^2)$ برای نشان‌دادن توزیع مختلط گوسی متقارن با متوسط μ و واریانس σ^2 برای متغیر تصادفی X استفاده می‌کنیم. $P(.)$، $F_x(.)$ و $f_x(.)$ به‌ترتیب برای نشان‌دادن احتمال، تابع چگالی احتمال (pdf)[۱۳] و cdf[۱۴] متغیر تصادفی X استفاده می‌شوند. $\Gamma(a)$ تابع گاما[۱۵] است.

۲ -مدل سیستم

در این مقاله ما یک سیستم ارتباطات بی‌سیم شامل یک گره مبدأ (S)، یک گره مقصد (D)، یک گره رله (R) و یک گره استراق سمع‌کننده (E) را در نظر می‌گیریم. سیستم ارتباطی مورد نظر در شکل ۱ نشان داده شده است. گره مبدأ (S)، گره رله (R) و گره استراق سمع‌کننده (E) تک آنتنه می‌باشند اما برای فعال‌کردن عملیات کاملاً دوطرفه، مقصد باید مجهز به دو مجموعه از آنتن‌ها باشد. به‌طور دقیق N_R آنتن دریافت و N_T آنتن ارسال. ما فرض می‌کنیم که هیچ لینک مستقیمی از گره مبدأ (S) به گره مقصد (D) وجود ندارد، بنابراین گره

مبدأ (S) با کمک یک گره رله (R) که پروتکل بازگشایی و ارسال را اتخاذ کرده است، با گره مقصد (D) ارتباط برقرار می‌کند، درحالی‌که گره استراق سمع‌کننده (E) تلاش می‌کند تا پیام ارسالی از طرف گره رله (R) را شنود کند. گره مقصد یک سیگنال تداخل به‌طرف گره استراق سمع‌کننده (E) برای تضعیف لینک گره استراق سمع‌کننده-گره رله ارسال می‌کند و هم‌زمان سیگنال مبدأ را دریافت می‌کند. حلقه خودتداخلی از طرف خروجی مقصد به ورودی مقصد با ضریب کانال $\mathbf{H}_{DD}$ دارای ابعاد $N_R \times N_T$ نشان داده می‌شود. h_{SR} بردار کانال 1×1 بعدی برای لینک مبدأ-رله است. $\mathbf{h}_{RD}$ بردار کانال $N_R \times 1$ بعدی برای لینک رله-مقصد است. h_{RE} بردار کانال 1×1 بعدی برای لینک رله-استراق‌سمع‌کننده است و $\mathbf{h}_{DE}$ بردار کانال $1\times N_T$ بعدی برای لینک مقصد-استراق سمع‌کننده است. $\alpha_{ij} = d_{ij}^{-\mu}$ اتلاف مسیر وابسته به فاصله است که در آن μ ضریب میرایی و d_{ij} فاصله انتشار بین گره i و j است. در این مقاله فرض می‌کنیم کانال‌ها یک مدل محوشدگی رایلی[۱۶] را تجربه می‌کنند و دارای توزیع گوسی با واریانس σ^2 و میانگین صفر هستند.

۲ ـ ۱ ـ مدل سیگنال‌ها

اگر x_S سیگنال ارسالی از گره مبدأ و دارای توزیع گوسی نرمال، p_S توان ارسالی در گره مبدأ و n_R نویز گوسی سفید جمع‌شونده (AWGN) با میانگین صفر و واریانس σ_R^2 در گره رله باشد، سیگنال دریافتی در گره رله به‌صورت زیر به‌دست آورده می‌شود:

$$y_R[n] = h_{SR}[n]\sqrt{\frac{p_S}{d_{SR}^{\mu}}}x_S[n] + n_R[n]. \quad (۱)$$

گره رله پروتکل بازگشایی و ارسال را اتخاذ می‌کند بنابراین بعد از دریافت سیگنال، ابتدا سیگنال x_S را رمزگشایی کرده و سپس سیگنال را به گره مقصد می‌فرستد. سیگنال ارسالی از گره رله به‌صورت زیر نشان داده می‌شود:

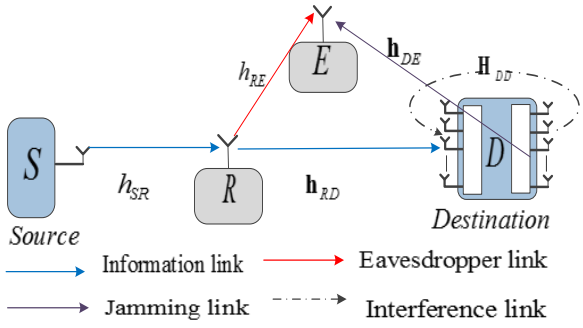
$$x_R[n] = \sqrt{p_R}x_S[n-\tau], \quad (۲)$$

که در آن τ تأخیر ناشی از زمان پردازش سیگنال است. سرانجام سیگنال‌های دریافتی در گره مقصد و گره استراق سمع‌کننده به‌ترتیب به‌صورت زیر بیان می‌شوند:

$$y_D[n] = \sqrt{\frac{p_R}{d_{RD}^{\mu}}}\mathbf{w}_r^{\dagger}\mathbf{h}_{RD}x_S[n-\tau] + \sqrt{p_d}x_J[n]\mathbf{w}_r^{\dagger}\mathbf{H}_{DD}\mathbf{w}_t + n_D[n], \quad (۳)$$

$$y_E[n] = \sqrt{\frac{p_R}{d_{RE}^{\mu}}}h_{RE}x_s[n-\tau] + \sqrt{\frac{p_d}{d_{DE}^{\mu}}}x_J[n]\mathbf{h}_{DE}\mathbf{w}_t + n_E[n], \quad (۴)$$

که در آن‌ها $x_J[n]$ سیگنال پارازیت ارسالی از گره مقصد است. $\mathbf{w}_r$ و $\mathbf{w}_t$ به‌ترتیب بردار پرتوی دریافت $N_R\times1$ بعدی و بردار ارسال $N_T\times1$ بعدی طراحی‌شده در گره مقصد با عملکرد کاملاً دوطرفه و دارای



شکل ۱: مدل سیستم و مدل ارسال سیگنال.

چندورودی-چندخروجی است. همچنین $n_D[n] \sim CN(0,\sigma_D^2)$ و $n_E[n] \sim CN(0,\sigma_E^2)$ به‌ترتیب نویز در گره مقصد و گره استراق سمع‌کننده هستند. بنابراین SINR در مقصد توسط رابطه زیر به‌دست می‌آید:

$$y_D = \min\left(\frac{p_S|h_{SR}|^2}{d_{SR}^{\mu}\sigma_R^2}, \frac{\frac{p_R}{d_{RD}^{\mu}}|\mathbf{w}_r^{\dagger}\mathbf{h}_{RD}|^2}{|\mathbf{w}_r^{\dagger}\mathbf{H}_{DD}\mathbf{w}_t|^2 p_d + \sigma_D^2}\right). \quad (۵)$$

SINR شنود برای گره استراق سمع‌کننده نیز به‌صورت زیر به‌دست می‌آید که در آن p_d توان ارسالی در گره مقصد است.

$$y_E = \frac{\frac{p_R}{d_{RE}^{\mu}}|h_{RE}|^2}{\frac{p_d}{d_{DE}^{\mu}}|\mathbf{h}_{DE}\mathbf{w}_t|^2 + \sigma_E^2}. \quad (۶)$$

همان‌طورکه ذکر شد، در سیستم پیشنهادی مورد نظر برای افزایش امنیت، گره مقصد سیگنال تداخلی به سمت گره استراق سمع‌کننده ارسال می‌کند و چون گره مقصد عملکردی کاملاً دوطرفه دارد، سیگنال خودتداخلی در گره مقصد ایجاد می‌شود. برای حذف این تداخل دو روش پرتودهی TZF، RZF را پیشنهاد می‌دهیم که همان‌طورکه در ادامه دیده می‌شود سیگنال خودتداخلی را کاملاً حذف می‌کنند و درعین‌حال امنیت سیستم را نیز افزایش می‌دهند. همچنین بازدهی روش پرتودهی MRC/MRT را نیز به‌عنوان یک روش پرتودهی با پیچیدگی پایین و برای مقایسه با طرح‌های TZF و RZF در ادامه بررسی می‌کنیم.

۲ ـ ۲ ـ طراحی بردار پرتوی دریافت و ارسال طرح TZF

در طرح TZF، مقصد از مزایای آنتن‌های متعدد ارسال برای حذف کامل خودتداخلی استفاده می‌کند. علاوه بر این طرح MRC [۲۴] در

ورودی مقصد استفاده می‌شود، به‌طوری‌که بردار پرتوی دریافت برابر با $\mathbf{w}_r = \frac{h_{RD}}{\|h_{RD}\|}$ است. بردار پرتوی ارسال بهینه $\mathbf{w}_t$ نیز با در نظرگرفتن این‌که γ_D ماکزیمم شود و خودتداخلی حذف گردد، به‌دست آورده می‌شود.

$$\max \left| \mathbf{w}_r^{\dagger} \mathbf{h}_{RD} \right|^2 \quad (۷)$$
$$s.t.\ \mathbf{h}_{RD}^{\dagger} \mathbf{H}_{DD} \mathbf{w}_t = 0.$$

درنتیجه بردار پرتوی ارسال برای طرح TZF برابر خواهد بود با $\mathbf{w}_t^{ZF} = \frac{\mathbf{B}\mathbf{h}_{DE}^{\dagger}}{\|\mathbf{B}\mathbf{h}_{DE}^{\dagger}\|}$ که $\mathbf{B} \sim \mathbf{I} - \frac{\mathbf{H}_{DD}^{\dagger}\mathbf{h}_{RD}\mathbf{h}_{RD}^{\dagger}\mathbf{H}_{DD}}{\|\mathbf{h}_{RD}^{\dagger}\mathbf{H}_{DD}\|^2}$ است [۲۴].

با جایگزینی $\mathbf{w}_r$ و $\mathbf{w}_t^{ZF}$ در (۵) و (۶)، SINR در گره مقصد و گره استراق سمع‌کننده به ترتیب به‌صورت زیر به دست آورده می‌شوند.

$$y_D^{TZF} = \min\left(\frac{p_S |h_{SR}|^2}{d_{SR}^{\mu}\sigma_R^2}, \frac{\frac{p_R}{d_{RD}^{\mu}}\|\mathbf{h}_{RD}\|^2}{\sigma_D^2} \right), \quad (۸)$$

و

$$y_E^{TZF} = \frac{\frac{p_R}{d_{RE}^{\mu}}|h_{RE}|^2}{\frac{p_d}{d_{DE}^{\mu}}\left|\mathbf{h}_{DE}\mathbf{w}_t^{ZF}\right|^2 + \sigma_E^2}, \quad (۹)$$

که در آن $\left|\mathbf{h}_{DE}\mathbf{w}_t^{ZF}\right|^2$ دارای توزیع chi-squares [۱۰] با درجه آزادی $2(N_T-1)$ است که به‌صورت $\left|\mathbf{h}_{DE}\mathbf{w}_t^{ZF}\right| \sim x_{2(N_T-1)}^2$ نشان داده می‌شود.

۳ ۲ -طراحی بردار پرتوی دریافت و ارسال طرح RZF

در این طرح بردار پرتوی ارسال با استفاده از قانون MRT [۲۵] برابر با $\mathbf{w}_t = \frac{\mathbf{h}_{DE}^{\dagger}}{\|\mathbf{h}_{DE}\|}$ قرار داده می‌شود و بردار پرتوی دریافت $\mathbf{w}_r$ با در نظرگرفتن این‌که γ_E مینیمم شود و خودتداخلی حذف گردد، به‌دست آورده می‌شود.

$$\max \left| \mathbf{w}_r^{\dagger} \mathbf{h}_{RD} \right|^2 \quad (۱۰)$$
$$s.t.\ \mathbf{w}_r^{\dagger} \mathbf{H}_{DD} \mathbf{h}_{DE}^{\dagger} = 0.$$

درنتیجه بردار پرتوی دریافت برای طرح RZF برابر خواهد بود با $\mathbf{w}_r^{ZF} = \frac{\mathbf{D}\mathbf{h}_{RD}}{\|\mathbf{D}\mathbf{h}_{RD}\|}$ که $\mathbf{D} \sim \mathbf{I} - \frac{\mathbf{H}_{DD}\mathbf{h}_{DE}^{\dagger}\mathbf{h}_{DE}\mathbf{H}_{DD}^{\dagger}}{\|\mathbf{h}_{DE}\mathbf{H}_{DD}\|^2}$ است [۲۵].

با جایگزینی $\mathbf{w}_t$ و $\mathbf{w}_r^{ZF}$ در (۵) و (۶)، SINR در گره مقصد و گره استراق سمع‌کننده به‌ترتیب به‌صورت زیر به‌دست آورده می‌شوند:

$$y_D^{RZF} = \min\left(\frac{p_S |h_{SR}|^2}{d_{SR}^{\mu}\sigma_R^2}, \frac{\frac{p_R}{d_{RD}^{\mu}}\left|\left(w_r^{ZF}\right)^{\dagger}\mathbf{h}_{RD}\right|^2}{\sigma_D^2} \right), \quad (۱۱)$$

$$y_E^{RZF} = \frac{\frac{p_R}{d_{RE}^{\mu}}|h_{RE}|^2}{\frac{p_d}{d_{DE}^{\mu}}\|\mathbf{h}_{DE}\|^2 + \sigma_E^2}, \quad (۱۲)$$

که در آن $\left|\left(\mathbf{w}_r^{ZF}\right)^{\dagger}\mathbf{h}_{RD}\right|^2$ دارای توزیع نمایی است [۲۵].

۴ ۲ -طرح MRC/MRT

درنهایت در طرح MRC/MRT ، $\mathbf{w}_r$ و $\mathbf{w}_t$ به‌ترتیب به‌صورت زیر به‌دست می‌آیند. ذکر این نکته ضروری است که طرح‌های TZF و RZF در شرایطی که خودتداخلی وجود نداشته باشد عملکرد یکسانی با طرح MRC/MRT دارند. اما طرح MRC/MRT در حضور خودتداخلی عملکرد بهینه‌ای ندارد و برای سیستم‌های نیمه دوطرفه یا دوطرفه با سطح خودتداخلی کم مناسب می‌باشد.

$$\mathbf{w}_r^{MRC} = \frac{\mathbf{h}_{RD}}{\|\mathbf{h}_{RD}\|},$$
$$\mathbf{w}_t^{MRT} = \frac{\mathbf{h}_{DE}^{\dagger}}{\|\mathbf{h}_{DE}\|}.$$

با جایگزینی $\mathbf{w}_r^{MRC}$ و $\mathbf{w}_t^{MRC}$ در (۵) و (۶)، SINR در گره مقصد و گره استراق سمع‌کننده به‌ترتیب به‌صورت زیر به‌دست آورده می‌شوند:

$$y_D^{MRC} = \min\left(\frac{p_S |h_{SR}|^2}{d_{SR}^{\mu}\sigma_R^2}, \frac{\frac{p_R}{d_{RD}^{\mu}}\|\mathbf{h}_{RD}\|^2}{p_d\left|\mathbf{w}_r^{\dagger}\mathbf{H}_{DD}\mathbf{w}_t\right|^2 + \sigma_D^2} \right), \quad (۱۳)$$

و

$$y_E^{MRC} = \frac{\frac{p_R}{d_{RE}^{\mu}}|h_{RE}|^2}{\frac{p_d}{d_{DE}^{\mu}}\|\mathbf{h}_{DE}\|^2 + \sigma_E^2}, \quad (۱۴)$$

که در آن $\|\mathbf{h}_{DE}\|^2$ و $\|\mathbf{h}_{RD}\|^2$ دارای توزیع Chi-squares با درجه‌های آزادی به‌ترتیب (N_R-1) و (N_T-1) می‌باشند.

۳ -تحلیل بازدهی سیستم

در این بخش، بر روی تحلیل عملکرد محرمانه سیستم ارتباطی بی‌سیم متشکل از یک گره مقصد کاملاً دوطرفه دارای چندورودی-چندخروجی و یک گره رله بازگشایی و ارسال تمرکز می‌کنیم. ظرفیت کانال از گره مبدأ به گره رله به‌صورت زیر به‌دست می‌آید:

$$C_{SR} = \log_2(1+\gamma_{SR}) = \log_2\left(1+\frac{p_S|h_{SR}|^2}{d_{SR}^{\mu}\sigma_R^2}\right). \quad (۱۵)$$

مشاهده می‌کنیم که ظرفیت کانال از گره مبدأ به گره رله با افزایش توان ارسالی گره مبدأ و یا کاهش فاصله بین گره مبدأ و گره رله افزایش می‌یابد.

به همین ترتیب ظرفیت کانال از گره رله به گره مقصد به‌صورت زیر به‌دست آورده می‌شود:

$$C_{RD}=\log_2(1+\gamma_{RD})=\log_2\left(1+\frac{\frac{p_R}{d_{RD}^{\mu}}\left|\mathbf{w}_r^{\dagger}\mathbf{h}_{RD}\right|^2}{\left|\mathbf{w}_r^{\dagger}\mathbf{H}_{DD}\mathbf{w}_t\right|^2 p_d+\sigma_D^2}\right). \quad (۱۶)$$

با بررسی رابطه فوق درمی‌یابیم که ظرفیت کانال از گره رله به گره مقصد با افزایش توان ارسالی گره رله و یا کاهش فاصله بین گره رله و گره مقصد افزایش می‌یابد.

ظرفیت کانال قانونی و کانال استراق سمع‌کننده برای پروتکل رله بازگشایی و ارسال به‌ترتیب به‌صورت زیر محاسبه می‌شوند:

$$C_D=\min(C_{SR},C_{RD}), \quad (۱۷)$$

که

$$C_D=\log_2\left(1+\min\left(\frac{p_S\left|h_{SR}\right|^2}{d_{SR}^{\mu}\sigma_R^2},\frac{\frac{p_R}{d_{RD}^{\mu}}\left|\mathbf{w}_r^{\dagger}\mathbf{h}_{RD}\right|^2}{\left|\mathbf{w}_r^{\dagger}\mathbf{H}_{DD}\mathbf{w}_t\right|^2 p_d+\sigma_D^2}\right)\right) \quad (۱۸)$$

و

$$C_E=\log_2\left(1+\frac{\frac{p_R}{d_{RE}^{\mu}}\left|h_{RE}\right|^2}{\frac{p_d}{d_{DE}^{\mu}}\left|\mathbf{h}_{DE}\mathbf{w}_t\right|^2+\sigma_E^2}\right). \quad (۱۹)$$

۳ ـ۱ ـنرخ محرمانه لحظه‌ای

با توجه به تعریف ظرفیت کانال محرمانه و کانال استراق سمع‌کننده، نرخ محرمانه لحظه‌ای (Instantaneous Secrecy Rate) [۲۶] به‌صورت زیر به‌دست می‌آید:

$$R_{SEC}^{DF}=C_D^{DF}-C_E^{DF}, \quad (۲۰)$$

که

$$R_{SEC}^{DF}=\log_2\left(1+\min\left(\frac{p_S\left|h_{SR}\right|^2}{d_{SR}^{\mu}\sigma_R^2},\frac{\frac{p_R}{d_{RD}^{\mu}}\left|\mathbf{w}_r^{\dagger}\mathbf{h}_{RD}\right|^2}{\left|\mathbf{w}_r^{\dagger}\mathbf{H}_{DD}\mathbf{w}_t\right|^2 p_d+\sigma_D^2}\right)\right)-\log_2\left(1+\frac{\frac{p_R}{d_{RE}^{\mu}}\left|h_{RE}\right|^2}{\frac{p_d}{d_{DE}^{\mu}}\left|\mathbf{h}_{DE}\mathbf{w}_t\right|^2+\sigma_E^2}\right). \quad (۲۱)$$

۳ ـ۲ ـنرخ محرمانه متوسط

در این زیربخش نرخ محرمانه متوسط (Average Secrecy Rate) که یک معیار عملکردی مهم برای ارزیابی امنیت سیستم‌ها است را برای طرح‌های پرتودهی TZF، RZF و MRC/MRT بررسی خواهیم کرد. نرخ محرمانه متوسط را می‌توان توسط رابطه زیر محاسبه کرد [۲۶]:

$$\bar{R}=\frac{1}{\ln 2}\int\frac{F_{\gamma_E}(x)}{1+x}\left(1-F_{\gamma_D}(x)\right)dx, \quad (۲۲)$$

که در آن $F_{\gamma_E}(x)$ و $F_{\gamma_D}(x)$ به‌ترتیب احتمال قطع در گره استراق سمع‌کننده و گره مقصد هستند.

۳ ـ۲ ـ۱ ـعملکرد طرح TZF

با جایگزینی $\mathbf{w}_r=\frac{\mathbf{h}_{RD}}{\|\mathbf{h}_{RD}\|}$ و $\mathbf{w}_t^{ZF}=\frac{\mathbf{B}\mathbf{h}_{DE}^{\dagger}}{\|\mathbf{B}\mathbf{h}_{DE}^{\dagger}\|}$ برای طرح پرتودهی TZF در (۱۶) ظرفیت‌کانال بین گره رله و گره مقصد به‌صورت زیر محاسبه می‌شود:

$$C_{RD}^{TZF}=\log_2\left(1+\frac{p_R\|\mathbf{h}_{RD}\|^2}{d_{RD}^{\mu}\sigma_D^2}\right). \quad (۲۳)$$

ظرفیت کانال قانونی برای پروتکل رله بازگشایی و ارسال در طرح TZF به‌صورت زیر به‌دست می‌آید:

$$C_D^{TZF}=\log_2\left(1+\min\left(\frac{p_s\left|h_{SR}\right|^2}{d_{SR}^{\mu}\sigma_R^2},\frac{p_R\|h_{RD}\|^2}{d_{RD}^{\mu}\sigma_D^2}\right)\right). \quad (۲۴)$$

سرانجام نرخ محرمانه لحظه‌ای برای طرح TZF می‌تواند به‌فرم زیر به‌دست آید:

$$R_{SEC}^{TZF}=\log_2\left(1+\min\left(\frac{p_S\left|h_{SR}\right|^2}{d_{SR}^{\mu}\sigma_R^2},\frac{p_R\left|(w_r)^{\dagger}h_{RD}\right|^2}{d_{RD}^{\mu}\sigma_D^2}\right)\right)-\log_2\left(1+\frac{\frac{p_R}{d_{RE}^{\mu}}\left|h_{RE}\right|^2}{\frac{p_d}{d_{DE}^{\mu}}\left|\mathbf{h}_{DE}\mathbf{w}_t^{ZF}\right|^2+\sigma_E^2}\right). \quad (۲۵)$$

برای محاسبه نرخ محرمانه متوسط برای طرح TZF بر اساس رابطه (۲۲) $F_{\gamma_E^{TZF}}(x)$ و $F_{\gamma_D^{TZF}}(x)$ مورد نیاز می‌باشند. در قضیه‌های (۱) و (۲) به‌ترتیب $F_{\gamma_E^{TZF}}(x)$ و $F_{\gamma_D^{TZF}}(x)$ بیان می‌شوند که در حقیقت معرف احتمال قطع در گره مقصد و گره استراق سمع‌کننده می‌باشند.

قضیه ۱: در سیستم مشارکتی امن پیشنهادی با روش شکل‌دهی پرتوی TZF، احتمال قطع (تابع توزیع تجمعی SINR دریافتی) در گره مقصد از رابطه زیر به‌دست می‌آید:

$$P_{out}^{D,TZF}=F_{\gamma_D^{TZF}}(x)=1-e^{\frac{-x}{a_0}}+e^{\frac{-x}{a_0}}\frac{\gamma\left(\frac{K}{2},\frac{x}{2a_1}\right)}{\Gamma\left(\frac{K}{2}\right)}. \quad (۲۶)$$

که در آن $K=2N_R$ و a_0 و a_1 در ضمیمه ۱ تعریف شده‌اند.

اثبات: به ضمیمه ۱ مراجعه شود.

مشاهده می‌شود که احتمال قطع در گره مقصد با افزایش تعداد آنتن‌های دریافتی (N_R) و کاهش توان ارسالی گره مبدأ و گره رله کاهش می‌یابد.

قضیه ۲: در سیستم مشارکتی امن پیشنهادی با روش شکل‌دهی پرتوی TZF، احتمال قطع (تابع توزیع تجمعی SINR دریافتی) در گره استراق سمع‌کننده از رابطه زیر به‌دست می‌آید:

$$P_{out}^{E,TZF}=F_{\gamma_E^{TZF}}(x)=1-e^{\frac{-x}{a_2}}+e^{\frac{-x}{a_2}}a_3x\sum_{K=0}^{N_T-2}\frac{1}{\mathrm{K!}}a_2^K\left(a_2+a_3x\right)^{-K-1}\Gamma\left(K+1\right).$$

(۲۷)

که در آن a_2 و a_3 در ضمیمه ۲ تعریف شده‌اند.

اثبات: به ضمیمه ۲ مراجعه شود.

مشاهده می‌کنیم که احتمال قطع در گره استراق سمع‌کننده با افزایش توان ارسالی گره مقصد افزایش می‌یابد.

درنهایت به‌کمک نتایج به‌دست‌آمده در قضیه‌های (۱) و (۲) و استفاده از رابطه (۲۲) نرخ محرمانه متوسط برای طرح TZF به‌دست می‌آید.

۳ ۲ ۴ -عملکرد طرح RZF

با جایگذاری $\mathbf{w}_r^{ZF}=\frac{\mathbf{Dh}_{RD}}{\left\|\mathbf{Dh}_{RD}\right\|}$ و $\mathbf{w}_t=\frac{\mathbf{h}_{DE}^{\dagger}}{\left\|\mathbf{h}_{DE}\right\|}$ در (۱۶) برای طرح پرتودهی RZF ظرفیت کانال بین گره رله و گره مقصد به‌صورت زیر به‌دست می‌آید:

$$C_{RD}^{RZF}=\log_2\left(1+\frac{p_R\left|\left(\mathbf{w}_r^{ZF}\right)^{\dagger}\mathbf{h}_{RD}\right|^2}{d_{RD}^{\mu}\sigma_D^2}\right).\qquad(۲۸)$$

ظرفیت کانال قانونی برای پروتکل رله‌ی بازگشایی و ارسال در طرح RZF به‌صورت زیر به‌دست می‌آید:

$$C_D^{RZF}=\log_2\left(1+\min\left(\frac{p_S\left|h_{SR}\right|^2}{d_{SR}^{\mu}\sigma_R^2},\frac{p_R\left|\left(w_r^{ZF}\right)^{\dagger}\mathbf{h}_{RD}\right|^2}{d_{RD}^{\mu}\sigma_D^2}\right)\right).\qquad(۲۹)$$

سرانجام نرخ محرمانه لحظه‌ای برای طرح RZF می‌تواند به‌فرم زیر به‌دست آید:

$$R_{SEC}^{RZF}=\log_2\left(1+\min\left(\frac{p_S\left|h_{SR}\right|^2}{d_{SR}^{\mu}\sigma_R^2},\frac{p_R\left|\left(\mathbf{w}_r^{ZF}\right)^{\dagger}\mathbf{h}_{RD}\right|^2}{d_{RD}^{\mu}\sigma_D^2}\right)\right)-\log_2\left(1+\frac{\frac{p_R}{d_{RE}^{\mu}}\left|h_{RE}\right|^2}{\frac{p_d}{d_{DE}^{\mu}}\left\|\mathbf{h}_{DE}\right\|^2+\sigma_E^2}\right).\qquad(۳۰)$$

برای محاسبه نرخ محرمانه متوسط برای طرح RZF بر اساس رابطه (۲۲) به $F_{\gamma_E^{RZF}}(x)$ و $F_{\gamma_D^{RZF}}(x)$ نیاز داریم که در قضیه‌های (۳) و (۴) به‌ترتیب به محاسبه آن‌ها می‌پردازیم.

قضیه ۳ : در سیستم مشارکتی امن پیشنهادی با روش شکل‌دهی پرتوی RZF، احتمال قطع (تابع توزیع تجمعی SINR دریافتی) درگره مقصد از رابطه زیر به‌دست می‌آید:

$$P_{out}^{D,RZF}=F_{\gamma_D^{RZF}}(x)=1-e^{\frac{-x}{a_0}}+e^{\frac{-x}{a_0}}\frac{\gamma\left(\frac{K}{2},\frac{x}{2a_1}\right)}{\Gamma\left(\frac{K}{2}\right)}.\qquad(۳۱)$$

اثبات: مشابه قضیه ۱.

مشاهده می‌شود که احتمال قطع در گره مقصد با افزایش تعداد آنتن‌های دریافتی (N_R) و افزایش توان ارسالی گره مبدأ و گره رله کاهش می‌یابد.

قضیه ۴ : در سیستم مشارکتی امن پیشنهادی با روش شکل‌دهی پرتوی RZF، احتمال قطع (تابع توزیع تجمعی SINR دریافتی) درگره استراق سمع‌کننده از رابطه زیر به‌دست می‌آید:

$$P_{out}^{E,RZF}=F_{\gamma_E^{RZF}}(x)=1-e^{\frac{-x}{a_2}}+e^{\frac{-x}{a_2}}a_3x\sum_{K=0}^{N_T-2}\frac{1}{\mathrm{K!}}a_2^K\left(a_2+a_3x\right)^{-K-1}\Gamma\left(K+1\right).$$

(۳۲)

اثبات: مشابه قضیه۲.

با بررسی رابطه فوق درمی‌یابیم که احتمال قطع در گره استراق سمع‌کننده با افزایش توان ارسالی گره مقصد و تعداد آنتن‌های ارسالی (N_T)، افزایش می‌یابد. بنابراین به کمک نتایج به‌دست آمده در قضیه‌های (۳) و (۴) و استفاده از رابطه (۲۲) نرخ محرمانه متوسط برای طرح RZF به‌دست می‌آید.

دقت کنید که اگر تعداد آنتن‌های ارسالی و دریافتی را به‌صورت زوج (N_T,N_R) نشان دهیم، با کمک رابطه (۲۲) و قضایای ۱، ۲، ۳ و ۴ به‌راحتی اثبات می‌شود که طرح‌های پرتودهی $RZF\left(N_T-1,N_R+1\right)$ و $TZF\left(N_T,N_R\right)$ دارای احتمال قطع یکسانی در گره استراق سمع‌کننده می‌باشند. در ضمن این طرح‌ها، احتمال قطع یکسانی در گره مقصد دارند.

درنتیجه طرح‌های پرتودهی *TZF* و *RZF* در حالات خاصی دارای نرخ محرمانه متوسط یکسان خواهند بود.

۳ ۲ ۳ -عملکرد طرح MRC/MRT

با جایگزینی $\mathbf{w}_r^{MRC}$ و $\mathbf{w}_t^{MRC}$ در (۲۱) نرخ محرمانه لحظه‌ای برای طرح MRC/MRT می‌تواند به فرم زیر به‌دست آید:

$$R_{SEC}^{MRC}=\log_2\left(1+\min\left(\frac{p_S\left|h_{SR}\right|^2}{d_{SR}^{\mu}\sigma_R^2},\frac{\frac{p_R}{d_{RD}^{\mu}}\left\|\mathbf{h}_{RD}\right\|^2}{\left|\mathbf{w}_r^{\dagger}\mathbf{H}_{DD}\mathbf{w}_t\right|^2p_d+\sigma_D^2}\right)\right)-\log_2\left(1+\frac{\frac{p_R}{d_{RE}^{\mu}}\left|h_{RE}\right|^2}{\frac{p_d}{d_{DE}^{\mu}}\left\|\mathbf{h}_{DE}\right\|^2+\sigma_E^2}\right).\qquad(۳۳)$$

برای محاسبه نرخ محرمانه متوسط برای طرح پرتودهی MRC/MRT بر اساس رابطه (۲۲) به $F_{\gamma_D^{MRC}}(x)$ و $F_{\gamma_E^{MRC}}(x)$ نیاز داریم. در قضیه (۵)، $F_{\gamma_D^{MRC}}(x)$ بیان می‌شود.

قضیه ۵ : در سیستم مشارکتی امن پیشنهادی با طرح MRC/MRT، احتمال قطع (تابع توزیع تجمعی SINR دریافتی) در گره مقصد از رابطه زیر به‌دست می‌آید:

$$P_S^{D,MRC}=F_{\gamma_D^{MRC}}(x)=1-e^{\frac{-x}{c_0}}\frac{\Gamma\left(\frac{k}{2},\frac{x}{2c_1}\right)}{\Gamma\left(\frac{k}{2}\right)}+\frac{e^{\frac{-x}{c_0}}e^{\frac{1}{c_2}}\Gamma\left(\frac{k}{2},\frac{x}{2c_1}+\frac{1}{c_2}\right)}{\left(1+\frac{2c_1}{c_2x}\right)^{\frac{k}{2}}\Gamma\left(\frac{k}{2}\right)}. \quad (۳۴)$$

که در آن $K=2N_R$ و c_0 ، c_1 و c_2 در ضمیمه ۳ تعریف شده‌اند.

اثبات: به ضمیمه ۳ مراجعه شود.

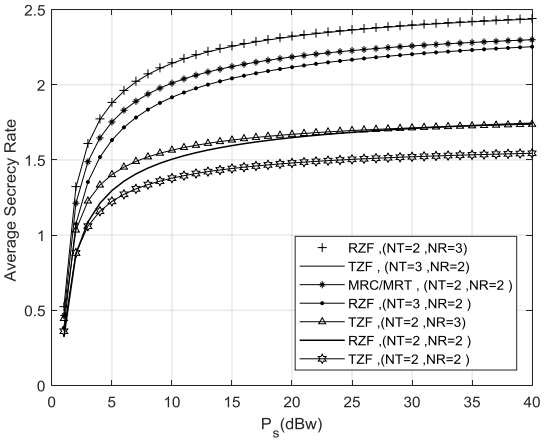
در سیستم مشارکتی امن پیشنهادی از آنجا که $\gamma_E^{RZF}=\gamma_E^{MRC}$ با کمک قضیه ۳، تابع توزیع تجمعی $F_{\gamma_E^{MRC}}(x)$ از رابطه زیر به‌دست می‌آید:

$$P_{out}^{E,MRC}=F_{\gamma_E^{MRC}}(x)=1-e^{\frac{-x}{a_0}}+e^{\frac{-x}{a_0}}a_1x\sum_{K=0}^{N_T-1}\frac{1}{K!}{a_0}^K\left(a_0+a_1x\right)^{-K-1}\Gamma(K+1). \quad (۳۵)$$

درنهایت با جایگذاری $F_{\gamma_D^{MRC}}(x)$ و $F_{\gamma_E^{MRC}}(x)$ که در رابطه (۳۴) و (۳۵) به‌دست آورده شد و با کمک رابطه (۲۲) نرخ محرمانه متوسط برای طرح MRC/MRT به‌دست می‌آید.

۴ -نتایج شبیه‌سازی

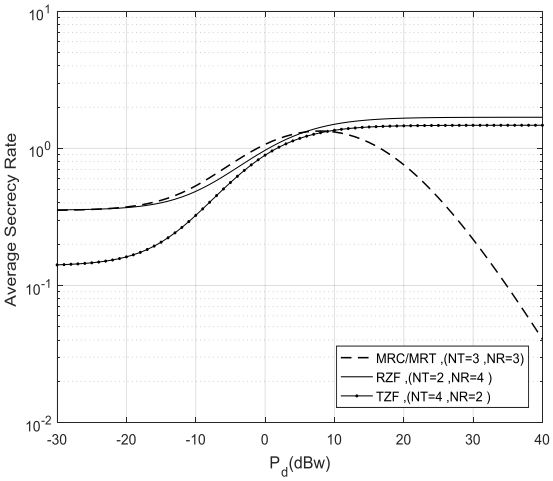
در این بخش عملکرد سیستم مشارکتی امن پیشنهادی ارزیابی می‌شود و صحت نتایج تئوری به‌دست آمده بررسی خواهد شد. در کلیه ساختارهای شبیه‌سازی مقدار واریانس نویز (σ_n^2)، برابر ۱ و مقدار واریانس کانال خودتداخلی (σ_{SI}^2) در گره مقصد کاملاً دوطرفه، برابر ۱/ قرار داده می‌شود.



شکل ۲: نرخ محرمانه متوسط برای طرح‌های پرتودهی TZF، RZF و MRC/MRT برحسب تغییرات توان ارسالی گره مبدأ یا گره رله

همچنین فاصله گره رله از گره مقصد و گره استراق سمع‌کننده برابر ۱ قرار داده می‌شود به‌طوری‌که $d_{SR}=d_{RD}=1$ و ضریب میرایی (μ) نیز برابر ۳ در نظرگرفته می‌شود. در شکل ۲ نرخ محرمانه متوسط برای طرح‌های پرتودهی TZF، RZF و MRC/MRT برحسب تغییرات توان ارسالی گره مبدأ و یا گره رله رسم شده است. (فرض شده است که $P_S^{out}=p_r=P_D^{D,MRC}=F_{\gamma_D^{MRC}}(x)$). همان‌طورکه در شکل ۲ مشخص است نرخ محرمانه متوسط با افزایش توان زیادتر شده است. با مقایسه طرح‌های پرتودهی TZF و RZF مشاهده می‌شود که $TZF(3,2)$ و $RZF(2,3)$ عملکردهای یکسانی دارند که مطابق با نتایجی است که در بخش قبلی به دست آمد. با بررسی شکل ۲ متوجه می‌شویم که در طرح TZF نرخ محرمانه متوسط با افزایش تعداد آنتن‌های ارسالی (N_T) به‌طور قابل توجهی افزایش می‌یابد. در طرح RZF نیز نرخ محرمانه متوسط با افزایش تعداد آنتن‌های دریافتی (N_R) افزایش می‌یابد.

در شکل ۳ نرخ محرمانه متوسط برای طرح‌های پرتودهی TZF، RZF و MRC/MRT برحسب تغییرات توان مقصد رسم شده است. همان‌طورکه در شکل ۳ مشخص است در طرح‌های RZF و TZF با افزایش توان مقصد قدرت سیگنال تداخل ارسالی بیشتر می‌شود و نرخ محرمانه متوسط افزایش می‌یابد، اما از یک جایی به بعد با زیاد شدن توان مقصد، تأثیر منفی سیگنال تداخل روی رله هم بیشتر می‌شود و عملکرد گام اول سیستم مشارکتی امن پیشنهادی یعنی لینک مبدأ-رله کاهش می‌یابد و درنهایت نرخ محرمانه متوسط نمی‌تواند از یک حدی بیشتر شود و اشباع می‌شود. همچنین با دقت در شکل ۳ متوجه می‌شویم که طرح MRC/MRT دارای یک نقطه ماکزیمم از نظر توان ارسالی مقصد است. در طرح MRC/MRT وقتی‌که توان ارسالی مقصد افزایش می‌یابد تا قبل از این‌که به نقطه ماکزیمم برسیم، زیاد شدن توان باعث افزایش سیگنال تداخل و کاهش SINR در گره استراق سمع‌کننده می‌شود، اما از آنجا که طرح MRC/MRT قابلیت حذف خودتداخلی را ندارد و با افزایش توان ارسالی مقصد، خودتداخلی زیاد می‌شود.



شکل ۳: نرخ محرمانه متوسط برای طرح‌های پرتودهی TZF، RZF و MRC/MRT برحسب تغییرات توان ارسالی گره مقصد

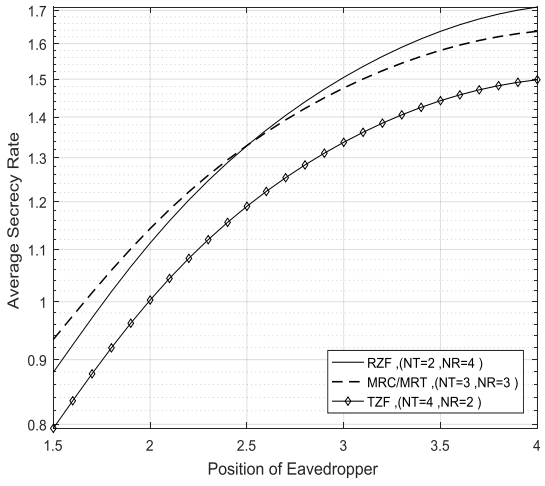
درنتیجه نسبت SINR دریافتی در گره مقصد کاهش می‌یابد. از طرف دیگر با افزایش توان ارسالی مقصد تأثیر سیگنال تداخل روی گره رله هم بیشتر می‌شود و SINR دریافتی در گام اول سیستم مشارکتی امن پیشنهادی یعنی لینک مبدأ-رله کاهش می‌یابد. بنابراین اثر منفی افزایش توان ارسالی بعد از نقطه ماکزیمم خیلی زیاد می‌شود و نرخ محرمانه متوسط کاهش می‌یابد.

با بررسی شکل ۳ مشاهده می‌شود که برای توان‌های ارسالی کمتر از توان بهینه، طرح MRC/MRT بهتر از طرح‌های TZF و RZF عمل می‌کند ولی بعد از نقطه توان ارسالی بهینه بازدهی طرح‌های TZF و RZF بهتر از MRC/MRT می‌شود.

در شکل ۴ نرخ محرمانه متوسط برحسب موقعیت گره استراق سمع‌کننده برای طرح‌های پرتودهی TZF، RZF و MRC/MRT رسم شده است.

با دقت در شکل ۴ متوجه می‌شویم که هرچه فاصله گره استراق سمع‌کننده از گره رله بیشتر شده و به مقصد نزدیک‌تر شود، نرخ محرمانه متوسط افزایش می‌یابد. دلیل این امر این است که با دورشدن گره استراق سمع‌کننده از گره رله، میزان سیگنال‌های اطلاعات کمتری از گره رله ره‌گیری و دریافت می‌شود. از طرف دیگر با نزدیک‌شدن گره استراق سمع‌کننده به گره مقصد، سیگنال‌های دریافتی در گره استراق سمع‌کننده دچار تضعیف بیشتری شده و بنابراین نرخ محرمانه متوسط با کاهش عملکرد گره استراق سمع‌کننده افزایش می‌یابد.

با بررسی شکل ۴ مشاهده می‌کنیم تا زمانی‌که فاصله گره استراق سمع‌کننده از گره رله کم باشد عملکرد طرح MRC/MRT از طرح RZF بهتر می‌باشد ولی با افزایش این فاصله، طرح RZF دارای عملکرد بهتری می‌باشد.



شکل ۴: نرخ محرمانه متوسط برای طرح‌های پرتودهی TZF، RZF و MRC/MRT برحسب موقعیت گره استراق سمع‌کننده

۵ -نتیجه‌گیری

در این مقاله امنیت لایه فیزیکی برای لینک گره مبدأ-گره مقصد در یک سیستم بی‌سیم مشارکتی امن که در آن گره مقصد حالت عملیاتی کاملاً دوطرفه را اتخاذ کرده و دارای چند آنتن ورودی و چند آنتن خروجی است، مطالعه شده است. در سیستم مورد نظر، گره مقصد به کمک یک گره رله بازگشایی و ارسال با گره مبدأ در حضور یک گره استراق سمع‌کننده ارتباط برقرار کرده و هم‌زمان با دریافت اطلاعات ارسالی از گره مبدأ، یک سیگنال تداخل به‌طرف گره استراق سمع کننده ارسال می‌کند که باعث تضعیف لینک گره رله-گره استراق سمع کننده می‌شود. طرح‌های پرتودهی مختلفی برای سیستم مورد نظر پیشنهاد داده شد و برای آن‌ها نرخ محرمانه لحظه‌ای و نرخ محرمانه متوسط محاسبه شد. نتایج کسب‌شده بیان‌گر این است که این طرح‌ها باعث حذف و یا کاهش قابل توجه حلقه خودتداخلی در گره مقصد می شوند. نشان داده شد که با افزایش توان ارسالی گره مبدأ یا گره رله، نرخ محرمانه متوسط برای طرح‌های پرتودهی مختلف افزایش می‌یابد درحالی‌که با افزایش توان گره مقصد، برای طرح‌های پرتودهی TZF و RZF نرخ محرمانه متوسط ابتدا افزایش یافته و سپس اشباع می‌شود ولی برای طرح پرتودهی MRC/MRT نرخ محرمانه متوسط با افزایش توان گره مقصد ابتدا افزایش یافته و به یک نقطه ماکزیمم رسیده و سپس کاهش می‌یابد. با مقایسه طرح‌های پرتودهی TZF و RZF دیده شد که $TZF\left(N_T,N_R\right)$ و $RZF\left(\mathrm{N}_T-1,N_R+1\right)$ عملکردهای یکسانی دارند که مطابق با نتایجی است که به‌دست آورده شد. درنهایت با بررسی شکل ۴ مشاهده می‌شود تا زمانی‌که فاصله گره استراق سمع‌کننده از گره رله کم باشد، عملکرد طرح MRC/MRT از طرح RZF بهتر می‌باشد ولی با افزایش این فاصله، طرح RZF دارای عملکرد بهتری می‌باشد.

ضمیمه ۱- اثبات قضیه ۱

$$F_{\gamma_D^{TZF}}(x)=\mathrm{p}\left(\gamma_D^{TZF}<x\right), \tag{۳۶}$$

$$F_{\gamma_D^{TZF}}(x)=\mathrm{p}\left(\min\left(\frac{p_S\left|h_{SR}\right|^2}{d_{SR}^{\mu}\sigma_R^2},\frac{p_R\left\|h_{RD}\right\|^2}{d_{RD}^{\mu}\sigma_D^2}\right)<x\right). \tag{۳۷}$$

با تعریف پارامترهای $a_0=\frac{p_S}{d_{SR}^{\mu}\sigma_R^2}$، $Z_1=\left|h_{SR}\right|^2$ و $Y_1=\left\|\mathbf{h}_{RD}\right\|^2$ تابع توزیع تجمعی $F_{\gamma_D^{TZF}}(x)$ به‌صورت زیر محاسبه $a_1=\frac{p_R}{d_{RD}^{\mu}\sigma_D^2}$ می‌شود:

$$\begin{aligned}F_{\gamma_D^{TZF}}(x)&=P\left(\min\left(a_0Z_1\,,\,\mathrm{a}_1Y_1\right)<x\right)\\&=1-p\left(a_0Z_1>x\right)p\left(a_1Y_1>x\right),\end{aligned} \tag{۳۸}$$

$$\begin{aligned}F_{\gamma_D^{TZF}}(x)&=1-\left(1-p\left(Z_1<\frac{x}{a_0}\right)\right)\left(1-\mathrm{p}\left(\mathrm{Y}_1<\frac{x}{a_1}\right)\right)\\&=1-\left(1-F_{\mathrm{Z}_1}\left(\frac{x}{a_0}\right)\right)\left(1-F_{\mathrm{Y}_1}\left(\frac{x}{a_1}\right)\right),\end{aligned} \tag{۳۹}$$

که در رابطه فوق Z_1 دارای توزیع نمایی و Y_1 دارای توزیع Chi-squares با درجه آزادی N_R ۲ می‌باشد. درنهایت با جایگذاری $F_{\mathrm{Z}_1}\left(\frac{x}{a_0}\right)=1-e^{\frac{-x}{a_0}}$ و $F_{\mathrm{Y}_1}\left(\frac{x}{a_1}\right)=\frac{\gamma\left(\frac{K}{2},\frac{x}{2a_1}\right)}{\Gamma\left(\frac{K}{2}\right)}$ در رابطه فوق، $F_{\gamma_D^{TZF}}(x)$ بیان شده در رابطه (۲۶) به‌دست می‌آید.

ضمیمه ۲ – اثبات قضیه ۲

$$F_{\gamma_E^{TZF}}(x)=\mathrm{p}\left(\gamma_E^{TZF}<x\right), \tag{۴۰}$$

$$F_{\gamma_E^{TZF}}(x)=\mathrm{p}\left(\frac{\frac{p_R\alpha_{RE}}{\sigma_E^2}\left|h_{RE}\right|^2}{\frac{p_d\alpha_{DE}}{\sigma_E^2}\left|\mathbf{h}_{DE}\mathbf{w}_t^{ZF}\right|^2+1}<x\right), \tag{۴۱}$$

برای راحتی در نوشتن پارامترهای $a_2=\frac{p_R\alpha_{RE}}{\sigma_E^2}$، $a_3=\frac{p_d\alpha_{DE}}{\sigma_E^2}$، $Z_2=\left|h_{RE}\right|^2$ و $Y_2=\left|\mathbf{h}_{DE}\mathbf{w}_t^{ZF}\right|^2$ را تعریف کرده و بر این اساس $F_{\gamma_E^{TZF}}(x)$ می‌تواند به‌صورت زیر محاسبه شود:

$$\begin{aligned}F_{\gamma_E^{TZF}}(x)&=p\left(\frac{a_2Z_2}{a_3Y_2+1}<x\right)\\&=1-p\left(Y_2<\frac{a_2Z_2-x}{a_3x}\right),\end{aligned} \tag{۴۲}$$

$$F_{\gamma_E^{TZF}}(x)=1-\int_0^{\infty}F_{Y_2}\left(\frac{a_2Z_2-x}{a_3x}\right)f_{Z_2}(z_2)dz_2, \tag{۴۳}$$

که در رابطه (۴۲)، Z_2 و Y_2 به‌ترتیب دارای توزیع نمایی و Chi-squares با درجه آزادی (N_T-1) ۲ می‌باشد به‌طوری‌که با جایگذاری $f_{Z_2}(\mathrm{z})=\frac{1}{\sigma_R^2}e^{\frac{-z_2}{\sigma_R^2}}$ و $F_Y\left(\frac{a_2Z_2-x}{a_3x}\right)=1-e^{-\frac{a_2Z_2-x}{a_3x\sigma_E^2}}\sum_{K=0}^{N_T-2}\frac{1}{\mathrm{K}!}\left(\frac{a_2Z_2-x}{a_3x\sigma_E^2}\right)^K$ در رابطه (۴۳)، $F_{\gamma_E^{TZF}}(x)$ به‌صورت زیر محاسبه می‌شود:

$$F_{\gamma_E^{TZF}}(x)=1-\int_{\frac{x}{a_2}}^{\infty}\left(1-e^{-\frac{a_2z_2-x}{a_3x\sigma_E^2}}\sum_{k=0}^{N_T-2}\frac{1}{k!}\left(\frac{a_2Z_2-x}{a_3x\sigma_E^2}\right)^K\right)\frac{1}{\sigma_R^2}e^{\frac{-z_2}{\sigma_R^2}}dz_2. \tag{۴۴}$$

با تعریف پارامترهای $a_4=\frac{a_2}{a_3x\sigma_E^2}$، $a_5=\left(\frac{a_2}{a_3x\sigma_E^2}+\frac{1}{\sigma_R^2}\right)$، $a_6=\frac{1}{a_3\sigma_E^2}$ و $a_7=\frac{x}{a_2}$ تابع توزیع تجمعی $F_{\gamma_E^{TZF}}(x)$ به‌صورت زیر به‌دست آورده می‌شود:

$$F_{\gamma_E^{TZF}}(x)=1-e^{\frac{-x}{\sigma_R^2a_2}}+\sum_{k=0}^{N_T-2}\frac{1}{\mathrm{k}!}\frac{1}{\sigma_R^2}e^{\frac{1}{a_3\sigma_E^2}}\int_{\frac{x}{a_2}}^{\infty}e^{-z_2a_5}\left(a_4z_2-a_6\right)^kdz_2, \tag{۴۵}$$

$$\begin{aligned}F_{\gamma_E^{TZF}}(x)&=1-e^{\frac{-x}{\sigma_R^2a_2}}+\sum_{k=0}^{N_T-2}\frac{1}{\mathrm{k}!}\frac{1}{\sigma_R^2}e^{\frac{1}{a_3\sigma_E^2}}a_4{}^K\int_{\frac{x}{a_2}}^{\infty}e^{-z_2a_5}\left(z_2-\frac{a_6}{a_4}\right)^kdz_2\\&=1-e^{\frac{-x}{\sigma_R^2a_2}}+\sum_{k=0}^{N_T-2}\frac{1}{\mathrm{k}!}\frac{1}{\sigma_R^2}e^{\frac{1}{a_3\sigma_E^2}}a_4{}^K\int_{\frac{x}{a_2}}^{\infty}e^{-z_2a_5}\left(z_2-a_7\right)^kdz_2.\end{aligned} \tag{۴۶}$$

اکنون با کمک معادله ۳,۳۸۲ در[۲۷]، تابع توزیع تجمعی $F_{\gamma_E^{TZF}}(x)$ بیان شده در رابطه **(۲۷)** به‌دست می‌آید.

ضمیمه ۳- اثبات قضیه ۵

با کمک y_D^{MRC} در رابطه (۱۳)، تابع توزیع تجمعی به‌فرم زیر نوشته می‌شود:

$$F_{\gamma_D^{MRC}}(x)=\mathrm{p}\left(\min\left(\frac{p_S\left|h_{SR}\right|^2}{d_{SR}^{\mu}\sigma_R^2},\frac{\frac{p_R}{d_{RD}^{\mu}\sigma_D^2}\left\|\mathbf{h}_{RD}\right\|^2}{\frac{p_d\left|\mathbf{w}_r^{\dagger}\mathbf{H}_{DD}\mathbf{w}_t\right|^2}{\sigma_D^2}+1}\right)<x\right). \tag{۴۷}$$

با تعریف پارامترهای $c_0=\frac{p_S}{d_{SR}^{\mu}\sigma_R^2}$ ، $Z_3=|h_{SR}|^2$ ، $Y_3=\|\mathbf{h}_{RD}\|^2$ ، $c_1=\frac{p_R}{d_{RD}^{\mu}\sigma_D^2}$ ، $S=\left|\mathbf{w}_r^{\dagger}\mathbf{H}_{DD}\mathbf{w}_t\right|^2$ و $c_2=\frac{p_d}{\sigma_D^2}$ تابع توزیع تجمعی $F_{\gamma_D^{MRC}}(x)$ به‌صورت زیر محاسبه می‌شود:

$$F_{\gamma_D^{MRC}}(x)=P\left(\min\left(c_0Z_3,\frac{c_1Y_3}{c_2S+1}\right)<x\right), \qquad (۴۸)$$

$$F_{\gamma_D^{MRC}}(x)=1-\left(1-F_{Z_3}\left(\frac{x}{c_0}\right)\right)\left(F_S\left(\frac{c_1Y_3-x}{c_2x}\right)\right). \qquad (۴۹)$$

که در رابطه فوق Z_3 و S دارای توزیع نمایی و Y_3 دارای توزیع Chi-squares با درجه آزادی $2N_R$ می‌باشد. درنهایت با جایگذاری $F_S\left(\frac{c_1Y_3-x}{c_2x}\right)=\int_0^{\infty}\left(1-e^{\frac{-(c_1Y_3-x)}{c_2x}}\right)f_{Y_3}(y_3)dy_3$ و $F_{Z_3}(\frac{x}{c_0})=1-\frac{1}{\sigma_R^2}e^{\frac{-x}{c_0\sigma_R^2}}$ در رابطه فوق، $F_{\gamma_D^{MRC}}(x)$ به‌صورت زیر به‌دست آورده می‌شود:

$$\begin{aligned}F_{\gamma_D^{MRC}}(x)=1-e^{\frac{-x}{c_0}}\int_{\frac{x}{c_1}}^{\infty}\frac{y_3^{\frac{k}{2}-1}e^{\frac{-y_3}{2}}}{2^{\frac{k}{2}}\Gamma\left(\frac{k}{2}\right)}dy_3\\ +e^{\frac{-x}{c_0}}e^{\frac{1}{c_2}}\int_{\frac{x}{c_1}}^{\infty}\frac{y_3^{\frac{k}{2}-1}e^{-y_3\left(\frac{1}{2}+\frac{c_1}{c_2x}\right)}}{2^{\frac{k}{2}}\Gamma\left(\frac{k}{2}\right)}dy_3,\end{aligned} \qquad (۵۰)$$

اکنون با کمک معادله ۳،۳۸۱ در[۲۷]، تابع توزیع تجمعی $F_{\gamma_D^{MRC}}(x)$ بیان شده در رابطه **(۳۴)** به‌دست می‌آید.

مراجع

[1] H. Deng, H. M. Wang, W. Guo and W. Wang, "Secrecy transmission with a helper: To relay or to jam," IEEE Trans. Inf. Forensics Security, vol. 10, no. 2, pp. 293–307, Feb. 2015.

[2] R. Zhang, L. Song, Z. Han and B. Jiao, "Physical layer security for two-way untrusted relaying with friendly jammers," IEEE Trans. Veh. Technol., vol. 61, no. 8, pp. 3693–3704, Oct. 2012.

[3] C. Jeong, I-M. Kim and D. Kim, "Joint secure beamforming design at the source and the relay for an amplify-and-forward MIMO untrusted relay system," IEEE Trans. Signal Process., vol. 60, no. 1, pp. 310-325, Jan. 2012.

[4] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," IEEE Trans. Signal Process., vol. 39, no. 10, pp. 4871-4884, Oct. 2011.

[۵] مرضیه نظام‌آبادی، ابوالفضل فلاحتی، همسوسازی تداخل فرصت‌طلب در شبکه‌های رادیو شناختگر با ارسال کد فضا-زمان کاربران ثانویه، مجله مهندسی برق دانشگاه تبریز، دوره ۴۶، شماره ۲- شماره پیاپی ۷۶، تابستان ۱۳۹۵، صفحه ۳۴۱-۳۳۳ .

[6] X. Wang, K. Wang and X. Zhang, "Secure relay beamforming with imperfect channel state information," IEEE Trans. Veh. Technol., vol. 62, no. 5, pp. 2140-2155, June 2013.

[7] H-M. Wang, M. Luo, X-G. Xia and Q. Yin, "Joint cooperative beamforming and jamming to secure AF relay systems with individual power constraint and no eavesdropper's CSI," IEEE Signal Proces. Lett., vol.۲۰ , no. 1, pp. 39-42, Jan. 2013.

[8] L. Dong, Z. Han, A. P. Petropulu and H. V. Poor, "Improving wireless physical layer security via cooperating relays," IEEE Trans. Sig. Proc., vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[9] G. Zheng, Li-Chia Choo, and K. K. Wong, "Optimal Cooperative Jamming To Enhance Physical Layer Security Using Relays," IEEE Trans. on Sig. Proc., vol. 59, no. 3, pp. 1317 - 1322, Mar. 2011.

[10] I. Krikidis, J. S. Thompson and S. McLaughlin, "Relay selection for secure cooperative networks with jamming," IEEE Trans. Wireless Commun., vol. 8, pp. 5003–5011, Oct. 2009.

[11] J. Vilela, M. Bloch, J. Barros and S. W. McLaughlin, "Wireless secrecy regions with friendly jamming," IEEE Trans. Inf. Forens. Sec., vol. 6, pp. 256–266, June 2011.

[12] S. Gerbracht, C. Scheunert and E. A. Jorswieck, "Secrecy Outage in MISO Systems With Partial Channel Information," IEEE Trans. Inf. Forens. Sec., vol. 7, no. 2, pp. 704-716, Apr. 2012.

[13] S. Luo, J. Li and A. Petropulu, "Outage Constrained Secrecy Rate Maximization Using Cooperative Jamming," in Proc.۲۰۱۲ IEEE Statistical Signal Processing Workshop (SSP2012), Ann Arbor, MI, Aug. 2012.

[14] Z. Ding, M. Peng and H. -H. Chen, "A general relaying transmission protocol for MIMO secrecy communications," IEEE Trans. Commun., vol. 60, pp. 3461–3471, Nov. 2012.

[15] J. Vilela, M. Bloch, J. Barros and S. W. McLaughlin, "Wireless secrecy regions with friendly jamming," IEEE Trans. Inf. Forens. Sec., vol. 6, pp. 256–266, June 2011.

[16] S. Gerbracht, C. Scheunert and E. A. Jorswieck, "Secrecy Outage in MISO Systems With Partial Channel Information," IEEE Trans. Inf. Forens. Sec., vol. 7, no. 2, pp. 704-716, Apr. 2012.

[17] S. Luo, J. Li and A. Petropulu, "Outage Constrained Secrecy Rate Maximization Using Cooperative Jamming," in Proc.۲۰۱۲ IEEE Statistical Signal Processing Workshop (SSP2012), Ann Arbor, MI, Aug. 2012.

[18] Jing Huang and A. Lee Swindlehurst, "Cooperative Jamming for Secure Communications in MIMO Relay Networks," IEEE Trans. Sig. Proc., vol. 59, no. 10, Oct. 2011.

[19] Yupeng Liu, Jiangyuan Li and A. P. Petropulu, "Destination assisted cooperative jamming for wireless physical-layer security," IEEE Trans. Inform. Forensics Security, vol. 8, no. 4, pp. 682–694, Apr. 2013.

[20] S. Gollakota and D. Katabi, "Physical layer wireless security made fast and channel independent," in Proc. IEEE Int. Conf. Comp. Commun., Shanghai, China, April 2011, pp. 1125–1133.

[21] T. Riihonen, S. Werner and R. Wichman, "Hybrid full-duplex/half-duplex relaying with transmit power adaptation," IEEE Trans. Wireless Commun., vol. 10, no. 9, pp. 3074-3085, Sept. 2011.

[22] A. Mukherjee and A. L. Swindlehurst, "A full-duplex active eavesdropper in MIMO wiretap channels: Construction and countermeasures," in Proc. Asilomar Conf. Sign. Systems Comp., Pacific Grove, CA, Nov. 2011, pp. 265-269.

[23] W. Li, M. Ghogho, B. Chen and C. Xiong, "Secure Communication via Sending Artificial Noise by the Receiver: Outage Secrecy Capacity/Region Analysis," IEEE Commun. Lett., vol. 16, no. 10, pp. 1628-1631, Oct. 2012.

[۲۴] محمدعلی محمدی، زهرا مبینی، نرخ قابل حصول ارسال هم‌زمان اطلاعات و توان برای سیستم مخابرات دوطرفه مجهز به آرایه آنتن عظیم، مجله مهندسی برق دانشگاه تبریز، پذیرفته شده، ۱۳۹۶.

[25] M. Mohammadi, B. K. Chalise, H. A. Suraweera, C. Zhong, G. Zheng and I. Krikidis, "Throughput analysis and optimization of wireless-powered multiple antenna full-duplex relay systems," IEEE Trans. Commun., vol. 64, no. 4, pp. 1769–1785, Apr 2016.

[26] M. Bloch, J. Barros, M. Rodrigues and S. McLaughlin, Wireless information-theoretic security, IEEE Transactions on Information Theory, 2008, 54(6): 2515–2534.

[27] I. S. Gradshteyn and I.M. Ryzhik, Table of Integrals, Series and Products,۷ th ed. New York, NY, USA: Academic, 2007.

زیرنویس‌ها

۱ Full-duplex
۲ Eavesdropper
۳ Decode and forward
٤ Amplify and forward
٥ Diversity
٦ Beamforming
۷ half-duplex
۸ Self-interference
۹ Degree of Freedom
۱۰ Transmit zero forcing
۱۱ Receive zero forcing
۱۲ Maximal ratio combining/ Maximal ratio transmission
۱۳ Probability density function
۱٤ Cumulative distribution function
۱٥ Gamma function
۱٦ Rayleigh Fading