ارزیابی عملکرد محرمانگی شبکه رله‌ای بافردار رادیوشناختی در کانال‌های محوشدگی رایلی

محسن ناصری[۱] **محمد جواد صابر**[۲] **سید محمد سجاد صدوق**[۳] **محمد ترابی**[۴]

۱- دانشجوی کارشناسی ارشد- دانشکده مهندسی برق- دانشگاه شهید بهشتی- تهران- ایران
m_naseri@sbu.ac.ir

۲- دانشجوی دکتری - دانشکده مهندسی برق – دانشگاه شهید بهشتی – تهران- ایران
* s_saber@sbu.ac.ir

۳- دانشیار- دانشکده مهندسی برق- دانشگاه شهید بهشتی- تهران- ایران
s_sadough@sbu.ac.ir

۴- استادیار- دانشکده مهندسی برق- دانشگاه شهید بهشتی- تهران- ایران
m_torabi@sbu.ac.ir

چکیده: در این مقاله، امنیت لایه فیزیکی در شبکه رله‌ای بافردار رادیوشناختی که از روش لایه زیرین طیف استفاده می‌کند، بر روی کانال‌هایی با محوشوندگی رایلی موردبررسی و ارزیابی قرار می‌گیرد. در این شبکه رادیوشناختی، ارسال اطلاعات از فرستنده به گیرنده، از طریق رله مجهز به بافر و در حضور شنودگر غیرفعال- با قابلیت شنود اطلاعات- صورت می‌گیرد. برای ارزیابی میزان امنیت اطلاعات تبادلی، احتمال قطع محرمانگی به‌عنوان معیاری مهم برای ارزیابی عملکرد محرمانگی شبکه در لایه فیزیکی در نظر گرفته‌شده و رابطه ریاضی احتمال قطع محرمانگی به‌صورت فرم بسته به دست می‌آید. نتایج عددی حاصل از رابطه ریاضی احتمال قطع محرمانگی با روش مونت-کارلو برای ارزیابی امنیت لایه فیزیکی سیستم موردنظر به ازای پارامترهای مختلف آورده می‌شود. همچنین تأثیر وجود بافر نیز در این سیستم، ارزیابی می‌گردد. با بررسی نتایج، ملاحظه می‌شود که صرف‌نظر از تأخیر به وجود آمده توسط بافر، وجود بافر در رله و افزایش طول آن از $L=2$ به $L=20$ موجب کاهش احتمال قطع محرمانگی سیستم از 10^{-2} به 10^{-3} می‌شود. این کاهش بیانگر بهبود ۱۰ برابری احتمال قطع محرمانگی است. همچنین نشان داده شده است که برای احتمال قطع 10^{-3} ، رله بافردار حدود $3\ \mathrm{dB}$ نسبت به بدون بافر عملکرد بهتری از لحاظ نسبت سیگنال به نویز دارد.

واژه‌های کلیدی: شبکه رادیوشناختی، امنیت لایه فیزیکی، شبکه‌های رله‌ای، بافر، احتمال قطع محرمانگی، محو شوندگی رایلی

* در حال حاضر، استادیار دانشکده مهندسی برق در دانشگاه خلیج فارس، بوشهر.

تاریخ ارسال مقاله: ۱۳۹۷/۰۵/۲۰
تاریخ پذیرش مشروط مقاله: ۱۳۹۷/۰۷/۱۹
تاریخ پذیرش مقاله: ۱۳۹۸/۰۴/۰۷
نام نویسنده‌ی مسئول: دکتر سید محمد سجاد صدوق، دانشیار
نشانی نویسنده‌ی مسئول: ایران، تهران، دانشگاه شهید بهشتی، دانشکدهٔ مهندسی برق، گروه مخابرات

[DOR: 20.1001.1.26765810.1398.16.4.19.0]
Journal of Iranian Association of Electrical and Electronics Engineers - Vol.16- No.4- Winter2018

۱- مقدمه

۱-۱- توضیحات اولیه

در سال‌های اخیر شبکه‌های بی‌سیم به دلیل قابلیت جابه‌جایی بسیار بالا نسبت به شبکه‌های سیمی رشد چشمگیر و قابل‌توجهی داشته‌اند. با استفاده از فناوری بی‌سیم کاربران می‌توانند بدون محدودیت مکانی، به اطلاعات موجود در شبکه دسترسی داشته باشند. با پیشرفت سریع مخابرات بی‌سیم، استفاده از دستگاه‌های تلفن همراه، گسترش زیادی پیداکرده و راه‌های ارتباطی افزایش چشمگیری یافته است [۱]. به‌منظور کاهش ترافیک ناشی از ازدیاد کاربران، روش‌هایی برای افزایش ظرفیت شبکه‌های بی‌سیم از قبیل گسترش پوشش‌دهی شبکه با استفاده از رله‌ها و فمتوسل‌ها، افزایش بعد فضا با استفاده از فناوری چند ورودی-چند خروجی بسیار بزرگ، بهبود بازدهی پهنای باند و بازدهی انرژی با استفاده از فناوری رادیوشناختی و مخابرات سبز پیشنهادشده است [۱، ۲]. کاربران در شبکه رادیوشناختی[۱] به دو نوع کاربران اولیه (کاربران مجوز دار)[۲] و کاربران ثانویه[۳] (کاربران بدون مجوز) تقسیم می‌شوند. کاربران شبکه ثانویه در سه روش: لایه زیرین[۴]، لایه رویی[۵] و ترکیبی[۶] طیف کاربران اولیه را به اشتراک گرفته و استفاده می‌کنند تا بتوانند پیام‌های خود را بدون تداخل با کاربران موجود در شبکه، ارسال نمایند [۳]. شبکه اولیه در زمان‌هایی از پهنای باند استفاده نمی‌کند. با استفاده از روش لایه زیرین، شبکه ثانویه تنها در این زمان‌ها، قادر به استفاده از طیف است؛ بنابراین شرط عدم تداخل فرستنده ثانویه با شبکه اولیه در حالت استفاده لایه زیرین از طیف اهمیت زیادی دارد. در این مدل، محدودیت توان باید بر توان ارسالی توسط فرستنده ثانویه اعمال شود به‌گونه‌ای که حداکثر توان تداخلی با شبکه اولیه نیز لحاظ گردد. تحقیقات گسترده‌ای پیرامون شبکه‌های رادیوشناختی به هنگام دسترسی به طیف در صورت ازدیاد کاربران صورت گرفته است [۳]. از طرفی به‌منظور کاهش فاصله کاربران و افزایش کیفیت سرویس‌دهی به آن‌ها [۲]، شبکه‌های رله‌ای[۷] با شبکه رادیوشناختی ادغام‌شده و شبکه رادیوشناختی رله‌ای[۸] را در حالت استفاده زیرین از طیف تشکیل داده‌اند که این شبکه از مزایای هر دو شبکه رادیوشناختی و شبکه مشارکتی بهره می‌برد [۷].

از طرفی، در سال‌های اخیر به دلیل ظهور و گسترش برنامه‌های مخرب که بیش‌تر دستگاه‌های موبایل را هدف قرار داده‌اند، فعالیت‌های سایبری در سیستم‌های ارتباطی بی‌سیم در حال افزایش است. ازاین‌رو تحقیقات گسترده‌ای در حوزه امنیت شبکه‌های بی‌سیم در برابر حملات مخرب صورت گرفته است [۴، ۵]. با توجه به این نکته که امواج رادیویی در محیط پخش[۹] می‌شوند، هر گیرنده‌ای که در ناحیه پوشش فرستنده رادیویی باشد، توانایی شنود ارتباطات بی‌سیم را دارد. انتشار رادیویی امواج در محیط موجب می‌شود که شبکه‌های ارتباطی بی‌سیم در قبال حملات ناخواسته به‌شدت آسیب‌پذیر شوند. نفوذگران می‌توانند با شکستن موانع امنیتی نه‌چندان قوی این شبکه‌ها، خود را به‌عنوان عضوی از اعضای شبکه قرار داده و به اطلاعات مبادله شده در شبکه دسترسی داشته باشند. همچنین می‌توانند در ارتباطات اعضای شبکه با یکدیگر اختلال ایجاد کرده یا از پهنای باند شبکه سوءاستفاده نمایند که تحت عناوین شنودگرهای فعال و غیرفعال[۱۰] شناخته می‌شوند[۴، ۵]. ازاین‌رو امنیت در شبکه‌های بی‌سیم با توجه به فراگیر شدن آن در عرصه‌های مختلف، اهمیت به سزایی دارد.

در رله‌های نیمه دوطرفه[۱۱] که بیشتر در سیستم‌های رله‌ای مرسوم مورداستفاده قرار می‌گیرد، رله مطابق با برنامه زمانی از پیش تعیین‌شده‌ای اقدام به ارسال و دریافت اطلاعات می‌کند؛ به‌طوری‌که این برنامه مستقل از کانال‌های ارسالی و دریافتی است [۶، ۸]. برنامه زمان‌بندی‌شده عملکرد سیستم‌های بی‌سیم را به‌شدت تضعیف می‌کند. باگذشت زمان، کیفیت کانال‌های ارسالی و دریافتی تغییرات زیادی می‌کنند. ازاین‌رو برنامه زمان‌بندی از پیش تعیین‌شده[۱۲]، می‌تواند مانع از استفاده کردن رله‌ها از بهترین کانال موجود برای ارسال و دریافت شود. درنتیجه به دلیل استفاده از برنامه زمانی مشخص، به‌خصوص در شبکه‌های چند رله‌ای، رله نمی‌تواند از بهترین کانال برای ارسال و دریافت بهره ببرد که منجر به محدودیت عملکرد سیستم می‌شود.

۱-۲- کارهای پیشین و نوآوری

اخیراً به‌کارگیری بافر[۱۳] در رله توجه زیادی را به خود جلب کرده است. این کار موجب اضافه شدن درجه آزادی در رله می‌شود که درنتیجه آن مشکل انتخاب بهترین کانال رفع می‌گردد [۹، ۱۰]. در مقایسه با پروتکل‌های رله‌ای متداول، پروتکل‌هایی که از بافر در رله استفاده می‌کنند، بهره گذردهی[۱۴]، چندگانگی[۱۵] و نسبت سیگنال به نویز[۱۶] قابل‌توجهی دارند. در حالت استفاده از رله بافردار، رله به برنامه زمانی از پیش تعین شده برای ارسال و دریافت در بازه‌های زمانی مختلف نیاز ندارد. هرچند استفاده از بافر در رله عملکرد سیستم را بهبود می‌بخشد و برای طراحی سیستم درجه آزادی جدیدی معرفی می‌نماید، اما باز هم چالش‌های عملی مربوط به خود را دارد. به‌عنوان‌مثال، ذخیره‌سازی داده‌ها در بافر رله، باعث به وجود آمدن تأخیر در سیستم می‌شود که این میزان تأخیر برای کاربردهای حساس به تأخیر ازجمله صدا، باید به‌خوبی مدیریت گردد [۱۰]. علاوه بر استفاده از بافر برای بهبود عملکرد سیستم، روش‌های مختلفی ازجمله شکل‌دهی پرتو[۱۷] [۲۲]، کدگذاری کانال [۲۳]، چندگانگی فضایی با استفاده از فناوری چندورودی-چندخروجی[۱۸] [۲۴] نیز وجود دارد. هرکدام از روش‌های فوق مزایا و معایبی دارند که تحلیل هر یک از آن‌ها در قالب این مقاله قرار نمی‌گیرد.

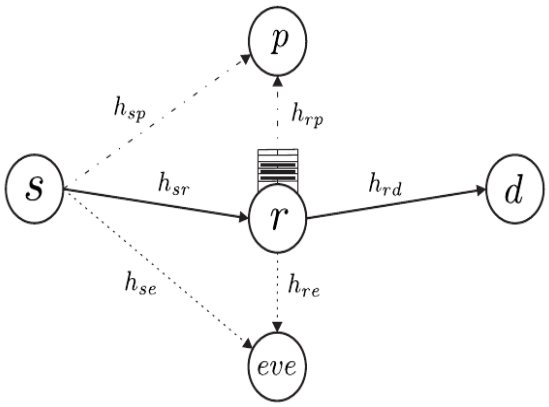
[DOR: 20.1001.1.26765810.1398.16.4.19.0]

در مطالعات اخیر، به دلیل مزایای شبکه‌های رله‌ای، امنیت شبکه‌های مشارکتی رله‌ای با ادغام مفهوم رادیوشناختی موردتوجه قرارگرفته است [۱۱]. امنیت لایه فیزیکی در شبکه‌های رادیوشناختی به دلیل مکانیزم‌های دسترسی به طیف، پیچیده‌تر از شبکه‌های بی‌سیم مرسوم است [۱۲، ۱۳]. در مرجع [۱۴] امنیت لایه فیزیکی در شبکه‌های مشارکتی غیر رادیوشناختی برای پروتکل‌های رله‌ای رایج موردبحث و بررسی قرارگرفته است. در مرجع [۱۰] نشان داده‌شده است که رله بافردار نسبت به رله معمولی در قبال تحمیل تأخیر به سیستم، عملکرد مناسب‌تر و قابل‌توجهی دارد. در [۱۱، ۱۵] شبکه رله‌ای رادیوشناختی در حالت بدون بافر و بافردار به لحاظ امنیتی موردبررسی قرارگرفته است. در مرجع [۱۱] محرمانگی شبکه رله‌ای رادیوشناختی موردبررسی قرارگرفته و تأثیر بافر و استفاده از آن منظور نگردیده است. در مرجع [۱۵] ضمن در نظر گرفتن قید محرمانگی و رله بافردار در شبکه رادیوشناختی، بر اساس عدم‌تغییر حالت بافر موجود در رله، احتمال قطع لینک پرش اول محاسبه‌شده است. در مرجع [۱۶] نیز تنها به بررسی شبکه رله‌ای بافردار پرداخته‌شده است درحالی‌که قید محرمانگی و امنیت در آن مورد بحث نبوده است.

با توجه به اهمیت امنیت و محرمانگی در شبکه‌های بی‌سیم، در این مقاله به بررسی محرمانگی شبکه رله‌ای بافردار رادیوشناختی در حالتی که کانال‌های ارتباطی توزیع رایلی[۱۹] دارند، پرداخته می‌شود. همچنین در این مقاله، در یک شبکه رادیوشناختی، ضمن در نظر گرفتن بافر در رله، عملکرد محرمانگی سیستم در حضور شنودگر غیرفعال به شیوه دقیق مورد ارزیابی قرارگرفته است؛ در این مقاله با فرض متقارن بودن سیستم، احتمال قطع لینک در پرش اول که مبنای محاسبه احتمال قطع محرمانگی کل سیستم است، بر اساس تغییرات سیگنال به نویز کانال‌ها و ظرفیت آن‌ها که شامل در نظر گرفتن حداقل قید محرمانگی موردنیاز برای برقراری لینک می‌شود، به دست آورده شده است.

۱-۳- بخش‌بندی مقاله

در ادامه و در بخش دوم، سیستم مدل پیشنهادی همراه با فرض‌های درنظرگرفته شده ارائه می‌شود. همان‌طور که در این بخش توضیح داده می‌شود، از بافر رله به‌منظور ایجاد درجه آزادی برای تصمیم‌گیری در شرایط مختلف استفاده می‌شود. با در نظر گرفتن توزیع کانال‌ها به‌صورت رایلی، نسبت سیگنال به نویز برای کانال‌های مختلف سیستم محاسبه می‌گردد. در بخش سوم، به‌منظور ارزیابی عملکرد محرمانگی سیستم در شبکه رله‌ای بافردار رادیوشناختی و ارزیابی میزان امنیت اطلاعات تبادلی، احتمال قطع محرمانگی به‌عنوان معیاری مهم برای ارزیابی عملکرد محرمانگی شبکه در لایه فیزیکی در نظر گرفته‌شده و رابطه ریاضی احتمال قطع محرمانگی با در نظر گرفتن وضعیت‌های مختلف بافر، به‌صورت فرم بسته به دست



شکل (۱): مدل سیستم شبکه رله‌ای بافردار رادیوشناختی

می‌آید. در بخش چهارم و نتایج، عملکرد محرمانگی سیستم مدل ارائه‌شده نسبت به پارامترهای مختلف و تأثیر آن‌ها بر احتمال قطع محرمانگی سنجیده می‌شود. همچنین نتایج شبیه‌سازی‌های مونت-کارلو نیز آورده می‌شوند که نشانگر دقت و صحت رابطه ریاضی به‌دست‌آمده است. بنابر اطلاع نویسندگان، کلیه نتایج ارائه شده در این مقاله کاملاً جدید بوده و گزارش مشابهی در سایر منابع پژوهشی وجود ندارد.

۲- مدل سیستم

شبکه موردبررسی در شکل ۱، شبکه رادیوشناختی رله‌ای بافردار است. نوع محوشدگی[۲۰] کانال‌های رایلی از نوع کند در نظر گرفته می‌شود به‌گونه‌ای که شرایط کانال در طول یک بازه ارسالی ثابت است و از یک بازه زمانی به بازه زمانی بعدی تغییر می‌کند. مطابق با شکل ۱، ساختار سیستم در شبکه اولیه شامل یک گیرنده (p) و در شبکه ثانویه شامل یک فرستنده (s)، یک گیرنده (d) و عنصر میان ارتباطی رله (r) در حضور شنودگر (eve) است.

هدف شنودگر در سیستم مفروض، صرفاً شنود اطلاعات انتقالی بین مسیرهای اصلی ارتباطی است و بر روی اطلاعات ارسالی تغییراتی ایجاد نمی‌کند؛ به‌عبارت‌دیگر شنودگر از نوع منفعل است. در شبکه ثانویه با فرض مسافت زیاد بین زوج فرستنده و گیرنده و اثرات سایه‌افکنی ناشی از محیط و سازه‌های موجود در آن، مسیر مستقیمی بین فرستنده و گیرنده در نظر گرفته نمی‌شود و این زوج، تنها از طریق رله به تبادل اطلاعات می‌پردازند. رله برای ذخیره داده‌ها به بافر Q با طول محدود L مجهز شده است. طول L بیانگر تعداد بسته‌های اطلاعاتی است که بافر رله در خود ذخیره می‌نماید. با توجه به هدف مسئله که بررسی محرمانگی این سیستم با مدل کانال رایلی است، تمامی کانال‌های ارتباطی توزیع رایلی دارند و به‌طور مستقل و یکسان توزیع‌شده‌اند. از طرفی برای راحتی در حل مسئله، فرض می‌شود که اطلاعات حالت تمامی کانال‌ها در مدل در نظر گرفته‌شده مشخص است و در گیرنده نسبت به آن‌ها اطلاعات کافی وجود دارد.

[DOR: 20.1001.1.26765810.1398.16.4.19.0]
Journal of Iranian Association of Electrical and Electronics Engineers - Vol.16- No.4- Winter2018

همچنین نویز سیستم به‌صورت نویز سفید گوسی جمع‌شونده با چگالی طیف توان N_0 فرض می‌شود.

ضرایب کانال برای ارتباط بین دو گره در مدل مذکور به‌صورت h_{XY} در نظر گرفته می‌شود که در آن $X \in \{s,r\}$ و $Y \in \{r,p,d,e\}$ است. از طرفی، با توجه به پیچیدگی کمتر و استفاده متداول‌تر، از روش نیمه دوطرفه برای انتقال اطلاعات رله استفاده می‌شود. در تبادل اطلاعات به‌صورت نیمه دوطرفه تنها یک عمل (ارسال/دریافت) در هر بازه زمانی صورت می‌گیرد؛ بنابراین در این مسئله، چگونگی وضعیت بافر رله، شاخص تصمیم‌گیری مهمی در انتخاب مسیر انتقالی مناسب به هنگام ارسال از طریق رله است. به‌منظور توصیف دقیق‌تر وضعیت بافر، حالت‌های مختلفی از قبیل تماماً پر، تماماً خالی و وجود حداقلی اطلاعات برای بافر برقرار است [۹]. رله در حالت تماماً پر صرفاً مسیر رله به گیرنده و در حالت تماماً خالی مسیر فرستنده به رله را برای دریافت و ارسال دارد. در حالت وجود حداقلی اطلاعات نیز بر اساس پروتکل انتخاب مسیر، از دو مسیر ممکن، یکی را برمی‌گزینند. در تمامی وضعیت‌های مذکور برای بافر، اگر سیستم در حالت قطع خود قرار گیرد به‌طوری‌که ظرفیت محرمانگی مسیر انتخاب‌شده کمتر از R_s بشود، تعداد بسته‌های اطلاعاتی موجود در بافر بدون تغییر باقی می‌ماند [۱۶].

در مدل‌سازی ریاضی مسئله، با توجه به دو پرشی بودن سیستم مشارکتی رله‌ای در نظر گرفته‌شده، SNR لحظه‌ای کانال‌ها به‌صورت رابطه [۱۱]

$$\gamma_{XY} = \frac{P_k |h_{XY}|^2}{\sigma^2}, \qquad (۱)$$

تعریف می‌شود که در آن h_{XY} ضرایب کانال، σ^2 واریانس نویز و P_k توان ارسالی در هر پرش است.

مطابق شرط تداخل در شبکه رادیوشناختی و مصون ماندن گیرنده اولیه از تداخل ناشی از ارسال‌های شبکه ثانویه، توان ارسالی فرستنده در هر پرش باید به‌گونه‌ای تنظیم می‌شود که کیفیت سرویس‌دهی به کاربر اولیه در شرایط مناسب خود قرار گیرد. با در نظر گرفتن این شرط، توان ارسالی برای s و r به‌صورت زیر حاصل می‌شود [۱۱]:

$$P_k = \min\left\{P_{\max}, \frac{I_{\max}}{|h_{kp}|^2}\right\}, \qquad (۲)$$

که $k \in \{s,r\}$ است. در این رابطه $P_{\max}$ بیشترین توان مجاز ارسالی در هر پرش و $I_{\max}$ آستانه توان تداخلی از پیش تعیین‌شده، برای کاربر اولیه است؛ بنابراین SNR لحظه‌ای کانال‌ها با ترکیب روابط (۱) و (۲) به‌صورت رابطه ذیل محاسبه می‌شود:

$$\gamma_{XY} = |h_{XY}|^2 \min\left\{\beta, \frac{\alpha}{|h_{kp}|^2}\right\} \qquad (۳)$$

که $\beta = \frac{P_{\max}}{N_0}$ و $\alpha = \frac{I_{\max}}{N_0}$ به ترتیب متوسط SNR در کاربران ثانویه و متوسط تداخل در گیرنده اولیه است. با توجه به اینکه ضرایب کانال‌ها توزیع رایلی دارند، بهره کانال یا به عبارتی توان دوم ضرایب کانال ($|h_{XY}|^2$)، طبق محاسبات توزیع نمایی دارد. تابع چگالی احتمال و تابع توزیع تجمعی توزیع نمایی به ترتیب به صورت‌های زیر نوشته می‌شود [۱۷]:

$$f_{|XY|^2}(z) = \left(\frac{1}{\Omega_z}\right)\exp\left\{-\frac{z}{\Omega_z}\right\} \qquad (۴)$$

$$F_{|XY|^2}(z) = 1-\exp\left\{-\frac{z}{\Omega_z}\right\} \qquad (۵)$$

که در روابط مذکور $\Omega = \frac{1}{\lambda} = \mathrm{E}\left[|h_{XY}|^2\right]$ است.

۳- احتمال قطع محرمانگی

ظرفیت محرمانگی تعریف‌شده توسط وینر به‌صورت تفاضل ظرفیت کانال اصلی از کانال شنودگر بیان می‌شود [۱۸]:

$$C_s = \left[C_d - C_e\right]^+ = \left[\log_2\left(\frac{1+\gamma_{Xr} \text{ or } \gamma_{Xd}}{1+\gamma_{Xe}}\right)\right]^+ \qquad (۶)$$

که در رابطه فوق، C_d و C_e به ترتیب ظرفیت کانال اصلی و ظرفیت کانال شنود شونده و $[x]^+ = \max(x,0)$ است.

درصورتی‌که ظرفیت محرمانگی سیستم از نرخ محرمانگی مشخصی برای ارسال کمتر شود، سیستم قطع خواهد بود. درنتیجه ارسال اطلاعات با نرخی بیش‌تر از نرخ محرمانگی مشخص‌شده، تضمینی برای حفظ و تأمین امنیت اطلاعات وجود ندارد. احتمال قطع محرمانگی طبق رابطه زیر تعریف می‌شود [۱۸]:

$$P_{out} = \Pr\{C_s < R_s\} \qquad (۷)$$

که در این رابطه R_s همان نرخ محرمانگی آستانه است ($R_s > 0$).

احتمال قطع محرمانگی که مطابق رابطه (۷) بیان می‌شود در هنگامی مطرح است که ظرفیت محرمانگی شبکه ارتباطی رابطه (۶) کمتر از نرخ محرمانگی موردنظر (R_s) برای ارسال اطلاعات در شبکه باشد. در این حالت شبکه ارتباطی نمی‌تواند اطلاعات را به‌طور محرمانه به گیرنده موردنظر برساند و درنتیجه سیستم ایمنی موردنظر برای ارسال اطلاعات در شبکه را ندارد.

در رابطه (۷) با تعیین مناسب نرخ محرمانگی آستانه که حداقل نرخ قابل‌قبول برای عملکرد صحیح محرمانگی سیستم است، کیفیت سرویس‌دهی در حد معینی تضمین می‌شود.

با فرض اینکه رله از پروتکل کدگشایی و ارسال، برای ارسال اطلاعات دریافتی استفاده می‌نماید و به‌صورت نیمه دوطرفه عمل می‌کند، درصورتی‌که مسیر فرستنده ثانویه به رله (sr) توسط پروتکل انتخاب مسیر برگزیده شود، توانایی دریافت اطلاعات را دارد و در حالتی که

[DOR: 20.1001.1.26765810.1398.16.4.19.0]

مسیر رله به گیرنده ثانویه (rd) انتخاب شود، برای ارسال اطلاعات به سمت مقصد آماده است. در هر دو حالت، ظرفیت محرمانگی کانال در هر پرش به‌صورت رابطه زیر خواهد بود [۱۹]:

$$C_s = \max\left\{0, \frac{1}{2}\log_2\left(\frac{1+P_k\,|h_{kd}|^2/N_0}{1+P_k\,|h_{ke}|^2/N_0}\right)\right\}. \qquad (۸)$$

از طرفی، برای تعیین هم‌زمان بهترین مسیر از بین مسیرهای موجود، برای ارتباط بین فرستنده و گیرنده از طریق رله در شبکه ثانویه، روش بیش‌ترین نسبت کانال اصلی به شنودگر در [۱۸] ارائه‌شده است. مطابق با روش بیش‌ترین نسبت، بهترین مسیر در شبکه رادیوشناختی به‌صورت زیر انتخاب می‌شود [۱۵]:

$$R^* = arg\max\left\{\frac{1+P_s\,|h_{sr}|^2/N_0}{1+P_s\,|h_{se}|^2/N_0}, \frac{1+P_r\,|h_{rd}|^2/N_0}{1+P_r\,|h_{re}|^2/N_0}\right\}. \qquad (۹)$$

در شبکه رله‌ای بافردار رادیوشناختی تنها در حالتی امکان انتخاب مسیر وجود دارد که بافر رله نه تماماً پر و نه تماماً خالی باشد؛ بنابراین در این حالت، مسیری که شرط فوق را ارضاء کند، انتخاب می‌شود.

در مدل‌سازی ریاضی، حالت‌های مختلف وضعیت بافر با "*زنجیره مارکف* " مدل‌سازی می‌شود. در زنجیره مارکف، هر "*حالت* " به تعداد بسته‌های اطلاعات در بافر گفته می‌شود. در مدل مذکور، ازآنجایی‌که طول بافر L است، تعداد $L+1$ حالت برای زنجیره مارکف، ایجاد می‌شود. افزایش یک واحدی تعداد حالت‌های زنجیره مارکف به دلیل در نظر گرفتن حافظه تماماً خالی بافر است. زنجیره مارکف توسط احتمالات حالت گذار توصیف می‌شود. برای محاسبه احتمال قطع محرمانگی با استفاده از پروتکل انتخاب رله به روش بیش‌ترین نسبت در ابتدا ماتریس حالت گذار زنجیره مارکف را مطابق آنچه در [۹، ۱۹، ۲۰] آمده است، تشکیل داده می‌شود. ماتریس حالت گذار طبق تعریف، ماتریسی مربعی است که احتمال برقراری ارتباط بین حالت‌های مختلف بافر را بیان می‌کند. همان‌طور که ذکر شد، $L+1$ حالت برای زنجیره مارکف به وجود می‌آید که درنتیجه ماتریس حالت گذار، ماتریسی با ابعاد $(L+1)\times(L+1)$ است. ماتریس حالت گذار با $\mathbf{A}$ نشان داده می‌شود. هر درایه ماتریس، احتمال حرکت از حالت s_i در زمان t به حالت s_j در زمان $t+1$ را نشان می‌دهد [۲۱].

$$A_{i,j} = \Pr(s_i \to s_j) = \Pr(X_{t+1} = s_j \mid X_t = s_i) \qquad (۱۰)$$

احتمال گذار بین حالت‌های مختلف، به وضعیت بافر رله و تعداد مسیرهای در دسترس در آن وضعیت بستگی دارد. برای مثال، چنانچه بافر رله پر/خالی باشد، رله نمی‌تواند داده‌ای دریافت/ارسال نماید. به عبارتی تنها یک مسیر برای اعمال پروتکل انتخاب مسیر باقی می‌ماند. به‌طورکلی، تعداد مسیرهای در دسترس، در روش بیش‌ترین نسبت برای سیستم مفروض به‌صورت زیر است [۲۱]:

$$D_l = \begin{cases} 2, & 0 < \Psi(Q) < L \\ 1, & \Psi(Q) = 0, L \end{cases} \qquad (۱۱)$$

که $\Psi(Q)$ تعداد بسته‌های اطلاعاتی ذخیره‌شده در بافر است. بر اساس فرضیات صورت گرفته پیرامون متقارن بودن مسیرها و توزیع مستقل و یکسان آن‌ها، چنانچه بافر در حالت s_l قرار گیرد، احتمال انتخاب مسیر معینی از میان مسیرهای موجود برابر با $1/D_l$ است که $0 < l < L+1$؛ بنابراین احتمال اینکه بافر از حالت s_l به حالت دیگری برود به‌صورت رابطه [۲۱]

$$P_{D_l} = \frac{1}{D_l}\left[1 - SOP(\theta)^{D_l}\right], \qquad (۱۲)$$

و احتمال عدم‌تغییر در حالت بافر در زمان قطع بودن، طبق رابطه [۲۱]

$$\bar{P}_{D_l} = 1 - \sum_{n=1}^{D_l} P_{D_l} = 1 - \frac{1}{D_l}\sum_{n=1}^{D_l}\left[1 - SOP(\theta)^{D_l}\right] \qquad (۱۳)$$

به دست می‌آید ($\theta = 2^{2R_s}$). بر اساس روابط (۱۲) و (۱۳) ماتریس حالت گذار به فرم زیر قابل‌محاسبه است [۲۱]:

$$A_{i,j} = \begin{cases} P_{D_l}, & s_i \in U_j \\ \bar{P}_{D_l}, & s_i \notin U_j \\ 0, & \text{O.W.} \end{cases} \qquad (۱۴)$$

در ماتریس حالت گذار، $i, j \in \{1, ..., L+1\}$ و U_j مجموعه‌ای شامل تمامی حالت‌هایی است که باحالت s_j ام در ارتباط است. در مجموعه U_j حالت‌هایی که در آن s_j با خودش در ارتباط است، منظور نمی‌گردد. طبق [۲۱] بردار احتمال حالت گذار به‌صورت

$$\kappa = (A - I + B)^{-1}\, b, \qquad (۱۵)$$

نوشته می‌شود که در آن $\kappa = [\kappa_1, \cdots, \kappa_{L+1}]$ توزیعی یکنواخت دارد. برای هر $i, j \in \{1, 2, \cdots, L+1\}$، $b = [1, 0, \cdots, 1]^T$ و $B_{i,j} = 1$ است. درحالتی‌که وضعیت بافر بدون تغییر باقی بماند، سیستم در حالت قطع خود قرار می‌گیرد.

احتمال قطع محرمانگی کل شبکه رله‌ای بافردار رادیوشناختی طبق مطالب فوق‌الذکر، به فرم

$$SOP_{\text{tot}}(R_s) = \sum_{i=1}^{L+1} \kappa_i \bar{P}_{D_l} \qquad (۱۶)$$

بازنویسی می‌شود که در آن R_s نرخ محرمانگی موردنظر مسئله است [۲۱].

۳-۱- احتمال قطع محرمانگی برای مسیر انتخابی

با فرض متقارن بودن مسیرها در هر پرش، احتمال قطع مسیر sr با احتمال قطع مسیر rd برابر است. ازاین‌رو برای محاسبه $\bar{P}_{D_l}$ در

[DOR: 20.1001.1.26765810.1398.16.4.19.0]
Journal of Iranian Association of Electrical and Electronics Engineers - Vol.16- No.4- Winter2018

رابطه (۱۶)، با توجه بـه رابطـه (۱۳)، لازم اسـت کـه احتمـال قطـع محرمانگی هر مسیر محاسبه شود. مشروط بر متقارن بودن مسیرهای اصلی، محاسبه احتمال قطع یکی از دو پرش برای تحلیـل و ارزیـابی مسئله کفایت می‌کند. با فرض انتخاب مسیر sr برای ارسال اطلاعات، احتمال قطع این مسیر به‌صورت زیر تعریف می‌گردد [۹]:

$$SOP = \Pr\{C_s < R_s, \gamma_{sr} > \gamma_{se}\} + \Pr\{\gamma_{sr} \le \gamma_{se}\}. \qquad (۱۷)$$

رابطه فوق بیان می‌دارد که سیستم در دو حالت زیر قطع خواهد بود:

۱. کانال اصلی شـرایط بـدتری از کانـال شـنود دارد و بـا ارسـال اطلاعات تمامی آن شنود می‌شود.

۲. کانال اصلی باوجود داشتن شرایط بهتر نسبت به کانال شنودگر، نرخ محرمانگی موردنظر برای ارسال را تأمین نمی‌کند.

در محاسبه رابطه (۱۷)، با توجه به P_k و فـرض $X = |h_{kp}|^2$، تـوان ارسـالی فرسـتنده برحسـب متغیـر تصـادفی X بـه صـورت $g(X) = \min\{\beta, \alpha / X\}$ به دست می‌آید کـه درنتیجـه بـه دلیـل وجود تابع مینیمم، انتگرال‌های موجود به دو بخش تقسیم می‌شـوند. شکل ساده‌شده رابطه (۱۷) به‌صورت زیر محاسبه می‌شود:

$$\begin{aligned} SOP = {} & \Pr\{C_s < R_s, \gamma_{sr} > \gamma_{se}, P_s = P_{\max}\} \\ & + \Pr\{\gamma_{sr} \le \gamma_{se}, P_s = P_{\max}\} \\ & + \Pr\{C_s < R_s, \gamma_{sr} > \gamma_{se}, P_s = I_{\max} / X\} \\ & + \Pr\{\gamma_{sr} \le \gamma_{se}, P_s = I_{\max} / X\}. \end{aligned} \qquad (۱۸)$$

با جایگـذاری (۴) و (۵) در عبـارت فـوق، احتمـال قطـع محرمـانگی سیستم برای پرش اول به‌صورت زیر به دست می‌آید:

$$\begin{aligned} SOP_{sr} = {} & 1 + \frac{\lambda_{se}}{\lambda_{se} + \lambda_{sr}\theta} \exp\left\{-\frac{\lambda_{sr}(\theta-1)}{\beta}\right\}\left(1 - \exp\left\{-\frac{\alpha\lambda_{sp}}{\beta}\right\}\right) \\ & + \frac{\lambda_{sp}\lambda_{se}}{\left(\lambda_{se} + \lambda_{sr}\theta\right)\left(\lambda_{sp} + \frac{\lambda_{sr}(\theta-1)}{\alpha}\right)} \exp\left\{-\left(\frac{\alpha\lambda_{sp}}{\beta} + \frac{\lambda_{sr}(\theta-1)}{\beta}\right)\right\}. \end{aligned} \qquad (۱۹)$$

درنهایت با جایگذاری رابطه (۱۹) در رابطه (۱۳) و جایگذاری نتیجـه به‌دست‌آمده در رابطه (۱۶)، احتمال قطع محرمانگی کل شبکه رله‌ای بافردار با محوشدگی رایلی کانال‌ها به فرم زیر به دست می‌آید:

$$\begin{aligned} SOP_{\text{tot}}(R_s) &= \sum_{i=1}^{L+1} \kappa_i \left(1 - \frac{1}{D_l} \sum_{n=1}^{D_l} \left[1 - SOP(\theta)^{D_l}\right]\right) \\ &= \sum_{i=1}^{L+1} \kappa_i \left(1 - \frac{1}{D_l} \sum_{n=1}^{D_l} \left[1 - \left(1 + \frac{\lambda_{se}}{\lambda_{se} + \lambda_{sr}\theta} \exp\left\{-\frac{\lambda_{sr}(\theta-1)}{\beta}\right\}\right)^{D_l} \right.\right. \\ & \qquad \left(1 - \exp\left\{-\frac{\alpha\lambda_{sp}}{\beta}\right\}\right) \\ & \qquad + \frac{\lambda_{sp}\lambda_{se}}{\left(\lambda_{se} + \lambda_{sr}\theta\right)\left(\lambda_{sp} + \frac{\lambda_{sr}(\theta-1)}{\alpha}\right)} \\ & \qquad \left.\left. \exp\left\{-\left(\frac{\alpha\lambda_{sp}}{\beta} + \frac{\lambda_{sr}(\theta-1)}{\beta}\right)\right\} \right]\right) \end{aligned} \qquad (۲۰)$$

۴- تحلیل نتایج عددی

پس از به دست آوردن رابطه‌ای برای احتمال قطع محرمانگی سیستم، به بررسی و تحلیل نتایج عددی و شبیه‌سازی‌ها پرداخته می‌شود. معیار ارزیابی کارایی سیستم رله‌ای بافردار رادیوشناختی در نظر گرفته‌شده، مطابق آنچه قبلاً ذکر شد، احتمال قطع محرمانگی است.

از پارامترهای قابل‌تغییر برای مقایسه حالات مختلف می‌توان به نسبت سیگنال به نویز کانال اصلی، نسبت سیگنال به نویز کانال شنود شونده، نسبت حداکثر توان تداخلی به ارسالی، نرخ محرمانگی موردنظر و طول بافر اشاره کرد. در ادامه به بحث پیرامون تغییر هر یک از پارامترهای مذکور و اثر آن‌ها بر عملکرد محرمانگی سیستم پرداخته می‌شود.

نتایج عددی حاصل از رابطه احتمال قطع محرمانگی و نتایج شبیه‌سازی مونت-کارلو سیستم مذکور با استفاده از نرم‌افزار MATLAB به‌دست‌آمده است. شبیه‌سازی سیستم پیشنهادی بر اساس روش مونت-کارلو انجام می‌گیرد، که ترتیب انجام آن در برنامه MATLAB به‌صورت زیر است:

- تولید ضرایب تمامی کانال‌های h_{sp}، h_{se}، h_{sr}، h_{rd}، h_{re} و h_{rp} به تعداد N (N=1000000) به‌صورت تصادفی، که توزیع رایلی دارند.
- محاسبه SNR کانال‌ها (γ_{sr} , γ_{se} , γ_{rd} , γ_{re}) با در نظرگرفتن شرط تداخل با شبکه اولیه بر اساس رابطه (۳).
- محاسبه ظرفیت محرمانگی در پرش اول و پرش دوم (C_{sr} , C_{rd}) بر اساس رابطه (۶)
- در نظر گرفتن حالات مختلف ایجادشده در بافر (تماماً پر، تماماً خالی، نه پر و نه خالی) و تعداد مسیرهای ممکن بر اساس توضیحات بخش سوم.
- تعیین احتمال قطع محرمانگی سیستم با شمارش تعداد حالاتی که $C_S < R_s$ است (N_{out}) به‌صورت $SOP = N_{out}/N$

در این سیستم تأخیر ناشی از بافر در سیستم در نظر گرفته نمی‌شود. در نتایج شبیه‌سازی‌هایی که پارامتر $P_{\max}$ و $I_{\max}$ تغییر نمی‌کنند، این پارامترها به ترتیب dB۲۰ و dB۱۰ فرض می‌شوند. فرض‌های استفاده‌شده در شبیه‌سازی‌ها مشابه فرض‌های متداول در کارهای پیشین و سیستم‌های عملی و کاربردی است.

به‌منظور مقایسه کمی عملکرد محرمانگی سیستم پیشنهادی در دو حالت وجود و عدم وجود بافر در رله، در جدول۱ نسبت سیگنال به نویز کانال اصلی به نسبت سیگنال به نویز کانال شنودگر با احتمال قطع محرمانگی سیستم به ازای مقادیر مشخصی، مورد مقایسه قرارگرفته است.

[DOR: 20.1001.1.26765810.1398.16.4.19.0]

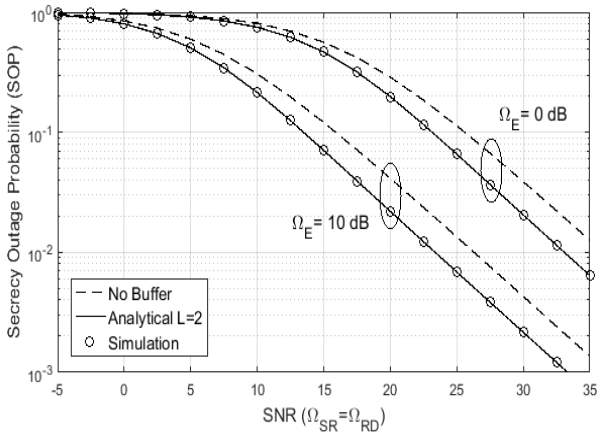
جدول ۱: مقایسه SNR کانال اصلی به SNR کانال شنودگر در حالت رله بافردار و بدون بافر به ازای مقادیر مشخص برای احتمال قطع محرمانگی

	نسبت سیگنال به نویز کانال اصلی به کانال شنودگر		
SOP	بدون بافر	بافردار L=2	بافردار L=20
10^{-2}	26.3 dB	23.3 dB	17 dB
10^{-3}	36.3 dB	33.3 dB	24.4 dB
10^{-5}	56.3 dB	53.3 dB	43.3 dB

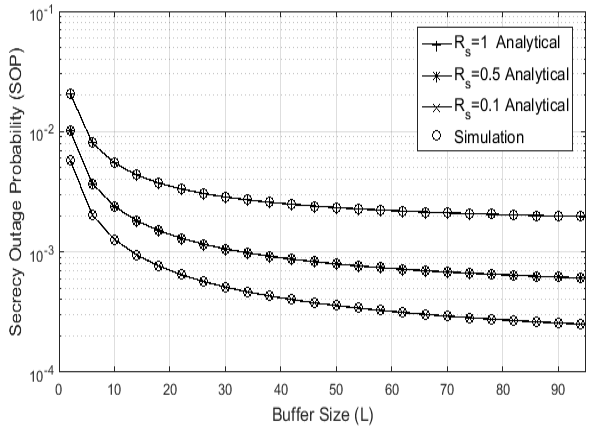
در شکل ۲ میزان تأثیر تغییرات SNR کانال‌های اصلی بر احتمال قطع محرمانگی سیستم آورده شده است. در این شکل، مقدار SNR مسیرهای اصلی که همان sr و rd هستند، از مقدار ۵- تا ۳۵ دسی‌بل تغییر می‌کند. طول بافر و نرخ محرمانگی موردنظر به ترتیب $L=2$ و $R_s=1$ فرض شده است. همان‌طور که مشاهده می‌شود، با بهبود شرایط محیطی احتمال قطع محرمانگی سیستم کاهش می‌یابد. همچنین تأثیر مخرب مسیرهای شنودگر بر عملکرد سیستم با افزایش SNR این مسیرها قابل‌مشاهده است. در ارزیابی دقیق‌تر عملکرد سیستم، اگر SNR مسیر شنودگر بزرگ‌تر از مسیر ارسالی بود، سیستم در حالت قطع خود قرار دارد و اطلاعاتی منتقل نمی‌شود. در SNR های پایین برای مسیر شنودگر، انتقال اطلاعات با موفقیت صورت می‌گیرد. برای مثال در $\Omega_d = 25\,\text{dB}$ با افزایش ۱۰ برابری SNR کانال شنود کننده از $\Omega_e = 0\,\text{dB}$ به $\Omega_e = 10\,\text{dB}$، احتمال قطع محرمانگی سیستم تقریباً افزایش ۱۰ برابری دارد و احتمال شنود اطلاعات بیشتر می‌شود.

از طرف دیگر، به‌منظور بررسی تأثیرات مقدار حافظه بافر بر عملکرد سیستم، در شکل ۳ احتمال قطع محرمانگی سیستم برحسب طول بافر برای R_s های مختلف ترسیم شده است. با دقت در شکل مذکور می‌توان دریافت که چنانچه طول بافر (L) زیاد فرض شود، احتمال قطع محرمانگی سیستم به‌احتمال ثابتی همگرا می‌شود. طول کم بافر، به دلیل تسریع در روند پر و خالی شدن بافر، احتمال قطع را افزایش می‌دهد، بدین‌صورت که در آن حالت‌ها شرایط کانال ارضا نمی‌گردد. نکته حائز اهمیت دیگر در شکل ۳ تغییرات نرخ محرمانگی هدف R_s و میزان حساسیت انتقال ایمن اطلاعات بر این تغییرات است. مطابق شکل، با افزایش R_s قابلیت شنود بر روی اطلاعات ارسالی بیش‌تر می‌شود که مطابق با نتایج تحلیلی و مفهوم نرخ محرمانگی موردنظر این رفتار قابل پیش‌بینی بود.

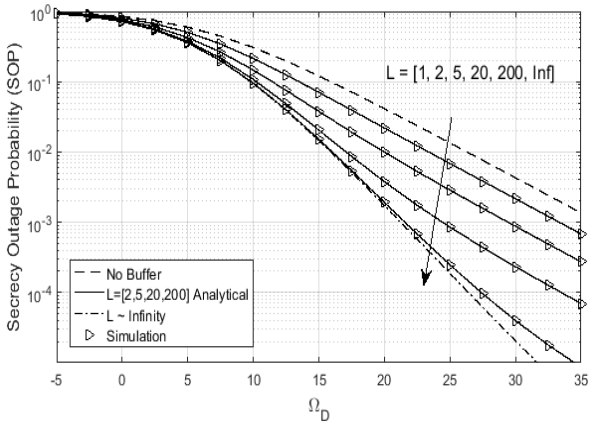
در شکل ۴ با فرض اینکه SNR کانال‌های اصلی به کانال‌های شنود شونده نرمالیزه شده و به عبارتی $\Omega_d = \frac{\Omega_{sr}}{\Omega_{se}} = \frac{\Omega_{rd}}{\Omega_{re}}$ فرض شده است، احتمال قطع محرمانگی سیستم به دست می‌آید. با دقت در شکل مذکور، می‌توان اثرگذاری تغییرات هم‌زمان SNR و مقدار حافظه بافر (طول بافر) را بر احتمال قطعی سیستم مشاهده نمود. همان‌طور که ملاحظه می‌شود، برای طول‌های زیاد بافر، با تغییر SNR کانال‌ها، احتمال قطع تغییرات چندانی ندارد و به مقدار معینی همگرا می‌شود.



شکل (۲): احتمال قطع محرمانگی برحسب SNR کانال‌های اصلی به ازای مقادیر مختلف SNR کانال‌های شنودگر



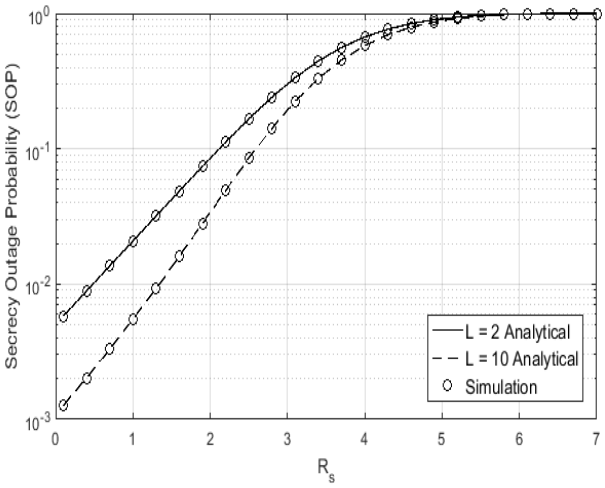
شکل (۳): احتمال قطع محرمانگی برحسب طول بافر به ازای مقادیر مختلف نرخ محرمانگی



شکل (۴): احتمال قطع محرمانگی برحسب SNR نرمالیزه شده کانال‌های اصلی به SNR کانال شنودگر به ازای طول‌های مختلف بافر

به‌منظور مشاهده روند تأثیرگذاری تغییرات نرخ محرمانگی هدف بر احتمال قطع سیستم، شکل ۵ رسم شده است. در این نمودار بعد از نرخ محرمانگی معینی (حدود ۴،۵)، سیستم کاملاً قطع است. نکته

[DOR: 20.1001.1.26765810.1398.16.4.19.0]
Journal of Iranian Association of Electrical and Electronics Engineers - Vol.16- No.4- Winter2018

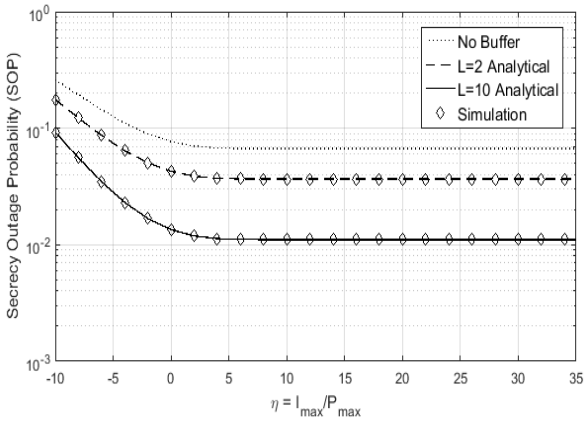


شکل (۵): احتمال قطع محرمانگی برحسب نرخ محرمانگی موردنظر به ازای مقادیر مختلف برای طول بافر

حائز اهمیت در تعیین نرخ محرمانگی آستانه، انتخاب مقدار مناسب آن است. به‌طوری‌که هر مقدار نرخ محرمانگی آستانه کوچک انتخاب شود، ظرفیت سیستم برای انتقال اطلاعات هم به همان نسبت کاهش خواهد داشت. اگرچه ایمنی اطلاعات انتقالی با انتخاب نرخ محرمانگی کوچک حفظ می‌شود، اما کاهش ظرفیت سیستم موجب کاهش کیفیت سرویس‌دهی و متعاقباً نارضایتی کاربران خواهد شد. احتمال قطع محرمانگی سیستم برای دو مقدار مختلف طول بافر $L=2,10$ در این شکل رسم شده است.

پارامتر دیگری که می‌تواند اثرات آن مورد ارزیابی قرار گیرد، نسبت توان تداخلی به توان ارسالی کاربران ثانویه است. در شکل ۶ احتمال قطع محرمانگی سیستم برحسب $I_{\max}/P_{\max}$ که بیانگر نسبت حداکثر توان تداخلی به حداکثر توان ارسالی در شبکه ثانویه است، رسم شده است. به ازای تغییرات $\eta = I_{\max}/P_{\max}$، تأثیر تغییرات نرخ محرمانگی بر احتمال قطع محرمانگی سیستم قابل‌مشاهده است. طبق $\min\{P_{\max}, I_{\max}/X\}$ رفتار شکل ۴ قابل پیش‌بینی بود، چراکه طبق فرضیات صورت گرفته $P_{\max}$ و $I_{\max}$ همواره اعدادی ثابت هستند و تنها متغیر موجود در عبارت فوق X است. لذا با توجه به این شرط که $I_{\max} < P_{\max}$، از SNR معینی که مستقیماً به نسبت دو توان تداخلی وابسته است به سمت SNR های بالاتر، منحنی به مقدار ثابتی همگرا می‌شود. چراکه با افزایش η در عبارت $\min\{P_{\max}, I_{\max}/X\}$ همواره مقدار ثابت $P_{\max}$ انتخاب می‌شود و درنتیجه احتمال قطع ثابت می‌ماند.

هم‌چنین در شکل‌های ۲ الی ۶ مشاهده می‌شود که نتایج شبیه‌سازی مونت-کارلو با نتایج عددی، مطابقت خوبی دارند که این امر صحت روابط به‌دست‌آمده و تحلیل‌های ریاضی را نشان می‌دهد.



شکل (۶): احتمال قطع محرمانگی برحسب نسبت حداکثر توان تداخلی فرستنده ثانویه به حداکثر توان ارسالی فرستنده ثانویه به ازای مقادیر مختلف برای طول بافر

۵- نتیجه‌گیری

با هدف بهبود امنیت لایه فیزیکی در شبکه رادیوشناختی رله‌ای بافردار و مقایسه با حالت بدون بافر در حالتی که کانال‌ها محوشدگی رایلی دارند، سیستم پیشنهادی مطرح گردید. در سیستم مفروض، شبکه رادیوشناختی متشکل از یک گیرنده اولیه، فرستنده و گیرنده ثانویه، رله مجهز به بافر و شنودگر است. شنودگر قابلیت شنود تمامی پیام‌های ارسالی شبکه ثانویه را دارد. در این شبکه معیار احتمال قطع محرمانگی به‌عنوان ارزیابی عملکرد شبکه موردبررسی قرار گرفت و فرم بسته برای احتمال قطع محرمانگی سیستم به دست آورده شد. با شبیه‌سازی روابط توسط نرم‌افزار MATLAB و استخراج شکل‌ها، اثرگذاری هر یک از پارامترهای موجود در مسئله به‌طور مفصل بحث شد. با توجه به نتایج به‌دست‌آمده، ملاحظه می‌شود که وجود شنودگر در شبکه به چه میزان می‌تواند محرمانگی سیستم موردنظر را در معرض خطر قرار دهد. ازاین‌رو می‌توان با تخصیص مقادیر مناسب برای پارامترهای مختلف که در قسمت نتایج بیان شد، عملکرد محرمانگی سیستم را بهبود بخشید یا به‌عبارت‌دیگر احتمال قطع محرمانگی سیستم را در حضور شنودگر کاهش داد.

مراجع

[۱] C. X. Wang, F. Haider, X. Gao, X. H. You, Y. Yang, D. Yuan, H. M. Aggoune, H. Haas, S. Fletcher, and E. Hepsaydir, "Cellular architcture and key technologies for ۵g wireless communication networks," IEEE Communications Magazine, vol.۵۲, pp.۱۲۲–۱۳۰, February ۲۰۱۴.

[۲] A. Nosratinia, T. E. Hunter, and A. Hedayat, "Cooperative communication in wireless networks," IEEE Communications Magazine, vol.۴۲, pp.۷۴–۸۰, Oct ۲۰۰۴.

[۳] S. Haykin, "Cognitive radio: brain-empowered wireless communications," IEEE Journal on Selected Areas in Communications, vol.۲۳, pp.۲۰۱–۲۲۰, Feb ۲۰۰۵.

[۴] Y. S. Shiu, S. Y. Chang, H. C. Wu, S. C. H. Huang, and H. H. Chen, "Physical layer security in wireless networks: a tutorial," IEEE Wireless Communications, vol.۱۸, pp.۶۶–۷۴, April ۲۰۱۱.

[۵] M. J. Saber and S. M. Sajad Sadough, "Multiband Cooperative Spectrum Sensing for Cognitive Radio in the Presence of Malicious

Users," in IEEE Communications Letters, vol. 20, no. 2, pp. 404-407, Feb. 2016.
[۶] Z. Ding, I. Krikidis, B. Rong, J. S. Thompson, C. Wang, and S. Yang, "On combating the half-duplex constraint in modern cooperative networks: protocols and techniques," IEEE Wireless Communications, vol.۱۹, pp.۲۰–۲۷, December ۲۰۱۲.
[۷] بیانی فر مهدی، رضوی زاده سید محمد. بررسی کارایی توان کانال تداخلی رله چند ورودی-چند خروجی انبوه. مجله مهندسی برق و الکترونیک ایران. ۱۳۹۶; ۱۴ (۲) :۱۱-۲۲
[۸] زراعتکار مقدم جواد، فرخی حمید، ندا ناصر. مدیریت تداخل در شبکه‌های رادیوشناختگر با استفاده از شکل‌دهی پرتو همکارانه تحت اطلاعات غیر دقیق کانال. مجله مهندسی برق و الکترونیک ایران. ۱۳۹۶; ۱۴ (۲) :۱-۹
[۹] محمدجواد صابر، "ارتقاء امنیت لایه فیزیکی در شبکه‌های رادیوشناختی"، رساله دکتری، دانشکده مهندسی برق، دانشگاه شهید بهشتی، ۱۳۹۶.
[۱۰] B. Xia, Y. Fan, J. Thompson, and H. V. Poor, "Buffering in a three-node relay network," IEEE Transactions on Wireless Communications, vol.۷, pp.۴۴۹۲–۴۴۹۶, November ۲۰۰۸.
[۱۱] R. Zhao, Y. Yuan, L. Fan, and Y. C. He, "Secrecy performance analysis of cognitive decode-and-forward relay networks in nakagami-m fading channels," IEEE Transactions on Communications, vol.۶۵, pp.۵۴۹–۵۶۳, Feb ۲۰۱۷.
[۱۲] R. K. Sharma and D. B. Rawat, "Advances on security threats and countermeasures for cognitive radio networks: A survey," IEEE Communications Surveys Tutorials, vol.۱۷, pp.۱۰۲۳–۱۰۴۳, Secondquarter ۲۰۱۵.
[۱۳] M. Elkashlan, L. Wang, T. Q. Duong, G. K. Karagiannidis, and A. Nallanathan, "On the security of cognitive radio networks," IEEE Transactions on Vehicular Technology, vol.۶۴, pp.۳۷۹۰–۳۷۹۵, Aug ۲۰۱۵.
[۱۴] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," IEEE Transactions on Signal Processing, vol.۵۸, pp.۱۸۷۵–۱۸۸۸, March ۲۰۱۰.
[۱۵] A. Sun, T. Liang, and Y. Zhang, "Secure performance analysis of buffer-aided cognitive relay networks," in ۲۰۱۵ IEEE International Conference on Computer and Communications (ICCC), pp.۴۹۰–۴۹۵, Oct ۲۰۱۵.
[۱۶] G. Chen, Z. Tian, Y. Gong, and J. Chambers, "Decode-and-forward buffer-aided relay selection in cognitive relay networks," IEEE Transactions on Vehicular Technology, vol.۶۳, pp.۴۷۲۳–۴۷۲۸, Nov ۲۰۱۴.
[۱۷] Papoulis, Athanasios, and S. Unnikrishna Pillai. Probability, random variables, and stochastic processes. Tata McGraw-Hill Education, ۲۰۰۲.
[۱۸] A. D. Wyner, "The wire-tap channel," The Bell System Technical Journal, vol.۵۴, pp.۱۳۵۵–۱۳۸۷, Oct ۱۹۷۵.
[۱۹] G. Chen, Z. Tian, Y. Gong, Z. Chen, and J. A. Chambers, "Max-ratio relay selection in secure buffer-aided cooperative wireless networks," IEEE Transactions on Information Forensics and Security, vol.۹, pp.۷۱۹–۷۲۹, April ۲۰۱۴.
[۲۰] J. Huang and A. L. Swindlehurst, "Buffer-aided relaying for two-hop secure communication," IEEE Transactions on Wireless Communications, vol.۱۴, pp.۱۵۲–۱۶۴, Jan ۲۰۱۵.
[۲۱] I. Krikidis, T. Charalambous, and J. S. Thompson, "Buffer-aided relay selection for cooperative diversity systems without delay constraints," IEEE Transactions on Wireless Communications, vol.۱۱, pp.۱۹۵۷–۱۹۶۷, May ۲۰۱۲.
[۲۲] Wang, Bo, Pengcheng Mu, and Zongze Li. "Secrecy rate maximization with artificial-noise-aided beamforming for MISO wiretap channels under secrecy outage constraint." IEEE Communications Letters 19.1 (2015): 18-21.
[۲۳] Wang, Chao, and Hui-Ming Wang. "On the secrecy throughput maximization for MISO cognitive radio network in slow fading channels." IEEE Transactions on Information Forensics and Security 9.11 (2014): 1814-1827.
[۲۴] Zhao, Hui, et al. "Secrecy outage on transmit antenna selection/maximal ratio combining in MIMO cognitive radio networks." IEEE Transactions on Vehicular Technology 65.12 (2016): 10236-10242.

زیرنویس‌ها

[1] Cognitive Radio
[2] Primary Users
[3] Secondary Users
[4] Underlay
[5] Overlay
[6] Interweave
[7] Relay Networks
[8] Cognitive Relay Networks (CRN)
[9] Broadcast
[10] Passive and Active Eavesdroppers
[11] Half-Duplex
[12] Pre-Scheduled Plan
[13] Buffer
[14] Throughput
[15] Diversity
[16] Signal-to-Noise (SNR)
[17] Beamforming
[18] Multi Input-Multi Output (MIMO)
[19] Rayleigh Distribution
[20] Fading

[DOR: 20.1001.1.26765810.1398.16.4.19.0]