

حسگری طیفی در حضور مهاجم هوشمند تقلیدکننده کاربر اولیه و تأثیر آن بر عملکرد و برون‌دهی شبکه‌های رادیوشناختی

علی کریمی^۱ عباس طاهرپور^۲

۱- کارشناسی ارشد- دانشکده فنی و مهندسی - دانشگاه بین‌المللی امام خمینی (ره)- قزوین - ایران
a.karimi@edu.ikiu.ac.ir

۲- استادیار- دانشکده فنی و مهندسی - دانشگاه بین‌المللی امام خمینی (ره)- قزوین - ایران
taherpour@ikiu.ac.ir

چکیده: شبکه‌های رادیوشناختی یکی از راهکارهای پیشنهادشده برای مقابله با کمبود طیف در سرویس‌های مبتنی بر مخابرات بی‌سیم است. حسگری طیفی فرایندی حیاتی در شبکه‌های رادیوشناختی است که هرگونه تداخل در عملکرد آن سبب آسیب رسیدن به شبکه می‌شود. در این مقاله مهاجم هوشمندی معرفی شده است که در طی زمان حسگری، طیف را حس می‌کند و به محض خارج شدن کاربر اولیه وارد کانال می‌شود و با تقلید رفتار کاربر اولیه سعی در تصاحب طیف دارد. ترافیک کاربر اولیه و مهاجم هوشمند تقلیدکننده کاربر اولیه به صورت فرایند مارکوف وابسته به زمان مدل شده است. سپس با محاسبه عملکرد شبکه رادیوشناختی و برون‌دهی شبکه کاربران ثانویه در حضور مهاجم هوشمند تقلیدکننده کاربر اولیه، تأثیر پارامترهای ترافیک کاربر اولیه و مهاجم هوشمند تقلیدکننده کاربر اولیه بر آن‌ها مورد بررسی قرار گرفته است. هم‌چنین حمله مهاجم تقلیدکننده کاربر اولیه در روش‌های سنتی و حمله به صورت هوشمند مورد مقایسه قرار گرفته است، نتایج نشان می‌دهند در حالت حمله به صورت هوشمند، برون‌دهی شبکه کاربران ثانویه بیشتر مورد آسیب قرار می‌گیرد و حتی در صورت انتخاب پارامترهای ترافیک حمله مناسب می‌توان برون‌دهی را به صفر رساند.

واژه‌های کلیدی: شبکه‌های رادیوشناختی، حسگری طیفی، امنیت شبکه، مهاجم هوشمند تقلیدکننده کاربر اولیه، برون‌دهی شبکه.

تاریخ ارسال مقاله: ۱۳۹۶/۱۲/۲۰

تاریخ پذیرش مشروط مقاله: ۱۳۹۷/۰۷/۲۳

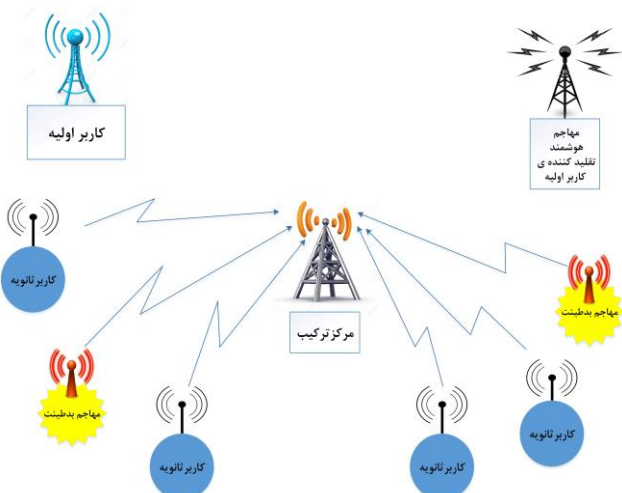
تاریخ پذیرش مقاله: ۱۳۹۸/۰۴/۰۷

نام نویسنده مسئول: دکتر عباس طاهرپور

نشانی نویسنده‌ی مسئول: ایران - قزوین - بلوار دانشگاه بین‌المللی امام خمینی (ره) - دانشگاه بین‌المللی امام خمینی (ره) - دانشکده فنی و مهندسی - گروه مهندسی برق.

رادپوشناختی سنتی [۹]، فرض می‌شود که کاربر اولیه در کل زمان دوره حسگری همیشه حضور دارد و یا این‌که در کل دوره غایب است. در مرجع [۱۰]، نویسندگان تنها وارد شدن و خارج شدن سیگنال کاربر اولیه در طی دوره حسگری کاربر ثانویه را در نظر گرفته‌اند، ولی ترافیک مهاجم تقلیدکننده کاربر اولیه هم چنان موضوعی است که به آن پرداخته نشده است. در مقالات مرتبط [۵، ۶، ۷]، این مطلب فرض می‌شود که مهاجم تقلیدکننده کاربر اولیه در طی دوره حسگری کاربر ثانویه همیشه وجود دارد و یا به‌طور کامل غایب است. برخلاف کارهایی که تاکنون در مبحث امنیت شبکه‌ها صورت گرفته است، در عمل یک مهاجم نمی‌تواند در تمام زمان‌ها حمله نماید، زیرا اگر مهاجمان تمام مدت کانال را اشغال نمایند و یا نتایج تحریف‌شده گزارش نمایند، مرکز تصمیم‌گیری آن‌ها را به‌آسانی شناسایی می‌نماید. یک راهکار مناسب مهاجمان برای غلبه بر این موضوع، حمله در زمان‌های خاص است.

هدف از این مقاله معرفی مهاجمی هوشمند و ارائه مدلی ریاضی برای رفتار آن است، زمانی که کاربر اولیه طیف را ترک می‌کند و یا زمانی که کاربر اولیه وجود ندارد، با تقلید رفتار کاربر اولیه وارد کانال می‌شود و طیف را در اختیار خود می‌گیرد. برای مدل نمودن ریاضی، برخلاف کارهای گذشته از زنجیره مارکوف پیوسته زمان استفاده



شکل (۱): شبکه رادپوشناختی ارائه‌شده، در حضور مهاجم هوشمند تقلیدکننده کاربر اولیه و مهاجمان تحریف‌کننده اطلاعات حسگری.

خواهد شد و پس از معرفی این مهاجم هوشمند، به مطالعه تأثیر آن بر روی عملکرد و برون‌دهی شبکه کاربران ثانویه پرداخته خواهد شد. مهاجم هوشمند به‌دقت رفتار کاربر اولیه را تحت نظر می‌گیرد تا با شبکه کاربر اولیه تداخل پیش نیاید، چراکه این امر مهندسین طراح را از وجود مهاجم آگاه می‌سازد و این موضوع برای مهاجمان مطلوب نیست، درحالی‌که در کارهای گذشته که به تحلیل حضور مهاجم تقلیدکننده کاربر اولیه پرداخته‌اند [۶، ۷]، در بسیاری از موارد، سیگنال مهاجم اکثر اوقات هم‌زمان با ورود کاربر اولیه به کار خود ادامه می‌داد و این امر سبب می‌شد که آن‌ها به‌سادگی شناخته می‌شدند.

با ارائه سرویس‌های متعدد مبتنی بر مخابرات بی‌سیم پیدا کردن راه‌هایی که سبب افزایش کارایی طیف شود به یک ضرورت تبدیل شده است. در شبکه‌های رادپوشناختی^۱ کاربران ثانویه^۲، به‌طور مداوم طیف را حس می‌کنند تا حفره‌های طیفی آن را شناسایی نمایند و در زمان‌هایی که کاربر اولیه روی طیف حضور ندارد، اطلاعات خود را روی باند فرکانسی بفرستند. یک کاربر ثانویه، ممکن است به علت طبیعت بدطینت^۳ بودن و یا خودخواه^۴ بودن خود اطلاعات غلط به شبکه رادپوشناختی القا کند. واضح است که به علت طراحی ذاتی، انعطاف‌پذیری و آزادی استفاده از حفره‌های طیفی فضای بازی در اختیار مهاجمان قرار داده می‌شود و این امر شبکه رادپوشناختی را مستعد انواع آسیب‌پذیری‌ها می‌کند.

از میان حمله‌های متفاوتی که یک شبکه رادپوشناختی با آن مواجه است، حمله‌های تقلیدکننده کاربر اولیه^۵ و حمله‌های تحریف‌کننده اطلاعات حسگری طیفی^۶ عملکرد شبکه رادپوشناختی را به‌شدت تحت تأثیر قرار می‌دهند. در حمله‌های تقلیدکننده رفتار کاربر اولیه، مهاجمان با تقلید خصوصیات سیگنال کاربر اولیه^۷ قانونی مانع استفاده سایر کاربران ثانویه از طیف می‌شوند. به‌عنوان مثال در مراجع [۱، ۲]، نویسندگان به معرفی این نوع از حمله‌های تقلیدکننده کاربر اولیه پرداخته‌اند. مهاجمان تحریف‌کننده اطلاعات حسگری طیفی یا مهاجمان بی‌زاسی^۸ در شبکه‌های رادپوشناختی، با تغییر اطلاعات حسگری طیفی^۹ ممکن است سبب شوند که کاربران ثانویه نتوانند به‌درستی حضور کاربر اولیه را تشخیص بدهند. این نوع مهاجمان از ماهیت مشارکتی بودن شبکه‌های رادپوشناختی سوءاستفاده می‌نمایند، به این شکل که مهاجم، اطلاعات حسگری طیفی غلط به مرکز ترکیب می‌فرستد، بنابراین مرکز ترکیب در مورد قابل‌استفاده بودن طیف دچار اشتباه می‌شود. در مرجع [۳]، تحلیل حمله‌های تحریف‌کننده اطلاعات حسگری طیفی مشارکتی و غیر مشارکتی ارائه شده است. طی سال‌های اخیر، محققان به دنبال مدل‌هایی از شبکه‌های رادپوشناختگر بوده‌اند که به واقعیت سامانه‌های مخابراتی نزدیک‌تر باشند [۴]. برای مقابله با انواع مهاجمانی که به صورتی ساده و بدون در نظر گرفتن تنظیمات اساسی شبکه‌های رادپوشناختی حمله می‌نمایند، راه‌کارهایی نیز ارائه شده است [۵، ۶]. به‌عنوان نمونه، در مرجع [۷]، نویسندگان یک شبکه رادپوشناختی اقتضایی متحرک^{۱۰}، با در نظر گرفتن ارتباط فضایی فضایی بین کاربران ثانویه و با حضور مهاجم تقلیدکننده کاربر اولیه سنتی ارائه نموده‌اند و سپس به ارزیابی عملکرد این شبکه تحت پارامترهای متفاوت پرداخته‌اند. ترافیک کاربران از مسائلی است که طی سال‌های اخیر توجه محققان را در شبکه‌های بی‌سیم عملی جلب کرده است [۸]، دلیل این امر این است که در عمل، در یک شبکه رادپوشناختی، کاربر اولیه در هر زمان که بخواهد می‌تواند وارد طیف شود و یا از آن خارج شود؛ درحالی‌که در مدل‌های شبکه‌های

۲- مدل شبکه رادیوشناختی و فرضیات اصلی

شکل ۱، ساختار ارائه شده برای شبکه رادیوشناختی جدید و با حضور مهاجم هوشمند تقلیدکننده رفتار کاربر اولیه و مهاجمان تحریف کننده اطلاعات حسگری، را به تصویر می کشد. در این شبکه یک مهاجم تقلیدکننده رفتار کاربر اولیه وجود دارد که به صورت هوشمند در نبود کاربر اولیه، با تقلید ویژگی های سیگنال کاربر اولیه وارد طیف می شود و سعی در فریب دادن کاربران ثانویه دیگر دارد تا به طور خودخواهانه طیف را در اختیار خود بگیرد؛ از طرف دیگر به طور هم زمان چندین مهاجم تحریف کننده اطلاعات حسگری که حتماً دارای هدف خودخواهانه نیستند در شبکه رادیو شناختگر مشارکتی ارائه شده پخش شده اند. مهاجمان تحریف کننده اطلاعات حسگری که در نبود کاربر اولیه قانونی، از وارد شدن مهاجم هوشمند تقلیدکننده رفتار کاربر اولیه به طیف آگاه می شوند، با ارسال پیغام پر بودن کانال به مرکز ترکیب سبب می شوند که مرکز ترکیب در اتخاذ تصمیم صحیح درباره کانال دچار مشکل بشود و حکم به پر بودن کانال توسط کاربر اولیه نماید که در نتیجه بقیه کاربران ثانویه نیز از حضور در طیف خودداری می نمایند و راه برای استفاده هر چه خودخواهانه تر مهاجم هوشمند باز می شود. این مقاله حاوی پارامترهای زیادی است، برای پرهیز از ابهام در درک مطالب، جدول ۱ که شامل پارامترهای اساسی

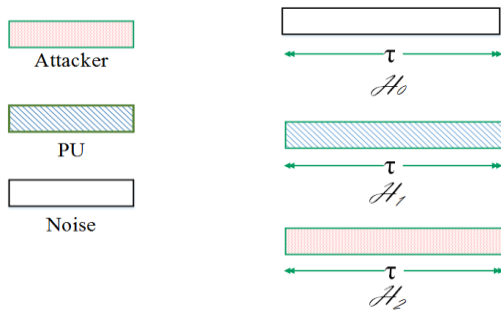
جدول (۱): پارامترها و تعریف های اصلی

| پارامتر | تعریف |
|------------|--|
| n_ℓ | نمونه های به دست آمده از نویز گاوسی سفید جمع شونده |
| s_ℓ | نمونه های سیگنال کاربر اولیه |
| w_ℓ | نمونه های سیگنال مهاجم تقلیدکننده کاربر اولیه |
| τ | طول زمان حسگری طیفی |
| L | تعداد کل نمونه های جمع شده از کانال در طی دوره حسگری |
| J | تعداد کل نمونه های جمع شده در یک قاب یا دوره تناوب |
| γ_p | نسبت سیگنال به نویز ارسال شده از کاربر اولیه |
| γ_w | نسبت سیگنال به نویز ارسال شده از مهاجم هوشمند |
| γ_s | نسبت سیگنال به نویز فرستنده کاربر ثانویه |
| C_j | ظرفیت کانال تحت فرضیه \mathcal{H}_j |
| R_{H_j} | برون دهی در دسترس شبکه تحت فرضیه \mathcal{H}_j |
| R_N | برون دهی در دسترس متوسط شبکه ثانویه |

است، ارائه شده است. در ساختار قاب بندی فرض شده شبکه، هر قاب شامل یک شکاف زمانی برای حسگری (τ) و یک شکاف زمانی برای انتقال اطلاعات است. تعداد نمونه های جمع شده از کانال در دوره حسگری L فرض می شود. در شکل ۲، مدل حسگری طیفی سنتی که مهاجم و یا کاربر اولیه در کل دوره حسگری، حضور دارند نمایش داده شده است. فرایند حسگری طیفی سنتی به شکل زیر فرمول بندی می شود [۷]:

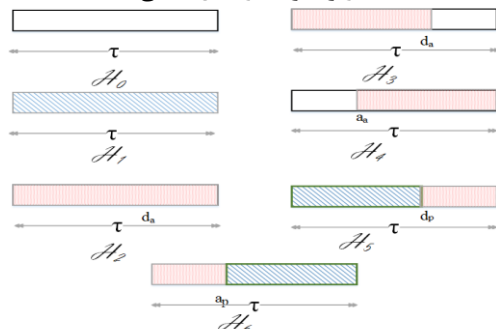
$$E = \begin{cases} \sum_{\ell=1}^L n_\ell^2 & , \mathcal{H}_0 \\ \sum_{\ell=1}^L (s_\ell + n_\ell)^2 & , \mathcal{H}_1 \\ \sum_{\ell=1}^L (w_\ell + n_\ell)^2 & , \mathcal{H}_2 \end{cases} \quad (1)$$

در عبارت ۱، $n_\ell, \forall \ell \in \{1, \dots, L\}$ ، نمونه های به دست آمده از نویز گاوسی سفید جمع شونده، $s_\ell, \forall \ell \in \{1, \dots, L\}$ ، نمونه های سیگنال کاربر اولیه، $w_\ell, \forall \ell \in \{1, \dots, L\}$ ، نمونه های سیگنال مهاجم تقلیدکننده کاربر اولیه و E خروجی آشکارساز انرژی است. \mathcal{H}_0 نمایش دهنده فرضیه ای است که کاربر اولیه و مهاجم همواره در طی دوره حسگری غایب هستند و بنابراین، خروجی آشکارساز فقط شامل نویز می شود، در فرضیه \mathcal{H}_1 ، در طی دوره حسگری کاربر اولیه همیشه حضور دارد و در نتیجه مهاجم غایب است و در فرضیه \mathcal{H}_2 در نبود کاربر اولیه، مهاجم از فرصت پیش رو استفاده می کند و در طیف همواره حضور دارد و با تقلید رفتار کاربر اولیه سعی می کند از ورود سایر کاربران ثانویه جلوگیری نماید. در شکل ۳ ترافیک کاربر اولیه همراه با مهاجم هوشمندی که به تقلید رفتار کاربر اولیه می پردازد و از ترافیک کاربر اولیه به عنوان فرصت حمله استفاده می کند، ارائه شده است. در این مدل فرض می شود که کاربر اولیه و مهاجم هوشمند تقلیدکننده کاربر اولیه حداکثر یک بار در طی دوره حسگری در هر قاب تغییر حالت می دهند که هر بار با خارج شدن کاربر اولیه مهاجم تقلیدکننده کاربر اولیه به سرعت وارد طیف می شود. فرض یک بار تغییر وضعیت برای این است که طول قاب به اندازه کافی کوچک است که دو بار تغییر وضعیت



شکل (۲): وضعیت شبکه (مهاجم و کاربر اولیه) طی دوره حسگری

کاربر ثانویه در مدل سنتی



شکل (۳): وضعیت شبکه (مهاجم و کاربر اولیه) طی دوره

حسگری کاربر ثانویه در مدل جدید

دادن در یک قاب چندان عملی به نظر نمی‌آید؛ بنابراین انتظار می‌رود که تعداد فرضیه‌ها برای آزمون فرضیه در این مدل افزایش پیدا نماید که این فرضیه‌ها در ۲ بررسی شده‌اند. در ۲، عبارت‌های d_p, a_a, d_a و a_p به ترتیب نشانگر لحظاتی که مهاجم کانال را ترک می‌کند یا در نبود کاربر اولیه وارد کانال می‌شود، لحظه‌ای که کاربر اولیه کانال را ترک می‌کند و یا لحظه‌ای که وارد کانال می‌شود، می‌باشند.

$$E = \begin{cases} \sum_{\ell=1}^L n_{\ell}^2 & , \mathcal{H}_0 \\ \sum_{\ell=1}^L (s_{\ell} + n_{\ell})^2 & , \mathcal{H}_1 \\ \sum_{\ell=1}^L (w_{\ell} + n_{\ell})^2 & , \mathcal{H}_2 \\ \sum_{\ell=1}^{d_a} (w_{\ell} + n_{\ell})^2 + \sum_{\ell=d_a+1}^L n_{\ell}^2 & , \mathcal{H}_3 \\ \sum_{\ell=1}^{a_a} n_{\ell}^2 + \sum_{\ell=a_a+1}^L (w_{\ell} + n_{\ell})^2 & , \mathcal{H}_4 \\ \sum_{\ell=1}^{d_p} (s_{\ell} + n_{\ell})^2 + \sum_{\ell=d_p+1}^L (w_{\ell} + n_{\ell})^2 & , \mathcal{H}_5 \\ \sum_{\ell=1}^{a_p} (w_{\ell} + n_{\ell})^2 + \sum_{\ell=a_p+1}^L (s_{\ell} + n_{\ell})^2 & , \mathcal{H}_6 \end{cases} \quad (2)$$

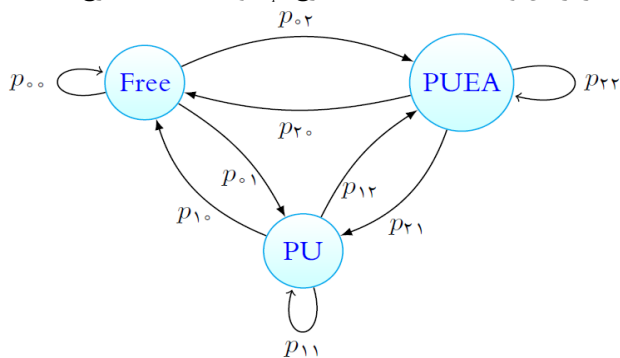
فرضیه‌های $\mathcal{H}_0, \mathcal{H}_1$ و \mathcal{H}_2 مشابه حسگری طیفی، بدون در نظر گرفتن ترافیک کاربران است. چون مهاجم، هوشمند در نظر گرفته شده است ممکن است مهاجم پس از مدتی حضور در طیف به دلیل ترس از شناخته شدن تصمیم به ترک طیف نماید که این حالت با فرضیه \mathcal{H}_3 نمایش داده شده است، هم‌چنین ممکن است که مهاجم تصمیم بگیرد اندکی دیرتر در طی زمان حسگری در طیف ظاهر شود که با فرضیه \mathcal{H}_4 مشخص شده است. حالت بعد حالتی است که کاربر اولیه به تعداد d_p نمونه زمانی در طیف حضور دارد و سپس تصمیم به ترک طیف می‌گیرد، این امر سبب می‌شود که مهاجم هوشمند از فرصت به‌دست‌آمده استفاده نماید و در طیف حضور یابد که سبب شکل‌گیری فرضیه \mathcal{H}_5 می‌شود. \mathcal{H}_6 بیانگر فرضیه‌ای است که در ابتدای دوره حسگری کاربر اولیه در طیف حضور ندارد و لذا مهاجم هوشمند سعی در اختیار گرفتن طیف را دارد، اما پس از مدتی با ظاهر شدن کاربر اولیه مهاجم هوشمند به‌منظور جلوگیری از شناسایی و دستگیری خود، به‌سرعت طیف را ترک می‌کند.

۳- مدل نمودن هم‌زمان ترافیک کاربر اولیه و مهاجم هوشمند تقلیدکننده کاربر اولیه

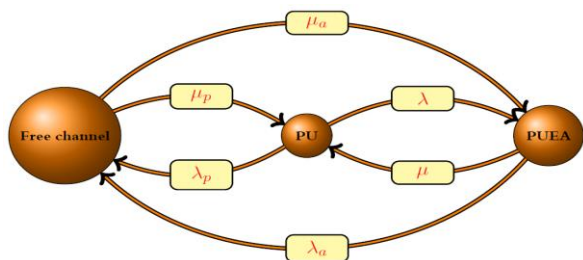
مهم‌ترین موضوع در مدل کردن ترافیک شبکه، به دست آوردن مدلی ریاضی برای رفتار کاربر اولیه و مهاجم هوشمند تقلیدکننده کاربر اولیه است تا بتوان در محاسبه عملکرد شبکه رادیوشناختی و هم‌چنین محاسبه برون‌دهی شبکه کاربران ثانویه، از آن بهره برد. با توجه به مشاهدات و اندازه‌گیری‌های صورت گرفته می‌توان فعالیت کاربران در

باند‌های فرکانسی متفاوت را به‌صورت زنجیره مارکوف مدل کرد برخلاف کارهای قبلی در زمینه مهاجم تقلیدکننده کاربر اولیه که بیشتر از زنجیره مارکوف دو‌حالتی برای مدل‌سازی ریاضی استفاده می‌گردید [۱۱، ۱۲]، در این مقاله مهاجم هوشمند به‌صورت یک حالت مستقل در روابط تحلیلی مارکوف پیوسته زمان در نظر گرفته می‌شود. در مدل مارکوف وابسته به زمان، کاربر اولیه و مهاجم هوشمند تقلیدکننده کاربر اولیه باهم یک فرایند مارکوف سه‌حالتی تشکیل می‌دهند. برای مدل نمودن ترافیک شبکه، زنجیره مارکوف $X = \{X(t) : t \geq 0\}$ که پارامتر زمان پیوسته $t \in [0, \infty)$ را شامل می‌شود، در نظر گرفته شده است. فرض می‌شود که Q ماتریس نرخ زنجیره مارکوف X و $P(t) \geq C$ تابع ماتریس گذار حالت آن باشد. این زنجیره مارکوف به‌صورت شکل ۴، در نظر گرفته شده است.

فضای حالت زنجیره مارکوف پیوسته X به‌صورت $S = \{0, 1, 2\}$ در نظر گرفته شده است که در آن ۰ بیان‌گر وضعیتی است که کاربر اولیه و مهاجم هوشمند تقلیدکننده کاربر اولیه در کانال وجود ندارند و به‌عبارت‌دیگر کانال خالی است. ۱ نشان‌گر حالتی است که کاربر اولیه در طیف حضور دارد و بنابراین مهاجم هوشمند تقلیدکننده کاربر اولیه از حضور در طیف خودداری می‌کند و حالت ۲ نشان‌گر وضعیتی است که مهاجم هوشمند تقلیدکننده کاربر اولیه وارد طیف شده است. گذار بین حالت‌های متفاوت داده شده همان‌طور که در شکل ۵، نشان داده شده است با نرخ‌های زیر در نظر گرفته شده است: وقتی که سیستم در حالت ۰ است، زنجیره تلاش می‌کند با نرخ μ_p به حالت ۱ و با نرخ μ_a به حالت ۲ وارد شود. هنگامی که سیستم در وضعیت ۱ است، تغییر از این وضعیت به حالت ۰ با نرخ λ_p و به حالت ۲ با نرخ λ



شکل (۴): احتمال‌های گذر مربوط به وضعیت سیستم حسگری در مدل ترافیک مارکوف وابسته به زمان



شکل (۵): نمودار حالت و نرخ تغییر گذار در مدل ترافیک مارکوف وابسته به زمان

$$P(\mathcal{H}_3) = \left(\sum_{d_a=1}^L a_b P_e P_{22}^{d_a} P_{20} P_{00}^{(J-d_a-1)} \right),$$

$$P(\mathcal{H}_4) = \left(\sum_{a_a=1}^L P_e a_e P_{00}^{a_a} P_{02} P_{22}^{(J-a_a-1)} \right),$$

$$P(\mathcal{H}_5) = \left(\sum_{d_p=1}^L P_b a_e P_{11}^{d_p} P_{12} P_{22}^{(J-d_p-1)} \right),$$

$$P(\mathcal{H}_6) = \left(\sum_{a_p=1}^L a_b P_e P_{22}^{a_p} P_{21} P_{11}^{(J-a_p-1)} \right),$$

۴- محاسبه عملکرد و برون‌دهی شبکه رادیو-شناختی در حضور مهاجم هوشمند تقلیدکننده کاربر اولیه

در این بخش به مطالعه تأثیر حضور مهاجم هوشمند تقلیدکننده کاربر اولیه بر عملکرد شبکه رادیوشناختی و برون‌دهی^{۱۱} شبکه کاربران ثانویه پرداخته می‌شود. به‌طور کلی برون‌دهی شبکه به نرخ داده‌های ارسال شده از طریق یک کانال مخابراتی که با موفقیت به مقصد می‌رسند، گفته می‌شود. با استفاده از قانون حد مرکزی، برای تعداد نمونه‌های بزرگ، تابع چگالی احتمال E در رابطه (۲) تحت هر فرضیه $\mathcal{H}_j, j \in \{0, \dots, 6\}$ می‌تواند با یک توزیع گاوسی تقریب زده شود [۱۲]. با استفاده از مقادیر میانگین و واریانس توزیع گاوسی تقریبی می‌توان احتمال‌های هشدار غلط شرطی و آشکارسازی شرطی تحت هر فرضیه را به دست آورد که اثبات و مقادیر میانگین و واریانس در مرجع [۱۵] آورده شده‌اند. به این ترتیب، احتمال هشدار غلط شرطی برای فرضیه \mathcal{H}_0 ، در مدل جدید حسگری طیفی به‌صورت زیر قابل محاسبه خواهد بود:

$$P_{fa, \mathcal{H}_0}(\eta, L) = \Pr\{E > \eta | \mathcal{H}_0\}_{\rightarrow E \sim N(L\sigma_n^2, 2L\sigma_n^4)} = Q\left(\frac{\eta - L\sigma_n^2}{\sqrt{2L}\sigma_n^2}\right) = Q\left(\frac{\eta}{\sqrt{2L}\sigma_n^2} - \sqrt{\frac{L}{2}}\right). \quad (7)$$

احتمال آشکارسازی شرطی تحت فرضیه \mathcal{H}_1 :

$$P_{d, \mathcal{H}_1}(\eta, L) = \Pr\{E > \eta | \mathcal{H}_1\}_{\rightarrow E \sim N(L(\gamma_p+1)\sigma_n^2, 2L(2\gamma_p+1)\sigma_n^4)} = Q\left(\frac{\eta}{\sqrt{2L(2\gamma_p+1)\sigma_n^2}} - (\gamma_p+1)\sqrt{\frac{L}{4\gamma_p+2}}\right). \quad (8)$$

احتمال هشدار غلط شرطی تحت فرضیه \mathcal{H}_2 :

$$P_{fa, \mathcal{H}_2}(\eta, L) = \Pr\{E > \eta | \mathcal{H}_2\}_{\rightarrow E \sim N(L(\gamma_w+1)\sigma_n^2, 2L(2\gamma_w+1)\sigma_n^4)} = Q\left(\frac{\eta}{\sqrt{2L(2\gamma_w+1)\sigma_n^2}} - (\gamma_w+1)\sqrt{\frac{L}{4\gamma_w+2}}\right). \quad (9)$$

صورت می‌پذیرد و وقتی که سیستم در وضعیت ۲ است، تغییر از این وضعیت به حالت ۰ با نرخ λ_a و به حالت ۱ با نرخ μ صورت می‌پذیرد که مقادیر پارامترهای ترافیک با استفاده از روش‌های آماری قابل تخمین زدن هستند [۱۳]. با به دست آوردن این مقادیر، احتمال این‌که کاربر اولیه قبل از t ثانیه وارد شود به‌صورت آماری با رابطه (۳) محاسبه شود و در صورتی که این احتمال از یک سطح آستانه تعیین‌شده توسط مهاجم هوشمند، کمتر باشد، حمله انجام شود.

$$P\{0 \leq X \leq t\} = \int_0^t \frac{1}{\lambda_p} e^{-\frac{1}{\lambda_p}x} dx = 1 - e^{-\frac{t}{\lambda_p}} \geq \varepsilon, \quad (3)$$

ماتریس نرخ و یا Q-ماتریس زنجیره مارکوف X برابر است با:

$$Q = \begin{pmatrix} -(\mu_p + \mu_a) & \mu_p & \mu_a \\ \lambda_p & -(\lambda_p + \lambda) & \lambda \\ \lambda_a & \mu & -(\lambda_a + \mu) \end{pmatrix}. \quad (4)$$

ماتریس گذار حالت زنجیره مارکوف ارائه‌شده به‌صورت رابطه (۵) قابل‌بیان خواهد بود که نحوه محاسبه و مقادیر عناصر ماتریس گذار P(t) به تفکیک، در ضمیمه اثبات شده‌اند.

$$P(t) = \begin{pmatrix} P_{00}(t) & P_{01}(t) & P_{02}(t) \\ P_{10}(t) & P_{11}(t) & P_{12}(t) \\ P_{20}(t) & P_{21}(t) & P_{22}(t) \end{pmatrix}. \quad (5)$$

احتمال‌های اولیه هر فرضیه در آزمون فرضیه ارائه‌شده در (۲)، با در نظر گرفتن کل نمونه‌های یک دوره تناوب به‌صورت رابطه (۶)، محاسبه می‌شود که با استفاده از عناصر ماتریس گذار و ضرب تعداد حالات رخداد احتمال‌های گذار زنجیره مارکوف که در آن فرضیه رخ می‌دهد، به دست می‌آید [۱۴] و در آن J تعداد کل نمونه‌های جمع شده در

$$\text{یک قاب یا دوره تناوب، } p_b = \frac{\lambda_p}{\lambda_p + \mu_p}, \quad p_e = \frac{\mu_p}{\lambda_p + \mu_p}$$

بودن کانال در هر لحظه توسط کاربر اولیه و مهاجم هوشمند تقلیدکننده کاربر اولیه می‌باشند، سایر پارامترها در جدول ۱ معرفی شده‌اند.

$$P(\mathcal{H}_0) = p_e a_e p_{00}^J + \left(\sum_{a_p=L+1}^{J-1} p_e P_{00}^{a_p} P_{01} P_{11}^{(J-a_p-1)} \right) + \left(\sum_{a_a=L+1}^{J-1} a_e P_{00}^{a_a} P_{02} P_{22}^{(J-a_a-1)} \right),$$

$$P(\mathcal{H}_1) = p_b a_e p_{11}^J + \left(\sum_{d_p=L+1}^{J-1} P_b P_{11}^{d_p} P_{10} P_{00}^{(J-d_p-1)} \right) + \left(\sum_{a_a=L+1}^{J-1} a_e P_{00}^{a_a} P_{02} P_{22}^{(J-a_a-1)} \right),$$

$$P(\mathcal{H}_2) = p_e a_b p_{22}^J + \left(\sum_{d_a=L+1}^{J-1} a_b P_{22}^{d_a} P_{20} P_{00}^{(J-d_a-1)} \right) + \left(\sum_{a_p=L+1}^{J-1} P_e P_{00}^{a_p} P_{01} P_{11}^{(J-a_p-1)} \right), \quad (6)$$

$$\begin{cases} P_{d,\mathcal{H}_6}(\eta, L, a_p) = Q\left(\frac{\eta - (L - a_p)(\gamma_p + 1)\sigma_n^2}{\sqrt{2(L - a_p)(2\gamma_p + 1)\sigma_n^2}}\right), \\ P_{fa,\mathcal{H}_6}(\eta, L, a_p) = Q\left(\frac{\eta - a_p(\gamma_p + 1)\sigma_n^2}{\sqrt{2a_p(2\gamma_w + 1)\sigma_n^2}}\right). \end{cases} \quad (13)$$

در نهایت، احتمال هشدار غلط و احتمال آشکارسازی غیرشرطی را می‌توان با میانگین‌گیری از احتمال‌های شرطی به دست آمده در بالا بر روی احتمال‌های رخ دادن فرضیه‌ها به دست آورد.

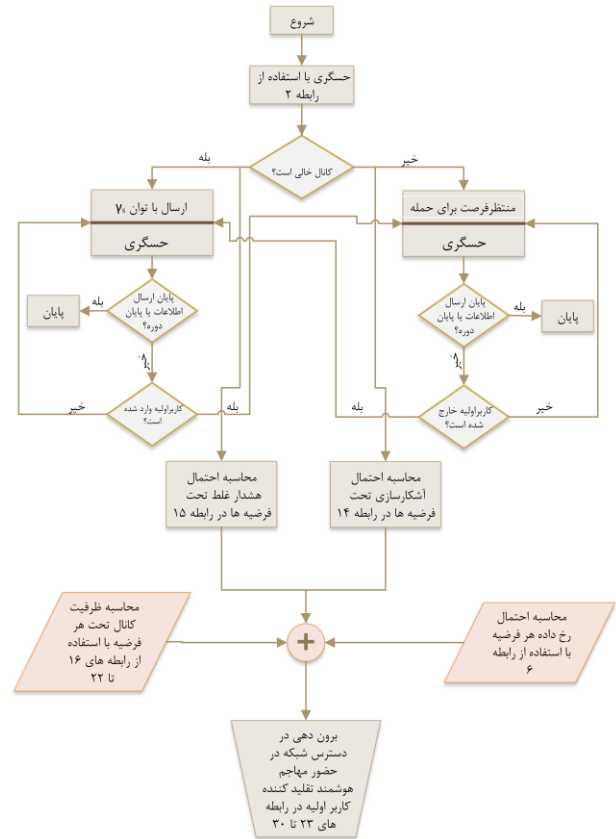
$$\begin{aligned} \bar{P}_{fa}(\eta, L) &= \frac{P(\mathcal{H}_0)P_{fa,\mathcal{H}_0}(\eta, L) + P(\mathcal{H}_2)P_{fa,\mathcal{H}_2}(\eta, L)}{1 - P(\mathcal{H}_1)} \\ &+ \frac{P(\mathcal{H}_3)}{1 - P(\mathcal{H}_1)} \sum_{d_a=1}^L P_{fa,\mathcal{H}_3}(\eta, L, d_a) \\ &+ \frac{P(\mathcal{H}_4)}{1 - P(\mathcal{H}_1)} \sum_{a_p=1}^L P_{fa,\mathcal{H}_4}(\eta, L, a_p) \\ &+ \frac{P(\mathcal{H}_5)}{1 - P(\mathcal{H}_1)} \sum_{d_p=1}^L P_{fa,\mathcal{H}_5}(\eta, L, d_p) \\ &+ \frac{P(\mathcal{H}_6)}{1 - P(\mathcal{H}_1)} \sum_{a_p=1}^L P_{fa,\mathcal{H}_6}(\eta, L, a_p), \end{aligned} \quad (14)$$

$$\begin{aligned} \bar{P}_d(\eta, L) &= \frac{P(\mathcal{H}_1)P_{d,\mathcal{H}_1}(\eta, L)}{P(\mathcal{H}_1) + P(\mathcal{H}_5) + P(\mathcal{H}_6)} \\ &+ \frac{P(\mathcal{H}_5)}{P(\mathcal{H}_1) + P(\mathcal{H}_5) + P(\mathcal{H}_6)} \sum_{d_p=1}^L P_{d,\mathcal{H}_5}(\eta, L, d_p) \\ &+ \frac{P(\mathcal{H}_6)}{P(\mathcal{H}_1) + P(\mathcal{H}_5) + P(\mathcal{H}_6)} \sum_{a_p=1}^L P_{d,\mathcal{H}_6}(\eta, L, a_p), \end{aligned} \quad (15)$$

که η سطح آستانه در کاربر ثانویه با نسبت سیگنال به نویز $(\gamma_p = \frac{\sigma_p^2}{\sigma_n^2})$ ارسال شده از کاربر اولیه و با نسبت سیگنال به نویز $(\gamma_w = \frac{\sigma_w^2}{\sigma_n^2})$ ارسال شده از مهاجم هوشمند تقلیدکننده کاربر اولیه است، هم‌چنین $Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty \exp\left(-\frac{u^2}{2}\right) du$ تابع متمم توزیع نرمال گاوسی است. برای محاسبه برون‌دهی شبکه کاربران ثانویه در ابتدا به مقدار ظرفیت کانال تحت هر فرضیه نیاز است. در فرضیه \mathcal{H}_0 ، ظرفیت کانال تحت تأثیر ترافیک کاربر اولیه و مهاجم هوشمند قرار می‌گیرد و به صورت لگاریتم در مبنای ۲ نسبت سیگنال به نویز سیگنال مطلوب γ_s به نسبت سیگنال به نویز سیگنال‌های دیگر، به صورت زیر قابل محاسبه است:

$$C_0(a_p, a_a) = \log_2 \left(1 + \frac{\gamma_s}{1 + \frac{J - a_p}{J - L} \gamma_p + \frac{J - a_a}{J - L} \gamma_w} \right), \quad (16)$$

که γ_s نسبت سیگنال به نویز فرستنده کاربر ثانویه و یا به عبارت دیگر نسبت سیگنال به نویز لینک ثانویه در یک انتقال نقطه‌به‌نقطه در شبکه کاربران ثانویه است. در فرضیه \mathcal{H}_1 ، کاربر اولیه در طول مدت حسگری در طیف حضور دارد، بنابراین ظرفیت کانال خواهد شد:



شکل (۶): بلوک دیاگرام روش پیشنهادی به همراه روابط استفاده‌شده در مقاله

به همین ترتیب، احتمال هشدار غلط شرطی که ناشی از حضور مهاجم هوشمند تقلیدکننده کاربر اولیه در کانال است، با شرط روی d_a برابر است با:

$$P_{fa,\mathcal{H}_3}(\eta, L, d_a) = Q\left(\frac{\eta - L - d_a \gamma_w}{2\sqrt{\frac{L}{2} + d_a \gamma_w}}\right). \quad (10)$$

در فرضیه \mathcal{H}_4 احتمال هشدار غلط شرطی ناشی از حضور مهاجم هوشمند، با شرط روی a_a برابر است با:

$$P_{fa,\mathcal{H}_4}(\eta, L, a_a) = Q\left(\frac{\eta + \gamma_w(a_a - L) - L}{\sqrt{2L + (4L - 4a_a)\gamma_w}}\right). \quad (11)$$

احتمال آشکارسازی شرطی و احتمال هشدار غلط شرطی تحت فرضیه \mathcal{H}_5 با شرط بر روی d_p به صورت زیر قابل محاسبه خواهند بود:

$$\begin{cases} P_{d,\mathcal{H}_5}(\eta, L, d_p) = Q\left(\frac{\eta - d_p(\gamma_p + 1)\sigma_n^2}{\sqrt{2d_p(2\gamma_p + 1)\sigma_n^2}}\right), \\ P_{fa,\mathcal{H}_5}(\eta, L, d_p) = Q\left(\frac{\eta - (L - d_p)(\gamma_w + 1)\sigma_n^2}{\sqrt{2(L - d_p)(2\gamma_w + 1)\sigma_n^2}}\right). \end{cases} \quad (12)$$

احتمال آشکارسازی شرطی و احتمال هشدار غلط شرطی تحت فرضیه \mathcal{H}_6 با شرط بر روی a_p به صورت زیر قابل محاسبه خواهند بود:



$$R_N(\eta, L) = \sum_{j=0}^6 R_{\mathcal{H}_j}(\eta, L), \quad (23)$$

که عناصر آن به صورت عبارات (۲۴-۳۰) به دست می آیند.

$$R_{\mathcal{H}_0}(\eta, L) = (1 - \bar{P}_{ia}(\eta, L)) \left(\frac{T - \tau}{T} \right) (p_e a_e p_{00} C_0(J, J) + \sum_{a_p=L+1}^{J-1} \sum_{a_a=L+1}^{J-1} p_e a_e (p_{00}^a p_{01} p_{11}^{J-a_p-1} + p_{00}^a p_{02} p_{22}^{J-a_a-1}) C_0(a_p, a_a)), \quad (24)$$

$$R_{\mathcal{H}_1}(\eta, L) = (1 - \bar{P}_d(\eta, L)) \left(\frac{T - \tau}{T} \right) (p_b a_e p_{11} C_1(J, J) + \sum_{d_p=L+1}^{J-1} \sum_{a_a=L+1}^{J-1} p_b a_e (p_{11}^d p_{10} p_{00}^{J-d_p-1} + p_{00}^a p_{02} p_{22}^{J-a_a-1}) C_1(d_p, a_a)), \quad (25)$$

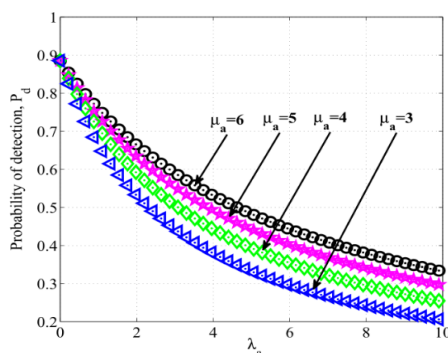
$$R_{\mathcal{H}_2}(\eta, L) = (1 - \bar{P}_{ia}(\eta, L)) \left(\frac{T - \tau}{T} \right) (p_e a_e p_{22} C_2(J, J) + \sum_{a_p=L+1}^{J-1} \sum_{a_a=L+1}^{J-1} p_e a_e (p_{00}^a p_{01} p_{11}^{J-a_p-1} + p_{22}^a p_{20} p_{00}^{J-a_a-1}) C_2(a_p, a_a)), \quad (26)$$

$$R_{\mathcal{H}_3}(\eta, L) = (1 - \bar{P}_{ia}(\eta, L)) \left(\frac{T - \tau}{T} \right) \times \sum_{d_a=1}^L p_e a_b p_{22}^d p_{20} p_{00}^{(J-d_a-1)} C_3(d_a), \quad (27)$$

$$R_{\mathcal{H}_4}(\eta, L) = (1 - \bar{P}_{ia}(\eta, L)) \left(\frac{T - \tau}{T} \right) \times \sum_{a_a=1}^L p_e a_e p_{00}^a p_{02} p_{22}^{(J-a_a-1)} C_4(a_a), \quad (28)$$

$$R_{\mathcal{H}_5}(\eta, L) = (1 - \bar{P}_{ia}(\eta, L)) (1 - \bar{P}_d(\eta, L)) \times \left(\frac{T - \tau}{T} \right) \sum_{d_p=1}^L p_b a_e p_{11}^d p_{12} p_{22}^{(J-d_p-1)} C_5(d_p), \quad (29)$$

$$R_{\mathcal{H}_6}(\eta, L) = (1 - \bar{P}_{ia}(\eta, L)) (1 - \bar{P}_d(\eta, L)) \times \left(\frac{T - \tau}{T} \right) \sum_{a_p=1}^L p_e a_b p_{22}^a p_{21} p_{11}^{(J-a_p-1)} C_6(a_p). \quad (30)$$



شکل (۷): احتمال آشکارسازی در مدل ترافیک مارکوف وابسته به زمان بر حسب λ_p و برای μ_p های متفاوت، برای $L = 40$ ، $\lambda_a = \mu_a = 5$ ، $\gamma_p = \gamma_w = -1dB$ و $T_s = 1ms$ ، $\lambda = \mu = 5$

$$C_1(d_p, a_a) = \log_2 \left(1 + \frac{\gamma_s}{1 + \frac{d_p - L}{J - L} \gamma_p + \frac{J - a_a}{J - L} \gamma_w} \right). \quad (17)$$

در فرضیه \mathcal{H}_2 ، کاربر اولیه در طول مدت حسگری در طیف حضور ندارد و لذا مهاجم هوشمند فرصتی برای استفاده از طیف پیدا می کند، بنابراین ظرفیت کانال خواهد شد:

$$C_2(d_a, a_p) = \log_2 \left(1 + \frac{\gamma_s}{1 + \frac{d_a - L}{J - L} \gamma_w + \frac{J - a_p}{J - L} \gamma_p} \right). \quad (18)$$

در فرضیه \mathcal{H}_3 ، فرض می شود که به طور کلی کاربر اولیه در طیف حضور نمی یابد در این حالت مهاجم هوشمند در طی زمان حسگری ابتدا مدتی در طیف ظاهر می شود اما سپس از ادامه حمله منصرف می شود و چون فرض شده است که کاربران در یک دوره تناوب فقط یکبار تغییر گذار می توانند بدهند، مهاجم هوشمند در طی دوره ارسال نیز در طیف حضور نمی یابد، لذا ظرفیت کانال برابر است با:

$$C_3 = \log_2(1 + \gamma_s). \quad (19)$$

در فرضیه \mathcal{H}_4 ، همانند حالت قبل فرض می شود که به طور کلی کاربر اولیه در طیف حضور نمی یابد در این حالت مهاجم هوشمند تقلیدکننده کاربر اولیه در طی زمان حسگری طیفی مدتی پس از ابتدای دوره حسگری به کانال می رسد و در طی دوره ارسال نیز باقی می ماند، بنابراین ظرفیت برابر خواهد شد با:

$$C_4 = \log_2 \left(1 + \frac{\gamma_s}{1 + \gamma_w} \right). \quad (20)$$

در فرضیه \mathcal{H}_5 ، کاربر اولیه ابتدا در طیف حضور دارد اما مدتی بعد از طیف خارج می شود و لذا در طی زمان دوره ارسال نیز نمی تواند وارد طیف شود و این بهترین فرصت برای مهاجم هوشمند است که وارد طیف شود و تا انتهای دوره نیز در طیف حضور یابد، در این حالت ظرفیت به صورت زیر خواهد بود:

$$C_5 = \log_2 \left(1 + \frac{\gamma_s}{1 + \gamma_w} \right). \quad (21)$$

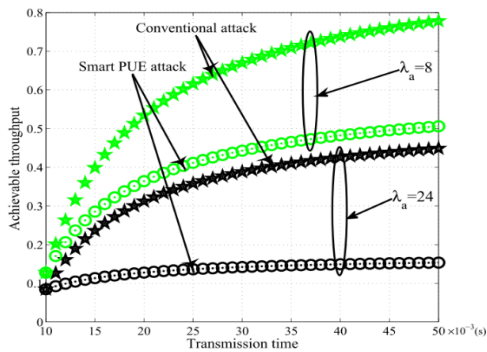
در فرضیه \mathcal{H}_6 ، مهاجم هوشمند ابتدا در طیف حضور می یابد اما با پی بردن به حضور کاربر اولیه، به سرعت از طیف خارج می شود و کاربر اولیه که وارد طیف شده است تا انتهای دوره تناوب نیز در طیف باقی می ماند؛ بنابراین ظرفیت کانال برابر خواهد بود با:

$$C_6 = \log_2 \left(1 + \frac{\gamma_s}{1 + \gamma_p} \right). \quad (22)$$

با انجام مراحل یادشده، ابزار موردنیاز برای محاسبه برون دهی شبکه رادیوشناختی با حضور مهاجم هوشمند تکمیل می شود و در نهایت برون دهی در دسترس متوسط شبکه ثانویه با جمع برون دهی در دسترس تحت تمام فرضیه ها [۱۴] به صورت زیر خواهد شد:

$$J = 65, L = 50, \mu_a = 24, \lambda_a = 10, \mu_p = \lambda = \mu = 5, \lambda_p = 30$$

$$\gamma_p = 1(W) = 0dB, \gamma_s = -1dB, \tau = 10ms, T_s = 1ms$$



شکل (۱۰): مقایسه برون‌دهی برای شبکه کاربران ثانویه در حمله‌های

سنتی و هوشمند، برحسب مدت‌زمان دوره انتقال و بر اساس $\lambda_p = 30$

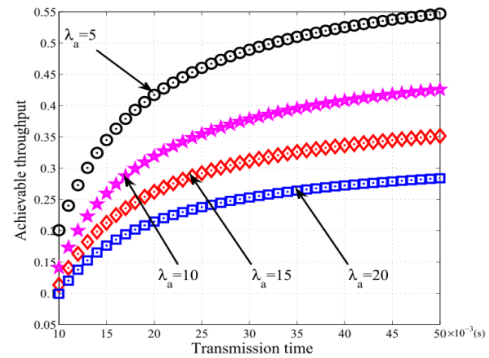
$$, \tau = 10ms, T_s = 1ms, J = 65, L = 50, \mu_a = 24, \mu_p = \lambda = \mu = 5$$

$$\gamma_p = \gamma_w = 1(W) = 0dB, \gamma_s = -1dB$$

شکل ۷، تأثیر ترافیک مهاجم هوشمند تقلیدکننده کاربر اولیه بر عملکرد آشکارساز را در مدل مارکوف وابسته برحسب λ_a برای μ_a های متفاوت نشان می‌دهد. همان‌طور که از شکل پیداست با افزایش مقدار λ_a ، احتمال آشکارسازی کاهش پیدا می‌کند، چون به‌طور میانگین مهاجم هوشمند مدت‌زمان بیشتری در طیف حضور دارد. همچنین افزایش در مقدار μ_a متناظر با افزایش در میانگین مدت‌زمانی است که کانال از مهاجم هوشمند خالی است که سبب افزایش احتمال آشکارسازی صحیح کاربر اولیه خواهد شد. شکل ۸، برون‌دهی در دسترس شبکه کاربران ثانویه برحسب مدت‌زمان دوره انتقال و برای شدت ترافیک و میانگین مدت‌زمان حضور مهاجم هوشمند متفاوت، به تصویر می‌کشد. همان‌طور که از شکل پیداست با افزایش مدت‌زمان انتقال اطلاعات، میزان برون‌دهی یا نرخ داده‌های ارسال شده از طریق کانال مخابراتی که با موفقیت به مقصد می‌رسند افزایش پیدا می‌کنند، دلیل این امر نیز افزایش مدت‌زمانی است که اطلاعات از طریق کانال ارسال می‌شوند. با افزایش λ_a یا به عبارتی افزایش میانگین مدت‌زمان حضور مهاجم هوشمند تقلیدکننده کاربر اولیه در طیف برون‌دهی همانند عملکرد شبکه رادیوشناختی کاهش

جدول (۳): مشخصات، ویژگی و نتایج حاصل از روش پیشنهادی

| ردیف | مشخصات، ویژگی و نتایج | حمله به شیوه سنتی | حمله مهاجم هوشمند تقلیدکننده کاربر اولیه ارائه شده |
|------|---------------------------|--|--|
| (۱) | حمله با استراتژی خاص | در نظر نمی‌گیرد حتی با وجود کاربر اولیه به حمله ادامه می‌دهد [۵] | مهاجم به‌دقت رفتار کاربر اولیه را تحت نظر می‌گیرد و در نبود سایر کاربران حمله می‌کند |
| (۲) | سطح حمله | لایه فیزیکی [۱۷] | لایه فیزیکی و توانایی حمله در ساختار قاب در لایه پیوند داده را دارد. |
| (۳) | تداخل یا شبکه کاربر اولیه | دارد | ندارد |
| (۴) | رفتار همکارانه | امکان‌پذیر نیست. | می‌تواند زمان حمله خود را |



شکل (۸): برون‌دهی در دسترس برای شبکه کاربران ثانویه برحسب

مدت‌زمان دوره انتقال و برای شدت ترافیک متفاوت و بر اساس

$$, \tau = 10ms, T_s = 1ms, J = 68, L = 40, \mu_p = \mu_a = \lambda = \mu = 5, \lambda_p = 30$$

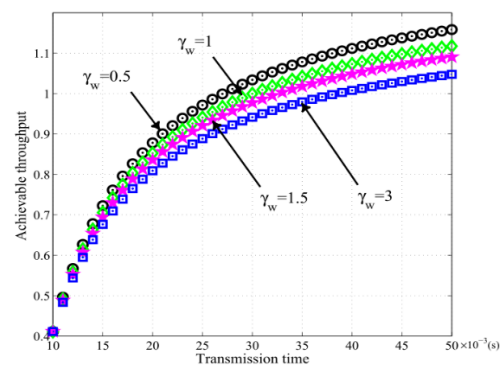
$$\gamma_p = \gamma_w = 1(W) = 0dB, \gamma_s = -1dB$$

۵- نتایج عددی و شبیه‌سازی

در این بخش نتایج شبیه‌سازی برای ارزیابی عملکرد شبکه رادیوشناختی و برون‌دهی شبکه کاربران ثانویه، در حضور مهاجم هوشمند تقلیدکننده کاربر اولیه ارائه شده است. در این مقاله از نرم‌افزار Matlab نسخه ۲۰۱۴ و سیگنال‌های با استاندارد پخش دیجیتال ویدیویی^{۱۲} و نسبت سیگنال به نویزهای متغیر برای انجام شبیه‌سازی استفاده شده است. به‌عنوان مثال با توجه به استاندارد پخش دیجیتال ویدیویی، طول قاب (T) و طول دوره ارسال (T-τ) به ترتیب برابر با (ms) ۶۰ ~ ۲۰ و (ms) ۵۰ ~ ۱۰ در نظر گرفته شده‌اند [۱۶]. سایر پارامترهای شبیه‌سازی نیز در جدول ۲ آورده شده‌اند.

جدول (۲): نمادها و عبارتهای استفاده شده در شبیه‌سازی

| نماد | تعریف |
|-------------------|--|
| T=20~60 (ms) | طول قاب |
| T-τ=10~50 (ms) | طول دوره‌ی ارسال |
| L = 40 ~ 50 | نمونه‌های جمع شده، در طول زمان دوره‌ی حسگری |
| J = 65 | نمونه‌های جمع شده، در طول یک دوره تناوب |
| $\gamma_s = -1dB$ | نسبت سیگنال به نویز در شبکه‌ی کاربران ثانویه |



شکل (۹): برون‌دهی برای شبکه کاربران ثانویه برحسب مدت‌زمان

دوره انتقال و برای نسبت سیگنال به نویزهای متفاوت و بر اساس

$$J = 65, L = 50, \lambda_a = 10, \mu_p = \lambda = \mu = 5, \lambda_p = 30$$

$$\gamma_p = \gamma_w = 1(W) = 0dB \text{ و } \gamma_s = -1dB, \tau = 10ms, T_s = 1ms$$

در شکل ۱۱، نیز همانند شکل ۱۰، همین مقایسه، برحسب مدت زمان دوره انتقال و برای پارامتر میانگین مدت زمان ماندگاری نمایی عدم حضور مهاجم هوشمند (μ_a) متفاوت، پرداخته شده است. افزایش μ_a در این حالت بدین معنی است که به طور میانگین مهاجم هوشمند مدت زمان کمتری در طیف حضور دارد و لذا تأثیر مخرب آن بر برون دهی شبکه ثانویه کمتر است که در نهایت منجر به افزایش برون دهی خواهد شد. در پایان مشخصات و ویژگی‌های روش پیشنهادی در جدول ۳ با مدل‌های سنتی حمله تقلیدکننده کاربر اولیه مقایسه شده- اند و نتایج حاصل از آن ارائه شده است.

۶- نتیجه گیری

در این مقاله به معرفی مهاجم هوشمندی پرداختیم که رفتار کاربر اولیه را در طی دوره حسگری کنترل می‌کند و زمانی که کاربر اولیه طیف را ترک می‌کند و یا زمانی که کاربر اولیه وجود ندارد، با تقلید رفتار کاربر اولیه وارد طیف می‌شود. سپس میحث حسگری طیفی با حضور این مهاجم هوشمند مورد بررسی قرار گرفت که برای مدل نمودن ترافیک کاربران از زنجیره مارکوف پیوسته زمان، بهره برده شد. به صورت تحلیلی عملکرد شبکه رادیوشناختی و هم‌چنین برای نخستین بار، برون‌دهی متوسط شبکه کاربران ثانویه در حضور مهاجم هوشمند تقلیدکننده کاربر اولیه مورد ارزیابی قرار گرفت و نشان داده شد که در حمله به صورت هوشمند شبکه رادیو شناختگر مورد آسیب جدی قرار می‌گیرد و حتی در صورت انتخاب مناسب پارامترهای ترافیک کاربران این امکان وجود دارد که برون‌دهی شبکه کاربران ثانویه به سمت صفر میل نماید. در نهایت شبیه‌سازی‌هایی برای اطمینان از درستی نتایج به دست آمده، ارائه شدند.

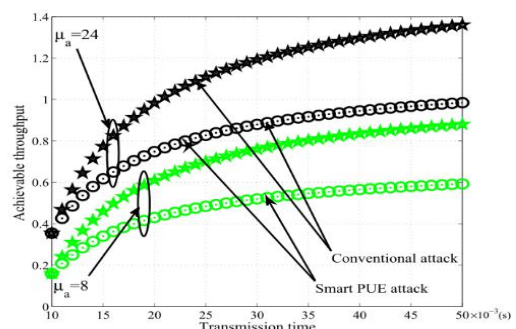
پیوست الف

برای به دست آوردن ماتریس گذار حالت $\mathbf{P}(t)$ ، ابتدا نیاز به محاسبه ماتریس $\mathbf{R}(s) = (s\mathbf{I} - \mathbf{Q})^{-1}$ است، با محاسبه ماتریس لاپلاس وارون $\mathbf{R}(s)$ ماتریس گذار حالت $\mathbf{P}(t)$ قابل محاسبه خواهد بود. با انجام مراحل بالا و حل معادلات عناصر ماتریس گذار به صورت عبارتهای (۳۹-۳۱) به دست می‌آیند. پس از به دست آوردن عناصر ماتریس گذار حالت، برای امتحان درستی و صحت آن‌ها، مراحل زیر امتحان گردید. یک ماتریس تصادفی است، بنابراین اولین امتحان برای پی بردن به صحت معادلات به دست آمده بالا، آزمون تصادفی بودن این ماتریس است. برای این که $\mathbf{P}(t)$ یک ماتریس تصادفی باشد، باید جمع عناصر روی یک ردیف آن برابر یک باشد، به عبارت دیگر داشته باشیم:

| | | | |
|---|--|--|-----|
| همانگ با مهاجم تحریرکننده اطلاعات حسگری تعیین کند. | | | |
| میزان اثرگذاری در برون‌دهی شبکه کاربران ثانویه برای $\gamma_s = -1dB$ | با توجه به شکل ۱۰: $R_N \frac{\lambda_a=24}{T-\tau=50ms} = 0.15$ bit/Second/Hz | با توجه به شکل ۱۰: $R_N \frac{\lambda_a=24}{T-\tau=50ms} = 0.44$ bit/Second/Hz | (۵) |

می‌یابد و دلیل آن اشتباه کاربران ثانویه در تشخیص حضور کاربران اولیه است، هرچقدر که مهاجم هوشمند حضور بیشتری در طیف داشته باشد احتمال این که کاربران ثانویه آن را با کاربر اولیه اشتباه بگیرند بیشتر می‌شود و لذا کاربران ثانویه از حضور در طیف و ارسال خودداری می‌کنند که نتیجه واضح آن کاهش برون‌دهی شبکه ثانویه خواهد بود. همان‌طور که از شکل ۹ پیداست با افزایش نسبت سیگنال به نویز مهاجم هوشمند، سیگنال مخرب قوی‌تری در شبکه رادیوشناختی وجود خواهد داشت و احتمال این که کاربران ثانویه مهاجم هوشمند را با کاربر اولیه اشتباه بگیرند، افزایش پیدا می‌کند و لذا کاربران ثانویه از حضور در کانال خودداری می‌نمایند که در نهایت این امر سبب کاهش برون‌دهی شبکه ثانویه خواهد شد.

برون‌دهی در دسترس برای شبکه کاربران ثانویه در حمله‌های سنتی تقلیدکننده کاربر اولیه و حمله مهاجم هوشمند تقلیدکننده کاربر اولیه، برحسب مدت‌زمان دوره انتقال و برای پارامتر میانگین مدت‌زمان ماندگاری نمایی حضور مهاجم هوشمند (λ_a) متفاوت، در شکل ۱۰، مقایسه شده‌اند. همان‌طور که از شکل پیداست در حمله مهاجم هوشمند چون مهاجم نسبت به حالت حمله سنتی تقلیدکننده کاربر اولیه فرصت‌های حمله بیشتری پیدا می‌کند لذا احتمال فریب خوردن کاربران ثانویه و در نتیجه حضور نیافتن آن‌ها در کانال افزایش می‌یابد. با کم شدن فرصت‌های حضور کاربران ثانویه در کانال، آن‌ها اطلاعات کمتری را می‌توانند ارسال نمایند که در نهایت این عوامل سبب می‌شود که برون‌دهی شبکه کاربران ثانویه در حالت حمله به صورت هوشمند بیشتر کاهش یابد. هم‌چنین هرچقدر که مقدار λ_a بیشتر شود، احتمال حضور مهاجم هوشمند نیز افزایش می‌یابد و برون‌دهی شبکه کاربران ثانویه بیشتر کاهش یابد.



شکل (۱۱): مقایسه‌ی برون‌دهی در دسترس برای شبکه کاربران ثانویه در حمله‌های سنتی تقلیدکننده کاربر اولیه و حمله مهاجم هوشمند تقلیدکننده کاربر اولیه، برحسب مدت‌زمان دوره انتقال و بر اساس

$$p_{00} = \frac{(\lambda\mu_p + \mu\mu_a + \mu_a\mu_p) + e^{-\rho}(\cosh(\beta t) - \frac{\sinh(\beta t)\zeta_{00}}{\beta}) \times f_{00}}{g}, \Theta = \frac{\lambda + \lambda_a + \lambda_p + \mu + \mu_a + \mu_p}{2}, \rho = \frac{\lambda + \lambda_a + \lambda_p + \mu + \mu_a + \mu_p}{2},$$

$$f_{00} = \lambda_a(\lambda + \mu + \mu_p) + \lambda_p(\lambda + \mu + \mu_a), \quad g = \lambda(\lambda_a + \lambda_p + \mu_p) + \lambda_a(\mu + \mu_p) + \lambda_p(\mu + \mu_a) + \mu_a(\mu + \mu_p), \quad (31)$$

$$\beta = \frac{1}{2} \left(\frac{\lambda^2 + \lambda_a^2 + \lambda_p^2 + \mu^2 + \mu_a^2 + \mu_p^2}{2} - \lambda(\lambda_a + \lambda_p - \mu - \mu_a + \mu_p) + \lambda_a(\lambda_p - \mu + \mu_a - \mu_p) - \lambda_p(\mu + \mu_a - \mu_p) - \mu(\mu_a - \mu_p) - \mu_a\mu_p \right)^{1/2},$$

$$\zeta_{00} = \Theta - \frac{\lambda_a(\lambda^2 + \mu^2 + \mu_p^2) + \lambda_p(\lambda^2 + \mu^2 + \mu_a^2) + \lambda\lambda_a(\mu + \mu_a + \mu_p) + 2\lambda\lambda_p(\mu + \mu_a) + 2\lambda_a\mu\mu_p + \lambda_p\mu(\mu_a + \mu_p)}{f_{00}}.$$

$$p_{01} = \frac{(\lambda\lambda_a + \lambda\lambda_p + \lambda_p\mu_a) - e^{-\rho}(\cosh(\beta t) - \frac{\sinh(\beta t)\zeta_{01}}{\beta}) \times f_{01}}{g}, \quad f_{01} = (\lambda\lambda_a + \lambda\lambda_p + \lambda_p\mu_a), \quad (32)$$

$$\zeta_{01} = \Theta - \frac{\lambda^2(\lambda_a + \lambda_p) + \lambda\lambda_a(\lambda_p + \lambda_a + \mu + \mu_a + \mu_p) + \lambda_a\lambda_p(\mu_a - \mu_p - \mu) + \lambda\lambda_p(\mu + 2\mu_a) - \lambda_p^2\mu + \lambda_p\mu_a^2}{f_{01}}.$$

$$p_{02} = \frac{(\lambda_a\mu + \lambda_p\mu + \lambda_a\mu_p) - e^{-\rho}(\cosh(\beta t) - \frac{\sinh(\beta t)\zeta_{02}}{\beta}) \times f_{02}}{g}, \quad f_{02} = (\lambda_a\mu + \lambda_p\mu + \lambda_a\mu_p), \quad (33)$$

$$\zeta_{02} = \Theta - \frac{\mu^2(\lambda_a + \lambda_p) + \lambda_p\mu(\mu_a + \mu_p + \lambda + \lambda_p) + \lambda\lambda_a(\mu - \lambda_p - \lambda_a) + \lambda_a\lambda_p(\mu - \mu_a + \mu_p) + \lambda_a\mu_p(2\mu + \mu_p)}{f_{02}}.$$

$$p_{10} = \frac{(\lambda\mu_p + \mu\mu_a + \mu_a\mu_p) - e^{-\rho}(\cosh(\beta t) - \frac{\sinh(\beta t)\zeta_{10}}{\beta}) \times f_{10}}{g}, \quad f_{10} = (\lambda\mu_p + \mu\mu_a + \mu_a\mu_p), \quad (34)$$

$$\zeta_{10} = \Theta - \frac{\mu_a\mu(\lambda_p + \lambda_a + \mu_a + \mu + \lambda) + \mu_a\mu_p(\mu + \mu_a + \lambda_a + 2\lambda) + \mu\mu_p(\lambda - \lambda_a - \lambda_p) + \mu_p(\lambda^2 - \lambda_a\mu_p)}{f_{10}}.$$

$$p_{11} = \frac{(\lambda\lambda_a + \lambda\lambda_p + \lambda_p\mu_a) + e^{-\rho}(\cosh(\beta t) - \frac{\sinh(\beta t)\zeta_{11}}{\beta}) \times f_{11}}{g}, \quad f_{11} = \mu(\lambda_a + \lambda_p + \mu_a) + \mu_p(\lambda + \lambda_a + \mu_a), \quad (35)$$

$$\zeta_{11} = \Theta - \frac{\mu(\lambda_a^2 + \lambda_p^2 + \mu_a^2 + 2\lambda_a\lambda_p) + \mu_p(\lambda^2 + \lambda_a^2 + \mu_a^2 + 2\lambda\mu_a) + \mu\mu_a(\lambda + 2\lambda_a + \lambda_p) + \lambda_a\mu_p(\lambda + \lambda_p + 2\mu_a)}{f_{11}}.$$

$$p_{12} = \frac{(\lambda_a\mu + \lambda_p\mu + \lambda_a\mu_p) - e^{-\rho}(\cosh(\beta t) - \frac{\sinh(\beta t)\zeta_{12}}{\beta}) \times f_{12}}{g}, \quad f_{12} = \lambda_a\mu + \lambda_p\mu + \lambda_a\mu_p, \quad (36)$$

$$\zeta_{12} = \Theta - \frac{\mu(\lambda_a^2 + \lambda_p^2 + 2\lambda_a\lambda_p) + \lambda_a\mu_p(\lambda + \lambda_p + \mu_a + \lambda_a + \mu_p) + \mu\mu_p(\lambda_p - \mu_a + \lambda_a - \lambda) + \mu\mu_a(\lambda_a - \mu)}{f_{12}}.$$

$$p_{20} = \frac{(\lambda\mu_p + \mu\mu_a + \mu_a\mu_p) - e^{-\rho}(\cosh(\beta t) - \frac{\sinh(\beta t)\zeta_{20}}{\beta}) \times f_{20}}{g}, \quad f_{20} = \lambda\mu_p + \mu\mu_a + \mu_a\mu_p, \quad (37)$$

$$\zeta_{20} = \Theta - \frac{\lambda\mu_p(\mu_p + \lambda + \lambda_a - \lambda_p + \mu + \mu_a) + \mu_a\mu_p(\lambda_p + \mu_p + 2\mu) - \lambda_p\mu_a(\mu_a + \lambda) + \mu\mu_a(\lambda + \mu) - \lambda\lambda_a\mu_a}{f_{20}}.$$

$$p_{21} = \frac{(\lambda\lambda_a + \lambda\lambda_p + \lambda_p\mu_a) - e^{-\rho}(\cosh(\beta t) - \frac{\sinh(\beta t)\zeta_{21}}{\beta}) \times f_{21}}{g}, \quad f_{21} = \lambda\lambda_a + \lambda\lambda_p + \lambda_p\mu_a, \quad (38)$$

$$\zeta_{21} = \Theta - \frac{\lambda_p\mu_a(\mu_a + \lambda_p + \mu + \mu_p + \lambda_a) + \lambda\lambda_p(\mu_p + \lambda_p + \mu_a + 2\lambda_a) + \lambda\mu_a(\lambda_a - \mu - \mu_p) + \lambda(\lambda_a^2 - \lambda\mu_p)}{f_{21}}.$$

$$p_{22} = \frac{(\lambda_a\mu + \lambda_p\mu + \lambda_a\mu_p) + e^{-\rho}(\cosh(\beta t) - \frac{\sinh(\beta t)\zeta_{22}}{\beta}) \times f_{22}}{g}, \quad f_{22} = \lambda(\lambda_a + \lambda_p + \mu_p) + \mu_a(\lambda_p + \mu + \mu_p), \quad (39)$$

$$\zeta_{22} = \Theta - \frac{\lambda(\lambda_a^2 + \lambda_p^2 + \mu_p^2) + \mu_a(\lambda_p^2 + \mu^2 + \mu_p^2) + \lambda\mu_p(\lambda_a + 2\lambda_p + \mu) + \lambda_p\mu_a(\mu + \lambda_a + 2\mu_p) + 2(\lambda\lambda_a\lambda_p + \mu\mu_a\mu_p)}{f_{22}}.$$

پیوست ب

برای به دست آوردن ماتریس گذار حالت $\mathbf{P}(t)$ ، ابتدا نیاز به محاسبه ماتریس $\mathbf{R}(s) = (s\mathbf{I} - \mathbf{Q})^{-1}$ است، با محاسبه ماتریس لاپلاس وارون $\mathbf{R}(s)$ ماتریس گذار حالت $\mathbf{P}(t)$ قابل محاسبه خواهد بود. با انجام مراحل بالا و حل معادلات عناصر ماتریس گذار به صورت عبارات‌های (۳۹-۳۱) به دست می‌آیند. پس از به دست آوردن عناصر ماتریس گذار حالت، برای امتحان درستی و صحت آن‌ها، مراحل زیر امتحان گردید. یک ماتریس تصادفی است، بنابراین اولین امتحان برای پی بردن به صحت معادلات به دست آمده بالا، آزمون تصادفی بودن این ماتریس است. برای این که $\mathbf{P}(t)$ یک ماتریس تصادفی باشد، باید جمع عناصر روی یک ردیف آن برابر یک باشد، به عبارت دیگر داشته باشیم:

$$\sum_{j=0}^2 p_{i,j} = 1, \quad (40)$$

که با جمع عناصر روی یک ردیف، درستی مطلب بالا تأیید شد. آزمون بعدی محاسبه حد $\mathbf{P}(t)$ در زمان نزدیک صفر است که باید این حد برابر با ماتریس یک باشد. به عبارت دیگر باید داشته باشیم:

$$\lim_{t \rightarrow 0} \mathbf{P}(t) = \mathbf{I}_{3 \times 3} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad (41)$$

که با جایگذاری معادلات درستی این مطلب نیز تأیید شد. هم‌چنین برای اطمینان از درستی معادلات به دست آمده آزمون دیگری نیز طرح و تأیید شد که آن عبارت است از:

$$\mathbf{P}'(0) = \mathbf{Q}. \quad (42)$$

مراجع

- [1] R. Yu, Y. Zhang, Y. Liu, S. Gjessing and M. Guizani, "Securing Cognitive Radio Networks against Primary User Emulation Attacks," IEEE Network, vol. 30, no. 6, pp. 62-69, November-December 2016.
- [2] Z. Pourgharehkhani, A. Taherpour, T. Khattab and R. Hamila, "Efficient collaborative spectrum sensing under the smart primary user emulation attacker network," in Proc. IEEE Global Communications Conference (GLOBECOM), San Diego, CA, pp. 1-7, 2015.
- [3] A. S. Rawat, P. Anand, H. Chen, and P. K. Varshney, "Collaborative spectrum sensing in the presence of byzantine attacks in cognitive radio networks," Transactions on signal processing, IEEE, vol. 59, no. 2, pp. 774-786, February 2011.
- [4] عباس زاده حمیده، حسینی سنو سید امین. "ساخت توپولوژی انرژی آگاه با مکانیزم نگهداری در شبکه‌های حسگر بی‌سیم"، مجله مهندسی برق و الکترونیک ایران، سال چهاردهم، شماره دوم، تابستان ۱۳۹۶.
- [5] ChunSheng Xin; Song, M., "Detection of PUE Attacks in Cognitive Radio Networks Based on Signal Activity Pattern," in Mobile Computing, IEEE Transactions on , vol.13, no.5, pp.1022-1034, May 2014.
- [6] Ta Duc-Tuyen; Nhan Nguyen-Thanh; Ciblat, P.; Van-Tam Nguyen, "Extra-sensing game for malicious primary user emulator attack in cognitive radio network," in Networks and Communications (EuCNC), 2015 European Conference on , pp.306-310, June 2015.

[7] D. Das and S. Das, "Adaptive resource allocation scheme for cognitive radio vehicular ad-hoc network in the presence of primary user emulation attack," in IET Networks, vol. 6, no. 1, pp. 5-13, 2017.

[8] ولی زهرا، هاشمی مسعود رضا، مقیم ندا. "شیوه‌های توزیع بار در مهندسی ترافیک"، مجله مهندسی برق و الکترونیک ایران، سال دوازدهم، شماره دوم، پاییز ۱۳۹۴.

[9] جلیل زراعتکارمقدم 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، سال چهاردهم، شماره دوم، تابستان ۱۳۹۶.

[10] Atef, A. Eltholth, A. S. Ibrahim and M. S. El-Soudani, "Energy detection of random arrival and departure of primary user signals in Cognitive Radio systems," in International Conference on Computer as a Tool, IEEE, Salamanca, pp. 1-6, September 2015.

[11] M. Wellens, and A. de Baynast, and P. Mahonen, "Exploiting Historical Spectrum Occupancy Information for Adaptive Spectrum Sensing," in Proc. of IEEE Wireless Communications and Networking Conference (WCNC), pp. 717-722, 2008.

[12] A. Karimi, A. Taherpour and Z. Pourgharehkhani, "Secure multiple antennas spectrum sensing under continuous attacking traffic," 8th International Symposium on Telecommunications (IST), Tehran, Iran, pp. 66-71, 2016.

[13] F. Zhang, W. Wang, and Z. Zhang, "A primary traffic aware opportunistic spectrum sensing for cognitive radio networks," in IEEE PIMRC, pp. 700-704, 2011.

[14] L. Tang, Y. Chen, E. L. Hines, and M. S. Alouini, "Effect of primary user traffic on sensing-throughput tradeoff for cognitive radios," in IEEE Trans. Wireless Commun., vol. 10, no. 4, pp. 1063-1068, Apr. 2011.

[15] Y. Zeng, Y.-C. Liang, E. Peh, and A. T. Hoang, "Sensing-throughput tradeoff for cognitive radio networks," IEEE Trans. Wireless Commun., vol. 7, no. 4, pp. 1326-1337, Apr. 2008.

[16] Digital Video Broadcasting (DVB); Framing structure, channel coding and modulation for digital terrestrial television (DVB-T), [Online]. Available in web site: <https://www.dvb.org/resources/public/standards>, 2015.

[17] W. Weifang, "Denial of service attacks in cognitive radio networks", Environmental Science and Information Application Technology (ESIAT), pp. 530-533, 2010.

زیر نویس‌ها

¹ Cognitive radio

² Secondary User (SU)

³ Malicious

⁴ Selfish

⁵ Primary User Emulation Attacks (PUEA)

⁶ Spectrum sensing data falsification attacks

⁷ Primary User (PU)

⁸ Byzantine attackers

⁹ Spectrum sensing

¹⁰ Vehicular ad-hoc cognitive radio network

¹¹ Throughput

¹² Digital Video Broadcasting (DVB)