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 به‌محض 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 به‌صورت 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 قرارگرفته است. هم‌چنین حمله مهاجم تقلیدکننده کاربر اولیه در روش‌های سنتی و حمله به‌صورت هوشمند مورد مقایسه قرارگرفته 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.

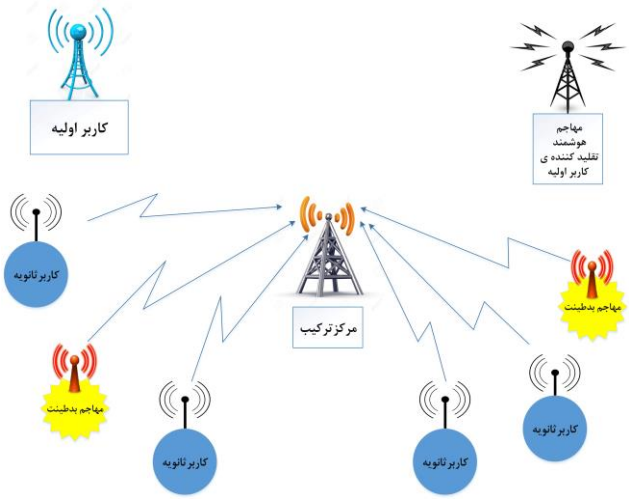
[DOR: 20.1001.1.26765810.1398.16.4.15.6]
Journal of Iranian Association of Electrical and Electronics Engineers - Vol.16- No.4- Winter2018

۱- مقدمه

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 رادیوشناختی[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 رادیوشناختی 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 رادیوشناختی را مستعد انواع آسیب‌پذیری‌ها می‌کند.

از میان حمله‌های متفاوتی که یک شبکه رادیوشناختی با آن مواجه است، حمله‌های تقلیدکننده کاربر اولیه[۵] و حمله‌های تحریف‌کننده اطلاعات حسگری طیفی[۶] عملکرد شبکه رادیوشناختی 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. به‌عنوان‌مثال در مراجع [۱، ۲]، نویسندگان به معرفی این نوع از حمله‌های تقلیدکننده کاربر اولیه پرداخته‌اند. مهاجمان تحریف‌کننده اطلاعات حسگری طیفی یا مهاجمان بیزانسی[۸] در شبکه‌های رادیوشناختی، 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 رادیوشناختی 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 ارائه‌شده است. طی سال‌های اخیر، محققان به دنبال مدل‌هایی از شبکه‌های رادیوشناختگر 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 رادیوشناختی حمله می‌نمایند، راه‌کارهایی نیز ارائه‌شده است [۵، ۶]. به‌عنوان نمونه، در مرجع [۷]، نویسندگان یک شبکه رادیوشناختی اقتضایی متحرک[۱۰]، با در نظر گرفتن ارتباط 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 رادیوشناختی، کاربر اولیه در هر زمان که بخواهد می‌تواند وارد طیف شود و یا از آن خارج شود؛ درحالی‌که در مدل‌های شبکه‌های رادیوشناختی 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 رادیوشناختی ارائه‌شده، در حضور مهاجم هوشمند تقلید کننده کاربر اولیه و مهاجمان تحریف کننده 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 مهندسان 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.

Journal of Iranian Association of Electrical and Electronics Engineers - Vol.16- No.4- Winter 2018

۲- مدل شبکه رادیوشناختی و فرضیات اصلی

شکل ۱، ساختار ارائه‌شده برای شبکه رادیوشناختی جدید و با حضور مهاجم هوشمند تقلیدکننده رفتار کاربر اولیه و مهاجمان تحریف‌کننده اطلاعات حسگری، را به تصویر می‌کشد. در این شبکه یک مهاجم تقلیدکننده رفتار کاربر اولیه وجود دارد که به‌صورت هوشمند در نبود کاربر اولیه، با تقلید ویژگی‌های سیگنال کاربر اولیه وارد طیف می‌شود و سعی در فریب دادن کاربران ثانویه دیگر دارد تا به‌طور خودخواهانه طیف را در اختیار خود بگیرد؛ از طرف دیگر به‌طور هم‌زمان چندین مهاجم تحریف‌کننده اطلاعات حسگری که حتماً دارای هدف خودخواهانه نیستند در شبکه رادیو شناختگر مشارکتی ارائه‌شده پخش‌شده‌اند. مهاجمان تحریف‌کننده اطلاعات حسگری که در نبود کاربر اولیه قانونی، از وارد شدن مهاجم هوشمند تقلیدکننده رفتار کاربر اولیه به طیف آگاه می‌شوند، با ارسال پیغام پر بودن کانال به مرکز ترکیب سبب می‌شوند که مرکز ترکیب در اتخاذ تصمیم صحیح درباره کانال دچار مشکل بشود و حکم به پر بودن کانال توسط کاربر اولیه نماید که درنتیجه بقیه کاربران ثانویه نیز از حضور در طیف خودداری می‌نمایند و راه برای استفاده هرچه خودخواهانه‌تر مهاجم هوشمند باز می‌شود. این مقاله حاوی پارامترهای زیادی است، برای پرهیز از ابهام در درک مطالب، جدول ۱ که شامل پارامترهای اساسی

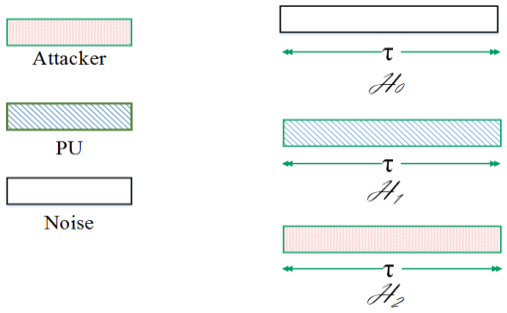
جدول (۱): پارامترها و تعریف‌های اصلی

پارامتر	تعریف
n_ℓ	نمونه‌های به‌دست‌آمده از نویز گاوسی سفید جمع شونده
s_ℓ	نمونه‌های سیگنال کاربر اولیه
w_ℓ	نمونه‌های سیگنال مهاجم تقلیدکننده کاربر اولیه
τ	طول زمان حسگری طیفی
L	تعداد کل نمونه‌های جمع شده از کانال در طی دوره حسگری
J	تعداد کل نمونه‌های جمع شده در یک قاب یا دوره تناوب
γ_p	نسبت سیگنال به نویز ارسال‌شده از کاربر اولیه
γ_w	نسبت سیگنال به نویز ارسال‌شده از مهاجم هوشمند
γ_s	نسبت سیگنال به نویز فرستنده کاربر ثانویه
C_j	ظرفیت کانال تحت فرضیه $\mathcal{H}_j$
$R_{\mathcal{H}_j}$	برون‌دهی در دسترس شبکه تحت فرضیه $\mathcal{H}_j$
R_N	برون‌دهی در دسترس متوسط شبکه ثانویه

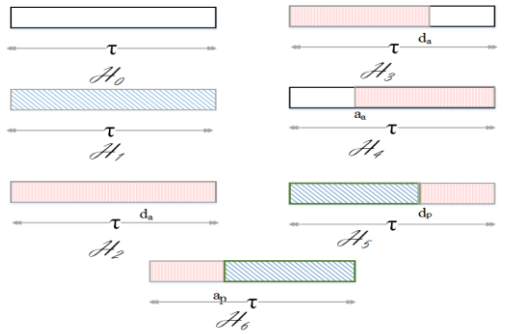
است، ارائه‌شده است. در ساختار قاب‌بندی فرض شده شبکه، هر قاب شامل یک شکاف زمانی برای حسگری (τ) و یک شکاف زمانی برای انتقال اطلاعات است. تعداد نمونه‌های جمع شده از کانال در دوره حسگری L فرض می‌شود. در شکل ۲، مدل حسگری طیفی سنتی که مهاجم و یا کاربر اولیه در کل دوره حسگری، حضور دارند نمایش داده شده است.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

$$E=\begin{cases}\sum_{\ell=1}^{L} n_\ell^2 & , \ \mathcal{H}_0 \\ \sum_{\ell=1}^{L}(s_\ell+n_\ell)^2 & , \ \mathcal{H}_1 \\ \sum_{\ell=1}^{L}(w_\ell+n_\ell)^2 & , \ \mathcal{H}_2\end{cases} \quad (۱)$$

در عبارت ۱، $n_\ell, \forall \ell \in \{1;\cdots L\}$، نمونه‌های به‌دست‌آمده از نویز گاوسی سفید جمع شونده، $s_\ell, \forall \ell \in \{1,\cdots,L\}$، نمونه‌های سیگنال کاربر اولیه، $w_\ell, \forall \ell \in \{1,\cdots,L\}$، نمونه‌های سیگنال مهاجم تقلیدکننده کاربر اولیه و E خروجی آشکارساز انرژی است. $\mathcal{H}_0$ نمایش‌دهنده فرضیه‌ای است که کاربر اولیه و مهاجم همواره در طی دوره حسگری غایب هستند و بنابراین، خروجی آشکارساز فقط شامل نویز می‌شود، در فرضیه $\mathcal{H}_1$، در طی دوره حسگری کاربر اولیه همیشه حضور دارد و درنتیجه مهاجم غایب است و در فرضیه $\mathcal{H}_2$ در نبود کاربر اولیه، مهاجم از فرصت پیش رو استفاده می‌کند و در طیف همواره حضور دارد و با تقلید رفتار کاربر اولیه سعی می‌کند از ورود سایر کاربران ثانویه جلوگیری نماید. در شکل ۳ ترافیک کاربر اولیه همراه با مهاجم هوشمندی که به تقلید رفتار کاربر اولیه می‌پردازد و از ترافیک کاربر اولیه به‌عنوان فرصت حمله استفاده می‌کند، ارائه شده است. در این مدل فرض می‌شود که کاربر اولیه و مهاجم هوشمند تقلیدکننده کاربر اولیه حداکثر یک‌بار در طی دوره حسگری در هر قاب تغییر حالت می‌دهند که هر بار با خارج شدن کاربر اولیه مهاجم تقلیدکننده کاربر اولیه به‌سرعت وارد طیف می‌شود. فرض یک‌بار تغییر وضعیت برای این است که طول قاب به‌اندازه 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

[DOR: 20.1001.1.26765810.1398.16.4.15.6]
Journal of Iranian Association of Electrical and Electronics Engineers - Vol.16- No.4- Winter2018

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 بررسی‌شده‌اند. در ۲، عبارت‌های d_a، a_a، d_p 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.

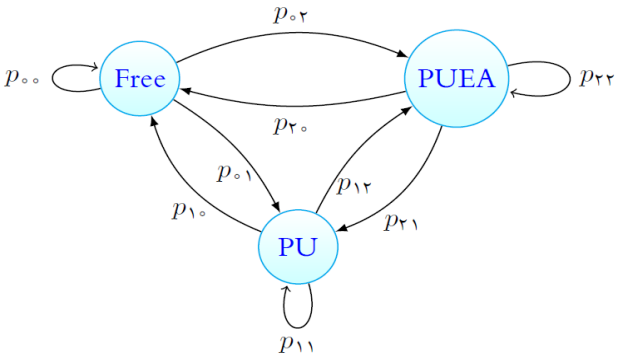
$$E=\begin{cases}\sum_{\ell=1}^{L} n_\ell^2 & , \mathcal{H}_0\\ \sum_{\ell=1}^{L}(s_\ell+n_\ell)^2 & , \mathcal{H}_1\\ \sum_{\ell=1}^{L}(w_\ell+n_\ell)^2 & , \mathcal{H}_2\\ \sum_{\ell=1}^{d_a}(w_\ell+n_\ell)^2+\sum_{\ell=d_a+1}^{L} n_\ell^2 & , \mathcal{H}_3\\ \sum_{\ell=1}^{a_a} n_\ell^2+\sum_{\ell=a_a+1}^{L}(w_\ell+n_\ell)^2 & , \mathcal{H}_4\\ \sum_{\ell=1}^{d_p}(s_\ell+n_\ell)^2+\sum_{\ell=d_p+1}^{L}(w_\ell+n_\ell)^2 & , \mathcal{H}_5\\ \sum_{\ell=1}^{a_p}(w_\ell+n_\ell)^2+\sum_{\ell=a_p+1}^{L}(s_\ell+n_\ell)^2 & , \mathcal{H}_6\end{cases} \quad (۲)$$

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 گرفته‌شده 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 داده‌شده 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.

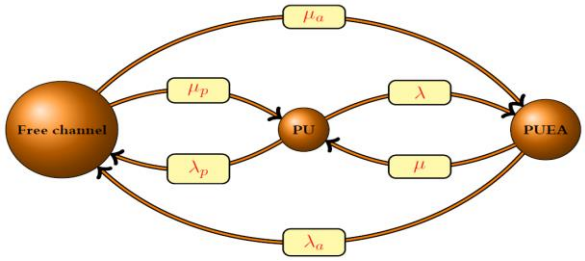
۳- مدل نمودن هم‌زمان ترافیک کاربر اولیه و مهاجم هوشمند تقلیدکننده کاربر اولیه

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 دوحالته 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 سه‌حالته تشکیل می‌دهند. برای مدل نمودن ترافیک شبکه، زنجیره مارکوف $X=\{X(t):t\geqslant 0\}$ که پارامتر زمان پیوسته $t\in[0,\infty)$ را شامل می‌شود، در نظر گرفته‌شده است. فرض می‌شود که $\mathbf{Q}$ ماتریس نرخ زنجیره مارکوف X و $\mathbf{P}(t)\,t\geqslant 0$، تابع ماتریس گذار حالت آن باشد. این زنجیره مارکوف به‌صورت شکل ۴، در نظر گرفته‌شده است.

فضای حالت زنجیره مارکوف پیوسته X به‌صورت $S:=\{0,1,2\}$ در نظر گرفته‌شده 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 داده‌شده همان‌طور که در شکل ۵، نشان داده شده است با نرخ‌های زیر در نظر گرفته‌شده است: وقتی‌که 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. هنگامی‌که 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

Journal of Iranian Association of Electrical and Electronics Engineers - Vol.16- No.4- Winter 2018

صورت می‌پذیرد و وقتی‌که 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.

$$P\{0 \le X \le t\} = \int_0^t \frac{1}{\lambda_p} e^{-\frac{1}{\lambda_p}x} dx = 1 - e^{-\frac{t}{\lambda_p}} \gtrless \varepsilon, \qquad (۳)$$

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

$$\mathbf{Q} = \begin{pmatrix} -(\mu_p + \mu_a) & \mu_p & \mu_a \\ \lambda_p & -(\lambda_p + \lambda) & \lambda \\ \lambda_a & \mu & -(\lambda_a + \mu) \end{pmatrix}. \qquad (۴)$$

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

$$\mathbf{P}(t) = \begin{pmatrix} p_{00}(t) & p_{01}(t) & p_{02}(t) \\ p_{10}(t) & p_{11}(t) & p_{12}(t) \\ p_{20}(t) & p_{21}(t) & p_{22}(t) \end{pmatrix}. \qquad (۵)$$

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 یک قاب یا دوره تناوب، $p_b = \frac{\lambda_p}{\lambda_p + \mu_p}$، $p_e = \frac{\mu_p}{\lambda_p + \mu_p}$، $a_b = \frac{\lambda_a}{\lambda_a + \mu_a}$ و $a_e = \frac{\mu_a}{\lambda_a + \mu_a}$ به ترتیب احتمال اشغال یا خالی بودن کانال در هرلحظه توسط کاربر اولیه و مهاجم هوشمند تقلیدکننده کاربر اولیه می‌باشند، سایر پارامترها در جدول ۱ معرفی‌شده‌اند.

$$\begin{aligned}
P(\mathcal{H}_0) &= p_e a_e p_{00}^{J} + \Big(\sum_{a_p=L+1}^{J-1} p_e p_{00}^{a_p} p_{01} p_{11}^{(J-a_p-1)}\Big) \\
&\quad + \Big(\sum_{a_a=L+1}^{J-1} a_e p_{00}^{a_a} p_{02} p_{22}^{(J-a_a-1)}\Big), \\
P(\mathcal{H}_1) &= p_b a_e p_{11}^{J} + \Big(\sum_{d_p=L+1}^{J-1} p_b p_{11}^{d_p} p_{10} p_{00}^{(J-d_p-1)}\Big) \\
&\quad + \Big(\sum_{a_a=L+1}^{J-1} a_e p_{00}^{a_a} p_{02} p_{22}^{(J-a_a-1)}\Big), \\
P(\mathcal{H}_2) &= p_e a_b p_{22}^{J} + \Big(\sum_{d_a=L+1}^{J-1} a_b p_{22}^{d_a} p_{20} p_{00}^{(J-d_a-1)}\Big) \\
&\quad + \Big(\sum_{a_p=L+1}^{J-1} p_e p_{00}^{a_p} p_{01} p_{11}^{(J-a_p-1)}\Big),
\end{aligned} \qquad (۶)$$

$$\begin{aligned}
P(\mathcal{H}_3) &= \Big(\sum_{d_a=1}^{L} a_b p_e p_{22}^{d_a} p_{20} p_{00}^{(J-d_a-1)}\Big), \\
P(\mathcal{H}_4) &= \Big(\sum_{a_a=1}^{L} p_e a_e p_{00}^{a_a} p_{02} p_{22}^{(J-a_a-1)}\Big), \\
P(\mathcal{H}_5) &= \Big(\sum_{d_p=1}^{L} p_b a_e p_{11}^{d_p} p_{12} p_{22}^{(J-d_p-1)}\Big), \\
P(\mathcal{H}_6) &= \Big(\sum_{a_p=1}^{L} a_b p_e p_{22}^{a_p} p_{21} p_{11}^{(J-a_p-1)}\Big),
\end{aligned}$$

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[11] شبکه کاربران ثانویه پرداخته می‌شود. به‌طورکلی برون‌دهی شبکه به نرخ داده‌های ارسال‌شده 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 $\mathcal{H}_j$, $j \in \{0,\cdots,6\}$ 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 قابل‌محاسبه خواهد بود:

$$\begin{aligned}
&P_{fa,\mathcal{H}_0}(\eta, L) = \Pr\{E > \eta \mid \mathcal{H}_0\}_{\to E \sim N(L\sigma_n^2, 2L\sigma_n^4)} = \\
&Q\Big(\frac{\eta - L\sigma_n^2}{\sqrt{2L}\,\sigma_n^2}\Big) = Q\Big(\frac{\eta}{\sqrt{2L}\,\sigma_n^2} - \sqrt{\frac{L}{2}}\Big).
\end{aligned} \qquad (۷)$$

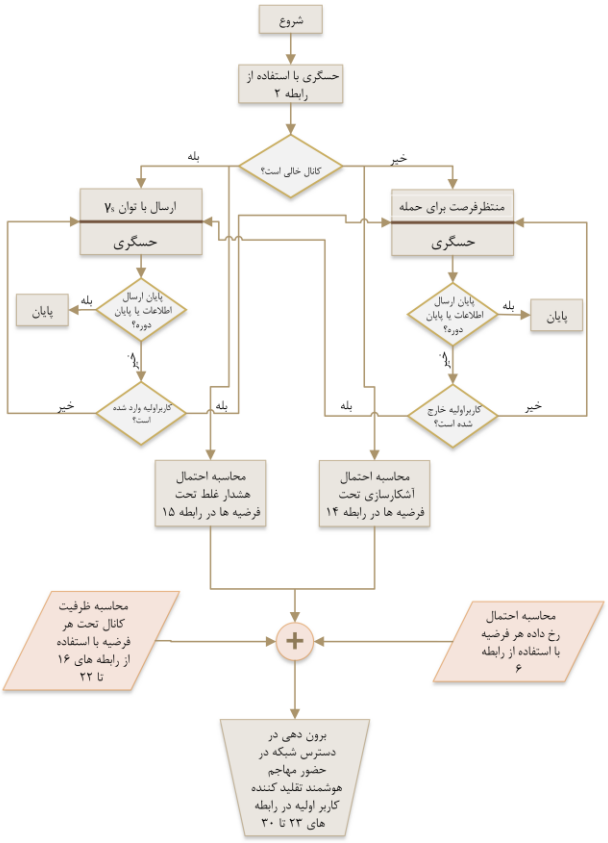
احتمال آشکارسازی شرطی تحت فرضیه $\mathcal{H}_1$:

$$\begin{aligned}
&P_{d,\mathcal{H}_1}(\eta, L) = \Pr\{E > \eta \mid \mathcal{H}_1\}_{\to E \sim N(L(\gamma_p+1)\sigma_n^2, 2L(2\gamma_p+1)\sigma_n^4)} = \\
&Q\Big(\frac{\eta}{\sqrt{2L(2\gamma_p+1)}\sigma_n^2} - (\gamma_p+1)\sqrt{\frac{L}{4\gamma_p+2}}\Big).
\end{aligned} \qquad (۸)$$

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

$$\begin{aligned}
&P_{fa,\mathcal{H}_2}(\eta, L) = \Pr\{E > \eta \mid \mathcal{H}_2\}_{\to E \sim N(L(\gamma_w+1)\sigma_n^2, 2L(2\gamma_w+1)\sigma_n^4)} = \\
&Q\Big(\frac{\eta}{\sqrt{2L(2\gamma_w+1)}\sigma_n^2} - (\gamma_w+1)\sqrt{\frac{L}{4\gamma_w+2}}\Big).
\end{aligned} \qquad (۹)$$

[DOR: 20.1001.1.26765810.1398.16.4.15.6]
Journal of Iranian Association of Electrical and Electronics Engineers - Vol.16- No.4- Winter2018



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:

$$P_{\text{fa},\mathcal{H}_3}(\eta,L,d_a)=Q\left(\frac{\eta-L-d_a\gamma_w}{2\sqrt{\frac{L}{2}+d_a\gamma_w}}\right). \qquad (۱۰)$$

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

$$P_{\text{fa},\mathcal{H}_4}(\eta,L,a_a)=Q\left(\frac{\eta+\gamma_w(a_a-L)-L)}{\sqrt{2L+(4L-4a_a)\gamma_w}}\right). \qquad (۱۱)$$

احتمال آشکارسازی شرطی و احتمال هشدار غلط شرطی تحت فرضیه $\mathcal{H}_5$ با شرط بر روی d_p به‌صورت زیر قابل‌محاسبه خواهند بود:

$$\begin{cases} P_{\text{d},\mathcal{H}_5}(\eta,L,d_p)=Q\left(\dfrac{\eta-d_p(\gamma_p+1)\sigma_n^2}{\sqrt{2d_p(2\gamma_p+1)\sigma_n^2}}\right), \\ P_{\text{fa},\mathcal{H}_5}(\eta,L,d_p)=Q\left(\dfrac{\eta-(L-d_p)(\gamma_w+1)\sigma_n^2}{\sqrt{2(L-d_p)(2\gamma_w+1)\sigma_n^2}}\right). \end{cases} \qquad (۱۲)$$

احتمال آشکارسازی شرطی و احتمال هشدار غلط شرطی تحت فرضیه $\mathcal{H}_6$ با شرط بر روی a_p به‌صورت زیر قابل‌محاسبه خواهند بود:

$$\begin{cases} P_{\text{d},\mathcal{H}_6}(\eta,L,a_p)=Q\left(\dfrac{\eta-(L-a_p)(\gamma_p+1)\sigma_n^2}{\sqrt{2(L-a_p)(2\gamma_p+1)\sigma_n^2}}\right), \\ P_{\text{fa},\mathcal{H}_6}(\eta,L,a_p)=Q\left(\dfrac{\eta-a_p(\gamma_p+1)\sigma_n^2}{\sqrt{2a_p(2\gamma_w+1)\sigma_n^2}}\right). \end{cases} \qquad (۱۳)$$

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

$$\begin{aligned} \overline{P_{fa}}(\eta,L)=&\frac{P(\mathcal{H}_0)P_{\text{fa},\mathcal{H}_0}(\eta,L)+P(\mathcal{H}_2)P_{\text{fa},\mathcal{H}_2}(\eta,L)}{1-P(\mathcal{H}_1)} \\ &+\frac{P(\mathcal{H}_3)}{1-P(\mathcal{H}_1)}\sum_{d_a=1}^{L}P_{\text{fa},\mathcal{H}_3}(\eta,L,d_a) \\ &+\frac{P(\mathcal{H}_4)}{1-P(\mathcal{H}_1)}\sum_{a_a=1}^{L}P_{\text{fa},\mathcal{H}_4}(\eta,L,a_a) \\ &+\frac{P(\mathcal{H}_5)}{1-P(\mathcal{H}_1)}\sum_{d_p=1}^{L}P_{\text{fa},\mathcal{H}_5}(\eta,L,d_p) \\ &+\frac{P(\mathcal{H}_6)}{1-P(\mathcal{H}_1)}\sum_{a_p=1}^{L}P_{\text{fa},\mathcal{H}_6}(\eta,L,a_p), \end{aligned} \qquad (۱۴)$$

$$\begin{aligned} \overline{P_{\text{d}}}(\eta,L)=&\frac{P(\mathcal{H}_1)P_{\text{d},\mathcal{H}_1}(\eta,L)}{P(\mathcal{H}_1)+P(\mathcal{H}_5)+P(\mathcal{H}_6)} \\ &+\frac{P(\mathcal{H}_5)}{P(\mathcal{H}_1)+P(\mathcal{H}_5)+P(\mathcal{H}_6)}\sum_{d_p=1}^{L}P_{\text{d},\mathcal{H}_5}(\eta,L,d_p) \\ &+\frac{P(\mathcal{H}_6)}{P(\mathcal{H}_1)+P(\mathcal{H}_5)+P(\mathcal{H}_6)}\sum_{a_p=1}^{L}P_{\text{d},\mathcal{H}_6}(\eta,L,a_p), \end{aligned} \qquad (۱۵)$$

که η سطح آستانه در کاربر ثانویه با نسبت سیگنال به نویز ($\gamma_p=\frac{\sigma_p^2}{\sigma_n^2}$) ارسال‌شده از کاربر اولیه و با نسبت سیگنال به نویز ($\gamma_w=\frac{\sigma_w^2}{\sigma_n^2}$) ارسال‌شده 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 به‌صورت لگاریتم در مبنای ۲ نسبت سیگنال به نویز سیگنال مطلوب γ_s به نسبت سیگنال به نویز سیگنال‌های دیگر، به صورت زیر قابل‌محاسبه است:

$$C_0(a_p,a_a)=\log_2\left(1+\frac{\gamma_s}{1+\frac{J-a_p}{J-L}\gamma_p+\frac{J-a_a}{J-L}\gamma_w}\right), \qquad (۱۶)$$

که γ_s نسبت سیگنال به نویز فرستنده کاربر ثانویه و یا به‌عبارت‌دیگر 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:

$$C_1(d_p,a_a)=\log_2\left(1+\frac{\gamma_s}{1+\frac{d_p-L}{J-L}\gamma_p+\frac{J-a_a}{J-L}\gamma_w}\right). \quad (۱۷)$$

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 می‌کند، بنابراین ظرفیت کانال خواهد شد:

$$C_2(d_a,a_p)=\log_2\left(1+\frac{\gamma_s}{1+\frac{d_a-L}{J-L}\gamma_w+\frac{J-a_p}{J-L}\gamma_p}\right). \quad (۱۸)$$

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

$$C_3=\log_2(1+\gamma_s). \quad (۱۹)$$

در فرضیه $\mathcal{H}_4$، همانند حالت قبل فرض می‌شود که به‌طورکلی کاربر اولیه در طیف حضور نمی‌یابد در این حالت مهاجم هوشمند تقلیدکننده کاربر اولیه در طی زمان حسگری طیفی مدتی پس از ابتدای دوره حسگری به کانال می‌رسد و در طی دوره ارسال نیز باقی می‌ماند، بنابراین ظرفیت برابر خواهد شد با:

$$C_4=\log_2\left(1+\frac{\gamma_s}{1+\gamma_w}\right). \quad (۲۰)$$

در فرضیه $\mathcal{H}_5$، کاربر اولیه ابتدا در طیف حضور دارد اما مدتی بعد از طیف خارج می‌شود و لذا در طی زمان دوره ارسال نیز نمی‌تواند 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 به‌صورت زیر خواهد بود:

$$C_5=\log_2\left(1+\frac{\gamma_s}{1+\gamma_w}\right). \quad (۲۱)$$

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

$$C_6=\log_2\left(1+\frac{\gamma_s}{1+\gamma_p}\right). \quad (۲۲)$$

با انجام مراحل یادشده، ابزار موردنیاز برای محاسبه برون‌دهی شبکه رادیوشناختی با حضور مهاجم هوشمند تکمیل می‌شود و درنهایت برون‌دهی در دسترس متوسط شبکه ثانویه با جمع برون‌دهی در دسترس تحت تمام فرضیه‌ها [۱۴] به‌صورت زیر خواهد شد:

$$R_N(\eta,L)=\sum_{j=0}^{6}R_{\mathcal{H}_j}(\eta,L), \quad (۲۳)$$

که عناصر آن به‌صورت عبارات (۲۴-۳۰) به دست می‌آیند.

$$R_{\mathcal{H}_0}(\eta,L)=\left(1-\overline{P_{fa}}(\eta,L)\right)\left(\frac{T-\tau}{T}\right)\left(p_e a_e p_{00}C_0(J,J)+\sum_{a_p=L+1}^{J-1}\sum_{a_a=L+1}^{J-1}p_e a_e\left(p_{00}^{a_p}p_{01}p_{11}^{J-a_p-1}+p_{00}^{a_a}p_{02}p_{22}^{J-a_a-1}\right)C_0(a_p,a_a)\right), \quad (۲۴)$$

$$R_{\mathcal{H}_1}(\eta,L)=\left(1-\overline{P_d}(\eta,L)\right)\left(\frac{T-\tau}{T}\right)\left(p_b a_e p_{11}C_1(J,J)+\sum_{d_p=L+1}^{J-1}\sum_{a_a=L+1}^{J-1}p_b a_e\left(p_{11}^{d_p}p_{10}p_{00}^{J-d_p-1}+p_{00}^{a_a}p_{02}p_{22}^{J-a_a-1}\right)C_1(d_p,a_a)\right), \quad (۲۵)$$

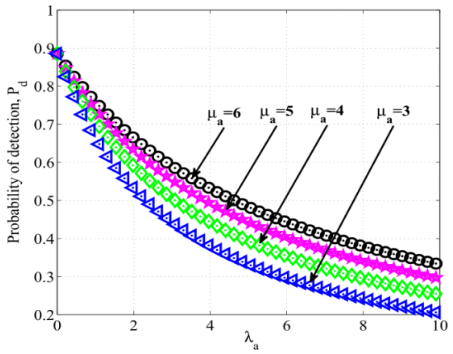
$$R_{\mathcal{H}_2}(\eta,L)=\left(1-\overline{P_{fa}}(\eta,L)\right)\left(\frac{T-\tau}{T}\right)\left(p_e a_b p_{22}C_2(J,J)+\sum_{a_p=L+1}^{J-1}\sum_{d_a=L+1}^{J-1}p_e a_b\left(p_{00}^{a_p}p_{01}p_{11}^{J-a_p-1}+p_{22}^{d_a}p_{20}p_{00}^{J-d_a-1}\right)C_2(a_p,d_a)\right), \quad (۲۶)$$

$$R_{\mathcal{H}_3}(\eta,L)=\left(1-\overline{P_{fa}}(\eta,L)\right)\left(\frac{T-\tau}{T}\right)\times\sum_{d_a=1}^{L}p_e a_b p_{22}^{d_a}p_{20}p_{00}^{(J-d_a-1)}C_3(d_a), \quad (۲۷)$$

$$R_{\mathcal{H}_4}(\eta,L)=\left(1-\overline{P_{fa}}(\eta,L)\right)\left(\frac{T-\tau}{T}\right)\times\sum_{a_a=1}^{L}p_e a_e p_{00}^{a_a}p_{02}p_{22}^{(J-a_a-1)}C_4(a_a), \quad (۲۸)$$

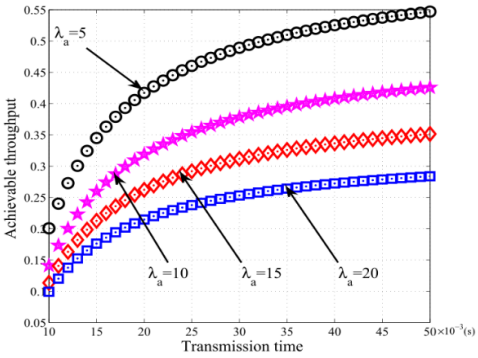
$$R_{\mathcal{H}_5}(\eta,L)=\left(1-\overline{P_{fa}}(\eta,L)\right)\left(1-\overline{P_d}(\eta,L)\right)\times\left(\frac{T-\tau}{T}\right)\sum_{d_p=1}^{L}p_b a_e p_{11}^{d_p}p_{12}p_{22}^{(J-d_p-1)}C_5(d_p), \quad (۲۹)$$

$$R_{\mathcal{H}_6}(\eta,L)=\left(1-\overline{P_{fa}}(\eta,L)\right)\left(1-\overline{P_d}(\eta,L)\right)\times\left(\frac{T-\tau}{T}\right)\sum_{a_p=1}^{L}p_e a_b p_{22}^{a_p}p_{21}p_{11}^{(J-a_p-1)}C_6(a_p). \quad (۳۰)$$



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

[DOR: 20.1001.1.26765810.1398.16.4.15.6]
Journal of Iranian Association of Electrical and Electronics Engineers - Vol.16- No.4- Winter2018



شکل (۸): برون‌دهی در دسترس برای شبکه کاربران ثانویه برحسب مدت‌زمان دوره انتقال و برای شدت ترافیک متفاوت و بر اساس

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

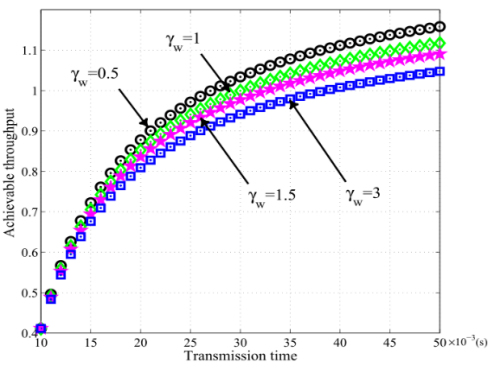
$\gamma_p = \gamma_w = 1(W) = 0dB$ و $\gamma_s = -1dB$.

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 ارائه‌شده 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 ($T-\tau$) به ترتیب برابر با ۶۰ ~ ۲۰ (ms) و ۵۰ ~ ۱۰ (ms) در نظر گرفته شده‌اند [۱۶]. سایر پارامترهای شبیه‌سازی نیز در جدول ۲ آورده شده‌اند.

جدول (۲): نمادها و عبارت‌های استفاده‌شده در شبیه‌سازی

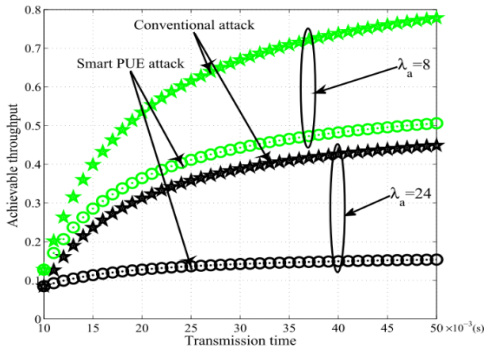
تعریف	نماد
طول قاب	T=20~60 (ms)
طول دوره‌ی ارسال	T-τ=10~50 (ms)
نمونه‌های جمع شده، در طول زمان دوره‌ی حسگری	$L = 40 \sim 50$
نمونه‌های جمع شده، در طول یک دوره تناوب	$J = 65$
نسبت سیگنال به نویز در شبکه‌ی کاربران ثانویه	$\gamma_s = -1dB$



شکل (۹): برون‌دهی برای شبکه کاربران ثانویه برحسب مدت‌زمان دوره انتقال و برای نسبت سیگنال به نویزهای متفاوت و بر اساس

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

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



شکل (۱۰): مقایسه برون‌دهی برای شبکه کاربران ثانویه در حمله‌های سنتی و هوشمند، برحسب مدت‌زمان دوره انتقال و بر اساس $\lambda_p = 30$,

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

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

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 پیدا است 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 ارسال‌شده 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

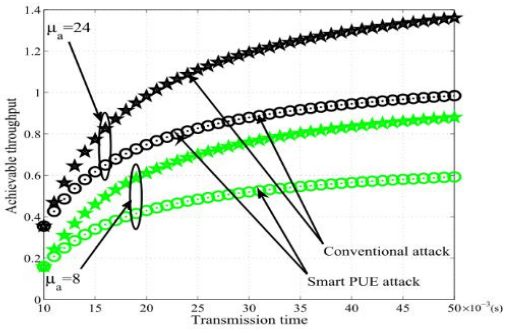
جدول (۳): مشخصات، ویژگی و نتایج حاصل از روش پیشنهادی

ردیف	مشخصات، ویژگی و نتایج	حمله به شیوه سنتی	حمله مهاجم هوشمند تقلیدکننده کاربر اولیه ارائه‌شده
(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 با شبکه کاربر اولیه	دارد	ندارد
(۴)	رفتار همکارانه	امکان‌پذیر نیست.	می‌تواند زمان حمله خود را

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

می‌یابد و دلیل آن اشتباه کاربران ثانویه در تشخیص حضور کاربران اولیه است، هرچقدر که مهاجم هوشمند حضور بیشتری در طیف داشته باشد احتمال این‌که 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 این‌که کاربران ثانویه، مهاجم هوشمند را با کاربر اولیه اشتباه بگیرند، افزایش پیدا می‌کند و لذا کاربران ثانویه از حضور در کانال خودداری می‌نمایند که درنهایت 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 درنتیجه حضور نیافتن آن‌ها در کانال افزایش می‌یابد. باکم شدن فرصت‌های حضور کاربران ثانویه در کانال، آن‌ها اطلاعات کمتری را می‌توانند ارسال نمایند که درنهایت 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 برون دهی 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

$$J = 65, L = 50, \lambda_a = 10, \mu_p = \lambda = \mu = 5, \lambda_p = 30$$
$$\gamma_p = \gamma_w = 1(W) = 0dB \text{ و } \gamma_s = -1dB, \tau = 10\text{ms}, T_s = 1\text{ms}.$$

در شکل ۱۱، نیز همانند شکل ۱۰، همین مقایسه، برحسب مدت‌زمان دوره انتقال و برای پارامتر میانگین مدت‌زمان ماندگاری نمایی عدم حضور مهاجم هوشمند (μ_a) متفاوت، پرداخته‌شده است. افزایش μ_a در این حالت بدین معنی است که به‌طور میانگین مهاجم هوشمند مدت‌زمان کمتری در طیف حضور دارد و لذا تأثیر مخرب آن بر برون دهی شبکه ثانویه کمتر است که درنهایت 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 شده‌اند و نتایج حاصل از آن ارائه شده است.

۶- نتیجه‌گیری

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 مبحث 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. به‌صورت 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 به‌صورت 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. درنهایت شبیه‌سازی‌هایی برای اطمینان از درستی نتایج به‌دست‌آمده، 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 به‌صورت 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. $\mathbf{P}(t)$ یک ماتریس تصادفی است، بنابراین اولین امتحان برای پی بردن به صحت معادلات به دست آمده بالا، آزمون تصادفی بودن این ماتریس است. برای این‌که $\mathbf{P}(t)$ یک ماتریس تصادفی باشد، باید جمع عناصر روی یک ردیف آن برابر یک باشد، به‌عبارت‌دیگر داشته باشیم:

[DOR: 20.1001.1.26765810.1398.16.4.15.6]
Journal of Iranian Association of Electrical and Electronics Engineers - Vol.16- No.4- Winter2018

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

$$f_{00}=\lambda_a(\lambda+\mu+\mu_p)+\lambda_p(\lambda+\mu+\mu_a),\quad g=\lambda(\lambda_a+\lambda_p+\mu_p)+\lambda_a(\mu+\mu_p)+\lambda_p(\mu+\mu_a)+\mu_a(\mu+\mu_p),\qquad(۳۱)$$

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

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

$$p_{01}=\frac{(\lambda\lambda_a+\lambda\lambda_p+\lambda_p\mu_a)-e^{-t\rho}(\cosh(\beta t)-\frac{\sinh(\beta t)\zeta_{01}}{\beta})\times f_{01}}{g},\quad f_{01}=(\lambda\lambda_a+\lambda\lambda_p+\lambda_p\mu_a),\qquad(۳۲)$$

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

$$p_{02}=\frac{(\lambda_a\mu+\lambda_p\mu+\lambda_a\mu_p)-e^{-t\rho}(\cosh(\beta t)-\frac{\sinh(\beta t)\zeta_{02}}{\beta})\times f_{02}}{g},\quad f_{02}=(\lambda_a\mu+\lambda_p\mu+\lambda_a\mu_p),\qquad(۳۳)$$

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

$$p_{10}=\frac{(\lambda\mu_p+\mu\mu_a+\mu_a\mu_p)-e^{-t\rho}(\cosh(\beta t)-\frac{\sinh(\beta t)\zeta_{10}}{\beta})\times f_{10}}{g},\quad f_{10}=(\lambda\mu_p+\mu\mu_a+\mu_a\mu_p),\qquad(۳۴)$$

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

$$p_{11}=\frac{(\lambda\lambda_a+\lambda\lambda_p+\lambda_p\mu_a)+e^{-t\rho}(\cosh(\beta t)-\frac{\sinh(\beta t)\zeta_{11}}{\beta})\times f_{11}}{g},\quad f_{11}=\mu(\lambda_a+\lambda_p+\mu_a)+\mu_p(\lambda+\lambda_a+\mu_a),\qquad(۳۵)$$

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

$$p_{12}=\frac{(\lambda_a\mu+\lambda_p\mu+\lambda_a\mu_p)-e^{-t\rho}(\cosh(\beta t)-\frac{\sinh(\beta t)\zeta_{12}}{\beta})\times f_{12}}{g},\quad f_{12}=\lambda_a\mu+\lambda_p\mu+\lambda_a\mu_p,\qquad(۳۶)$$

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

$$p_{20}=\frac{(\lambda\mu_p+\mu\mu_a+\mu_a\mu_p)-e^{-t\rho}(\cosh(\beta t)-\frac{\sinh(\beta t)\zeta_{12}}{\beta})\times f_{20}}{g},\quad f_{20}=\lambda\mu_p+\mu\mu_a+\mu_a\mu_p,\qquad(۳۷)$$

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

$$p_{21}=\frac{(\lambda\lambda_a+\lambda\lambda_p+\lambda_p\mu_a)-e^{-t\rho}(\cosh(\beta t)-\frac{\sinh(\beta t)\zeta_{21}}{\beta})\times f_{21}}{g},\quad f_{21}=\lambda\lambda_a+\lambda\lambda_p+\lambda_p\mu_a,\qquad(۳۸)$$

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

$$p_{22}=\frac{(\lambda_a\mu+\lambda_p\mu+\lambda_a\mu_p)+e^{-t\rho}(\cosh(\beta t)-\frac{\sinh(\beta t)\zeta_{22}}{\beta})\times f_{22}}{g},\quad f_{22}=\lambda(\lambda_a+\lambda_p+\mu_p)+\mu_a(\lambda_p+\mu+\mu_p),\qquad(۳۹)$$

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

[DOR: 20.1001.1.26765810.1398.16.4.15.6]

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 به‌صورت 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. $\mathbf{P}(t)$ یک ماتریس تصادفی است، بنابراین اولین امتحان برای پی بردن به صحت معادلات به دست آمده بالا، آزمون تصادفی بودن این ماتریس است. برای این‌که $\mathbf{P}(t)$ یک ماتریس تصادفی باشد، باید جمع عناصر روی یک ردیف آن برابر یک باشد، به‌عبارت‌دیگر داشته باشیم:

$$\sum_{j=0}^{2} p_{i,j} = 1, \qquad (۴۰)$$

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 یکه باشد. به‌عبارت‌دیگر باید داشته باشیم:

$$\lim_{t\to 0}\mathbf{P}(t) = \mathbf{I}_{3\times 3} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad (۴۱)$$

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

$$\mathbf{P}'(0) = \mathbf{Q}. \qquad (۴۲)$$

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. Pourgharehkhan, 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.

[۴] عباس زاده حمیده، حسینی سنو سید امین. "ساخت توپولوژی انرژی‌آگاه 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.

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

[۹] 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. Pourgharehkhan, "Secure multiple antennas spectrum sensing under continuous attacking traffic," 8'th 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.

زیرنویس‌ها

[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)

[DOR: 20.1001.1.26765810.1398.16.4.15.6]
Journal of Iranian Association of Electrical and Electronics Engineers - Vol.16- No.4- Winter2018