مجله علمی پژوهشی «علوم و فناوری‌های پدافند نوین»
سال ششم، شماره ۲، تابستان ۱۳۹۴؛ ص ۱۵۱-۱۴۵

بهبود سنجش مشارکتی طیف در حضور کاربران ثانویه مخرب در شبکه‌های رادیو شناختی

سعید خباز خِرامه[۱]، سید محمد علوی[۲*]، سید محمد سجاد صدوق[۳]

۱- دانشجوی کارشناسی ارشد ۲- استادیار دانشگاه جامع امام حسین (ع) ۳- استادیار دانشگاه شهید بهشتی

(دریافت: ۹۴/۰۱/۰۴، پذیرش: ۹۴/۰۲/۲۲)

چکیده

در شبکه‌های رادیوشناختی سنجش دقیق طیف از اهمیت بالایی برخوردار است. نتایج سنجش غلط می‌تواند هم موجب اتلاف طیف و هم باعث تداخل مضر با کاربران اولیه شود. به منظور بهبود دقت، سنجش مشارکتی طیف که در آن یک گروه از کاربران ثانویه به طور مشارکتی طیف حضور کاربر اولیه را سنجش می‌کنند، معرفی می‌شود. با این حال، این روش پنجره‌ای را برای استفاده کاربران مخربی که ممکن است اقدام به ارسال داده غلط به مرکز ترکیب داده کنند، باز می‌کند. این نوع ارسال داده غلط به مرکز ترکیب داده که به شدت می‌تواند موجب اختلال در عملکرد شبکه شود را اصطلاحاً حملات تحریف داده سنجش یا SSDF گویند. در این مقاله، با تمرکز بر رفتار آماری کاربران ثانویه و با استفاده از الگوریتم EM احتمالات آشکارسازی و هشدار غلط کاربران و در نتیجه حالت صحیح طیف تخمین زده می‌شوند. نتایج عددی، بیانگر بهبود عملکرد سنجش مشارکتی طیف در حضور کاربران مخرب نسبت به روش‌های اعتبار پایه رایج به منظور مقابله با حملات SSDF هستند. همچنین نتایج حاصل بیانگر افزایش سرعت سیستم و کاهش هزینه مخابراتی است.

کلید واژه‌ها: **شبکه‌های رادیوشناختی، کاربر ثانویه، سنجش مشارکتی طیف، کاربران مخرب، حملات SSDF، الگوریتم EM.**

Improving Cooperative Spectrum Sensing in the Presence of Malicious Secondary Users in Cognitive Radio Networks

S. Khabbaz Kherameh, S. M. Alavi[*], S. M. S. Sadoogh
Imam Hossein University

(Received: 24/03/2015; Accepted: 12/05/2015)

Abstract

Accurate spectrum sensing is very important in cognitive radio networks. False sensing results in either waste of spectrum or harmful interference to primary users. To improve accuracy, cooperative spectrum sensing, in which a set of secondary users cooperatively sense the presence of the primary user, has emerged. This technique, however, opens a window for malicious users, who may send false data to the fusion center. This kind of sending false data to the fusion center, which can severely disturb the network, is called spectrum sensing data falsification (SSDF) attacks. In this paper, focusing on stochastic behavior of secondary users and using Expectation-Maximization (EM) algorithm, detection and false alarm probabilities and then the true spectrum state are estimated. Numerical results show improvement in cooperative spectrum sensing operation in respect of common reputation based methods for defending against SSDF attacks. The results also show an increasing in system's speed and a reduction in communication's cost.

Keywords: Cognitive Radio Networks, Secondary User, Cooperative Spectrum Sensing, Malicious Users, SSDF Attacks, EM Algorithm.

[*]Corresponding Author E-mail: Malavi@ihu.ac.ir

۱. مقدمه

طی یک دهه گذشته ارائه استانداردها و کاربردهای چندرسانه‌ای جدید بی‌سیم موجب افزایش تعداد کاربران و همچنین افزایش نرخ‌های ارسال داده شده است. این حجم روزافزون داده باید از طریق همان طیف‌های ثابت تخصیص داده شده به کاربران ارسال گردد. این امر در کنار استفاده ناکارآمد از طیف‌های ثابت تخصیص داده شده، سبب شده است تا روش بهره‌گیری از طیف فرکانسی بی‌سیم با یک چالش اساسی به نام کمبود طیف مواجه گردد [۱]. با توجه به محدودیت‌های طبیعی طیف فرکانسی بی‌سیم، واضح است که روش‌های استاتیک فعلی تخصیص فرکانس نمی‌توانند این نیازها را برآورده کند. بنابراین روش‌های جدیدی که بتواند راهکارهای دیگری برای بهره‌برداری از طیف موجود را پیشنهاد دهند، مانند دسترسی دینامیک به طیف (DSA[1]) مورد نیاز است. رادیو شناختگر[2] به عنوان راه‌حلی برای مشکل کمبود طیف، مطرح شده که استفاده فرصت‌طلبانه از باندهای فرکانسی خالی را ممکن می‌سازد [۲].

در اصطلاح رادیو شناختگر، کاربران اولیه[3] به کاربرانی اطلاق می‌شود که دارای اولویت بیشتر یا حق قانونی برای استفاده از بخش مشخصی از طیف فرکانسی هستند. در طرف مقابل کاربران ثانویه[4] قرار دارند که یا دارای مجوز استفاده از طیف نیستند و یا دارای اولویت پایین‌تر بوده و باید به نحوی از طیف استفاده کنند که هیچ‌گونه تداخل مضری برای کاربران اولیه ایجاد نکنند. مهم‌ترین وظیفه یک رادیو شناختگر (کاربر ثانویه)، سنجش طیف یا آشکارسازی حفره‌های طیفی است. حفره طیف به عنوان یک باند فرکانسی که به یک کاربر اولیه تخصیص داده شده، اما در یک زمان خاص و مکان جغرافیایی معین توسط آن کاربر استفاده نمی‌شود، تعریف می‌گردد. با توجه به اینکه اساس سنجش طیف بر روش‌های رایج آشکارسازی سیگنال است، مطلوب، نرخ آشکارسازی صحیح بالا و هشدار غلط پایین می‌باشد تا هم تداخل کاربران ثانویه با فرستنده‌های اولیه و هم اتلاف طیف کاهش یابد [۳].

به منظور سنجش طیف در شبکه‌های رادیو شناختی، هر کاربر ثانویه می‌تواند به تنهایی و با استفاده از روش‌های رایج آشکارسازی (مانند: آشکارساز انرژی، فیلتر منطبق و...) طیف مربوط به کاربر اولیه را بسنجد و در مورد طیف مورد نظر تصمیم‌گیری کند که به این روش سنجش طیف، سنجش محلی طیف[5] گویند. در عمل وجود عواملی مانند محوشدگی و یا پدیده سایه می‌تواند به شدت عملکرد این نوع از سنجش طیف را کاهش دهد. برای افزایش دقت و کاهش اثرات محوشدگی و سایه، سنجش مشارکتی طیف[6] پیشنهاد می‌شود که در آن کاربران داده‌های حاصل از سنجش خود را به اشتراک می‌گذارند [۴].

اگرچه سنجش مشارکتی طیف دقت تخمین حالت طیف را بالاتر می‌برد ولی در برابر خطرات بالقوه کاربران ثانویه مخرب آسیب‌پذیر است. این کاربران می‌توانند به طور عمد داده‌های حاصل از سنجش را به طور غلط به مرکز ترکیب داده ارسال کنند و موجب تصمیم اشتباه آن شوند. این نوع تهاجمات را تهاجمات SSDF[7] گویند [۵]. ثابت می‌شود که حتی حضور یک کاربر مخرب با رویکرد SSDF می‌تواند اثرات زیان‌باری را بر شبکه‌های رادیوشناختی وارد نماید [۶].

اکثر روش‌های موجود به منظور مقابله با حملات SSDF، بر پایه متریک اعتباری[8] است که هر کاربر اعتبارش را از مرکز ترکیب داده (یا سایر کاربران) دریافت می‌کند. به این نوع از روش‌ها، اعتبارپایه (RB[9]) گویند که در آن‌ها اعتبار هر کاربر بر اساس مقایسه گزارش‌های آن کاربر نسبت به اکثریت گزارش‌های کاربران و مقایسه با یک آستانه از پیش تعریف شده محاسبه می‌شود.

الگوریتم آشکارسازی ارائه شده در برخی گزارش‌ها [۶ و ۷]، مقادیر اعتبار کاربران ثانویه را بر اساس گزارشات قبلی‌شان محاسبه می‌کند. بر این اساس، اگر مشاهدات کافی موجود نباشد، متریک اعتبار می‌تواند ناپایدار باشد. به همین دلیل میزان ثبات هر کاربر را نیز محاسبه می کنند. اگر میزان ثبات و مقدار اعتبار کمتر از یک آستانه مشخص باشند، کاربر ثانویه به عنوان یک کاربر پرت در نظر گرفته خواهد شد و گزارش‌های آن در تصمیم‌گیری نهایی لحاظ نخواهد شد. یکی از عیوب روش این است که تنها یک کاربر مخرب را در نظر گرفته است. شبیه‌سازی‌ها نشان می‌دهند که اگر درصد کاربران مخرب کمتر از ۴۰٪ باشد، احتمال ایزوله شدن کاربران مخرب بیش از ۹۵٪ خواهد بود [۷]. برای وزن‌دهی به هر کاربر ثانویه از WSPRT[10] استفاده شده است [۸]. خروجی (باینری) هر کاربر مشابه خروجی مرکز ترکیب داده باشد، متریک اعتبار کاربر یک واحد افزایش می‌یابد و در غیر این صورت یک واحد کاهش می‌یابد. برخلاف برخی گزارش ها [۷]، اگر گره‌ای مکرراً بدرفتاری کند و در صورتی که بعد از مدتی دوباره رفتار مناسب داشته باشد، متریک اعتبار کاربر بازیابی خواهد شد.

اکثر روش‌های مقابله با حملات SSDF، آشکارسازی کاربران مخرب را از آشکارسازی حالت طیف، به طور جداگانه انجام می‌دهند. اخیراً کارهای ارزشمندی انجام شده است که در آن ها کاربران مخرب را توأماً با حالت طیف، آشکار می‌کنند. در گزارشی یک الگوریتم آشکارسازی سریع که در آن کاربران (صادق و مخرب) را در بیش از دو گروه گروه‌بندی می‌کند و توأماً حالت طیف را نیز تخمین می‌زند، ارائه شده است[۹]. در این گزارش، فرض شده است که کاربران هر گروه، دارای احتمالات آشکارسازی و هشدار غلط یکسان هستند. همچنین برای سادگی فرض شده است که گروه اول، گروه کاربران صادق است.

[1] Dynamic Spectrum Access
[2] Cognitive Radio
[3] Primary Users
[4] Secondary Users
[5] Local Spectrum Sensing
[6] Cooperative Spectrum Sensing
[7] Spectrum Sensing Data Falsification
[8] Reputation Metric
[9] Reputation Based
[10] Weighted Sequential Probability Ratio Test

یک الگوریتم DSND[1] برای آشکارسازی کاربران پرت استفاده شده است[۱۰]. یک کاربر ثانویه، کاربر پرت شناخته خواهد شد اگر گزارش‌هایش به مرکز ترکیب داده خیلی دور یا خیلی نزدیک به گزارش‌های ارسالی سایر کاربران باشد. نویسندگان دو نوع تهاجم را بررسی کرده‌اند: (۱) تهاجم مستقل[2] که در آن کاربر مخرب دانشی راجع به گزارش‌های کاربران معتبر ندارد و (۲) تهاجم همبسته[3] که در آن کاربر مخرب از گزارش سایر کاربران آگاه است. نتایج عددی نشان می‌دهند که در حالت تهاجم مستقل، کاربر مخرب بعد از تعداد زیادی سنجش طیف همیشه آشکار خواهد شد. برای تهاجم همبسته، اگر مهاجم اطلاعات دقیقی راجع به احتمالات آشکارسازی و هشدار غلط در اختیار داشته باشد، ممکن است آشکار نشود. با این حال در مقاله مزبور، توضیحات کافی بیان نشده است که چرا کاربر ثانویه‌ای که دارای گزارش‌های نزدیک به سایر کاربران باشد، مخرب محسوب می‌شود.

یک روش مقابله با حملات SSDF را در یک مدل توزیع شده برای شبکه‌های رادیویی اقتضایی[4] ارائه شده است[۱۱]. تفاوت کلیدی این کار با سایر کارهای توضیح داده شده در این بخش این است که هیچ مرکز ترکیب داده‌ای استفاده نشده است. کاربران ثانویه با مبادله اطلاعات بین یکدیگر به طور مستقل راجع به حضور یا عدم حضور کاربر اولیه تصمیم‌گیری می‌کنند. هر کاربر ثانویه از آشکارسازی انرژی برای تشخیص حضور یا عدم حضور کاربر اولیه استفاده می‌کند. سپس مشاهدات خود را با استفاده از اطلاعات دریافتی از همسایه‌های خود به‌روزرسانی می‌کند و این اطلاعات به‌روزرسانی شده را به سایرین ارسال می‌کنند. اطلاعات ارسال شده توسط مهاجمان بالقوه به گونه‌ای فیلتر می‌شود که هر کاربر ثانویه بیشینه انحراف اطلاعات دریافتی از مقدار متوسط را محاسبه می‌کند. کاربران با بیشینه انحراف، مهاجم در نظر گرفته می‌شوند و ورودی حاصل از آن‌ها در طول محاسبه نهایی (که به طور مستقل توسط هر کاربر انجام می‌شود) کنار گذاشته می‌شود.

با استفاده از الگوریتم EM رفتار آماری کاربران ثانویه تخمین زده شده است [۱۲]. لازم به ذکر است که این مرجع شباهت‌هایی در تخمین احتمالات آشکارسازی و هشدار غلط با مقاله ما دارد. در این مقاله به منظور تشخیص کاربر مخرب از صادق از یک متریک اعتبار استفاده شده است. اما این متریک هنگامی‌که کاربران دارای احتمال آشکارسازی و احتمال هشدار غلط برابری داشته باشند، عملکرد مناسبی نخواهد داشت.

در گزارشی با استناد به اینکه کلیه کاربران در حال سنجش محیط یک کاربر اولیه هستند، بنابراین فرض همبستگی داده‌های حاصل از سنجش کاربران نسبت به عدم همبستگی داده‌ها به واقعیت نزدیک‌تر است. برای لحاظ این فرض داده‌های حاصل از سنجش در زمان‌های مختلف را در یک مدل مارکوف مخفی مورد بررسی قرار می‌دهد و بعد از حصول احتمالات آشکارسازی و هشدار غلط کاربران، آن‌ها را در دو گروه صادق و مخرب دسته‌بندی می‌کند [۱۳].

در این مقاله، یک شبکه رادیو شناختی با دو گروه کاربر صادق و مخرب را در نظر گرفته شده است. مشارکت در سنجش به صورت متمرکز فرض شده است که در آن یک مرکز ترکیب داده گزارش‌های کاربران ثانویه را جمع‌آوری می‌کند و در مورد طیف تصمیم‌گیری می‌کند. در این مقاله ابتدا با استفاده از الگوریتم EM[5]، احتمالات آشکارسازی و هشدار غلط هر کاربر در مرکز ترکیب داده در هر لحظه از زمان تخمین زده می‌شوند و سپس مرکز ترکیب داده با استفاده از این مقادیر تخمین زده شده، حالت صحیح طیف را تخمین می‌زند. نتایج شبیه‌سازی‌ها بیانگر افزایش دقت در تخمین احتمالات آشکارسازی و هشدار غلط و در نتیجه حالت طیف در مقایسه با روش‌های رایج RB می‌باشد به طوری که هم سرعت عملکرد سامانه مشارکتی افزایش و هم تعداد کاربران لازم برای مشارکت کاهش می‌یابد. در بخش دوم این مقاله، روش تحقیق شامل مدل سامانه و فرضیات، نحوه تخمین احتمالات آشکارسازی و هشدار غلط کاربران با استفاده از EM و روابط مسئله بحث خواهند شد و در بخش سوم، نتایج شبیه‌سازی و بررسی عملکرد سامانه صورت می‌پذیرد. در نهایت نتیجه‌گیری پایانی بیان خواهد شد.

۲. روش تحقیق

در این بخش ابتدا مدل سامانه و فرضیات مسئله بیان می‌شود و سپس بر اساس این فرضیات و با اعمال روش EM پارامترهای مسئله شامل احتمالات آشکارسازی و هشدار غلط هر کاربر ثانویه از دید مرکز ترکیب داده و در نهایت با استفاده از این مقادیر، حالت طیف در هر لحظه از زمان تخمین زده می‌شود.

۲-۱. مدل سامانه و فرضیات

یک شبکه رادیو شناختی با L کاربر ثانویه که در حال مانیتورینگ باند طیف یک کاربر اولیه به منظور تشخیص حضور و یا عدم حضور آن کاربر اولیه می‌باشند، در نظر گرفته شود. فرض می‌شود که کاربران ثانویه طیف را به صورت مستقل می‌سنجند و گزارش‌های ارسالی کاربران به مرکز ترکیب داده از یکدیگر مستقل باشند.

در زمان $t \in \{1,2,\dots,T\}$ کاربر lام $(l = 1,2,\dots,L)$ یک تصمیم (مشاهده) باینری $u_{lt} \in \{0,1\}$ مبنی بر آزاد یا اشغال بودن طیف مورد نظر دارد که $u_{lt} = 0$ بیانگر تصمیم کاربر مبنی بر آزاد بودن طیف و $u_{lt} = 1$ بیانگر تصمیم کاربر مبنی بر اشغال بودن طیف است.

اشغال و آزاد بودن طیف را به ترتیب با دو فرضیه H_1 و H_0 نمایش

[1] Double – Sided Neighbor Distance
[2] Independent Attack
[3] Dependent Attack
[4] Ad-Hoc Network
[5] Expectation Maximization

داده و ماتریس فرضیه H را به صورت زیر تعریف می‌شود:

$$H = \begin{bmatrix} h_{01} & h_{02} & \cdots & h_{0T} \\ h_{11} & h_{12} & \cdots & h_{1T} \end{bmatrix}_{2\times T} \quad (۱)$$

که در آن، هر ستون بیانگر حالت طیف در یک زمان است. در هر لحظه از زمان، یکی از عناصر ستون صفر و دیگری یک است. اگر $h_{0t} = 1$ آنگاه $h_{1t} = 0$ خواهد بود و این یعنی در زمان t کانال آزاد است و فرضیه H_0 برقرار است.

فرض می‌شود که در طول بازه مشاهدات کاربران، شرایط کانال (محوشدگی و سایه) ثابت باشد. همچنین فرض می‌شود که داده‌های دریافتی از کاربران مختلف در طول زمان و کاربر به کاربر مستقل از یکدیگر باشند.

احتمالات آشکارسازی و هشدار غلط هر کاربر به صورت زیر حاصل می‌شود:

$$\tilde{p}_{il} = pr(u_{lt} = 1 | h_{it} = 1), i = 0,1 \quad (۲)$$

که در آن، $\tilde{p}_{1l}$ و $\tilde{p}_{0l}$ به ترتیب بیانگر احتمالات آشکارسازی و هشدار غلط از دید کاربر ثانویه می‌باشند.

در زمان t هر کاربر یک تک بیت باینری $d_{lt} \in \{0,1\}$ را به عنوان گزارش ارسالی به مرکز ترکیب داده ارسال می‌کند. در صورتی که کاربر صادق باشد $d_{lt} = u_{lt}$ و در غیر این صورت با فرض بدون خطا بودن کانال بین کاربران ثانویه و مرکز ترکیب داده، کاربر مخرب خواهد بود.

رفتار کاربران در کانال بین آن‌ها و مرکز ترکیب داده را به صورت زیر تعریف می‌شود:

$$\rho_{il} = pr(d_{lt} = 1 | u_{lt} = i), \quad i = 0,1 \quad (۳)$$

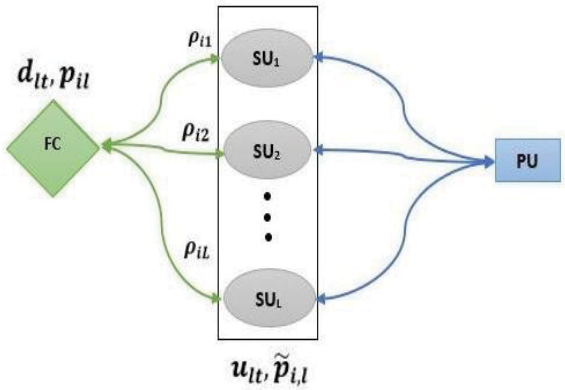
که در آن، ρ_{0l} بیانگر میزان تمایل کاربر برای هشدار غلط و ρ_{1l} میزان تمایل به ارسال صحیح در حالت اشغال بودن طیف به مرکز ترکیب داده (FC[1]) است. احتمالات آشکارسازی و هشدار غلط هر کاربر از دید FC که اساس تصمیم‌گیری FC بر طیف است، به صورت زیر محاسبه خواهند شد:

$$p_{il} = pr(d_{lt} = 1 | h_{it} = 1) = \rho_{1l}\tilde{p}_{il} + \rho_{0l}(1 - \tilde{p}_{il}), \quad i = 0,1 \quad (۴)$$

با فرض عاری از خطا بودن کانال بین کاربران ثانویه و FC، می‌توان ρ_{il} را بیانگر راهبرد تهاجم کاربران مخرب دانست. همچنین فرض می‌شود که کاربران مخرب راهبرد تهاجم خود را مکرراً تغییر نمی‌دهند و این به واقعیت نزدیک‌تر است زیرا تغییرات مکرر راهبرد تهاجم میزان خرابکاری و تأثیر آن را از دید کاربر مخرب کاهش خواهد داد [۱۴].

توجه به این نکته لازم است که در حالتی که کانال بین کاربران ثانویه و FC را نویزی و دارای خطا در نظر بگیرید، می‌توان اثرات خطای کانال را در فاکتور ρ_{il} دید. بنابراین روش ارائه شده علاوه بر کاربران مخرب، قادر به تشخیص حضور کاربران بدرفتار غیر متعمد که به علت شرایطی مثل محوشدگی و سایه در این کانال، داده غلط ارسال می‌کنند نیز می‌باشد.

مرکز ترکیب داده T داده ارسالی از هر کاربر را جمع‌آوری می‌کند و ماتریس گزارش‌های دریافتی کاربران را به صورت $D = [d_{lt}], l = 1,2,\dots,L \ , t = 1,2,\dots,T$ تشکیل می‌دهد و هدف آن آشکارسازی ماتریس H است. در این فرایند FC همچنین احتمالات آشکارسازی و هشدار غلط هر کاربر را به‌دست می‌آورد و ماتریس $P = [p_{il}]$ را تشکیل می‌دهد. شکل (۱) شمای کلی سامانه مورد بحث را به تصویر می‌کشد.



شکل ۱. سامانه رادیوشناختی بر اساس مفروضات مسئله

احتمالات پیشین هر فرضیه را در ماتریس $\Phi = [\phi_{it}]$ نمایش داده می‌شود که در آن $\phi_{it} = Pr(h_{it} = 1)$ است. واضح است که $\sum_{i=0}^{1} \phi_{it} = 1$.

در نهایت مجموعه دو پارامتری $\Theta \triangleq \{P, \Phi\}$ را تعریف می‌شود و در بخش بعد این پارامترها از طریق الگوریتم EM و با استفاده از ماتریس گزارش‌های کاربران یعنی D در FC تخمین زده می‌شوند.

۲-۲. اعمال روش EM در تخمین پارامترهای مسئله و تخمین حالت طیف

تخمین پارامترهای مسئله: یک تخمین با معیار ML برای Θ به صورت زیر خواهد بود:

$$\widehat{\Theta} = argmax_{\Theta} \Pr(D|\Theta) \quad (۵)$$

و از آنجایی که محاسبه مستقیم $\Pr(D|\Theta)$ امکان‌پذیر نیست، می‌توان این تابع را به صورت زیر محاسبه کرد:

$$\Pr(D|\Theta) = \sum_H Pr(D, H|\Theta) \quad (۶)$$

به علت پیچیدگی محاسبه این تابع، تخمین پارامترهای Θ در یک فرم بسته امکان‌پذیر نخواهد بود. بنابراین از الگوریتم EM برای تخمین پارامترها استفاده خواهد شد. ابتدا باید تابع $Pr(D, H|\Theta)$ را

[1] Fusion Center

به‌دست آورید که به صورت زیر حاصل می‌شود:

$$Pr(D,H|\Theta) = Pr(D|H;\Theta)Pr(H|\Theta)$$
$$= \prod_{l=1}^{L}\left[\prod_{t=1}^{T}\prod_{i=0}^{1}\left(p_{il}^{d_{lt}}(1-p_{il})^{(1-d_{lt})}\phi_{it}^{\frac{1}{L}}\right)^{h_{it}}\right] \quad (۷)$$

که در آن، $Pr(D|H;\Theta)$ طبق رابطه (۴) بیان کننده p_{il} و $Pr(H|\Theta)$ برابر خواهد بود با ϕ_{it}.

پس از محاسبه رابطه $Pr(D,H|\Theta)$ نوبت به محاسبه تابع شباهت لگاریتمی[1] زیر خواهد بود:

$$L(\Theta;D,H) = \log Pr(D,H|\Theta)$$
$$= \sum_{l=1}^{L}\sum_{t=1}^{T}\sum_{i=0}^{1}\left\{\left[d_{lt}\log p_{il} + (1-d_{lt})\log(1-p_{il}) + \frac{1}{L}\log\phi_{it}^{h_{it}}\right]\right\} \quad (۸)$$

هر تکرار الگوریتم EM شامل دو مرحله خواهد بود: (۱) مرحله امیدگیری[2] و (۲) مرحله بیشینه‌گیری[3]

مرحله امیدگیری: ابتدا تابع $Q(\Theta;\Theta^{old})$ با امیدگیری از تابع $L(\Theta;D,H)$ روی تابع توزیع احتمال متغیر مخفی[4] (H) یعنی $Pr(H|D;\Theta^{old})$ حاصل می‌شود، که Θ^{old} تخمین مرحله قبل Θ می‌باشد.

$$Q(\Theta;\Theta^{old}) \triangleq E_{(H)|D;\Theta^{old}}[L(\Theta;D,H)] \quad (۹)$$
$$= \sum_{l=1}^{L}\sum_{t=1}^{T}\sum_{i=0}^{1}\left\{E_{(H)|D;\Theta^{old}}[h_{it}]\left[d_{lt}\log p_{il} + (1-d_{lt})\log(1-p_{il}) + \frac{1}{L}\log\phi_{it}\right]\right\}$$

تعریف می‌کنیم:

$$\alpha(i,t) = E[h_{it}|D;\Theta^{old}]$$
$$= Pr(h_{it}=1|D;\Theta^{old}) \quad (۱۰)$$

که در آن، $Pr(h_{it}=1|D;\Theta^{old})$ به صورت زیر حاصل خواهد شد:

$$Pr(h_{it}=1|D;\Theta^{old}) = Pr(h_{it}=1|d_t;\Theta^{old}) \quad (۱۱)$$
$$= \frac{Pr(d_t|h_{it}=1;\Theta^{old})Pr(h_{it}=1|\Theta^{old})}{\sum_{j=0}^{1}\{Pr(d_t|h_{jt}=1;\Theta^{old})Pr(h_{jt}=1|\Theta^{old})\}}$$
$$= \frac{\phi_{it}^{old}\prod_{l=1}^{L}\left((p_{il}^{old})^{d_{lt}}(1-p_{il}^{old})^{(1-d_{lt})}\right)}{\sum_{j=0}^{1}\left[\phi_{jt}^{old}\prod_{l=1}^{L}\left((p_{jl}^{old})^{d_{lt}}(1-p_{jl}^{old})^{(1-d_{lt})}\right)\right]}$$

رابطه (۹) با استفاده از رابطه (۱۱) به صورت زیر تبدیل می‌شود:

$$Q(\Theta;\Theta^{old}) = \frac{1}{L}\sum_{l=1}^{L}\sum_{t=1}^{T}\sum_{i=0}^{1}\alpha(i,t)\log\phi_{it} \quad (۱۲)$$
$$+\sum_{l=1}^{L}\sum_{t=1}^{T}\sum_{i=0}^{1}\alpha(i,t)[d_{lt}\log p_{il} + (1-d_{lt})\log(1-p_{il})]$$

مرحله بیشینه‌گیری:

در دومین مرحله تابع $Q(\Theta;\Theta^{old})$ را نسبت به پارامترهای مجموعه Θ بیشینه می‌کنیم.

• بیشینه کردن $Q(\Theta;\Theta^{old})$ نسبت به احتمالات آشکارسازی و هشدار غلط حاصل از ماتریس P.

$$\frac{\partial Q}{\partial p_{il}} = \sum_{t=1}^{T}\alpha(i,t)\left(\frac{d_{lt}}{p_{il}} - \frac{(1-d_{lt})}{(1-p_{il})}\right) = 0 \quad (۱۳)$$
$$p_{il}^{new} = \frac{\sum_{t=1}^{T}\alpha(i,t)d_{lt}}{\sum_{t=1}^{T}\alpha(i,t)}$$

• بیشینه‌گیری نسبت به ϕ_{it}

می‌توان با استفاده از قید $\sum_{i=0}^{1}\phi_{it}=1$ و استفاده از روش ضرایب لاگرانژ[5]، تابع $Q(\Theta;\Theta^{old})$ را نسبت به ϕ_{it} بیشینه کرد و ϕ_{it} بهینه را یافت.

$$\tilde{Q}(\Theta,\vartheta_t;\Theta^{old}) \triangleq Q(\Theta;\Theta^{old}) + \vartheta_t\left[\sum_{i=0}^{1}\phi_{it} - 1\right] \quad (۱۴)$$
$$\frac{\partial\tilde{Q}}{\partial\phi_{it}} = \alpha(i,t)\frac{1}{\phi_{it}} + \vartheta_t = 0$$

با ضرب طرفین در ϕ_{it} و جمع روی i، $\vartheta_t=-1$ خواهد بود و بنابراین

$$\phi_{it}^{new} = \alpha(i,t) \quad (۱۵)$$

تخمین حالت طیف: برای حصول ماتریس H می‌توان به صورت زیر عمل کرد:

$$\hat{h}_{0t} = \begin{cases}1, & \hat{\emptyset}_{0t} > \hat{\emptyset}_{1t}\\ 0, & else\end{cases}$$
$$\hat{h}_{1t} = \begin{cases}1, & \hat{\emptyset}_{1t} > \hat{\emptyset}_{0t}\\ 0, & else\end{cases} \quad (۱۶)$$

به طور خلاصه، الگوریتم کلی مسئله به صورت زیر می‌باشد:

ورودی: D
خروجی: H

شروع
- برای t=1:T
- مقداردهی اولیه پارامترهای مجموعه Θ، $\Theta_{ini}^{old}=\{p_{ini}^{old},\phi_{ini}^{old}\}$
- محاسبه مقادیر جدید پارامترهای مجموعه Θ یعنی $\Theta^{new}=\{p^{new},\phi^{new}\}$ با استفاده از (۱۳) و (۱۵)
- تخمین حالت طیف در زمان t با استفاده از رابطه (۱۶)

پایان

۳. نتایج و بحث

به منظور بررسی عملکرد روش پیشنهادی، خطای تخمین احتمالات آشکارسازی و هشدار غلط و همچنین خطای تخمین طیف را در مقایسه با روش رایج RB مقایسه شده است. روابط (۱۷ و ۱۸) به

[1] Log Likelihood Function
[2] Expectation Step
[3] Maximization Step
[4] Latent Variable
[5] Lagrange Multiplier Method

ترتیب بیانگر خطای تخمین حالت طیف و خطای تخمین احتمالات آشکارسازی و هشدار غلط (خطای تخمین ماتریس P) می‌باشند.

$$\Delta_H = \frac{1}{2T}\sum_{i=0}^{1}\sum_{t=1}^{T}|h_{it} - \hat{h}_{it}| \qquad (۱۷)$$

$$\Delta_P = \frac{1}{\sqrt{2}L}\sum_{l=1}^{L}\sqrt{(p_{0l} - \hat{p}_{0l})^2 + (p_{1l} - \hat{p}_{1l})^2} \qquad (۱۸)$$

قبل از ورود به بررسی نتایج عددی، لازم است مختصراً روش RB شرح داده شود. در RB حالت طیف به صورت زیر تخمین زده می‌شود [۸ و ۱۵]:

$$\hat{h}_{1t} = \begin{cases} 1, & \sum_{l=1}^{L} d_{lt} > q \\ 0, & else \end{cases} \quad ,for: t = 1,2,\dots,T. \qquad (۱۹)$$

پس از تخمین حالت طیف، احتمالات آشکارسازی و هشدار غلط هر کاربر به صورت زیر حاصل خواهد شد.

$$\hat{p}_{il} = \frac{\sum_{t=1}^{T}\hat{h}_{it}d_{lt}}{\sum_{t=1}^{T}\hat{h}_{it}} \qquad (۲۰)$$

دو گروه کاربر یکی صادق و دیگری مخرب را در نظر بگیرید. کاربران صادق دارای احتمال آشکارسازی $p_d = 0.85$ و احتمال هشدار غلط $p_{fa} = 0.2$ می‌باشند.

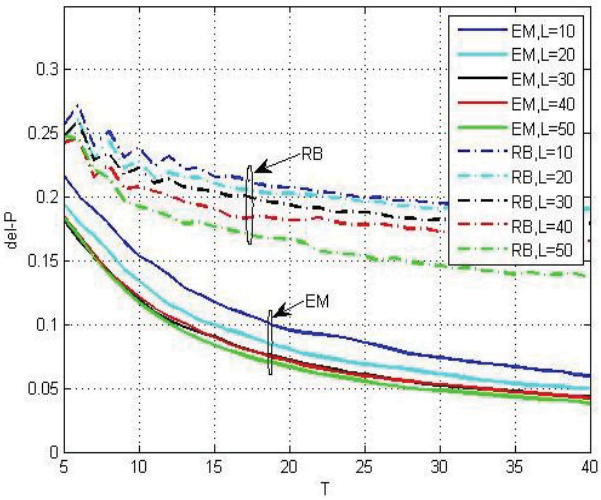
فرض کنید کاربران مخرب دارای سطح تهاجم $\rho_0 = 0.75$ و $\rho_1 = 0.2$ هستند و این بدان معناست که این کاربران در کانال بین خود و FC با احتمال ۰/۷۵ میل به هشدار غلط و با احتمال ۰/۲ میل به آشکارسازی دارند. با استفاده از رابطه (۴) احتمال آشکارسازی و هشدار غلط کاربران مخرب برابر خواهد بود با $p_d = 0.28$ و $p_{fa} = 0.64$. همچنین ۶۰٪ کل کاربران صادق و ۴۰٪ مخرب هستند. نتایج حاصله با اجرای ۱۰۰۰۰ تکرار Monte Carlo و میانگین‌گیری روی این تعداد حاصل شده است.

۳-۱. بررسی خطای تخمین احتمالات آشکارسازی و هشدار غلط

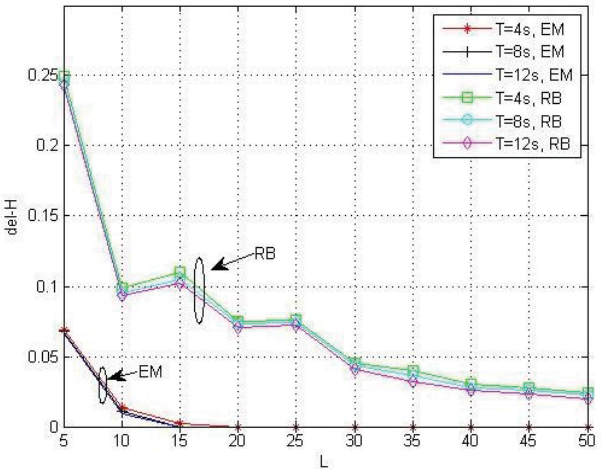
شکل (۲) مقایسه خطای حاصل از رابطه (۱۸) را در طول زمان و برای L = {10,20,30,40,50} را نشان می‌دهد. همان‌طور که از شکل پیداست، سامانه EM به ازای تمام Lها دارای بیشینه خطا و کمینه خطای کمتری نسبت به سامانه RB است. همچنین سامانه مبه ویژه برای L = {30,40,50} حساس به تغییر در مقدار L نیست و این یعنی به ازای L های کمتر نیز می‌توان به خطای مطلوب (نسبت به سامانه RB) رسید. ضمناً با افزایش T خطا میل به صفر شدن دارد.

۳-۲. بررسی خطای تخمین حالت طیف

برای این منظور رابطه (۱۷) بر اساس تعداد کاربران L و برای بازه‌های زمانی مشخص بررسی شده است. همان‌طور که از شکل (۳) مشاهده می‌شود، در تخمین طیف به روش EM تنها با تعداد حدود ۱۵ کاربر می‌توان خطای تخمین را حتی با ۴ ثانیه سنجش، به صفر رسانید و الگوریتم به ازای زمان‌های بررسی شده، به طول بازه سنجش حساس نشده است. این در حالی است که در روش RB حتی به ازای ۵۰ کاربر نیز خطای تخمین خواهیم داشت و این بدان معناست که تعداد کاربران لازم برای مشارکت در روش EM نسبت به روش RB کاهش قابل ملاحظه‌ای می‌یابد و این کاهش هزینه مخابراتی و پیچیدگی سنجش مشارکتی را در پی خواهد داشت. البته در RB نیز الگوریتم حساس به زمان نشده است و با توجه به زمان‌های در نظر گرفته شده، نتایج به ازای هر تعداد کاربر برای این زمان‌ها به یکدیگر نزدیک است.



شکل ۲. بررسی خطای تخمین احتمالات آشکارسازی و هشدار غلط



شکل ۳. بررسی خطای تخمین حالت طیف

۴. نتیجه‌گیری

در این مقاله مسئله سنجش مشارکتی طیف در حضور کاربران مخرب ثانویه در شبکه‌های رادیو شناختی بررسی شد. به منظور مقابله با حملات SSDF، با استفاده از الگوریتم EM دقت تخمین احتمالات آشکارسازی و هشدار غلط و در نتیجه دقت تخمین حالت طیف افزایش داده شد. با توجه به نتایج شبیه‌سازی‌ها، خطای تخمین پارامترهای مسئله شامل احتمالات آشکارسازی و هشدار غلط و همچنین خطای تخمین حالت طیف به میزان قابل توجهی نسبت به روش رایج RB کاهش می‌یابند، به طوری که خطای حاصل از تخمین ماتریس P با استفاده از الگوریتم EM دارای مقادیر بیشینه و کمینه کمتری نسبت به روش RB است و با افزایش بازه سنجش این

خطا به صفر میل خواهد کرد و این افزایش دقت تخمین منجر به تخمین دقیق‌تر حالت صحیح طیف خواهد شد. همچنین علی‌رغم اینکه سنجش مشارکتی طیف دقت سنجش را نسبت به سنجش محلی بالاتر می‌برد ولی نیازمند صرف هزینه مخابراتی برای به اشتراک گذاشتن داده‌های حاصل از سنجش است. به وضوح از نتایج پیداست که در روش پیشنهادی زمان و تعداد کاربران مورد نیاز برای تخمین حالت طیف در چارچوب سنجش مشارکتی کاهش می‌یابد و این به معنای افزایش سرعت سامانه و کاهش هزینه مخابراتی است.

۵. مراجع

[1] Engelman, R. "Fcc Report of the Spectrum Efficiency Working Group"; FCC Spectrum Policy Task Force, 2002.

[2] Akyildiz, I. F.; Lee, W. "Next Generation/Dynamic Spectrum Access/Cognitive Radio Wireless Networks: A Survey"; Computer Networks 2006, 13, 2127-2159.

[3] Haykin, S. "Cognitive Radio: Brain-Empowered Wireless Communications"; IEEE J. Selected Areas in Communications 2005, 2, 201-220.

[4] Yifeng, C.; Huazhong, U. "Optimal Data Fusion of Collaborative Spectrum Sensing under Attack in Cognitive Radio Networks Network"; IEEE Net. 2014, 1, 17-23.

[5] Jana, S.; Kai, Z. "Trusted Collaborative Spectrum Sensing for Mobile Cognitive Radio Networks"; IEEE Trans. Information Forensics and Security 2013, 9, 1497-1507.

[6] Wenkai, W.; Husheng, L. "Attack-Proof Collaborative Spectrum Sensing in Cognitive Radio Networks"; In Proc. of IEEE Int. Information Sci. and Syst. 2009, 130-134.

[7] Rawat, A. S.; Anand, P. "Countering Byzantine Attacks in Cognitive Radio Networks"; In Proc. of IEEE Int. Acoustics Speech and Signal Processing (ICASSP) 2010, 3098-3101.

[8] Ruiliang, C.; Jung-Min, P.; Kaigui, B. "Robust Distributed Spectrum Sensing in Cognitive Radio Networks"; In Proc. of IEEE Int. INFOCOM 2008, 13-18.

[9] Soltanmohammadi, E.; Naraghi-Pour, M. "Fast Detection of Malicious Behavior in Cooperative Spectrum Sensing"; IEEE J. Selected Areas in Communications 2014, 3, 377-386.

[10] Husheng, L.; Zhu, H. "Catch Me if You Can: An Abnormality Detection Approach for Collaborative Spectrum Sensing in Cognitive Radio Networks"; IEEE Trans. Wireless Communications 2010, 11, 3554-3565.

[11] Yu, F. R.; Tang, H. "Defence Against Spectrum Sensing Data Falsification Attacks in Mobile Ad Hoc Networks with Cognitive Radios"; In Proc. of IEEE Int. MILCOM 2009, 1-7.

[12] Du, Jun.; Chaocan, X. "Counteracting Malicious Users in Cognitive Radio Networks over Imperfect Reporting Channels"; In Proc. of IEEE Int. Wireless Communications and Signal Processing (WCSP) 2014, 1-6.

[13] He, Xiaofan.; Dia, H.; and Ning, P. "HMM-Based Malicious User Detection for Robust Collaborative Spectrum Sensing"; IEEE J. Selected Areas in Communications. 2013, 11, 2196-2208.

[14] Penna, F.; Yifan, S. "Detecting and Counteracting Statistical Attacks in Cooperative Spectrum Sensing"; IEEE Trans. Signal Proc. 2012, 4, 1806-1822.

[15] Huifang, C.; Xu, J.; Lei, X. "Reputation-Based Collaborative Spectrum Sensing Algorithm in Cognitive Radio Networks"; In Proc. of IEEE Int. Personal, Indoor and Mobile Radio Communications 2009, 582-587.

[16] Zhang, Y.; Zheng, J.; Chen, H. H. "Cognitive Radio Networks: Architectures, Protocols, and Standards"; AUERBACH Publications, 2010.