آشکارسازی و تعیین وفقی حملهٔ اختلال فریبنده در شبکه‌های رادیوشناختگر

زهرا قره‌خانی[۱]، کمال شاه‌طالبی[۲]، سیدمحمد صابرعلی[۳]

۱- دانشجوی کارشناسی ارشد، گروه مهندسی برق - دانشگاه اصفهان- اصفهان- ایران
gharekhanizahra@gmail.com
۲- دانشیار، گروه مهندسی برق - دانشگاه اصفهان- اصفهان- ایران
shahtalebi@eng.ui.ac.ir
۳- استادیار، گروه مهندسی برق - دانشگاه اصفهان- اصفهان- ایران
sm.saberali@eng.ui.ac.ir

چکیده: در این مقاله روشی نوین برای آشکارسازی حملهٔ جمر فریبنده و تمایز سیگنال ارسالی آن با سیگنال کاربر واقعی در شبکه‌های رادیوشناختگر ارائه شده است. در روش پیشنهادی از داده‌های عادی دریافتی در یک ساختار تخمین‌زن برای تخمین خطی هر نمونه بر حسب نمونه‌های قبلی استفاده شده است. ضرائب (وزن‌های) تخمین با ضرائبی مقایسه می‌شود که از قبل و براساس دریافت دنبالهٔ مرجع به دست آمده و اصالت انتساب و ارسال این دنباله از طرف کاربر اولیه احراز شده است. اختلاف کم نرم ضرائب این دو تخمین، نشان‌دهندهٔ ارسال دنبالهٔ دادهٔ عادی از طرف کاربر اولیه و اختلاف زیاد آن دو، نشان‌دهندهٔ ارسال آن از طرف حمله‌کنندهٔ فریبنده و اشغال کانال است. الگوریتم استفاده‌شده در تخمین ضرائب، الگوریتم NLMS است. تجزیه و تحلیل انجام‌شده و نتایج شبیه‌سازی، نشان‌دهندهٔ عملکرد مطلوب روش پیشنهادی است.

واژه‌های کلیدی: الگوریتم NLMS، حمله‌کنندهٔ فریبنده، رادیوشناختگر، کاربر اولیه، کاربر ثانویه

۱- مقدمه

شبکه‌های رادیوشناختگر نمونه‌ای ازمخابرات بی‌سیم هستند که در آن‌ها فرستنده‌های شبکه‌ای موسوم به شبکهٔ ثانویه، به‌طور هوشمندانه، کانال‌های در حال استفاده و همچنین کانال‌های بدون استفاده (خالی) را از شبکهٔ دیگری موسوم به شبکهٔ اولیه، تشخیص می‌دهند و در انتقال داده، تنها از کانال‌های خالی آن استفاده می‌کنند. به این ترتیب، تشخیص طیف و اطمینان از اشغال‌نشدن آن توسط کاربران اولیه، ازجمله مباحث بسیار مهم در این شبکه‌ها هستند.

حملهٔ فریبنده یکی از انواع حملاتی است که متوجه بخش تشخیص طیف در شبکه‌های رادیوشناختگر است. در این حمله، عنصری، خواه از داخل شبکهٔ ثانویه و یا خارج از آن (که از آن با عنوان حمله‌کنندهٔ فریبنده، و یا به اختصار حمله‌کننده یا جمر (Jammer) یاد می‌شود)، تلاش می‌کند باوجود خالی‌بودن کانالی از شبکهٔ اولیه، کاربران شبکهٔ ثانویه را فریب دهد و این تصور را برای آنها به وجود آورد که کاربری از کاربران اولیه، آن کانال را اشغال کرده است و امکان استفاده از آن وجود ندارد.

روش‌های گوناگونی برای شناسایی و تشخیص این نوع حمله‌ها ارائه شده است. در مراجع [۱] و [۲]، تشخیص و آشکارسازی حملهٔ فریبنده با بررسی موقعیت‌های مکانی صورت گرفته است. در مقابل، راه‌کارهای دیگری نیز پیشنهاد شده‌اند که تمرکزی بر روی موقعیت و مختصات فرستنده‌ها ندارند؛ بلکه معیار تشخیص و تصمیم‌گیری خود

[۱] تاریخ ارسال مقاله: ۱۳۹٤/۹/۳۰
تاریخ پذیرش مقاله: ۱۳۹٦/۰۱/۲٦
نام نویسندهٔ مسئول: کمال شاه‌طالبی
نشانی نویسندهٔ مسئول: ایران - اصفهان - خیابان هزار جریب - دانشگاه اصفهان- گروه مهندسی برق

را از طریق تعیین هویت فرستنده از روی سیگنال فرستاده‌شده اعمال می‌کنند. روش ارائه‌شده در [۳] به همین صورت عمل می‌کند. در این روش، مشخصات هویتی فرستنده، ازجمله فرکانس حامل و اختلاف فاز از روی سیگنال فرستندهٔ کاربر اولیه تعیین می‌شود. کاربر ثانویه (که قصد اشغال باند کاربر اولیه را دارد) پس از دریافت و استخراج مشخصات سیگنال و هویت آن، این هویت را با هویت‌های ذخیره‌شدهٔ قبلی، مقایسه و معتبربودن یا نبودن فرستندهٔ کنونی را تعیین می‌کند.

در روش‌های مطرح‌شده، نیازمندی کاربر ثانویه به آگاهی قبلی از برخی از مشخصات فرستندهٔ کاربر اولیه، مانند دانستن محل فرستنده یا آگاهی از هویت کاربر اولیه یا وجود برخی محدودیت‌ها، چون ثابت‌بودن آنتن کاربر اولیه یا اینکه هویت این کاربر در سیگنال ارسالی موجود باشد و یا آگاهی از فرکانس‌های گردشی، سبب شده است که این راه‌حل‌ها محدود به تنها برخی شبکه‌ها و برخی کاربران شود. نویسندگان در [٤]، روشی مبتنی بر الگوی فعالیت سیگنال ارائه کرده‌اند؛ به گونه‌ای که کاربر ثانویه پس از دریافت سیگنال، الگوی آن را استخراج می‌کند که به‌صورت دنباله‌ای ON/OFF است. درواقع، هر دورهٔ ON نشان‌دهندهٔ مدت زمانی است که فرستنده در حال ارسال و اشغال کانال است. متناظر با آن، هر دورهٔ OFF مدت زمانی را نشان می‌دهد که فرستنده کانال را خالی کرده است. پس از دریافت الگوی سیگنال، از آن‌ها با بردارهای پایه استفاده می‌کند تا سیگنال اصلی را بازسازی کند و از این طریق، در هر زمان، سیگنال بازسازی‌شده را با سیگنال بازسازی‌شدهٔ اولیه، مقایسه و به این ترتیب، حضورداشتن یا نداشتن حمله‌کننده را مشخص می‌کند. اندیشهٔ به‌کاررفته در این روش از رفتار متفاوت جمر و کاربر اولیه الهام گرفته شده است. درواقع، حمله‌کننده به دلیل هدف خراب‌کارانهٔ خود و ایجاد اختلال در شبکه با افزایش دورهٔ ON در ارسال‌های خود، الگوی متفاوتی را ایجاد می‌کند و همین الگوی متفاوت، زمینه‌ساز تشخیص او می‌شود.

یکی دیگر از روش‌های آشکارسازی و مقابله با حملات تقلید از کاربر اولیه در [۵] ارائه شده است. در این روش تصمیم‌گیری نهایی درمورد اشغال یا خالی‌بودن طیف به‌صورت مشارکتی و بر اساس نتایجی انجام می‌شود که جداگانه از هر کاربر ثانویه به دست می‌آید.

با بررسی مقالات مختلفی که در زمینهٔ حملهٔ فریبنده در شبکه‌های رادیوشناختگر مطرح شده است، نکات درخور توجهی به دست می‌آید که در ادامه آنها را بررسی می‌کنیم. تقریباً تمامی روش‌های تشخیص حملهٔ فریبنده، ساختاری دو مرحله‌ای دارند. در مرحلهٔ اول، کاربر ثانویه، حضور سیگنال و به عبارتی دیگر اشغال طیف را تشخیص می‌دهد. این تشخیص معمولاً با آشکارسازی انرژی صورت می‌گیرد. در مرحلهٔ دوم، با تکنیک‌های ابداعی مطرح‌شده، تشخیص عامل اشغال کانال (یک کاربر واقعی اولیه یا حمله‌کنندهٔ فریبنده) انجام می‌شود. در این مقاله نیز فرض برآن است که به‌صورت پیش‌فرض، مرحلهٔ اول، یعنی تشخیص حضور یک سیگنال به کمک آشکارساز انرژی انجام‌شده و آنچه که در روش پیشنهادی، در تشخیص جمر از کاربر اولیه مطرح می‌شود، پس از طی این مرحله صورت می‌گیرد.

یکی از اطلاعاتی که به طراحان در اجرای مرحلهٔ دوم روش خود کمک می‌کند، بررسی خواص ذاتی اطلاعات فرستنده است؛ اطلاعاتی که در فرآیند انتقال اطلاعات، خدشه‌دار نشده‌اند و در محل هر گیرنده‌ای مشخص هستند. ازجمله مهم‌ترین این اطلاعات، نوع مدولاسیون استفاده‌شده و اندازهٔ پارامترهای آن، همانند نرخ بیت و مواردی از این نوع هستند. به‌طور مثال، اگر در تشخیص ماهیت مدولاسیون سیگنال اشغال‌کنندهٔ باند فرکانسی، مشخص شد که نوع مدولاسیون منطبق با مدولاسیون فرستندهٔ شبکهٔ اولیه نیست، معلوم می‌شود که عامل اشغال کانال، یک حمله‌کنندهٔ فریبنده است.

با توجه به اینکه معمولاً بهره‌برداری از ویژگی‌های مدولاسیون سیگنال‌ها، با استفاده از تئوری ایستان گردشی سیگنال‌ها انجام می‌شود، در برخی از مقالات منتشرشده در این زمینه، در مرحلهٔ دوم از اجرای روش، توابع خودهمبستگی گردشی یا طیفی سیگنال‌ها (مرجع [٦] را مشاهده کنید)، محاسبه و از نتایج حاصل برای تصمیم‌گیری استفاده می‌شود.

همچنین روش‌هایی مبتنی بر شناسایی الگوی رفتار سیگنال در [۷] و شکل تکمیلی آن در [۸] معرفی شده‌اند که

در آن با به‌کارگیری شبکهٔ عصبی مصنوعی، به آشکارساختن تمایز میان سیگنال کاربر اولیه و حمله‌کننده پرداخته می‌شود. علاوه بر روش‌های بیان‌شده، روش‌های مبتنی بر الگوهای رمزنگاری، همانند آنچه در مراجع [۹] و [۱۰] ارائه شده است، روش‌های مبتنی بر مقادیر ویژهٔ بیشینه و کمینهٔ کوواریانس سیگنال دریافتی (مرجع [۱۱] را ملاحظه کنید) و روش‌های بین لایه‌ای (مرجع [۱۲] را ملاحظه کنید) نیز برای آشکارسازی حملهٔ تقلید از کاربر اولیه به‌کار می‌روند.

آگاهی گیرندهٔ ثانویه (گیرنده‌ای که کانال را بررسی می‌کند) از کانال ارتباطی بین خود و فرستندهٔ اولیه، دانش بسیار ارزشمندی برای این تشخیص است؛ اما متأسفانه در شرایط عملی، پذیرش چنین فرضی چندان پذیرفتنی به نظر نمی‌رسد؛ زیرا دریافت اطلاعات کانال نیازمند همکاری شبکه‌های اولیه و ثانویه است و این همکاری در دستهٔ وسیعی از این شبکه‌ها مطرح نیست. با وجود این، استفادهٔ هم‌زمان از ویژگی‌ها و ماهیت سیگنال‌های دریافتی و اطلاعات کانال (با فرض در اختیاربودن آن)، مطمئناً به روشی بسیار قدرتمند در تشخیص حملهٔ فریبنده منجر می‌شود.

هدف از این مقاله استفادهٔ هم‌زمان از دانش مربوط به کانال و نیز ویژگی‌های ایستان گردشی سیگنال‌هاست. در به‌کارگیری این دو، نوآوری‌هایی صورت گرفته است که روش پیشنهادی را از روش‌های کنونی متمایز می‌کند. در استفاده از دانش مربوط به کانال، با توجه به فرض معقول عدم‌همکاری بین شبکه‌های اولیه و ثانویه، از تکنیک ساده‌ای برای مشخص‌کردن تأثیر کانال در سیگنال دریافتی استفاده می‌شود. به کمک یک ساختار تخمین‌زن وفقی (به‌صورت خاص، الگوریتم Normalized Least Mean Square: NLMS) این تأثیر مشخص می‌شود (درواقع تأثیر (امضای) کانال در بردار وزن تخمین‌زده‌شده با الگوریتم، لحاظ می‌شود). در این تکنیک به همکاری بین شبکه‌های اولیه و ثانویه نیاز نیست و تنها فرضی که در نظر گرفته شده است، دراختیارداشتن سیگنال مرجع و درخور اعتمادی از طرف فرستندهٔ اولیه است. فرض بر این است که این سیگنال در برهه‌ای از زمان دریافت شده است که در آن، حمله‌کننده عملکردی در شبکه نداشته است.

در استفاده از ویژگی‌های ایستان گردشی سیگنال‌ها نیز، با روشی وفقی و به کمک همان الگوریتم NLMS، بدون نیاز به محاسبهٔ توابع خودهمبستگی یا طیفی گردشی (که به‌طور متعارف در روش‌های پیشنهادی دیگر مطرح‌شده و لازمهٔ آن، استفاده از میزان زیادی داده و محاسبات است) عمل شده است.

بر این اساس در بخش ۲، ساختار ابتدایی روش پیشنهادی مطرح شده است. در این ساختار، صرفاً اطلاعات غیرمستقیم مربوط به کانال در تشخیص حمله استفاده شده است. سپس در بخش ۳ با چگونگی استفاده از ویژگی‌های ایستان گردشی سیگنال‌ها (ماهیت سیگنال) در ساختار پیشنهادی آشنا می‌شویم. در بخش ٤ نقش افزایش تعداد آنتن‌ها در بهبود عملکرد روش پیشنهادی ارائه شده است. در هر بخش به فراخور، مثال‌های شبیه‌سازی مطرح شده است. نهایتاً در بخش ۵ نتایج و پیشنهادهایی برای ادامهٔ کار ارائه شده است.

۲- ساختار روش پیشنهادی

در این بخش، ساده‌ترین شکل روش پیشنهادی مطرح شده است. در ساختار ابتدایی روش، از ویژگی‌های ایستان گردشی سیگنال دریافتی استفاده نشده است و آشکارسازی تنها با لحاظ‌کردن اطلاعات تزریق‌شدهٔ کانال در سیگنال دریافتی انجام می‌شود.

فرض کنید دنبالهٔ مرجع $\{y_n^r\}_{n=1}^N$ نمونه‌های سیگنال دریافتی از یک فرستندهٔ اولیه در محل گیرندهٔ ثانویه باشد. بالانویس r نشان‌دهندهٔ مرجع‌بودن این دنباله است. فرض بر این است که در زمان دریافت این دنباله، حمله‌کننده هیچ تحرکی در شبکه نداشته است. درواقع، مطمئن هستیم که این دنباله قطعاً از طرف کاربر اولیه بوده و صحت انتساب آن به کاربر اولیه احراز شده است. برای این منظور از یکی از روش‌های زیر برای اطمینان از این موضوع استفاده می‌شود:

دنبالهٔ مدّنظر در حالت کم‌باری شبکه دریافت شود (در این شرایط با توجه به وجود کانال‌های آزاد، جمر انگیزه‌ای برای اشغال کانال و نشان‌دادن خود به عنوان یک کاربر اولیه نخواهد داشت)؛

استفادهٔ هم‌زمان از چند روش متفاوت تشخیص و تأیید اکثریت آنها به انتساب سیگنال به کاربر اولیه؛

همکاری چند کاربر ثانویه با هم در احراز این انتساب و تأیید اکثریت.

در این دنباله از یک ساختار خطی برای تخمین هر نمونه بر حسب نمونهٔ قبلی استفاده شده است. به عبارت دیگر، فرض کنید $\hat{y}_n^r$ یک تخمین خطی از y_n^r بر حسب M نمونهٔ قبلی باشد:

$$\hat{y}_n^r = \sum_{k=1}^{M} w_k^{r^*} y_{n-k}^r, \quad n = M+1,\ldots,N \qquad (۱)$$

در رابطهٔ (۱)، نماد * نشان‌دهندهٔ مزدوج مختلط است. میزان خطای تخمین یعنی

$$v_n^r = y_n^r - \hat{y}_n^r \qquad (۲)$$

بستگی به نوع تخمین‌زن و میزان همبستگی بین y_n^r و نمونه‌های متقدم ($\{y_k^r\}_{k=n-M}^{n-1}$) دارد. در این همبستگی، به‌طور مشخص، عملکرد کانال نقش مستقیمی دارد و تأثیر (امضای) آن در ضرائب تخمین ظاهر می‌شود.

هرگاه هدف بهترین تخمین خطی با معیار میانگین مربع خطا از هر نمونه (در اینجا y_n^r) بر حسب M نمونهٔ قبلی باشد، ضرائب تخمین براساس مبانی تئوریک تخمین [۱۳]، از اصل تعامد و به کمک دستگاه زیر تعیین می‌شوند.

$$E\left[\left(y_n^r - \sum_{k=1}^{M} w_k^{r^*} y_{n-k}^r\right) y_l^{r^*}\right] = 0, \quad l = n-1,\ldots,n-M$$

که در آن E نشان‌دهندهٔ میانگین است. متأسفانه با چنین معیاری، فرض ثابت‌بودن ضرائب و وابسته‌نبودن آنها به n (که لازمهٔ عملکرد روش پیشنهادی است)، تنها در صورت ایستان فرض‌کردن سیگنال دریافتی، پذیرفتنی است. علاوه بر این، برای تعیین ضرائب، لازم است تابع خودهمبستگی دنبالهٔ دریافتی معلوم باشد (این تابع نیز علاوه بر ماهیت سیگنال به کانال وابسته است). این هر دو مشکل را با جایگزینی الگوریتم وفقی NLMS به‌عنوان تخمین‌زن، برطرف می‌کنیم. اگرچه این الگوریتم در ابتدا تقریبی از تخمین با معیار کمینه‌سازی میانگین مربعات خطا و در محیط ایستان مطرح شده است، در کامل‌ترین نمونه از تحقیقات انجام‌شده در [۱٤] در می‌یابیم که الگوریتم NLMS از منظر مقابله با تأثیر انرژی کل خطاها در سیستم (در بدترین حالت)، الگوریتمی بهینه است. در روال بررسی این بهینگی، مفاهیم ایستانی نقشی در اثبات ندارد و تنها ثابت‌بودن ضرائب تخمین، مدّنظر است. به این ترتیب، در شرایط غیرایستانی نیز، مشروط به ثابت‌ماندن کانال، نتیجهٔ عملکرد الگوریتم نوسان زیادی نخواهد داشت. این نوسان اندک با انتخاب گام الگوریتم به اندازهٔ کافی کوچک (μ در رابطهٔ (۵))، تضمین خواهد شد. نتایج شبیه‌سازی نیز تأییدکنندهٔ این موضوع هستند.

از دیگر دلائل استفاده از الگوریتم NLMS، سادگی و توانایی بسیار خوب آن در تطبیق با تغییرات شرایط است.

با تعریف بردار ضرائب به‌صورت

$$W^r = \left[w_1^r, w_2^r \ldots, w_M^r\right]^T$$

و بردار ورودی به‌صورت

$$Y_n^r = \left[y_{n-1}^r, y_{n-2}^r \ldots, y_{n-M}^r\right]^T$$

از روابط (۱) و (۲) خواهیم داشت:

$$y_n^r = W^{r^H} Y_n^r + v_n^r \qquad (۳)$$

در این رابطه، H نشان‌دهندهٔ ترانهادهٔ مزدوج مختلط بردار است. روال عملکرد الگوریتم در تخمین W^r، به‌صورت ارائه‌شده در روابط (٤) و (۵) و برای $n = M+1,\ldots,N$ است (در اجرای الگوریتم، شرایط اولیه را به‌صورت $W_{|M}^r = [0,0\ldots,0]^T$ در نظر می‌گیریم). توجه داشته باشید که بردار Y_n^r و اسکالر y_n^r که لازمهٔ اجرای الگوریتم است، هردو از دنبالهٔ مرجع در اختیار هستند. $W_{|n}^r$، برآورد الگوریتم در گام nام از روال زیر تعیین می‌شود:

$$e_n^r = y_n^r - W_{|n-1}^{r^H} Y_n^r \qquad (٤)$$

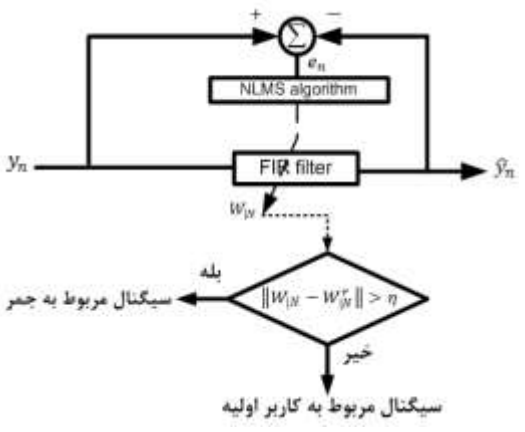
$$W_{|n}^r = W_{|n-1}^r + \frac{\mu}{Y_n^{r^H} Y_n^r} Y_n^r e_n^{r^*} \qquad (۵)$$

فرض کنید که حداکثر در $n = N$ همگرایی الگوریتم رخ می‌دهد. در این صورت مقدار $W_{|N}^r$ برآورد الگوریتم از W^r ذخیره می‌شود. در صورتی که فرض کنیم کانال ارتباطی، عاملی برای همبستگی بین نمونه‌های متوالی y_n^r

باشد، در این صورت، مقدار $W_{|N}^{r}$ علاوه بر ویژگی‌های ماهیتی سیگنال دریافتی، تابعی از فیزیک کانال نیز هست.

پس از تعیین و ذخیره‌سازی $W_{|N}^{r}$، در شرایط عادی، با فرض تغییرنکردن وضعیت کانال و با دریافت دنباله‌ای از سیگنال ($\{y_n\}_{n=1}^{N}$)، مجدداً الگوریتم NLMS را این‌بار با درنظرگرفتن دنبالهٔ دریافتی $\{y_n\}_{n=1}^{N}$ اجرا می‌کنیم. روابط مربوطه مشابه روابط (٤) و (٥) و تنها با حذف بالانویس r خواهند بود (دقت کنید در اینجا n نشان‌دهندهٔ برههٔ زمانی مربوط به دنبالهٔ $\{y_n\}_{n=1}^{N}$ است (منظور اینکه اگرچه برای هردو دنبالهٔ $\{y_n^r\}_{n=1}^{N}$ و $\{y_n\}_{n=1}^{N}$ از زیرنویس مشابه n استفاده شده است، زمان دریافت این دو دنباله یکسان نیست)). به این ترتیب، با توجه به فرض تغییرنکردن کانال، در شرایط متعارف، نتیجهٔ تخمین یعنی $W_{|N}$ باید فاصلهٔ چندانی با $W_{|N}^{r}$ نداشته باشد. پس با مقایسهٔ $\|W_{|N}-W_{|N}^{r}\|$ با یک سطح آستانهٔ مناسب (η)، به حضور کاربر اولیه و یا حمله‌کننده رأی می‌دهیم. شکل (۱) ساختار روش پیشنهادی را نشان می‌دهد.

بررسی این موضوع که الگوریتم NLMS در هر دو اجرا به پاسخی نزدیک به هم می‌رسد ($W_{|N}\approx W_{|N}^{r}$)، از نظر تحلیلی تا حدودی دشوار بوده است و اثبات آن به لحاظ‌کردن فرضیات ساده‌کننده‌ای در مدل و ماهیت سیگنال‌ها و کانال نیاز دارد؛ اما با درنظرگرفتن مفهومی به نام خطای میانگین مربعات اضافی و یا Excess Mean Square Error (EMSE)



شکل (۱): ساختار ابتدایی روش پیشنهادی

می‌توان از نتیجهٔ تحقیقات انجام‌شده در مرجع [۱۵] در این زمینه استفاده کرد. EMSE درواقع، میانگین مربع نرم اختلاف پاسخ الگوریتم با بردار ناشی از حل مسئلهٔ تخمین به کمک تحلیل‌های آماری است. اگر این بردار را با W_o و EMSE مربوط به اجرای الگوریتم با دنبالهٔ $\{y_n^r\}_{n=1}^{N}$ را با ζ^r نشان دهیم، آنگاه ([۱۵]):

$$\zeta^r=\lim_{N\to\infty}E\left[\left\|W_{|N}^{r}-W_o\right\|^2\right]=\frac{0.5\mu\phi}{1-0.5\mu\phi}\sigma^2 \qquad (٦)$$

که در آن، ϕ تابعی مثبت از مشخصات آماری سیگنال‌های درگیر در مسئله، μ گام الگوریتم و σ^2 توان نویز اندازه‌گیری (در بحث مربوط به این مقاله: توان خطای تخمین – مطرح شده در رابطهٔ (۲)) است.

به همین ترتیب اگر EMSE مربوط به اجرای الگوریتم با دنبالهٔ $\{y_n\}_{n=1}^{N}$ را با ζ نشان دهیم، آن‌گاه در صورتی که منشأ این دنباله کاربر اولیه باشد:

$$\zeta=\lim_{N\to\infty}E\left[\left\|W_{|N}-W_o\right\|^2\right]=\frac{0.5\mu\phi}{1-0.5\mu\phi}\sigma^2 \qquad (٧)$$

توجه دارید که به دلیل تغییرنکردن شرایط آماری، مقدار W_o در هر دو رابطهٔ (٦) و (٧) یکسان است.

با توجه به اینکه:

$$E\left[\left\|W_{|N}-W_{|N}^{r}\right\|^2\right]=E\left[\left\|W_{|N}-W_o+W_o-W_{|N}^{r}\right\|^2\right]$$

$$\le E\left[\left\|W_{|N}-W_o\right\|^2\right]+E\left[\left\|W_o-W_{|N}^{r}\right\|^2\right]+2E\left[\left\|W_{|N}-W_o\right\|\left\|W_o-W_{|N}^{r}\right\|\right]$$

و اینکه (نامساوی کوشی – شوارتز)

$$E^2\left[\left\|W_{|N}-W_o\right\|\left\|W_o-W_{|N}^{r}\right\|\right]\le E\left[\left\|W_{|N}-W_o\right\|^2\right]E\left[\left\|W_o-W_{|N}^{r}\right\|^2\right]$$

خواهیم داشت:

$$E\left[\left\|W_{|N}-W_{|N}^{r}\right\|^2\right]\le E\left[\left\|W_{|N}-W_o\right\|^2\right]+E\left[\left\|W_o-W_{|N}^{r}\right\|^2\right]$$

$$+2\left(E\left[\left\|W_{|N}-W_o\right\|^2\right]E\left[\left\|W_o-W_{|N}^{r}\right\|^2\right]\right)^{0.5}$$

با استفاده از نامساوی‌های (٦) و (٧) در نامساوی اخیر نتیجه می‌گیریم:

$$\lim_{N\to\infty}E\left[\left\|W_{|N}-W_{|N}^{r}\right\|^2\right]\le\frac{2\mu\phi}{1-0.5\mu\phi}\sigma^2 \qquad (٨)$$

رابطهٔ (۸) نشان‌دهندهٔ این موضوع است که با انتخاب گام الگوریتم (μ) به اندازهٔ کافی کوچک و با فرض وجود

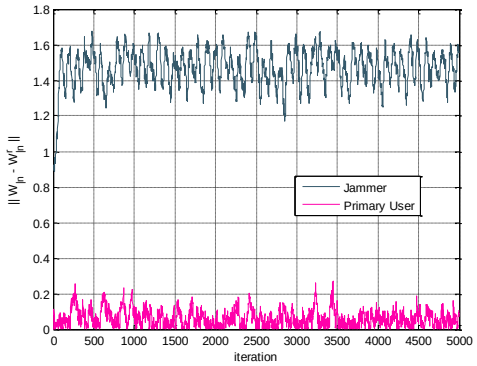
همبستگی بین نمونه‌های دریافتی (کوچک‌بودن توان خطای تخمین (σ^2)، نشأت‌گرفته از وضعیت فیزیکی کانال و ماهیت سیگنال ارسالی) و دراختیارداشتن داده‌های کافی (بزرگ‌بودن N) پاسخ الگوریتم و نتیجهٔ تخمین آن بر اساس دنبالهٔ عادی دریافتی از کاربر اولیه ($W_{|N}$)، نزدیک به نتیجهٔ اجرای آن بر اساس دنبالهٔ مرجع ($W^r_{|N}$) خواهد بود.

نکتهٔ آخری که در این قسمت به آن اشاره می‌کنیم، پیچیدگی الگوریتم است. پیچیدگی محاسباتی این الگوریتم (تعداد عملیات ضرب در هر گام اجرا) از مرتبهٔ M است؛ بنابراین پیچیدگی اجرای کامل روش پیشنهادی از مرتبهٔ NM خواهد بود. اگرچه تحلیل تئوریک مطرح‌شده در روابط (٦) تا (٨) بر مبنای بزرگ‌بودن N بیان شده است، واقعیت آن است که در همان گام‌های اولیه از اجرای الگوریتم، نتیجهٔ حاصل از آن مشخص شده است؛ بنابراین در عمل روش پیشنهادی پیچیدگی بسیار اندکی خواهد داشت. در بین روش‌های تشخیص حضور سیگنال (و نه حتی تشخیص جمر از کاربر اولیه)، آشکارساز انرژی پیچیدگی به مراتب پایین‌تری از روش پیشنهادی دارد. با وجود این، آشکارساز انرژی تنها حضور سیگنال است و ماهیت آن را آشکار نمی‌کند. علاوه بر آن، میزان داده‌های لازم برای همگرایی آن (N) معمولاً بزرگ است. آشکارساز دیگری که درخور مقایسه با روش پیشنهادی است، آشکارساز مبتنی بر فیلتر منطبق است که در پیاده‌سازی آن به آگاهی از ماهیت و جزئیات فیزیکی سیگنال‌ها نیاز است. در بین روش‌های دیگری که با تمرکز به تفکیک جمر از سیگنال کاربر اولیه مطرح شده‌اند (از جمله روش‌های مطرح در مراجع [٦] تا [٨] این مقاله)، عملکرد روش، مبتنی بر ویژگی‌های فرکانسی سیگنال‌هاست؛ بنابراین، عملیاتی نظیر انجام FFT و یا محاسباتی به‌منظور تعیین توابع چگالی طیفی در آنها مطرح می‌شود که اجرای آن‌ها نخست به استفاده از داده‌های بسیار نیاز دارد و دوم، پیچیدگی محاسباتی را بالا می‌برد. بنابراین از منظر پیچیدگی، روش پیشنهادی در جایگاه مناسب‌تری نسبت به دیگر روش‌های مطرح قرار می‌گیرد. اگرچه نقطهٔ اتکای روش به دراختیارداشتن دنبالهٔ مرجع برای تخمین W^r، یعنی امضای کانال (و البته امضای ویژگی‌های سیگنال) نیاز دارد، عامل منفی در مقایسه با دیگر روش‌ها تلقی می‌شود؛ اما در عمل شناخت شبکه و مکانیسم‌های ساده‌ای ازقبیل اطلاعات بین لایه‌ای و داده‌های هم‌زمانی برای دریافت و استفاده از این دنباله وجود دارد.

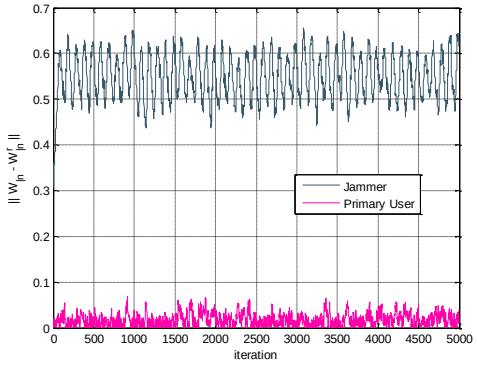
در اینجا مناسب است با ارائهٔ یک مثال کاربردی حاصل عملکرد روش پیشنهادی را مشاهده کنیم. فرض کنید هم فرستندهٔ کاربر اولیه و هم جمر از مدولاسیون BPSK استفاده می‌کنند. برای کانال بین کاربر اولیه و کاربر ثانویه و نیز کانال بین حمله‌کننده و کاربر ثانویه، دو حالت در نظر می‌گیریم. در حالت اول، هر دو کانال به‌صورت تخت و فاقد ISI (و البته با بهرهٔ متفاوت) و در حالت دوم، هر دو دارای ISI و مدل شده با ۷ خط تأخیر انشعاب‌دار (و متمایز از همدیگر) هستند. ضرائب کانال مربوط به هر دو فرستنده به‌صورت تصادفی و به گونه‌ای انتخاب شده است که میزان سیگنال به نویز (نسبت به هر سمبل) ۱۰ دسی‌بل در هر دو حالت حاصل شود. برای الگوریتم نیز مقدار M برابر ۵ لحاظ شده و گام الگوریتم برابر۸/۱۰۰ درنظر گرفته شده است. در شکل ۲- الف نتایج حاصل از اجرای روش پیشنهادی را برای حالت اول مشاهده می‌کنید. همانطور که در شکل ۲- الف نشان داده شده است، در همان گام‌های ابتدایی اجرای الگوریتم، نرم خطا در حالتی که فرستندهٔ سیگنال در حالت عادی، کاربر اولیه بوده است، در حدود ۲/۱۰ و در صورتی که فرستنده، حمله‌کننده باشد، برابر ۲، است. در این مثال و در تمام مثال‌های بعدی فرض بر این است که اجرای الگوریتم برای دنبالهٔ مرجع قبلاً انجام شده و تخمین وزن مربوطه به دست آمده و ذخیره شده است.

نتایج حاصل از اجرای الگوریتم برای حالت دوم نیز در شکل ۲- ب رسم شده است. در این حالت نیز، عملکرد الگوریتم نسبتاً رضایت‌بخش است. خصوصاً توجه کنید که انتخاب طول ۵ برای داده‌های استفاده‌شده در تخمین هر مشاهدهٔ الگوریتم، از تعداد تأخیرهای تأثیرگذار در تداخل (۷ خط تأخیر) کمتر است. با وجود این، عملکرد درستی از الگوریتم مشاهده می‌شود. این عملکرد منطبق با واقعیت مقاوم‌بودن الگوریتم در شرایط غیرایستانی است.

نکتهٔ دیگری که به آن اشاره می‌شود، همگرایی سریع الگوریتم



الف)



ب)

شکل (۲): نرم خطای اوزان الف) کانال تخت ب) کانال دارای ISI

است. درواقع، اگرچه اجرای الگوریتم تا $N=5000$ پیش رفته، در همان گام‌های نخست پاسخ الگوریتم به پاسخ اجرای مرجع نزدیک شده است.

در مطالب مطرح‌شده تا کنون درمورد ویژگی آنتن یا آنتن‌های گیرندهٔ ثانویه، مطلبی بیان نکرده‌ایم. درواقع، تلویحاً پذیرفته‌ایم که گیرندهٔ ثانویه تنها یک آنتن همه‌جهته دارد. در چنین شرایطی عملکرد الگوریتم در صورتی که حمله‌کننده و فرستندهٔ اولیه در محیط دایره‌ای به مرکز گیرندهٔ ثانویه بوده و کانال ارتباطی آنها تخت باشد، نتیجهٔ یکسانی در تخمین را موجب خواهد شد.

در این حالت، با فرض سفیدبودن و ناهمبستگی نمونه‌های دنبالهٔ پیام، دنبالهٔ دریافتی نیز صرف‌نظر از اینکه از طرف کاربر اولیه و یا حمله‌کننده ارسال شده باشد، دنباله‌ای با نمونه‌های ناهمبسته بوده است و حاصل تخمین الگوریتم به بردار صفر همگرا می‌شود. به عبارت دیگر،

$$W_{|N}^{r} \approx W_{|N} \approx 0$$

و برابری فوق، مستقل از ماهیت فرستنده خواهد بود؛ بنابراین امکان متمایزسازی فرستندهٔ اولیه از حمله‌کننده از بین می‌رود. حتی در صورت وجود همبستگی در دنبالهٔ اطلاعات که به وجود همبستگی در دنبالهٔ دریافتی منجر می‌شود، اگر حمله‌کننده سیگنالی منطبق با مشخصات سیگنال کاربر اولیه ارسال کرده باشد (از لحاظ میزان توان، نوع مدولاسیون، الگوی همبستگی و ...) و با فرض نسبت سیگنال به نویز یکسان در محل گیرندهٔ ثانویه، بردار تخمین الگوریتم به $W_{|N}^{r}$ همگرا شده است؛ بنابراین، گیرندهٔ ثانویه کانال را به خطا اشغال شدهٔ کاربر اولیه تلقی می‌کند.

از لحاظ احتمالی، شرایط دیگری که حمله کننده، سیگنالی به سمت گیرندهٔ ثانویه ارسال کند، به‌گونه‌ای که با استفاده از دنبالهٔ دریافتی در محل گیرنده، پروسهٔ تخمین، به نتایج یکسان و نزدیک به $W_{|N}^{r}$ منجر شود، پایین خواهد بود. برای افزایش اطمینان از وقوع‌نیافتن چنین حالتی، ساختار روش پیشنهادی را با درنظرگرفتن ویژگی‌های ماهیتی سیگنال بهبود می‌بخشیم. ویژگی‌های مدّنظر که شکل گرفته از ماهیت فیزیکی سیگنال ارسالی هستند، تأثیر مستقیمی در نتیجهٔ عملکرد الگوریتم دارند. عملکرد مناسب روش بهبودیافته در صورتی است که حمله‌کننده و کاربر اولیه دست‌کم در یکی از دو مورد کانال انتقالی و یا نوع و پارامترهای مدولاسیون با همدیگر اختلاف داشته باشند.

۳- بهبود راه‌کار پیشنهادی با استفاده از ویژگی ایستان گردشی سیگنال‌ها

فرآیند آماری y_n با میانگین صفر، فرآیند ایستان گردشی نامیده می‌شود. اگر تابع خودهمبستگی آن به‌صورت زیر باشد

$$R_x[n,n+l]=E[y_n y_{n+l}^{*}]$$
$$=\sum_{l=0}^{L} R_y^{\alpha_l}[l]\exp(j2\pi\alpha_l n)$$

که در آن $R_y^{\alpha_l}[l]$ و تبدیل فوریهٔ آن $S_y^{\alpha_l}(f)$، به ترتیب تابع خودهمبستگی گردشی و چگالی طیف توان گردشی با فرکانس گردشی α_l نامیده می‌شوند. $\alpha_0=0$ یک فرکانس گردشی برای تمام فرآیندهای ایستان گردشی است. هر

فرکانس گردشی نشان‌دهندهٔ فاصلهٔ فرکانسی بین یک سیگنال ایستان گردشی و سیگنال انتقال‌یافتهٔ فرکانسی همبسته با آن است. به عبارت دیگر، وجود فرکانس گردشی α_l، نشان‌دهندهٔ همبستگی بین سیگنال y_n و سیگنال $y_n \exp(j2\pi\alpha_l n)$ می‌باشد.

تقریباً تمامی سیگنال‌های مدوله‌شده، ویژگی‌های ایستان گردشی دارند و با این مدل تطبیق مناسبی دارند. فرکانس‌های گردشی این سیگنال‌ها، ترکیب‌های خطی متنوعی از نرخ بیت و فرکانس حامل (پارامترهای مدولاسیون) هستند [١٦]. به‌طور مثال، فرکانس‌های گردشی یک سیگنال BPSK با فرکانس حامل f_c و زمان بیت T_b به‌صورت $\frac{k}{T_b}$، $2f_c+\frac{k}{T_b}$ و $-2f_c+\frac{k}{T_b}$ هستند. در این سه عبارت، k برابر صفر و یا یک عدد صحیح مثبت یا منفی دلخواه است.

به این ترتیب، شیوهٔ منطقی در بررسی حضورداشتن یا نداشتن یک سیگنال، بررسی وجودداشتن یا نداشتن ویژگی‌های ایستان گردشی مدّنظر در سیگنال‌هاست. تقریباً در تمام روش‌هایی که تا چند سال گذشته بر این مبنا عمل می‌کرده‌اند، از دنبالهٔ سیگنال دریافتی و انتقال یافته‌های فرکانسی آن برای محاسبهٔ توابع خودهمبستگی گردشی یا چگالی طیف توان گردشی استفاده شده است. این نکته کمی تعجب‌برانگیز است که در بیشتر تحقیقات انجام‌شده، از ویژگی بنیادی این فرآیندها، یعنی همبستگی فرکانسی به‌صورت مستقیم استفاده نشده و تنها به نتیجهٔ آن در تخمین توابعی دیگر (مثلاً توابع خودهمبستگی گردشی) توجه شده است. روش مطرح‌شده در مرجع [١٧] در تشخیص طیف، نمونه‌ای از استفادهٔ مستقیم از مفهوم همبستگی فرکانسی است. با درنظرداشتن این ویژگی، در این مقاله نیز از این خاصیت به‌صورت مستقیم استفاده می‌کنیم. به این معنا که اثرات ایستان گردشی‌بودن، مستقیماً در یک ساختار تخمین‌زن وفقی استفاده می‌شود. شکل (٣) ساختار پیشنهادی را نشان می‌دهد. همانند آنچه در بخش ٢ بیان شد، در اینجا نیز فرض کنید دنبالهٔ مرجع $\{y_n^r\}_{n=1}^N$، نمونه‌های سیگنال دریافتی از یک فرستندهٔ اولیه در محل گیرندهٔ ثانویه باشد. در زمان دریافت این دنباله، حمله‌کننده هیچ فعالیتی در شبکه نداشته و صحت انتساب دنبالهٔ به کاربر اولیه احراز شده است. علاوه بر آن، فرض کنید دنبالهٔ دریافتی، نمونه‌های یک فرآیند ایستان گردشی با فرکانس‌های گردشی معلوم $\{a_l\}_{l=0}^L$ باشند، بر این اساس و در ادامهٔ روشی که در بخش ٢ بیان شد، در اینجا هر نمونه را بر اساس انتقال یافته‌های فرکانسی نمونه‌های قبلی تخمین می‌زنیم. به عبارت دیگر،

$$\hat{y}_n^r = \sum_{l=0}^{L}\sum_{k=1}^{M} w_{l,k}^{r^*} y_{n-k}^r e^{j2\pi\alpha_l(n-k)}, \quad n = M+1,\ldots,N \tag{٩}$$

در عمل می‌توان تعداد فرکانس‌های گردشی انتخابی را کمتر از تعداد کل آنها ($L+1$)در نظر گرفت. برای استفاده از الگوریتم NLMS، برای $l = 0,1,\ldots,L$ بردارهای زیر را تعریف می‌کنیم:

$$W_l^r = \left[w_{l,1}^r,\ldots w_{l,M}^r\right]^T \tag{١٠}$$

$$Y_{l,n}^r = \left[y_{n-1}^r e^{j2\pi\alpha_l(n-1)},\ldots,y_{n-M}^r e^{j2\pi\alpha_l(n-M)}\right]^T \tag{١١}$$

با این تعریف رابطهٔ (٩) به‌صورت زیر بیان می‌شود

$$\hat{y}_n^r = \sum_{l=1}^{L} Y_{l,n}^{r^H} W_l^r, \quad n = M+1,\ldots,N \tag{١٢}$$

$L+1$ الگوریتم NLMS برای تخمین اوزان $W_l^r = \left[w_{l,1}^r,\ldots w_{l,M}^r\right]^T$ به‌صورت زیر عمل می‌کنند:

$$e_n^r = y_n^r - \sum_{l=1}^{L} W_{l|n-1}^{r^H} Y_{l,n}^r \tag{١٣}$$

$$W_{l|n}^r = W_{l|n-1}^r + \frac{\mu}{Y_{l,n}^{r^H} Y_{l,n}^r} Y_{l,n}^r e_n^{r^*} \tag{١٤}$$

توجه کنید که e_n^r برای همهٔ الگوریتم‌ها یکسان است.

حال اگر تعریف کنیم:

$$\overline{W}^r = [W_1^{r^T},\ldots,W_L^{r^T}]^T$$

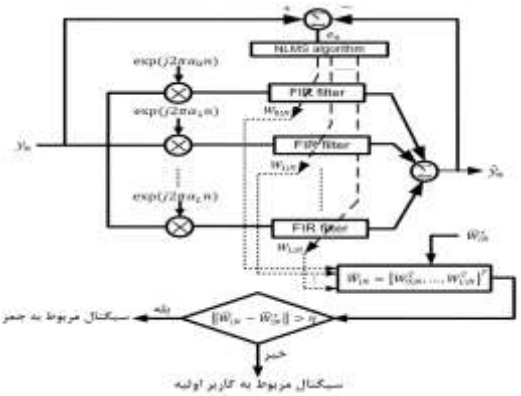
و

$$\overline{W}_{|n}^r = [W_{1|n}^{r^T},\ldots,W_{L|n}^{r^T}]^T$$

در این صورت، هدف از اجرای $L+1$ الگوریتم مطرح‌شده، برآورد $\overline{W}^r$ با تعیین گام‌به‌گام $\overline{W}_{|n}^r$ است. اگر فرض کنیم به اندازهٔ کافی داده در اختیار بوده (N به اندازه‌ی کافی بزرگ

بوده) و الگوریتم‌ها همگی همگرا شده‌اند، در این صورت $\overline{W}_{|N}^{r}$ برآورد مناسبی از $\overline{W}^{r}$ خواهد بود. این برآورد شاهدی در شرایط عادی است.

پس از تعیین و ذخیره‌سازی $\overline{W}_{|N}^{r}$، در شرایط عادی، با فرض تغییرنکردن وضعیت کانال و با دریافت دنباله‌ای از سیگنال $\{y_n\}_{n=1}^{N}$، مجدداً $L+1$ الگوریتم NLMS را این‌بار با درنظرگرفتن دنبالهٔ دریافتی $\{y_n\}_{n=1}^{N}$ اجرا می‌کنیم. روابط مربوطه مشابه روابط (۱۳) و (۱۴) و تنها با حذف بالانویس r خواهند بود (همانند قبل دقت کنید در اینجا n نشان‌دهندهٔ برههٔ زمانی مربوط به دنبالهٔ $\{y_n\}_{n=1}^{N}$ بوده است و اگرچه برای هردو دنبالهٔ $\{y_n^r\}_{n=1}^{N}$ و $\{y_n\}_{n=1}^{N}$ از زیرنویس یکسان n استفاده شده است، زمان این دو دنباله یکسان نیست). به این ترتیب با توجه به فرض تغییرنکردن کانال، در شرایط متعارف واضح است که نتیجهٔ تخمین یعنی $\overline{W}_{|N}$ باید فاصلهٔ چندانی با $\overline{W}_{|N}^{r}$ نداشته باشد. پس با مقایسهٔ $\left\|\overline{W}_{|N}-\overline{W}_{|N}^{r}\right\|$ با یک سطح آستانهٔ مناسب، به حضور کاربر اولیه و یا حمله‌کننده رأی می‌دهیم. شکل (۳) ساختار روش پیشنهادی تکمیل‌شده را نشان می‌دهد. با مقایسهٔ دو شکل (۱) و (۳) و نیز با توجه به آنکه $a_0=0$ است، مشخص می‌شود که ساختار ابتدایی حالت خاصی از ساختار تکمیلی با $L=0$ است. به این ترتیب از لحاظ پیچیدگی، روش تکمیل‌شده پیچیدگی $L+1$ برابر نسبت به ساختار ابتدایی را خواهد داشت؛ اما در عین حال به دلیل استفادهٔ مطلوب از همبستگی فرکانسی، کیفیت تخمین، بهبود چشمگیری پیدا می‌کند. از لحاظ



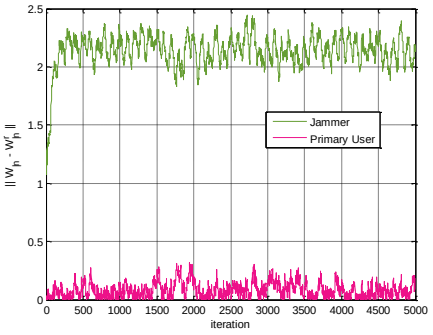
شکل (۳): ساختار تکمیلی روش پیشنهادی

تئوریک، استفاده از این همبستگی موجب کاهش خطای تخمین (σ^2) در نامساوی (۸) خواهد شد. درواقع، اگرچه در بدترین حالت نامساوی (۸) برای روش تکمیلی با توجه به افزایش ابعاد بردار اوزان و اجرای هم‌زمان $L+1$ الگوریتم به‌صورت

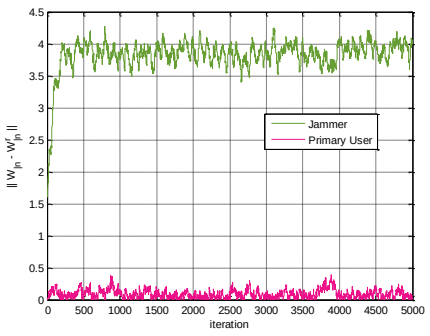
$$\lim_{N\to\infty} E\left[\left\|\overline{W}_{|N}-\overline{W}_{|N}^{r}\right\|^2\right] \le \frac{2(L+1)\mu\phi}{1-0.5\mu\phi}\sigma^2$$

بیان خواهد شد، توان خطای تخمین (σ^2) با توجه به نوع مدولاسیون و تعداد فرکانس‌های گردشی استفاده‌شده، نسبت به قبل کاهش شدیدی خواهد داشت.

برای بررسی کارایی ساختار تکمیلی، مثال قبلی و مربوط به حالت تداخل به طول ۷ را این‌بار با درنظرگرفتن ساختار تکمیلی و لحاظ‌کردن فرکانس‌های گردشی، درخور توجه قرار می‌دهیم. شکل ۴-الف نتایج را با درنظرگرفتن دو فرکانس گردشی $\alpha=\pm 2f_c$ نشان می‌دهد $(f_c=0005)$. با مقایسهٔ نمودار این شکل با نمودار شکل ۲-ب افزایش قدرت تمایز روش در این حالت مشخص می‌شود.



الف)



ب)

شکل (۴): نرم خطای اوزان الف) به ازای دو فرکانس گردشی ب) به ازای پنج فرکانس گردشی

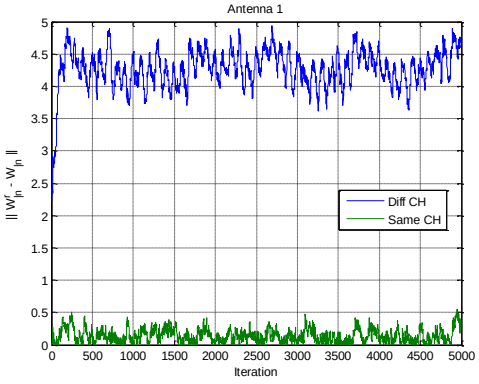
شکل ٤- ب نتیجهٔ حاصل استفاده از پنج فرکانس گردشی $\pm 2f_c$ و $\pm 2f_c + \frac{1}{T_b}$ و $\frac{2}{T_b}$ در ساختار را نشان می‌دهد ($T_b = 2000$). ملاحظه می‌کنید که افزایش تعداد فرکانس‌های گردشی استفاده‌شده، قدرت تمایز الگوریتم را بهبود بخشیده است.

٤- آشکارسازی حملهٔ جمینگ با استفاده از چندین آنتن آشکارساز

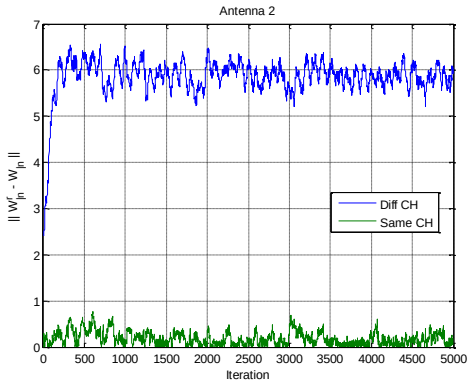
تجهیز گیرندهٔ ثانویه به بیش از یک آنتن و خصوصاً آنتن‌های جهت‌دار (و یا همکاری چند گیرندهٔ ثانویه تک آنتنهٔ آشکارسازهای قرارگرفته در موقعیت‌های فیزیکی متفاوت)، این امکان را به وجود می‌آورد که در شرایط خیلی خاص که حمله‌کننده همزمان ویژگی‌های فیزیکی سیگنال و کانال بین کاربر اولیه و کاربر ثانویه را تقلید کرده است، همچنان حضور آن را تشخیص دهیم. در این حالت، امکان تقلید تمام کانال‌های ارتباطی فرستندهٔ اولیه با آنتن‌های گیرندهٔ (گیرنده‌های) ثانویه، برای جمر ممکن نخواهد بود. مراحل آشکارسازی برای چندین آنتن آشکارساز همانند مراحل آشکارسازی با تنها یک آشکارساز است. پس از اعلام نتیجهٔ آشکارساز انرژی در هر آنتن و به‌طور مثال تأیید حضور سیگنالی با توان چشمگیر، بر روی سیگنال دریافتی از هر یک از آنتن‌هایی که با توجه به مختصات آن تا فرستنده، آشکارساز انرژی آن‌ها چنین سیگنالی را با این توان مطلوب دریافت کرده است، به طور جداگانه و مستقل از آنتن‌های دیگر، الگوریتم NLMS، اجرا و نتیجه با وزن تخمینی حاصل از دریافت دنبالهٔ مرجع از آن آنتن مقایسه می‌شود.

برای بررسی عملکرد در این حالت، مجدداً مثال مطرح‌شدهٔ قبلی و در حالت تداخل را در نظر می‌گیریم. با وجود این، اکنون حمله‌کننده، تقریباً امکان تقلید کانال بین فرستندهٔ اولیه و گیرندهٔ ثانویه را داشته است. فرض می‌کنیم کاربر ثانویه دو آنتن جهت‌دار دارد. برای آنتن اول زاویهٔ دریافت سیگنال از کاربر اولیه برابر ۳۰ درجه و زاویهٔ دریافت از جمر برابر ۵۰ درجه بوده است. این زوایا برای آنتن دوم به ترتیب برابر ٤٥ و ۸۰ درجه بوده است. همانند قبل ۵ فرکانس گردشی در ساختار استفاده شده است. نتایج در نمودارهای شکل (۵) ارائه شده است. همان‌طور که مشاهده می‌کنید، قدرت تفکیک در آنتن ۲ به مراتب نسبت به آنتن ۱ بیشتر است. این ویژگی به دلیل اختلاف زاویهٔ بیشتر بین فرستندهٔ اولیه و جمر از منظر این آنتن نسبت به آنتن ۱ است.

اکنون و پس از آشنایی با ساختار روش پیشنهادی و عملکرد آن در شرایط گوناگون، در ادامه این روش را با روش‌های آشکارسازی حملهٔ تقلید از کاربر اولیه در [٦] و [۸] مقایسه می‌کنیم. این مراجع، برای آشکارسازی حملهٔ تقلید از کاربر اولیه (شکل خاصی از حملهٔ جمینگ فریبنده) در رادیوشناختگر، از ویژگی‌های سیگنال‌ها بهره گرفته‌اند. خواص ایستان گردشی سیگنال‌ها در مرجع [٦] و الگوی رفتار سیگنال‌ها در مرجع [۸] استفاده شده‌اند.



الف)

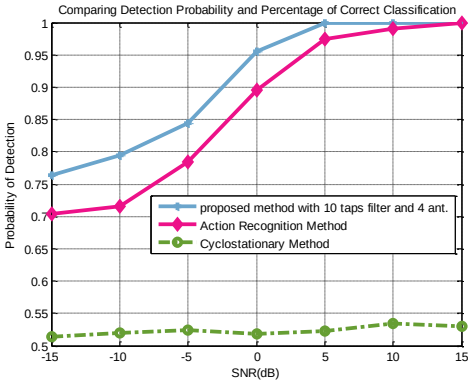


ب)

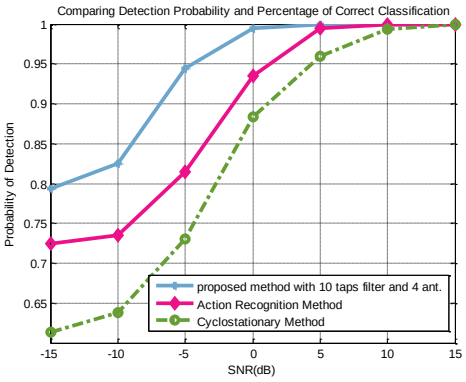
شکل(۵): اثر نزدیک‌شدن زوایای دریافت از دو فرستنده الف) به ازای زوایای ۳۰ و ۵۰ ب) به ازای زوایای ٤٥ و ۸۵

روش ایستان گردشی استفاده‌شده در مرجع [۶]، همانند بیشتر روش‌های دیگر مبتنی بر خواص ایستان گردشی سیگنال‌ها، بر محاسبهٔ توابع چگالی طیفی گردشی سیگنال دریافتی متمرکز است (توابعی که مطابق روش پیشهادی در این مقاله، لزومی به تعیین آنها نیست). شکل این توابع وابسته به نوع مدولاسیون سیگنال دریافتی است. به این ترتیب با محاسبهٔ این توابع، نوع مدولاسیون سیگنال ارسالی معلوم می‌شود؛ بنابراین تفاوت یا تشابه مدولاسیون‌ها در این تابع، مشخص و از این طریق به حضورداشتن یا نداشتن حمله‌کننده پی برده می‌شود. در روش دوم (مرجع [۸]) به ویژگی‌های فیزیکی و الگوی یک سیگنال توجه شده است و معیار تشخیص حمله، تفاوت میان این ویژگی‌ها در حوزهٔ فرکانس است؛ بنابراین اخذ FFT بخشی از محاسبات در این روش خواهد بود.

برای مقایسهٔ روش پیشنهادی با این دو روش، شرایطی کاملاً فرضی را در نظر می‌گیریم که جمر فریبنده توانسته است کانال مربوط به کاربر اولیه را تخمین بزند (در محل گیرندهٔ ثانویه، کانال‌ها تقریباً یکسان تلقی می‌شود). در این مقایسه یک بار مدولاسیون سیگنال‌های کاربر اولیه و جمر فریبنده را از نوع ماهیتاً یکسان PSK (BPSK و QPSK) و بار دیگر از نوع متفاوت (BPSK و BFSK) در نظر گرفته‌ایم. کانال دارای تداخل به طول ۷، تعداد نمونه‌های استفاده‌شده در تخمین الگوریتم برابر ۱۰، تعداد فرکانس‌های گردشی استفاده‌شده برابر ۵، گام ۰/۰۸ و تعداد آنتن برابر ۴ هستند. شبیه‌سازی از $SNR = -15dB$ تا $SNR = 15dB$ برای دو کانال مربوط به کاربر اولیه و جمر فریبنده انجام شده و تصمیم‌گیری بر اساس نتایج حاصل از تمام آنتن‌ها و با رأی‌گیری محافظه‌کارانه انجام شده است. همان‌طور که در شکل ۶-الف مشاهده می‌کنید، در حالتی که سیگنال‌های مربوط به کاربر اولیه و حمله‌کننده با مدولاسیون یکسان (PSK) از سوی فرستنده‌ها ارسال می‌شوند، روش ایستان گردشی کارایی مناسبی ندارد؛ زیرا اساس کار آن، تمایز قائل‌شدن بین دو مدولاسیون است که تنها یکی از آن‌ها را پذیرفتنی (مربوط به کاربر اولیه) می‌داند. مزیت روش پیشنهادی ما تمرکز هم‌زمان بر روی کانال و ویژگی‌های سیگنال است که باعث می‌شود حتی در مواجهه با دو سیگنال مشابه نیز کارایی مناسبی حاصل شود. از سوی دیگر، اگرچه روش دوم کارایی مناسبی



الف)



ب)

شکل (۶): مقایسهٔ روش پیشنهادی با روش‌های مبتنی بر ایستان گردشی [۶] و شناسایی الگوی رفتار [۸] الف) کانال‌ها یکسان و مدولاسیون مشابه ب) کانال‌ها یکسان و مدولاسیون متفاوت

خصوصاً در سیگنال به نویزهای بالا دارد، این روش متکی به شناسایی الگوهای سیگنال ارسالیِ کاربر اولیه است. لازمهٔ شناسایی این الگوها در سیگنال دریافتی، استفاده از تعداد زیادی داده و آنالیز آن درحوزهٔ فرکانس است؛ اما همان‌طور که در مثال‌های قبلی مشاهده شد، الگوریتم پیشنهادی با دریافت تعداد اندکی از نمونه‌های سیگنال ورودی، همگرا و به تصمیم‌گیری منجر می‌شود. هرچند در شرایطی که کانال ارتباطی فرستندهٔ اولیه و کاربر ثانویه و مشخصات سیگنال ارسالی، هم‌زمان با جمر تقلید شده است، استفاده از چند آشکارساز (آنتن) و یا مشارکت بین چند گیرندهٔ ثانویه برای تشخیص جمر لازم است. با تغییر ماهیتی مدولاسیون‌های

کاربر اولیه و جمر، عملکرد روش [٦] نیز بهبود پیدا می‌کند (شکل ٦- ب).

در انتها توجه به دو ویژگی مثبت استفاده از چند آنتن در گیرنده (در قبال افزایش پیچیدگی) مطرح می‌شود.

در حالت چند آنتنه، با دریافت نتایج و آشکارسازی جمر از سوی یک دسته از آنتن‌ها و آشکارنکردن آن و اعلام کاربر اولیه به جای جمر از سوی بقیه، مشخص می‌شود که جمر توانسته این گروه را فریب دهد. این موضوع اگرچه نشان‌دهندهٔ عملکرد هوشمندانه‌ی جمر است، با آنالیز سیگنال هر دو دسته، راستای جمر تشخیص داده می‌شود.

ویژگی دوم در استفاده از چند آنتن جهت‌دار، در شرایطی است که در محیط، چندین کاربر اولیه وجود دارد. در صورت وجود تنها یک آنتن همه‌جهته، لازم است با دریافت هر دنبالهٔ ورودی، وزن تخمینی و متناظر با این دنباله، با اوزان مرجع تخمینی و متناظر با هر یک از دنباله‌های مرجع تمام کاربران اولیه، سنجیده شود و وجودداشتن یا نداشتن جمر اعلام شود. در صورت استفاده از چند آنتن جهت‌دار با دسته‌بندی کاربران اولیه و اختصاص هر دسته به یک آنتن، زمان بررسی و رسیدن به تصمیم‌گیری کاهش می‌یابد.

۵- نتیجه‌گیری

در این مقاله، روش ساده‌ای برای آشکارسازی حملهٔ فریبنده در شبکه‌های رادیوشناختگر ارائه شد که در آن با استفاده از الگوریتم NLMS، هر نمونه از دنبالهٔ دریافتی بر حسب نمونه‌های قبلی تخمین زده می‌شد. حاصل مقایسهٔ بردار وزن حاصل با بردار وزنی که به شکل مشابه، ولی با دریافت یک دنبالهٔ دادهٔ مرجع و مطمئن (از لحاظ مربوط بودن به کاربر اولیه) به دست آمده است، به تعیین ماهیت فرستندهٔ داده منجر می‌شد. هزینهٔ سادگی و کارایی روش، نیاز الگوریتم به دنبالهٔ مرجع (ارسالی از طرف کاربر اولیه) است. بررسی تحلیلی و نتایج شبیه‌سازی نشان‌دهندهٔ عملکرد مناسب روش پیشنهادی بود.

مراجع

[1] R. Chen, J. Park, "Ensuring Trustworthy Spectrum Sensing in Cognitive Radio Networks", 1st IEEE Workshop on Networking Technologies for Software Defined Radio Networks (SDR), pp. 110-119, 25-25 2006.

[2] R. Chen, J. Park, and J. H. Reed, "Defense against Primary User Emulation Attacks in Cognitive Radio Networks", IEEE Journal on Selected Areas in Communications, Vol. 26, No. 1, pp.25- 37, 2008.

[3] N. Nguyen, R. Zheng, and Z. Han, "On Identifying Primary User Emulation Attacks in Cognitive Radio Systems Using Nonparametric Bayesian Classification", IEEE Trans. on Signal Process., Vol. 60, No. 3, pp. 1432–1445, 2012.

[4] X. ChunSheng, M. Song, "Detection of PUE Attacks in Cognitive Radio Networks Based on Signal Activity Pattern", IEEE Trans. on Mobile Computing, Vol. 13, No. 5, pp.1022-1034, 2014.

[5] Z. Jin, S. Anand, and K. P. Subbalakshmi, "Robust Spectrum Decision Protocol against Primary User Emulation Attacks in Dynamic Spectrum Access Networks", Global Telecom. Conference (GLOBECOM) IEEE, pp. 1-5, 2010.

[6] D. Pu, Y. Shi, A. V. Ilyashenko, and A. M. Wyglinski, "Detecting Primary User Emulation Attack in Cognitive Radio Networks", Global Telecom. Conference (GLOBECOM) IEEE, pp. 1-5, 2011.

[7] D. Pu, A. M. Wyglinski, "Primary User Emulation Detection Using Frequency Domain Action Recognition", IEEE Pacific Rim Conference on Communications, Computers, and Signal Processing, 23-26, 2011.

[8] D. Pu, A. M. Wyglinski, "Primary-User Emulation Detection Using Database-Assisted Frequency-Domain Action Recognition", IEEE Trans. on Vehicular Technology, Vol. 63, No. 9, pp.4372-4382, 2014.

[9] X. Zhou, Y. Xiao, and Y. Li, "Encryption and Displacement Based Scheme of Defense against Primary User Emulation Attack", 4th IET International Conference on Wireless, Mobile & Multimedia Networks, pp. 44-49, 2011.

[10] M. Thanu, "Detection of Primary User Emulation Attacks in Cognitive Radio Networks", International Conf. on Collaboration Technologies and Systems (CTS), pp. 605-608, 2012.

[11] Y. Zeng, Y. C. Liang, "Maximum-Minimum Eigenvalue Detection for Cognitive Radio", 18th Annual IEEE International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), pp. 01-05, 3-7 2007.

[12] C. Sorrells, P. Potier, L. Qian, and X. Li, "Anomalous Spectrum Usage Attack Detection in Cognitive Radio Wireless Networks", IEEE International Conference on Technologies for Homeland Security, pp. 384-389, 15-17, 2011.

[13] T. Kailath, A. H. Sayed, and B. Hassibi, "Linear Estimation", Prentice-Hall, 2000.
[14] B. Hassibi, "Indefinite Metric Spaces in Estimation, Control and Adaptive Filtering", Ph.D. Dissertation, Stanford University, Aug. 1996.
[15] S. C. Chan, Y. Zhou, "Convergence Behavior of NLMS Algorithm for Gaussian Inputs: Solutions Using Generalized Abelian Integral Functions and Step Size Selection", Springer Journal of Proc. Sys., Vol. 59, No. 3, pp.255–265, 2010.
[16] W. Gardner, "Cyclostationarity in Communications and Signal Processing", IEEE Press 1994.
[17] F. Rahimzadeh, "New Spectrum Sensing Methods in Wireless Cognitive Radio Systems", MSc Thesis, University of Isfahan, Jan. 2014.