شبیه‌سازی و تحلیل امنیت یک لینک ارتباطی بر اساس اختلال دوستانه

محسن شیخی لیسار

چکیده

ازآنجایی‌که تعداد دستگاه‌های متصل و اهمیت ارتباطات سیّار افزایش می‌یابد، باید تأکید بیشتری بر روی امنیت قرار داده شود. این گزارش کاربرد اختلال دوستانه را به‌عنوان یک تکنیک امنیت لایه فیزیکی موردبررسی قرار می‌دهد که در آن از نویز ساختگی به‌منظور تضعیف کانال بین فرستنده و استراق سمع کننده استفاده می‌شود. به‌طوری‌که سیگنال اختلال ساختگی، تداخل غیرقابل‌پیش‌بینی را برای دستگاه‌های غیرمجاز ایجاد نموده، اما توسط دستگاه‌های مجاز مجهز به کلید مخفی قابل بازیابی است. به‌عبارتی‌دیگر، دستگاه مجاز می‌تواند سیگنال تداخل ایجادشده را با استفاده کلید مخفی به اشتراک گذاشته‌شده بازسازی و سپس حذف نماید.

به دلیل پشتیبانی سیستم‌های ارتباطی از چندین نوع مدولاسیون (به‌عنوان‌مثال پخش ویدیوی دیجیتال (DVB) که مجموعه‌ای از استانداردهای بین‌المللی آزاد برای تلویزیون دیجیتال است)، لذا شبیه‌سازی تکنیک موردنظر با مدولاسیون‌های BPSK، QPSK، 16-QAM و 64-QAM برای گیرنده‌ی قانونی و استراق سمع کننده مورد ارزیابی قرار می‌گیرد. نتایج نشان داد که نرخ خطای به‌دست‌آمده با مدولاسیون‌های گوناگون با در نظر گرفتن کانال AWGN در لینک موردنظر به ترتیب ۵۰درصد، ۷۵درصد، ۹۴درصد و ۹۸ درصد برای استراق سمع کننده به دست می‌آید. همچنین تکنیک موردنظر بر روی لینک 802.11a/g موردبررسی قرار گرفت که نرخ خطای سمبل ۵۵ درصد برای استراق سمع کننده نیز به دست آمد.

واژگان کلیدی: اختلال دوستانه، استراق سمع کننده، دستگاه های غیرمجاز، نرخ خطای بیت

۱- مقدمه

ارتباطات بی‌سیم یکی از مهم‌ترین دستاوردهای بشر است زیرا انتقال اطلاعات به گره‌های دوردست را بدون نیاز به سیم فراهم می‌کند. انتقال رادیویی از راه دور توسط مارکونی در سال ۱۹۰۱ انجام شد. از آن زمان، بسیاری از مزایای ارتباطات بی‌سیم زندگی انسان‌ها را تسهیل کرده است. به‌طور جالب‌توجهی ماهیت بدون سیم ارتباطات بی‌سیم، استفاده از آن را در مقایسه با سیستم‌های سیمی که همیشه یک کابل در آن‌ها موردنیاز است درحالی‌که طول کابل می‌تواند نگرانی اصلی باشد، بسیار راحت می‌کند. علاوه بر این، سیستم‌های بی‌سیم قادر به ارائه خدمات برای تعداد زیادی از کاربران هستند. همچنین، سیستم‌های ارتباطی بی‌سیم هزینه‌های نصب و نگهداری ارزان‌تری را در مقایسه با ارتباطات زمینی دارند که در آن نه‌تنها همه مسیرها باید سیمی شوند بلکه تغییر در برنامه کابل گذاری شامل هزینه‌های اضافی نیز می‌شود.

اختلال فرکانس رادیویی موجب تداخل عمدی می‌شود که ارتباطات بی‌سیم را بر روی لایه فیزیکی مختل می‌کند. بنابراین، اختلال به‌عنوان یک تهدید جدی برای شبکه‌های بی‌سیم مطرح می‌شود [1]، [2]، [3]. به‌طورمعمول، اختلال می‌تواند همچنین به نفع ارتباطات بی‌سیم استفاده شود. ازاین‌رو به دو سناریوی کاربرد کلی معمولاً در ادبیات پرداخته می‌شود: (۱) اختلال به‌عنوان تداخل عمدی برای جلوگیری از دستیابی داده‌های نامعتبر به دستگاه‌های قانونی [4]، [5]، و (۲) اختلال به‌عنوان روشی برای جلوگیری از استراق سمع روی ارتباطات کاربر [6]، [7].

با توجه به ماهیت پخش رسانه بی‌سیم، شبکه‌های بی‌سیم بسیار در معرض چالش‌های امنیتی مثل حمله اختلال یا استراق سمع قرار دارند. اگرچه رمزنگاری را می‌توان برای محافظت از اطلاعات محرمانه یک بسته فریم داده استفاده کرد، اما برای جلوگیری نشت اطلاعات کانال جانبی از سرتیترهای رمزگذاری نشده کافی نیست. علاوه بر این، در بسیاری از استانداردهای بی‌سیم، فریم‌های مدیریت و کنترل اغلب به‌صورت آشکار ارسال می‌شود. عملیات مختلف دستورالعمل‌های بی‌سیم، مانند ایجاد کلیدهای نشست، به مبادله این فریم‌ها متکی هستند. همچنین، محدودیت‌های سخت‌افزاری مانند قابلیت محاسباتی پایین و توان محدود کاربران بی‌سیم باعث می‌شود رمزنگاری در برخی شبکه‌های بی‌سیم غیرعملی شود. ازاین‌رو تکنیک اختلال دوستانه پیشنهادی می‌تواند با ایجاد شبه نویز و جمع شدن آن در کانال با داده‌های اصلی، نرخ خطای بیت را برای استراق سمع کننده به‌شدت افزایش دهد. لذا ازآنجایی‌که این شبه نویز ساختگی با گیرنده از طریق کلید به اشتراک گذاشته شده است، می‌توان با حذف آن نرخ خطای بیت را برای گیرنده مجاز کاهش داد.

بنابراین روی سناریوی کاربردی زیر تمرکز می‌کنیم. یک مهاجم به دنبال ارسال پیام‌های مخرب به دستگاه مجاز است. برای حفاظت از این دستگاه‌های مجاز، یک دستگاه خارجی به نام اختلال‌گر دوستانه را معرفی می‌کنیم. اختلال دوستانه وعده یک مکانیسم حفاظت ساده و مؤثر برای دستگاه‌های بی‌سیم را می‌دهد. در این کار، ابتدا تکنیک اختلال دوستانه را روی لینک موردنظر برای مدولاسیون‌های BPSK، QPSK، 16-QAM و 64-QAM مورد ارزیابی قرار می‌دهیم سپس به‌عنوان بخشی از ارزیابی دنیای واقعی، اختلال دوستانه را برای ساده‌ترین پروتکل ارتباطی در نقاط دسترسی وای فای شبیه‌سازی می‌نماییم.

۲- کارهای مرتبط

یکی از حوزه‌های تحقیقاتی که به‌سرعت درحال‌توسعه است، استفاده از وسایل نقلیه هوایی بدون سرنشین به دلیل پتانسیل آن‌ها برای ارائه پوشش بی‌سیم با سرعت‌بالا به شبکه‌های ارتباطی زمینی است. قابل‌ذکر است که اکثر مقالات در مورد اختلال دوستانه بر استفاده از اختلال‌گرهای زمینی متمرکزشده‌اند. ژِو، چِن و همکاران [8] عملکرد محرمانه یک وسیله نقلیه هوایی بدون سرنشین که مجهز به یک اختلال‌گر هوا به زمین و یک شبکه ارتباطی زمینی متشکل از یک جفت فرستنده و گیرنده مجاز و یک استراق سمع کننده است را موردبررسی قرار می‌دهند. نتایج شبیه‌سازی و تحلیلی نشان می‌دهد که یک اختلال‌گر وسیله نقلیه هوایی بدون سرنشین می‌تواند به‌طور قابل‌توجهی پوشش اختلال را در مقایسه با یک اختلال‌گر زمین بهبود بخشد.

لی و همکاران [9] از کدگذاری شبکه لایه فیزیکی و اختلال دوستانه برای بهبود امنیت لایه فیزیکی خود در ارتباطات مشارکتی دو پرشِ بی‌سیم استفاده می‌کنند، که شامل یک جفت منبع-مقصد با کمک چندین گره میانی در حضور یک استراق سمع کننده است. با ارسال سیگنال اختلال حامل پیام باینری تصادفی از اختلال‌گر انتخاب‌شده و استفاده از کدگذاری شبکه فیزیکی در گره رله انتخاب‌شده، این سیستم می‌تواند برای کانال مقصد-رله خوب عمل کند، درنتیجه نرخ محرمانگی بهتری به دست آید. بنابراین از سیگنال اختلال برای تضعیف کانال استراق سمع کننده در مرحله اول بدون تداخل در کانال قانونی استفاده می‌شود، و در مرحله دوم با استفاده از مزایای اختلال و مشخصه‌های کدگذاری شبکه فیزیکی، استراق سمع کننده را از بهره‌برداری از شبکه، می‌توان خارج کرد.

ژوران لی و هونگ نینگ [10] یک طرح ضد استراق سمع جدید را، با معرفی نویز ساختگی ناشی از اختلال‌گرهای دوستانه که در شبکه‌های بی‌سیم بکار گرفته‌شده‌اند، پیشنهاد می‌کنند. به‌طور خاص، یک مدل تحلیلی را برای تعیین خطر استراق سمع شبکه بی‌سیم با اختلال‌گرهای دوستانه پیشنهاد می‌کنند. در این رویکرد هم تلفات مسیر در مقیاس بزرگ و هم محوشدگی رایلی در نظر گرفته‌شده است. همچنین احتمال حمله استراق سمع را با طرح اختلال دوستانه و بدون این طرح مقایسه کرده و نتایج عددی به‌دست‌آمده نشان می‌دهد که خطر استراق سمع شبکه‌های بی‌سیم می‌تواند به‌طور قابل‌توجهی با کمک اختلال‌گرهای دوستانه کاهش یابد.

رادیو شناخت گر به‌طور گسترده به‌عنوان یک رویکرد دسترسی به طیف پویا شناخته می‌شود. یونس ساریکایا و همکاران [11] یک الگوریتم کنترل پویای بهینه طراحی کردند تا به‌طور مشترک تخصیص پهنای باند و توان را تعیین کند. درنتیجه کنترل جریان در یک شبکه رادیو شناخت گر با اختلال دوستانه تعیین‌شده است.

رویکرد اختلال دوستانه به دلیل مزیتی که دارد اخیراً بیشتر موردتوجه قرارگرفته و مقالات متعددی در این رابطه وجود دارد. اختلال مشارکتی رویکردی است که اخیراً به‌منظور بهبود امنیت لایه فیزیکی برای شبکه‌های بی‌سیم در حضور استراق سمع کننده پیشنهادشده است. زمانی که منبع پیام خود را به مقصد ارسال می‌کند، یک گره رله یک سیگنال اختلال را برای ایجاد اختلال در استراق سمع کننده ارسال می‌کند. یانگ و همکاران [12] یک طرح اختلال مشارکتی گره دوگان تصادفی را پیشنهاد دادند، تا از

انتقال ایمن در یک کانال خط دیدمستقیم برای گره‌های توزیع‌شده آماری اطمینان حاصل شود. نتایج عددی نشان می‌دهد که این طرح ازنظر احتمال قطع، بسیار بهتر از طرح مرسوم اختلال مشارکتی است. ازنقطه‌نظر واقعیت، اختلال مشارکتی تصادفی هزینه سیستم کمتری برای همگامی دارد، و تمام کمک‌کننده‌ها تنها نیاز به دانستن بهره کانال خود دارند، هیچ اطلاعات سراسری دیگری نباید به اشتراک گذاشته شود.

۳- تکنیک اختلال دوستانه بر روی لینک موردنظر

در این بخش پس‌ازاینکه یک لینک برای استراق سمع کننده و لینک دیگری برای گیرنده قانونی شبیه‌سازی شد، نویز ساختگی نیز اعمال می‌شود. نتایج نشان می‌دهد که با مدولاسیون BPSK برای هر دو گیرنده قانونی و استراق سمع کننده نرخ خطای ۵۰ درصد به دست می‌آید. ازاین‌رو شبیه‌سازی خود را تعمیم داده تا اختلال ساختگی را بتوان از گیرنده قانونی حذف نمود. بنابراین فیلتر وفقی پیشنهاد شد، زیرا ازآنجایی‌که seed نویز ساختگی با گیرنده به اشتراک گذاشته شده است، می‌توان نویز ساختگی را در گیرنده بازسازی نموده و از سیگنال دریافتی تفریق شود. لذا حائز اهمیت است، قبل از اینکه نویز بازسازی‌شده از سیگنال دریافتی کم شود، تأخیر سیگنال دریافتی تخمین زده شود، زیرا در غیر این صورت همان نرخ خطای بیت ۵۰درصد برای هر دو استراق سمع کننده و گیرنده قانونی به دست خواهد آمد. ازاین‌رو از همگام‌سازی سیگنال دریافتی با نویز ساختگی بازسازی‌شده در گیرنده استفاده می‌شود تا تأخیر سیگنال دریافتی به دست آید. سپس می‌توان نویز ساختگی را دقیقاً از همان‌جایی که به داده‌های اصلی اضافه‌شده است تفریق نمود. در پایان نیز نتایج شبیه‌سازی با مدولاسیون‌های BPSK، QPSK، 16-QAM، 64-QAM و در لینک 802.11a/g مورد ارزیابی قرار می‌گیرد.

۳-۱- پارامترهای شبیه‌سازی

پارامترهای شبیه‌سازی در شکل(۱) نشان داده‌شده است. شبیه‌سازی برای ۱۰۰ ثانیه با نرخ نمونه‌برداری ۰.۰۰۱ ثانیه انجام می‌شود. به‌عبارتی‌دیگر برای ۱۰۰ ثانیه زمان شبیه‌سازی، ۱۰۰۰۰۰ نمونه ارسال می‌شود. بنابراین نرخ خطای بیت برای هردو گیرنده قانونی و استراق سمع کننده بر اساس این ۱۰۰،۰۰۰ نمونه بیان می‌شود. به عبارتی، با افزایش نرخ سیگنال به نویز در هر مرحله، یک‌بار شبیه‌سازی را اجرا نموده و نرخ خطای بیت برحسب نرخ سیگنال به نویز محاسبه می‌شود. در پایان نقاط به‌دست‌آمده برای بازه‌های مطرح‌شده ترسیم می‌شود.

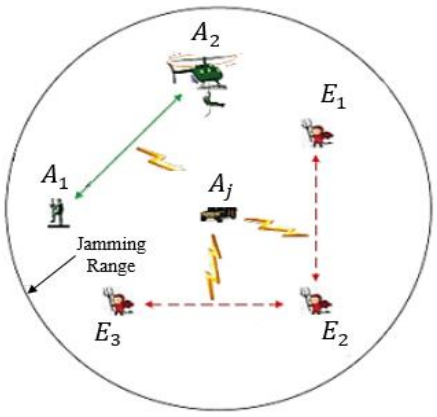
شکل(۱) پارامترهای شبیه‌سازی برای تکنیک موردنظر

۳-۲- فرضیات

- دستگاه‌های مجاز یک کلید مخفی به‌عنوان seed را به اشتراک می‌گذارند.
- زمان در دستگاه‌های مجاز همگام می‌باشد.
- آفست فرکانسی بین اختلال‌گر و دستگاه‌های مجاز در محدوده‌ی مشخصی می‌باشد.
- اختلال‌گر به آنتن همه جهتی مجهز شده است.

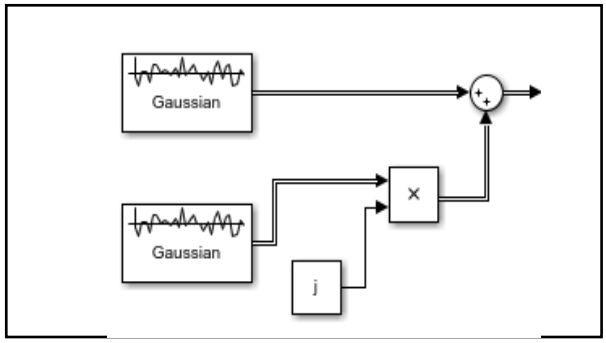
۳-۳- مدل پیشنهادی

شکل(۲) مدل پیشنهادی را نشان می‌دهد که به‌منظور سادگی فقط یک اختلال‌گر در آن وجود دارد. فرض بر این است که دستگاه‌های مجاز و غیرمجاز در یک ناحیه هستند. دستگاه‌های مجاز با A_1 ، A_2 و اختلال‌گر با A_j و دستگاه‌های غیرمجاز با E_1، E_2، E_3 نشان داده‌شده‌اند. دستگاه‌های مجاز و اختلال‌گر کلید مخفی k را به اشتراک می‌گذارند. اختلال‌گر A_j از نویز گوسی سفید و k به‌عنوان seed برای انتشار سیگنال X_j استفاده می‌نماید.



شکل(۲) مدل پیشنهادی

همان‌طور که در شکل(۳) ملاحظه می‌کنید، به دلیل مختلط بودن سمبل‌های لایه فیزیکی از دو نویز گوسی با Seedهای متفاوت، جهت مختلط کردن سیگنال اختلال ساختگی استفاده می‌کنیم.

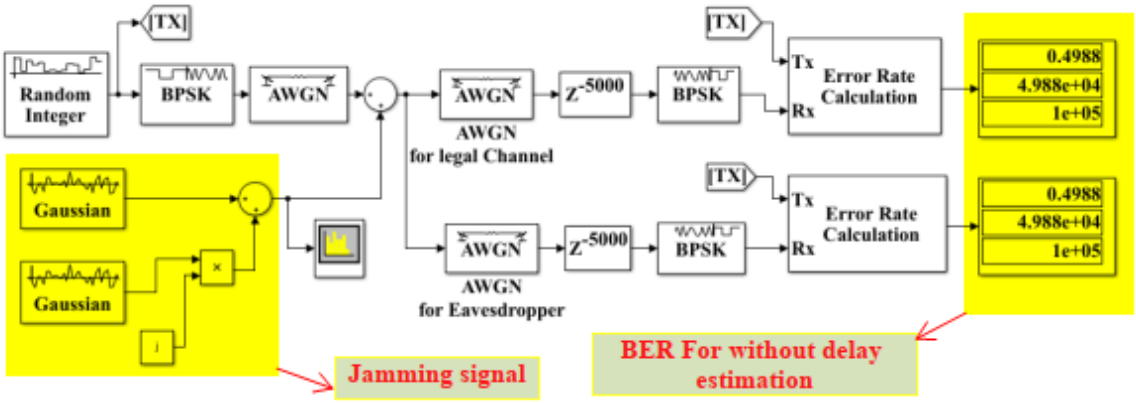


شکل(۳) **سیگنال اختلال تولیدشده**

همچنین، اختلال‌گر موردنظر از یک کلید مخفی منحصربه‌فرد به اشتراک گذاشته‌شده به‌عنوان Seed، به‌منظور تولید سیگنال اختلال دوستانه استفاده می‌نماید. ازاین‌رو، با تغییر Seed سیگنال اختلال موردنظر، در هر بار می‌توان سیگنال اختلال شبه تصادفی جدید ایجاد کرد.

۳-۴- شبیه‌سازی لینک موردنظر بعد از اعمال نویز ساختگی

همان‌طور که در شکل(۴) مشاهده می‌کنید بعد از اضافه کردن نویز ساختگی، نرخ خطای به‌دست‌آمده تقریباً ۵۰درصد برای هر دو گیرنده قانونی و استراق سمع کننده به دست می‌آید. لذا نیاز است که نویز ساخته‌شده در گیرنده قانونی حذف شود. ازاین‌رو در مدل پیشنهادی فیلتر وفقی معرفی‌شده است. بنابراین قبل از استفاده از فیلتر وفقی، تأخیر سیگنال دریافتی باید تخمین زده شود.



شکل(۴) شبیه‌سازی لینک موردنظر بعد از اعمال نویز ساختگی

۳-۵- همگام‌سازی سیگنال اختلال با سیگنال دریافتی و تخمین تأخیر

برای ایجاد هماهنگ‌سازی با اختلال‌گر، دستگاه مجاز می‌تواند از همبستگی برای پیدا کردن مکان نمونه‌های دریافتی $y_{i,k},\dots,y_{i,l}$ در سمبل‌هایی که به‌صورت محلی تولیدشده‌اند استفاده نمایند. همبستگی یک رویکرد محبوب برای شناسایی الگوهای سیگنال شناخته‌شده در سمت گیرنده می‌باشد. فرض کنید طول همبستگی برابر با L باشد. دستگاه مجاز می‌تواند در ابتدا $y_{i,k},\dots,y_{i,k+L-1}$ را با اولین L سیگنال در $r_{d,0},r_{d,1},\dots,r_{d,n-1}$ هم‌تراز نموده، همبستگی را محاسبه نماید، هم‌ترازی را با یک نمونه شیفت داده و همبستگی را مجدداً تا زمانی که یک پیک در خروجی کرولیتور شناسایی شود محاسبه نماید.

به‌عنوان‌مثال فرض کنید همبستگی خروجی برابر با Γ می‌باشد:

$$\begin{aligned}\Gamma &= \sum_{n=0}^{L-1} y_{i,k+n}.r^*_{i',k'+n} \\ &= \sum_{n=0}^{L-1}\left[he^{j\gamma}e^{j2\pi\Delta f_g t_{i,k+n}}.r_{i,k+n}+n_{i,k+n}\right].r^*_{i',k'+n}\end{aligned} \quad (۱)$$

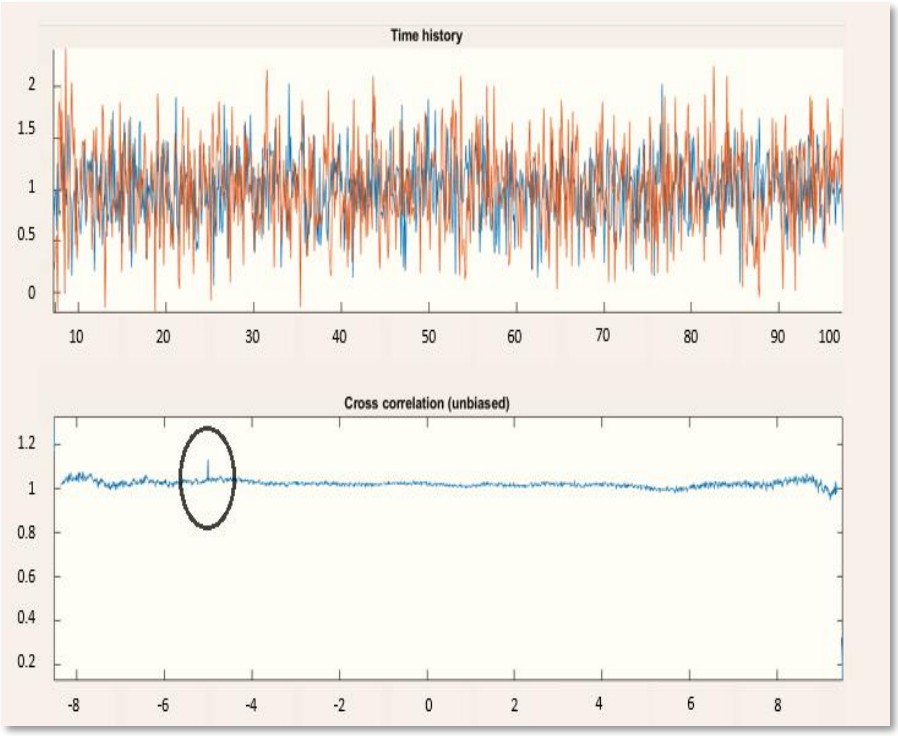
$r_{i',k'+n}$ یک سیگنال می‌باشد که در دنباله‌ی سیگنال اختلال تولیدی که به‌صورت محلی تولیدشده است وجود دارد و $r^*_{i',k'+n}$ مزدوج مختلط آن می‌باشد. همان‌طور که $r^*_{i',k'+n}$ مستقل از نویز می‌باشد، $r_{i',k'+n}$ می‌تواند حذف شود. درصورتی‌که هم‌ترازی صحیح پیدا شود، $i=i'$ و $k=k'$ خواهد شد و خواهیم داشت:

$$\Gamma \approx he^{j\gamma}\sum_{n=0}^{L-1}\left|r_{i,k+n}\right|^2 e^{j2\pi\Delta f_g t_{i,k+n}} \quad (۲)$$

بخش آفست فرکانسی $e^{j2\pi\Delta f_g t_{i,k+n}}$ فازهای پویا را برای اجزای منحصربه‌فرد در جمع فوق معرفی می‌نماید که ممکن است منجر به حذف سیگنال شود. بنابراین دستگاه مجاز باید آفست فرکانسی را قبل از اینکه همبستگی بتواند برای همگام‌سازی مورداستفاده قرار گیرد، جبران نماید. پس از جبران آفست فرکانسی خروجی همبستگی به‌صورت زیر نشان داده می‌شود.

$$\Gamma \approx he^{j\gamma}\sum_{n=0}^{L-1}\left|r_{i,k+n}\right|^2 e^{j2\pi\Delta f_g t_{i,k+n}} \cdot e^{-j2\pi\Delta f_g t_{i,k+n}} \approx he^{j\gamma}\sum_{n=0}^{L-1}\left|r_{i,k+n}\right|^2 \quad (۳)$$

بنابراین همان‌طور که در شکل(۵) مشاهده می‌کنید، به‌عنوان‌مثال اگر سیگنال دریافتی ۵ ثانیه تأخیر داشته باشد خروجی همبستگی، تأخیر را بعد از کرولیت کردن نویز بازسازی‌شده و سیگنال دریافتی نشان خواهد داد.



شکل(۵) همگام‌سازی سیگنال اختلال بازتولیدشده با سیگنال دریافتی

۴- حذف نویز ساختگی در لینک قانونی با استفاده از فیلتر وفقی

وقتی مطالعه درباره‌ی فیلترهای وفقی آغاز می‌شود اهمیت زیادی دارد تا نگاهی دقیق‌تر به مفهوم دو کلمه اصلی فیلتر و وفقی شود. صفت وفقی درباره‌ی سیستم‌هایی بکار می‌رود که تلاش آن‌ها بر وفق دادن رفتار خود نسبت به محیطی است که در آن قرار دارند. به‌بیان‌دیگر سیستم‌هایی وفقی هستند که می‌کوشند تا با تغییر مقدار پارامترهای خود عملکردشان را به نحوی متناسب با محیط اطراف خود تنظیم کنند. در این فرایند سیستمی که پارامترهای آن دچار تغییرات شده است، فیلتر نام دارد. پایه و اساس

فیلترهای وفقی را می‌توان با فیلتر وینر مورد ارزیابی قرارداد که برای تولید یک تخمین از یک فرآیند تصادفی موردنظر مورداستفاده قرار می‌گیرد. فیلتر وینر میانگین خطای مربع بین فرآیند تصادفی تخمین زده‌شده و فرایند موردنظر را به حداقل می‌رساند. این نوع از فیلتر، به دلیل سختی محاسبه ماتریس معکوس خودهمبستگی قابلیت پیاده‌سازی نداشت لذا فیلترهای جدیدی بنام LMS به‌منظور سادگی بیشتر این مسئله پیشنهاد شد.

در فیلتر LMS، وزن‌های بهینه همان‌طور که در رابطه(۴) نشان داده می‌شود با یک وزن اولیه شروع‌شده و وزن‌های بعدی نیز با استفاده از وزن اولیه و گام μ محاسبه می‌شوند. ازاین‌رو به‌صورت لحظه‌ای وزن‌های بهینه بعد از محاسبه خطا در هر مرحله به دست می‌آید.

$$w[n+1] = w[n] + \mu u[n].e^{*}[n] \tag{۴}$$

مسئله دیگر انتخاب گام بهینه است. ازآنجایی‌که مقدار تغییر وزن، به تخمین گرادیان بستگی دارد، لذا هرچقدر گام انتخاب‌شده بزرگ‌تر باشد، آنگاه تخمین گرادیان با خطای بیشتری مواجه می‌شود. همچنین اگر زمان گام کوچک‌تر باشد، زمان همگرایی به وزن‌های بهینه طولانی می‌شود.

حداقل مربعات بازگشتی(RLS) یک الگوریتم فیلتر وفقی است که به‌صورت بازگشتی با در نظر گرفتن خطاهای قبلی، ضرایبی را می‌یابد که تابع هزینه حداقل مربعات خطی وزنی مربوط به سیگنال‌های ورودی را کمینه می‌کند. در مقایسه با اغلب رقبایش، RLS هم‌گرایی بسیار سریعی را نشان می‌دهد. بااین‌حال، این مزیت با هزینه پیچیدگی محاسباتی بالا به دست می‌آید.

ایده فیلتر RLS به حداقل رساندن تابع هزینه C با انتخاب مناسب ضرایب فیلتر W_n، به‌روزرسانی فیلتر به هنگام رسیدن داده‌های جدید است. سیگنال خطا با e(n) و سیگنال موردنظر با d(n) نمایش داده می‌شود.

ازاین‌رو، خطا نیز به تخمین $\hat{d}(n)$ بستگی دارد:

$$e(n) = d(n) - \hat{d}(n) \tag{۵}$$

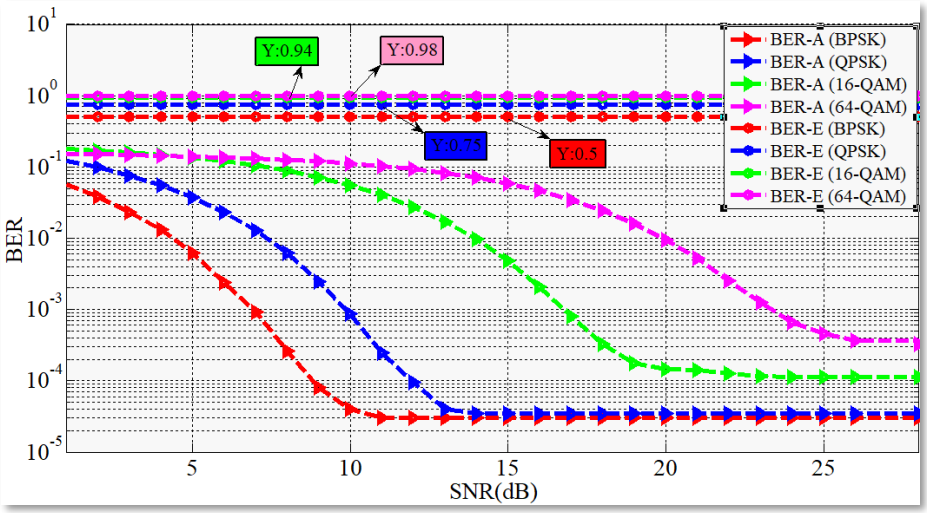
تابع خطای حداقل مربعات وزنی تابع هزینه C که ما می‌خواهیم به حداقل برسانیم تابعی از e(n) است، ازاین‌رو به ضرایب فیلتر نیز بستگی دارد:

$$C(W_n) = \sum_{i=0}^{n} \lambda^{n-i} e^2(i) \tag{۶}$$

که در آن $0 < \lambda \leq 1$ فاکتور فراموشی است که به‌صورت نمایی وزنی کم‌تر به نمونه‌های خطای قدیمی‌تر می‌دهد. بنابراین بعد از اضافه کردن فیلتر وفقی نرخ خطای به‌دست‌آمده برای گیرنده مجاز به‌شدت کاهش می‌یابد.

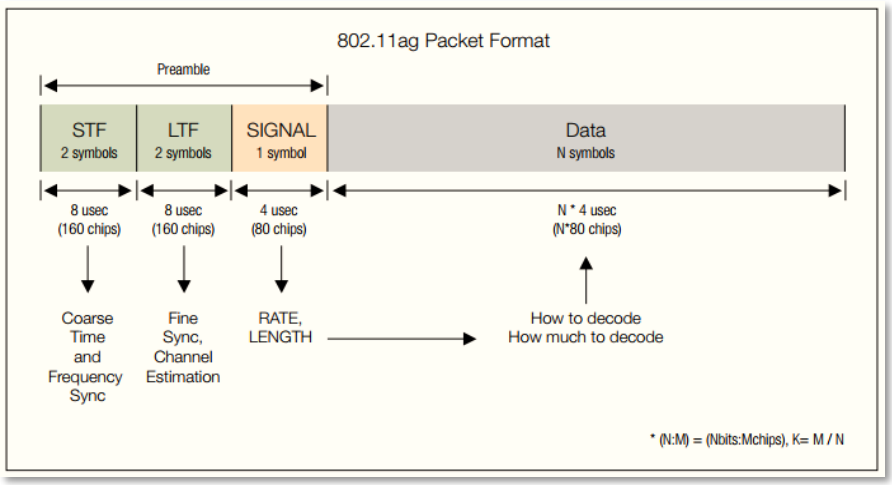
۵- نتایج شبیه‌سازی

همانطورکه در شکل(۶) مشاهده می‌شود نرخ خطای بیت به‌دست‌آمده در استراق سمع کننده با مدولاسیون‌های BPSK، QPSK، 16-QAM و 64-QAM به ترتیب ۰.۵، ۰.۷۵، ۰.۹۴، ۰.۹۸ است. و در گیرنده قانونی نیز به‌طور خاصی این نرخ خطای بیت با افزایش نرخ سیگنال به نویز، کاهش می‌یابد.



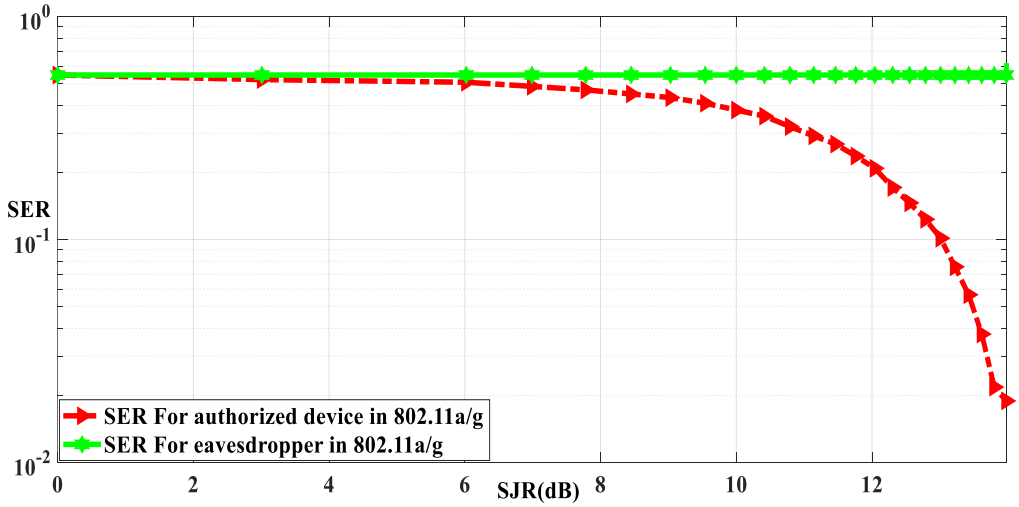
شکل(۶) نرخ خطای بیت برای دستگاه مجاز و استراق سمع کننده

شبیه‌سازی تکنیک اختلال دوستانه را همان‌طور که مشاهده کردید در سناریوهای مختلف مورد ارزیابی قراردادیم. اکنون تکنیک موردنظر را بر روی یکی از استانداردهای وای فای به‌عنوان‌مثال 802.11a/g اعمال می‌کنیم. ساختار لایه فیزیکی استاندارد 802.11a/g در شکل(۷) ارائه‌شده است. برای هر بسته در این استاندارد، ۵۳ سمبل ارسال می‌شود که ابتدا توسط مدولاسیون QPSK مدوله می‌شوند، سپس سمبل‌های مدولاسیون OFDM با اعمال ۱۱ سمبل گارد، ۱۶ دوره چرخشی ، مجموعاً ۸۰ سمبل ساخته می‌شود.



شکل(۷) ساختار بسته استاندارد 802.11a/g

همانطورکه در شکل(۸) مشاهده می‌کنید، با افزایش نرخ توان سیگنال به توان اختلال می‌توان به نرخ خطای سمبل کمینه‌ای در گیرنده مجاز دست‌یافت، درحالی‌که برای استراق سمع کننده نرخ خطای سمبل همواره بیشینه است.



شکل(۸) **شبیه‌سازی نرخ خطای سمبل در 802.11a/g**

۶- نتیجه‌گیری

اختلال به‌طور مرسوم به‌عنوان یک مخرب برای انتقال بی‌سیم در نظر گرفته‌شده است. بااین‌حال، در ارتباطات امن، می‌تواند مفید واقع شود، و از آن برای امنیت داده‌های ارسالی استفاده کرد. در این گزارش، ما برای دستیابی به ارتباطات محرمانه در حضور یک استراق سمع کننده، طرح اختلال دوستانه را پیشنهاد کرده‌ایم. همان‌طور که مشاهده کردید نرخ خطای بیت به‌دست‌آمده در سناریوهای مختلف نشان داد که می‌توان امنیت یک لینک ارتباطی را بر اساس این تکنیک تضمین کرد. به‌عبارتی‌دیگر نرخ خطای بیت به‌دست‌آمده برای استراق سمع کننده همواره بیشینه بوده و نسخه‌ی مخدوشی از سیگنال ارسالی را می‌بیند. همچنین سناریوی موردنظر بر روی استاندارد 802.11a/g از وای فای به‌منظور بررسی و تحلیل تکنیک موردنظر بسط داده شد. نتایج نشان داد که در نرخ سیگنال به نویزهای بالا می‌توان به نرخ خطای سمبل کمینه‌ای در گیرنده مجاز دست‌یافت، درحالی‌که برای استراق سمع کننده نرخ خطای سمبل همواره بیشینه است.

فهرست

[1] G. Lin and G. Noubir, “On link layer denial of service in data wireless LANs,” *Wirel. Commun. Mob. Comput.*, vol. 5, no. 3, pp. 273–284, 2005.

[2] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, “A survey on jamming attacks and countermeasures in WSNs,” *IEEE Commun. Surv. Tutorials*, vol. 11, no. 4, pp. 42–56, 2009.

[3] K. Pelechrinis, M. Iliofotou, and S. V Krishnamurthy, “Denial of service attacks in wireless networks: The case of jammers,” *IEEE Commun. Surv. tutorials*, vol. 13, no. 2, pp. 245–257, 2010.

[4] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu, “They can hear your heartbeats: non-invasive security for implantable medical devices,” in *Proceedings of the ACM SIGCOMM 2011 conference*, 2011, pp. 2–13.

[5] Y. S. Kim and P. Tague, “Proximity-based wireless access control through considerate jamming,” in *Proceedings of the ACM MobiCom workshop on Security and privacy in mobile environments*, 2014, pp. 19–24.

[6] A. Sheikholeslami, D. Goeckel, H. Pishro-Nik, and D. Towsley, “Physical layer security from inter-session interference in large wireless networks,” in *2012 Proceedings IEEE INFOCOM*, 2012, pp. 1179–1187.

[7] J. P. Vilela, P. C. Pinto, and J. Barros, “Position-based jamming for enhanced wireless secrecy,” *IEEE Trans. Inf. Forensics Secur.*, vol. 6, no. 3, pp. 616–627, 2011.

[8] Y. Zhou, P. L. Yeoh, H. Chen, Y. Li, W. Hardjawana, and B. Vucetic, “Secrecy outage probability and jamming coverage of UAV-enabled friendly jammer,” in *2017 11th International Conference on Signal Processing and Communication Systems (ICSPCS)*, 2017, pp. 1–6.

[9] D. Li, S. Yan, X. Zhang, and Y. Shang, “Combined physical network coding and friendly jamming for secure wireless cooperative communications,” *IEEE Veh. Technol. Conf.*, 2017.

[10] X. Li and H. N. Dai, “Friendly-Jamming: An anti-eavesdropping scheme in wireless networks,” *18th IEEE Int. Symp. A World Wireless, Mob. Multimed. Networks, WoWMoM 2017 - Conf.*, pp. 1–3, 2017.

[11] Y. Sarikaya, O. Ercetin, and O. Gurbuz, “Control of Cognitive Networks with Friendly Jamming as a Service,” *IEEE Trans. Cogn. Commun. Netw.*, vol. 4, no. 2, pp. 299–313, 2018.

[12] B. Yang, W. Wang, J. Fan, and Q. Yin, “Friendly cooperation jamming for secrecy in LOS channel,” *2012 Int. Conf. Wirel. Commun. Signal Process. WCSP 2012*, pp. 0–3, 2012.