مقاله پژوهشی

مخابرات پنهان ترکیبی با استفاده از روش طیف گسترده و اختلال کمک‌کننده

مرتضی شفیعی نیستانک و ایمان کاظمی

چکیده: امروزه مخابره پنهان با هدف برقراری ارتباط با احتمال آشکارسازی پایین (LPD) به‌سرعت در مخابرات تجاری و نظامی در حال توسعه است. یکی از روش‌های رایج برای این منظور، استفاده از نویز مصنوعی به‌منظور گمراه‌سازی گیرنده غیرمجاز و بالابردن حاشیه اطمینان برای ارسال و دریافت داده است. از سوی دیگر ایجاد نویز مصنوعی در طیف فرکانسی یا بازه زمانی وسیع، چالشی مهم برای فرستنده و گیرنده مجاز خواهد بود. همچنین برقراری هم‌زمانی دقیق برای قطع و وصل نویز مصنوعی به‌گونه‌ای که به همراه سیگنال ارسالی بتواند نویز محیط را برای گیرنده غیرمجاز شبیه‌سازی کند، بسیار دشوار است. در این مقاله با ایده استفاده از روش طیف گسترده دنباله مستقیم (DS-SS) به همراه ایجاد اختلال خودی به‌عنوان نویز مصنوعی، روشی ترکیبی برای برقراری مخابره پنهان با رفع مشکلات فوق و با کیفیت و ظرفیت مخابره مناسب پیشنهاد شده است. در این صورت گسترش طیف سیگنال ارسالی، ایجاد نویز مصنوعی با سطح توان و هزینه پایین و به‌صورت دائم را امکان‌پذیر کرده و نیازی به برقراری هم‌زمانی قطع و وصل بین نویز مصنوعی و سیگنال ارسالی نیز نخواهد بود. نتایج شبیه‌سازی و تحلیل عددی نشان می‌دهند در شرایط $JSR = -5\,dB$، استفاده از نویز مصنوعی بر اساس اختلال باند جزئی، ضمن ایجاد حاشیه اطمینان ۱٫۸ dB برای فریب‌دادن شنودگر، کیفیت قابل قبول مخابره را بین فرستنده و گیرنده فراهم نموده و برای $E_b/N > 8.3\,dB$ احتمال خطای مناسب 10^{-3} را در شرایط شبیه‌سازی نتیجه خواهد داد. بررسی برای سایر انواع اختلال نشان می‌دهد که غیر از اختلال چندآهنگ، امکان استفاده از انواع نویز مصنوعی برای روش پیشنهادی وجود دارد. به عنوان مثال اختلال تک‌آهنگ نیز با ایجاد ۲٫۶ dB حاشیه اطمینان، احتمال خطای 10^{-3} را برای $E_b/N > 10.9\,dB$ بین فرستنده و گیرنده ایجاد خواهد کرد.

کلیدواژه: **اختلال، دنباله مستقیم (DS)، طیف گسترده، مخابرات پنهان، نویز مصنوعی.**

۱- مقدمه

امنیت در شبکه‌های ارتباطی مدرن مسئله بسیار مهمی است. از گذشته تاکنون، دیدگاه‌های گوناگونی برای برقراری امنیت ارتباطات در بخش‌های مختلف سیستم‌های مخابراتی اعم از بخش داده، سیگنال و انتشار مطرح شده است. ایجاد امنیت و مخفی‌سازی محتوا در بخش داده شبکه‌های مخابراتی، عموماً بر اساس رمزنگاری[1] انجام می‌شود [۱]. همچنین با دیدگاه پنهان‌سازی داده، ایده نهان‌نگاری[2] توسعه یافت که بر اساس آن می‌توان بخشی از پیام را که حاوی اطلاعات محرمانه است، درون پیام دیگری که به آن حامل[3] یا پوشش[4] گفته می‌شود، پنهان نمود [۲]. در بخش سیگنال سیستم‌های مخابراتی، انواع روش طیف گسترده[5] (SS) برای برقراری امنیت ارائه شده‌اند [۳] و [۴]. روش‌هایی نظیر شکل‌دهی پرتو[6] [۵]، ارسال رگباری[7] [۶] و مخابرات پنهان[8] (CC) [۷] به کمک نویز مصنوعی[9] (AN) [۸] نیز امنیت مخابره در بخش انتشار سیستم مخابراتی را تأمین می‌کنند. همه این روش‌ها برای تأمین یکی از دو هدف احتمال آشکارسازی پایین[10] (LPD) یا احتمال شنود پایین[11] (LPI) برای سیگنال مخابراتی طراحی و پیشنهاد شده‌اند [۴]. در روش‌های دارای احتمال آشکارسازی پایین (LPD)، پنهان‌کردن وجود ارتباط و در روش‌های دارای احتمال شنود پایین (LPI)، نامفهوم‌کردن پیام ارسالی مورد توجه هستند.

مخابرات پنهان در واقع، هنر انتقال داده بدون شناسایی‌شدن توسط کاربر غیرمجاز است. ایده مخابرات پنهان برای ایجاد احتمال آشکارسازی پایین (LPD)، اولین بار توسط گوستاو سیمونز[12] در سال ۱۹۸۴ با مثالی از «پیام مخفی زندانی‌ها» ارائه شد [۹]. در مدل سیمونز دو زندانی آلیس و باب[13] در سلول‌های جداگانه زندانی شده و برای طرح‌ریزی نقشه فرار، نیاز به ارتباط با یکدیگر دارند. پیام‌های آنها همواره تحت نظر نگهبان (ویلی[14]) منتقل می‌شود و اگر هر گونه نقشه توطئه‌آمیزی شناسایی شود، این دو زندانی به انفرادی برده می‌شوند. بنابراین آلیس و باب برای موفقیت در فرار باید راهکاری برای مبادله پیام‌ها به‌صورت مخفی بیابند [۱۰]. در ادبیات مخابرات پنهان، مخفی‌کردن سیگنال در نویز بسیار قابل توجه بوده و در سال‌های اخیر، نظر بسیاری از پژوهشگران را به خود جلب کرده است [۱۱] تا [۱۳].

1. Cryptography
2. Steganography
3. Carrier
4. Cover
5. Spread Spectrum
6. Beam Forming
7. Burst
8. Covert Communications
9. Artificial Noise
10. Low Probability of Detection
11. Low Probability of Interception
12. Gustavus Simmons
13. Alice and Bob
14. Willie

این مقاله در تاریخ ۲۵ شهریور ماه ۱۴۰۲ دریافت و در تاریخ ۲۳ آذر ماه ۱۴۰۲ بازنگری شد.

مرتضی شفیعی نیستانک (نویسنده مسئول)، دانشکده مهندسی برق و کامپیوتر، دانشگاه صنعتی مالک اشتر، تهران، ایران، (email: mshafiee@mut.ac.ir).

ایمان کاظمی، دانشکده مهندسی برق و کامپیوتر، دانشگاه صنعتی مالک اشتر، تهران، ایران، (email: Iman_kazemi@mut.ac.ir).

در این مقاله با استفاده توأم از روش طیف گسترده دنباله مستقیم (DS-SS)[۱] به‌همراه ایجاد نویز مصنوعی (AN) از طریق روش‌های مختلف مختل‌سازی[۲] نظیر مختل‌سازی تک‌آهنگ[۳] و چندآهنگ[۴]، مختل‌سازی جاروب خطی[۵]، مختل‌سازی نویز باند جزئی (PBNJ)[۶] و مختل‌سازی مدولاسیون فرکانسی (FMJ)[۷]، روشی برای برقراری مخابره پنهان بین آلیس و باب ارائه شده است. نویز مصنوعی در واقع سیگنال فریبی است که توسط فرستنده خودی ایجاد و منتشر می‌گردد و در کارکرد شنودگر محیطی ایجاد تداخل نمی‌کند؛ بلکه درصدد جلب توجه شنودگر به‌منظور فریب آن است [۱۴].

نتایج شبیه‌سازی و تحلیل‌ها نشان می‌دهند که بازیابی سیگنال اصلی توسط گیرنده (باب) با نرخ خطای بیت (BER) قابل قبول $۱۰^{-۳}$ امکان‌پذیر است؛ در حالی که شنودگر (ویلی) امکان تشخیص مخابره را نخواهد داشت. با توجه به خواص روش طیف گسترده (DS-SS)، روش پیشنهادی ضمن برقراری مخابره پنهان، مزایایی نظیر ارسال سیگنال با سطح توان پایین، دشواربودن آشکارسازی سیگنال برای گیرنده غیرمجاز، کاهش احتمال نفوذ به شبکه مخابراتی، توأم‌بودن خواص (LPD) و (LPI) برای مخابره و همچنین مقاوم‌شدن سیگنال در مقابل آثار مخرب ناشی از تداخل[۸] سایر کاربران، محوشوندگی چندمسیری[۹] و امکان برقراری برقراری دسترسی چندگانه بر اساس CDMA[۱۰] را به دنبال خواهد داشت. به بیان دیگر در این مقاله، نوآوری‌های زیر به‌منظور بهبود کیفیت و ظرفیت مخابره پنهان در مقایسه با سایر فعالیت‌ها پیشنهاد شده است:

- در مخابره پنهان به کمک نویز مصنوعی باید سطح نویز شنودگر در زمان ارسال فرستنده و عدم ارسال، ثابت بماند تا شنودگر متوجه تبادل اطلاعات فرستنده و گیرنده نشود. این امر مستلزم برقراری هم‌زمانی دقیق بین نویز مصنوعی و فرستنده است. در این مقاله با پیشنهاد استفاده از طیف گسترده برای ارسال و دریافت سیگنال، چالش نیاز به هم‌زمانی قطع و وصل نویز مصنوعی از بین رفته و سیگنال فرستنده به‌صورت پیوسته قابل ارسال است. با رفع این چالش ضمن افزایش ظرفیت ارسال می‌توان محل فیزیکی نویز مصنوعی را از فرستنده جدا نمود و پنهان‌مانی مخابره را افزایش داد.
- یکی از چالش‌های استفاده از نویز مصنوعی برای مخابره پنهان، نیاز به ارسال نویز پرتوان در طیف فرکانسی یا بازه زمانی وسیع است. با پیشنهاد استفاده ترکیبی از نویز مصنوعی و روش طیف گسترده، امکان فریب شنودگر با نویز مصنوعی توان پایین فراهم شده و پیاده‌سازی روش با ظرفیت ارسال دائمی مقرون‌به‌صرفه خواهد شد.

بخش ۲ به مرور فعالیت‌های مرتبط گذشته پرداخته است. بخش ۳ اصول روش طیف گسترده دنباله مستقیم (DS-SS) را مرور می‌کند. در بخش ۴ به معرفی انواع مدل‌های رایج ایجاد اختلال پرداخته می‌شود. در مقاله از این مدل‌ها برای ایجاد نویز مصنوعی محیطی به‌منظور فریب شنودگر و پنهان‌سازی مخابره از دید وی استفاده شده است. بخش ۵ مدل و روش پیشنهادی مسئله برای مخابره پنهان را به‌صورت تحلیلی ارائه نموده و در بخش ۶ ضمن ارائه نتایج شبیه‌سازی به تحلیل و نتیجه‌گیری خواهیم پرداخت. نهایتاً مقاله با بخش ۷ به‌عنوان جمع‌بندی و ارائه پیشنهادهایی برای ادامه فعالیت خاتمه می‌یابد.

۲- فعالیت‌های مرتبط

روش‌های طیف گسترده از اوایل قرن بیستم در ارتباطات نظامی مورد توجه قرار گرفتند. مروری بر انواع روش‌های طیف گسترده در [۳] و [۴] صورت گرفته است. در [۱۲] روشی مبتنی بر نهان‌نگاری بر اساس مدل نویز جمع‌شونده پیشنهاد شده که اطلاعات سیگنال را به نویز تبدیل کرده و تلاش می‌کند با مخفی‌کردن اطلاعات به‌صورت نویز ساختگی آمیخته با نویز AWGN[۱۱] کانال، امنیت داده‌ها را برقرار نموده و باعث مقاومت روش پیشنهادی در برابر استراق سمع شود. در [۱۳] آقای بش[۱۲] و همکاران با ارائه یک قانون حداقل ریشه مربعات (SRL)[۱۳] برای کانال AWGN نشان دادند در استفاده از N کانال، حداکثر از مرتبه $O(\sqrt{N})$ بیت را می‌توان به‌طور قابل اعتماد و مخفیانه در حضور شنودگر (ویلی) به گیرنده اصلی (باب) منتقل کرد. در [۱۲] و [۱۳]، مدل کانال به‌طور خاص به کانال AWGN محدود شده و در روابط و تحلیل‌های به‌دست‌آمده، اثری از تداخلات محیط و وجود اختلال به چشم نمی‌خورد.

در سال‌های اخیر برای بهبود کیفیت مخابرات پنهان و در نتیجه برقراری امنیت در مخابرات بی‌سیم، مطالعات فراوانی انجام شده که برخی از این مطالعات مربوط به عدم قطعیت نویز[۱۴] می‌شود [۱۵] و [۱۶]. عدم قطعیت نویز یک فرض عملی است که در آن اطلاعاتی از توان نویز در سمت شنودگر وجود ندارد یا بسیار محدود است. در [۱۵] تا [۱۹] به بررسی عملکرد مخابرات پنهان در کانال‌های غیرگوسی و تأثیر مشترک عدم قطعیت کانال و عدم قطعیت نویز بر روی احتمال خطای تشخیص سیگنال در سمت شنودگر و گیرنده در کانال‌هایی نظیر کانال محوشدگی رایلی و ناکاگامی پرداخته شده و راه حل‌هایی برای مسائل فوق ارائه گردیده است. مراجع [۲۰] تا [۲۳] نیز از سیستم‌های چندآنتنه برای بهبود کیفیت مخابرات پنهان استفاده کرده‌اند. مراجع [۲۰] و [۲۱] نشان داده‌اند که افزایش تعداد آنتن در فرستنده و گیرنده در بهبود عملکرد مخابرات پنهان نقش مؤثری ایفا می‌کند. همچنین در [۲۲] و [۲۳] از اختلال چندآنتنه با هدف کمک به فرستنده استفاده شده است. در پیشنهادهای این مراجع، طرفین ارتباط از ارسال اختلال برای فریب شنودگر بهره می‌برند. مرجع [۲۴] نیز یک روش مخابره پنهان را با کمک مختل‌ساز شناختی[۱۵] به‌منظور فریب و گمراه‌سازی شنودگر پیشنهاد داده است. در روش پیشنهادشده، مختل‌ساز شناختی از انتقال پیام فرستنده (آلیس) آگاه است و بر اساس نتایج سنجش خود، تعیین می‌کند که آیا سیگنال اختلال را ارسال کند یا خیر. در این کار زمانی اختلال فعال می‌شود که آلیس داده‌ای ارسال نمی‌کند و زمانی که آلیس در حال ارسال پیام است، اختلال خاموش می‌شود. همچنین نشان داده شده که عملکرد مختل‌ساز شناختی، افزایش نرخ پنهان[۱۶] را نسبت به مختل‌ساز غیرآگاه[۱۷] به ارمغان آورده و در

1. Direct Sequence-Spread Spectrum
2. Jamming
3. Single Tone Jamming
4. Multi Tone Jamming
5. Linear Sweeping Jamming
6. Partial-Band Noise Jamming
7. Frequency-Modulated Jamming
8. Interference
9. Multipath Fading
10. Code Division Multiple Access
11. Additive White Gaussian Noise
12. Bash
13. Square Root Law
14. Noise Uncertainty
15. Cognitive Jammer
16. Covert Rate
17. Non-Informed Jammer

جدول ۱: خلاصه فعالیت‌های انجام‌شده در زمینه مخابرات پنهان.

ردیف	مرجع	سال انتشار	توضیح روش	نکات
۱	[۳] و [۴]	۱۹۹۴ و ۱۹۹۵	مروری بر انواع روش‌های طیف گسترده	+ به معرفی روش‌ها و مبانی نظری پرداخته شده است.
۲	[۱۲]	۲۰۱۱	روش پنهان‌نگاری با استفاده از کدهای بلوکی خطی	– محدودبودن الگوریتم به کانال AWGN – نداشتن حاشیه اطمینان در مخابره پنهان – عدم مقاومت روش در برابر تداخلات محیطی
۳	[۱۳]	۲۰۱۳	محاسبه ظرفیت ارسال به کمک قانون حداقل ریشه مربعات	– محدودبودن الگوریتم به کانال AWGN – عدم مقاومت روش در برابر تداخلات محیطی – نداشتن حاشیه اطمینان در مخابره پنهان
۴	[۱۵] تا [۱۷]	۲۰۱۷ و ۲۰۱۹	بررسی اثر عدم قطعیت نویز در مخابرات پنهان	+ محاسبه احتمال خطا در کانال غیرگوسی – نداشتن حاشیه اطمینان در مخابره پنهان – نیاز به هماهنگی بین اختلال با فرستنده - هزینه بالای اختلال به‌دلیل بالابودن سطح سیگنال
۵	[۱۸]	۲۰۲۰	استفاده از نویز مصنوعی برای مخابرات پنهان	+ تصادفی‌بودن ارسال تداخل روی کانال شنودگر غیرمجاز – نداشتن حاشیه اطمینان در مخابره پنهان – عدم مقایسه عملکرد و اثرگذاری انواع نویز مصنوعی
۶	[۱۹]	۲۰۲۱	استفاده از اختلال چندآهنگ برای مخابرات پنهان در کانال محوشدگی	+ برتری توان عملکردی اختلال چندآهنگ نسبت به تک‌آهنگ – تحت تأثیر قرارگرفتن مخابرات پنهان فرستنده- گیرنده تحت اختلال چندآهنگ
۷	[۲۰] تا [۲۳]	۲۰۱۹ و ۲۰۲۱	بهبود کیفیت مخابرات پنهان در حضور محوشدگی با استفاده از سیستم‌های چندآنتنه	+ بهبود عملکرد مخابرات پنهان با افزایش تعداد آنتن – عدم مقایسه عملکرد و اثرگذاری انواع نویز مصنوعی – نداشتن حاشیه اطمینان در مخابره پنهان – نیاز به هماهنگی بین اختلال و فرستنده
۸	[۲۴]	۲۰۲۰	استفاده از نویز مصنوعی شناختی برای مخابره پنهان	– محدودبودن الگوریتم به کانال AWGN – نداشتن حاشیه اطمینان در مخابره پنهان – عدم مقایسه عملکرد و اثرگذاری انواع نویز مصنوعی
۹	[۱۶]	۲۰۲۱	حذف اختلال شنودگر مخابرات پنهان با استفاده از کدگذاری گوسی و مدولاسیون زمان- فرکانس	– عدم مقایسه عملکرد در برابر انواع اختلال – تصادفی‌بودن ارسال تداخل

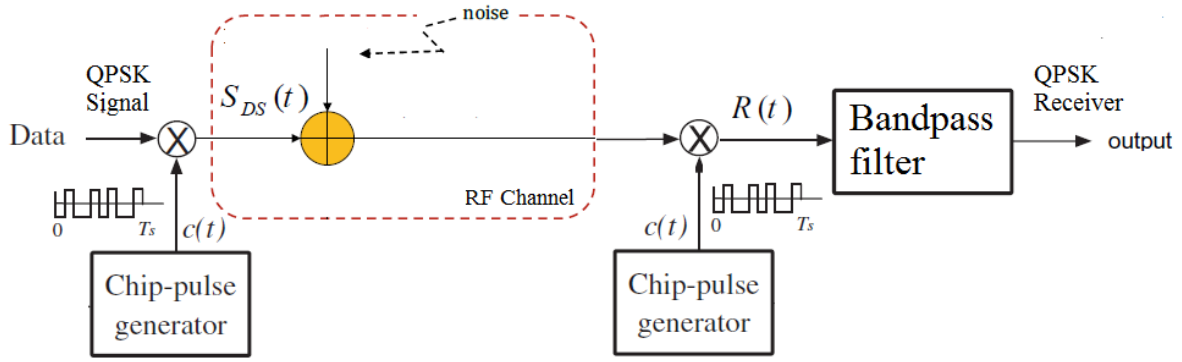
عین حال مانع تشخیص انتقال پیام توسط شنودگر (ویلی) می‌شود. در [۲۵] شنودگر به‌منظور ازبین‌بردن امکان ارتباط بین طرفین مخابره در کانال، اختلال ایجاد می‌کند. بر این اساس الگوریتم پیشنهادی برای گیرنده، اختلال شنودگر را تخمین زده و از سیگنال دریافتی فرستنده خودی حذف می‌کند. جدول ۱ خلاصه‌ای از فعالیت‌های انجام‌شده در زمینه مخابرات پنهان را به همراه برخی مزایا و معایب این روش‌ها نشان می‌دهد.

همان طور که اشاره شد در این مقاله بر ایجاد مخابرات پنهان با استفاده توأم از روش طیف گسترده (DS-SS) و ارسال اختلال خودی به عنوان نویز مصنوعی تمرکز شده است. در این صورت بدون نیاز به برقراری هم‌زمانی یا قطع ارتباط می‌توان بدون آگاهی شنودگر به مخابره دائمی اقدام نمود. از گذشته تاکنون تحقیقات گوناگونی بر عملکرد روش‌های طیف گسترده در حضور انواع تداخل و اختلال صورت گرفته که می‌توان از نتایج آنها برای تحلیل مدل پیشنهادی استفاده نمود [۲۶] تا [۲۸]. در مخابرات طیف گسترده، اختلال توسط فرستنده غیرخودی (مهاجم) انجام شده و هدف اصلی سیستم مخابراتی از به‌کارگیری روش طیف گسترده، مقابله با این اختلال است؛ اما در مخابرات پنهان از اختلال به‌عنوان نویز مصنوعی و توسط سیستم مخابرات خودی با هدف کمک به مخفی‌سازی ارسال و دریافت و ایجاد شرایط LPD برای سیگنال ارسالی استفاده می‌شود. با این دیدگاه، مراجع قبلی از نویز مصنوعی به‌تنهایی و برای بالابردن سطح آستانه شنودگر استفاده کرده‌اند. در مقاله حاضر ایده استفاده ترکیبی از نویز مصنوعی و روش طیف گسترده به‌منظور فراهم‌نمودن امکان مخابره پیوسته، استفاده از نویز مصنوعی توان پایین و عدم نیاز به هم‌زمانی قطع و وصل پیشنهاد شده است.

۳- روش طیف گسترده دنباله مستقیم (DS-SS)

روش دنباله مستقیم (DS)، یکی از انواع روش‌های طیف گسترده برای برقراری ارتباط با احتمال آشکارسازی پایین (LPD) می‌باشد. در این روش مطابق شکل ۱، کد $C(t)$ یک دنباله متناوب گسترش‌دهنده طیف شبه‌نویز (PN)[1] است که سیگنال باند باریک حاوی اطلاعات با پهنای باند W_S را در پهنای باند W_C گسترده می‌کند؛ به‌طوری که معمولاً $W_C \gg W_S$ می‌باشد. امروزه تنوع وسیعی از کدهای شبه‌نویز با خواص و قابلیت‌های متفاوت پیشنهاد شده که معروف‌ترین آنها کدهای با طول حداکثر[2] می‌باشند [۲۹]. این کدها رایج‌ترین انواع کدهای PN هستند که با دوره تناوب $N = ۲^m - ۱$ توسط شیفت رجیسترهای خطی با m خانه ساخته می‌شوند. سیگنال طیف گسترده دنباله مستقیم از ضرب مستقیم کد شبه‌نویز در سیگنال مدوله‌شده دیجیتال (مثلاً سیگنال با مدولاسیون QPSK) ایجاد می‌شود. بنابراین فرستنده، حاصل‌ضرب سیگنال مدوله‌شده و کد گسترش طیف $C(t)$ با دوره پالس چیپ[3] T_C را روی کانال مخابراتی ارسال می‌نماید.

1. Pseudo Noise
2. Maximal Length Sequences
3. Chip Duration



شکل ۱: بلوک دیاگرام روش طیف گسترده دنباله مستقیم (DS-SS).

با درنظرگرفتن دوره پالس سمبل[1] داده برابر T_S، ضریب گسترش پهنای باند طیف L را می‌توان به‌صورت (۱) نشان داد. مطابق شکل ۱ با توجه به اینکه سیگنال ارسالی $S_{DS}(t)$ در حوزه زمان حاصل‌ضرب دو سیگنال است، پهنای باند گسترش‌یافته آن در حوزه فرکانس برابر مجموع پهنای باند سیگنال مدوله‌شده (در اینجا سیگنال QPSK) و کد گسترش طیف $C(t)$ خواهد بود و با توجه به اینکه معمولاً $L \gg 1$، پهنای باند طیف سیگنال گسترش‌یافته، مطابق (۲)، تقریباً L برابر پهنای طیف سیگنال مدوله‌شده اصلی خواهد بود [۳۰]

$$L = \frac{T_S}{T_C} \qquad (۱)$$

$$W_C = (L+1)W_S \approx LW_S \qquad (۲)$$

همان طور که اشاره گردید در این مقاله با استفاده از دو خاصیت ضداختلال‌بودن (AJ)[2] و احتمال آشکارسازی پایین سیگنال DS، شرایط مناسب برای مخابره پنهان بین فرستنده و گیرنده دور از تشخیص شنودگر فراهم شده است. همچنین به‌صورت توأم با ایجاد نویز مصنوعی توسط اختلال، بدون اثرگذاری روی دریافت گیرنده، فعالیت مخابره برای شنودگر بیشتر مخفی خواهد شد.

٤- مدل‌های رایج سیگنال اختلال

همان طور که ذکر گردید می‌توان از انواع اختلال به‌عنوان نویز مصنوعی در مخابرات پنهان استفاده نمود. امروزه روش‌های متنوعی برای ایجاد اختلال با مشخصات مختلف در محیط‌های مخابراتی و نظامی وجود دارند که کاربردی‌ترین آنها در ادامه آمده‌اند [۳۱].

٤-۱ اختلال تک‌آهنگ

مطابق (۳)، مختل‌ساز تک‌آهنگ ارتباط و آشکارسازی سیگنال را در یک نقطه فرکانسی خاص مثل f_J مسدود می‌سازد [۳۲]. در (۳)، A دامنه اختلال و ϕ فاز آن بوده و اختلال فعالیت مخابراتی را در ناحیه پوشش و در فرکانس f_J تحت تأثیر قرار می‌دهد

$$J(t) = Ae^{j(2\pi f_J t+\phi)} \qquad (۳)$$

٤-۲ اختلال چندآهنگ

مختل‌ساز چندآهنگ مطابق با (۴) به‌منظور پوشش وسیع‌تر پهنای باند مخابراتی در M نقطه فرکانسی مختلف ایجاد می‌گردد [۳۲] و [۳۳] که در این رابطه نیز A دامنه اختلال و ϕ_m فاز آن در M نقطه فرکانسی است

$$J(t) = \sum_{m=1}^{M} Ae^{j(2\pi f_m t+\phi_m)} \qquad (۴)$$

٤-۳ اختلال جاروب خطی

این نوع مختل‌ساز که با عنوان اختلال مدوله‌شده فرکانس خطی LFM نیز شناخته می‌شود، مطابق (۵) قابلیت برقراری ارتباط را در یک پهنای باند فرکانسی مشخص، مسدود می‌سازد [۳۲]. در این رابطه نیز A دامنه، ϕ فاز و k محدوده پهنای باند مختل‌کننده را تعیین می‌کنند

$$J(t) = Ae^{j(2\pi f_c t+\pi kt^2+\phi)} \qquad (۵)$$

٤-٤ اختلال نویز باند جزئی (PBNJ)

این نوع مختل‌ساز، نویز گوسی سفید را در محدوده‌ای حول فرکانس مختل‌کننده، ایجاد کرده و تشخیص سیگنال اصلی را در این پهنای باند دشوار می‌سازد. به نظر می‌رسد که عملکرد این نوع اختلال از لحاظ مختل‌کردن یک محدوده فرکانسی مسطح، مشابه اختلال جاروب خطی باشد؛ اما چگالی طیف توان آن در محدوده فرکانسی اختلال از جنس نویز گوسی است و می‌تواند با بیشترین آنتروپی، فضای فرکانسی مورد نظر را مختل نماید [۳۲] و [۳۴]. در (۶)، A دامنه، ϕ فاز و $U(t)$ نویز گوسی با متوسط f_J و واریانسی که توسط توان مورد نیاز برای اختلال تعیین می‌گردد، هستند

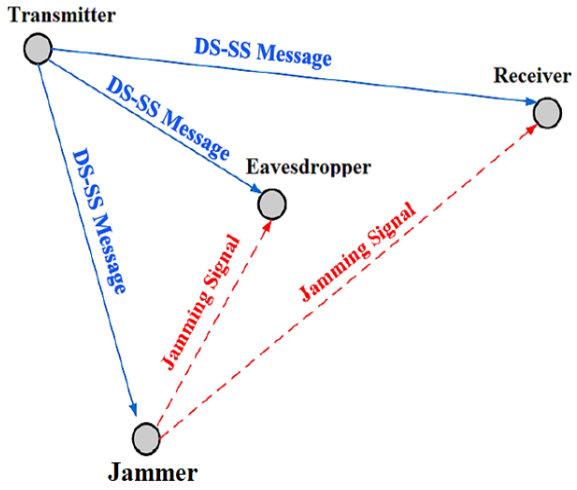
$$J(t) = AU(t)e^{j(2\pi f_J t+\phi)} \qquad (۶)$$

٤-۵ اختلال مدولاسیون فرکانسی

مختل‌ساز مدولاسیون فرکانسی نیز سیگنالی با چگالی طیف توان گوسی داشته و به‌عنوان تداخل باند وسیع در نظر گرفته می‌شود. همان طور که از نام مدولاسیون FM مشخص است در این نوع مختل‌کننده، سیگنال پیام $\zeta(t)$ در فرکانس سیگنال حامل اختلال حضور دارد [۳۲] و [۳۵] و به عبارت دیگر، فرکانس سیگنال این اختلال به‌صورت $f(t) = f_c + k_{jm}\zeta(t)$ می‌باشد که در آن f_c فرکانس حامل و k_{jm} فاکتور حساسیت فرکانس نام دارند. مدل سیگنال اختلال مدولاسیون فرکانسی به‌صورت (۷) خواهد بود که در این رابطه، A دامنه سیگنال مختل‌کننده است

$$J(t) = Ae^{j2\pi f_c t + j2\pi k_{jm}\int_{-\infty}^{t}\zeta(\tau)d\tau} \qquad (۷)$$

1. Symbol Duration
2. Anti-Jamming



شکل ۲: مدل سیستم مخابرات پنهان پیشنهادی.

۵- مدل پیشنهادی مخابره پنهان ترکیبی

روش مخابره پنهان ترکیبی را مطابق با شکل ۲ پیشنهاد می‌دهیم. طبق شکل فرستنده در حضور شنودگر، پیامی را برای گیرنده ارسال می‌کند. برای ایجاد شرایط احتمال آشکارسازی پایین (LPD) و احتمال شنود پایین (LPI) و پنهان‌نمودن مخابره از دید شنودگر، فرستنده از روش طیف گسترده دنباله مستقیم (DS-SS) برای ارسال سیگنال استفاده می‌کند. همچنین به‌طور هم‌زمان و به‌منظور بالابردن سطح نویز در گیرنده شنودگر و کمک به مخابره پنهان، یک منبع اختلال مجزای خودی به‌طور پیوسته و بدون نیاز به قطع و وصل، نویز مصنوعی را روی کانال ارسال می‌کند. اگرچه نویز مصنوعی می‌تواند مستقیماً توسط فرستنده نیز ارسال گردد، برای عدم شناسایی مکان و اطمینان بیشتر از LPDبودن ارتباط، استفاده از منبع مجزا برای ارسال اختلال پیشنهاد شده است. در این صورت ارتباط بین فرستنده و گیرنده نیز می‌تواند به‌طور پیوسته با استفاده از روش DS-SS و در نتیجه بدون اطلاع شنودگر و منبع اختلال برقرار شود. بنابراین سیگنال دریافتی در گیرنده که باید حذف گسترش روی آن با استفاده از ضرب مجدد در کد گسترش طیف $C(t)$ انجام شود، به‌صورت (۸) است که $U(t)$ و $J(t)$ به‌ترتیب سیگنال ارسالی فرستنده و نویز مصنوعی و $n(t)$ نویز گوسی محیط با متوسط صفر و چگالی طیف توان $S_n(f)=N/2$ خواهند بود

$$R(t)=U(t)+J(t)+n(t) \qquad (۸)$$

در این صورت می‌توان نشان داد که با فرض برقراری هم‌زمانی و انجام صحیح گسترش و حذف گسترش طیف با تقریب خوبی، احتمال خطای گیرنده بهینه در کانال AWGN، صرف نظر از اینکه از DS-SS استفاده کنیم یا خیر، بدون تغییر می‌ماند. مثلاً [۳۰] نشان داده در کانال AWGN برای سیستم طیف گسترده DS با مدولاسیون BPSK، احتمال خطا با تقریب خوبی برابر احتمال خطای گیرنده PSK باینری متداول (غیر طیف گسترده) و به‌صورت (۹) خواهد بود که در آن E_b انرژی هر بیت (پالس) سیگنال دریافتی و N چگالی طیف نویز گیرنده است

$$P_b=Q\left(\sqrt{\frac{2E_b}{N}}\right) \qquad (۹)$$

بنابراین در روش پیشنهادی با توجه به اینکه گیرنده و شنودگر، علاوه بر سیگنال فرستنده و نویز کانال، نویز مصنوعی را نیز به‌صورت سیگنال اختلال دریافت می‌کنند، احتمال خطای گیرنده تحت تأثیر نویز مصنوعی به‌صورت گسترش‌یافته و شنودگر تحت تأثیر همان نویز مصنوعی ولی به‌صورت مستقیم و با توان بالا قرار خواهند گرفت. در واقع در گیرنده با فرض پهنای باندهای سیگنال ارسالی، کد گسترش‌دهنده و اختلال به‌ترتیب برابر W_S، W_C و W_j و با توجه به ضرب کد و گسترش‌یافتن سیگنال اختلال به‌صورت $J(t)=j(t)\times c(t)\Leftrightarrow J(f)*C(f)$ طبق (۲) پهنای باند سیگنال اختلال گسترش‌یافته به‌طور تقریبی مطابق (۱۰) خواهد بود

$$W_C+W_j=LW_S+W_j \qquad (۱۰)$$

از سوی دیگر با توجه به اینکه گیرنده مطابق با سیگنال ارسالی فرستنده طراحی شده است، بخشی از نویز مصنوعی با پهنای باندی معادل پهنای باند سیگنال ارسالی دریافت می‌شود $(W_S=W_j)$ و بعد از حذف گسترش، پهنای باند $J(t)$ برابر با $(1+L)W_S$ خواهد بود. به عبارت دیگر، نویز مصنوعی $J(t)$ توسط کد گسترش‌دهنده $C(t)$، تقریباً به میزان L برابر گسترده می‌شود [۲۹]. همچنین با فرض اینکه اختلال نویز مصنوعی دارای توان P_j و پهنای باند W_S باشد، طیف اختلال قبل و بعد از حذف گسترش به‌ترتیب برابر (۱۱) و (۱۲) خواهد بود

$$S_j(f)=\frac{P_j}{W_S}$$
$$f_c-\frac{1}{2}W_S\le f\le f_c+\frac{1}{2}W_S \qquad (۱۱)$$

$$S_j(f)=\frac{P_j}{(L+1)W_S}$$
$$f_c-\frac{1}{2}(L+1)W_S\le f\le f_c+\frac{1}{2}(L+1)W_S \qquad (۱۲)$$

بنابراین عملیات حذف گسترش DS-SS که در گیرنده انجام می‌شود، سطح طیف توان نویز مصنوعی را به اندازه $1/(L+1)$ کاهش داده و مشکلی برای آشکارسازی داده ارسالی در گیرنده ایجاد نخواهد شد. همچنین با حضور اختلال، احتمال خطای گیرنده کانال AWGN در (۹) به‌صورت (۱۳) بازنویسی می‌گردد [۳]

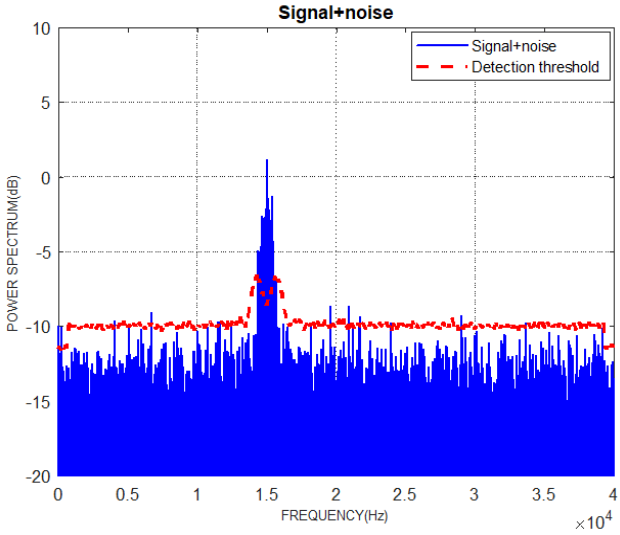
$$P_b=Q\left(\sqrt{\frac{2E_b}{N+S_J(f)}}\right) \qquad (۱۳)$$

از سوی دیگر مطابق (۱۴) نسبت اختلال (جمر[1]) به سیگنال (JSR) با افزایش ضریب گسترش طیف کاهش می‌یابد و علی‌رغم اثرگذاری روی شنودگر، تأثیر کمتری در گیرنده خواهد داشت

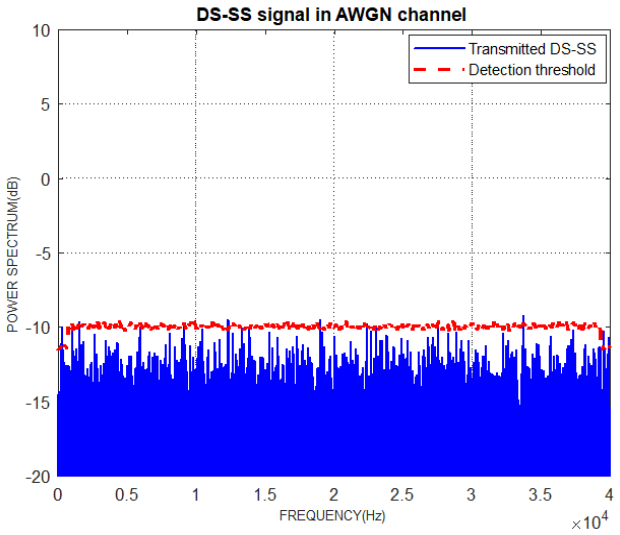
$$JSR=\frac{\frac{E_b}{P_j}}{\frac{(L+1)W_S}{\frac{E_b}{P_j}}}=\frac{1}{L+1} \qquad (۱۴)$$

اگر اختلال را از نوع باند وسیع در نظر بگیریم و با فرض درنظرگرفتن پهنای باند اختلال برابر با $LW_S=W_j$، پهنای باند $J(t)$ پس از حذف گسترش بر اساس (۱۰) برابر $2LW_S$ می‌شود که نشان می‌دهد پهنای باند طیف دو برابر نسبت به حالت باند باریک گسترده خواهد شد. از این رو پس از عملیات حذف گسترش، نسبت اختلال به سیگنال JSR به

1. Jammer



شکل ۳: شناسایی ارتباط توسط شنودگر (ارسال عادی).



شکل ۴: عدم شناسایی ارتباط توسط شنودگر (طیف گسترده).

نسبت $1/(2L)$ کاهش خواهد یافت و می‌توان انتظار داشت که اولاً با کاهش JSR ضمن مختل‌شدن فرایند شنود توسط شنودگر، به احتمال خطای بیت بهتری برای ارتباط فرستنده و گیرنده نسبت به حالت غیرطیف گسترده دست یابیم. ثانیاً هزینه مصرف توان اختلال خودی که از چالش‌های اصلی است نیز کاهش چشم‌گیری خواهد یافت؛ در نتیجه امکان اختلال پیوسته در کل بازه زمانی به‌راحتی فراهم شده و افزایش ظرفیت ارسال اطلاعات را به دنبال خواهد داشت.

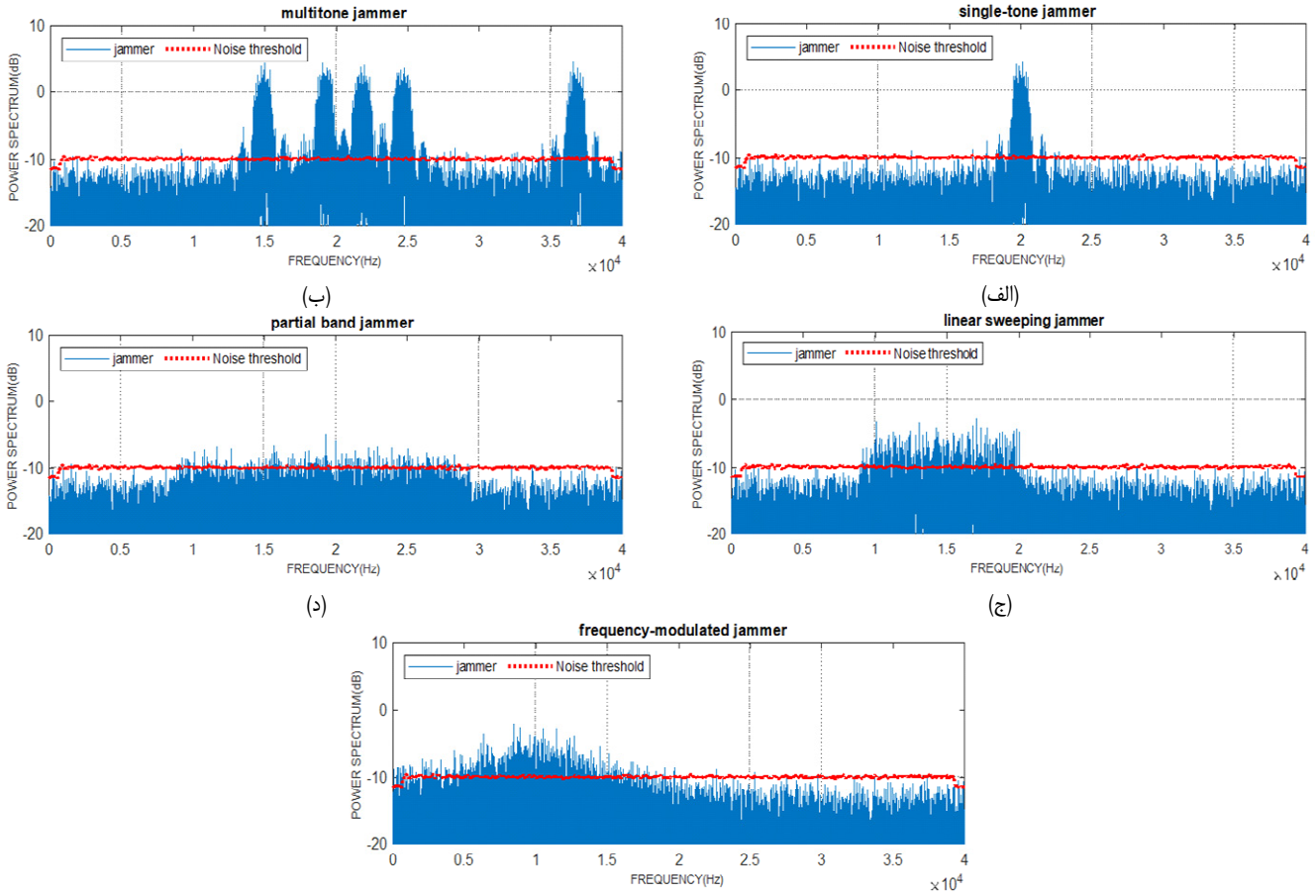
۶- ارزیابی روش پیشنهادی

به منظور ارزیابی، شبیه‌سازی‌ها را بر اساس روش طیف گسترده DS با استفاده از کد طول محدود بارکر [۳۶] با طول $L=13$ و در نتیجه بهره پردازش ۱۱ dB انجام می‌دهیم. همچنین مدولاسیون QPSK، کانال انتقال را AWGN و شنودگر را با آشکارساز از نوع CA-CFAR[1] [۳۷] در نظر می‌گیریم. این آشکارساز در سیستم‌های عملی رایج بوده و به‌صورت خودکار سطح آستانه خود را برای داشتن احتمال هشدار کاذب[2] ثابت، تغییر می‌دهد. سطح آستانه این آشکارساز بر اساس میانگین‌گیری و تخمین توان متوسط نویز محیط تعیین می‌شود. به‌منظور ارزیابی عملکرد شنودگر در شناسایی و تشخیص ارتباط بین فرستنده و گیرنده، آشکارسازی را در حوزه فرکانس بررسی می‌کنیم. ابتدا با فرض اینکه فرستنده، سیگنالی با فرکانس حامل ۱۵ KHz و مدولاسیون QPSK روی کانال AWGN ارسال می‌کند، مطابق شکل ۳ مشاهده می‌شود در حالت عادی و بدون استفاده از روش طیف گسترده، سیگنال ارسالی توسط شنودگر با استفاده از آشکارساز CA-CFAR قابل شناسایی خواهد بود. اکنون با فرض اینکه شنودگر این سطح آستانه را برای آشکارسازی و تفکیک سیگنال از نویز در حوزه فرکانس ثبت کرده باشد، ارتباط را در حالت پیشنهادی که سیگنال فرستنده به‌صورت طیف گسترده دنباله مستقیم DS روی کانال AWGN ارسال می‌شود، بررسی می‌کنیم. همان طور که در شکل ۴ دیده می‌شود در این حالت، عملاً شناسایی سیگنال ارسالی توسط شنودگر غیرممکن است. همچنین شکل ۵ طیف فرکانسی سیگنال گسترده‌شده فرستنده را با حضور سیگنال‌های اختلال مختلف و به‌منظور بررسی اثر افزودن نویز مصنوعی به محیط ارتباط نشان می‌دهد.

1. Cell Averaging Constant False Alarm Rate
2. False Alarm Probability

همان طور که ذکر گردید در شبیه‌سازی‌ها از کد بارکر با طول ۱۳، بهره پردازش ۱۱ dB و نسبت $JSR=5\,\text{dB}$ استفاده گردیده است و مدولاسیون مورد استفاده برای سیگنال ارسالی را نیز QPSK در نظر می‌گیریم. در این صورت با توجه به ارسال اختلال روی کانال ارتباطی، سطح آستانه آشکارساز شنودگر باید افزایش پیدا کند؛ در غیر این صورت شنودگر درگیر نرخ بالای احتمال هشدار کاذب (P_{Fa}) ناشی از اختلال می‌شود و هرچه توان اختلال بیشتر باشد منجر به افزایش بیشتر آستانه آشکارسازی شنودگر خواهد شد و در نتیجه، سیگنال فرستنده با حاشیه اطمینان بیشتری ارسال می‌گردد. بر این اساس شکل ۶ متوسط توان دریافتی از محیط توسط شنودگر را در حضور سیگنال‌های اختلال مختلف و به‌ازای $JSR=5\,\text{dB}$ نشان می‌دهد.

مطابق شکل با توجه به اینکه در روش پیشنهادی، ارسال سیگنال را در حالت طیف گسترده در نظر گرفتیم و با توجه به ایجاد حاشیه اطمینان برای سیگنال ارسالی توسط نویز مصنوعی کمکی، می‌توان از اختلال‌های با سطح توان متوسط پایین‌تری نسبت به [۶]، [۲۴] و [۲۵] استفاده نمود. در نتیجه، این پایین‌بودن سطح اختلال، ارسال دائم آن را با هزینه و مصرف توان پایین ممکن می‌کند و باعث افزایش ظرفیت مخابره پنهان به‌صورت LPD خواهد شد. همچنین در مقایسه با [۸] که از ترکیب نویز مصنوعی با ارسال سیگنال به‌صورت رگباری استفاده کرده است، مشاهده می‌شود اولاً روش پیشنهادی، امکان ارسال نویز مصنوعی با سطح توان پایین را فراهم نموده که پاسخی به یکی از چالش‌های مهم مخابرات پنهان است و ثانیاً در روش ارائه‌شده [۸]، ارسال پیوسته داده امکان‌پذیر نبوده و داده با تأخیر زمانی و ظرفیت پایین‌تری ارسال می‌شود که روش پیشنهادی، این دو مشکل را نیز مرتفع نموده است. سطح آستانه آشکارساز شنودگر و حاشیه اطمینان ایجادشده توسط نویز مصنوعی برای هر کدام از تکنیک‌های اختلال، مطرح و به‌ازای نسبت‌های مختلف JSR در جدول ۲ محاسبه و ارائه شده است. مطابق نتایج عددی جدول مشاهده می‌شود سطح آستانه شنودگر و در نتیجه حاشیه اطمینان مخابره پنهان با کاهش نسبت اختلال به سیگنال کاهش می‌یابد. به عبارت دیگر هرچه نسبت نویز مصنوعی به سیگنال بالاتر باشد، شنودگر در تشخیص ارتباط مشکل بیشتری خواهد داشت و کیفیت مخابره پنهان افزایش می‌یابد. همچنین با توجه به گسترش طیف سیگنال ارسالی در هزینه و مصرف توان نویز مصنوعی صرفه‌جویی شده و می‌توان با ارسال دائم نویز مصنوعی با توان پایین، ظرفیت مخابره پنهان را نیز افزایش داد.



شکل ۵: چگالی طیف توان سیگنال ارسالی در حضور انواع اختلال $JSR = ۵\,\text{dB}$، (الف) اختلال تک‌آهنگ، (ب) اختلال چندآهنگ، (ج) اختلال جاروب خطی، (د) اختلال نویز باند جزئی و (ه) اختلال مدولاسیون فرکانسی.

جدول ۲: سطح آستانه شنودگر و حاشیه اطمینان مخابره پنهان.

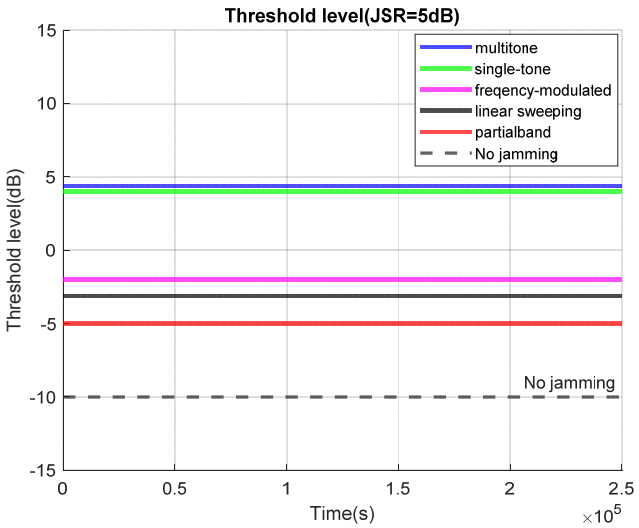
JSR	۱۰ dB		۵ dB		۰ dB		−۵ dB	
نوع اختلال	سطح آستانه شنودگر	حاشیه اطمینان ارسال	سطح آستانه شنودگر	حاشیه اطمینان ارسال	سطح آستانه شنودگر	حاشیه اطمینان ارسال	سطح آستانه شنودگر	حاشیه اطمینان ارسال
تک‌آهنگ	۱۴٫۱ dB	۲۵٫۱ dB	۴ dB	۱۵ dB	−۴٫۱ dB	۶٫۹ dB	−۸٫۴ dB	۲٫۶ dB
چندآهنگ	۱۷٫۵ dB	۲۸٫۵ dB	۴٫۱ dB	۱۵٫۱ dB	−۳٫۵ dB	۷٫۵ dB	−۸٫۴ dB	۲٫۶ dB
جاروب خطی	۳٫۸ dB	۱۴٫۸ dB	−۳٫۱ dB	۷٫۹ dB	−۸٫۸ dB	۲٫۲ dB	−۹٫۲ dB	۱٫۸ dB
نویزی باند جزئی	۰٫۵ dB	۱۱٫۵ dB	−۵ dB	۶ dB	−۹٫۴ dB	۱٫۶ dB	−۹٫۲ dB	۱٫۸ dB
مدولاسیون فرکانسی	۶٫۸ dB	۱۷٫۸ dB	−۲ dB	۹ dB	−۷٫۷ dB	۳٫۳ dB	−۹٫۱ dB	۱٫۹ dB

از سوی دیگر، اگرچه شکل ۶ و جدول ۲ امکان مخابره پنهان LPD با حاشیه اطمینان کافی در شنودگر را نشان می‌دهند، باید موفقیت مخابره را از دیدگاه فرستنده و گیرنده نیز مورد توجه قرار دهیم. شکل ۷ نمودار نرخ خطای بیت (BER) را نسبت به انرژی بیت بر نویز محیط (E_b/N) در حضور انواع نویز مصنوعی نشان می‌دهد. در این شکل نیز از مدولاسیون QPSK، کد بارکر با طول ۱۳ و در نتیجه بهره پردازش ۱۱ dB و نسبت $JSR = -۵\,\text{dB}$ به‌منظور داشتن کمترین هزینه ایجاد اختلال و بالابردن ظرفیت مخابره پنهان برای فرستنده استفاده شده است. مطابق شکل مشاهده می‌شود با فرض احتمال خطای مطلوب بین فرستنده و گیرنده معادل $۱۰^{-۳}$، غیر از اختلال چندآهنگ، سایر اختلال‌ها امکان برقراری مخابره موفق را برای $E_b/N > ۸٫۳\,\text{dB}$ در اختیار قرار می‌دهند.

به عبارت دیگر و بر اساس جدول ۲، اختلال چندآهنگ حاشیه اطمینان خوبی را برای مخابره پنهان از دید شنودگر ایجاد می‌کند؛ ولی امکان مخابره با احتمال خطای قابل قبول را نیز از فرستنده و گیرنده خواهد گرفت. البته در فعالیت‌های آتی می‌توان تأثیر انواع مختلف کد طیف گسترده و طول‌های (بهره پردازش) مختلف کد را نیز بر کیفیت و ظرفیت مخابره پنهان ترکیبی با استفاده از روش طیف گسترده و اختلال کمک‌کننده به‌صورت تحلیلی، شبیه‌سازی و عددی بررسی نمود. همچنین تحلیل اثر نسبت JSR بر کیفیت شنود و مخابره و هزینه توان تحمیلی آن بر شنودگر نیز قابل بررسی خواهند بود.

۷- جمع‌بندی

در این مقاله به‌منظور بهبود کیفیت و ظرفیت مخابرات پنهان، استفاده توأم از تکنیک طیف گسترده DS-SS به همراه نویز مصنوعی را پیشنهاد دادیم. پیش از این استفاده از نویز مصنوعی در مخابرات پنهان و استفاده از طیف گسترده در مقابل اختلال غیرخودی در مخابرات تجاری و نظامی



شکل ۶: میانگین توان دریافتی شنودگر.

جدول ۳: نتایج روش پیشنهادی ($JSR=-5\,\mathrm{dB}$).

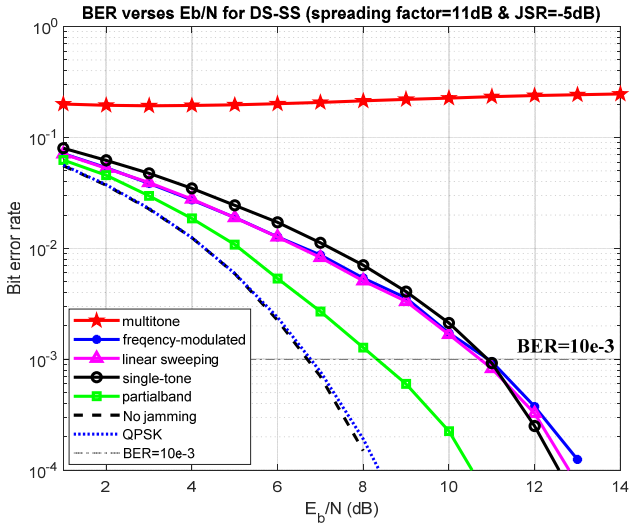
نوع اختلال	سطح آستانه شنودگر	حاشیه اطمینان ارسال	$E_b/N@(BER<10^{-3})$
تک‌آهنگ	−۸٫۴ dB	۲٫۶ dB	۱۰٫۹ dB
چندآهنگ	−۸٫۴ dB	۲٫۶ dB	غیرقابل قبول
جاروب خطی	−۹٫۲ dB	۱٫۸ dB	۱۰٫۷ dB
باند جزئی	−۹٫۲ dB	۱٫۸ dB	۸٫۳ dB
مدولاسیون فرکانسی	−۹٫۱ dB	۱٫۹ dB	۱۰٫۹۱ dB

رایج بوده‌اند؛ اما ایده استفاده از ترکیب نویز مصنوعی با طیف گسترده و هر دو توسط فرستنده خودی در این مقاله پیشنهاد و موفقیت‌آمیزبودن ایده به کمک شبیه‌سازی و تحلیل عددی نتایج، بررسی شده و حالات مناسب آن تعیین گردید.

روش طیف گسترده دنباله مستقیم با گسترش طیف سیگنال فرستنده و مخفی‌نمودن آن در زیر سطح نویز محیط، ارتباط را در برابر شنودگر مقاوم می‌کند. همچنین نویز مصنوعی حتی با سطح توان و هزینه پایین، حاشیه اطمینان خوبی برای عدم شناسایی سیگنال توسط شنودگر ایجاد می‌کند؛ ضمن اینکه امکان ایجاد اختلال در بازه وسیع زمانی یا فرکانسی بدون نیاز به همزمانی قطع و وصل با فرستنده فراهم خواهد شد. با توجه به آنکه در طرح پیشنهادی از اختلال کم‌توان پیوسته به‌عنوان نویز مصنوعی خودی استفاده شد، هزینه یافتن کد برای شنودگر نیز بسیار بیشتر از حالت طیف گسترده خواهد بود. به عبارت دیگر حتی در صورت تشخیص وجود نویز مصنوعی، شنودگر باید در شرایط کانال با اختلال ناشناخته که گیرنده را اشباع نموده است، فضای کدهای محتمل و محاسبات همبستگی آنها را دنبال کند که پیچیدگی محاسباتی زیادی را به او تحمیل خواهد کرد. همچنین در کارهای آتی می‌توان اثر استفاده از انواع کدهای خطی (کدهای گولد[1]، کازامی[2]، والش[3] و ...) و کدهای غیرخطی را برای افزایش بیش از پیش پیچیدگی برای شنودگر بررسی نمود.

نهایتاً نتایج شبیه‌سازی و تحلیل عددی مطابق جداول ۲ و ۳ نشان می‌دهد که در شرایط $JSR=-5\,\mathrm{dB}$، استفاده از نویز مصنوعی بر اساس

1. Gold Codes
2. Kasami Codes
3. Walsh Codes



شکل ۷: منحنی BER برحسب E_b/N به‌ازای اختلال‌های مختلف ($JSR=-5\,\mathrm{dB}$).

اختلال باند جزئی، ضمن ایجاد حاشیه اطمینان ۱٫۸ dB برای فریب شنودگر، بهترین کیفیت مخابره را بین فرستنده و گیرنده فراهم نموده و برای $E_b/N>8.3\,\mathrm{dB}$ احتمال خطای مناسب 10^{-3} را در شرایط شبیه‌سازی نتیجه خواهد داد. از سوی دیگر اختلال تک‌آهنگ با ایجاد ۲٫۶ dB حاشیه اطمینان، همین احتمال خطا را برای $E_b/N>10.9\,\mathrm{dB}$ بین فرستنده و گیرنده ایجاد خواهد کرد. سایر انواع اختلال غیر از اختلال چندآهنگ نیز با حاشیه‌های اطمینان مطابق جدول ۳ قابل استفاده هستند.

به‌منظور تکمیل پژوهش انجام‌شده در فعالیت‌های آتی می‌توان موارد زیر را برای روش پیشنهادی مورد بررسی قرار داد:

الف) مقایسه هزینه و مصرف توان استفاده از انواع مختلف اختلال در ازای کیفیت و ظرفیت مخابره پنهان برقرارشده و تعیین نقطه مناسب مصالحه

ب) بررسی اثر انواع مختلف کدهای خطی و غیرخطی طیف گسترده با طول‌های مختلف بر کیفیت مخابره پنهان حاصل

مراجع

[1] S. Vaudenay, A Classical Introduction to Cryptography: Applications for Communications Security, Springer Science & Business Media, 2006.

[2] F. Y. Shih, Digital Watermarking and Steganography: Fundamentals and Techniques, CRC Press, 2017.

[3] R. L. Peterson, D. E. Borth, and R. E. Ziemer, *An Introduction to Spread-Spectrum Communications*, Prentice-Hall Inc, 1995.

[4] M. K. Simon, et al., Spread Spectrum Communications Handbook, vol. 2, Citeseer, 1994.

[5] A. S. Biswas, *et al.*, "Orthogonal coded spread spectrum digital beamforming-based 5G receiver," *Arabian J. for Science and Engineering*, vol. 48, pp. 5757-5769, 2023.

[6] H. Jung, *et al.*, "Design of anti-jamming waveforms for time-hopping spread spectrum systems in tone jamming environments," *IEEE Trans. on Vehicular Technology*, vol. 69, no. 1, pp. 728-737, Jan. 2019.

[7] C. U. Baek, J. W. Jung, and D. W. Do, "Study on the structure of an efficient receiver for covert underwater communication using direct sequence spread spectrum," *Applied Sciences*, vol. 8, no. 1, Article ID: 58, 2018.

[8] W. He, *et al.*, "Optimal transmission probabilities of information and artificial noise in covert communications," *IEEE Communications Letters*, vol. 26, no. 12, pp. 2865-2869, Dec. 2022.

[9] G. J. Simmons, "The prisoners' problem and the subliminal channel," in D. Chaum (ed.), *Advances in Cryptology, Proc. of Crypto*, pp. 51-52, New York: Plenum Press, 1984.

[10] W. Mazurczyk and L. Caviglione, "Steganography in modern smartphones and mitigation techniques," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 1, pp. 334-357, First Quarter 2014.

[11] S. Lee, R. J. Baxley, M. A. Weitnauer and B. Walkenhorst, "Achieving undetectable communication," *IEEE J. of Selected Topics in Signal Processing*, vol. 7, no. 9, pp. 1195-1205, Oct. 2015.
[12] P. N. Safier, I. S. Moskowitz, and P. Cotae, "On the baseband communication performance of physical layer steganography," in *Proc. 45th IEEE Annual Conf. on Information Sciences and Systems*, 6 pp., Baltimore, MD, USA, 23-25 Mar. 2011.
[13] B. A. Bash, D. Goeckel, and D. Towsley, "Limits of reliable communication with low probability of detection on AWGN channels," *IEEE J. on Selected Areas in Communications*, vol. 31, no. 9, pp. 1921-1930, Sept. 2013.
[14] D. Goeckel, *et al.*, "Artificial noise generation from cooperative relays for everlasting secrecy in two-hop wireless networks," *IEEE J. on Selected Areas in Communications*, vol. 29, no. 10, pp. 2067-2076, Dec. 2011.
[15] B. He, *et al.*, "On covert communication with noise uncertainty," *IEEE Communications Letters*, vol. 21, no. 4, pp. 941-944, Apr. 2017.
[16] H. Q. Ta and S. W. Kim, "Covert communication under channel uncertainty and noise uncertainty," in *Proc. IEEE Int. Conf. on Communications, ICC'19*, 6 pp., Shanghai, China, 20-24 May 2019.
[17] S. Sodagari, "Covert communications against an adversary with low-SNR sensing capability in nakagami fading," *IEEE Sensors Letters*, vol. 4, no. 5, pp. 2475-1472, May. 2020.
[18] K. Li, P. A. Kelly, and D. Goeckel, "Optimal power adaptation in covert communication with an uninformed jammer," *IEEE Trans. on Wireless Communications*, vol. 19, no. 5, pp. 3463-3473, May 2020.
[19] T. X. Zheng, *et al.*, "Wireless covert communications aided by distributed cooperative jamming over slow fading channels," *IEEE Trans. on Wireless Communications*, vol. 20, no. 11, pp. 7026-7039, Nov. 2021.
[20] K. W. Huang, H. Deng, and H. M. Wang, "Jamming aided covert communication with multiple receivers," *IEEE Trans. on Wireless Communications*, vol. 20, no. 7, pp. 4480-4494, Jul. 2021.
[21] T. X. Zheng, H. –M. Wang, D. W. K. Ng, and J. Yuan, "Multi-antenna covert communications in random wireless networks," *IEEE Trans. on Wireless Communications*, vol. 18, no. 3, pp. 1974 - 1987, Mar. 2019.
[22] X. Chen, *et al.*, "Multi-antenna covert communication via full-duplex jamming against a warden with uncertain locations," *IEEE Trans. on Wireless Communications*, vol. 20, no. 8, pp. 5467-5480, Aug. 2021.
[23] O. Shmuel, A. Cohen, and O. Gurewitz, "Multi-antenna jamming in covert communication," *IEEE Trans. on Communications*, vol. 69, no. 7, pp. 4644-4658, Jul. 2021.
[24] W. Xiong, Y. Yao, X. Fu, and S. Li, "Covert communication with cognitive jammer," *IEEE Wireless Communications Letters*, vol. 9, no. 10, pp. 1753-1757, Oct. 2020.
[25] H. Choi, S. Park, and H. N. Lee, *Covert Anti-Jamming Communication Based on Gaussian Coded Modulation*, Applied Sciences, 2021.
[26] T. Arbi, B. Geller, and O. P. Pasquero, "Direct-sequence spread spectrum with signal space diversity for high resistance to jamming," in *Proc. IEEE Military Communications Conf., MILCOM'21*, pp. 670-676, San Diego, CA, USA, 29 Nov.-2 Dec. 2021.
[27] S. N. Kirillov and A. A. Lisnichuk, "The procedure of multi-criteria synthesis of DSSS radio signals to adapt prospective wireless communication systems to the action of narrowband interference," in *Proc. IEEE Moscow Workshop on Electronic and Networking Technologies, MWENT'20*, 5 pp., Moscow, Russia, 11-13 Mar. 2020.
[28] F. G. A. K. Bawahab, *et al.*, "Performance evaluation and mathematical analysis of direct sequence and frequency hopping spread spectrum systems under wideband interference," *International J. of Advances in Intelligent Informatics*, vol. 4, no. 3, pp. 180-191, Nov. 2018.
[29] R. C. Dixon, *Spread Spectrum Systems: with Commercial Applications*, John Wiley, 1994.
[30] B. P. Lathi, *Modern Digital and Analog Communication Systems*, Oxford University Press Inc, 1990.
[31] K. Grover, A. Lim, and Q. Yang, "Jamming and anti-jamming techniques in wireless networks: a survey," *International J. of Ad Hoc and Ubiquitous Computing*, vol. 17, no. 4, pp. 197-215, Dec. 2014.
[32] Y. Wang, *et al.*, "Complicated interference identification via machine learning methods," in *Proc. 4th IEEE Int. Conf. on Electronic Information and Communication Technology, ICEICT'21*, pp. 400-405, Xi'an, China, 15-20 Aug. 2021.
[33] L. Milstein, S. Davidovici, and D. Schilling, "The effect of multiple-tone interfering signals on a direct sequence spread spectrum communication system," *IEEE Trans. on Communications*, vol. 30, no. 3, pp. 436 - 446, Mar. 1982.
[34] J. J. Liang, L. D. Jeng, and C. H. Wang, "A new partial-band noise jamming model for frequency-hopped MFSK systems," in *Proc. 2nd IEEE Int. Symp. on Wireless Communication Systems*, pp. 200-204, Siena, Italy, 5-7 Sept. 2005.
[35] J. Granlund, *Interference in Frequency-Modulation Reception*, 1949.
[36] J. Mikulka and S. Hanus, "CCK and barker coding implementation in IEEE 802.11b Standard," in *Proc. 17th IEEE Int. Conf. on Radioelektronika*, 4 pp., Brno, Czech Republic, 24-27 Apr. 2007.
[37] H. Finn and R. Johnson, "Adaptive detection mode with threshold control as a function of spatially sampled clutter-level estimates," *RCA Rev.*, vol. 29, no. 4, pp. 414-464, 1968.

مرتضی شفیعی استادیار مجتمع دانشگاهی برق و کامپیوتر، دانشگاه صنعتی مالک اشتر (MUT)، تهران، ایران است. او دکترای مهندسی برق را در سال ۱۳۹۷ از دانشکده مهندسی برق، دانشگاه علم و صنعت ایران (IUST)، تهران، ایران دریافت کرد. علایق تحقیقاتی او مخابرات طیف گسترده، مخابرات ماهواره‌ای، شبکه‌های حسگر بی‌سیم (WSNs)، پردازش ابری، سنجش طیف و رادیوی شناختی (CR)، پیاده سازی رادیوی نرم‌افزاری، مخابرات پنهان (CC) و شبکه‌های مخابرات زیرآب بوده است.

ایمان کاظمی تحصیلات خود را در مقاطع کارشناسی و کارشناسی ارشد مهندسی برق به‌ترتیب در سال‌های ۱۳۸۹ و ۱۳۹۲ از دانشگاه آزاد اسلامی یادگار امام خمینی (ره) به پایان رسانده است. او هم‌اکنون دانشجوی دکتری دانشگاه صنعتی مالک اشتر در رشته مهندسی برق مخابرات سیستم می‌باشد. زمینه‌های تحقیقاتی مورد علاقه او عبارتند از: مخابرات پنهان (CC)، مخابرات ماهواره‌ای، پردازش سیگنال، پردازش تصویر دیجیتال، پردازش تصاویر ابرتفکیکی و فراتفکیک‌پذیری (Super/Hyper Resolution) می‌باشد.