Journal of Electronical & Cyber Defence
Vol. 10, No. 1, Spring 2022, Serial No. 37

Improving security of wireless telecommunication networks based on covert communication in presence of a controlled noise using multiple beamforming

F. Samsami Khodadad*, F. Azarang, M. Forouzesh, S. M. J. Asgari Tabatabaee

Assistant Professor, Amol Specialized University of New Technologies, Amol, Iran*

(Received: 16/03/2021, Accepted: 18/01/2022)

ABSTRACT

In Wireless Telecommunication, maintaining the security and the transmitted bit rate are very important. However, in conventional networks, covert communication is often the transmitted bit rate very limited. This may be for maintaining the security in covert communication in the sense that the data signal must be covert inside the base noise. In this article, we present different plans to maintaining the security and increase the transmitted bit rate in covert communication. The basis of the proposed method is transmitting controlled noise signal to increase the probability of detection error in the eavesdropper and increase the covert rate in the legal receiver to send the main message to the legal receiver. In the proposed method, also, the beam forming technique is presented and applied to increase the covert rate and reduce the interference in the receiver. To evaluate this scheme, an optimization problem is formulated. Various simulations and numerical results proves the efficiency of our proposal in its ability to increase security in telecommunications networks based on covert communication via controlled noise

.**Keywords:** Physical layer security, Covert communication, controlled noise

*Corresponding Author Email: samsami.farid@gmail.com

نشریه علمی "پدافند الکترونیکی و سایبری"
سال دهم، شماره ۱، بهار ۱۴۰۱، ص ۱۹- ۱۱

علمی- پژوهشی

بهبود امنیت یک ارتباط بی‌سیم مبتنی بر مخابره‌ی پنهان در حضور نویز کنترل شده با استفاده از پرتو چندگانه

فرید صمصامی خداداد[1*]، سیده فاطمه آذرنگ[2]، مسلم فروزش[3]، سید محمد جواد عسگری طباطبائی[4]

۱- استادیار، دانشکده‌ی مهندسی فناوری‌های نوین، دانشگاه تخصصی فناوری‌های نوین آمل، آمل، ۲- دانشجوی کارشناسی ارشد، دانشکده‌ی مهندسی فناوری‌های نوین، دانشگاه تخصصی فناوری‌های نوین آمل، آمل، ۳- دکتری، دانشگاه تربیت مدرس، تهران، ٤- استادیار، دانشگاه تربت حیدریه، تربت حیدریه، ایران

(دریافت: ۱۳۹۹/۱۲/۲٦، پذیرش: ۱٤۰۰/۱۲/۲۲)

چکیده

در ارتباطات بی سیم حفظ امنیت و نرخ بیت ارسالی بسیار حائز اهمیت می‌باشد. با این حال در شبکه‌های متداول، مخابره پنهان اغلب دارای نرخ بیت محدود است؛ چراکه به دلیل حفظ امنیت در مخابره پنهان، باید سیگنال داده را درون نویز پایه‌ای مخفی نمود. در این مقاله، به ارائه طرحی به منظور حفظ امنیت و افزایش نرخ بیت در مخابره پنهان پرداخته شده است. اساس روش پیشنهادی، ارسال نویز کنترل شونده برای افزایش احتمال خطای تشخیص در شنودگر و افزایش نرخ پنهان در گیرنده‌ی مجاز است. در طرح پیشنهاد شده از روش شکل‌دهی پرتو برای افزایش نرخ پنهان و کاهش تداخل در گیرنده مجاز بهره گرفته شده است. در نهایت برای ارزیابی این طرح، یک مسئله بهینه‌سازی فرمول‌بندی می‌شود و یک الگوریتم تکراری برای حل آن ارائه داده می‌شود. شبیه‌سازی و نتایج عددی متنوع صحت ادعا را در توانایی روش ارائه شده در امنیت شبکه‌های مخابراتی بی‌سیم مبتنی بر مخابره پنهان با استفاده از پارازیت‌سازی را نشان می‌دهند.

کلیدواژه‌ها: امنیت لایه‌ی فیزیکی، مخابره پنهان، برداشت انرژی

۱- مقدمه

صنعت مخابرات بی‌سیم در چند دهه اخیر پیشرفت های چشمگیری داشته است، به گونه‌ای که امروزه نسبت به مخابرات سیمی بیشتر مورد استفاده قرار می‌گیرد. اما به دلیل اینکه سیگنال در فضای آزاد منتشر می‌شود، سیگنالی که توسط فرستنده به گیرنده اصلی ارسال می‌شود توسط گیرنده‌های اطراف از جمله گیرنده‌های غیر مجاز و شنودگران قابل دریافت خواهد بود به همین دلیل تامین امنیت در مخابره بی سیم بسیار ضروری خواهد بود. برای برقراری امنیت در مخابره بی‌سیم مطالعات فراوانی انجام شده است و روش‌های مختلفی برای ارسال امن در شبکه‌های مخابره بی‌سیم مورد بحث و بررسی قرار گرفته است. یکی از روش‌های برقراری امنیت استفاده از الگوریتم رمزنگاری می‌باشدکه براساس محاسبات و پردازش صورت می‌گیرد.

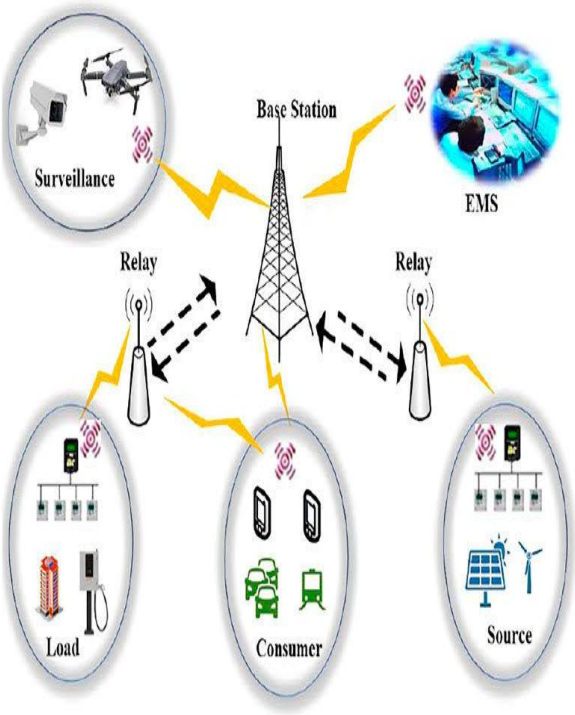
یکی دیگر از روش های برقراری امنیت، امنیت در لایه فیزیکی است که براساس نظریه تئوری اطلاعات می‌باشد. در روش‌های امنیت گفته شده هدف آن می‌باشد که از دسترسی شنودگر به محتوای پیام جلوگیری شود. روش دیگری برای برقراری امنیت وجود دارد که توسط آن می توان مخابره ای که بین فرستنده و گیرنده صورت می گیرد را از دید یک شنودگر پنهان کرد، که مخابره پنهان نام دارد. در این مقاله به مطالعه روش‌های امنیت در شبکه های مخابراتی بی‌سیم می‌پردازیم و با مفهوم مخابره پنهان آشنا می‌شویم.

در نهایت با توجه به اینکه حجم زیادی از اطلاعات مهم و محرمانه از طریق شبکه‌های بی‌سیم جابه‌جا می‌شود، امنیت موضوعی مهم در ارتباطات بی‌سیم است شکل (۱).

از آن جا که این شبکه ها در دنیای کنونی هرچه بیشتر در حال گسترش هستند، و با توجه به ماهیت این دسته از شبکه ها که براساس سیگنال های رادیویی اند، مهم ترین نکته در راه استفاده از این تکنولوژی، آگاهی از نکات قوت و ضعف آن است. نظر به لزوم آگاهی از خطرات استفاده از این شبکه ها، با وجود امکانات نهفته در آن ها که به مدد پیکربندی صحیح می توان به سطح قابل قبولی از بعد امنیتی دست یافت. در اینجا تحت عنوان " امنیت در شبکه های بی سیم" ، به روش های پیکربندی صحیح که احتمال رخ داد حملات را کاهش می‌دهند بپردازیم.

* رایانامه نویسنده مسئول: Samsami@ausmt.ac.ir

ناشر: دانشگاه جامع امام حسین (ع)



شکل (۱): مدل جامعی از یک شبکه بی سیم

۱-۱- روش های مخابره امن

برای برقراری امنیت در مخابره بی‌سیم مطالعات فراوانی انجام شده است و روش‌های مختلفی برای ارسال امن در شبکه‌های مخابره بی‌سیم مورد بحث و بررسی قرار گرفته است. که هدف اصلی این مقاله می باشد.

۱-۱-۱- رمزنگاری

یکی از روش‌های ارسال امن روش رمزنگاری می‌باشد در این روش فرستنده و گیرنده بر یک الگوریتم خاص توافق می‌کنند و گیرنده اصلی با داشتن الگوریتم به راحتی می‌تواند پیام را تفسیر کند. برای مثال در رمزنگاری کلید متقارن یک کلید در فرستنده و گیرنده برای رمز کردن به اشتراک گذاشته می‌شود که عملیات رمزنگاری و رمزگشایی براساس این کلید انجام می‌شود. فرستنده با استفاده از الگوریتم رمزنگاری و کلید متقارن موجود، شروع به رمزنگاری پیام می‌کند، تنها فرستنده و گیرنده مجاز می‌توانند از کلید استفاده کنند. وقتی گیرنده مجاز سیگنال را دریافت می‌کند آن را توسط کلید موجود رمزگشایی می‌کند. ولی شنودگر به دلیل نداشتن کلید توانایی رمزگشایی پیام را ندارد و یک پیام نامفهوم یا متفاوت از پیام اصلی دریافت خواهد کرد. همان‌طور که می‌بینید این روش به طور کامل محرمانه نمی‌باشد چون اگر شنودگر به کلید دستیابی داشته باشد می‌تواند پیام محرمانه را رمزگشایی کند. این روش به دلیل موضوعاتی از قبیل توزیع و مدیریت کلیدها (برای رمزنگاری متقارن) و پیچیدگی زیاد محاسبات (برای رمزنگاری نامتقارن) برای شبکه¬های بزرگ مناسب نخواهد بود [۱].

۱-۱-۲- ارسال امن در لایه فیزیکی

امروزه روش های زیادی برای ارسال امن در شبکه‌های مخابراتی بی‌سیم مبتنی بر پردازش سیگنال و کدینگ در لایه فیزیکی مورد بحث و بررسی قرار گرفته است. یکی از روش های ارسال امن در لایه فیزیکی، ارسال امن طیف گسترده می‌باشد. در این روش هر گیرنده کد مخصوص به خود را دارد و با استفاده از این کد اختصاصی سیگنال خود را آشکارسازی می‌کند ولی گیرنده های غیر مجاز به دلیل اینکه از کد مربوطه اطلاعی ندارند توانایی آشکارسازی سیگنال دریافتی را نخواهند داشت. ارسال امن تئوری اطلاعاتی یکی دیگر از روش های برقراری امنیت در لایه فیزیکی می‌باشد. اساس کار در این روش کاهش احتمال آشکارسازی در ،گیرنده غیرمجاز یا شنودگر و افزایش احتمال آشکارسازی در گیرنده مجاز می‌باشد. این روش‌ها مبتنی بر فنون پردازش سیگنال و کدینگ می‌باشد و هیچگونه محدودیتی از قبیل توانایی محاسباتی و یا داشتن کلید و کد درنظر گرفته نمی-شود [۲].

۱-۱-۳- مخابره پنهان

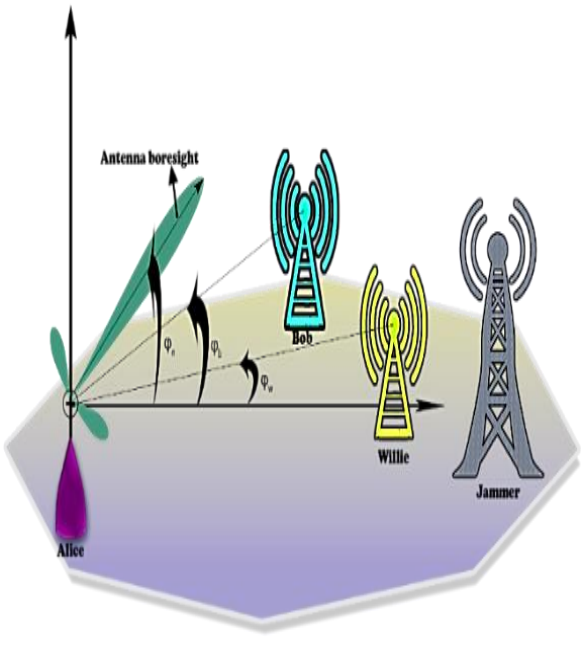
در روش‌های گفته شده هدف آن است که از دسترسی شنودگر به محتوای پیام جلوگیری شود، یعنی گیرنده سیگنال را دریافت می‌کند ولی توانایی آشکارسازی آن را ندارد. اما در عین حال شرایطی وجود دارد که نیاز است ارتباط بین فرستنده و گیرنده به صورت پنهان صورت گیرد درواقع، پنهان کردن وجود مخابره بین فرستنده و گیرنده از دید یک گیرنده غیرمجاز هدف می‌باشد. این نوع مخابره را می‌توان در مخابرات نظامی که لازم است ارسال داده از دید شنودگران پنهان شود، استفاده کرد.ارتباطات بی‌سیم به‌خاطر ماهیت پخشی بودن، ذاتاً عمومی و آشکار هستند که برای حفظ امنیت نامطلوب است؛ زیرا به هر فرستنده‌ی تأییدنشده‌ای اجازه شناسایی یا استراق‌سمع در ارتباطات بی‌سیم را می‌دهند. در[۳,۴] به‌منظور حفظ امنیت در شبکه‌های بی‌سیم، روش‌های زیادی مطرح شده است که در این روش‌ها بیشتر هدف، حفظ محتوای پیام از دید شنودگر بوده است. درصورتی‌که در بعضی از موارد حفاظت از محتوای پیام کافی نیست؛ بلکه هدف، پنهان کردن مخابره بین فرستنده و گیرنده از دید شنودگر است. برای رفع این مشکل، مخابره‌ی پنهان با هدف پنهان کردن مخابره بین فرستنده و گیرنده از دید

یک شنودگر مطرح می‌شود. نتایج در [۵] نشان می‌دهد که امنیت لایه‌های فیزیکی[1] با بهره‌گیری از خصوصیات فیزیکی محیط بی‌سیم به برقراری ارتباط ایمن کمک می‌کند. در [۳] دو مورد متداول DF[2] و AF[3]، به‌منظور تقویت امنیت لایه‌های فیزیکی مورد مطالعه قرار می‌گیرد. تأثیرات ارتباط پنهان بر روی یک کانال AWGN[4] در [۶, ۷] بررسی شده است.

در [۸] به ارائه‌ی روشی پرداخته می‌شود که در آن یک سیگنال پارازیت در فرستنده قرار دارد و به آن این امکان را می‌دهد تا نرخ بیت بیشتری را درحالی‌که پنهان است، ارسال کند. ارتباطات پنهان در زمینه‌ی شبکه‌های رله در [۹]، مورد بررسی قرار گرفته است که نشان می‌دهد رله می‌تواند اطلاعات محرمانه را بدون انتقال اطلاعات منبع به مقصد به‌صورت پنهان منتقل کند(شکل (۴)). طرح‌های TS[5] و PS[6] را در رله‌ی خودپایدار برای برداشت انرژی در نظر گرفته و محدودیت عملکرد شناسایی فرستنده (آلیس) را بررسی کرده است [۱۰]. تحلیل‌های [۱۰] همچنین نشان می‌دهد که حداقل بازده تبدیل انرژی مورد نیاز تحت $\mathcal{H}_1$ که همان η_1^* است، برای رسیدن به این Ψ^* در طرح‌های TS و PS برابر است که نشان می‌دهد هزینه‌ی دستیابی به محدودیت‌های ارتباطات پنهان، رله یکسان است؛ گرچه Ψ^* قابل دسترسی می‌تواند متفاوت باشد. در سیستم‌های ارتباطی بی‌سیم کاربردی، معمولاً CSI از طریق بازخورد CSI[7] از گیرنده به فرستنده به دست می‌آید [۴]. پروتکل‌های EH [۷]، به‌عنوان مثال پروتکل‌های رله‌گذاری مبتنی بر سوئیچینگ زمانی[8] و پروتکل رله‌گذاری مبتنی بر تقسیم توان[9] به‌منظور دستیابی به سیستم‌های کارآمد از لحاظ انرژی مورد بررسی قرار می‌گیرد. در [۱۱] به مسئله‌ی ارتباط پنهان و انتقال ایمن در شبکه‌های رله نامعتبر ـزمانی که چندین شنودگر در شبکه وجود دارد- پرداخته است. تحلیل‌های [۱۱] همچنین نشان می‌دهد که با افزایش تعداد رله‌ها میزان نرخ پنهان قابل دست‌یابی افزایش می‌یابد. محدودیت‌ها و هزینه‌های مرتبط با اجرا شدن مخابره‌ی پنهان برای انتقال اطلاعات یک رله‌ی خودپایدار به مقصد در [۱۲] بررسی شده است.

در[۱۳] به بررسی ارتباط پنهان در شبکه‌های همیار NOMA پرداخته شده است. همچنین عملکرد ارتباط پنهان در شبکه‌های دسترسی چندگانه‌ی غیرمتعامد با رله‌ی تقویت و ارسال مورد مطالعه قرار می‌گیرد. علاوه‌براین، به تحلیل عملکرد ارتباط پنهان تحت کیفیت متفاوت خدمات (QOS) و الزامات احتمال خطای تشخیص پرداخته شده است. یک سیستم ارتباطی پنهان چند آنتنه تحت کانال‌های محوشدگی در [۱۴] ارائه شده است. نتایج [۸] نشان می‌دهد که اگر یک نویز کنترل شونده تک آنتنه ارسال گردد، نسبت سیگنال به نویز در گیرنده موردنظر کاهش می‌یابد. برای حل این مسئله، سیگنال‌های نویز کنترل شونده را به چندین آنتن مجهز می‌کنند. دراین صورت هم توان ارسالی افزایش می‌یابد و هم تداخل در گیرنده کاهش می‌یابد. همچنین به‌منظور افزایش نرخ بیت، فرستنده را به آرایه‌ای از آنتن مجهز کرده تا ارسال سیگنال داده به‌صورت شکل‌دهی دو بعدی به سمت گیرنده موردنظر انجام شود.

برای برقراری امنیت در مخابرات بی‌سیم مطالعات فراوانی انجام شده است و روش‌های مختلفی برای ارسال امن در شبکه‌های بی‌سیم مورد بحث و بررسی قرار گرفته است. روش‌های الگوریتم رمزنگاری [۱۵, ۱۶] و ارسال امن در لایه‌ی فیزیکی [۱۷-۱۹] را پیشنهاد داده‌اند که به‌منظور حفظ محتوای پیام از دید شنودگر عملکرد مناسبی دارد. با این وجود در روش‌های امنیت که بیان شد هدف آن است که از دسترسی شنودگر به محتوای پیام جلوگیری شود. این بدان معنا است که گیرنده سیگنال را دریافت می‌کند ولی توانایی آشکارسازی آن را ندارد.



شکل (۲): مدل سیستم

[1] Physical layer security
[2] Decod-and-forward
[3] Amplify -and-forward
[4] Additive white guassian noise
[5] Time switching
[6] Power splitting
[7] Channel State Information
[8] Time Switching Based Relaying
[9] Power Splitting Based Relaying

یطی وجود دارد که نیاز است ارسال بین فرستنده و گیرنده به‌صورت پنهان صورت گیرد، به‌عبارت‌دیگر پنهان کردن وجود مخابره بین فرستنده و گیرنده از دید یک شنودگر هدف است. در جهت رسیدن به این هدف روش دیگری را می‌توان در حوزه‌ی برقراری امنیت نام برد که مخابره‌ی پنهان است و هدف آن پنهان کردن مخابره بین فرستنده و گیرنده از دید یک شنودگر است [۷, ۲۳-۲۰].

۱-۲- ارتباطات پنهان توسط یک رله‌ی خود پایدار

۱-۲-۱- معرفی سیستم

در برخی از حالت‌های شبکه های ارتباطی بی‌سیم، به جای مخابره مستقیم به مقصد، یک گره منبع اطلاعات را با کمک یکی از گره‌های همسایه خود به عنوان رله مخابره می‌کند. ارتباطات پنهان در زمینه شبکه‌های رله در [۱۵] مورد بررسی قرار گرفت، که نشان داد رله می‌تواند اطلاعات محرمانه را بدون انتقال اطلاعات منبع به مقصد به صورت پنهانی منتقل کند. با دستگاه-های همه‌گیرشده‌ی اینترنت اشیاء[1] (به عنوان مثال برنامه‌های شهرهای هوشمند، سیستم‌های حمل و نقل هوشمند، دستگاه-های همراه) که در زندگی روزمره به کار می‌روند، حجم بی‌سابقه ای از اشیاء و دستگاه های متصل به هم وجود دارد که اطلاعات حساس و محرمانه‌ای مانند مکان واقعی و اطلاعات فیزیولوژیکی مرتبط به سلامتی را ذخیره و از طریق کانال‌های بی‌سیم تبادل می‌کنند. به همین ترتیب نگرانی‌های زیادی در مورد امنیت و حفظ حریم ارتباطات بی‌سیم در اینترنت اشیا پدیدار شده که گمان می‌رود بزرگترین مانع برای استقبال گسترده از اینترنت اشیا باشد. ارتباطات پنهان می‌تواند وجود مخابرات بی‌سیم را پنهان کند و از این رو قادر است در برنامه های بیشمار نوظهور IoT[2]، مشکلات حریم خصوصی را برطرف کند. در برخی از سناریوهای کاربردی IoT ، یک تکنیک امیدوارکننده به نام برداشت انرژی بی‌سیم و پردازش اطلاعات، فرصت‌های جدید و بسیار خوبی را برای حل مشکلات انرژی محدود ارائه می‌دهد [۱۶-۲۲]. با استفاده از این تکنیک، گره مبدا، انرژی را از طریق ارتباطات پنهان به رله فرستاده و سپس از رله درخواست می‌کند تا به ارسال اطلاعات به مقصد کمک نماید. انرژی و توان منابع ارزشمندی هستند و به همین خاطر گره‌ی مبدا اجازه نمی‌دهد که گره رله از قدرت برداشت شده برای مخابره اطلاعات دیگر بجای اطلاعات منبع به مقصد استفاده نماید. بدین گونه، مخابره اطلاعات خود رله باید از منبع پنهان بماند تا پنهان بودن مخابره تضمین شود. رله به ارسال اطلاعات خود در کنار ارسال اطلاعات پیام منبع به صورت پنهان می‌پردازد. این درحالی است که منبع تلاش می‌کند تا این مخابره پنهان را برای شناسایی استفاده غیرقانونی از منابع (توان حاصل از برداشت انرژی) که تنها برای ارسال اطلاعات منبع به مقصد اختصاص یافته است، شناسایی کند.

در این مقاله به منظور بررسی کارایی مخابره پنهان در شبکه‌های مخابرات بی‌سیم، راه‌حل‌هایی برای رسیدن به عملکرد بهینه ارائه می‌شود. راهکاری که در این طرح ارائه می‌شود، ارسال سیگنال نویز کنترل شونده همراه سیگنال پیام می‌باشد که در این صورت سیگنال پیام می‌تواند توسط سیگنال نویز کنترل شونده پنهان شود. این امر موجب می شود که بتوان سیگنال داده را با توان بیشتری ارسال کرد اما این موضوع تداخل را در گیرنده اصلی بالا می برد و برای حل این موضوع استفاده از روش شکل‌دهی پرتو ارائه می‌شود. در این روش سیگنال‌های نویز کنترل شونده و سیگنال‌های فرستنده را به چندین آنتن مجهز می‌کنیم. در این صورت فرستنده قادر به انجام شکل‌دهی دو بعدی سیگنال پیام به سمت گیرنده مورد نظر می‌باشد. ادامه مقاله به‌صورت زیر سازماندهی می‌شود: در بخش ۳، مدل سیستم ارائه می‌شود. در بخش ۴، مسئله بهینه سازی جهت ارزیابی طرح مطرح می‌شود و راه‌حل مسئله ارائه می‌شود. در بخش (۵)، سناریو و پارامترهای شبیه‌سازی ارائه می‌شوند و نتایج شبیه‌سازی توضیح داده شده و در نهایت بخش آخر شامل مقایسه و نتیجه‌گیری است.

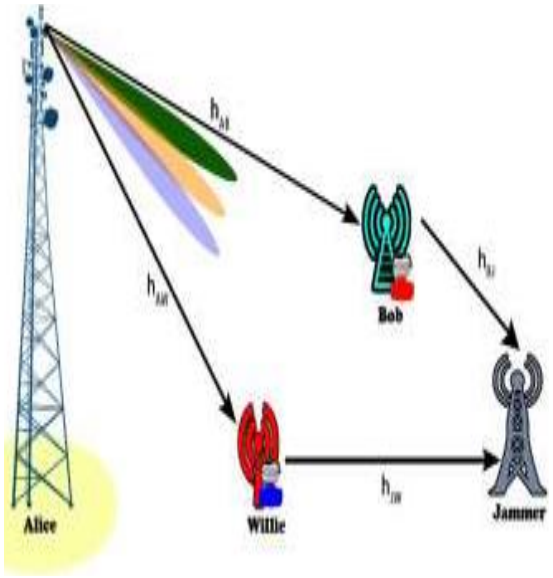
۲- علائم و اختصارات

در این مقاله فرستنده، گیرنده اصلی،گیرنده غیر خودی و نویز کنترل شونده را به ترتیب با حروف t، r، ch و n نمایش می‌دهیم.

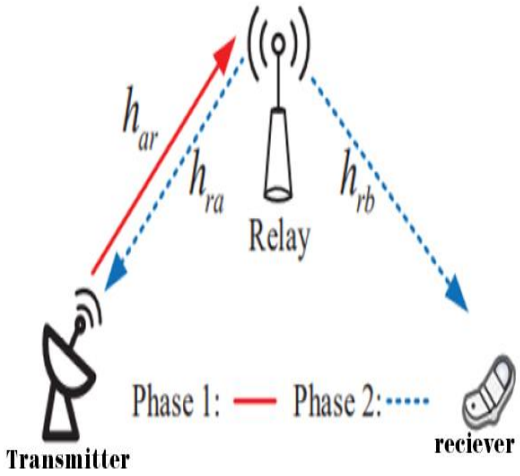
۳- مدل سیستم

مدل سیستم پیشنهادی مطابق شکل (2) می‌باشد که از یک فرستنده ، یک گیرنده غیرخودی، یک گیرنده اصلی و یک نویز کنترل شونده تشکیل می‌شود. فرض می‌کنیم که فرستنده به یک آرایه آنتن مجهز است که N_t نام دارد که می‌خواهد داده‌ها را بصورت پنهانی به گیرنده مورد نظر انتقال بدهد و با استفاده از پرتوهای دوبعدی این انتقال را انجام می‌دهد. همچنین فرض می‌شود که سیگنال نویز کنترل شونده یک چند آنتنی با آنتن-های N_n است. در این مدل گیرنده و سرپرست بصورت تک آنتنی درنظر گرفته می‌شوند.

[1] Internet of things
[2] Internet of Things



شکل (۳): مخابره ی پنهان با پرتو چندگانه



شکل (۴): مخابره‌ی پنهان توسط یک رله‌ی مجهز به آنتن

موقعیت مکانی گیرنده و سیگنال نویز کنترل شونده و گیرنده غیر خودی را می‌توان بصورت زیر بیان نمود:

$$(x_r, y_r, z_r)$$
$$(x_n, y_n, z_n) \qquad (۱)$$
$$(x_{ch}, y_{ch}, z_{ch})$$

ضریب کانال گاوسی از فرستنده تا گیرنده اصلی، فرستنده تا گیرنده غیرخودی، نویز کنترل شونده تا گیرنده اصلی و نویز کنترل شونده تا گیرنده غیرخودی برابر است با :

$$\mathrm{h}_{tr} \sim \mathcal{CN}\ (0_{\mathrm{N_t}\times 1}, \mathrm{C_{tr}})$$
$$\mathrm{h}_{\mathrm{tch}} \sim \mathcal{CN}\ (0_{\mathrm{N_t}\times 1}, \mathrm{C_{tch}}) \qquad (۲)$$
$$\mathrm{h}_{\mathrm{nr}} \sim \mathcal{CN}\ (0_{\mathrm{N_n}\times 1}, \mathrm{C_{nr}})$$
$$\mathrm{h}_{\mathrm{nch}} \sim \mathcal{CN}\ (0_{\mathrm{N_n}\times 1}, \mathrm{C_{nch}})$$

که C_{ij} ماتریس کواریانس کانال بین گره های i و j می‌باشد و 0 بیانگر ماتریس صفرمی‌باشد شکل (۳).

بردار سیگنال پیام فرستنده در هر اسلات زمانی را می‌تواند بصورت زیر بیان نمود:

$$S_t = [s_t^1, s_t^2, \dots, s_t^n] \qquad (۳)$$

که s_tبیانگر بردار سیگنال پیام می‌باشد.

سیگنال منتقل شده توسط فرستنده برابر هست با :

$$X_t^\ell = w_t s_t^\ell \qquad (۴)$$

که $w_t \in \mathbb{C}^{N_t\times 1}$ بیانگر بردار پرتویی برای انتقال پیام است.

SNR دریافتی در گره گیرنده اصلی برابر است با :

$$SNR = \frac{d_{tr}^{-\alpha} p_t \mathrm{Tr}(H_{tr})}{\sigma_r^2} \qquad (۵)$$

سیگنال دریافت شده درگره m در هر بازه‌ی زمانی به صورت زیر می‌باشد :

$$y_m^\ell = \begin{cases} d_{nm}^{\frac{-\alpha}{2}} h_{nm}^H w_t s_n^\ell + n_m^\ell , \\ d_{tm}^{\frac{-\alpha}{2}} \sqrt{p_t} h_{tm}^H w_t s_t^\ell + d_{nm}^{\frac{-\alpha}{2}} h_{nm}^H w_n s_n^\ell + n_1^\ell \end{cases} \qquad (۶)$$

که به ترتیب α ، d_{tm}، d_{nm}و $(.)^H$ افت مسیر ، فاصله بین فرستنده و گره m، فاصله بین نویز کنترل شده و گره m و عملگر هرمتین می‌باشند $n_m^\ell \sim \mathcal{CN}\ (0, \sigma_m^2)$ ، نویز سفید گاوسی[1]دریافت شده در گره m است. پارامتر های ψ_0 و ψ_1 به ترتیب بیانگر تصمیم فرستنده برای ارسال داده و عدم ارسال می‌باشد.

۱-۳- شرایط ایجاد مخابره پنهان

قاعده تصمیم گیری بهینه در گیرنده غیرخودی برای کاهش خطا به‌صورت زیر می‌باشد:

$$\begin{cases} \frac{Y_{ch}}{n} < \vartheta & \psi_0 \\ \frac{Y_{ch}}{n} > \vartheta & \psi_1 \end{cases} \qquad (۷)$$

که $Y_{ch} = \sum_\ell^n \left|y_{ch}^\ell\right|^2$ و ϑ آستانه تصمیم گیری می‌باشد.

با توجه به توضیحات گفته شده، هنگامی می توان گفت که ارسال پنهان صورت پذیرفته است که شرط زیر در این مخابره اقناع شود [۸] و [۹] :

[1] Additive white guassian noise(AWGN)

$$\text{Any for } \varepsilon \geq 0 \quad \mathbb{P}_{MD} + \mathbb{P}_{FA} \geq 1 - \epsilon, \quad as \ n \to \infty \tag{۸}$$

احتمالات از دست دادن آشکارسازی و هشدار اشتباه را می‌توان بصورت زیر نوشت[۲۲]:

$$\mathbb{P}_{FA} = \begin{cases} e^{-\frac{(\vartheta - \sigma_{ch}^2)}{d_{nch}^{-\alpha} w_n^H C_{nch} w_n}}, & \vartheta - \sigma_{ch}^2 > 0, \\ 1, & \vartheta - \sigma_{ch}^2 \leq 0. \end{cases} \tag{۹}$$

$$\begin{cases} 1 + \dfrac{1}{d_{tch}^{-\alpha} p_t w_t^H C_{tch} w_t - d_{nch}^{-\alpha} w_n^H C_{nch} w_n} \times \\ \left[+ d_{nch}^{-\alpha} w_n^H C_{nch} w_n e^{-\frac{(\vartheta - \sigma_{ch}^2)}{d_{nch}^{-\alpha} w_n^H C_{nch} w_n}} - d_{tch}^{-\alpha} \right. \\ \left. \times p_t w_t^H C_{tch} w_t e^{-\frac{(\vartheta - \sigma_{ch}^2)}{d_{tch}^{-\alpha} p_t w_t^H C_{tch} w_t}} \right], \\ \vartheta - \sigma_{ch}^2 > 0, \\ 0, \quad \vartheta - \sigma_{ch}^2 \leq 0 \end{cases} \tag{۱۰}$$

۲-۳- آستانه تصمیم گیری بهینه از دیدگاه گیرنده غیرخودی

انتظار گیرنده غیر خودی، به حداقل رساندن $\mathbb{P}_{MD} + \mathbb{P}_{FA}$ است. بنابراین به منظور بدست آوردن v_{op} ، $\frac{\partial(\mathbb{P}_{MD} + \mathbb{P}_{FA})}{\partial v} = 0$ قرار می‌دهیم. به همین منظور می‌توانv_{op} با توجه به روابط در [۲۸]به صورت زیر نوشت:

$$v_{op} = \frac{(d_{nch}^{-\alpha} w_n^H C_{nch} w_n)(d_{tch}^{-\alpha} p_t w_t^H C_{tch} w_t)}{d_{tch}^{-\alpha} p_t w_t^H C_{tch} w_t - d_{nch}^{-\alpha} w_n^H C_{nch} w_n} \times \ln\left(\frac{d_{tch}^{-\alpha} p_t w_t^H C_{tch} w_t}{d_{nch}^{-\alpha} w_n^H C_{nch} w_n}\right) + \sigma_{ch}^2 \tag{۱۱}$$

که $\theta_{ch} = \tan^{-1}\left(\frac{y_{ch}}{x_{ch}}\right)$[۲۳].

۳-۳- توان دریافت شده در فرستنده

در این طرح فرستنده انرژی خود را از منبع و باتری موجود می گیرد و از این انرژی برای مخابره‌ی سیگنال پیام استفاده می‌کند. بنابراین با توجه به مصرف کلی شبکه می توان گفت که توان موجود در فرستنده در رابطه زیر صدق می‌کند:

$$p_t \leq p_t^{max} \tag{۱۲}$$

رای ارزیابی این طرح، یک مسئله بهینه سازی را فرمول بندی می‌شود و یک الگوریتم تکراری برای حل آن ارائه خواهد شد.

۴- مسئله بهینه سازی ارائه شده و راه حل آن در جهت ارزیابی طرح پیشنهادی

۱-۴- مسئله بهینه سازی

در این طرح نرخ مخابرات در گیرنده اصلی بیشینه می‌شود، توان ارسالی در فرستنده را بهینه می‌کند و اقناع شدن شرط مخابره پنهان می باشد. مسئله بهینه سازی زیر در نظر گرفته می‌شود :

$$\underset{w_n, p_t}{\text{Max}} \ p_r \log\left(1 + \frac{d_{tr}^{-\alpha} p_t \text{Tr}(H_{tr})}{d_{nr}^{-\alpha} |w_n^H h_{nr}|^2 + \sigma_r^2}\right)$$

$$\begin{aligned} &: \ C_1 \ : \ p_t \leq p_t^{max} \ s.t. \\ &C_2 \ : Tr(w_n w_n^H) \leq p_n^{max}, \\ &C_3 : d_{tch}^{-\alpha} \sigma_{h_{tch}}^2 p_t - \ d_{nch}^{-\alpha} \sigma_{h_{nch}}^2 \text{Tr}(w_n) \leq \\ &\qquad t \ , \\ &C_4 \\ &: \ln\left(\frac{d_{nch}^{-\alpha} \sigma_{h_{nch}}^2 \text{Tr}(w_n)}{d_{tch}^{-\alpha} \sigma_{h_{tch}}^2 p_t}\right) d_{nch}^{-\alpha} \sigma_{h_{nch}}^2 \text{Tr}(w_n) \\ &- t \ln(\varepsilon) \leq 0, \end{aligned} \tag{۱۳}$$

این تابع هزینه، نرخ دریافتی در گیرنده است. درنتیجه هدف به حداکثر رساندن نرخ دریافتی در گیرنده می‌باشد.که در این مسئله احتمال ارسال داده در یک اسلات زمانی است. بنابراین نرخ متوسط در گیرنده به صورت تابع هزینه بالا تعریف می‌شود که معیاری برای ارزیابی شبکه می‌باشد یعنی هرچه نرخ پنهان در گیرنده افزایش یابد می‌توان به یک شبکه مطلوب دست پیدا کرد. $H_{tr} = h_{tr} h_{tr}^H$ ، p_r احتمال انتقال داده در هر بازه زمانی است. علاوه براین d_{tr}، d_{nr} و σ_r^2 به ترتیب فاصله‌ی بین فرستنده وگیرنده، فاصله‌ی نویز کنترل شونده تا گیرنده و واریانس نویز در گیرنده می‌باشند.

از آنجا که تابع هدف مقعر نمی باشد می‌شود بنابراین نمی‌توانیم از روش‌هایی که مربوط به مسائل بهینه سازی مقعر هستند، استفاده کنیم . در نتیجه از آنجایی که داخل لگاریتم یک عبارت کسری قرار دارد، می توان از تقریب dc [۲۴] استفاده کرد و تابع هدف را به یک تابع مقعر تقریب زد. در نهایت مسئله، یک مسئله مقعر شده است و با استفاده از تولباکس cvx در متلب به حل آن می پردازیم [۲۵].

۵- نتایج شبیه سازی

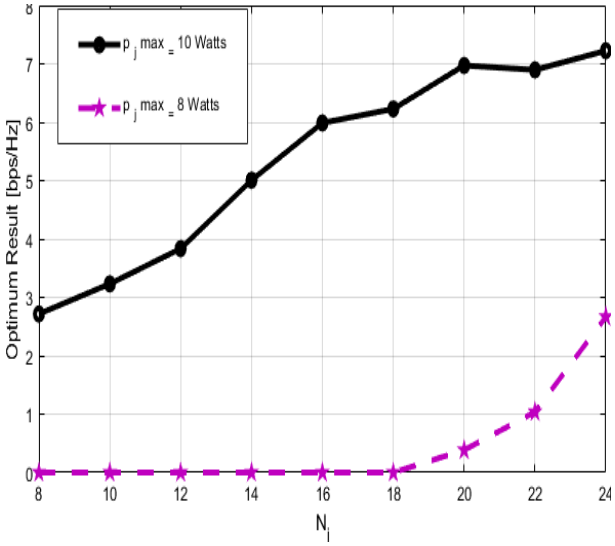
در این قسمت طرح پیشنهادی را با کمک نتایج شبیه‌سازی مورد بررسی قرار می‌دهیم. پارامترهای شبیه‌سازی شامل : $\varepsilon = 0.1$, $\varphi_{3dB} = 10^{\circ}$, $\theta_{3dB} = 70^{\circ}$ $\sigma^2_{h_{jch}} = 1$, $\sigma^2_{h_{tch}} = 1$, $p_r = 0.5$ $N_n = 8$, $\Omega_{max} = 17dB$ و $\eta = 0.2$ و محل گره ها عبارتند از :

$L_t = (0,0.1.5)$, $L_n = (0,-5,9)$
$L_r = (10,0,9)$ $L_{ch} =, (5,0,9)$. فرض می‌کنیم که فرستنده در (۰ ,۰) قرار دارد.

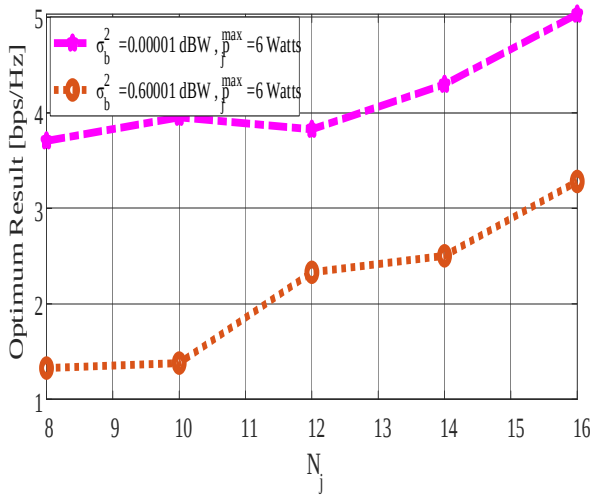
شکل(۵) تاثیر تعداد آنتن های نویز کنترل شونده را بر نرخ پنهان در هنگام استفاده از تکنیک شکل دهی دو بعدی نشان می‌دهد و همچنین مقایسه تاثیر حداکثر توان مجاز در نویز کنترل شونده را بر روی مقدار بهینه نشان می‌دهد. در نتیجه هرچه تعداد آنتن ها در سیگنال های نویز کنترل شونده بیشتر می‌شود، می توان پیام بیشتری را همراه با سیگنال های نویز کنترل شونده با حفظ شرط مخابره پنهان، ارسال کرد.

شکل (۶) تاثیر تعداد آنتن را در نویز کنترل شونده بر نرخ پنهان نشان می‌دهد. علاوه براین درصد بهبود کارایی شبکه را برای دو مقدار متفاوت واریانس نویز گیرنده ترسیم کرده. همان طور که مشاهده می‌شود، با افزایش واریانس نویز در گیرنده، مقدار بهینه کاهش پیدا می‌کند. همان طور که می‌دانیم واریانس نویز، همان دامنه طیف توان نویز می‌باشد. درنتیجه افزایش واریانس نویز در گیرنده اصلی به معنی افزایش مقدار توان نویز می‌باشد که سبب تداخل در گیرنده اصلی می‌شود. درنتیجه مقدار کمتری سیگنال پیام در گیرنده دریافت می‌شود، بنابراین نرخ پنهان نیز کاهش می‌یابد. با توجه به شکل با افزایش تعداد آنتن‌ها نرخ بیشتر می‌شود و نمودار با مقدار واریانس کمتر نرخ بیشتری را می‌دهد و هرچه مقدار واریانس افزایش می-یابد سطح نرخ کاهش می‌یابد.

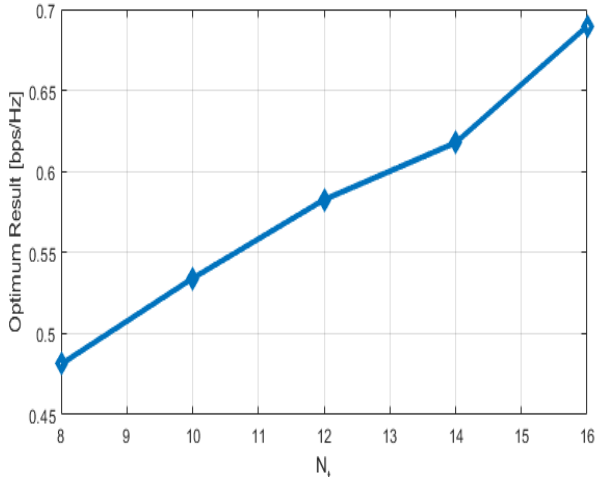
شکل(۷) مقدار بهینه را با توجه به افزایش تعداد آنتن‌ها در سیگنال‌های فرستنده نشان می‌دهد. همان طور که مشاهده می‌شود، با افزایش تعداد آنتن ها نرخ بهینه رو به افزایش می‌باشد.



شکل (۵). مقدار بهینه در مقابل تعداد آنتن های نویز کنترل شونده



شکل (۶). نرخ پنهان در مقابل تعداد آنتن‌های نویز کنترل شونده و واریانس نویز گیرنده



شکل (۷). مقدار بهینه در مقابل تعداد آنتن های فرستنده

۶- نتیجه‌گیری

وجود چندین آنتن در گره های سیستم مورنظر برای هدایت سیگنال اصلی و سیگنال پارازیت یکی از مزایای بسیار قابل توجه برای یک مخابره پنهان می‌باشند. مسئله بهینه سازی مطرح شده، نا محدب است بنابراین توان از تقریب dc [۲۸] استفاده کرد و تابع هدف را به یک تابع مقعر تقریب زد و با استفاده از تولباکس cvx در متلب به حل آن پرداخت [۲۹].

افزایش توان نویز کنترل کننده، در بهبود عملکرد سیستم بسیار موثر می‌باشد.با افزایش واریانس نویز در گیرنده، نرخ بهینه رو به کاهش می‌باشد زیرا با افزایش واریانس مقدار تابع هدف در مسئله مطرح شده کوچک می‌شود و درنتیجه مقدار بهینه نیز کاهش می‌یابد.

۷- مراجع

[1] C. Chen and M. A. Jensen, "Secret key establishment using temporally and spatially correlated wireless channel coefcients," *IEEE Transactions on Mobile Computing*, vol.10, no.2, pp.205–215, 2011.

[2] M. Di Renzo and M. Debbahua, "Wireless physical-layer security: The challenges ahead," in Advanced Technologies for Communications, 2009. ATC'09. International Conference on, pp.313–316, IEEE, 2009.

[3] M. Bloch and J. Barros, Physical-layer security: from information theory to security engineering. Cambridge University Press, 2011.

[4] T. Q. Duong, X. Zhou, and H. V. Poor, Trusted communications with physical layer security for 5G and beyond. Institution of Engineering & Technology, 2017.

[5] A. D. Wyner, "The wire tap channel," Bell system technical journal, vol. 54, no. 8, pp. 1355-1387, 1975.

[6] B. A. Bash, D. Goeckel, and D. Towsley, "Square root law for communication with low probability of detection on AWGN channels," in 2012 IEEE International Symposium on Information Theory Proceedings, 2012: IEEE, pp. 448-452.

[7] B. A. Bash, D. Goeckel, and D. Towsley, "Limits of reliable communication with low probability of detection on AWGN channels," IEEE journal on selected areas in communications, vol. 31, no. 9, pp. 1921-1930, 2013.

[8] T. V. Sobers, B. A. Bash, S. Guha, D. Towsley, and D. Goeckel, "Covert communication in the presence of an uninformed jammer," IEEE Transactions on Wireless Communications, vol. 16, no. 9, pp. 6193-6206, 2017.

[9] J. Hu, S. Yan, X. Zhou, F. Shu, J. Li, and J. Wang, "Covert communication achieved by a greedy relay in wireless networks," IEEE Transactions on Wireless Communications, vol. 17, no. 7, pp. 4766-4779, 2018.

[10] J. Hu, Y. Wu, R. Chen, F. Shu, and J. Wang, "Optimal detection of UAV's transmission with beam sweeping in covert wireless networks," IEEE Transactions on Vehicular Technology, vol. 69, no. 1, pp. 1080-1085, 2019.

[11] M. Forouzesh, P. Azmi, A. Kuhestani, and P. L. Yeoh, "Covert communication an secure transmission over untrusted relaying networks in the presence of multiple wardens," IEEE Transactions on Communications, vol. 68, no. 6, pp. 3737-3749, 2020.

[12] J. Hu, S. Yan, X. Zhou, F. Shu, and J. Wang, "Covert Transmission with Harvested Energy by a Wireless Powered Relay," arXiv preprint arXiv:1805.08925, 2018.

[13] O. A. Topal and G. K. Kurt, "Covert Communication in Cooperative NOMA Networks," in 2020 28th Signal Processing and Communications Applications Conference (SIU), 2020: IEEE, pp. 1-4.

[14] M. Choubin and A. Taherpour, "Optimization of distributed detection in energy harvesting wireless sensor networks with multiple antenna fusion center," Transactions on Emerging Telecommunications Technologies, vol. 31, no. 3, p. e3848, 2020.

[15] L. Yuda, J. Liang, W. Hu, and X. Xiaoming, "Multi-Antenna Covert Communication Achieved by Exploiting a Public Communication Link," in 2020 International Conference on Wireless Communications and Signal Processing (WCSP), 2020: IEEE, pp. 883-888.

[16] Y. Mao, G. Yu, and C. Zhong, "Energy consumption analysis of energy harvesting systems with power grid," IEEE Wireless Communications Letters, vol. 2, no. 6, pp. 611-614, 2013.

[17] R. Zhang and C. K. Ho, "MIMO broadcasting for simultaneous wireless information and power transfer," *IEEE Transactions on Wireless Communications*, vol. 12, no. 5, pp. 1989-2001, 2013.

[18] R. Sinha and P. Jindal, "A study of physical layer security with energy harvesting in single hop relaying environment," in 2017 4th international conference on signal processing and integrated networks (SPIN), 2017: IEEE, pp. 530-533.

[19] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, Handbook of applied cryptography. CRC press, 2018.

[20] J. Talbot, D. Welsh, and D. J. A. Welsh, Complexity and cryptography: an introduction. Cambridge University Press, 2006.

[21] Y. Feng, S. Yan, Z. Yang, N. Yang, and W.-P. Zhu, "TAS-based incremental hybrid decode–amplify–forward relaying for physical layer security enhancement," IEEE Transactions on

Communications, vol. 65, no. 9, pp. 3876-3891, 2017.

[22] J. Hu, S. Yan, F. Shu, J. Wang, J. Li, and Y. Zhang, "Artificial-noise-aided secure transmission with directional modulation based on random frequency diverse arrays," IEEE Access, vol. 5, pp. 1658-1667, 2017.

[23] S. Yan, X. Zhou, N. Yang, B. He, and T. D. Abhayapala, "Artificial-noise-aided secure transmission in wiretap channels with transmitter-side correlation," IEEE Transactions on wireless Communications, vol. 15, no. 12, pp. 8286-8297, 2016.

[24] B. A. Bash, D. Goeckel, D. Towsley, and S. Guha, "Hiding information in noise: Fundamental limits of covert wireless communication," IEEE Communications Magazine, vol. 53, no. 12, pp. 26-31, 2015.

[25] M. R. Bloch, "Covert communication over noisy channels: A resolvability perspective," IEEE Transactions on Information Theory, vol. 62, no. 5, pp. 2334-2354, 2016.

[26] D. Goeckel, B. Bash, S. Guha, and D. Towsley, "Covert communications when the warden does not know the background noise power," *IEEE Communications Letters*, vol. 20, no. 2, pp. 236-239, 2015.

[27] L. Wang, G. W. Wornell, and L. Zheng, "Fundamental limits of communication with low probability of detection," *IEEE Transactions on Information Theory*, vol. 62, no. 6, pp. 3493-3503, 2016.