University of Qom
Engineering Management and Soft Computing
JEMSC.QOM
Online ISSN: 2538-2675

Secure medical image transmission for healthcare applications using cooperative relaying based on physical layer security

Ali Kuhestani[1], Seyed Mohammadali Sebtonabi[2], Roozbeh Rajabi[3] and Mohammadreza Keshavarzi[4]

1. Assistant Professor of Telecommunication Engineering at Qom University of Technology, Email: kuhestani@qut.ac.ir
2. Ph.D. Student of Telecommunication Engineering at Shahed Univeristy. Email: sma.sebtonabi1373@yahoo.com
3. Assistant Professor of Telecommunication Engineering at Qom University of Technology, Email: rajabi@qut.ac.ir
4. ICT Research Institute, Iran Telecommunication Research Center (ITRC), Tehran, Iran, Email: mrkeshavarzi@itrc.ac.ir

Article Info

Article type:
Research Article

Article history:
Received 18 Aug 2024
Received in revised form 10 Sep 2024
Accepted 15 Sep 2024
Published online 21 Sep 2024

Keywords:
Eavesdropper,
Secure image transmission,
Secrecy Capacity,
Relay.

ABSTRACT

In this article, a new idea and method to protect image against illegal users has been proposed. Considering that in medical images, most of the experts' emphasis is on the part of the image that shows the disease, in this article, the image is first divided into two parts namely, main and background parts, and then the transmitter estimats regarding the capacity of legal and non-legal channels. Here, the transmitter decides whether to send the main part or the background part, i.e., when the capacity of the legal channel is greater than the capacity of the eavesdropping channel, the main part of the image is sent, and when the capacity of the eavesdropping channel is greater than the legal channel, the background part is sent. In addition, in this article, due to the large distance between the transmitter and the receiver and the effect of the path loss, a relay is adopted to boost the signal. Simulation results are provided to highlight the effectiveness of our proposed cooperative relaying idea.

Cite this article: Kuhestani, A. & others. (2024). Secure medical image transmission for healthcare applications using cooperative relaying based on physical layer security. *Enginiiring Management and Soft Computing, 10* (1). 213-237. **DOI**: https://doi.org/

DOI: https://doi.org/

Publisher: University of Qom

JEMSC.QOM
شاپا الکترونیکی: ۲۶۷۵-۲۵۳۸

مدیریت مهندسی و رایانش نرم

دانشگاه قم

ارسال امن تصویر پزشکی با استفاده از رله مشارکتی و مبتنی بر امنیت لایه فیزیکی

علی کوهستانی[۱]، سیدمحمدعلی سبط‌النبی[۲]، روزبه رجبی[۳] و محمدرضا کشاورزی[۴]

۱. استادیار، دانشکده مهندسی برق و کامپیوتر، دانشگاه صنعتی قم، قم، ایران. رایانامه: kuhestani@qut.ac.ir

۲. دانشجوی دکتری مخابرات سیستم، دانشکده فنی و مهندسی، دانشگاه شاهد، تهران، ایران. رایانامه: sma.sebtonabi1373@yahoo.com

۳. استادیار، دانشکده مهندسی برق و کامپیوتر، دانشگاه صنعتی قم، قم، ایران. رایانامه: rajabi@qut.ac.ir

۴. استادیار، پژوهشکده فناوری ارتباطات، پژوهشگاه ارتباطات و فناوری اطلاعات، تهران، ایران. رایانامه: mrkeshavarzi@qut.ac.ir

اطلاعات مقاله

نوع مقاله: مقاله پژوهشی

تاریخ دریافت: ۱۴۰۳/۰۵/۲۸

تاریخ بازنگری: ۱۴۰۳/۰۶/۲۰

تاریخ پذیرش: ۱۴۰۳/۰۶/۲۵

تاریخ انتشار: ۱۴۰۳/۰۶/۳۱

کلیدواژه‌ها:
ارسال امن تصویر،
رله،
ظرفیت محرمانگی.

چکیده

در این مقاله، ایده و روش جدیدی مبتنی بر رله مشارکتی جهت حفاظت اطلاعات تصویر از دسترسی کاربر غیرقانونی، پیشنهاد و بررسی خواهد شد. با توجه به اینکه در تصاویر پزشکی، بیشتر تاکید متخصصان روی بخشی از تصویر است که بیماری را نشان می‌دهد، در این مقاله ابتدا تصویر به دو بخش اصلی و پس‌زمینه تقسیم می‌شود و سپس فرستنده با تخمین ظرفیت محرمانگی کانال‌های قانونی و غیرقانونی نسبت به ارسال بخش اصلی و یا بخش پس‌زمینه تصمیم‌گیری می‌کند. هرگاه ظرفیت کانال قانونی از ظرفیت کانال شنودگر بیشتر باشد، بخش اصلی تصویر ارسال می‌شود و هرگاه ظرفیت کانال شنودگر از کانال قانونی بیشتر باشد، بخش پس‌زمینه ارسال می‌گردد. درضمن در این مقاله، به‌دلیل وجود فاصله بین فرستنده و گیرنده و اثر تلف مسیر، از ارسال مبتنی بر رله تقویت و ارسال برای مخابره اطلاعات استفاده می‌شود. نتایج شبیه‌سازی نیز نشانگر موثر و مفیدبودن این ایده برای جلوگیری از شنود اطلاعات توسط کاربران غیرقانونی می‌باشد.

استناد: کوهستانی، علی؛ سبط‌النبی، سیدمحمدعلی؛ رجبی، روزبه؛ کشاورزی، محمدرضا. (۱۴۰۳). «ارسال امن تصویر پزشکی با استفاده از رله مشارکتی و مبتنی بر امنیت لایه فیزیکی». *مدیریت مهندسی و رایانش نرم*، دوره ۱۰ (۱). صص: ۲۳۷-۲۱۳. https://doi.org/

ناشر: دانشگاه قم

۱) مقدمه

اینترنت اشیا[1] (IoT) با هدف اتصال سراسری تجهیزات و دستگاه‌ها در طیف گسترده‌ای از برنامه‌های کاربردی ازجمله دستگاه‌های پوشیدنی هوشمند در مراقبت‌های بهداشتی، نظارت از راه دور و شبکه‌های پزشکی، سعی در ارتقاء کیفیت زندگی بشریت دارد [۱]. ویژگی پخش ذاتی رسانه بی‌سیم، IoT را مستعد خطرات امنیتی و حریم خصوصی مانند استراق سمع، تجزیه‌وتحلیل ترافیک، پارازیت (Jamming) و حمله انکار سرویس[2] (DoS) کرده‌است [۲, ۳]. بطورخاص الزامات امنیتی برنامه‌های کاربردی مراقبت‌های بهداشتی بسیار مهم است زیرا به داده‌های حیاتی افراد دسترسی پیدا می‌کنند. علاوه‌براین، از منظر کیفیت خدمات[3] (QoS)، تاخیری که به‌دلیل انتقال تصاویر پزشکی در اندازه بزرگ به شبکه تحمیل می‌شود، می‌تواند به چالش قابل‌توجهی برای سیستم‌های مراقبت بهداشتی IoT تازه ظهور تبدیل شود.

بطور سنتی، ارتباطات تصویر پزشکی بی‌سیم از طریق روش‌های رمزنگاری مبتنی بر کلید یا تکنیک‌های واترمارک دیجیتال تحقق می‌یابد. با این وجود، با رشد روزافزون قابلیت‌های محاسباتی رایانه‌های مدرن، عملکرد روش‌های سنتی انتقال تصویر دیگر قابل اتکا نیست [۴]. همچنین طرح‌های مرسوم، به زیرساخت‌هایی نیاز دارند که نمی‌توانند به‌خوبی با افزایش تعداد دستگاه‌ها پیاده گردند. برخلاف تکنیک‌های رایج رمزنگاری، امنیت لایه فیزیکی[4] (PLS) برای محافظت از ارتباطات بی‌سیم در برابر تهدیدات امنیتی در سال‌های اخیر بطور گسترده‌ای مورد استفاده قرار گرفته‌است [۴, ۵]. PLS از ویژگی‌های ذاتی کانال بی‌سیم برای انتقال امن استفاده می‌کند که باعث می‌شود انتقال اطلاعات در کاربردهای مراقبت‌های بهداشتی IoT قابل پذیرش باشد.

۲) پیشینه تحقیق

اقدامات تحقیقاتی زیادی در حوزه PLS برای مطالعه ظرفیت محرمانگی[5] (SC) انجام شده‌است که از آن به‌عنوان حداکثر نرخ داده‌ای که می‌توان بطور امن و قابل اطمینان منتقل نمود، تعبیر می‌شود. به‌عبارت ریاضیاتی، این ظرفیت برابر است با تفاوت بین ظرفیت کانال اصلی و کانال شنود [۶–۸]. با این حال، طراحی ارسال مبتنی بر SC، نرخ داده قابل قبول بسیار پایین‌تری را منجر می‌شود که درنتیجه آن، شبکه مخابراتی تاخیر بالایی را تحمل می‌نماید. در سناریوی عملی ارسال تصویر حتی وقتی که تعداد کمی از بسته‌ها به‌درستی دریافت شوند، تصویر اصلی را نمی‌توان به‌درستی بازیابی کرد. از این رو، به‌دلیل اهداف متضاد، محرمانگی کامل برای چنین سیستم‌هایی قابل تحقق نیست [۹–۱۲].

در حوزه ارسال داده مبتنی بر PLS، محققان در [۹] تخصیص تطبیقی منابع را در یک سیستم نقطه‌به‌نقطه با کمک کدگذاری فواره‌ای[6] (FC) که برای ارسال امن تصویر پزشکی انتخاب شده بود، بررسی کردند. قابل ذکر است که یک شنودگر تک‌آنتنه (ایو) در مدل پیشنهادی آنها درنظر گرفته شده‌است. در مرجع [۱۰]، یک شبکه بی‌سیم تک‌ورودی–

[1] Internet of Things
[2] Denial of Service
[3] Quality of Service
[4] Physical Layer Security
[5] Secrecy Capacity
[6] Fountain code

تک‌خروجی[۷] (SISO) با کمک FC با تاکید بیشتر بر دو جنبه دیگر یعنی محتوای تصویر و تاخیر انتقال قابل تحمل، مورد بررسی قرار گرفت و ثابت گردید FC به‌عنوان یک تکنیک کم‌هزینه می‌تواند محرمانه‌بودن ارسال را در لایه فیزیکی افزایش دهد [۱۱-۱۳]. در ارسال مبتنی بر کد فواره‌ای، داده‌های اصلی ابتدا به یک سری Nتایی از بسته‌های منبع تقسیم می‌شوند سپس آنها به‌صورت خطی ترکیب می‌شوند تا تعداد بالقوه نامحدودی از بسته‌های کدگذاری‌شده فواره به‌دست آید. اگر و تنها اگر حداقل N بسته FC مستقل با موفقیت دریافت شود [۱۱]، پیام منبع را می‌توان بطور کامل در گیرنده بازیابی کرد. در [۱۲, ۱۳]، انتقال امن مبتنی بر FC با بکارگیری تکنیک‌های پیچیده‌تر مانند پارازیت مشارکتی و انتخاب رله برای ایجاد یک لینک قانونی با کیفیت بالا، در شبکه‌های مشارکتی اعمال گردید. با این حال، استفاده از سیگنال‌های پارازیت مانند نویز مصنوعی ممکن است برای برنامه‌های مراقبت‌های بهداشتی مضر باشد. بجز کار [۹] که یک سناریوی ساده SISO را درنظر می‌گیرد، هیچ تحقیقی در زمینه انتقال بی‌سیم امن برای برنامه‌های مراقبت‌های بهداشتی IoT با تمرکز بر محتوای داده وجود ندارد.

یکی از انواع داده‌ها که نیاز به طرح ارسال متفاوت و نیز لینک پرظرفیت دارد، داده‌های مربوط به تصویر و ویدئو است. برقراری امنیت ارسال این دسته از داده‌ها، نیاز به ارائه روش متفاوتی نسبت به داده‌های متن دارد. در این راستا در مرجع [۱۴] نویسندگان از دنباله‌های درهم‌سازی‌شده چبی‌شف برای بهبود امنیت انتقال تصویر در لایه فیزیکی شبکه‌های مخابراتی نوری مرئی استفاده کرده‌اند. در این مرجع اثبات شده‌است که امنیت لایه فیزیکی با استفاده از "دنباله درهم‌سازشده آشوبی چبی‌شف" می‌تواند بهبود یابد و کارآیی نرخ خطای بیت با پیش-کدگذاری DFT[8] بهبود یافته‌است. در مرجع [۹] نیز یک طرح ارسال امن برای انتقال بی‌سیم تصویر براساس کدگذاری فواره‌ای و تخصیص منبع وفقی پیشنهاد شده‌است. این روش دو مزیت عمده دارد: اول اینکه پیچیدگی پیاده‌سازی و هزینه کمتری نسبت به رمزنگاری سنتی دارد. دوم اینکه تاخیر ارسال کمی دارد. برای رسیدن به این دو هدف از راهکار جدیدی استفاده شده‌است. این راهکار جدید، ترکیبی از کدگذاری فواره‌ای در لایه کاربردی و تخصیص منابع وفقی در لایه فیزیکی است. به این ترتیب، با احتمال زیاد گیرنده قانونی می‌تواند تعداد کافی از بسته‌های آبشاری را قبل از اینکه به شنودگر برسد، دریافت کند و محرمانگی انتقال را بهبود دهد. همچنین روشی براساس کدگذاری جمع آثار برای برآوردن نیازمندی‌های تاخیر انتقال بکار گرفته شده‌است [۱۵]. بعد از تقسیم تصویر منبع به دو بخش ناحیه موردنظر[۹] (ROI) و پس‌زمینه[۱۰] (BG)، فرستنده می‌تواند بطور هم‌زمان یک بسته فواره‌ای ROI و یک بسته فواره‌ای BG را بفرستد که در آن بسته فواره‌ای ROI به‌عنوان داده لایه بهبود و بسته فواره‌ای BG به‌عنوان داده لایه پایه عمل می‌کند. در کدگذاری جمع آثار، رمزگشاشدن داده لایه بهبود به درست رمزگشاشدن داده لایه پایه بستگی دارد. این نکته نه‌تنها تاخیر انتقال را کاهش می‌دهد بلکه امکان شنود را نیز کاهش می‌دهد. زیرا درصورتیکه بسته فواره‌ای BG به‌درستی توسط شنودگر رمزگشا نشود امکان شنود بسته آبشاری ROI را نخواهد داشت [۱۰].

[7] Single Input – Single Output
[8] Discrete Fourier Transform
[9] Region of Interest
[10] Background

به‌عنوان یک رویکرد نوین در طراحی و بهینه‌سازی سیستم‌ها، روش‌های یادگیری ماشین و بطور خاص یادگیری عمیق در سال‌های اخیر در زمینه‌های مختلف سیستم‌های مخابرات بی‌سیم نسل جدید بکار گرفته شده‌اند [۱۶]. درخصوص ارسال امن اطلاعات می‌توان از تلفیق روش‌های یادگیری عمیق[11] و امنیت لایه فیزیکی نیز بهره برد. در همین رابطه در مرجع [۱۷] یک ارسال محتوا-آگاه[12] را مبنای کار خود قرار داده‌است. در این مرجع با تعدادی شنودگر روبرو هستیم که براساس توزیع پواسن[13] در محیط قرارگرفته‌اند. ارسال محتوا-آگاه به این معنی است که بخش‌های مهم تصویر براساس روش لبه‌یابی اولویت‌بندی شوند و در فرآیند انتقال تصویر بخش‌های با اولویت بالاتر ارسال شوند. نحوه ارسال نیز براساس احتمال شنود اطلاعات انجام می‌شود یعنی براساس درجه محرمانگی. اگر احتمال شنود اطلاعات بیشتر از درصد تعیین‌شده قرار داشت در آن بازه زمانی بجای ارسال بسته‌های پراهمیت، بسته‌های اطلاعاتی با درجه اهمیت کمتر ارسال خواهند شد تا بدین طریق از انتشار محتوای تصویر جلوگیری شود. در این مرجع با معرفی معیار احتمال نقض کیفیت سرویس به کمک مفاهیم یادگیری ماشین، سعی می‌کند تا این احتمال را بهینه کند و بدین طریق از شنود و نرسیدن بسته‌های اطلاعاتی تا حد زیادی جلوگیری نماید. همچنین در مقاله [۱۷] برای ارسال بسته‌های با اولویت کمتر نیز از روش پرتودهی بهره می‌برد تا این بسته‌ها با کمترین احتمال به شنودگرها برسند. در پایان نیز با استفاده از معیار اندیس شباهت ساختاری، میزان شباهت تصاویر دریافت‌شده در شنودگر و گیرنده قانونی را مورد بررسی قرار می‌دهد.

جهت روشن‌شدن اهمیت طرح پیشنهادی در این مقاله، کارهای [۱۸] -[۲۰] نیز مطالعه و مقایسه می‌شوند. در مقاله [۱۸]، نویسندگان برای امن‌سازی داده‌های موجود در تصویر، از روش رمزگذاری استفاده کرده‌اند. روش پیشنهادی این مقاله به دو بخش تقسیم می‌شود: آشفتگی و انتشار. در مرحله آشفتگی؛ موقعیت پیکسل با کمک الگوریتم شبکه‌های عصبی عمیق به‌صورت تصادفی تغییر داده می‌شود و سپس کلید تصادفی تولید می‌گردد تا کاربری که به کلید دسترسی ندارد نتواند به اطلاعات تصویر دسترسی پیدا کند. مزیت پژوهش انجام‌گرفته در مقاله ما نسبت به مرجع [۱۸] این است که در مرجع [۱۸] برای ایجاد پراکندگی پیکسل‌های تصویر از اعداد تصادفی و شبکه‌های عصبی عمیق استفاده شده‌است که این کار، حجم محاسباتی نسبتا زیادی دارد و از طرفی به‌دلیل افزایش قدرت محاسباتی شنودگرها، احتمال تشخیص الگوریتم (شکستن رمز) و به‌دست‌آوردن کلید توسط کاربران غیرقانونی وجود دارد. درحالیکه در پژوهش حاضر به‌دلیل وجود رله و درنظرگرفتن ظرفیت کانال‌های قانونی و غیرقانونی، زمانی اقدام به انتقال تصویر صورت می‌گیرد که از امن بودن انتقال اطلاعات، اطمینان کامل حاصل شده باشد. از طرفی در مرجع [۱۸] تاثیر فاصله در عملکرد الگوریتم ارائه‌شده لحاظ نشده‌است درحالیکه در پژوهش حاضر، تاثیر فاصله بر عملکرد الگوریتم مورد بررسی قرار گرفته‌است. همچنین در مرجع [۱۹] برای تغییر پیکسل‌ها در سه بعد، از روش‌های آشوب استفاده می‌شود و برای تولید کلید رمزگذاری نیز از سیستم Rossler بهبودیافته استفاده می‌شود. سیستم Rossler بهبودیافته، نسخه پیشرفته سیستم Rossler اصلی است که برای رفتار آشفته بهتر و امنیت بهبودیافته بهینه شده‌است. ازجمله مسائلی که در مرجع [۱۹] می‌توان به آن اشاره کرد افزایش بیش از حد پیچیدگی محاسباتی است. همچنین هیچ معیاری در رابطه با احتمال دسترسی و یا شکسته‌شدن رمز و دسترسی کلید به

[11] Deep Learning
[12] Content Aware
[13] Poisson

کاربر(های) قانونی قرار داده نشده‌است. در طرح پیشنهادی مرجع [۲۰] نیز اثر انگشت پزشک، رمزگذاری شده و پرونده سلامت بیمار را در یک تصویر غیرقابل‌توجه جاسازی می‌کند. در این پژوهش، یک الگوریتم رمزگذاری آشفته مبتنی بر یک کلید جایگشت برای رمزگذاری تصویر پزشکی و بردار ویژگی اثر انگشت استفاده شده‌است. این الگوریتم همانند روش‌های قبلی رمزگذاری، با مسئله پیچیدگی محاسباتی روبروست. همچنین معیاری که بتوان تصویر ارسالی و دریافتی را با یکدیگر مقایسه کرد و همچنین معیاری برای مقایسه تصویر در گیرنده قانونی و شنودگر وجود ندارد و از این بابت امکان سنجش پروتکل امنیتی به‌صورت شهودی فراهم نمی‌باشد.

در تمام مقالات بررسی‌شده، برای ارسال تصویر، باید بخش‌های مهمتر آن (ROI) که مدنظر است استخراج گردد و سپس بسته به شرایط کانال، اگر وضعیت لینک قانونی یعنی فرستنده-گیرنده از لینک شنودگر یعنی فرستنده-شنودگر بهتر بود، بخش‌های مهم تصویر (ROI) ارسال گردد و در غیر این صورت، بخش‌های کم‌اهمیت تصویر (BG) برای ارسال آماده گردند.

۳) روش تحقیق

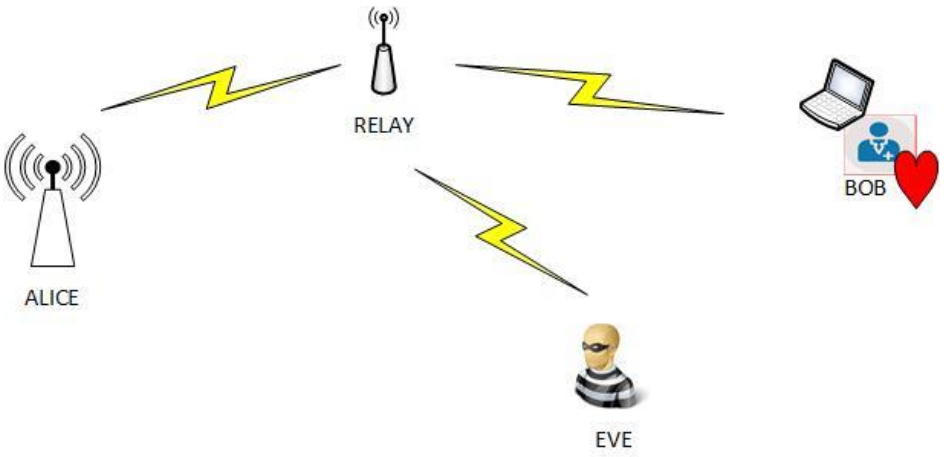
اصول روش تحقیق در این پژوهش شامل دو مرحله سیستم مدل پیشنهادی و پیش‌پردازش می‌باشد که در ادامه به بررسی این دو روش می‌پردازیم.

۳-۱) سیستم مدل پیشنهادی

اولین مرحله این پژوهش با توجه به نوع داده ما، پردازش تصویر می‌باشد. در این مرحله، بخش اصلی تصویر (ROI) از بخش پس‌زمینه آن (BG) جدا می‌گردد زیرا هدف اصلی حفظ محرمانگی بخش‌هایی از تصویر می‌باشد که اطلاعات بیشتری دارد و یا اصطلاحا آنتروپی بیشتری دارد. بعد از انجام این اقدام، دوباره هرکدام از این بخش‌ها به بخش‌های کوچکتر تقسیم می‌شوند تا کدبندی شده و آماده ارسال گردند. در این مقاله، شبکه مورد مطالعه، چهار گره دارد: یک فرستنده، یک رله تقویت و ارسال[۱۴] (AF)، یک شنودگر (گیرنده غیرقانونی) و یک گیرنده (گیرنده قانونی). فرستنده در هر لحظه با بررسی کانال قانونی برآیند فرستنده-رله-گیرنده و مقایسه آن با کانال شنودگر-گیرنده نسبت به نوع بسته ارسالی تصمیم‌گیری می‌کند. اگر ظرفیت کانال قانونی برآیند از ظرفیت کانال شنودگر بیشتر بود و یا به‌عبارت‌دیگر، اگر ظرفیت برآیند کانال قانونی از کانال شنود بیشتر بود در آن صورت ابتدا حداکثر نرخ ارسال، درنظر گرفته می‌شود تا نرخ ارسال ما از نرخ ارسال کانال شنود بیشتر شود و سپس با اعمال توان مناسب، ابتدا بسته‌های اطلاعاتی را به رله و سپس به گیرنده ارسال می‌کنیم. اما اگر در لحظاتی ظرفیت کانال شنودگر از ظرفیت کانال قانونی بیشتر بود، در این صورت به‌جای درگیرکردن رله، بسته‌های پس‌زمینه را بطور مستقیم به گیرنده ارسال می‌کنیم و سپس برای تشخیص این موضوع که این بسته جزء بسته‌های مهم اطلاعاتی نیست، فرستنده یک بیت صفر نیز به دنبال بسته ارسال می‌کند که البته این بیت حاوی اطلاعات مهم و خاصی نیست. توجه شود که فرآیند ارسال، با محدودیت زمانی و محدودیت تکرار مواجه است. بنابراین فرآیند ارسال زمانی به اتمام خواهد رسید که یا تمام بسته‌های اطلاعاتی در همان مدت تعیین‌شده، به پایان برسد و یا اینکه

[14] Amplify and Forward

زمان تکرار فرآیند به اتمام برسد و در این صورت نیز انجام فرآیند ارسال متوقف می‌شود. در شکل ۱، سیستم مدل پیشنهادی رسم شده‌است.



شکل ۹. سیستم مدل ارائه شده

در این قسمت مرحله‌به‌مرحله، پروتکل امنیتی روش پیشنهادی را بیان می‌کنیم.

۱) تقسیم تصویر به دو بخش ROI و BG.

۲) تقسیم‌کردن هرکدام از بخش‌های بالا به قسمت‌های کوچکتر یعنی N_{ROI} و N_{BG}.

۳) اختصاص یک توان مشخص در فرستنده و رله.

۴) تعیین SNR[15] لحظه‌ای کانال برآیند فرستنده–رله– گیرنده و شنودگر–رله با توجه به توان تخصیص‌داده‌شده.

۵) اگر در مرحله ۴ کانال برآیند فرستنده–رله–گیرنده بیشتر از کانال شنودگر–رله بود بسته‌های محرمانه، کدگذاری و ارسال می‌شوند در غیر این صورت بسته‌های پس‌زمینه در کانال مستقیم فرستنده–گیرنده، کدگذاری و ارسال می‌شوند.

۶) در مرحله آخر، شنودگر و گیرنده قانونی، بسته‌های دریافت‌شده از رله را کدگشایی می‌کنند.

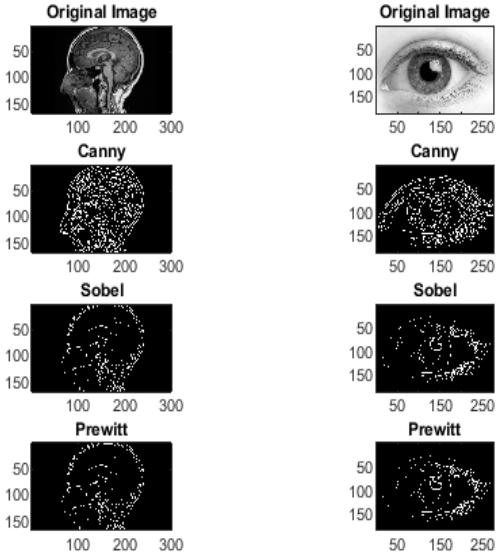
۷) این فرآیند زمانی به اتمام می‌رسد که یا مهلت دفعات ارسال به اتمام برسد و یا اینکه فرستنده تمام بسته‌های اطلاعاتی را ارسال کرده باشد.

۲–۳) پیش‌پردازش

با توجه به اینکه نوع داده این پژوهش از نوع تصویر می‌باشد بنابراین لازم است قبل از ارسال، یک پردازش ابتدایی روی آن صورت گیرد تا بخش‌های برجسته و مهم تصویر که موردنظر ما هست، استخراج شود. این اقدام که به بخش‌بندی[16] تصویر معروف است باعث می‌شود بخش‌هایی از تصویر که مدنظر ما نیست و عملا تاثیری در محتوای اصلی ندارد، حذف شود و بسته به‌عنوان بسته محرمانه درنظر گرفته نشود. بنابراین برای اینکه بتوانیم حجم اطلاعات خود را کاهش دهیم تا انتقال بخش‌های اصلی که شامل بخش‌های تشخیصی آن نیز می‌شود در بازه زمانی کوتاهتری انجام پذیرد، بخش پس‌زمینه

[15] Signal to Noise Ratio
[16] Segmentation

تصویر را حذف می‌کنیم. در مبحث پردازش تصویر، برای جداسازی دو بخش از تصویر، روش‌های گوناگونی وجود دارد که از برجسته‌ترین آنها می‌توان به لبه‌یابی[۱۷] تصاویر اشاره کرد. لبه‌ها، پیکسل‌هایی از تصاویر هستند که میزان روشنایی آنها با پیکسل‌های مجاورشان بطور ناگهانی تغییر می‌کند. ازجمله تکنیک‌های تشخیص لبه می‌توان به روش سوبل[۱۸]، کنی[۱۹]، رابرتز[۲۰]، پرویتز[۲۱] و غیره اشاره کرد. البته بیان جزئیات این مطالب از حوزه این پژوهش خارج می‌باشد لذا فقط به شبیه‌سازی و نمایش یک نمونه از هرکدام اکتفا می‌کنیم.



شکل ۱۰. بخش‌بندی تصویر براساس روش‌های مختلف لبه‌یابی

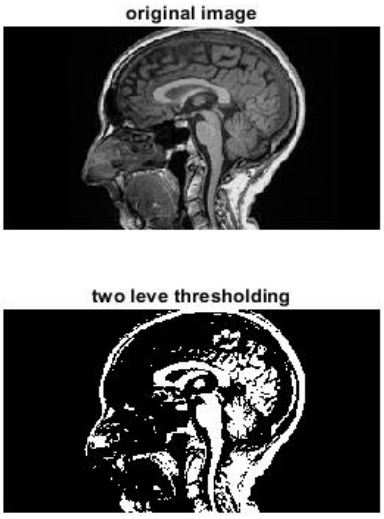
یکی دیگر از راه‌های بخش‌بندی تصویر، استفاده از آستانه‌گذاری[۲۲] است. آستانه‌گذاری به روش‌های مختلفی انجام می‌شود که ازجمله آن می‌توان به آستانه‌گذاری دوسطحی، آستانه‌گذاری چندسطحی و آستانه‌گذاری آتسو اشاره کرد که در ادامه به توضیح این روش‌ها می‌پردازیم:

در آستانه‌گذاری دوسطحی تصویر؛ با اعمال یک سطح آستانه، پیکسل‌هایی که کمتر از سطح آستانه تعیین شده، به مقدار صفر و پیکسل‌های بیشتر از سطح آستانه به مقدار ۲۵۵ نگاشت می‌شوند و درنهایت یک تصویر دودویی خواهیم داشت. بیان ریاضی آستانه‌گذاری دوسطحی به‌صورت زیر است:

$$x(i,j) < T, x(i,j) = 0$$
$$x(i,j) > T, x(i,j) = 255 \qquad (۱)$$

در ادامه یک نمونه از این نوع آستانه‌گذاری قرار داده شده‌است:

[17] Edge detection
[18] Sobel
[19] Canny
[20] Roberts
[21] Prewitt
[22] Thresholding

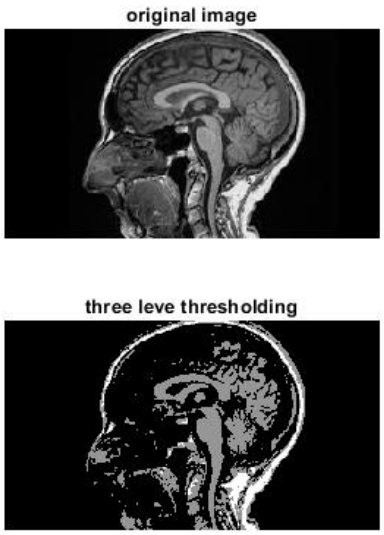


شکل ۱۱. یک نمونه آستانه‌گذاری دوسطحی

در آستانه‌گذاری چندسطحی نیز ابتدا یک سطح آستانه تعیین می‌کنیم و پیکسل‌های با مقادیر کمتر از آن را به عدد صفر نگاشت می‌دهیم و با تعیین مقادیر بعدی آستانه، پیکسل‌هایی که چنین مقادیری داشته باشند یعنی بین حد آستانه قبلی و این حد تعیین‌شده قرارگرفته‌اند، به مقدار تعیین‌شده نگاشت داده می‌شوند و با تعیین حد آستانه مقدار نهایی، پیکسل‌هایی که بیشتر از مقدار تعیین‌شده هستند به مقدار نهایی تعیین‌شده، نگاشت داده می‌شوند. در ادامه بیان ریاضی آستانه سه‌سطحی آورده شده‌است:

$$\begin{matrix} x(i,j) < T_1, & x(i,j) = 0 \\ T_1 \le x(i,j) < T_2, & x(i,j) = l_1 \\ x(i,j) \ge T_2, & x(i,j) = l_2 \end{matrix} \qquad (۲)$$

در اینجا نتیجه اعمال یک نمونه آستانه‌گذاری سه‌سطحی را مشاهده می‌کنیم:



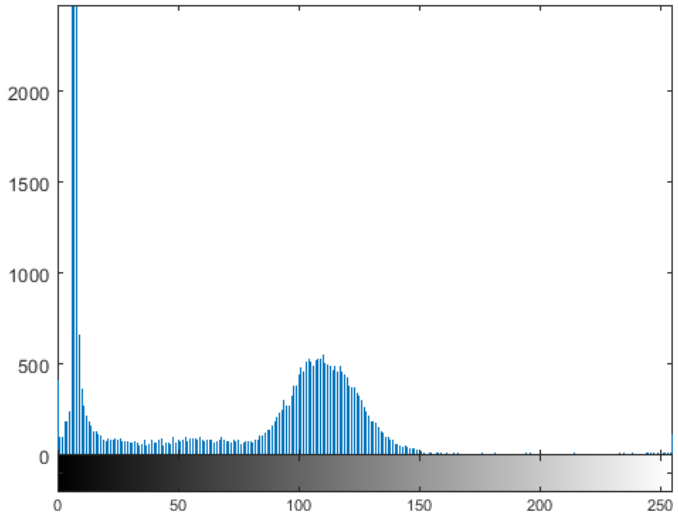
شکل ۱۲. یک نمونه آستانه‌گذاری چندسطحی

یکی دیگر از راه‌های بخش‌بندی تصویر استفاده از روش آستانه‌گذاری آتسو[۲۳] می‌باشد. در روش آتسو به ازای هر گزینه از حد آستانه، هیستوگرام تصویر به دو گروه تقسیم می‌شود سپس طبق رابطه زیر واریانس بین‌کلاسی بین دو گروه محاسبه می‌شود:

$$\sigma_w^2(t) = w_0(t).\sigma_0^2(t) + w_1(t).\sigma_1^2(t) \quad (۳)$$

این کار به ازای همه گزینه‌ها (۲۵۵-۰) تکرار می‌شود و به ازای هرکدام، واریانس بین‌کلاسی محاسبه می‌شود. در انتها واریانس بین‌کلاسی کلیه حد آستانه‌ها باهم مقایسه می‌شوند و حد آستانه بهینه انتخاب می‌شود. حد آستانه‌ای، بهینه است که در آن واریانس بین‌کلاسی ماکزیمم شود. به‌عبارتی حد آستانه‌ای، بهینه است که باعث شود میانگین دو قله هیستوگرام بیشترین فاصله را نسبت به هم داشته باشند.

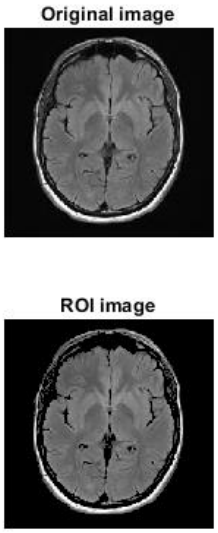
بنابر مطالب ذکرشده، این روش آستانه‌گذاری برای تصاویری مناسب است که هیستوگرام آن شامل دو قله باشد. روش آتسو حد آستانه‌ای انتخاب می‌کند که باعث شود دو قله هیستوگرام بطور کامل از هم تفکیک شوند. به‌عبارت‌دیگر؛ این روش حد آستانه‌ای انتخاب می‌کند که دارای بیشترین واریانس بین‌کلاسی باشد. اکنون تصویری را مورد بررسی قرار می‌دهیم که هیستوگرام آن دارای دو قله می‌باشد و هیستوگرام آن را رسم می‌کنیم.



شکل ۱۳. هیستوگرام تصویر

با مشاهده هیستوگرام تصویر و با توجه به اینکه هیستوگرام آن دو قله دارد، روش آتسو می‌تواند برای بخش‌بندی قسمت اصلی تصویر از بخش حاشیه آن مناسب باشد.

[23] Otsu



شکل ١٤. تصویر بالا: تصویر اولیه و تصویر پایین: ناحیه موردنظر تصویر

بخش‌بندی‌هایی که در اینجا به آنها اشاره‌شد، به این دلیل در پژوهش حاضر مورد استفاده قرار می‌گیرد که قسمت‌های مهم و اصلی تصویر را از بخش‌هایی که از اهمیت محرمانگی کمتری برخوردار است، جدا کند. تا زمانی معیار بیشینه شباهت را برای سنجش کارآیی مدل پیشنهادی مورد ارزیابی قرار می‌دهیم که منحنی‌های استخراج‌شده صرفا بر مبنای بخش‌های اصلی تصویر باشد تا بتوان به کمک این مبنا، عملکرد رله و شنودگر را بطور دقیق و بر مبنای بسته‌های اطلاعاتی محرمانه، بررسی کرد.

۴) بررسی و تحلیل سیستم مدل پیشنهادی

همانطورکه در بخش قبل بیان گردید در ابتدا باید تصویر را به دو بخش ناحیه موردنظر (ROI) و پس‌زمینه (BG) تبدیل کنیم و بعد از آن نیز هرکدام از این بخش‌ها را به N بسته اطلاعاتی که عبارتنداز N_{bg} و N_{roi} هستند، تقسیم کنیم تا آماده ارسال شوند. در ادامه به سراغ ایده اصلی این پژوهش می‌رویم. ایده اصلی ما در این مقاله، استفاده از رله در ارتباط بی‌سیم هست زیرا رله‌کردن مشارکتی یکی از روش‌های امنیت لایه فیزیکی است. با توجه به مسئله تلف مسیر[۲۴]، توان سیگنال به‌دلیل بُعد مسافت به‌مرور کاهش می‌یابد و همین امر موجب می‌شود که کیفیت سیگنال دریافتی در گیرنده، پایین باشد. بنابراین لازم است تا با قراردادن رله مشارکتی در مسیر فرستنده-گیرنده با افزایش توان سیگنال، اثر تلف مسیر را کاهش دهیم و حتی‌المقدور سیگنال قابل قبولی در گیرنده، دریافت نماییم. با توجه به اینکه با تصویر پزشکی سروکار داریم، کیفیت سیگنال دریافتی در گیرنده اهمیت خاصی خواهد داشت. بنابراین ما در این مرحله به جای ارسال مستقیم از فرستنده به گیرنده، از ارسال باواسطه کمک می‌گیریم. یعنی سیگنال را ابتدا به رله و سپس به گیرنده ارسال می‌کنیم. مزیت دیگر ارسال به کمک رله به جای ارسال مستقیم، این است که توانی که رله برای باز-ارسالی سیگنال دریافتی استفاده می‌کند منجر به افزایش ظرفیت محرمانگی کانال قانونی می‌شود چراکه با اعمال این توان بر روی کانال قانونی، ظرفیت کانال

[24] Path loss

برآیند فرستنده-رله-گیرنده نسبت به کانال شنودگر افزایش می‌یابد و همین امر موجب تضمین محرمانگی مخابره می‌شود. پس ما تا اینجا باید دو موضوع را اثبات کنیم: اول اینکه آیا کانال فرستنده-رله نسبت به کانال مستقیم فرستنده-گیرنده دارای ظرفیت محرمانگی بیشتری می‌باشد؟ و دوم اینکه آیا برآیند کانال قانونی یعنی فرستنده-رله-گیرنده نسبت به برآیند کانال شنودگر دارای ظرفیت بیشتری است؟ در ادامه به اثبات این دو مسئله می‌پردازیم.

در ابتدا به بررسی موضوع اول می‌پردازیم و با تغییر توان فرستنده و قراردادن سه گیرنده و یک رله در مختصات مختلف، ظرفیت محرمانگی آنها را به کمک شبیه‌سازی مونت‌کارلو[۲۵] رسم و نتایج را باهم مقایسه می‌کنیم (شکل ۹ و شکل ۱۰). اما باید توجه داشت که ارسال ما دارای دو مرحله[۲۶] است و ما باید برآیند کانال‌های قانونی و شنودگر را بررسی نماییم. پس ابتدا به معرفی کانال خود می‌پردازیم و سپس برآیند دو کانال را محاسبه می‌کنیم.

کانال مخابراتی از نوع فیدینگ می‌باشد و ضمنا ضرایب کانال[۲۷] در یک اسلات زمانی، ثابت می‌ماند و از هر اسلات به اسلات دیگر تغییر می‌کند. این ضرایب به‌صورت فرآیند تابع توزیع گاوسی مختلط هستند. رابطه ضرایب کانال به‌صورت مقابل می‌باشد $CN(0,\sigma_{i,j}^2)$ که $\sigma_{i,j}^2 = d_{i,j}^{-\alpha}$. در این رابطه d فاصله دو گره و α تلف مسیر است. SNR سیستم نیز برابر است با $\rho = \frac{P}{N_0}$ که در این رابطه P توان ارسالی گره مبدأ می‌باشد و N_0 توان نویز است. SNR دریافتی در گره jنیز برابر است با $\gamma_{i,j} = \rho|h_{i,j}|^2$.

اکنون به معرفی کانال برآیند می‌پردازیم:

از آنجاییکه در این مقاله، ارسال به واسطه رله صورت می‌گیرد، پس باید ظرفیت محرمانگی در هر دو مرحله ارسال بیشتر از ظرفیت کانال شنودگر باشد تا بتوان یک کانال محرمانه را ایجاد کرد. برای تحقق این امر ما کانال برآیند فرآیند ارسال را درنظر می‌گیریم و ظرفیت برآیند و ظرفیت محرمانگی را در این حالت بررسی می‌کنیم. برآیند کانال قانونی عبارت است از کانال فرستنده-رله-گیرنده. برآیند کانال شنودگر نیز عبارت است از کانال شنودگر-گیرنده. با توجه به اینکه فاصله شنودگر تا فرستنده زیاد است، همین امر موجب شده تا احتمال شنود در مرحله اول درنظر گرفته نشود. اکنون سیگنال‌های دریافتی در گره‌های مختلف را بررسی می‌کنیم.

سیگنال‌های دریافتی در رله برابر است با:

$$y_r = \sqrt{P_s} h_{sr} x_s + n_0 \qquad (۴)$$

سیگنال دریافتی در شنودگر برابر است با:

$$y_{eve} = \sqrt{P_r} h_{reve} x_r + n_0 \qquad (۵)$$

سیگنال دریافتی در گیرنده برابر است با:

$$y_d = \sqrt{P_r} h_{rd} y_d + n_0 \qquad (۶)$$

---

[25] Monte_Carlo
[26] Hop
[27] Channel Coefficient

اکنون با توجه به سیگنال‌های دریافتی، باید برآیند دو کانال قانونی و شنودگر را درنظر بگیریم که برای این کار باید SNR دریافتی در گیرنده که درحقیقت همان SNR_{e2e} است را حساب کنیم. برآیند SNR دریافتی در گیرنده برابر است با:

$$\gamma_{e2e\_d} = P_s P_r |h_{ar} h_{rb}|^2 \quad (۷)$$

برآیند SNR دریافتی در شنودگر نیز برابر است با:

$$\gamma_{e2e\_eve} = P_r |h_{reve}|^2 \quad (۸)$$

و اکنون ظرفیت دو کانال قانونی و شنودگر را با استفاده از روش شبیه‌سازی مونت‌کارلو محاسبه می‌کنیم. بر این اساس، ظرفیت برآیند کانال قانونی برابر می‌شود با:

$$C_{e2e\_d} = log_2(1 + \gamma_{e2e\_d}) \quad (۹)$$

همچنین ظرفیت برآیند کانال شنودگر برابر می‌شود با:

$$C_{e2e\_eve} = log_2(1 + \gamma_{eve}) \quad (۱۰)$$

به کمک شبیه‌سازی مونت‌کارلو ظرفیت این دو کانال را در شکل‌های ۹ و ۱۰ مشاهده می‌کنیم. در ادامه معیار نقض کیفیت سرویس را در پروتکل پیشنهادی بررسی می‌کنیم.

با توجه به اینکه در پروتکل پیشنهادی، از رله استفاده شده‌است پس باید ابتدا فرمول بسته QVP را با توجه به حضور رله بنویسیم.

$$p^{vio} = \Pr\left(T_{tot,D} > T_{req}\right) + \sum_{k=N}^{T_{req}} \Pr\left(T_{tot,D} = k\right) \Pr\left(T_{tot,E} \le k\right) \quad (۱۱)$$

در رابطه بالا، $T_{tot,E}$ و $T_{tot,D}$ به‌ترتیب تعداد بسته‌های اطلاعاتی هستند که شنودگر و گیرنده قانونی نیاز دارند تا تصویر را بطور کامل بازیابی کنند. T_{req} نیز محدودیت ارسال را تعیین می‌کند.

$$T_{tot,D} = N + N_{out} \quad (۱۲)$$

که در رابطه بالا N_{out} تعداد دفعات خاموشی است که در کانال برآیند فرستنده-رله-گیرنده اتفاق می‌افتد و احتمال وقوع آن را با α نمایش می‌دهیم و در ادامه نیز فرمول بسته آن را نیز به‌دست خواهیم آورد.

تعداد دفعات وقوع خاموشی را می‌توان به‌صورت یک تابع توزیع منفی[۲۸] درنظر گرفت و تابع جرم احتمال[۲۹] آن را به‌صورت زیر بیان نمود:

$$f_{N_{out}}(k) = \Pr(N_{out} = k) = \binom{N + k - 1}{k} \alpha^k (1 - \alpha)^N, k = 0,1,2, \dots \quad (۱۳)$$

[28] Negative Binomial Distribution
[29] Probability Mass Function

تابع جرم احتمال $T_{tot,D}$ نیز به‌صورت زیر قابل‌محاسبه می‌باشد:

$$f_{T_{tot,D}}(k) = \Pr(N_{out} = k - N) = \begin{cases} \binom{k-1}{k-N}\alpha^{(k-N)}(1-\alpha)^N & k \geq N \\ 0 & \\ 0, & k < N \end{cases} \quad (۱۴)$$

درنتیجه محاسبه قسمت اول رابطه (۱۱) به‌صورت زیر محاسبه می‌شود:

$$\Pr\left(T_{tot,D} > T_{req}\right) = 1 - Pr\left(T_{tot,D} \leq T_{req}\right) = 1 - \sum_{k=N}^{T_{req}} \binom{k-1}{k-N} \alpha^{k-N}(1-\alpha)^N \quad (۱۵)$$

اکنون احتمال وقوع خاموشی در کانال اصلی را که در حقیقت همان α می‌باشد، محاسبه می‌کنیم.

$$\begin{aligned} \alpha = Pr\left(\gamma_{SR} < \frac{2^{2R-1}}{2}\right) \Pr\left(\frac{1}{2}\log\left(1 + SNR_D^{(1)}\right) < R\right) \\ + \Pr\left(\gamma_{SR} > \frac{2^{2R-1}}{2}\right) \\ \times \Pr\left(\frac{1}{2}\log\left(1 + SNR_D^{(1)} + SNR_D^{(2)}\right) < R\right) \end{aligned} \quad (۱۶)$$

اکنون تابع جرم احتمال را برای شنودگر محاسبه می‌کنیم.

$$\begin{aligned} \Pr\left(T_{tot,E} \leq k\right) &= \sum_{p=N}^{k} Pr\left(T_{tot,E} = p\right) \\ &= \sum_{p=N}^{k} f_{T_{tot,E}}(p) = \sum_{p=N}^{k} \binom{p-1}{p-N} \beta^{p-N}(1-\beta)^N \end{aligned} \quad (۱۷)$$

در رابطه بالا، β احتمال خاموشی در کانال فرستنده به شنودگر می‌باشد که از طریق رابطه زیر به‌دست می‌آید:

$$\begin{aligned} \beta = Pr\left(\gamma_{SR} < \frac{2^{2R-1}}{2}\right) \Pr\left(\frac{1}{2}\log\left(1 + SNR_E^{(1)}\right) < R\right) \\ + \Pr\left(\gamma_{SR} > \frac{2^{2R-1}}{2}\right) \times \Pr\left(\frac{1}{2}\log\left(1 + SNR_E^{(1)} + SNR_E^{(2)}\right) < R\right) \end{aligned} \quad (۱۸)$$

که در رابطه بالا، باکمک [۱۷] داریم:

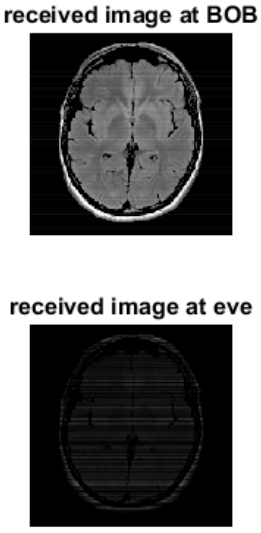
$$\begin{aligned} &\Pr\left(\gamma_{SR} < \frac{2^{2R-1}}{2}\right) = 1 - e^{-\frac{1}{2}\lambda_{SR}(2^{2R}-1)} \\ &\Pr\left(\gamma_{SR} > \frac{2^{2R-1}}{2}\right) = e^{-\frac{1}{2}\lambda_{SR}(2^{2R}-1)} \\ &\Pr\left(\frac{1}{2}\log\left(1 + SNR_E^{(1)} + SNR_E^{(2)}\right) < R\right) \\ &\qquad = 1 - e^{-\frac{\lambda_{RD}}{2}(2^{2R}-1)} \\ &\qquad - \frac{\lambda_{RD}\lambda_{JD}}{2\lambda_{SD}} e^{-\frac{\lambda_{RD}}{2}(2^{2R}-1)+\lambda_{JD}\left(1-\frac{\lambda_{RD}}{2\lambda_{SD}}\right)} \times A \end{aligned} \quad (۱۹)$$

$$A = Ei\left(-((2^{2R}-1)+\frac{\lambda_{JD}}{\lambda_{SD}})\left(\lambda_{SD}-\frac{\lambda_{RD}}{2}\right)\right) - Ei\left(-\frac{\lambda_{JD}}{\lambda_{SD}}\left(\lambda_{SD}-\frac{\lambda_{RD}}{2}\right)\right)$$

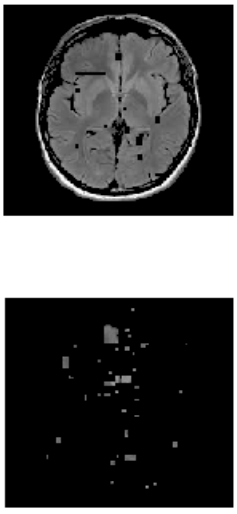
رسم منحنی‌های مربوطه براساس معیار QVP در شکل ۱۵ آمده‌است.

۵) یافته‌ها و نتایج پژوهش

در این بخش به بررسی نتایج عددی می‌پردازیم. در ابتدا تصویر را به دو صورت بدون استفاده از رله و به کمک رله ارسال می‌کنیم تا بتوان اثر وجود رله را در این مدل بررسی کنیم. در دو تصویری که در ادامه قرار داده‌شده‌است توان در فرستنده ۱۰ دسی بل-وات در گرفته شده‌است:



شکل ۱۵. تصویر بازسازی‌شده در گیرنده و شنودگر از طریق ارسال مستقیم

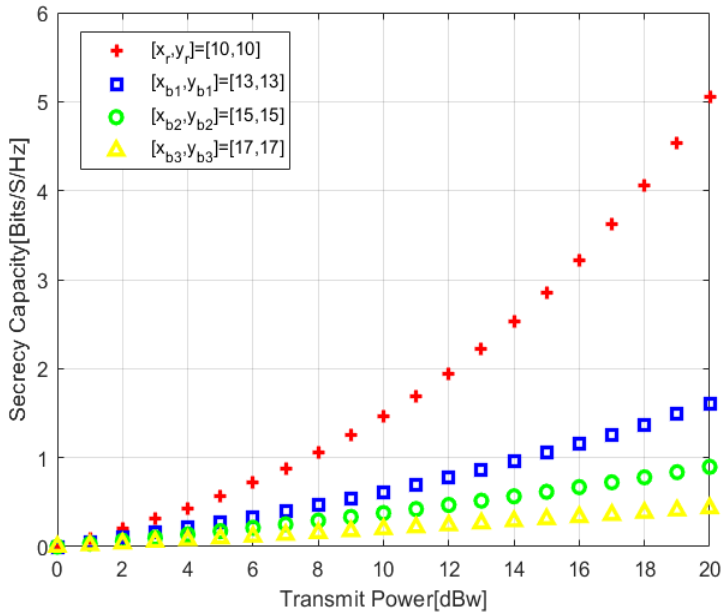


شکل ۱۶. تصویر بازسازی‌شده در گیرنده و شنودگر از طریق ارسال به واسطه رله

با مقایسه شکل ۷ و شکل ۸ می‌توان به این نتیجه رسید که با ارسال بسته‌های تصویر بطور مستقیم و بدون رله به‌دلیل وجود مسئله تلف مسیر و کاهش توان، ظرفیت محرمانگی کانال قانونی کاهش می‌یابد و منجر می‌شود کانال شنودگر، بتواند بسته‌های اطلاعاتی بیشتری را به‌دست آورد. این در حالی است که در وضعیت ارسال به واسطه رله؛ با تخصیص توان مناسب، ظرفیت محرمانگی کانال قانونی نسبت به کانال شنودگر افزایش پیدا کرده‌است و درنتیجه شنودگر به بسته‌های کمتری دسترسی پیدا کرده‌است.

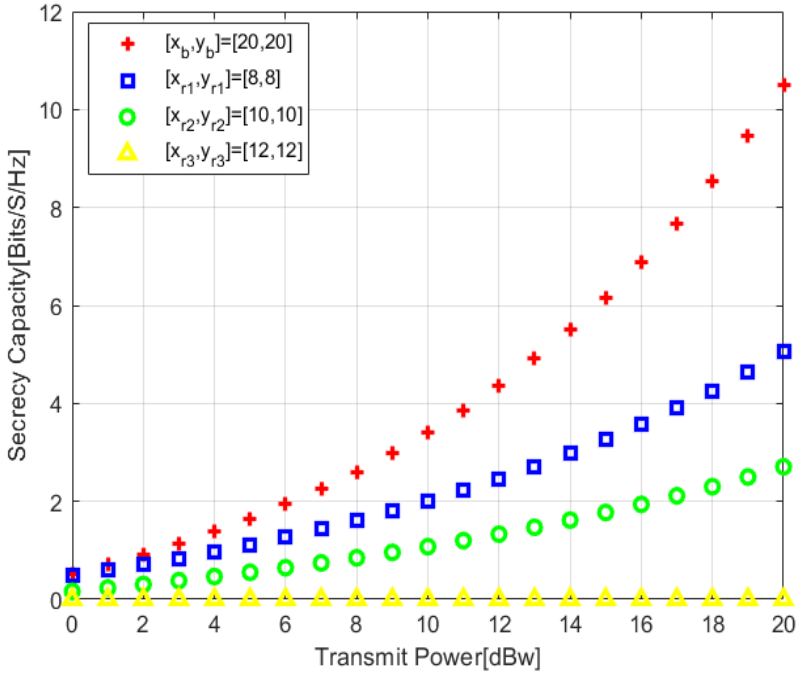
تصاویر بالا، حاصل ارسال سیگنال با توان صفر دسی‌بل-وات و محدودیت ارسال ۲۰۰ مرتبه می‌باشد و همچنین شنودگر در مختصات (۱۵و ۱۵) قرار گرفته‌است. با دقت در تصاویر سمت راست که توسط گیرنده بازیابی شده‌است، متوجه می‌شویم که بعضی از پیکسل‌های تصویر بازیابی نشده‌اند زیرا با توجه به توان پایین فرستنده، نرخ ارسال کاهش می‌یابد و با توجه به محدودیت تعداد دفعات ارسال منجر به این مسئله می‌شود که فرستنده بخشی از پیکسل‌های تصویر را نتواند ارسال کند. نکته دیگر که قابل‌توجه می‌باشد این است که چون تعداد این پیکسل‌ها بسیار کم هستند عملا تاثیری در محتوای اصلی ندارد و تصویر کاملا قابل‌شناسایی می‌باشد. در تصویر سمت چپ نیز شنودگر توانسته به بعضی از بخش‌های تصویر دسترسی پیدا کند و دلیل آن امر این است که برآیند کانال شنودگر در بعضی از لحظات نسبت به ظرفیت برآیند کانال قانونی، بیشتر می‌باشد.

اکنون با تغییر توان فرستنده و قراردادن سه گیرنده و یک رله در مختصات مختلف، ظرفیت محرمانگی آنها را به کمک شبیه‌سازی مونت‌کارلو رسم و نتایج را باهم مقایسه می‌کنیم. لازم به ذکر است که در تمام شبیه‌سازی‌های انجام‌گرفته، از مدولاسیون QPSK استفاده می‌کنیم. مدل نویز، نرمال با میانگین صفر و واریانس ۱ می‌باشد. مقدار تلف مسیر نیز ۳ درنظر گرفته شده‌است.



شکل ۱۷. تاثیر فاصله گیرنده از فرستنده در ظرفیت محرمانگی

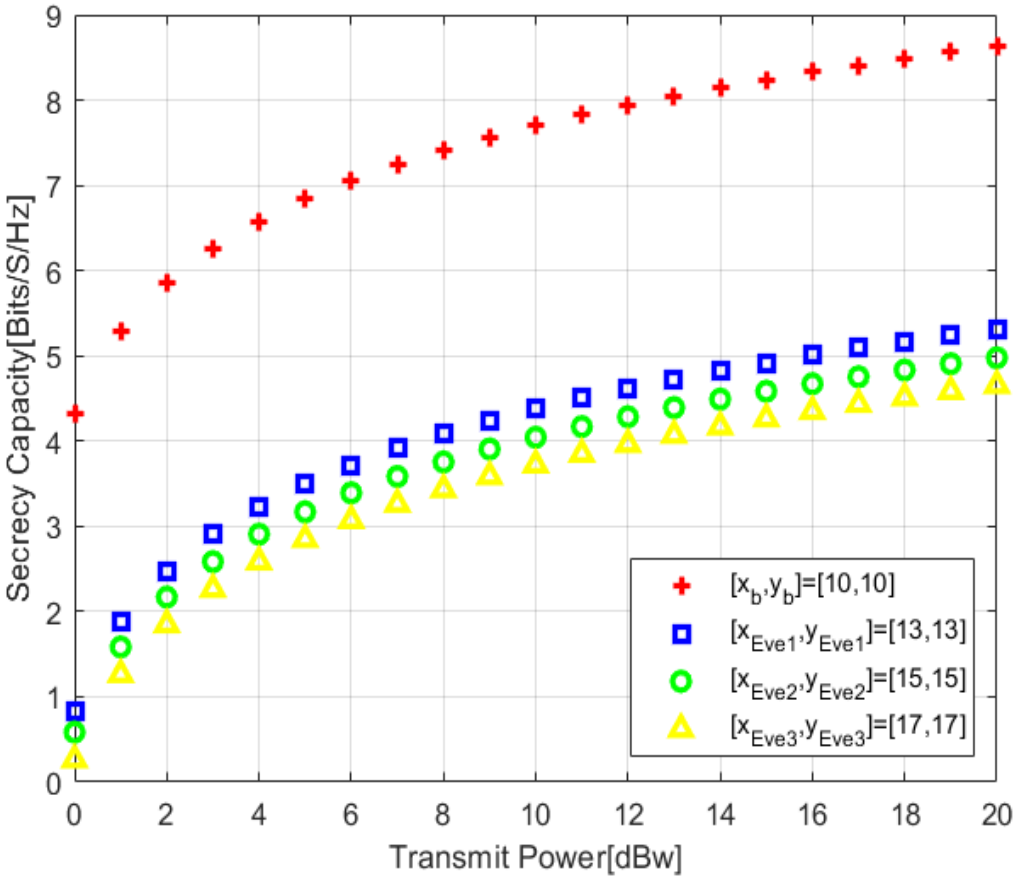
متغیر مستقل در این منحنی‌ها، فاصله هر گره از فرستنده می‌باشد و با توجه به میزان فاصله، ما دارای یک ظرفیت محرمانگی مشخصی هستیم و از این مشاهدات می‌توان نتیجه گرفت که افزایش فاصله گیرنده نسبت به یک گره در شبکه، منجر به کاهش ظرفیت محرمانگی می‌شود. بنابراین می‌توان به این نتیجه رسید که کانال مستقیم فرستنده به گیرنده برای ارسال محرمانه اطلاعات، کانال امنی نخواهد بود زیرا به‌دلیل نزدیکی به شنودگر، ظرفیت محرمانگی پایینی دارد. ولی رله، هم به‌دلیل نزدیکی به فرستنده و هم دوربودن از شنودگر برای ارسال اطلاعات، کانال امنی خواهد بود. بنابراین می‌توان به این نتیجه رسید که دلیل قراردادن رله در مسیر کانال قانونی، افزایش ظرفیت محرمانگی است که هم به افزایش نرخ ارسال کمک می‌کند و هم باعث ایجاد یک کانال امن می‌گردد. در ادامه همین مطلب، موضوع فاصله را با کمک تغییر مختصات مکانی رله نسبت به فرستنده اعمال می‌کنیم.



شکل ۱۸. تاثیر فاصله رله در ظرفیت محرمانگی

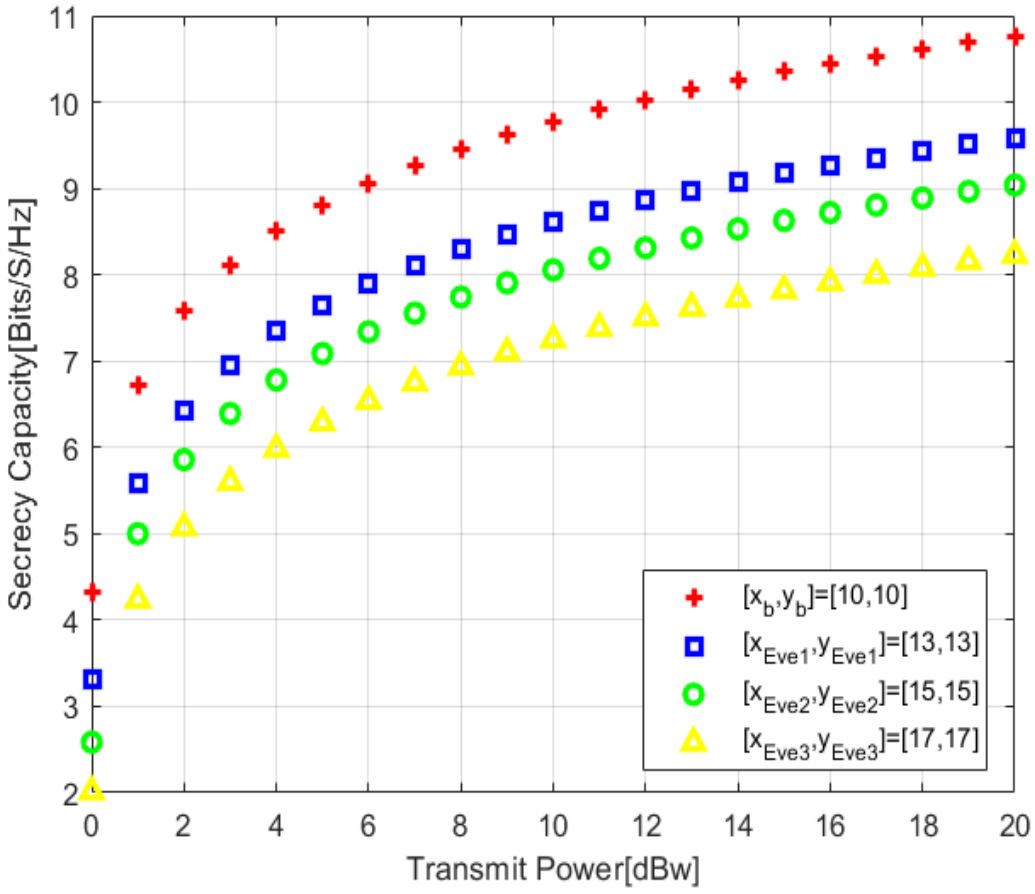
در این منحنی‌ها نیز ظرفیت محرمانگی سه رله و یک شنودگر برحسب توان ارسالی از طرف فرستنده، رسم شده‌اند که با توجه به منحنی‌ها می‌توان به این نتیجه رسید که اولین رله به‌دلیل کمترین فاصله‌ای که با فرستنده دارد، دارای بیشترین ظرفیت محرمانگی است و هرچه این فاصله افزایش یابد، ظرفیت محرمانگی نیز کمتر می‌شود.

تحلیل‌هایی که تا به اینجا مطرح شد فقط ارسال در مرحله اول یعنی از فرستنده به رله را درنظر داشت و هدف فقط تبیین تاثیر فاصله در ارسال اطلاعات بوده‌است.



شکل ۱۹. ظرفیت کانال‌های برآیند

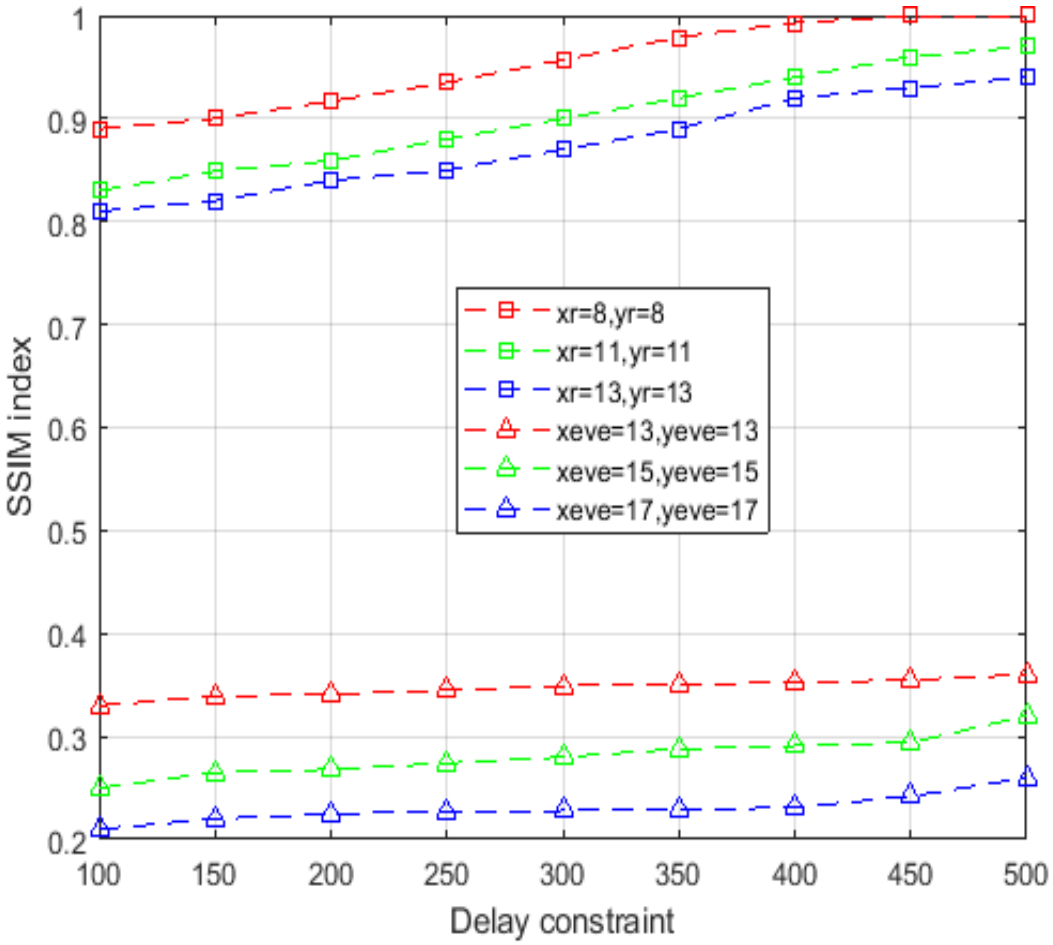
در شکل ۱۱ توان رله برابر با ۱۰ دسی‌بل–وات است و برآیند ظرفیت کانال قانونی در حالتی محاسبه‌شده‌است که مختصات شنودگر در سه حالت متفاوت قرارگرفته‌است. در هر سه حالت با نزدیک‌ترشدن به رله، ظرفیت کانال شنودگر بطور محسوسی افزایش پیدا نمی‌کند و دلیل این موضوع هم ارسال توان از طرف فرستنده می‌باشد. با این اقدام، برآیند ظرفیت کانال قانونی افزایش پیدا کرده اما ظرفیت کانال شنودگر به‌دلیل دوربودن از فرستنده و وجود عامل تلف مسیر بطور قابل‌ملاحظه‌ای افزایش نمی‌یابد. پس ما در هر توانی که فرستنده اعمال می‌کند می‌توانیم با تنظیم نرخی، داده‌های خود را به سمت رله بفرستیم که از ظرفیت شنودگر بیشتر باشد ولی در این شرایط، به اطلاعات خاصی دسترسی پیدا نمی‌کنیم. البته باید به این موضوع توجه داشت که چون شبیه‌سازی براساس روش مونت_کارلو انجام گرفته‌است، این امکان وجود دارد که شنودگر به بخشی از اطلاعات دسترسی پیدا کند اما درمجموع داده‌های بازیابی‌شده در شنودگر مبهم خواهند بود و عملا محرمانگی موردنظر ما برقرار خواهد شد. در ادامه همین موضوع، بررسی می‌کنیم که تغییر توان رله چه تاثیری در محرمانگی ما ایجاد می‌کند.



شکل ۲۰. ظرفیت کانال برآیند با اعمال توان رله

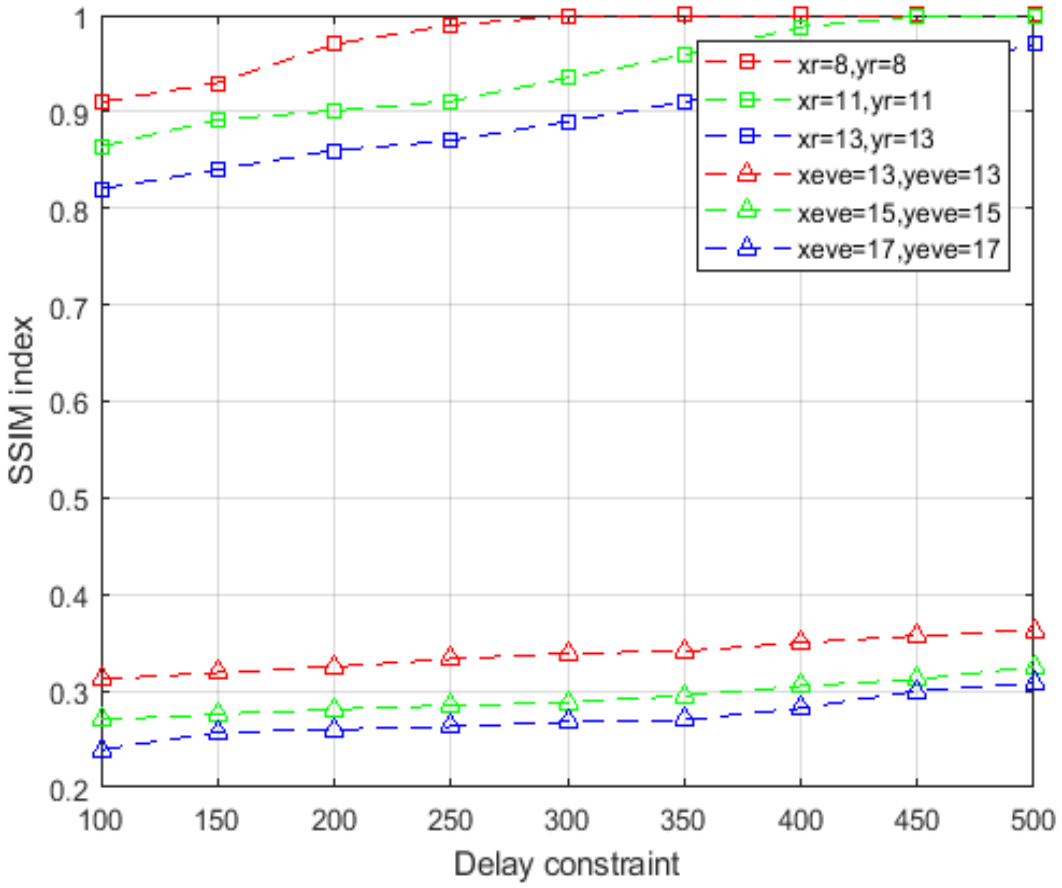
از منحنی‌های تصویر صفحه قبل مشخص است که افزایش توان رله، باعث افزایش ظرفیت شنودگرها می‌شود و البته همانطورکه در بخش قبل هم بیان گردید هر رله‌ای که نزدیک‌تر باشد، بیشتر تحت تاثیر توان قرار می‌گیرد و ظرفیتش بیشتر افزایش پیدا می‌کند. اعمال توان از فرستنده به رله موجب می‌شود ظرفیت کانال قانونی برآیند نسبت به شنودگرهایی که با مختصات مختلف در مسیر رله تا گیرنده قرار دارد، بیشتر باشد و درنتیجه محرمانگی مدنظر ما حاصل شود. با مقایسه و تحلیل دو تصویر قبل می‌توان به این نتیجه رسید که افزایش توان در رله بیشتر به سود شنودگر خواهد بود زیرا ظرفیت آن افزایش پیدا می‌کند. بنابراین بهتر است تا با اعمال توان مناسب در فرستنده و نرخ مناسب نسبت به ارسال اطلاعات اقدام کنیم.

اکنون با استفاده از معیارهای شباهت ساختاری و احتمال نقض کیفیت سرویس (QVP) به بررسی عملکرد پروتکل معرفی‌شده می‌پردازیم. در ابتدا معیار شباهت ساختاری تصویر بازیابی‌شده در گیرنده و شنودگر را بررسی می‌کنیم.



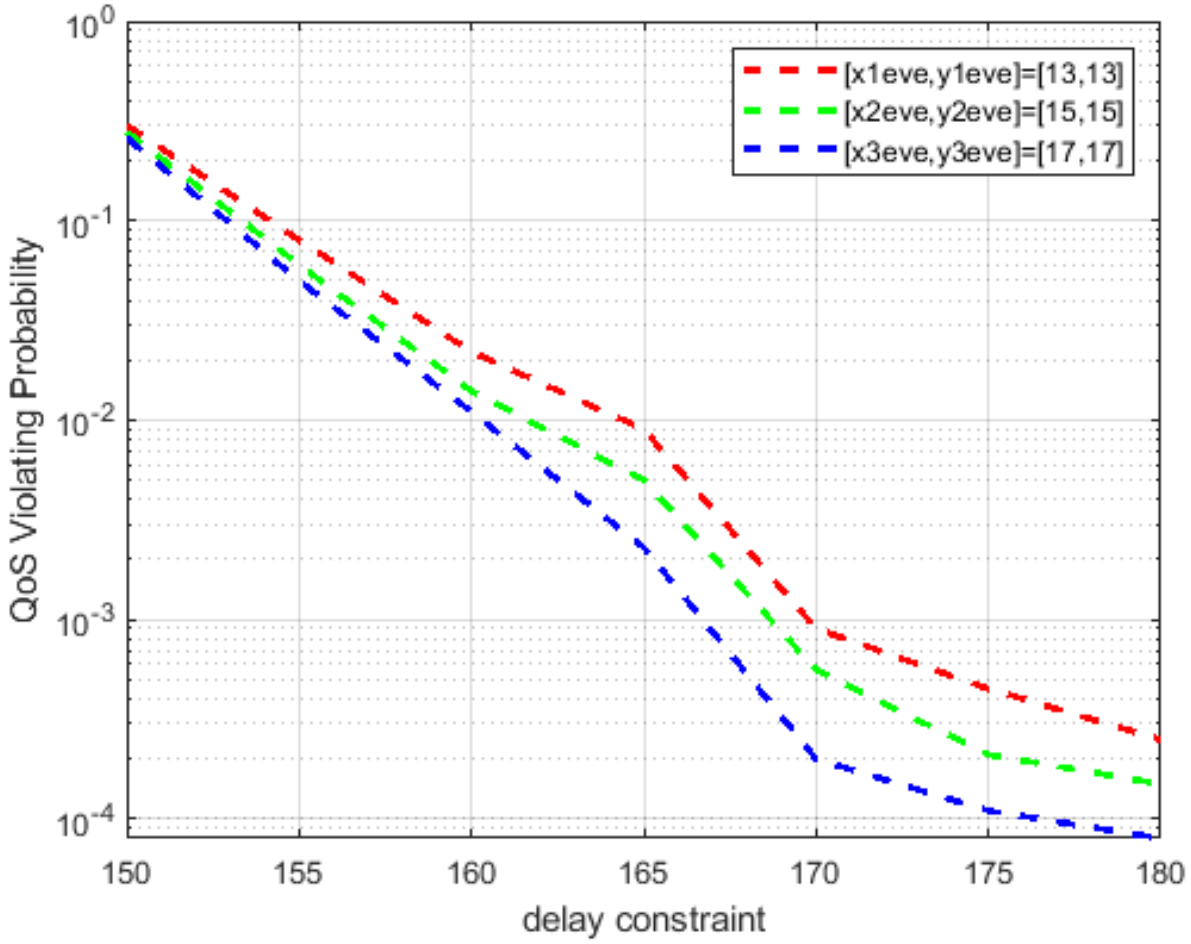
شکل ۲۱. تاثیر فاصله گره‌ها بر روی کیفیت تصویر دریافتی برای توان ارسالی ۱۰ دسی‌بل-وات

در شکل ۱۳ مختصات مکانی دو گره رله و شنودگر را تغییر می‌دهیم تا نتایج را تحلیل کنیم. در این تصویر، منحنی‌های رسم‌شده در قسمت بالا، رله‌هایی با مختصات متفاوت می‌باشند. با نزدیک‌کردن رله به فرستنده متوجه می‌شویم کیفیت تصویر دریافتی افزایش می‌یابد که این نتیجه دریافت سیگنال باکیفیت مرحله اول خواهد بود. البته باید توجه داشت که رله، توانایی افزایش کیفیت تصویر دریافتی در فاز دوم ارسال را ندارد و فقط می‌تواند از کاهش کیفیت تصویر دریافتی در گیرنده جلوگیری کند. زیرا رله از محتوای تصویر اطلاعی ندارد که بتواند آن را بهبود دهد بلکه فقط وظیفه بازارسالی سیگنال دریافت‌شده را برعهده دارد. در قسمت پایین تصویر نیز کیفیت سیگنال دریافتی در شنودگرها مشخص شده‌است. این نکته در مورد شنودگرها نیز صادق است که با نزدیک‌شدن به گره فرستنده و یا رله، سیگنال باکیفیت‌تری دریافت می‌کنند. البته شنودگر در هر حال باز هم نمی‌تواند محتوای اصلی تصویر را دریابد و دلیل این موضوع، همان ارسال سیگنال بر مبنای حداکثر ظرفیت محرمانگی است که باعث می‌شود شنودگر تعداد زیادی از بیت‌های تصویر را از دست بدهد.



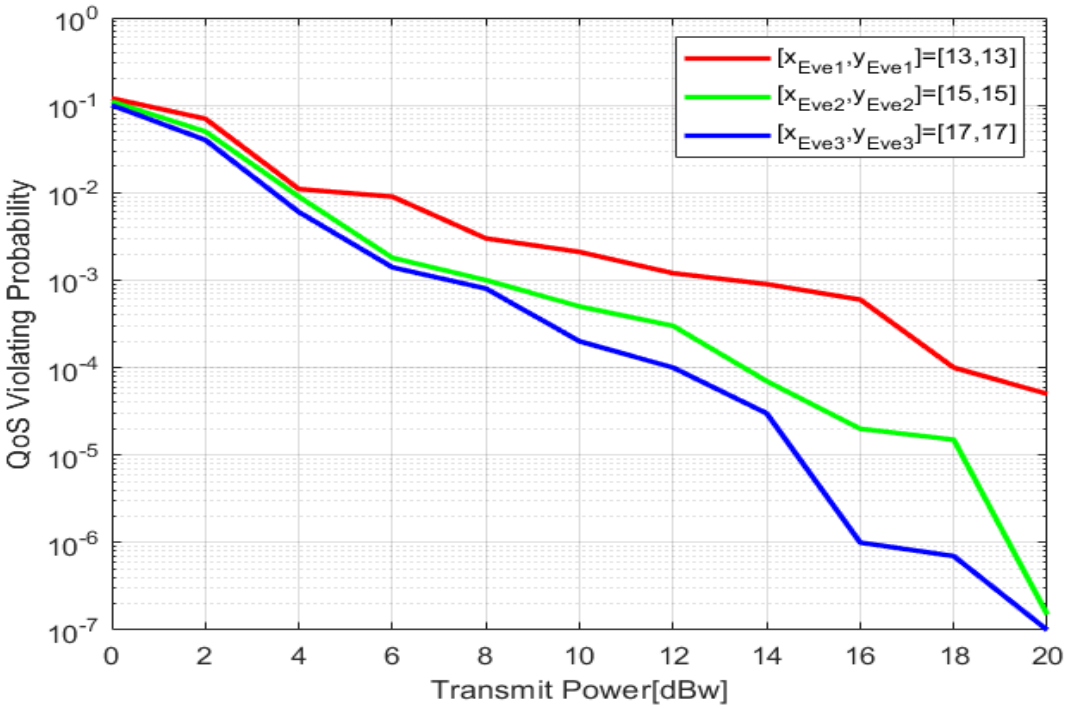
شکل ۲۲. تاثیر فاصله گره‌ها بر روی کیفیت تصویر دریافتی توان ارسالی ۲۰ دسی بل-وات

با افزایش توان سیگنال ارسالی از ۱۰ دسی‌بل-وات به ۲۰ دسی‌بل-وات متوجه می‌شویم که با افزایش زمان برای بازیابی تصویر می‌توانیم سریع از حالت ۱۰ دسی‌بل-وات به تصویری برسیم که ازنظر ساختار، بیشترین شباهت را به تصویر اولیه دارد. دلیل این اتفاق این است که با افزایش توان فرستنده، ظرفیت محرمانگی لینک قانونی افزایش می‌یابد. بنابراین می‌توانیم بسته‌های اطلاعاتی را با نرخ بیشتری ارسال کنیم و این بسته‌ها سریع‌تر به گیرنده برسند. درنتیجه احتمال اینکه به محدودیت تاخیر در ارسال برخورد کنیم، کمتر می‌شود و همین امر باعث می‌گردد تصویر دریافتی در گیرنده به تصویر ارسالی از فرستنده بسیار نزدیک باشد. از طرفی چون نرخ ارسال خود را بالا می‌بریم، شنودگر نیز در هر شنود به بیت‌های بیشتری دسترسی دارد اما چون ظرفیت کمتری دارد امکان شنود تمام بسته‌ها را پیدا نمی‌کند و تصویری که کدگشایی می‌کند به تصویر اولیه نزدیک نمی‌باشد.



شکل ۲۳. تاثیر محدودیت ارسال روی معیار احتمال نقض کیفیت سرویس

از شکل ۱۵ می‌توان برداشت کرد که با افزایش فاصله شنودگر نسبت به فرستنده، ظرفیت کانال قانونی افزایش پیدا خواهد کرد و درنتیجه احتمال نرسیدن بسته‌های اطلاعاتی در اثر محدودیت ارسال کاهش می‌یابد لذا این امر منجر به کاهش احتمال نقض کیفیت سرویس خواهد شد. همچنین افزایش زمان برای بازیابی تصویر، تاثیر مثبتی برای شنودگر ندارد زیرا به همان نسبت که زمان بازیابی اطلاعات افزایش می‌یابد، حجم بسته‌های اطلاعاتی ارسالی در هر بازه زمانی، کاهش می‌یابد و درنتیجه احتمال نقض کیفیت سرویس نیز بسیار پایین خواهد بود. از طرفی به‌دلیل اینکه در رابطه (۱۱) بخش اول آن غالب است درنتیجه افزایش تاخیر قابل‌تحمل سیستم برای بازیابی اطلاعات منجر می‌شود که گیرنده با دشواری و محدودیت زمانی کمتری روبرو گردد و بتواند اکثر بسته‌های اطلاعاتی را بازیابی کند و بخش اول این رابطه کاهش یابد و درنتیجه در کاهش احتمال کل رابطه (۱۷) موثر خواهد بود. در ادامه، تاثیر افزایش توان فرستنده را بر روی معیار QVP بررسی می‌کنیم.

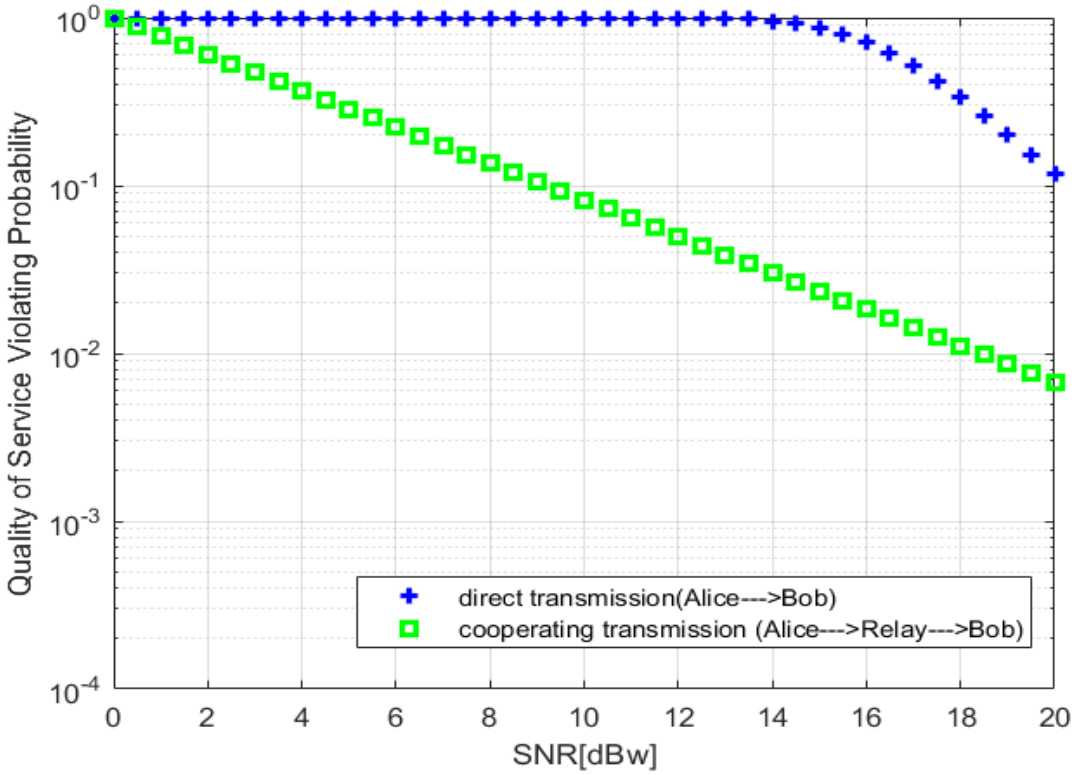


شکل ۲۴. تاثیر افزایش توان فرستنده روی معیار احتمال نقض کیفیت سرویس

این نمودار در حالتی رسم شده‌است که توان رله، ۱۰ دسی‌بل–وات می‌باشد. در منحنی‌های رسم‌شده، مشخص است که با افزایش توان فرستنده یا به عبارتی SNR فرستنده، به‌دلیل افزایش ظرفیت کانال قانونی، احتمال محدودیت تاخیر کاهش می‌یابد و همین امر منجر کاهش احتمال نقض کیفیت سرویس خواهد شد. از طرفی فاصله شنودگر نیز روی کیفیت سیگنال تاثیر می‌گذارد و باعث می‌شود هرچه دورتر باشد، احتمال نقض کیفیت سرویس کاهش‌یابد.

۶) مقایسه با روش‌های پیشین

در این روش پیشنهادی، ارسال تصویر با استفاده از یکی از روش‌های مبتنی بر امنیت لایه فیزیکی یعنی رله مشارکتی انجام شد. همچنن با استفاده از تنظیم توان فرستنده، نرخ ارسال را حداکثر قرار دادیم تا ارسال سریع‌تر صورت گیرد. در بررسی و مقایسه این پروتکل با روش‌های پیشین، شنودگر دسترسی کمتری به اطلاعات تصویر پیدا می‌کند و عملا معیار اندیس شباهت ساختاری در پروتکل پیشنهادی ما، شرایط بهتری دارد. درضمن به‌دلیل ارسال سریع‌تر اطلاعات، معیار احتمال نقض کیفیت سرویس نیز کم می‌شود. علاوه بر این موضوع، در این روش از توان اضافی استفاده نمی‌کنیم و اطلاعات کم‌ارزش‌تر را بطور مستقیم ارسال می‌کنیم تا توان رله استفاده نشود و عملا از توان بطور بهینه بهره می‌بریم. در ادامه استفاده از معیار احتمال نقض کیفیت سرویس روش پیشنهادی خود را با مرجع [۱۵] مقایسه می‌کنیم.



شکل ۲۵. مقایسه معیار qvp در دو حالت ارسال مستقیم و با واسطه رله

۷) نتیجه‌گیری

در این مقاله، یک طرح نوین جهت ارسال امن تصویر با کمک یک رله AF ارائه گردید. در شبیه‌سازی‌ها، ابتدا تاثیر فاصله گره‌های یک شبکه را بر روی ظرفیت محرمانگی مورد بررسی قرار دادیم و به این نتیجه رسیدیم که ارسال در مواقعی که شنودگر با فرستنده فاصله دارد اگر به‌صورت مشارکتی صورت گیرد، مؤثرتر خواهد بود. سپس با افزودن رله به شبکه و محاسبه برآیند کانال‌های قانونی و شنودگر به این نتیجه رسیدیم که افزایش توان فرستنده به‌دلیل اینکه رله در نزدیکی آن قرار دارد، موجب افزایش ظرفیت کانال قانونی و به تبع آن افزایش نرخ ارسال می‌گردد. این افزایش نرخ ارسال، باعث کاهش تاخیر در دریافت اطلاعات شده و درنهایت با بررسی دو معیار اندیس شباهت ساختاری و احتمال نقض کیفیت سرویس، نسبت به عملکرد نتیجه‌بخش رله در کیفیت تصویر دریافتی در گیرنده و همچنین عدم توانایی شنودگر در دسترسی به اطلاعات، اطمینان پیدا کردیم.

منابع

A. A. Alarood, M. Faheem, M. A. Al-Khasawneh, A. I. A. Alzahrani and A. A. Alshdadi, "Secure medical image transmission using deep neural network in e-health applications," *Healthcare Technology Letters*, pp. 87-98, 2023, doi: 10.1109/ICCWorkshops50388.2021.9473492.

A. Chorti *et al.*, "Context-Aware Security for 6G Wireless: The Role of Physical Layer Security," *IEEE Communications Standards Magazine* ,vol. 6, no. 1, pp. 102-108, 2022, doi: 10.1109/MCOMSTD.0001.2000082.

C. Han, L. Sun, and Q. Du, "Securing Image Transmissions via Fountain Coding and Adaptive Resource Allocation," in *2016 IEEE 83rd Vehicular Technology Conference (VTC Spring)*, 15-18 May 2016 2016, pp. 1-5, doi: 10.1109/VTCSpring.2016.7504468.

C. Jiang, H. Zhang, Y. Ren, Z. Han, K. C. Chen, and L. Hanzo, "Machine Learning Paradigms for Next-Generation Wireless Networks," *IEEE Wireless Communications*, vol. 24, no. 2, pp. 98-105, 2017, doi: 10.1109/MWC.2016.1500356WC.

D. Impedovo, . G. Pirlo and . G. Pirlo, "A Medical Image Encryption Scheme for Secure Fingerprint-Based Authenticated Transmission," *applied sciences*, pp. 1-19, 2023, doi: 10.1109/ICCWorkshops50388.2021.9473492.

H. Niu, M. Iwai, K .Sezaki, L. Sun, and Q. Du, "Exploiting Fountain Codes for Secure Wireless Delivery," *IEEE Communications Letters*, vol. 18, no. 5, pp. 777-780, 2014, doi: 10.1109/LCOMM.2014.030914.140030.

L. Mucchi *et al.*, "How 6G Technology Can Change the Future Wireless Healthcare," in *2020 2nd 6G Wireless Summit (6G SUMMIT)*, 17-20 March 2020 2020, pp. 1-6, doi: 10.1109/6GSUMMIT49458.2020.9083916.

L. Sun and H. Xu, "Fountain-Coding-Based Secure Communications Exploiting Outage Prediction and Limited Feedback," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 1, pp. 740-753, 2019, doi: 10.1109/TVT.2018.28858

L. Sun, D. Huang, and A. L. Swindlehurst, "Fountain-Coding Aided Secure Transmission With Delay and Content Awareness," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 7, pp. 7992-7997, 2020, doi: 10.1109/TVT.2020.2992619.

L. Sun, P. Ren, Q. Du, and Y. Wang, "Fountain-Coding Aided Strategy for Secure Cooperative Transmission in Industrial Wireless Sensor Networks," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 1, pp. 291-300, 2016, doi: 10.1109/TII.2015.250944

M. ES-SABRY, N. EL AKKAD, M. MERRAS, K. SATORI, W. EL-SHAFAI, T. ALTAMEEM and M. M. FOUDA, "Securing Images Using High Dimensional Chaotic Maps and DNA Encoding Techniques," *IEEE Access*, vol. 11, pp. 100856-10878, 2023, doi: 10.1109/ICCWorkshops50388.2021.9473492.

M. Letafati, A. Kuhestani, and H. Behroozi, "Three-Hop Untrusted Relay Networks With Hardware Imperfections and Channel Estimation Errors for Internet of Things," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2856-2868, 2020, doi: 10.1109/TIFS.2020.2978627.

M. Letafati, A. Kuhestani, D. W. K. Ng, and H. Behroozi, "A New Frequency Hopping-Aided Secure Communication in the Presence of an Adversary Jammer and an Untrusted Relay," in *2020 IEEE International Conference on Communications Workshops (ICC Workshops)*, 7-11 June 2020 2020, pp. 1-7, doi: 10.1109/ICCWorkshops49005.2020.9145441.

M. Letafati, A. Kuhestani, H. Behroozi, and D. W. K. Ng, "Jamming-Resilient Frequency Hopping-Aided Secure Communication for Internet-of-Things in the Presence of an Untrusted Relay," *IEEE Transactions on Wireless Communications*, vol. 19, no. 10, pp. 6771-6785, 2020, doi: 10.1109/TWC.2020.3006012.

M. Letafati, A. Kuhestani, K. K. Wong, and M. J. Piran, "A Lightweight Secure and Resilient Transmission Scheme for the Internet of Things in the Presence of a Hostile Jammer," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4373-4388, 2021, doi: 10.1109/JIOT.2020.3026475.

M. Letafati, H. Behroozi, B. H. Khalaj, and E. A. Jorswieck, "Content-Based Medical Image Transmission Against Randomly-Distributed Passive Eavesdroppers," in *2021 IEEE International Conference on Communications Workshops (ICC Workshops)*, 14-23 June 2021 2021, pp. 1-7, doi: 10.1109/ICCWorkshops50388.2021.9473492 .

S. B. Baker, W. Xiang, and I. Atkinson, "Internet of Things for Smart Healthcare: Technologies, Challenges, and Opportunities," *IEEE Access*, vol. 5, pp. 26521-26544, 2017, doi: 10.1109/ACCESS.2017.2775180

S. Khan and I. Chatzigeorgiou, "Opportunistic Relaying and Random Linear Network Coding for Secure and Reliable Communication," *IEEE Transactions on Wireless Communications*, vol. 17, no. 1, pp. 223-234, 2018, doi: 10.1109/TWC.2017.2764891.

Y. Lu and L. D. Xu, "Internet of Things) IoT) Cybersecurity Research: A Review of Current Research Topics," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2103-2115, 2019, doi: 10.1109/JIOT.2018.2869847.

Z. Wang and W. Qiu, "Secure Image Transmission over DFT-precoded OFDM-VLC systems based on Chebyshev Chaos scrambling," *Optics Communications*, vol. 397, pp. 84-90, 2017/08/15/ 2017, doi: https://doi.org/10.1016/j.optcom.2017.03.076.