Journal of Electronical & Cyber Defence
Vol. 9, No. 4, 2022, Serial No. 36

The Analysis and Design of Secure Wireless Networks in the Presence of Users with Different Security Needs Based on Covert Communication and Secure Transmission of Information Theory in the Presence of a Friendly Jammer

F. Samsami Khodadad[1], P. Baei[2], M. Forouzesh[3], S. M. J. Asgari Tabatabaee[4]

*Assistant Professor, Faculty of New Technologies Engineering, Amol University of New Technologies, Iran

(Received: 27/01/2021, Accepted: 04/04/2021)

ABSTRACT

In this paper, we investigate the information theory security in conjunction with covert communication on a network in the presence of a single transmitter (Alice), a friendly jammer, a single untrusted user, two legitimate users, and a single channel warden (Willie). In the considered network, one of the authorized users, Bob, needs a secure and covert communication, and therefore his message must be sent securely, and at the same time, the existence of his communication with the transmitter should not be detected by the channel's warden, Willie, Meanwhile, another authorized user, Carol, needs covert communication. The purpose of secure communication is to prevent the message being decoded by the untrusted user who is present on the network, which leads us to use one of the physical layer security methods, named the secure transmission of information theory and also known as the secure capacity of information theory. In some cases, in addition to protecting the content of the message, it is important for the user that, the existence of the transmission is not detected by an adversary, which leads us to covert communication. But as we know, the main problem in covert communication is the low transmission rate, because we have to reduce the transmission power so that the main message gets hidden in the background noise. In this study, in addition to the joint implementation of the security of information theory and the covert communication, we want to examine the average transmission rate according to the limitations and requirements of covert communication and the quality of service requested by users using the power method which is artificial noise creation in the network by a friendly jammer.

Keywords: Secure transmission, Covert Communication, physical layer security, artificial noise, Friendly jammer

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

نشریه علمی "پدافند الکترونیکی و سایبری"
سال نهم، شماره ۴، زمستان ۱۴۰۰، ص ۷۶- ۶۷

علمی– پژوهشی

تحلیل و طراحی شبکه‌های بی‌سیم امن در حضور کاربران با نیازمندی امنیتی متفاوت مبتنی بر مخابره پنهان و ارسال امن تئوری اطلاعاتی در حضور اخلال‌گر دوستانه

فرید صمصامی خداداد[1*]، پویا بائی[2]، مسلم فروزش[3]، سید محمد جواد عسگری طباطبائی[4]

۱- استادیار، ۲- دانشجوی کارشناسی ارشد، دانشکده مهندسی فناوری‌های نوین، دانشگاه تخصصی فناوری‌های نوین آمل، آمل، ۳- استاد مشاور، دانشکده مهندسی برق و کامپیوتر، دانشگاه تربیت مدرس،تهران، ۴-استادیار، دانشگاه تربت حیدریه، تربت حیدریه، ایران

(دریافت: ۱۳۹۹/۱۱/۰۸، پذیرش: ۱۴۰۰/۰۱/۱۵)

چکیده

در این مقاله استفاده توأم از امنیت تئوری اطلاعاتی با مخابره پنهان را در شبکه‌ای در حضور یک فرستنده (Alice)، یک اخلال‌گر دوستانه (Friendly jammer)، یک کاربر غیرقابل‌اعتماد، دو کاربر مجاز و یک ناظر کانال (Willie) مورد بررسی قرار می‌دهیم. در شبکه مورد نظر یکی از کاربران مجاز یعنی کاربر ۱ (Bob) به مخابره امن و پنهان نیاز داشته و بنابراین پیام او باید به صورت امن ارسال شده و در عین حال نباید وجود مخابره وی با فرستنده توسط ناظر کانال آشکارسازی شود، در همین حین کاربر مجاز دیگر یعنی کارول (Carol) به مخابره پنهان نیاز دارد. هدف در مخابره امن جلوگیری از کدگشایی پیام، توسط شنودگر حاضر در شبکه می‌باشد که این امر ما را به سمت استفاده از یکی از روش‌های امنیت لایه فیزیکی یعنی ارسال امن تئوری اطلاعاتی که ظرفیت امن تئوری اطلاعاتی نیز نامیده می‌شود، سوق می‌دهد. همچنین در برخی از موارد علاوه بر محافظت از محتوای پیام، عدم آشکارسازی وجود مخابره توسط دشمن نیز برای کاربر اهمیت دارد، که این امر ما را به سمت مخابره پنهان هدایت می‌کند. اما همان‌طور که می‌دانیم مشکل اصلی در مخابره پنهان، نرخ پایین ارسال می‌باشد، چراکه باید توان ارسال را به میزانی پایین آورد که پیام اصلی در نویز پنهان شود. در این مقاله می‌خواهیم در کنار استفاده توأم از امنیت تئوری اطلاعاتی و مخابره پنهان، به کمک روش توان یعنی ایجاد نویز مصنوعی در شبکه توسط اخلال‌گر دوستانه، نرخ میانگین ارسالی را با توجه به محدودیت‌ها و الزامات مخابره پنهان و همچنین کیفیت سرویس درخواستی کاربران موردبررسی قرار دهیم.

واژگان کلیدی: مخابره امن، مخابره پنهان، امنیت لایه فیزیکی، نویز مصنوعی، اخلال‌گر دوستانه

۱- مقدمه

با توجه به استفاده روزافزون شبکه‌های بی‌سیم در کاربردهای اعم از نظامی و غیرنظامی، ایجاد امنیت در این نوع از شبکه‌ها که به دلیل طبیعت همه پخشی در معرض حملات گوناگونی مانند شنود و تجزیه‌وتحلیل ترافیک قرار دارند، چالشی مهم و حیاتی محسوب می‌شود. بنابراین به اشتراک‌گذاری اطلاعات محرمانه به گونه‌ایی قابل‌اطمینان در حضور دشمنان بسیار مهم می‌باشد. دشمنان ممکن است به‌منظور دستیابی غیرمجاز و یا تغییر اطلاعات و یا حتی ایجاد اختلال در عملکرد شبکه حملات مختلفی را انجام دهند [۱ و ۲]. روش‌های امنیتی نظیر روش‌های رمزگذاری که در لایه‌های بالاتر شبکه مورداستفاده قرار می‌گیرند، به دلیل پیشرفت روزافزون دستگاه‌های محاسباتی شنود به‌طور کامل محرمانه نیستند و این امکان وجود دارد که شنودگر با شکستن کلید رمز (حتی بعد از گذشت چند سال) به محتوای پیام ما دسترسی پیدا کند و این موضوع در برخی شرایط با رویکرد امنیتی بالا مساعد نخواهد بود. با توجه به روش رمزگذاری متقارن مانند استاندارد رمزگذاری داده معمولاً یک کلید اختصاصی مشترک میان دو کاربر به اشتراک گذاشته می‌شود؛ اگر این دو کاربر کلید اختصاصی را نداشته باشند کانال حفاظت‌شده جداگانه‌ای برای تبادل کلید مشترک موردنیاز است. در عوض استفاده از یک کانال اضافی، روش‌های لایه فیزیکی برای اشتراک کلید مخفی مورداستفاده قرار می‌گیرد. استفاده از طرح‌های حفاظت لایه فیزیکی کار دشمنان را برای رمزگشایی اطلاعات انتقال‌یافته مشکل می‌سازد [۳]. روش‌های امنیتی قدیمی بر این پایه بوده‌اند که قدرت محاسباتی شنودگر کم بوده و بنابراین قادر به آشکارسازی کلید مخفی نیست. اما همان‌طور که می‌دانیم تجهیزات ازنظر توانایی محاسباتی رو به رشد می‌باشند. بنابراین روش‌های امنیت تئوری اطلاعاتی[2] ایده‌ای نویدبخش برای امنیت مخابرات بی‌سیم می‌باشد که در آن روش‌های امنیتی اضافی استفاده نمی‌شود [۴]. روش‌های امنیتی قدیمی، حفاظت در مقابل شنود را از طریق رمزگذاری، تضمین

[2] Information theoretic security

*رایانامه نویسنده مسئول: samsami.farid@gmail.com

ناشر: دانشگاه جامع امام حسین (ع)

تمامیت پیام در هوا پیشنهاد می‌کردند. هرچند در سال‌های اخیر نشان داده‌شده است که حتی روش‌های رمزگذاری تقویت‌شده نیز توسط دشمنان قادر به شکست می‌باشند [۵]. روش‌های امنیت لایه فیزیکی[1] با استفاده از مشخصات دینامیکی رسانه بی‌سیم اطلاعات به‌دست‌آمده توسط شنودگر کانال را به حداقل می‌رسانند و این در حالی است که روش‌های امنیت لایه فیزیکی در درجه اول عدم آشکارسازی وجود مخابره میان دو کاربر را فراهم نمی‌کنند [۶]. به طور کلی می‌توان گفت که روش‌های ارسال امن در لایه فیزیکی به ۵ دسته اصلی: ظرفیت امن تئوری اطلاعاتی،روش‌های کانال، کدگذاری، روش‌های توان و روش‌های آشکارسازی سیگنال تقسیم‌بندی می‌شوند [۳]. ارسال امن در لایه فیزیکی معمولاً با استفاده از مفهوم کانال شنود مدل می‌شود. در این مدل فرستنده تلاش می‌کند که با گیرنده مورد نظرش مخابره‌ای امن داشته باشد، به طوری که شنودگر نتواند پیام‌های محرمانه را دریافت نماید. بر طبق بیان وینر، برای برقراری امنیت بدون نیاز به رمزنگاری، باید سیگنال دریافت شده در شنودگر یک نمونه خفیف شده، ضعیف‌تر و غیرقابل آشکارسازی نسبت به سیگنال دریافت شده در گیرنده اصلی باشد، یعنی کانال شنودگر باید نسبت به کانال اصلی نویزی‌تر باشد [۷].

همان‌طور که می‌دانیم، شرایطی وجود دارد که نیاز است ارسال بین فرستنده و گیرنده به صورت پنهان صورت گیرد. به عبارت دیگر، هدف پنهان کردن وجود مخابره بین فرستنده و گیرنده از دید یک ناظر کانال می‌باشد. کاربردهایی برای مخابره پنهان می‌توان نام برد ازجمله: در مخابرات نظامی گاهی لازم است فعالیت فرستنده در ارسال داده در یک منطقه جغرافیایی، از دید شنودگران پنهان شود، چرا که ممکن است دشمن در صورت فهمیدن فعالیت ارسال، عملیاتی را صورت دهد [۸].

جدای از محافظت از محتوای مخابره، مخابره پنهان که معمولاً مخابره با احتمال پایین آشکارسازی نامیده می‌شود سعی دارد تا یک انتقال بی‌سیم را میان دو کاربر تأمین نماید، که درعین‌حال تضمین می‌کند احتمال آشکارسازی این انتقال توسط یک ناظر بسیار کم و قابل‌چشم‌پوشی می‌باشد. چنین مخابره‌هایی برای سیاست مردان و کاربردهای نظامی که به پنهان نگاه‌داشتن مخابره‌های خود از طریق کانال بی‌سیم علاقه دارند بسیار مطلوب می‌باشد. مخابره پنهان در سال‌های اخیر توجهات زیادی را به خود جلب کرده و به‌عنوان یک روش نوین در قالب امنیت مخابرات بی‌سیم ظاهرشده است [۷ و ۸]. در پژوهش‌های [۱۱] و [۱۲] ثابت کرده‌اند برای انتقال امن بدون نیاز به رمزنگاری، در صورتی نرخ ارسال مثبت در دسترس قرار خواهد گرفت که ناظر کانال از توان نویز دریافتی در گیرنده خود قطعیت نداشته باشد. همچنین در [۸] نشان داده‌شده است در صورتی‌که از یک اخلال‌گر کمک بگیریم نرخ ارسال مثبت برای ما در دسترس قرار خواهد گرفت. استراتژی گیرنده کاملاً دوطرفه در بسیاری از پژوهش‌ها ازجمله در [۱۳ و ۱۴] استفاده‌شده است، در این استراتژی گیرنده می‌تواند هم‌زمان با دریافت پیام از منبع، سیگنال‌های پارازیت را به‌منظور گمراه‌سازی متخاصم در باند فرکانسی مشابه ارسال نمایند. در پژوهش‌های [۱۵، ۱۶ و ۶] احتمالات و شرایط مخابره پنهان را در یک کانال محوشدگی گاوسی استاتیک با استفاده از ایجاد نویز ساختگی (AN) که توسط یک گیرنده دوطرفه تولید می‌شود موردبررسی قرارگرفته است که در [۶] سطح مطلوب پنهان بودن با کنترل توان تصادفی نویز مصنوعی[2] قابل‌دستیابی می‌باشد.

در [۱۷] بهبود امنیت توسط اختلال مشارکتی که با کمک سیگنال اختلال ارسالی توسط کاربران و یا گره‌های رله کمک‌کننده به دست می‌آید موردبررسی قرارگرفته است. در [۱۸] امنیت لایه فیزیکی را در حضور متخاصمی که قادر است حالت خود را از شنودگر به حالت اخلال‌گری تغییر دهد موردبررسی قرارگرفته است. در حالت اول که شنودگری نامیده شده است، دشمن سعی در شنود کانال کاربر مجاز را دارد و در حالت دوم که اخلال‌گری نامیده شده است، دشمن به‌منظور گمراه‌سازی گیرنده اصلی سیگنال اختلال ارسال می‌نماید.

در پژوهش [۱۹] نشان داده شد که ارسال سیگنال پارازیت (اختلال) به طور چشمگیری می‌تواند نرخ مخابره پنهان را افزایش دهد، ضمناً اگر بتوانیم بروز اختلال در گیرنده موردنظر (کاربر ۱) را کاهش دهیم، نرخ ارسال در مخابره پنهان بیش از این خواهد بود. در شبکه موردمطالعه در [۱۹] به منظور کاهش اختلال در گیرنده قانونی از یک اخلال‌گر دارای چندین آنتن که از شکل پرتودهی فضای خالی استفاده می‌کند، و یک فرستنده چند آنتنی با آنتن‌های سه‌بعدی که قابلیت پرتودهی به سمت گیرنده موردنظر و به‌طور بالقوه به‌دوراز ناظر کانال دارد به کار گرفته‌شده است.

به طور کلی می‌توان گفت ایجاد اختلال در مقابل شنودگران از آنجایی معرفی شد که نحوه شکل پرتودهی به‌تنهایی به منظور تخریب کانال شنودگر پاسخگوی انتقال امن نبود. ایجاد نویز مصنوعی روشی برای ایجاد اختلال در شبکه می‌باشد که گاهی اوقات می‌تواند توسط فرستنده [۲۰] و یا حتی گیرنده قانونی [۲۱] نیز صورت بپذیرد، اما این روش‌های ایجاد اختلال با توجه

[1] physical layer security

[2] Artificial noise

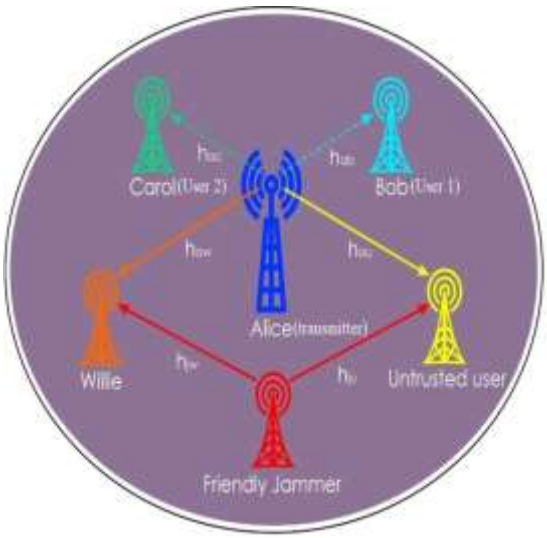
به شرایط کانال و ایجاد خود تداخلی شدید بازدهی شبکه را کاهش می‌دهند [۲۲]. در عوض یک روش مؤثرتر، به‌کارگیری اخلال‌گر دوستانه[1] در شبکه می‌باشد. این اخلال‌گر دوستانه به‌منظور کاهش نسبت سیگنال به نویز به‌علاوه تداخل شنودگر، در عوض هزینه استفاده از انرژی و رابط اضافی، نویز مصنوعی ارسال می‌نماید [۲۳].

در ادامه اهداف اصلی خود در این مقاله را به طور خلاصه تشریح می‌کنیم:

- در این مدل، شبکه‌ای را موردمطالعه قرار خواهیم داد که در آن دو نوع از کاربران مجاز با سطوح امنیتی متفاوت حضور دارند. یکی از این کاربران مجاز به مخابره امن و پنهان و دیگری تنها به مخابره پنهان نیاز دارد.

در این طرح به‌منظور افزایش نرخ میانگین[2]، از یک اخلال‌گر خارجی دوستانه استفاده کرده و تأثیر حضور آن را مورد تحقیق قرار می‌دهیم.

پیکربندی این مقاله در ادامه توضیح داده شده است. در بخش دوم، مدل سیستم پیشنهادی و همچنین الزامات مخابره امن، و مخابره پنهان را مورد بررسی قرار خواهیم داد. در بخش سوم به بیان مسئله بهینه‌سازی پرداخته و راه‌حلی برای آن خواهیم یافت. در بخش چهارم نتایج عددی را ارائه داده و در بخش پنجم از این مقاله نتیجه‌گیری خواهیم داشت.



شکل (۱): مدل سیستم پیشنهادی: انتقال امن و پنهان توأمان در حضور اخلال‌گر دوستانه.

۲- مدل سیستم

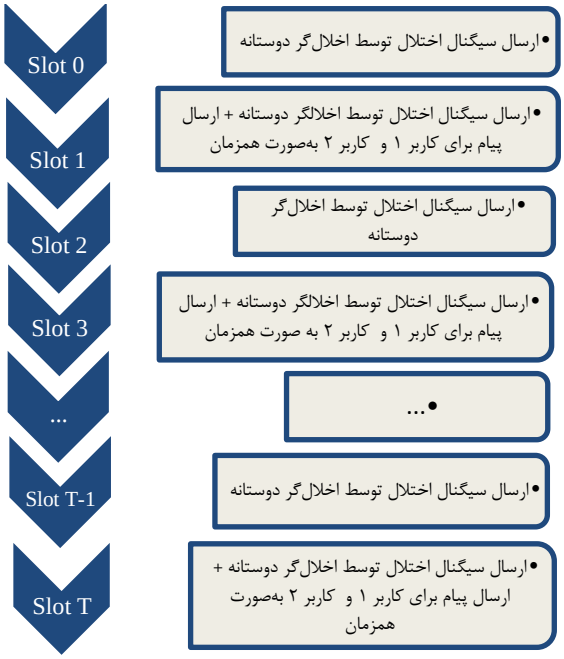
۲-۱- سناریوی مخابره و فرضیات

مدل سیستم در نظر گرفته‌شده، در شکل (۱) نشان داده شده است که شامل یک فرستنده (Alice)، یک کاربر غیرقابل اعتماد، دو کاربر مجاز (Bob) و (Carol)، یک ناظر (Willie) و یک اخلال‌گر دوستانه می‌باشد. لازم به‌ذکر است که ماهیت کاربر غیرمجاز برای شبکه مشخص نبوده و بنابراین می‌تواند شنودگر باشد. فاصله فرستنده (آلیس) و کاربر ۱ (کاربر ۱) ، فرستنده (آلیس) و کاربر ۲ (کارول)، فرستنده (آلیس) و ناظر کانال (ویلی)، فرستنده (آلیس) و کاربر غیرقابل‌اعتماد، اخلال‌گر دوستانه و ناظر کانال (ویلی)، و اخلال‌گر دوستانه و کاربر غیرقابل‌اعتماد به ترتیب d_{ab}، d_{ac}، d_{aw}، d_{au}، d_{jw}، d_{ju} می‌باشد. ضرایب محوشدگی کانال میان فرستنده (آلیس) و کاربر ۱ (باب) ، فرستنده (آلیس) و کاربر ۲ (کارول)، فرستنده (آلیس) و ناظر کانال (ویلی)، فرستنده (آلیس) و کاربر غیرقابل‌اعتماد، اخلال‌گر دوستانه و ناظر کانال (ویلی)، و اخلال‌گر دوستانه و کاربر غیرقابل‌اعتماد به ترتیب h_{ab}، h_{ac}، h_{au}، h_{aw}، h_{jw} و h_{ju} بوده و این کانال‌ها توزیع مختلط گاوسی با میانگین صفر و واریانس یک دارند. در این مقاله فرض شده است که همه ضرایب کانال در یک بازه زمانی ثابت بوده و در بازه دیگر تغییر کرده و از یکدیگر مستقل می‌باشند.

در مدل شبکه پیشنهادی فرض شده است که فرستنده در یک بازه زمانی هیچ ارسالی به دو کاربری که پیام امن و مخابره پنهان نیاز دارند نداشته، و در بازه زمانی دیگری به هر دو ارسال خواهد داشت. ازآنجایی‌که شنودگر کانال منفعل می‌باشد، در شبکه موردنظر فرض شده است که اطلاعات حالت کانال ناظر در دسترس نیست. دلیل منفعل بودن ناظر کانال آن است که در صورت فعال بودن به انجام مخابره پنهان کمک خواهد کرد که این برای او مطلوب نیست. همچنین در این سیستم کانال زمان گسسته با Q بازه زمانی در نظر گرفته‌شده است که طول هرکدام از این بازه‌ها n سمبل می‌باشد. بنابراین بردار سیگنال ارسالی به کاربر ۱ به‌صورت $\mathbf{x_b}=[\mathbf{x_b^1},\mathbf{x_b^2},...,\mathbf{x_b^n}]$ و بردار سیگنال ارسالی به کاربر ۲ به‌صورت $\mathbf{x_c}=[\mathbf{x_c^1},\mathbf{x_c^2},...,\mathbf{x_c^n}]$ بوده و بردار سیگنال ارسالی توسط اخلال‌گر دوستانه موجود در شبکه به کاربر غیرمجاز به‌صورت $\mathbf{x_{ju}}=[\mathbf{x_{ju}^1},\mathbf{x_{ju}^2},...,\mathbf{x_{ju}^n}]$ و بردار سیگنال ارسالی از اخلال‌گر دوستانه به ناظر شبکه به‌صورت $\mathbf{x_{jw}}=[\mathbf{x_{jw}^1},\mathbf{x_{jw}^2},...,\mathbf{x_{jw}^n}]$ بوده، که در آن

[1] Friendly jammer
[2] Average rate

n تعداد سمبل‌های یک بازه زمانی می‌باشد. لازم به ذکر است که آلیس $\mathbf{X_b}$ و $\mathbf{X}_c$ را به خاطر الزامات مخابره پنهان به‌صورت پیوسته ارسال نمی‌کند. شکل (۲) بلوک دیاگرام فرضیه ارسال در شبکه مورد نظر را نشان می‌دهد.



شکل (۲): بلوک دیاگرام فرضیه ارسال فرستنده در شبکه مورد نظر

۲-۲- امنیت تئوری اطلاعاتی

ارسال امن تئوری اطلاعاتی یکی از روش‌های برقراری امنیت در لایه فیزیکی می‌باشد. اساس کار در این‌گونه روش‌ها کاهش احتمال آشکارسازی در گیرنده غیرمجاز یا شنودگر و افزایش احتمال آشکارسازی در گیرنده مجاز می‌باشد. در ارسال امن تئوری اطلاعاتی در گیرنده‌های غیرمجاز یا شنودگران هیچ‌گونه محدودیتی از قبیل توانایی محاسباتی و یا داشتن کلید و کد در نظر گرفته نمی‌شود. همانطور که گفته شد، در این روش هیچ نیازی به پروتکل‌های رمزنگاری نیست و در نتیجه پیچیدگی‌های آن را نخواهد داشت. در ادبیات امنیت لایه فیزیکی به تفاضل ظرفیت کانال اصلی و کانال شنودگر ظرفیت امن گفته می‌شود، نرخ امن به مقدار حداکثر اطلاعات متقابل میان فرستنده و گیرنده مجاز گفته شده و به صورت زیر تعریف می‌شود:

$$C_s = \max\left[I(X;Y) - I(X;Z)\right]^+ \qquad (۱)$$

در معادله فوق $I(.)$ اطلاعات متقابل و $[x]^+ = \max\{x,0\}$ تعریف می‌شود. همچنین x سیگنال ارسالی و Z ،Y سیگنال‌های دریافتی در گیرنده اصلی و شنودگر می‌باشند. با توجه به این رابطه ظرفیت امن[1] را می‌توان به‌صورت زیر نوشت:

$$C_s = \left[C_B - C_E\right]^+ \qquad (۲)$$

که در این رابطه C_B ظرفیت شانون[2] برای گیرنده قانونی و C_E ظرفیت شانون شنودگر می‌باشد.

همان‌طور که گفته شد آنتن فرستنده آلیس در یک بازه زمانی مشخص هیچ ارسالی به هیچ یک از دو کاربر مجاز نداشته و در بازه زمانی دیگری به هر دو کاربر مجاز شبکه یعنی کاربر ۱ که مخابره امن و پنهان و کاربر ۲ (کارول) که به مخابره پنهان نیاز دارد ارسال خواهد داشت. همچنین لازم به‌ذکر است همان‌طور که پیش‌تر گفته شد در شبکه موردنظر از یک اخلال‌گر دوستانه به‌منظور تخریب کانال ناظر شبکه (ویلی) استفاده‌شده و بنابراین نویز ایجادشده توسط اخلال‌گر دوستانه برای کاربران قانونی شبکه یعنی کاربر ۱ و کاربر ۲ (کارول) شناخته‌شده بوده و می‌توانند آن را در گیرنده خود حذف کنند و بنا بر فرضیات فوق بردار سیگنال دریافت شده در هر گره m این شبکه (کاربر ۱، کاربر ۲ (کارول)، کاربر غیرقابل‌اعتماد و ویلی) در هر بازه زمانی به‌صورت زیر خواهد بود:

$$y_m = \begin{cases} \dfrac{\sqrt{p_j}h_{jm}x_j}{d_{jm}^{a/2}} + \mathbf{N_m}, & \psi_0 \\ \dfrac{\sqrt{p_{ab}}h_{am}x_b}{d_{am}^{a/2}} + \dfrac{\sqrt{p_{ac}}h_{am}x_c}{d_{am}^{a/2}} + \dfrac{\sqrt{p_j}h_{jm}x_j}{d_{jm}^{a/2}} + \mathbf{N}_m, & \psi_1 \end{cases} \qquad (۳)$$

که در رابطه فوق p_j ، p_{ab} و p_{ac} به ترتیب توان اخلال‌گر دوستانه، توان انتقال از فرستنده به گیرنده‌ای که مخابره امن (کاربر ۱) و پنهان و گیرنده‌ای که مخابره پنهان می‌خواهد (کارول) می‌باشد، α نماینده تلفات مسیر و $\mathbf{N}_m \sim CN\left(0,\sigma_m^2\right)$ نشان‌دهنده نویز سفید گوسی مختلط اضافه‌شده در گیرنده گره m می‌باشد. در معادله فوق نماد ψ_0 بیانگر این است که فرستنده به گیرنده‌های مجاز در شبکه که مخابره امن و پنهان می‌خواهند ارسالی نداشته و در مقابل ψ_1 بیانگر ارسال پیام در بازه زمانی مشخص می‌باشد. لازم به ذکر است، ازآنجایی‌که فرستنده آلیس تک آنتن می‌باشد، توان ارسالی به هرکدام از گیرنده‌های مجاز شبکه درصدی از توان کل آنتن آلیس را تشکیل می‌دهند و می‌توان به جهت ساده‌سازی روابط، توان ارسالی به کاربر ۲ (کارول) را به‌صورت $p_{ac} = 1 - p_{ab}$ در نظر گرفت و همچنین می‌توان گفت که توان کل انتقال در P محدود شده است که این فرضی معمول در [۲۴] می‌باشد، در ادامه توان اخلال‌گر دوستانه

[1] Secrecy capacity
[2] Shannon capacity

و توان آنتن فرستنده آلیس را برای هر بازه زمانی به‌صورت $\begin{cases} p_j P_{j\max} & \psi_0 \\ 0 & \psi_0 \end{cases}$ و $\begin{cases} p_j P_{j\max} & \psi_1 \\ (p_{ab}+p_{ac})P_{\max}=P_{\max} & \psi_1 \end{cases}$ در نظر می‌گیریم، که در این روابط $p_j, p_{ab} = [0,1]$ می‌باشند و از این فرض در روابط استفاده‌شده است. در ادامه برای محاسبه نسبت سیگنال به تداخل به‌علاوه نویز و به‌منظور ساده‌سازی روابط، متغیر $\gamma_m = \frac{P_{\max}|h_{am}|^2}{\sigma_m^2 d_{am}^{\alpha}}$ را در نظر می‌گیریم. بنابراین نسبت سیگنال به تداخل به‌علاوه نویز در گیرنده کاربر ۱ به‌صورت زیر خواهد بود:

$$\gamma_B^{\ell} = \begin{cases} 0 & \psi_0 \\ \dfrac{p_{ab}\gamma_b}{p_{ac}\gamma_b + 1} & \psi_1 \end{cases} \quad (۴)$$

همچنین نسبت سیگنال به تداخل به‌علاوه نویز در گیرنده کاربر غیرقابل‌اعتماد به صورت زیر خواهد بود:

$$\gamma_U^{\ell} = \begin{cases} p_j\gamma_u & \psi_0 \\ \dfrac{p_{ab}\gamma_u}{p_{ac}\gamma_u + p_j\gamma_j + 1} & \psi_1 \end{cases} \quad (۵)$$

که در رابطه فوق $\gamma_j = \frac{P_{j\max}|h_{ju}|^2}{d_{ju}^{\alpha}\sigma_u^2}$ بوده و در انتها نسبت سیگنال به تداخل به‌علاوه نویز برای کاربری که به مخابره پنهان نیاز دارد یعنی کاربر ۲ (کارول) به‌صورت زیر خواهد بود:

$$\gamma_C^{\ell} = \begin{cases} 0 & \psi_0 \\ \dfrac{p_{ac}\gamma_c}{p_{ab}\gamma_c + 1} & \psi_1 \end{cases} \quad (۶)$$

در انتها نرخ امن یا همان امنیت تئوری اطلاعاتی در گیرنده کاربر ۱ به‌صورت زیر محاسبه خواهد شد:

$$R_{\sec}(\mathbf{P}) = \left[\log_2\left(1+\gamma_B^{\ell}\right) - \log_2\left(1+\gamma_U^{\ell}\right)\right]^+ \quad (۷)$$

در معادله فوق $[x]^+ = \max\{x,0\}$ تعریف‌شده و ماتریس $\mathbf{P}$ شامل درایه‌های p_{ab} و p_j می‌باشد.

۲-۳- مخابره پنهان

معیار ناظر کانال (ویلی) به‌منظور شناسایی وجود مخابره میان دو گره، بر اساس تجزیه‌وتحلیل توان سیگنال دریافت شده در گیرنده خود می‌باشد و بر این اساس در مورد وجود مخابره میان فرستنده (آلیس) و گیرنده موردنظرش (کارول و یا کاربر ۱) تصمیم خواهد گرفت. به‌طور خلاصه می‌توان گفت که ناظر کانال با یک فرضیه باینری مواجه است. زمانی که فرستنده به گیرنده موردنظر ارسال داشته باشد و تصمیم ناظر کانال بر اساس توان سیگنال دریافت شده بر عدم وجود مخابره باشد، آشکارسازی ازدست‌رفته با احتمال p_{MD} خواهیم داشت. همچنین زمانی که فرستنده ارسال پیام به گیرنده موردنظر نداشته باشد اما تصمیم ناظر کانال بر وجود مخابره باشد، هشدار اشتباه با احتمال p_{FA} خواهیم داشت. باید توجه داشت که شرط لازم برای برقراری مخابره پنهان میان دو گره آن است که به ازای هر $\varepsilon \geq 0$ زمانی که $n \to \infty$ شرط زیر برقرار باشد [۸]:

$$for\ any\ \varepsilon \geq 0,\ p_{MD} + p_{FA} \geq 1-\varepsilon \quad as \quad n \to \infty \quad (۸)$$

همچنین قاعده تصمیم‌گیری بهینه در شنودگر برای کاهش خطا ی آشکارسازی به‌صورت زیر خواهد بود [۸]:

$$\begin{cases} \frac{Y_w}{n} < \theta & \psi_0 \\ \frac{Y_w}{n} > \theta & \psi_1 \end{cases} \quad (۹)$$

که در رابطه فوق $Y_w = \sum_{\ell=1}^{n} |y_w^{\ell}|^2$ توان کل دریافت شده در گیرنده ناظر در هر بازه زمانی بوده و θ حد آستانه تصمیم‌گیری ناظر می‌باشد.

در ادامه احتمالات هشدار اشتباه و آشکارسازی از دست‌رفته را محاسبه خواهیم کرد.

۲-۴- احتمال هشدار اشتباه و آشکارسازی ازدست‌رفته

احتمال آشکارسازی ازدست‌رفته و هشدار اشتباه را می‌توانیم به‌ترتیب به صورت زیر محاسبه نماییم:

$$p_{FA} = P\left(\frac{Y_w}{n} > \theta \middle| \Psi_0\right) \quad (۱۰)$$

$$p_{MD} = P\left(\frac{Y_w}{n} < \theta \middle| \Psi_1\right) \quad (۱۱)$$

به‌منظور محاسبه احتمالات فوق، به تابع توزیع احتمال متغیر تصادفی γ_w^{ℓ} نیاز خواهیم داشت. فرض شده محوشدگی در این شبکه توزیع رایلی داشته و بنابراین هر سمبل سیگنال دریافت شده در گیرنده ناظر کانال (ویلی) یعنی y_w^{ℓ} توزیع آماری گاوسی مختلط به‌صورت زیر خواهد داشت:

$$y_w^{\ell} \sim CN\left(0, \sigma_w^2 + \gamma_w^{\ell}\right) \quad (۱۲)$$

که در رابطه فوق داریم:

$$\gamma_w^{\ell} = \begin{cases} p_j P_{j\max} d_{jw}^{-\alpha} |h_{jw}|^2 & \psi_0 \\ P_{\max} d_{aw}^{-\alpha} |h_{aw}|^2 + p_j P_{j\max} d_{jw}^{-\alpha} |h_{jw}|^2 & \psi_1 \end{cases} \quad (۱۳)$$

درنتیجه تابع چگالی احتمال γ_w^{ℓ} به‌صورت زیر خواهد بود:

$$f_{\psi}\left(\gamma_w^{\ell}\right)=\begin{cases}\dfrac{1}{\lambda_b}\times\left(e^{-\frac{\gamma_w^{\ell}}{\lambda_b}}\right) & \gamma_w^{\ell}>0,\psi_0\\ \dfrac{1}{\lambda_a-\lambda_b}\times\left(e^{-\frac{\gamma_w^{\ell}}{\lambda_a}}-e^{-\frac{\gamma_w^{\ell}}{\lambda_b}}\right) & \gamma_w^{\ell}>0,\psi_1\end{cases} \quad (۱۴)$$

که در رابطه فوق $\lambda_a=P_{\max}d_{aw}^{-\alpha}$ و $\lambda_b=p_jP_{j\max}d_{jw}^{-\alpha}$ است. همان‌طور که می‌دانیم جمع n متغیر تصادفی با توزیع مربع خی با دو درجه آزادی، دارای توزیع مربع خی با $2n$ درجه آزادی خواهد بود. با توجه به مطالب فوق، Y_w دارای توزیع مربع خی با $2n$ درجه آزادی خواهد بود. بنابراین خواهیم داشت:

$$p_{FA}=P\left(\frac{Y_w}{n}>\theta|\psi_0\right)=P\left(\left(\sigma_w^2+\gamma_w^{\ell}\right)\frac{\chi_{2n}^2}{n}>\theta|\psi_0\right) \quad (۱۵)$$

$$p_{MD}=P\left(\frac{Y_w}{n}<\theta|\psi_1\right)=P\left(\left(\sigma_w^2+\gamma_w^{\ell}\right)\frac{\chi_{2n}^2}{n}<\theta|\psi_1\right) \quad (۱۶)$$

در روابط فوق، χ_{2n}^2 متغیر تصادفی مربع خی با درجه آزادی $2n$ می‌باشد. اگر $n\to\infty$ باشد و این احتمال را در نظر بگیریم که شرایط کانال به گونه‌ایی است که مخابره پنهان کامل شده است، با توجه به قانون اعداد بزرگ، $\frac{\chi_{2n}^2}{n}$ به سمت ۱ همگرا می‌شود، و با توجه به تئوری همگرایی غالب لبسگو[1]، زمانی که $n\to\infty$ باشد، می‌توانیم $\frac{\chi_{2n}^2}{n}$ را با ۱ جایگزین نماییم. با استفاده از نتایج فوق احتمال‌های هشدار اشتباه و آشکارسازی ازدست‌رفته به‌صورت زیر خواهیم داشت:

$$p_{FA}=\begin{cases}\left(e^{-\frac{\left(\theta-\sigma_w^2\right)}{\lambda_b}}\right) & \theta-\sigma_w^2\ge 0\\ 1 & \theta-\sigma_w^2<0\end{cases} \quad (۱۷)$$

$$p_{MD}=\begin{cases}\dfrac{\left(\lambda_a\right)}{\left(\lambda_a-\lambda_b\right)}\times\left[1-e^{-\frac{\left(\theta-\sigma_w^2\right)}{\lambda_a}}\right]-\cdots & \\ \dfrac{\left(\lambda_b\right)}{\left(\lambda_a-\lambda_b\right)}\times\left[1-e^{-\frac{\left(\theta-\sigma_w^2\right)}{\lambda_b}}\right] & \theta-\sigma_w^2\ge 0\\ 0 & \theta-\sigma_w^2<0\end{cases} \quad (۱۸)$$

[1] Lebesgue's Dominated Convergence Theorem

۲-۵- حد آستانه بهینه تصمیم‌گیری ناظر کانال

ازآنجایی‌که هدف متخاصم حداقل‌سازی $P_{FA}+P_{MD}$ می‌باشد، متخاصم هیچ‌گاه مقدار θ را به‌طوری‌که $\theta<\sigma_w^2$ باشد انتخاب نخواهد کرد، چراکه در چنین حالتی $P_{FA}+P_{MD}=1$ خواهد بود. بنابراین عبارتی برای حالت $\theta>\sigma_w^2$ انتخاب خواهیم کرد. با توجه به مطالب فوق برای به‌دست آوردن حد آستانه بهینه تصمیم‌گیری ناظر کانال θ_{op}، عبارت $\frac{\partial\left(P_{FA}+P_{MD}\right)}{\partial\theta}=0$ را در نظر می‌گیریم و θ بهینه ناظر کانال به‌صورت زیر به دست خواهد آمد:

$$\theta_{op}=\frac{\left(P_{\max}d_{aw}^{-\alpha}\times p_j\ P_{j\max}\ d_{jw}^{-\alpha}\right)}{\left(P_{\max}\ d_{aw}^{-\alpha}-p_jP_{j\max}\ d_{jw}^{-\alpha}\right)}\times\ln\left(\frac{P_{\max}d_{aw}^{-\alpha}}{p_jP_{j\max}d_{jw}^{-\alpha}}\right)+\sigma_w^2 \quad (۱۹)$$

۳- مسئله بهینه‌سازی

در این بخش به‌منظور برآورد مدل شبکه پیشنهادی مسئله بهینه‌سازی را پیشنهاد می‌دهیم که در آن هدف اصلی بیشینه‌سازی نرخ میانگین با توجه به محدودیت‌های توان، کیفیت سرویس و الزامات مخابره پنهان می‌باشد. در بازه‌های زمانی ارسالی در فرستنده آلیس نرخ کل ارسال به‌صورت زیر به دست می‌آید:

$$R_{secT}(p_{ab},p_j)=\log_2\left(1+\frac{p_{ac}\gamma_c}{p_{ab}\gamma_c+1}\right)+\cdots \left[\begin{matrix}\log_2\left(1+\frac{p_{ab}\gamma_b}{p_{ac}\gamma_b+1}\right)-\cdots\\ \log_2\left(1+\frac{p_{ab}\gamma_u}{p_{ac}\gamma_u+p_j\gamma_j+1}\right)\end{matrix}\right] \quad (۲۱)$$

در نتیجه مسئله بهینه‌سازی را به‌صورت زیر تعریف خواهیم کرد:

$$\max_{p_{ab},p_j,t}\ \log_2\left(1+\frac{(1-p_{ab})\gamma_c}{p_{ab}\gamma_c+1}\right)+\cdots \left[\begin{matrix}\log_2\left(1+\frac{p_{ab}\gamma_b}{(1-p_{ab})\gamma_b+1}\right)-\cdots.\\ \log_2\left(1+\frac{p_{ab}\gamma_u}{(1-p_{ab})\gamma_u+p_j\gamma_j+1}\right)\end{matrix}\right] \quad (۲۲)$$

s.t.

$$0\le p_j\le 1 \quad (a-۲۲)$$

$$0\le p_{ab}\le 1 \quad (b-۲۲)$$

$$\left[\log_2\left(1+\gamma_B^{\ell}\right)-\log_2\left(1+\gamma_U^{\ell}\right)\right]\ge R_{Sec}^{\min} \quad (c-۲۲)$$

$$\log_2\left(1+\frac{p_{ac}\gamma_c}{p_{ab}\gamma_c+1}\right)\ge R_{Cov}^{\min} \quad (d-۲۲)$$

$$\min\left(P_{FA}+P_{MD}\right)\geq 1-\varepsilon \qquad \text{(e-۲۲)}$$

با جایگذاری θ_{op} در رابطه (22.e) خواهیم داشت:

$$\left(\frac{\lambda_b}{\lambda_a-\lambda_b}\right)\times\ln\left(\frac{\lambda_b}{\lambda_a}\right)\leq\ln(\varepsilon) \qquad \text{(e-۲۲)}$$

که در رابطه فوق $\lambda_a = P_{\max} d_{aw}^{-\alpha}$ و $\lambda_b = p_j P_{j\max} d_{jw}^{-\alpha}$ بوده و بنابراین فرمول بهینه‌سازی را به‌صورت زیر خواهیم داشت:

$$\max_{p_{ab},p_j,t}\ \log_2\left(1+\frac{(1-p_{ab})\gamma_c}{p_{ab}\gamma_c+1}\right)+\ldots \left[\begin{array}{l}\log_2\left(1+\frac{p_{ab}\gamma_b}{(1-p_{ab})\gamma_b+1}\right)-\ldots.\\ \log_2\left(1+\frac{p_{ab}\gamma_u}{(1-p_{ab})\gamma_u+p_j\gamma_j+1}\right)\end{array}\right] \qquad \text{(۲۲)}$$

$$s.t.$$

$$(22.a),(22.b),(22.c),(22.d)$$

$$\left(\frac{p_j P_{j\max} d_{jw}^{-\alpha}}{P_{\max} d_{aw}^{-\alpha}-p_j P_{j\max} d_{jw}^{-\alpha}}\right)\times\cdots \ln\left(\frac{p_j P_{j\max} d_{jw}^{-\alpha}}{P_{\max} d_{aw}^{-\alpha}}\right)\leq\ln(\varepsilon) \qquad \text{(e-۲۲)}$$

الگوریتم (۱): الگوریتم مقداردهی اولیه پیشنهادی

۱. مقدار اولیه: $\mu=0$ قرار دهید (μ شماره مقدار اولیه می‌باشد)، و مقدار اولیه دلخواه به $p_{ab}(0)$ و $p_j(0)$ اختصاص دهید.

۲. $p_{ab}=p_{ab}(\mu)$ و $p_j=p_j(\mu)$ را تنظیم نمایید.

۳. مسئله بهینه‌سازی (۲۶) را برحسب p_{ab} و p_j حل کرده و نتایج را در $p_{ab}(\mu+1)$ و $p_j(\mu+1)$ ذخیره نمایید.

۴. درصورتی‌که $|R(\mu+1)-R(\mu)|\leq\tau$ شد، (R تابع هدف بوده و τ حد آستانه دلخواه می‌باشد)

الگوریتم متوقف شود.

در غیر این صورت

$K=k+1$ قرار داده و به مرحله دوم بازگردید.

۴- حل مسئله بهینه‌سازی

همان‌طور که مشاهده می‌شود مسئله (۲۲)، و قیدهای (۲۲- c) و (۲۲- b) و (۲۲- e) محدب نبوده و بنابراین به‌منظور حل این مسئله نمی‌توانیم از نرم‌افزارهای حل مسائل بهینه‌سازی محدب مانند CVX استفاده نماییم. به‌منظور محدب سازی قید(۲۲- e)، پس از تغییر متغیر $t=P_{\max} d_{aw}^{-\alpha}-p_j P_{j\max} d_{jw}^{-\alpha}$ و برخی اعمال ریاضی بر روی قید (۲۲- e)، می‌بایست فرمول بهینه‌سازی که در ادامه ذکر شده است حل شود.

$$\max_{p_{ab},p_j,t}\ \log_2\left(1+\frac{(1-p_{ab})\gamma_c}{p_{ab}\gamma_c+1}\right)+\ldots \left[\begin{array}{l}\log_2\left(1+\frac{p_{ab}\gamma_b}{(1-p_{ab})\gamma_b+1}\right)-\ldots\\ \log_2\left(1+\frac{p_{ab}\gamma_u}{(1-p_{ab})\gamma_u+p_j\gamma_j+1}\right)\end{array}\right] \qquad \text{(۲۲)}$$

$$s.t.$$

$$(22.a),(22.b),(22.c),(22.d)$$

$$p_j P_{j\max} d_{jw}^{-\alpha}\times\ln\left(\frac{p_j P_{j\max} d_{jw}^{-\alpha}}{P_{\max} d_{aw}^{-\alpha}}\right)\ldots \qquad \text{(f-۲۲)}$$

$$-t\times\ln(\varepsilon)\leq 0$$

$$P_{\max} d_{aw}^{-\alpha}-p_j P_{j\max} d_{jw}^{-\alpha}\leq t \qquad \text{(h-۲۲)}$$

همچنین به منظور محدب مسئله (22)، و قیدهای (22.c) و (22.d) نیز می‌توانیم از روش تفاضل دو تابع محدب استفاده نماییم. ابتدا تابع بهینه‌سازی را در نظر می‌گیریم، بنابراین خواهیم داشت:

$$\Xi(p_{ab},p_j)=\Gamma(p_{ab},p_j)-\Omega(p_{ab},p_j) \qquad \text{(۲۳)}$$

که در رابطه فوق:

$$\begin{cases}\Gamma(p_{ab},p_j)=\log_2(\gamma_c+1)+\ldots\\ \log_2(\gamma_b+1)+\log_2\left((1-p_{ab})\gamma_u+p_j\gamma_j+1\right)\\ \Omega(p_{ab},p_j)=\log_2(p_{ab}\gamma_c+1)+\ldots\\ \log_2((1-p_{ab})\gamma_b+1)+\log_2(\gamma_u+p_j\gamma_j+1)\end{cases} \qquad \text{(۲۴)}$$

با به‌کارگیری روش DC می‌توانیم رابطه $\Omega(p_{ab},p_j)$ را به‌صورت زیر بازنویسی کنیم:

$$\Omega(p_{ab},p_j)\simeq\tilde{\Omega}(p_{ab},p_j)=\Omega(p_{ab}(\mu-1),p_j(\mu-1))\ldots +\nabla^T\Omega(p_{ab}(\mu-1),p_j(\mu-1))\ldots \times\left[p_{ab}-p_{ab}(\mu-1),p_j-p_j(\mu-1)\right] \qquad \text{(۲۵)}$$

که در رابطه فوق μ مقدار اولیه و $\nabla\Omega(p_{ab},p_j)$ گرادیان $\Omega(p_{ab},p_j)$ بوده و به‌صورت زیر محاسبه می‌شود:

$$\nabla\Omega(p_{ab},p_j)= \left[\begin{array}{l}\frac{P_{\max}|h_{ac}|^2 d_{ac}^{-\alpha}}{(\sigma_c^2+p_{ab}P_{\max}|h_{ac}|^2 d_{ac}^{-\alpha})\ln(2)}-\ldots\\ \frac{P_{\max}|h_{ab}|^2 d_{ab}^{-\alpha}}{(\sigma_b^2+(1-p_{ab})P_{\max}|h_{ac}|^2 d_{ab}^{-\alpha})\ln(2)},\cdots\\ \frac{P_{j\max}|h_{ju}|^2 d_{ju}^{-\alpha}}{(\sigma_u^2+P_{\max}|h_{ac}|^2 d_{ju}^{-\alpha}+p_j P_{j\max}|h_{ju}|^2 d_{ju}^{-\alpha})\ln(2)}\end{array}\right] \qquad \text{(۲۶)}$$

و در نهایت تابع هدف به‌صورت $\Gamma(p_{ab},p_j)-\tilde{\Omega}(p_{ab},p_j)$ نوشته می‌شود. همانند تابع هدف برای تقریب قیدهای (۲۲- c) و (۲۲- d) نیز می‌توان از روش تفاضل دو تابع محدب استفاده نمود. درنتیجه قید (۲۲- c) را به‌صورت زیر خواهیم داشت:

$$\mathrm{T}(p_{ab}, p_j) - \tilde{\Lambda}(p_{ab}, p_j) \geq 0 \quad (۲۷)$$

که در رابطه فوق داریم:

$$\begin{aligned} &\mathrm{T}(p_{ab}, p_j) = \log_2(\sigma_b^2 + P_{\max}|h_{ab}|^2 d_{ab}^{-\alpha}) + ... \\ &\log_2(\sigma_u^2 + (1-p_{ab})P_{\max}|h_{au}|^2 d_{au}^{-\alpha} + ... \\ &p_j P_{j\max}|h_{ju}|^2 d_{ju}^{-\alpha}) - R_{\min \sec} \end{aligned} \quad (۲۸)$$

$$\begin{aligned} &\Lambda(p_{ab}, p_j) = \log_2(\sigma_b^2 + P_{\max}|h_{ab}|^2 d_{ab}^{-\alpha}) + ... \\ &\log_2(\sigma_u^2 + P_{\max}|h_{au}|^2 d_{au}^{-\alpha} + p_j P_{j\max}|h_{ju}|^2 d_{ju}^{-\alpha}) \end{aligned} \quad (۲۹)$$

و همچنین برای قید (22.d) خواهیم داشت:

$$\mathrm{K}(p_{ab}, p_j) - \tilde{\Sigma}(p_{ab}, p_j) \geq 0 \quad (۳۰)$$

که در رابطه (27) داریم:

$$\mathrm{K}(p_{ab}, p_j) = \log_2(\sigma_c^2 + P_{\max}|h_{ac}|^2 d_{ac}^{-\alpha}) - R_{\min \mathrm{cov}} \quad (۳۱)$$

$$\Sigma(p_{ab}, p_j) = \log_2(\sigma_c^2 + p_{ab}P_{\max}|h_{ac}|^2 d_{ac}^{-\alpha}) \quad (۳۲)$$

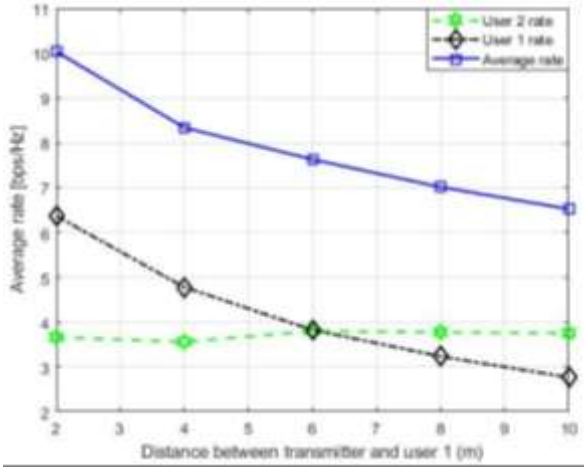
همچنین لازم به ذکر است که $\tilde{\Lambda}$ و $\tilde{\Sigma}$ همانند رابطه (25) محاسبه می‌شوند. در انتها مسئله بهینه‌سازی زیر را می‌توانیم با استفاده از تولباکس‌های حل مسائل محدب همانند CVX حل نماییم.

$$\max_{P_{ab}, P_j, t} \left(\Gamma(p_{ab}, p_j) - \tilde{\Omega}(p_{ab}, p_j)\right) \quad (۳۳)$$

$$s.t.: \\ (22.a), (22.b), (22.f), (22.h), (27), (30)$$

۵- نتایج عددی و شبیه‌سازی

در این بخش نتایج عددی به منظور بررسی عملکرد شبکه پیشنهادی ارائه شده‌اند و برای ارزیابی روش پیشنهادی از شبیه سازی مونت کارلو استفاده می‌کنیم. پارامترهای شبیه‌سازی در مدل سیستم در نظر گرفته شده در جدول (۱) ارائه شده است. در این بخش سعی داریم نحوه عملکرد سیستم را با توجه به تغییر فواصل کاربران از فرستنده و تأثیر افزایش توان فرستنده زمانی که کاربران در فاصله‌ای ثابت از فرستنده قرار دارند، نشان دهیم. در انجام این شبیه‌سازی‌ها کانال میان کاربران اعم از کاربران مجاز و غیرمجاز به صورت تصادفی با توزیع مختلط گوسی با میانگین صفر و واریانس ۱ در نظر گرفته شده است که در یک بازه زمانی ارسال ثابت بوده و در بازه زمانی دیگر تغییر می‌کنند و از یک‌دیگر مستقل هستند. همچنین تلفات مسیر و اثرات محوشدگی کانال نیز با پارامتر α مدل شده‌اند. $R_{Sec}^{\min}$ و $R_{Cov}^{\min}$ حداقل میزان نرخ درخواستی کاربران مجاز شبکه یعنی کاربر ۱ و کاربر ۲ (کارول) می‌باشد که با توجه به نیازمندهای امنیتی این دو کاربر و شرایط مخابره امن و مخابره پنهان باید تأمین گردند. $P_{\max}$ و $P_{j\max}$ حداکثر توان ارسالی توسط آنتن فرستنده آلیس می‌باشد که گره کنترل‌کننده شبکه با توجه به کیفیت سرویس درخواستی کاربران مجاز شبکه و شرایط کانال و فواصل کاربران توان اختصاص یافته به هر کاربر را به صورت هوشمند کنترل می‌نماید.

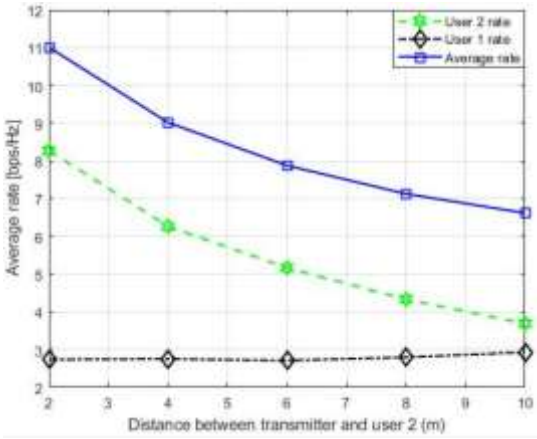


شکل (۱): تأثیر فاصله کاربر ۱ (باب) از فرستنده (آلیس) بر نرخ میانگین ارسالی

جدول (۱): پارامترهای شبیه‌سازی

$1-\varepsilon$	کران پایینی احتمال خطای آشکارسازی ویلی	
d_{ab}	فاصله آلیس و گیرنده کاربر ۱ (باب) برحسب m	۱۰ m
d_{ac}	فاصله میان آلیس و گیرنده کاربر ۲ (کارول)	۱۰ m
d_{au}	فاصله میان آلیس و کاربر غیرقابل‌اعتماد	۱۰ m
d_{aw}	فاصله میان آلیس و گیرنده ویلی	۱۰ m
d_{ju}	فاصله میان اخلال‌گر دوستانه و کاربر غیرقابل‌اعتماد	۱۰ m
d_{jw}	فاصله میان اخلال‌گر دوستانه و کاربر غیرقابل‌اعتماد	۱۰ m
$R_{Sec}^{\min}$	کیفیت سرویس[1] کاربر ۱ برحسب [bps/Hz]	۰/۵
$R_{Cov}^{\min}$	کیفیت سرویس کاربر ۲ (کارول) برحسب [bps/Hz]	۰/۱
α	المان تلفات مسیر	۲
σ_m^2	واریانس هر گره برحسب dBW	-۳۰
$P_{j\max}$	توان کل اخلال‌گر دوستانه برحسب dBW	۴
$P_{\max}$	توان کل آنتن آلیس برحسب dBW	۲

[1] Quality of Service

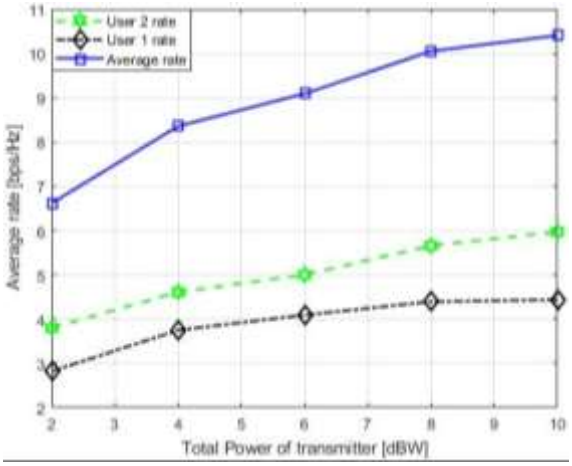


شکل (۲): تأثیر فاصله کاربر ۲ (کارول) از فرستنده (آلیس) بر نرخ میانگین ارسالی

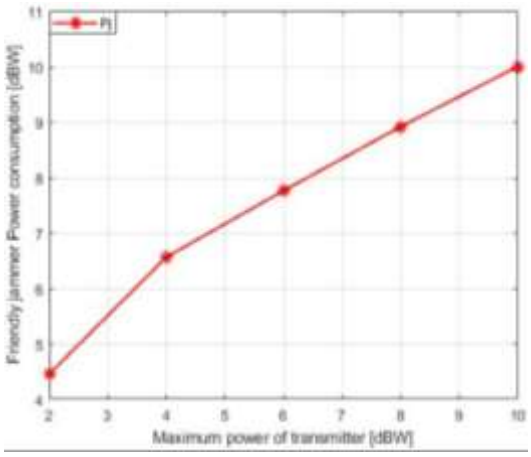
شکل (۳) تأثیر فاصله کاربر ۱ (باب) از فرستنده را نمایش می‌دهد. مشاهده می‌شود که با افزایش فاصله کاربر ۱ (باب) از فرستنده (آلیس) نرخ میانگین شبکه کاهش می‌یابد. همچنین این شکل بیان‌گر نرخ ارسال‌شده جداگانه برای کاربر ۱ (باب) و کاربر ۲ (کارول) می‌باشد. همان‌طور که مشاهده می‌شود در هیچ یک از این فواصل نرخ هیچ‌کدام از کاربران صفر نشده، و حداقل کیفیت سرویس درخواستی آن‌ها نیز تأمین‌شده است.

شکل (۴) بیان‌گر تأثیر فاصله کاربر ۲ (کارول) از فرستنده (آلیس) بر نرخ میانگین بوده و همچنین نرخ ارسال‌شده جداگانه برای کاربران مجاز شبکه را نشان می‌دهد. همچنین با مقایسه این نمودار با نمودار (۳) می‌توان نتیجه گرفت که تأثیر فاصله کاربر ۲ (کارول) از فرستنده (آلیس) بر نرخ میانگین بیشتر از تأثیر فاصله کاربر ۱ (باب) از فرستنده می‌باشد.

شکل (۵) نماینده تأثیر افزایش توان بیشینه ارسالی فرستنده می‌باشد. با افزایش توان ارسالی فرستنده نرخ میانگین شبکه با توجه به الزامات مخابره پنهان و امنیت تئوری اطلاعاتی تا ۶۰٪ افزایش می‌یابد. در این نمودار توان بشینه قابل استفاده برای اخلال‌گر تا dBW ۱۰ در نظر گرفته شده است.



شکل (۳): تأثیر افزایش توان بیشینه فرستنده، $P_{j\max} = 10dBW$



شکل (۴): توان مصرفی اخلال‌گر دوستانه در مقایسه با توان کل فرستنده

شکل (۶) میزان توان بیشینه ارسالی در اخلال‌گر دوستانه با توجه به توان بیشینه فرستنده را نشان می‌دهد. همان‌طور که مشاهده می‌شود سیستم به‌صورت هوشمند توسط گره کنترل‌کننده مرکزی شبکه توان بیشینه اخلال‌گر دوستانه را با توجه به توان بیشینه ارسالی فرستنده و الزامات مخابره امن و پنهان و فاصله از کاربران اعم از مجاز و غیرمجاز تنظیم می‌کند. همان‌طور که مشاهده می‌شود با افزایش توان بیشینه فرستنده توان اخلال‌گر دوستانه توسط گره کنترل‌کننده شبکه افزایش می‌یابد.

۶- نتیجه‌گیری

در این مقاله امنیت تئوری اطلاعاتی توأم با مخابره پنهان را با توجه به نیازمندی‌های متفاوت امنیتی کاربران حاضر در شبکه در حضور اخلال‌گر دوستانه موردبررسی قراردادیم. در شبکه مورد تحقیق، دو کاربر مجاز که یکی از آن‌ها مخابره امن و پنهان (کاربر ۱) و دیگری به مخابره پنهان (کاربر ۲) نیاز دارد حضور دارند. در این شبکه فرض شده است که فرستنده (آلیس) در یک بازه زمانی به هیچ یک از دو کاربران ارسالی نداشته و در بازه زمانی دیگر به هر دو کاربر مجاز شبکه به صورت هم‌زمان ارسال خواهد داشت. برای سیستم مورد نظر مسئله بهینه‌سازی پیشنهاد دادیم که در آن هدف ما بیشینه‌سازی نرخ میانگین شبکه با توجه به الزامات مخابره پنهان و امنیت تئوری اطلاعاتی و همچنین تأمین کیفیت سرویس درخواستی کاربران هست. از آنجایی که این مسئله بهینه‌سازی محدب نبوده است، از روش تقریب محدب به منظور محدب‌سازی مسئله بهینه‌سازی استفاده کردیم. نتایج شبیه‌سازی تأثیر افزایش فواصل کاربران مجاز شبکه از فرستنده و همچنین تأثیر افزایش توان ارسالی فرستنده را بر نرخ میانگین شبکه نشان دادند. همچنین مشاهده شد که شبکه به صورت هوشمند توان مصرفی در اخلال‌گر دوستانه را با توجه به شرایط شبکه و توان ارسالی فرستنده تنظیم می‌نماید.

۷- مراجع

[1] C. S. R. Murthy and B. S. Manoj, Ad hoc wireless networks: architectures and protocols. 2004.

[2] F. Samsami Khodadad and G. A. Hodtani, "Detection of Spread Spectrum multi-user direct Sequence Signals with the help of Information Theory criteria," J. Electron. Cyber Def., vol. 2, no. 1, 2014 (in Persian).

[3] Y. S. Shiu, S. Y. Chang, H. C. Wu, S. C. H. Huang, and H. H. Chen, "Physical layer security in wireless networks: A tutorial," IEEE Wirel. Commun., vol. 18, no. 2, pp. 66–74, 2011, doi: 10.1109/MWC.2011.5751298.

[4] N. Yang, S. Yan, J. Yuan, R. Malaney, R. Subramanian, and I. Land, "Artificial noise: Transmission optimization in multi-input single-output wiretap channels," IEEE Trans. Commun., vol. 63, no. 5, 2015, doi: 10.1109/TCOMM.2015.2419634.

[5] M. Bloch and J. Barros, Physical–layer security: From information theory to security engineering, vol. 9780521516. 2011.

[6] J. Hu, K. Shahzad, S. Yan, X. Zhou, F. Shu, and J. Li, "Covert Communications with a Full-Duplex Receiver over Wireless Fading Channels," in IEEE International Conference on Communications, 2018, vol. 2018-May, doi: 10.1109/ICC.2018.8422941.

[7] A. D. Wyner, "The Wire- Tap Channel," Bell Syst. Tech. J., vol. 54, no. 8, 1975, doi: 10.1002/j.1538-7305.1975.tb02040.x.

[8] T. V. Sobers, B. A. Bash, S. Guha, D. Towsley, and D. Goeckel, "Covert Communication in the Presence of an Uninformed Jammer," in IEEE Transactions on Wireless Communications, 2017, vol. 16, no. 9, doi: 10.1109/TWC.2017.2720736.

[9] B. A. Bash, D. Goeckel, D. Towsley, and S. Guha, "Hiding information in noise: Fundamental limits of covert wireless communication," in IEEE Communications Magazine, 2015, vol. 53, no. 12, pp. 26–31, doi: 10.1109/MCOM.2015.7355562.

[10] M. R. Bloch, "Covert Communication over Noisy Channels: A Resolvability Perspective," in IEEE Transactions on Information Theory, 2016, vol. 62, no. 5, doi: 10.1109/TIT.2016.2530089.

[11] S. Lee, R. J. Baxley, M. A. Weitnauer, and B. Walkenhorst, "Achieving undetectable communication," IEEE J. Sel. Top. Signal Process., vol. 9, no. 7, 2015, doi: 10.1109/JSTSP.2015.2421477.

[12] B. He, S. Yan, X. Zhou, and V. K. N. Lau, "On covert communication with noise uncertainty," IEEE Commun. Lett., vol. 21, no. 4, 2017, doi: 10.1109/LCOMM.2016.2647716.

[13] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," IEEE Trans. Signal Process., vol. 61, no. 20, 2013, doi: 10.1109/TSP.2013.2269049.

[14] M. Abedi, N. Mokari, H. Saeedi, and H. Yanikomeroglu, "Secure robust resource allocation using full-duplex receivers," 2015, doi: 10.1109/ICCW.2015.7247229.

[15] M. Duarte, C. Dick, and A. Sabharwal, "Experiment-driven characterization of full-duplex wireless systems," IEEE Trans. Wirel. Commun., vol. 11, no. 12, 2012, doi: 10.1109/TWC.2012.102612.111278.

[16] D. Bharadia, E. McMilin, and S. Katti, "Full duplex radios," 2013, doi: 10.1145/2486001.2486033.

[17] L. Wang, Y. Cai, Y. Zou, W. Yang, and L. Hanzo, "Joint Relay and Jammer Selection Improves the Physical Layer Security in the Face of CSI Feedback Delays," IEEE Trans. Veh. Technol., vol. 65, no. 8, 2016, doi: 10.1109/TVT.2015.2478029.

[18] M. Forouzesh, P. Azmi, and N. Mokari, "Reduce impact of false detection of adversary states on the secure cooperative network," 2017, doi: 10.1109/ISTEL.2016.7881822.

[19] M. Forouzesh, P. Azmi, N. Mokari, and D. Goeckel, "Covert Communication Using Null Space and 3D Beamforming: Uncertainty of Willie's Location Information," IEEE Trans. Veh. Technol., vol. 69, no. 8, pp. 8568–8576, 2020, doi: 10.1109/TVT.2020.2997074.

[20] Y. Wen, Y. Huo, L. Ma, T. Jing, and Q. Gao, "A Scheme for Trustworthy Friendly Jammer Selection in Cooperative Cognitive Radio Networks," IEEE Trans. Veh. Technol., vol. 68, no. 4, 2019, doi: 10.1109/TVT.2019.2895639.

[21] S. Sharifian, F. Lin, and R. Safavi-Naini, "Secret key agreement using a virtual wiretap channel," 2017, doi: 10.1109/INFOCOM.2017.8057119.

[22] K. Cumanan et al., "Physical Layer Security Jamming: Theoretical Limits and Practical Designs in Wireless Networks," IEEE Access, vol. 5, 2017, doi: 10.1109/ACCESS.2016.2636239.

[23] K. Cumanan, Z. Ding, M. Xu, and H. V. Poor, "Secure multicast communications with private jammers," in IEEE Workshop on Signal Processing Advances in Wireless Communications, SPAWC, 2016, vol. 2016-August, doi: 10.1109/SPAWC.2016.7536824.

[24] L. Wang, M. Elkashlan, J. Huang, N. H. Tran, and T. Q. Duong, "Secure transmission with optimal power allocation in untrusted relay networks," IEEE Wirel. Commun. Lett., vol. 3, no. 3, 2014, doi: 10.1109/WCL.2014.031114.140018.