Security of UAV Relay Networks based on Covert Communication in the Presence of an Eavesdropping UAV

V. R. Soltaninia , S. Talati*, M. R. Hasani Ahangar, P. Baei, F. Samsami Khodadad

* Instructor, Shahid Sattari University of Aviation Sciences and Technology, Tehran, Iran

(Received: 29/06/2022, Accepted: 24/12/2022)

ABSTRACT

This paper proposes the use of a trusted decoder and forward (DF) Unmanned Aerial Vehicle (UAV) relay to establish a covert communication between a terrestrial transmitter (Alice) and a receiver (Bob), which is located in a remote area outside the allowable transmitting radius of Alice. The terrestrial transmitter uses the Maximum Ratio Transmission (MRT) technique and several antennas to send the covert signal, and also the UAV relay operates in a Full-Duplex frequency band so that in addition to relaying Alice's signal message to Bob, it also sends disturbance signals to increase the covert transmission detection error by the eavesdropping UAV. In this paper, the source-based jamming scheme (SBJ) is used to avoid the need of using an external jammer in the network. First, the covert transmission conditions in the mentioned network have been investigated and the optimal detection thresholds of the eavesdropping UAV have been obtained with respect to the terrestrial transmitter and the UAV relay. In the simulations, the effects of using multiple antennas at the transmitter as well as the location of the eavesdropping UAV have been investigated to indicate the effectiveness of the proposed covert communication relay scheme with the help of a UAV relay.

Keywords: Wireless Networks, UAV relay, Ad-hoc Networks, Covert Communication, Multiple Antennas.

* Corresponding Author Email: Saeed.talati@yahoo.com

نشریه علمی "پدافند الکترونیکی و سایبری"

سال یازدهم، شماره ۲، تابستان ۱۴۰۲، ص۴۵-۵۶

علمی – پژوهشی

امنیت در شبکه‌های پهپاد رله مبتنی بر مخابرهٔ پنهان با حضور پهپاد شنودگر

وحیدرضا سلطانی‌نیا[۱]، سعید طلعتی[۲*]، محمدرضا حسنی آهنگر[۳]، پویا بائی[۴]، فرید صمصامی خداداد[۵]

۱- دانشجوی دکترا، ۲- مربی، دانشگاه علوم و فنون هوایی شهید ستاری، ۳- استاد، دانشگاه جامع امام حسین(ع)، تهران، ٤- کارشناسی ارشد، ٤- استادیار، مدیر پژوهش و فناوری، دانشگاه تخصصی فناوری های نوین آمل، آمل، ایران

(دریافت: ۱۴۰۱/۰۴/۰۸، پذیرش: ۱۴۰۱/۰۶/۱۵)

چکیده

در این مقاله استفاده از یک پهپاد رله قابل‌اعتماد کدگشا و انتقال‌دهنده (DF[۱]) به‌منظور برقراری مخابره پنهان میان یک فرستنده (آلیس) و یک گیرنده‌ای (باب) که در منطقه‌ای دورافتاده و خارج از شعاع مجاز ارسالی آلیس قرار دارد، پیشنهادشده است. فرستندهٔ زمینی از فن حداکثر نسبت انتقال (MRT[۲]) و چندین آنتن برای ارسال سیگنال پیام استفاده می‌کند و همچنین پهپاد رله در حالت کاملاً دوطرفه[۳] کار می‌کند، به‌گونه‌ای که در کنار رله کردن سیگنال پیام آلیس به سمت باب، به‌منظور افزایش خطای آشکارسازی مخابرهٔ پنهان توسط پهپاد شنودگر، سیگنال اختلال نیز ارسال می‌نماید. در این مقاله طرح جمینگ مبتنی بر منبع (SBJ[۴]) به کار گرفته‌شده است تا نیاز به استفاده یک اخلال‌گر (جَمر) جداگانه در شبکه جلوگیری شود. ابتدا شرایط مخابرهٔ پنهان در شبکهٔ مذکور مورد بررسی قرار گرفته است و حد آستانه‌های بهینهٔ آشکارسازی پهپاد شنودگر با توجه به فرستندهٔ زمینی و همچنین پهپاد رله به‌دست‌آمده است. در شبیه‌سازی‌ها تأثیرات به‌کارگیری چندین آنتن در فرستنده و همچنین مکان پهپاد شنودگر مورد بررسی قرار گرفته است تا بیانگر اثربخشی طرح ارائه‌شدهٔ رلهٔ مخابره پنهان با کمک پهپاد رله باشد.

کلیدواژه‌ها: شبکه‌های بی‌سیم، پهپاد رله، شبکه‌های ad-hoc، مخابرهٔ پنهان، چندین آنتن

۱- مقدمه

امروزه پهپادها به دلیل تحرک‌پذیری بالا، مقرون‌به‌صرفه بودن، سهولت در به‌کارگیری و همچنین دارابودن لینک‌های دید مستقیم که کیفیت بالاتری نسبت به ایستگاه‌های زمینی ارائه می‌دهند برای به‌کارگیری و رفع نیازهای مختلف در شبکه‌های مخابراتی بی‌سیم به‌شدت موردتوجه قرار دارند. درحالی‌که می‌توان اذعان کرد که پهپادها دارای طیف گسترده‌ای از کاربردها از جمله کاربردهای نظامی، نظارتی و مراقبی هستند، برقراری مخابرهٔ بی‌سیم به کمک پهپاد به‌ویژه درزمانی که زیرساخت موجود ازکارافتاده باشد، به‌عنوان عامل کلیدی برای بسیاری از عملیات‌ها مانند عملیات نجات موردتوجه قرار گرفته‌اند. باوجود تمامی موارد گفته‌شده در مورد بهینه بودن استفاده از پهپادها، باید اعتراف کرد که شبکه‌های مخابراتی پهپاد نیز مانند هر شبکهٔ مخابراتی بی‌سیم دیگر به دلیل طبیعت همه پخشی این شبکه‌ها در برابر حملاتی نظیر سرقت اطلاعات مهم که از سوی شنودگران سوءاستفاده‌گر و همچنین در مناطق جنگی از سوی دشمن صورت می‌گیرد آسیب‌پذیر هستند.

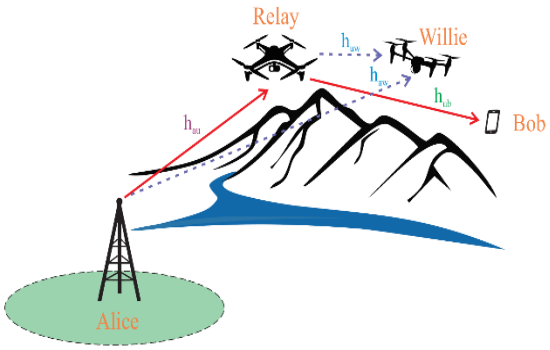
همان‌طور که می‌دانیم روش‌های امنیتی‌ای که به‌منظور برقراری امنیت مخابره در لایه‌های بالاتر شبکه مورداستفاده قرار می‌گیرند (مانند روش‌های رمزنگاری) به‌طور کامل محرمانه نیستند، چراکه دستگاه‌های محاسباتی شنود مخابره روزبه‌روز در حال پیشرفت می‌باشند و ممکن است که شنودگر حتی پس از گذشت چندین سال با شکستن کلید رمز داده‌ی رمزنگاری‌شده به محتوای پیام محرمانه (پیامی که ممکن است شامل اطلاعات نظامی و یا سایر اطلاعات فوق محرمانه باشد) دسترسی یابد چراکه در سال‌های اخیر نشان داده‌شده است که حتی روش‌های رمزنگاری تقویت‌شده نیز توسط دشمنان قادر به شکست است و این موضوع در برخی شرایط با رویکرد امنیتی بالا مانند مخابرات نظامی مناسب نخواهد بود [۱]. در سال‌های اخیر مخابرهٔ پنهان توجهات زیادی را به خود جلب کرده است. در مخابرهٔ پنهان در کنار محافظت از محتوای مخابرهٔ انجام‌شده میان دو کاربر، سعی می‌شود که یک انتقال بی‌سیم را میان دو کاربر به‌گونه‌ای فراهم نماید که احتمال آشکارسازی مخابرهٔ انجام‌شده میان آن دو بسیار کم باشد. چنین روش مخابره‌ای برای ارگان‌های دولتی و نظامی که علاقه‌ی زیادی به پنهان نگه‌داشتن فعالیت‌هایشان در کانال‌های بی‌سیم دارند به‌شدت مطلوب و موردتوجه است [۲]. همچنین در پژوهش [۳]، بر مسائل مخابرهٔ پنهان شبکه‌های بی‌سیم به کمک پهپاد تمرکز شده است. در پژوهش [۴] به

* رایانامه نویسنده مسئول: Saeed.talati@yahoo.com

[1] Decode and Forward
[2] Maximum Ratio Transmission
[3] Full-Duplex
[4] Source-based Jamming

مشکل حیاتی پنهان‌سازی پهپاد برای انتقال بی‌سیم توسط فناوری نوظهور مخابرهٔ پنهان پرداخته‌شده است، زیرا در سناریوهای نظارت نظامی، افشای اطلاعات موقعیت مکانی پهپاد ممکن است منجر به حمله شود. به‌طورکلی کارایی امنیت شبکه‌های پهپاد می‌تواند به‌وسیله تنظیم پویای مسیر حرکت پهپاد و توان انتقالی آن به‌طور هم‌زمان بهبود یابد، یعنی موجب افزایش کیفیت کانال برای لینک‌های مجاز و کاهش کیفیت کانال برای لینک‌های استراق سمع شود [۵]. در پژوهش‌های [۶] و [۷] عملکرد نرخ پنهان برای یک شبکه رله یک‌طرفه با یک طرح رله فرصت‌طلب مورد بررسی قرار گرفت. بااین‌وجود، تمام مطالعات فعلی به‌شدت بر عدم قطعیت نویز شبکه‌های بی‌سیم تکیه‌دارند که همیشه نمی‌توان آن را تضمین کرد. در پژوهش [۸] سامانه‌ای که یک پهپاد به‌عنوان رله‌ی شبکه تحت شرایط حضور یک شنودگر عمل می‌کند مورد بررسی قرارگرفته است که در آن هدف بیشینه‌سازی میانگین نرخ محرمانه‌ی قابل‌دستیابی با بهینه‌سازی تخصیص توان انتقال در طول زمان پرواز پهپاد است. همچنین در پژوهش [۹] طرحی مبنی بر ایجاد اختلال مشارکتی با کمک از اهرم ایجاد اختلال توسط سایر پهپادهای مجاور برای ایمن کردن ارتباطات پهپاد مورد بررسی قرارگرفته است. از نمونه‌های دیگر ایجاد اختلال به‌منظور برآورده سازی امنیت مخابره در شبکه‌های بی‌سیم پهپاد می‌توان به پژوهش [۱۰] اشاره نمود که در آن از یک پهپاد رله‌ی غیرقابل‌اعتماد استفاده‌شده است که در حالت کاملاً دوطرفه به‌منظور ایجاد سیگنال اختلال بهره می‌برد.

با استناد به [۱۱]، درصورتی‌که خود تداخلی به‌طور کامل و مناسب انجام شود، ازآنجایی‌که ارتباط کاملاً دوطرفه[1] (FD) نسبت به ارتباط نیمه دوطرفه[2] (HD) از گین مالتی‌پلکسینگ بالاتری برخوردار است، ایجاد ارتباط کاملاً دوطرفه یکی از روش‌های کلیدی در مخابرات نسل پنجم و کاربردهای فراتر از آن محسوب می‌شود.



شکل (۱). مدل سیستم پیشنهادی برای بکارگیری پهپاد رله در حضور یک پهپاد شنودگر (Willie)

همان‌طور که گفته شد هدف اصلی مخابرهٔ پنهان اطمینان از غیرقابل تشخیص بودن اطلاعات انتقال است [۱۲]. همچنین یک پهپاد می‌تواند به‌عنوان اخلال‌گر برای افزایش امنیت مخابرات بی‌سیم در شبکه‌های پهپاد بکار رود، بطوریکه این پهپاد به‌عنوان اخلالگر به انتشار نویز مصنوعی برای بهبود امنیت مخابره مشغول می‌شود. در [۱۳] طرحی مورد بررسی قرارگرفته است که دو پهپاد در آن وجود دارد؛ یکی از پهپادها پیام محرمانه را به کاربر روی زمین انتقال می‌دهد و پهپاد دیگر به تولید نویز مصنوعی برای تداخل استراق سمع کننده می‌پردازد. در پژوهش [۱۴] استفاده از یک پهپاد رله تمام دوطرفه برای کمک به شبکه مخابرهٔ پنهان پیشنهادشده است. پژوهش [۱۵] به بررسی تحلیل عملکرد برای یک سیستم ارتباطی پنهان جدید می‌پردازد که در آن از یک پهپاد به‌عنوان جمر دوستانه برای محافظت از انتقال مخفی از آلیس به باب در برابر استراق سمع شنودگر استفاده می‌شود.

در ادامه اهداف اصلی ما در این پژوهش به‌صورت زیر است:

- در این پژوهش سعی داریم تا با کمک شیوهٔ جدید مخابره که مخابرات پنهان نامیده می‌شود و کاربرد زیادی در مخابرات نظامی و کاربردهای شهروندی در نسل‌های مخابراتی آینده خواهد داشت یک سیستم ad-hoc را مورد بررسی قرار دهیم.
- در سیستم ad-hoc پیشنهادی، استفاده از یک پهپاد رله به‌منظور ایجاد ارتباط میان فرستنده و گیرنده‌ای که به دلیل خارج بودن از حد شعاع فرستنده امکان برقراری ارتباط میان آن‌ها به‌صورت مستقیم امکان‌پذیر نیست را مورد بررسی و تحقیق قرار خواهیم داد.
- در سیستم موردنظر شرایط پهپاد بودن شنودگر دشمن که قصد آشکارسازی وجود مخابره و دسترسی به محتوای پیام ارسال‌شده را دارد و این به‌نوبهٔ خود به دلیل باکیفیت‌تر بودن لینک‌های ارتباطی پهپادها شرایط را سخت‌تر می‌کند، عملکرد شبکه را در شرایطی مورد بررسی قرار خواهیم داد که پهپاد رله در باند فرکانسی کاملاً دوطرفه عمل کند.
- در این پژوهش به بررسی میزان تأثیرگذاری استفاده از چندین آنتن فرستنده بر نرخ میانگین شبکه را نیز مورد بررسی قرار خواهد گرفت.

۲- تشریح سیستم پیشنهادی

در مدل سامانه‌ای که در این پژوهش در نظر گرفته‌شده است، به دلیل خسارات واردشده به شبکهٔ مخابراتی ارسال مستقیم پیام‌های محرمانه به گیرنده‌ی موردنظر به دلیل خارج بودن از حداکثر شعاع پوشش ایستگاه‌های مخابراتی زمینی، میسر نیست؛

[1] Full-Duplex
[2] Half-Duplex

بنابراین برای حل مشکل ایجاد ارتباط مخابراتی، پیشنهادشده است که از یک سیستم مخابراتی پهپاد رله‌ی کدگشا-انتقال‌دهنده‌ی کاملاً دوطرفه که به یک آنتن جهت ارسال داده و یک آنتن جهت دریافت داده مجهز است و این پهپاد در تمام طول زمان رله باحالت شبه ایستا معلق است استفاده شود. همان‌طور که در شکل (۱) نشان‌داده‌شده است، یک ایستگاه پایه زمینی فرستنده با تعداد M آنتن (Alice)، سعی دارد با کاربر زمینی شبکه (Bob) که تک آنتنِ بوده و امکان ایجاد ارتباط مستقیم با آن وجود ندارد مخابره نماید، به‌گونه‌ای که این مخابره بایستی از دید یک پهپاد دشمن (Willie) تک آنتن که در محدودهٔ انتقال پیام پنهان حضور دارد مخفی مانده و از آشکارسازی وجود انتقال یک پیام در دو فاز انتقال پیام، توسط این پهپاد متخاصم جلوگیری شود.

در مدل سیستم زمانی که فرستنده و یا پهپاد رله تصمیم به ارسال پیام بگیرند، وضعیت آن‌ها در طول بازهٔ زمانی ارسال ثابت باقی می‌ماند. در دو فاز انتقال پیام، فرستندهٔ زمینی و پهپاد رله از استراتژی روشن –خاموش استفاده می‌کنند. در این استراتژی زمانی که پهپاد رله تصمیم به ارسال داده به گیرندهٔ خود ندارد به ارسال سیگنال اختلال می‌پردازد. همچنین در سیستم موردنظر فرض شده است که فرستنده و پهپاد رله برای ارسال سیگنال پیام از کتاب کد گاوسی استفاده کرده و پهپاد رله برای ارسال سیگنال پارازیت به‌منظور تخریب کانال شنودگر و بالابردن خطای آشکارسازی مخابرهٔ پنهان وی از جمینگ گاوسی استفاده خواهد کرد. همچنین در مدل سیستم، اطلاعات حالت کانال شنودگر در فرستنده و پهپاد رله موجود نیست و علت این امر آن است که شنودگر در حالت منفعل (پسیو) قرار داشته و تنها به عمل شنود برای آشکارسازی مخابره و دسترسی به محتوای پیام محرمانه مبادرت دارد. علت منفعل بودن پهپاد شنودگر هم آن است که اگر فعال باشد به تکمیل‌شدن مخابرهٔ پنهان کمک خواهد کرد که این موضوع برای وی مناسب نخواهد بود [۱].

۲-۱- مدل کانال گره‌های شبکه

با توجه به مدل کانال نظر گرفته‌شده در [۱۶]، در مدل سیستم پیشنهاد فرض شده است که ضرایب کانال[1] میان گره‌های شبکه از یک مدل تلفات مسیر مقیاس بزرگ[2] a_{ij} و محوشدگی مقیاس کوچک[3] رایلی[4] h_{ij} پیروی می‌کند که آن را به‌صورت زیر نمایش می‌دهیم:

$$g_{ij} = a_{ij} h_{ij} \ , \quad i\,j \in \{au, aw, ub, uw\} \qquad (۱)$$

که در رابطه‌ی فوق با توجه به چند آنتنِ بودن فرستنده، کانال میان آلیس و پهپاد رله، آلیس و پهپاد شنودگر به ترتیب به‌صورت $\mathbf{h_{au}} @\left[h_{au_1},\mathrm{K}\,,h_{au_{Na}}\right]\in \pounds^{1\times N_a}$ که $h_{au_i}:\ \mathcal{CN}(0,1)$ است و $\forall k\in\{1,\mathrm{K}\,,N_a\}$، با $\mathbf{h}_{aw}=\left[h_{aw_1},\mathrm{K}\,,h_{aw_M}\right]\in \pounds^{1\times N_a}$ $h_{aw_k}:\ \mathcal{CN}(0,1), \forall k\in\{1,\mathrm{K}\,,N_a\}$ هست، همچنین کانال میان پهپاد رله و پهپاد شنودگر و پهپاد رله و باب به ترتیب به‌صورت $h_{ub}:\ \mathcal{CN}(0,1)$ و $|h_{uw}|^2=1$ است.

همچنین لازم به ذکر است که تلفات مسیر مقیاس بزرگ a_{ij} در نظر گرفته‌شده برای پیوند[5] هوا به زمین[6] ترکیبی از کانال‌های دید مستقیم (LoS)[7] و دید غیرمستقیم (NloS)[8] است که این کانال‌ها را می‌توان به‌صورت زیر تعریف نمود:

$$a_{ij}=\begin{cases}\sqrt{\lambda_L d_{ij}^{-\xi_L}}, & LoS\ link\\ \sqrt{\lambda_{NL} d_{ij}^{-\xi_{NL}}}, & NLos\ link\end{cases} \qquad (۲)$$

که در روابط فوق ξ_L و ξ_{NL} المان‌های تلفات مسیر به ترتیب برای کانال‌های دیدمستقیم و غیرمستقیم را نمایش می‌دهند. همچنین λ_L و λ_{NL} به ترتیب نماینده‌ی تلفات مسیر قراردادی در کانال دیدمستقیم و غیرمستقیم بوده و به عواملی همچون تراکم انسداد، ارتفاع و تراکم ساختمان‌ها و موانع اطراف بستگی دارد و $d_{ij}=\sqrt{H^2+r_{ij}^2}$ بیانگر فاصله‌ی میان دو گره موردنظر است. در ادامه برای محاسبه‌ی دو المان تلفات مسیر ξ_L و ξ_{NL} داریم [۱۷]:

$$\begin{cases}\xi_L=\xi\left(1-p_L\right)+\xi_0 & LoS\ link\\ \xi_{NL}=\xi\left(p_L\right)+\xi_0 & NLoS\ link\end{cases} \qquad (۳)$$

که در رابطه‌ی فوق ξ و ξ_0 نشان‌دهنده‌ی ضرایب تلفات مسیر پایه هستند. در ادامه برای احتمال اتصال به پهپاد رله، به‌احتمال اتصال کانال‌های دیدمستقیم و غیرمستقیم نیز نیاز داریم که به‌صورت زیر است:

$$\begin{cases}p_L=\dfrac{1}{1+\alpha.\exp\left(-\beta.\left(\theta_{ij}-\alpha\right)\right)}\\ p_{NL}=1-p_L\end{cases} \qquad (۴)$$

که در معادلات فوق α و β نشان‌دهنده‌ی پارامترهای ثابت محیط، $\theta_{ij}=\sin^{-1}\left(\dfrac{H}{d_{ij}}\right)$ درجه‌ی زاویه‌ی ارتفاع

[1] Channel Coefficient
[2] Large-scale path-loss
[3] Small-scale fading
[4] Rayleigh fading
[5] Link
[6] Air-to-ground
[7] Light of Sight
[8] Non-Light-of-Sight

پهپاد رله نسبت به گره‌ی دیگر در شبکه بوده، H ارتفاع پهپاد و $r_{ij}=\sqrt{\left(x_i-x_j\right)^2+\left(y_i-y_j\right)^2}$ فاصله‌ی یک گره‌ی مستقر بر روی زمین و تصویر پهپاد بر روی صفحه‌ی زمین است.

با فرض اینکه فرستنده (آلیس) از $\mathbf{h}_{au}$ اطلاع دارد، می‌تواند از بردار پیش کدگذاری[1] $\mathbf{w}_a$ به‌منظور دسترسی به فن **MRT** در پهپاد رله به‌صورت زیر دسترسی پیدا کند:

$$\mathbf{w}_a=\frac{\mathbf{h}_{au}^H}{\left\|\mathbf{h}_{au}\right\|} \qquad (۵)$$

که در معادله‌ی فوق $\mathbf{w}_a\in \pounds^{M\times 1}$ بوده و $\mathbf{h}_{au}^H$ ماتریس هرمتین ضرایب کانال است.

۲-۲- طرح رلهٔ مشارکتی[2]

در فاز اول انتقال فرستنده تصمیم می‌گیرد که با توان P_a ارسال کند یا خیر و این دو رخداد به ترتیب با Ψ_1 و Ψ_0 نمایش داده می‌شود. زمانی که فرستنده (آلیس) تصمیمی مبنی بر ارسال داده داشته باشد، پیام‌های خود را بر روی دنباله‌ای از n سمبل $\mathbf{x_a}(i)$ نگاشت می‌کند. لازم به ذکر است که بدون توجه به ارسال و یا عدم ارسال پیام توسط فرستنده (آلیس)، پهپاد رله در فاز اول به‌منظور گمراه‌سازی پهپاد شنودگر با توان $P_j\le P_u$ به‌طور متوالی به ارسال سیگنال پارازیت $\mathbf{x}_j=\left[x_j(1),x_j(2),\mathrm{K},x_j(n)\right]$ مبادرت خواهد داشت. فرض شده است که سمبل‌ها توزیع یکسان مستقل (i.i.d) داشته و شرط $\mathrm{E}\left[\left|x_a(i)\right|^2\right]=1$ و $\mathrm{E}\left[\left|x_j(i)\right|^2\right]=1$ را ارضا کرده و $i=1,\mathrm{K},n_1$ شناسه‌ی سمبل است. لازم به ذکر است که خود تداخلی[3] ایجادشده توسط پهپاد رله‌ی کاملاً دوطرفه را تا حد زیادی می‌توان توسط روش حذف خود تداخلی[4] از بین برد؛ بنابراین خود تداخلی باقی‌مانده توسط $r(i)$ نشان داده می‌شود که $r(i):\ \mathcal{CN}\left(0,\upsilon P_r\sigma^2\right)$ است با ضریب $0<\upsilon<1$ [۱۸]. با توجه به موارد گفته‌شده فرستنده (آلیس) در فاز اول زمانی که در حالت انتقال باشد، سیگنال $\mathbf{x_a}$ را توسط بردار $\mathbf{w_a}$ با توان ثابت P_a پیش کدگذاری می‌کند و زمانی که تصمیم بگیرد در حالت خاموش باشد هیچ سیگنال را ارسال نخواهد کرد و سیگنال دریافتی در پهپاد رله برابر صفر خواهد بود؛ بنابراین سیگنال دریافت شده در پهپاد رله زمانی که فرستنده تصمیم به ارسال سیگنال داده بگیرد به‌صورت زیر خواهد بود:

$$y_{au}(i)=\sqrt{P_a}\,a_{au}\,\mathbf{h}_{au}^H\,\mathbf{w}_a\,x_a(i)+r(i)+n_u(i), \qquad (۶)$$

که $n_u(i)$ نویز مختلط گوسی دریافت شده در پهپاد رله با واریانس σ_u^2 است، به‌عبارت‌دیگر $n_u(i):\ \mathcal{CN}\left(0,\sigma_u^2\right)$؛ بنابراین نرخ انتقال میان فرستنده (آلیس) و پهپاد رله را به‌صورت زیر خواهد بود:

$$R_{au}\left(P_a,P_j\right)=\log_2\left(1+\gamma_{au}\right) \qquad (۷)$$

که در رابطهٔ فوق $\gamma_{au}=\dfrac{P_a a_{au}^2\left\|\mathbf{h_{au}}\right\|^2}{\left(\sigma_u^2+\upsilon P_j\sigma^2\right)}$ بیانگر نسبت سیگنال به نویز[5] (SNR) است.

همچنین سیگنال دریافت شده در پهپاد شنودگر برای فاز اول انتقال به‌صورت زیر خواهد بود:

$$y_{aw}(i)=\begin{cases}\sqrt{P_j}\,a_{uw}h_{uw}\,x_j(i)+n_w(i), & \Psi_0\\ \sqrt{P_a}\,a_{aw}\mathbf{h}_{aw}\mathbf{w}_a x_a(i)+\mathrm{L} & \\ \sqrt{P_j}\,a_{uw}h_{uw}\,x_j(i)+n_w(i), & \Psi_1\end{cases} \qquad (۸)$$

که $n_w(i)$ نشان‌دهنده‌ی نویز سفید گوسی اضافه‌شده در گیرنده‌ی پهپاد شنودگر بوده، $P_j\le P_u$ و $n_w(i):\ CN\left(0,\sigma_w^2\right)$ است.

در فاز دوم انتقال، پهپاد رله سیگنال باند پایه $x_b(t)$ ارسالی خود برای گیرنده‌ی موردنظر را با توان P_b پردازش می‌کند، به‌عبارت‌دیگر پهپاد رله درصدی از توان P_u را برای ارسال بسته‌های داده به گیرنده‌ی موردنظر خودمصرف کرده و باقیمانده‌ی توان اختصاص‌یافته‌ی خود را صرف ارسال سیگنال اختلال به‌منظور گمراه‌سازی پهپاد شنودگر خواهد کرد و $t=1,\mathrm{K},n_2$ و $\mathrm{E}\left[\left|x_b(t)\right|^2\right]=1$ و $\mathrm{E}\left[\left|x_j(t)\right|^2\right]=1$ است؛ بنابراین سیگنال دریافتی در گیرنده‌ی قانونی شبکه (باب) و پهپاد شنودگر به‌صورت زیر خواهد بود:

$$y_{ij}=\begin{cases}\sqrt{P_j}\,a_{ui}h_{ui}x_j(t)+n_i(t), & \Psi_0\\ \left(\sqrt{P_b}\,x_b(t)+\sqrt{P_j}\,x_j(t)\right)a_{ui}h_{ui}+n_i(t), & \Psi_1\end{cases} \qquad (۹)$$

که در رابطه‌ی فوق $i\in\{b,w\}$ بوده و $n_i(t)$ نشان‌دهنده‌ی نویز سفید گوسی اضافه‌شده[1]، $P_b+P_j\le P_u$ است؛ بنابراین

[1] Precoding
[2] Cooperative Relaying
[3] Self-interference
[4] Self-interference cancellation
[5] Signal-to-Noise Ratio

نرخ انتقال میان پهپاد رله و گیرنده‌ی باب را به‌صورت زیر خواهیم داشت:

$$R_{ub}\left(P_b,P_j\right)=\log_2\left(1+\gamma_{ub}\right) \quad (۱۰)$$

که در رابطهٔ فوق $\gamma_{ub}=\dfrac{a_{ub}^2P_b\left|h_{ub}\right|^2}{\sigma_b^2+a_{ub}^2P_j\left|h_{ub}\right|^2}$ نشان‌دهندهٔ نسبت سیگنال به نویز دریافتی در باب خواهد بود.

۲-۳- معیارهای مخابرهٔ پنهان

در هر بازهٔ زمانی که ارسال داده توسط ایستگاه پایه زمینی و یا پهپاد رله صورت می‌گیرد، پهپاد شنودگر (ویلی) بر اساس متوسط توان دریافتی توسط یک رادیو متر آشکارساز توان[۲] تعیین می‌کند که آلیس و یا پهپاد رله در حال ارسال سیگنال پیام به گیرنده‌ی موردنظر خود هستند و یا خیر. این معیار با مقایسه‌ی متوسط توان دریافتی T_{ij} از $n-$سمبل $y_{ij}[s]$ با یک حد آستانه‌ی معین ϑ_{ij} به دست می‌آید و خود به‌تنهایی می‌تواند معیاری کاربردی و کافی باشد. بر اساس [۱۹] قانون تصمیم‌گیری پهپاد شنودگر به‌صورت زیر خواهد بود:

$$T_{ij}=\frac{1}{n}\sum_{s=1}^{n}\left|y_{ij}[s]\right|^2\underset{\Psi_0}{\overset{\Psi_1}{\gtrless}}\vartheta_{ij} \quad (۱۱)$$

که در معادله‌ی فوق $ij=\{aw,uw\}$ و $n=\{n_1,n_2\}$ و $y_{ij}[s]$ نشان‌دهنده‌ی سمبل‌های دریافت شده در گیرنده‌ی ویلی است. بر اساس معادله‌ی (۱۱) زمانی که $T_{ij}>\vartheta_{ij}$ باشد ویلی تصمیم خواهد گرفت که فرستنده در حال ارسال پیام است (Ψ_1)، همچنین زمانی که $T_{ij}<\vartheta_{ij}$ باشد تصمیم ویلی مبنی بر خاموش بودن فرستنده (Ψ_0) خواهد بود؛ بنابراین ϑ_{ij} مبنای تصمیم‌گیری پهپاد شنودگر بوده و تأثیر بسزایی در میزان دقت پهپاد شنودگر خواهد داشت و در بخش‌های پیشرو این حد آستانه‌ی تصمیم‌گیری را بهینه‌سازی خواهیم کرد.

بر اساس فرضیات صورت گرفته برای استراتژی ارسال بسته‌های داده‌ی فرستنده و پهپاد رله، پهپاد شنودگر ممکن است دو نوع اشتباه در آشکارسازی مخابرهٔ پنهان (از فرستنده به پهپاد رله و از پهپاد رله به گیرنده‌ی موردنظر) انجام دهد. بر اساس پروتکل در نظر گرفته‌شده برای مخابره، ممکن است فرستنده در حالت خاموش باشد اما ویلی بر اساس میزان توان دریافتی در رادیو متر خود تصمیم بگیرد که فرستنده و یا پهپاد رله در حال ارسال داده می‌باشند که این اشتباه را بر اساس معیار نیمن-پیرسون[۳] به‌عنوان هشدار اشتباه[۴] (FA) نامیده می‌شود.

همچنین ممکن است فرستنده و یا پهپاد رله در حال ارسال داده باشند اما پهپاد شنودگر بر اساس توان دریافتی در گیرنده‌ی خود تصمیم بر عدم ارسال بگیرد که این اشتباه را آشکارسازی ازدست‌رفته[۵] (MD) می‌نامیم؛ بنابراین پهپاد شنودگر سعی خواهد داشت تا احتمال خطای آشکارسازی خود یعنی $P_{eror}=P_{FA}+P_{MD}$ را به حداقل برساند.

همچنین زمانی که $n_1\to\infty$ باشد، زمانی مخابره را پنهان می‌نامیم که به ازای هر $\varepsilon>0$، شرط زیر برقرار باشد [۱۹]:

$$P_{FA}^{ij}+P_{MD}^{ij}\geq 1-\varepsilon \quad (۱۲)$$

که در رابطهٔ فوق:

$$P_{FA}^{ij}=\Pr\left(T_{ij}^{\Psi_0}\geq\vartheta_{ij}\left|\Psi_0\right.\right) \quad (۱۳)$$

$$P_{MD}^{ij}=\Pr\left(T_{ij}^{\Psi_1}\leq\vartheta_{ij}\left|\Psi_1\right.\right) \quad (۱۴)$$

۲-۳-۱- احتمالات هشدار اشتباه

همان‌طور که گفته شد یکی از اشتباهات ویلی، احتمال هشدار اشتباه خواهد بود. برای فاز اول انتقال با توجه به رابطه‌ی (۵) می‌توان نتیجه گرفت که $\mathbf{w}_a$ توزیع رایلی $\mathbf{h}_{aw}$ را تغییر نخواهد داد و بنابراین $|h_{aw}w_a|^2$ توزیع نمایی خواهد داشت [۲۰]. با توجه به موارد گفته‌شده و همچنین مدل سیگنال دریافت شده در گیرنده‌ی رادیو متر ویلی در فازهای اول و دوم در رابطه‌های (۸) و (۹) احتمال هشدار اشتباه به ترتیب در فازهای اول و دوم انتقال بسته‌های داده به‌صورت زیر محاسبه خواهد شد:

$$P_{FA}^{aw}=\Pr\left(\left(a_{uw}^2P_j+\sigma_w^2\right).\frac{\chi^2\left(2n_1\right)}{n_1}\geq\vartheta_{aw}\left|\Psi_0\right.\right) \quad (۱۵)$$

$$P_{FA}^{uw}=\Pr\left(\left(a_{uw}^2P_j+\sigma_w^2\right).\frac{\chi^2\left(2n_2\right)}{n_2}\geq\vartheta_{uw}\left|\Psi_0\right.\right) \quad (۱۶)$$

که در رابطهٔ فوق $\chi^2\left(2n\right)$ متغیر تصادفی خی‌دو[۶] با $2n$ درجه آزادی است.

قضیه ۱: به دلیل اینکه در شبکهٔ موردنظر مخابره با طول بلوک نامحدود در نظر گرفته‌شده است n_1 و n_2 را به سمت بی‌نهایت میل می‌دهیم (اجازه می‌دهیم که $n_1,n_2\to\infty$) و این احتمال را در نظر می‌گیریم که شرایط کانال به‌گونه‌ای بوده است که مخابرهٔ پنهان کامل شده است [۲۱]. با توجه به قانون قوی اعداد بزرگ[۷] (SLLN)، $\dfrac{\chi^2\left(2n\right)}{n}$ به سمت ۱ میل می‌کند و همچنین بر اساس تئوری همگرایی غالب لبسگو[۸]،

[1] AWGN
[2] Radiometer Power Detector
[3] Nyman-Pearson
[4] False Alarm
[5] Missed Detection
[6] Chi-squared
[7] Strong Law of Large Numbers
[8] Lebesgue's Dominated Convergence Theorem

زمانی که $n\to\infty$ باشد می‌توانیم $\frac{\chi^2(2n)}{n}$ را با ۱ جایگزین نماییم، بنابراین احتمال هشدار اشتباه در فاز اول و دوم را می‌توان به ترتیب به‌صورت زیر بازنویسی نمود:

$$\mathrm{P}_{FA}^{ij}=\Pr\left(a_{uw}^2P_j+\sigma_w^2\geq\vartheta_{ij}\,|\Psi_0\right) \quad (۱۷)$$

درنتیجه، احتمال هشدار اشتباه برای فازهای اول و دوم به‌صورت زیر خواهد شد:

$$\mathrm{P}_{FA}^{ij}=\begin{cases}e^{-\frac{\vartheta_{ij}-\sigma_w^2}{a_{uw}^2P_j}} & \vartheta_{ij}-\sigma_w^2>0\\ 1 & \vartheta_{ij}-\sigma_w^2\leq 0\end{cases} \quad (۱۸)$$

۲-۳-۲- احتمالات آشکارسازی ازدست‌رفته

می‌توان گفت اشتباه دیگری که ممکن است ویلی در مورد آشکارسازی مخابرهٔ پنهان فرستنده مرتکب شود را احتمال آشکارسازی ازدست‌رفته نامیدیم. برای فاز اول با توجه به مدل سیگنال دریافت شده در رابطه‌ی (۸) برای زمانی که فرستنده در حال انتقال پیام است و اینکه $\mathbf{h}_{aw}$ و h_{uw} از یکدیگر مستقل بوده و توزیع یکسان دارند و مدل سیگنال دریافت شده در ویلی برای فاز دوم در رابطه‌ی (۹) و همچنین با توجه به آنچه در قضیه ۱ گفته شد، احتمال آشکارسازی از دسته رفته برای فازهای اول و دوم انتقال به ترتیب به‌صورت زیر خواهد بود:

$$\mathrm{P}_{MD}^{aw}=\Pr\left(P_aa_{aw}^2+P_ra_{uw}^2+\sigma_w^2\geq\vartheta_{aw}\,|\Psi_1\right) \quad (۱۹)$$

$$\mathrm{P}_{MD}^{uw}=\Pr\left(a_{uw}^2\left(P_b+P_j\right)+\sigma_w^2\geq\vartheta_{aw}\,|\Psi_1\right) \quad (۲۰)$$

در انتها احتمال آشکارسازی ازدست‌رفته را برای فازهای اول و دوم به‌صورت زیر خواهیم داشت:

(۲۱)

$$\mathrm{P}_{MD}^{aw}=\begin{cases}\dfrac{a_{aw}^2P_a}{a_{aw}^2P_a-a_{uw}^2P_j}\left(1-e^{-\frac{\vartheta_{aw}-\sigma_w^2}{a_{aw}^2P_a}}\right)+\\ \dfrac{a_{uw}^2P}{a_{aw}^2P_a-a_{uw}^2P_j}\left(e^{-\frac{\vartheta_{aw}-\sigma_w^2}{a_{uw}^2P_j}}-1\right), & \vartheta_{aw}-\sigma_w^2>0\\ 0, & \vartheta_{aw}-\sigma_w^2\leq 0\end{cases}$$

$$\mathrm{P}_{MD}^{uw}=\begin{cases}1-e^{-\frac{\vartheta_{uw}-\sigma_w^2}{a_{uw}^2\left(P_b+P_j\right)}} & \vartheta_{aw}-\sigma_w^2>0\\ 0 & \vartheta_{aw}-\sigma_w^2\leq 0\end{cases} \quad (۲۲)$$

۲-۳-۳- بهینه‌سازی حد آستانهٔ آشکارسازی پهپاد شنودگر

هدف پهپاد شنودگر به‌حداقل‌رساندن خطای آشکارسازی خود خواهد بود. به‌منظور یافتن حد آستانهٔ آشکارسازی بهینه از دید پهپاد شنودگر، مسئلهٔ بهینه‌سازی به‌صورت زیر نوشته می‌شود:

$$\min_{\vartheta}\ \mathrm{P}_{FA}^{ij}+\mathrm{P}_{MD}^{ij} \quad (۲۳)$$

به‌منظور دستیابی به مقدار بهینهٔ ϑ از دید پهپاد شنودگر، تابع هدف را به‌صورت زیر به دست خواهیم آورد:

$$\vartheta_{op}=\begin{cases}\vartheta_{ij}^*, & \vartheta-\sigma_w^2\geq 0\\ there\,is\,not\,optimal\,\vartheta, & \vartheta-\sigma_w^2<0\end{cases} \quad (۲۴)$$

همان‌طور که از تابع هدف فوق مشخص است مقدار بهینه‌ای برای $\vartheta-\sigma_w^2<0$ وجود نخواهد داشت، چراکه هیچ‌گاه پهپاد شنودگر حد آستانه‌ی آشکارسازی مخابرهٔ پنهان رادیو متر خود را کمتر از مقدار نویز سفید گاوسی اضافه‌شده‌ی دریافتی در گیرنده‌ی خود انتخاب نخواهد کرد؛ بنابراین مقدار بهینه حد آستانه‌ی آشکارسازی مخابرهٔ پنهان تنها برای زمانی وجود خواهد داشت که $\vartheta-\sigma_w^2\geq 0$ باشد که به‌منظور به دست آوردن حد آستانه بهینه‌ی آشکارسازی پهپاد ϑ_{ij}^*، عبارت $\frac{\partial\left(\mathrm{P}_{FA}+\mathrm{P}_{MD}\right)}{\partial\vartheta_{ij}}=0$ را برای هر فاز انتقال سیگنال پیام در نظرخواهیم گرفت؛ بنابراین با توجه به‌احتمال هشدار اشتباه به‌دست‌آمده در (۱۸) و همچنین احتمال آشکارسازی ازدست‌رفته در روابط (۲۱) و (۲۲) حد آستانه‌ی آشکارسازی بهینه ϑ_{au}^* به ترتیب برای فاز اول و دوم انتقال به‌صورت زیر خواهد بود:

$$\vartheta_{aw}^*=\frac{\left(a_{aw}^2P_a\right)\left(a_{uw}^2P_j\right)}{\left(a_{aw}^2P_a-a_{uw}^2P_j\right)}\ln\left(\frac{a_{aw}^2P_a}{a_{uw}^2P_j}\right)+\sigma_w^2 \quad (۲۵)$$

$$\vartheta_{uw}^*=\frac{\left(a_{uw}^2P_j\right)\left(P_b+P_j\right)}{P_b}.\ln\left(\frac{\left(P_b+P_j\right)}{P_j}\right)+\sigma_w^2 \quad (۲۶)$$

۲-۴- بهینه‌سازی توأمان برای آلیس و پهپاد رله

در این بخش بیت‌های انتقال مؤثر قابل‌دستیابی η که از فرستندهٔ زمینی (آلیس) به گیرنده‌ی قانونی زمینی (باب) ارسال می‌شود را بهینه خواهیم کرد. هدف ما در این طرح در کنار دستیابی به مخابرهٔ پنهان، بیشینه‌سازی بیت‌های انتقال مؤثر $\eta=\min\left(R_{au},R_{ub}\right)$ است؛ بنابراین مسئله‌ی بهینه‌سازی با توجه به شروط مخابرهٔ پنهان و همچنین محدودیت توان مصرفی، به‌صورت زیر تعریف می‌شود:

$$\max_{P_a,P_b,P_j}\ \eta \quad (۲۷)$$

$$s.t.\ P_a \le P_{a_{\max}} \quad (۲۸)$$

$$P_j \le P_u \quad (۲۹)$$

$$P_b + P_j \le P_u \quad (۳۰)$$

$$\min_{\vartheta_{aw}^*}\left(\mathrm{P}_{FA}^{aw}+\mathrm{P}_{MD}^{aw}\right)\ge 1-\varepsilon \quad (۳۱)$$

$$\min_{\vartheta_{uw}^*}\left(\mathrm{P}_{FA}^{uw}+\mathrm{P}_{MD}^{uw}\right)\ge 1-\varepsilon \quad (۳۲)$$

که در مسئله‌ی بهینه‌سازی فوق قیدهای (۳۱) و (۳۲) به ترتیب شروط مخابرهٔ پنهان برای فاز اول انتقال و فاز دوم انتقال سیگنال پیام بوده و ε یک حد آستانه‌ی اطمینان از مخابرهٔ پنهان است.

۲-۴-۱- حل مسئلهٔ بهینه‌سازی

مسئله‌ی بهینه‌سازی (۲۷) غیر محدب است، بنابراین نمی‌توانیم از روش‌های بهینه‌سازی که محدب هستند برای شبیه‌سازی و ارزیابی عملکرد سیستم پیشنهادشده استفاده نماییم؛ بنابراین در مرحله‌ی اول باید مسئله‌ی بهینه‌سازی موردنظر را به یک مسئله‌ی محدب قابل‌حل توسط تولباکس‌های نرم‌افزار متلب مانند CVX تبدیل نماییم. به‌منظور حل مشکل غیر محدب بودن (۲۷)، از روش تقریب محدب متوالی (SCA[1]) استفاده خواهیم کرد. بدین منظور ابتدا با کمک روش تفاضل دو تابع محدب (DC)[2]، R_{au} را به‌صورت تفاضل دو تابع محدب نوشته و آن را به‌صورت زیر بازنویسی می‌کنیم:

$$R_{au}\left(\mathbf{P}_1\right)=\log_2\left(1+\frac{P_a a_{au}^2\left\|\mathbf{h_{au}}\right\|^2}{\left(\sigma_u^2+\upsilon P_j\sigma^2\right)}\right) \quad (۲۸)$$
$$=\Delta\left(\mathbf{P}_1\right)-\Phi\left(\mathbf{P}_1\right)$$

که در رابطهٔ فوق داریم:

$$\begin{cases}\Delta\left(P_a,P_j\right)=\log_2\left(P_a a_{au}^2\left\|\mathbf{h_{au}}\right\|^2+\upsilon P_j\sigma^2+\sigma_u^2\right)\\ \Phi\left(P_j\right)=\log_2\left(\sigma_u^2+\upsilon P_j\sigma^2\right)\end{cases} \quad (۲۹)$$

سپس با استفاده از یک تقریب خطی $\Phi\left(P_j\right)$ را به‌صورت زیر خواهیم داشت:

$$\begin{cases}\Phi\left(P_j\right)=\Phi\left(P_j\right);\ \Phi\left(P_j\left(\kappa-1\right)\right)+\mathrm{L}\\ \nabla^T\Phi\left(P_j\left(\kappa-1\right)\right)\left(P_j-P_j\left(\kappa-1\right)\right)\end{cases} \quad (۳۰)$$

که در رابطه‌ی فوق ∇ عملگر گرادیان، κ شماره‌ی تکرار بوده و $\nabla\Phi\left(P_j\left(\kappa-1\right)\right)$ به‌صورت زیر محاسبه می‌شود:

$$\nabla\Phi\left(P_j\right)=\frac{\upsilon.\sigma^2}{\left(\sigma_u^2+\upsilon.\sigma^2.P_j\left(\kappa-1\right)\right).\ln(2)} \quad (۳۱)$$

درنتیجه $R'_{au}=\Delta\left(P_a,P_j\right)-\Phi\left(P_j\right)$ خواهد بود.

سپس در مرحلهٔ بعد برای فاز دوم انتقال، R_{ub} را به‌صورت تفاضل دو تابع محدب نوشته و خواهیم داشت:

$$R_{ub}\left(P_b,P_j\right)=\log_2\left(1+\frac{a_{ub}^2P_b\left|h_{ub}\right|^2}{\sigma_b^2+a_{ub}^2P_j\left|h_{ub}\right|^2}\right) \quad (۳۲)$$
$$=\Pi\left(P_b,P_j\right)-\mathrm{Z}\left(P_j\right)$$

که در رابطهٔ فوق خواهیم داشت:

(۳۳)

$$\begin{cases}\Pi\left(P_b,P_j\right)=\log_2\left(a_{ub}^2P_b\left\|\mathbf{h}_{ub}\right\|^2+a_{ub}^2P_j\left\|\mathbf{h}_{ub}\right\|^2+\sigma_b^2\right)\\ \mathrm{Z}\left(P_j\right)=\log_2\left(a_{ub}^2P_j\left\|\mathbf{h}_{ub}\right\|^2+\sigma_b^2\right)\end{cases}$$

سپس با استفاده تقریب خطی برای $\mathrm{Z}\left(P_j\right)$ همانند (۳۰)، $\nabla\mathrm{Z}\left(P_j\left(\kappa-1\right)\right)$ را به‌صورت زیر خواهیم داشت:

(۳۴)

$$\nabla\mathrm{Z}\left(P_j\left(\kappa-1\right)\right)=\frac{a_{ub}^2.\left\|\mathbf{h}_{ub}\right\|^2}{\left(a_{ub}^2.\left\|\mathbf{h}_{ub}\right\|^2.P_j\left(\kappa-1\right)+\sigma_b^2\right)}$$

درنتیجه $R'_{ub}=\Pi\left(P_b,P_j\right)-\mathrm{Z}\left(P_j\right)$ خواهد بود.

پس‌ازاین مرحله با جایگذاری ϑ_{aw}^* از رابطه‌ی (۲۵) در قید (۳۱)، آن را به‌صورت زیر بازنویسی خواهیم کرد:

$$\frac{a_{uw}^2P_j}{a_{aw}^2P_a-a_{uw}^2P_j}.\ln\left(\frac{a_{uw}^2P_j}{a_{aw}^2P_a}\right)\le\ln\left(\varepsilon\right) \quad (۳۵)$$

اما همان‌طور که می‌بینیم هنوز رابطهٔ فوق محدب نیست که با انتخاب یک متغیر کمکی $m=a_{aw}^2P_a-a_{uw}^2P_j$ و برخی اعمال ریاضی بر روی آن، می‌توانیم رابطهٔ مذکور را به‌صورت زیر بازنویسی کنیم:

$$a_{uw}^2P_j.\ln\left(\frac{a_{uw}^2P_j}{a_{aw}^2P_a}\right)\le m.\ln\left(\varepsilon\right) \quad (۳۶)$$

$$a_{aw}^2P_a-a_{uw}^2P_j\le m \quad (۳۷)$$

در مرحله‌ی بعد پس از جایگذاری ϑ_{uw}^* از رابطه‌ی (۲۶) در قید (۳۲) می‌توان آن را به‌صورت زیر نوشت:

$$1+e^{\left(\frac{P_b+P_j}{P_b}\right)\ln\left(\frac{P_j}{P_b+P_j}\right)}-e^{\left(\frac{P_j}{P_b}\right)\ln\left(\frac{P_j}{P_b+P_j}\right)}\ge 1-\varepsilon \quad (۳۸)$$

که با ساده‌سازی و برخی عملیات ریاضی روی رابطه‌ی (۳۸)، خواهیم داشت:

[1] Successive Convex Approximation
[2] Difference of two Concave functions

$$P_b.\ln\left(P_b\right)+P_j.\ln\left(P_j\right)-\mathrm{L}$$
$$\left(P_b+P_j\right).\ln\left(P_b+P_j\right)\le P_b.\ln\left(\varepsilon\right) \quad (۳۹)$$

همان‌طور که مشاهده می‌شود می‌توان رابطه‌ی (۳۹) را با استفاده از روش (DC) به‌صورت تفاضل دو تابع محدب نوشت و خواهیم داشت:

$$\Sigma\left(P_b,P_j\right)=\Xi\left(P_b,P_j\right)-\Omega\left(P_b,P_j\right) \quad (۴۰)$$

که در رابطهٔ قبل داریم:

$$\begin{cases}\Xi\left(P_b,P_j\right)=P_b.\ln\left(P_b\right)+P_j.\ln\left(P_j\right)\\ \Omega\left(P_b,P_j\right)=\left(P_b+P_j\right).\ln\left(P_b+P_j\right)\end{cases} \quad (۴۱)$$

همانند رابطه‌ی (۳۰) برای تقریب $\Omega\left(P_b,P_j\right)$، $\nabla\Omega\left(P_b\left(\kappa-1\right),P_j\left(\kappa-1\right)\right)$ را به‌صورت زیر خواهیم داشت:

$$\begin{cases}\nabla\Omega\left(P_b\left(\kappa-1\right),P_j\left(\kappa-1\right)\right)=\\ \left[1+\ln\left(P_b+P_j\right),1+\ln\left(P_b+P_j\right)\right]\end{cases} \quad (۴۲)$$

درنتیجه قید (۳۲) را به‌صورت $\Xi\left(P_b,P_j\right)-\Omega\left(P_b,P_j\right)$ می‌توان نوشت.

سرانجام مسئله‌ی بهینه‌سازی محدب شده‌ی موردنظر (۲۷) را به‌صورت زیر خواهیم داشت:

$$\max_{P_a,P_b,P_j,m}\ \eta' \quad (۴۳)$$

$$S.t.\ \ (۲۸),(۲۹),(۳۰),(۳۶),(۳۷) \quad (۴۴)$$

$$\Xi\left(P_b,P_j\right)-\Omega\left(P_b,P_j\right) \quad (۴۵)$$

که در رابطهٔ فوق $\eta'=\min\left(R'_{au},R'_{ub}\right)$ است.

۳- شبیه‌سازی و نتایج عددی

در این بخش به‌منظور تأیید نتایج تئوری که در این پژوهش به‌دست‌آمده‌اند، شبیه‌سازی نتایج عددی را ارائه خواهیم کرد. همچنین در این بخش نمودارهایی به‌منظور ارائهٔ پیشنهادهای برای طراحی شبکه‌های مخابراتی پهپادها به‌منظور برآورده‌کردن مخابرات پنهان آورده شده‌اند.

در شبیه‌سازی‌ها پارامترهای انتشار رادیویی برای شرایط محیط شهری به‌صورت $\alpha=4.88$، $\beta=0$. $\xi_0=1,\xi=0$ ، $\lambda_{NL}=-50\,dB,\lambda_L=-40\,dB$ است. همچنین توان نویز دریافتی در پهپادهای شنودگر و پهپاد رله $\sigma_u=\sigma_w=-70\,dBm$ بوده و بیشینه‌ی توان اختصاص‌یافته برای فرستندهٔ زمینی (آلیس) و پهپاد رله به‌صورت $P_{a_{\max}}=P_{u_{\max}}=30\,dBm$ و . $\upsilon=0$ در نظر گرفته‌شده است. همچنین مختصات مکانی آلیس، باب، پهپاد رله و پهپاد شنودگر در فضای سه‌بعدی به ترتیب به‌صورت $A(-400,0,0)$، $B(400,0,0)$، $U(0,0,6)$ و $W(150,0,650)$ بوده و تعداد آنتن‌های فرستندهٔ آلیس $N_a=10$ و حد آستانه‌ی اطمینان $\varepsilon=0.1$ در نظر گرفته‌شده است.

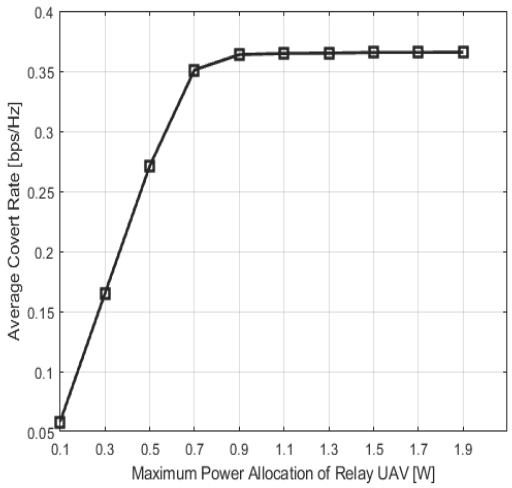
الگوریتم ۱: الگوریتم مقداردهی اولیه پیشنهادی

۱- مقدار اولیه: $\mu=0$ قرار دهید (μ شماره‌ی مقدار اولیه است) و مقدار اولیه دلخواه به $P_a(0)$، $P_j(0)$ و $P_b(0)$ اختصاص دهید.

۲- $P_a=P_a(\mu)$، $P_j=P_j(\mu)$ و $P_b=P_b(\mu)$ را تنظیم نمایید.

۳- مسئله‌ی بهینه‌سازی (۴۳) را برحسب P_a، P_j و P_b حل کرده و نتایج را در $P_a(\mu+1)$، $P_j(\mu+1)$ و $P_b(\mu+1)$ ذخیره نمایید.

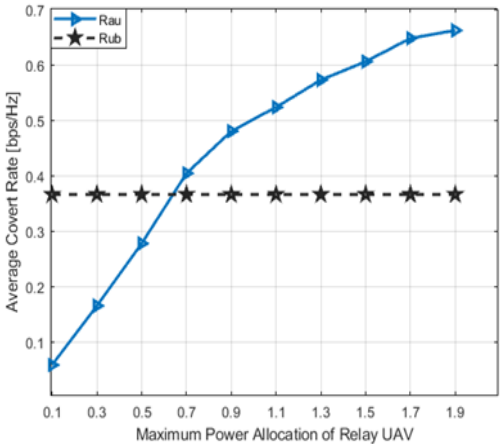
۴- درصورتی‌که $\left|R(\mu+1)-R(\mu)\right|\le\tau$ شد، (R تابع هدف بوده و τ حد آستانه‌ی دلخواه است) الگوریتم متوقف شود. در غیر این صورت $K=K+1$ قرار داده و به مرحله‌ی دوم بازگردید.



شکل (۲). نرخ میانگین شبکه بر حسب افزایش بیشینه‌ی توان ارسال پهپاد رله

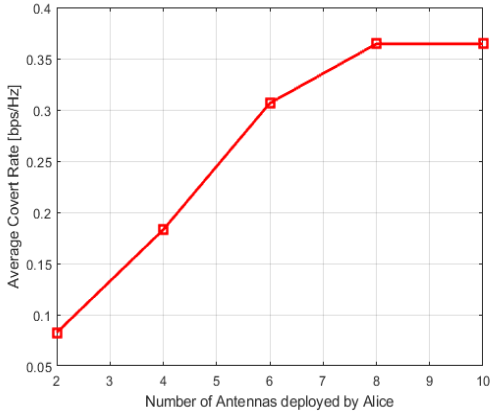
شکل (۲) میانگین نرخ پنهان در دسترس شبکه را برحسب میزان افزایش بیشینهٔ توان ارسال پهپاد رله نمایش می‌دهد. همان‌طور که در این شکل مشاهده می‌شود، زمانی که از ۰٫۱ وات تا ۰٫۷ وات افزایش می‌یابد میانگین نرخ پنهان شبکه نیز صعودی خواهد بود، اما از ۰٫۷ وات به بعد می‌توان گفت که میانگین نرخ

پنهان شبکه ثابت مانده است و با افزایش بیشینهٔ توان ارسال پهپاد رله افزایشی نخواهیم داشت. همان‌طور که در شکل (۳) نشان‌داده‌شده است، علت این امر آن است که میانگین نرخ پنهان شبکه از آلیس به پهپاد رله کمتر از میانگین نرخ پنهان از پهپاد رله به گیرندهٔ زمینی است و طبق مسئلهٔ بهینه‌سازی بعد از توان ۰/۷ وات، میانگین نرخ پنهان شبکه ثابت و برابر نرخ پنهان از پهپاد رله به باب خواهد بود.

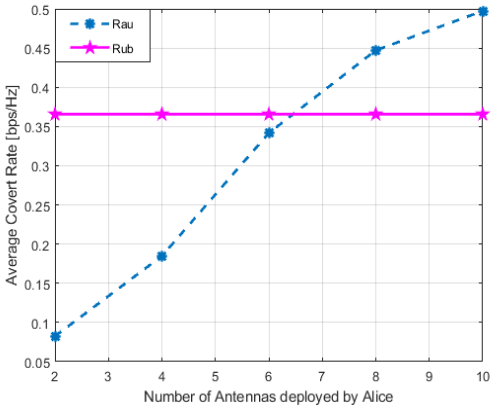


شکل (۳). میانگین نرخ پنهان شبکه از فرستنده به پهپاد رله (R_{au}) و از پهپاد رله به گیرنده‌ی زمینی (R_{ub}) برحسب افزایش توان پهپاد رله

شکل (۴) بیانگر میانگین نرخ پنهان شبکه با افزایش تعداد آنتن‌های بکار گرفته‌شده در فرستندهٔ زمینی (آلیس) است. در این نمودار مشاهده می‌کنیم که با افزایش تعداد آنتن‌های به کار گرفته‌شده در فرستنده میانگین نرخ پنهان شبکه به‌طور چشم‌گیری افزایش می‌یابد و این در حالی است که توان ارسال در پهپاد رله و همچنین توان ارسالی توسط فرستنده ثابت مانده است. علت این امر آن است که با افزایش تعداد آنتن‌ها پوشش فضایی بهتری در ارسال سیگنال‌های داده صورت می‌گیرد و با توجه به شرایط مخابرهٔ پنهان، علاوه بر اینکه مخابرهٔ پنهان حفظ‌شده است میانگین نرخ پنهان شبکه به‌طور چشم‌گیری افزایش می‌یابد. می‌توان نتیجه گرفت که در مواردی که محدودیت افزایش توان ارسالی برای شبکه وجود دارد، به‌کارگیری تعداد آنتن‌های بیشتر می‌تواند نرخ پوشش فضایی بهتری را در اختیار قرار داده و میانگین نرخ پنهان بالاتری را با حفظ شرایط مخابرهٔ پنهان در اختیار قرار دهد؛ اما طبق موارد گفته‌شده در مورد نرخ میانگین برای شکل (۲)، همان‌طور که در شکل (۵) نیز مشاهده می‌شود بعد از به‌کارگیری بیش از ۶ آنتن در فرستنده میانگین نرخ از فرستنده به پهپاد رله بیشتر از میانگین نرخ پنهان از پهپاد رله به گیرنده‌ی زمینی خواهد شد که بر طبق مسئله‌ی بهینه‌سازی میانگین نرخ شبکه، حداقل نرخ دو فاز انتقال خواهد بود و بنابراین طبق نمودار شکل (۵) میانگین نرخ پنهان شبکه برابر R_{ub} خواهد بود.



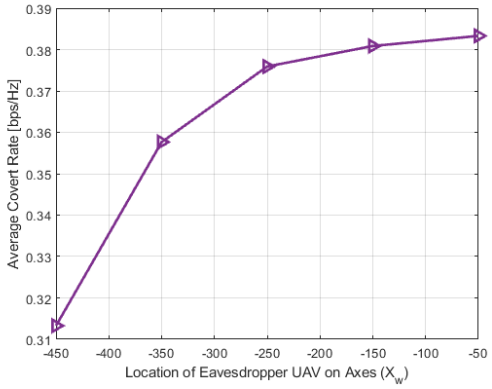
شکل (۴). میانگین نرخ پنهان شبکه بر حسب تعداد آنتن‌های بکار گرفته شده در فرستنده زمینی



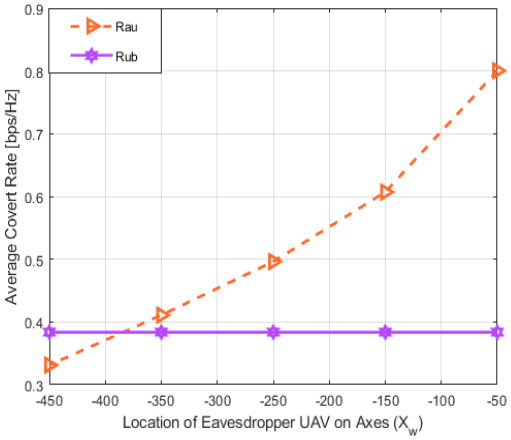
شکل (۵). میانگین نرخ پنهان شبکه از فرستنده به پهپاد رله (R_{au}) و از پهپاد رله به گیرنده‌ی زمینی (R_{ub}) برحسب تعداد آنتن‌های فرستنده زمینی

شکل (۶) میانگین نرخ پنهان شبکه برحسب تغییر مکان پهپاد شنودگر بر روی محور X-ها را نمایش می‌دهد. همان‌طور که از شکل (۶) مشهود است، ابتدا پهپاد شنودگر در حوالی فرستندهٔ زمینی قرار داشته و سپس از آن دور می‌شود. همان‌طور که از این نمودار مشاهده می‌شود با دورشدن پهپاد شنودگر از فرستنده میانگین نرخ پنهان شبکه نزدیک به ۲۲٪ افزایش می‌یابد؛ اما با تجزیه‌وتحلیل شکل (۷) که میانگین نرخ پنهان شبکه را برای فازهای اول و دوم انتقال نشان می‌دهد، درمی‌یابیم که میانگین نرخ پنهان شبکه در فاز اول انتقال با دورشدن پهپاد شنودگر از فرستندهٔ زمینی به طور قابل‌توجهی افزایش‌یافته است. همچنین همان‌طور که شکل (۷) نشان می‌دهد فاصلهٔ پهپاد شنودگر از پهپاد رله بر میزان نرخ پنهان آن تأثیرگذار نخواهد بود. علت این امر آن است که در مخابرات پنهان، شرط ارضاشدن پنهان بودن مخابره به نسبت فاصله شنودگر از فرستنده داده و

فرستنده سیگنال اختلال یعنی به $\frac{\text{فاصله شنودگر از فرستنده سیگنال داده}}{\text{فاصله شنودگر از فرستنده سیگنال اختلال}}$ وابسته است که در مدل سیستم پیشنهادی چون مبدأ داده و سیگنال اختلال در یک مکان قرار دارند این نسبت برابر یک خواهد بود و با افزایش یا کاهش فاصله بین فرستنده و شنودگر تغییری در نرخ امن مشاهده نمی‌شود. همان‌طور که می‌دانیم در عمل یافتن مکان دقیق شنودگر کار دشواری خواهد بود و معمولاً فرستنده تخمینی از محل قرارگیری احتمالی شنودگر دارد و این تخمین همراه با خطا خواهد بود؛ بنابراین یکی از چالش‌هایی که در مخابرهٔ پنهان با آن مواجه خواهیم بود، تخمین مکان شنودگر در شبکه خواهد بود تا فرستنده توان ارسال سیگنال داده و همچنین توان ارسال سیگنال اختلال خود را تنظیم نماید تا خطای آشکارسازی مخابرهٔ پنهان را در شنودگر افزایش دهد. با مدل در نظر گرفته‌شده سیستم برای انتقال از پهپاد رله به گیرنده‌ی زمینی که کیفیت لینک بالاتری را پهپاد شنودگر تجربه خواهد کرد، مستقل از تخمین مکان پهپاد شنودگر خواهد بود.



شکل (۶). میانگین نرخ پنهان شبکه بر حسب تغییر مکان پهپاد شنودگر بر روی محور Xها



شکل (۷). میانگین نرخ پنهان شبکه از فرستنده به پهپاد رله (R_{au}) و از پهپاد رله به گیرنده‌ی زمینی (R_{ub}) بر حسب تغییر مکان پهپاد شنودگر بر روی محور Xها

۴- نتیجه‌گیری

در این پژوهش مخابرهٔ پنهان را در شرایطی مورد بررسی قرار داده‌ایم که یک پهپاد شنودگر در منطقه‌ای سعی در آشکارسازی مخابرهٔ پنهان یک فرستندهٔ زمینی و پهپاد رله را دارد. در این مقاله شرایط مخابرهٔ پنهان را بررسی کردیم و میانگین نرخ پنهان شبکه را با توجه به محدودیت‌های مخابرهٔ پنهان به دست آوردیم و عملکرد شبکه را مورد بررسی قراردادیم. در این شبکه به‌منظور جلوگیری از نیاز به استفاده از یک اخلال‌گر جداگانه از طرح SBJ بهره بردیم تا هم از هزینه‌های به‌کارگیری یک اخلال‌گر جداگانه جلوگیری شود و هم آمادگی شرایطی که در آن استفاده از اخلال‌گر جداگانه فراهم نیست را داشته باشیم. همچنین در شبیه‌سازی‌ها تأثیر به‌کارگیری چندین آنتن در فرستنده را مشاهده نمودیم و دیدیم که استفاده از فن MRT نقش چشمگیری در افزایش نرخ پنهان شبکه خواهد داشت. در انتها تأثیر مکان‌های مختلف پهپاد شنودگر را بر میانگین نرخ پنهان شبکه دیدیم و متوجه شدیم با افزایش فاصلهٔ شنودگر از فرستنده نرخ پنهان در فاز اول انتقال به طور قابل‌توجهی افزایش می‌یابد اما مکان شنودگر بر میانگین نرخ پنهان شبکه در فاز دوم انتقال تأثیری نخواهد داشت و علت این امر را در تحلیل مربوط به شکل (۷) بررسی کردیم.

۵- مراجع

[1] F. Samsami Khodadad, P. Baee, M. Forouzesh, and S. M. J. Asgari Tabatabaie, "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 presence of Friendly Jammer," Sci. J. Electron. Cyber Def., vol. 9, no. 4, pp. 67–76, 2022. [in Persian]

[2] 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.

[3] X. Jiang et al., "Covert Communication in UAV-Assisted Air-Ground Networks," IEEE Wirel. Commun., vol. 28, no. 4, 2021, doi: 10.1109/MWC.001.2000454.

[4] S. Yan, S. V. Hanly, I. B. Collings, and D. L. Goeckel, "Hiding Unmanned Aerial Vehicles for Wireless Transmissions by Covert Communications," in IEEE International Conference on Communications, 2019, vol. 2019-May. doi: 10.1109/ICC.2019.8761271.

[5] X. Zhou, S. Yan, J. Hu, J. Sun, J. Li, and F. Shu, "Joint Optimization of a UAV's Trajectory and Transmit Power for Covert Communications," IEEE

[18] R. Zhang, X. Chen, M. Liu, N. Zhao, X. Wang, and A. Nallanathan, “UAV Relay Assisted Cooperative Jamming for Covert Communications over Rician Fading,” IEEE Trans. Veh. Technol., 2022, doi: 10.1109/TVT.2022.3164051.

[19] 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.

[20] X. Chen, M. Sheng, N. Zhao, W. Xu, and D. Niyato, “UAV-Relayed Covert Communication Towards a Flying Warden,” IEEE Trans. Commun., 2021, doi: 10.1109/TCOMM.2021.3106354.

[21] K. Shahzad, X. Zhou, and S. Yan, “Covert Communication in Fading Channels under Channel Uncertainty,” in IEEE Vehicular Technology Conference, 2017. doi: 10.1109/VTCSpring.2017.8108525 .

[22] S. Talati, M.R, Hassani Ahangar; “Radar Data Processing Using a Combination of Principal Component Analysis Methods and Self-Organized and Digitizing Learning Vector Neural Networks”, Electronic and Cyber Defense, vol. 9, no. 2, pp. 1-7, 2021.

[23] S. Talati, P. Etezadifar; “Providing an Optimal Way to Increase the Security of Data Transfer Using Watermarking in Digital Audio Signals”, MJTD, vol. 10, no. 1, 2020 .

[24] S. Hashemi, S. Barati, S. Talati, H. Noori; “A genetic algorithm approach to optimal placement of switching and protective equipment on a distribution network”. Journal of Engineering and Applied Sciences. vol. 11, pp. 1395-1400, 2016.

[25] S. Hashemi, M. Abyari, S. Barati, T. Tahmasebi, S. Talati; “A proposed method to controller parameter soft tuning as accommodation FTC after unknown input observer FDI”. Journal of Engineering and Applied Sciences, vol. 11, pp. 2818-2829, 2016.

[26] S. Talati, A. Rahmati, and H. Heidari, “Investigating the Effect of Voltage Controlled Oscillator Delay on the Stability of Phase Lock Loops”, MJTD, vol. 8, no. 2, pp. 57-61, 2019.

[27] S. Talati, S.M. Alavi; “Radar Systems Deception using Cross-eye Technique”. Majlesi Journal of Mechatronic Systems, vol. 9, no. 3, pp. 19-21. 2020.

[28] S. Talati, M.R Hasani Ahangar; “Analysis, Simulation and Optimization of LVQ Neural Network Algorithm and Comparison with SOM”, MJTD, vol. 10, no. 1, 2020.

[29] S. Talati, M.R. Hassani Ahangar; “Combining Principal Component Analysis Methods and Self-Organized and Vector Learning Neural Networks for Radar Data”, Majlesi Journal of Telecommunication Devices, vol. 9, no. 2, pp. 65-69, 2020.

[30] M.R. Hassani Ahangar, S. Talati, A. Rahmati, H. Heidari; “The Use of Electronic Warfare and Information Signaling in Network-based Warfare”.

Trans. Signal Process., vol. 67, no. 16, 2019, doi: 10.1109/TSP.2019.2928949.

[6] J. Hu, S. Yan, X. Zhou, F. Shu, and J. Wang, “Covert communication in wireless relay networks,” in 2017 IEEE Global Communications Conference, GLOBECOM 2017 - Proceedings, 2017, vol. 2018-Janua. doi: 10.1109/GLOCOM.2017.8254008.

[7] J. Hu, S. Yan, X. Zhou, F. Shu, J. Li, and J. Wang, “Covert communication achieved by a greedy relay in wireless networks,” IEEE Trans. Wirel. Commun., vol. 17, no. 7, 2018, doi: 10.1109/TWC.2018.2831217.

[8] Q. Wang, Z. Chen, W. Mei, and J. Fang, “Improving Physical Layer Security Using UAV-Enabled Mobile Relaying,” IEEE Wirel. Commun. Lett., vol. 6, no. 3, 2017, doi: 10.1109/LWC.2017.2680449.

[9] C. Zhong, J. Yao, and J. Xu, “Secure UAV Communication With Cooperative Jamming and Trajectory Control,” IEEE Commun. Lett., vol. 23, no. 2, 2019, doi: 10.1109/LCOMM.2018.2889062.

[10] T. Nuradha, K. T. Hemachandra, T. Samarasinghe, and S. Atapattu, “Physical-layer security for untrusted UAV-Assisted full-duplex wireless networks,” 2019. doi: 10.1109/GCWkshps45667.2019.9024575.

[11] H. Wang, J. Wang, G. Ding, J. Chen, Y. Li, and Z. Han, “Spectrum sharing planning for full-duplex UAV relaying systems with underlaid D2D Communications,” IEEE J. Sel. Areas Commun., vol. 36, no. 9, 2018, doi: 10.1109/JSAC.2018.2864375.

[12] P. H. Che, M. Bakshi, and S. Jaggi, “Reliable deniable communication: Hiding messages in noise,” 2013. doi: 10.1109/ISIT.2013.6620765.

[13] Y. Cai, F. Cui, Q. Shi, M. Zhao, and G. Y. Li, “Dual-UAV-Enabled secure communications: Joint trajectory design and user scheduling,” IEEE J. Sel. Areas, Vol. 87, 73-82, 2019. doi:10.2528/PIERM19092802

[14] R. Zhang, X. Chen, M. Liu, N. Zhao, X. Wang, and A. Nallanathan, “UAV Relay Assisted Cooperative Jamming for Covert Communications over Rician Fading,” IEEE Trans. Veh. Technol., p. 1, 2022, doi: 10.1109/TVT.2022.3164051.

[15] W. Liang, J. Shi, Z. Tie, and F. Yang, “Performance Analysis for UAV-Jammer Aided Covert Communication,” IEEE Access, vol. 8, 2020, doi: 10.1109/ACCESS.2020.3001069.

[16] X. Yu, S. Wei, and Y. Luo, “Finite Blocklength Analysis of Gaussian Random Coding in AWGN Channels under Covert Constraint,” IEEE Trans. Inf. Forensics Secur., vol. 16, 2021, doi: 10.1109/TIFS.2020.3032292.

[17] V. U. Prabhu and M. R. D. Rodrigues, “On wireless channels with m-antenna eavesdroppers: Characterization of the outage probability and ε-outage secrecy capacity,” IEEE Trans. Inf. Forensics Secur., vol. 6, no. 3 PART 1, 2011, doi: 10.1109/TIFS.2011.2159491.

Majlesi Journal of Telecommunication Devices, vol. 9, no. 2, pp. 93-97, 2020.

[31] S. Talati, P. Etezadifar; "Providing an Optimal Way to Increase the Security of Data Transfer Using Watermarking in Digital Audio Signals", MJTD, vol. 10, no. 1, 2020 .

[32] M. Aslinezhad, O. Mahmoudi, S. Talati; "Blind Detection of Channel Parameters Using Combination of the Gaussian Elimination and Interleaving". Majlesi Journal of Mechatronic Systems, vol. 9, no. 4, pp. 59-67, 2020.

[33] S. Talati, A. Amjadi; "Design and Simulation of a Novel Photonic Crystal Fiber with a Low Dispersion Coefficient in the Terahertz Band". Majlesi Journal of Mechatronic Systems, vol. 9, no. 2, pp. 23-28, 2020.

[34] S. Talati, S.M. Alavi, H. Akbarzade, "Investigating the Ambiguity of Ghosts in Radar and Examining the Diagnosis and Ways to Deal with it". Majlesi Journal of Mechatronic Systems, vol. 10, no. 2, 2021 .

[35] P. Etezadifar, S. Talati, "Analysis and Investigation of Disturbance in Radar Systems Using New Techniques of Electronic Attack". Majlesi Journal of Telecommunication Devices, vol. 10, no. 2, pp. 55-59, 2021.

[36] S. Talati, B. Ebadi, H. Akbarzade; "Determining of the fault location in distribution systems in presence of distributed generation resources using the original post phasors". QUID, pp. 1806-1812, Special Issue No.1-. April 2017. ISSN: 1692-343X, Medellín-Colombia.

[37] S. Talati, M. Akbari-Thani, M.R Hassani Ahangar; "Detection of Radar Targets Using GMDH Deep Neural Network", Radar Journal, vol. 8, no. 1, pp. 65-74, 2020.

[38] S. Talati, R. Abdollahi, V.R. Soltaninia, M. Ayat; "A New Emitter Localization Technique Using Airborne Direction Finder Sensor". Majlesi Journal of Mechatronic Systems, vol. 10, no. 4, pp. 5-16, 2021.

[39] V. Soltaninia, S. Talati, S.M. Khatmi, Ghaffari; Presenting a New Steganography Method Based on Wavelet Transform in Gray Image. Majlesi Journal of Telecommunication Devices, vol. 12, no. 2, pp. 105-111,2023.doi: 10.30486/mjtd.2023.1983555.1031.

[40] S. Talati, P. EtezadiFar, M.R. Hassani Ahangar, M. Molazade; Investigation of Steganography Methods in Audio Standard Coders: LPC, CELP, MELP. Majlesi Journal of Telecommunication Devices, vol. 12, no. 1, pp. 7-15, 2023. doi: 10.30486/mjtd.2022.695928.

[41] S. Talati, S.M. Ghazali, V.R. SoltaniNia; "Design and construct full invisible band metamaterial-based coating with layer-by-layer structure in the microwave range from 8 to 10 GHz" Journal of Physics D: Applied Physics. Vol. 56, no. 17, 2023. DOI 10.1088/1361-6463/acb8c7.

[42] S.M. Ghazali. J. Mazloum, Y. Balaghi; "Modified binary salp swarm algorithm in EEG signal classification for epilepsy seizure detection" Biomedical Signal Processing and Control. vol. 78, 2022.