استراق سمع فعال با کمک UAV برای بهبود امنیت شبکه‌های مخابرات مشارکتی

سمانه دزفولی‌زاده[1] زهرا مبینی[2]

۱- دانش آموخته کارشناسی ارشد- دانشکده فنی و مهندسی، دانشگاه شهرکرد، شهرکرد، ایران
samane.d1371@gmail.com

۲- استادیار- دانشکده فنی و مهندسی، دانشگاه شهرکرد، شهرکرد، ایران
z.mobini@sku.ac.ir

چکیده: در این مقاله استفاده از هواپیمای بدون سرنشین برای بهبود امنیت لایه فیزیکی و نظارت بر یک شبکه مخابرات مشارکتی پیشنهاد شده است. به طور مشخص در سیستم پیشنهادی از هواپیمای بدون سرنشین به عنوان دیده‌بان قانونی برای نظارت بر لینک‌های ارتباطی مشکوک در یک شبکه رله کننده مشارکتی با پروتکل بازگشایی-و-ارسال استفاده شده است. بطوریکه هواپیمای بدون سرنشین با شنود اطلاعات ارسالی و/یا با فرستادن سیگنال‌های تداخلی، گیرنده یا رله غیرمجاز را به‌اشتباه وادار می‌کند و باعث افزایش نرخ استراق سمع در گره دیده‌بان می‌شود. بر اساس موقعیت قرارگیری هواپیمای بدون سرنشین و فاصله نسبی آن از فرستنده‌های مشکوک یعنی مبدا و رله، دو سناریو با هدف بهبود امنیت سیستم، به صورت تطبیقی پیشنهاد می‌شود: ۱) تداخل‌گر-شنودگر، ۲) شنودگر-کمک‌کننده/ شنودگر-شنودگر/شنودگر-تداخل‌گر. در ادامه نرخ استراق سمع برای دو سناریو استخراج می‌شود و نشان داده می‌شود که سناریوهای پیشنهادی در این مقاله نسبت به روش‌های رایج بازدهی خیلی بهتری دارند. همچنین نشان می‌دهیم که، برای حصول بهترین بازدهی نرخ استراق سمع، هواپیمای بدون سرنشین باید وقتی که نزدیک به مبدا است سناریو ۲ را اجرا کند و بالعکس وقتی نزدیک به رله است سناریو ۱ را اجرا کند.

واژه‌های کلیدی: هواپیمای بدون سرنشین، دیده‌بان قانونی، نرخ استراق سمع، مخابرات مشارکتی.

نوع مقاله: پژوهشی

DOI: 10.29252/jiaeee.18.3.980

تاریخ ارسال مقاله : ۱۳۹۸/۶/۲۳

تاریخ پذیرش مشروط مقاله: ۱۳۹۹/۰۶/۲۰

تاریخ پذیرش مقاله: ۱۳۹۹/۷/۲

نام نویسنده‌ی مسئول: دکتر زهرا مبینی

نشانی نویسنده‌ی مسئول: ایران، شهرکرد، بلوار رهبر، دانشگاه شهرکرد، دانشکده فنی و مهندسی، گروه الکترونیک و مخابرات. کد پستی: 81186-34141.

۱- مقدمه

ارتباطات بی‌سیم یک ابزار کارآمد و راحت برای برقراری ارتباط بین مردم و دستگاههای بی‌سیم است. بااین‌حال، با توجه به ماهیت بازپخش رسانه‌های بی‌سیم، ارتباطات بین آنها در معرض تهدید امنیتی قرار دارد و برقراری اتصالات قابل‌اعتماد در این شبکه‌ها یک کار چالش‌برانگیز است. امروزه ضرورت نظارت بر فعالیت‌های دستگاه‌های بی‌سیم به‌ویژه تهدیدات امنیتی افزایش‌یافته است. امنیت لایه فیزیکی[۱] به‌عنوان یک روش امیدوارکننده برای برقراری ارتباطات امن، در سال‌های اخیر توجه زیادی را به خود جلب کرده است [۶-۱]. در این میان تکنیک‌های مختلفی مانند ارسال نویز مصنوعی[۲] و سیگنال تداخل‌گر و روش‌های دیگر برای بهبود امنیت عملکرد لایه فیزیکی پیشنهادشده است [۸-۷]. هم‌چنین ارتباطات بی‌سیم ممکن است توسط کاربران مخرب به‌منظور ارتکاب جرائم یا حملات تروریستی مورد سوءاستفاده قرار گیرد[۹]؛ بنابراین نیازهای رو به رشد برای سازمانهای مجاز و قانونی مانند سازمان‌های دولتی در نظارت بر ارتباطات مشکوک برای اطمینان از امنیت و جلوگیری از حملات تروریست دیده می‌شود. در مقاله[۱۲-۱۰] یک الگوی جدیدی در امنیت بی‌سیم با بررسی این‌که چگونه دیده‌بان[۳] قانونی نظارت بر اطلاعات قانونی را انجام می‌دهد، پیشنهادشده است. به‌طور خاص در این مقاله نویسندگان یک رویکرد جدیدی را پیشنهاد داده‌اند که در آن دیده‌بان قانونی به‌طور هدفمند سیگنال تداخل‌گر[۴] را برای دخالت در لینک مشکوک ارسال می‌کند.در مقاله [۱۴-۱۳] روش جدید دیگری در امنیت لایه فیزیکی پیشنهاد می‌شود که استراق سمع فعال[۵] و مداخله قانونی از طریق تکنیک‌هایی مانند تداخل یا حقه‌بازی[۶] باعث افزایش امنیت می‌شوند. برای استراق سمع فعال در مقاله [۱۵] رویکرد دیگری بر اساس حقه‌بازی پیشنهاد می‌شود. برای به حداکثر رساندن نرخ استراق سمع در این مقاله دو روش برای دیده‌بان قانونی طراحی‌شده است که می‌تواند به‌صورت سازگار به‌عنوان یک استراق سمع کننده اطلاعات، مخرب تداخل یا یک کمک‌کننده سازنده در دو بازه زمانی عمل کند. در هر سناریو، پرتو تداخل‌گر و قدرت تداخل‌گر بهینه استخراج می‌شوند. نتایج عددی در این مقاله نشان می‌دهد که سناریوهای پیشنهادی عملکرد بهتری نسبت به بسیاری از طرح‌های سنتی دارند. البته توجه داشته باشید که برای فعال کردن استراق سمع و تداخل‌گر به‌صورت هم‌زمان، دیده‌بان باید مجهز به دو آنتن باشد که یکی برای دریافت اطلاعات و دیگری برای ارسال است؛ برای بهبود امنیت می‌توان از ویژگی محو شدن در محیط بی‌سیم، نویز و تداخل استفاده کرد تا کاربر غیرمجاز را وادار به‌اشتباه کرد.

از طرف دیگر در سال‌های اخیر استفاده از هواپیماهای بدون سرنشین یا UAV[۷] به‌عنوان ایستگاه پایه هوایی یا رله هوایی برای بهبود اتصال و پوشش دستگاه‌های بی‌سیم زمینی در شبکه‌های مخابرات مشارکتی بسیار مورد توجه قرار گرفته است. در مقایسه با ایستگاه پایه زمینی، مزیت استفاده از ایستگاه‌های هوایی، توانایی آن‌ها در ارایه ارتباطات از ارتفاع بالا با دید مستقیم یا LoS[۸] است. شبکه‌های رله کننده مشارکتی با کمک UAV نیز می‌توانند ارتباطات قابل اطمینانی برای کاربران زمینی فراهم کنند و ظرفیت شبکه را به میزان زیادی افزایش دهد. در مقایسه با رله زمینی، رله هوایی قادر به دست‌یابی به بازده قابل توجهی است. به‌عبارت‌دیگر، رله هوایی با کمک بهینه‌سازی توان و ارتفاع قرار گیری قادر به بهبود بازدهی طیفی، توانی و امنیت شبکه است. یکی دیگر از تکنولوژی‌هایی که می‌تواند به بهبود بازدهی در شبکه‌های مخابرات مشارکتی کمک کند، استفاده از رله هوایی متحرک یا سیار است. در این حالت مسیر حرکت UAV به‌صورت پویا تنظیم می‌شود تا بازدهی ارتباط را از طریق پیدا کردن مسیر و موقعیت مکانی بهینه بهبود دهد. در مقایسه با رله ثابت، رله سیار دارای چندین مزیت کلیدی است. سیستم‌های رله سیار بر اساس تقاضا، مقرون به‌صرفه‌تر هستند و می‌تواند برای وقایع غیرمنتظره یا موقت مانند پاسخ اضطراری، عملیات نظامی و امنیتی بسیار سریع‌تر به کار گرفته شوند [۱۶]. هم‌چنین به‌منظور فراهم کردن ارتباط کوتاه مدت، استفاده موقتی از UAV به عنوان ایستگاه پایه هوایی یا رله در مقایسه با نصب موقت ایستگاه پایه زمینی یا رله سریع‌تر و ارزان‌تر است. علاوه بر این در مناطق یا کشورهایی که زیرساخت سلولی بسیار گران است، استفاده از هواپیماهای بدون سرنشین به‌عنوان رله سیار یا ایستگاه پایه هوایی بسیار مفید است، زیرا نیاز به برج‌ها و کابل‌ها را حذف می‌کند. همچنین، تحرک بالای رله سیار همواره فرصت‌های جدیدی را برای بهبود عملکرد از طریق تنظیم پویای مکان‌های رله برای بهتر کردن محیط ارتباطی ارایه می‌دهد. این تکنیک به‌ویژه برای سرویس‌های تأخیر پذیر یا delay tolerant در شبکه [۱۹-۱۷] کاربرد بسیار دارد. به‌طور کلی استفاده ازUAV به‌عنوان ایستگاه پایه هوایی باعث افزایش بازدهی، ظرفیت و پوشش‌دهی شبکه می‌شود و استفاده از آن اخیرا بسیار مورد استقبال قرار گرفته است [۲۰].

در زمینه امنیت لایه فیزیکی، استراق سمع کنندگان غیرقانونی زیادی وجود دارد که قصد دارند به اطلاعات محرمانه دست یابند؛ حتی مجرمان و توریست‌ها، می‌توانند تهدیدات مهمی برای امنیت ملی ایجاد کنند. بنابراین، برای جلوگیری از جرائم و حملات توریستی، برای سازمان‌های دولتی نظارت قانونی بر هرگونه لینک‌های مشکوک یک نیاز جدی است که رفتارهای غیرعادی را شناسایی کند. برای نظارت بر ارتباطات بی‌سیم، یک روش ساده روشی است که در آن دیده‌بان قانونی به‌راحتی به لینک‌های مشکوک گوش دهد. بااین‌وجود، دیده‌بان قانونی ممکن است به‌طورکلی از فرستنده مشکوک دور باشد و اطلاعات را نتواند آشکارسازی کند. با توجه به اهمیت موضوع، مقالات زیادی وجود دارد که ارتباطات مشکوک را با استفاده از یک دیده‌بان قانونی موردمطالعه قرار می‌دهند [۲۳-۲۱].

در این مقاله با توجه به مزایای بالقوه‌ای هواپیماهای بدون سرنشین در افزایش امنیت، سطح پوشش و بازدهی شبکه، طرح جدیدی برای استفاده از UAV به عنوان دیده‌بان قانونی ارایه می‌شود. به طور مشخص، در این مقاله برای اولین بار طرحی امن برای نظارت بر ارتباطات مشکوک و در معرض تهدید شبکه‌های رله کننده مشارکتی با کمک هواپیمای بدون سرنشین پیشنهاد می‌شود. در شبکه رله کننده مشارکتی مورد نظر یک گره مبدأ، یک گره مقصد، یک گره رله وجود دارد. در این شبکه علاوه بر این‌که لینک مستقیمی از گره مبدأ به گره مقصد وجود دارد، گره مبدأ با کمک گره رله (که پروتکل بازگشایی و ارسال DF[9] را اتخاذ کرده است) با گره مقصد ارتباط برقرار می‌کند. برای نظارت بر اطلاعات ارسالی از مبدأ به مقصد، مبدأ به رله و رله به مقصد از UAV استفاده‌شده است که مانند یک دیده‌بان قانونی عمل می‌کند و سعی می‌کند پیام ارسالی از مبدأ و رله مشکوک را شنود کند. در این مقاله پروتکل اشتراک‌گذاری زمانی را در نظر می‌گیریم، به‌عبارتی کل ارتباط در دو فاز انجام می‌شود. در فاز اول (یا بازه زمانی اول) مبدأ اطلاعات را می‌فرستد و رله گوش می‌دهد و سپس رله اطلاعات رمزگشایی‌شده را در فاز دوم (یا بازه زمانی دوم) به سمت مقصد می‌فرستد. در طرح پیشنهادی ما UAV با استراق سمع کردن اطلاعات و با فرستادن سیگنال نویز و تداخل کاربر غیرمجاز را به‌اشتباه وادار می‌کند. به طور مشخص در این مقاله بر اساس موقعیت قرارگیری و فاصله دیده‌بان قانونی UAV از فرستنده‌های مشکوک

یعنی مبدأ و رله، برای هواپیمای بدون سرنشین دو استراتژی زیر با هدف بهبود امنیت سیستم، به صورت تطبیقی پیشنهاد می‌شود:

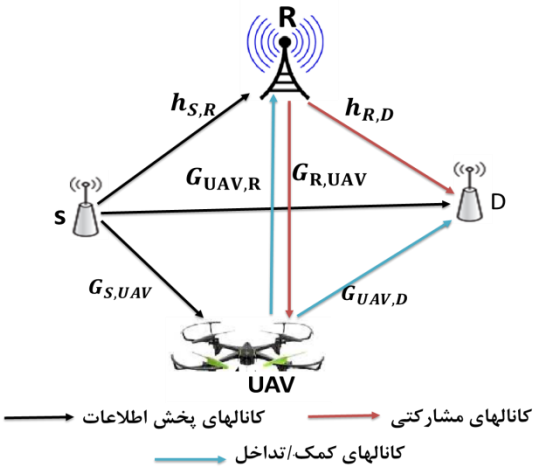
۱) تداخل‌گر-شنودگر، ۲) شنودگر–کمک‌کننده، شنودگر- شنودگر یا شنودگر-تداخل‌گر. در استراتژی اول هواپیمای بدون سرنشین در نقش تداخل‌گر در فاز اول ارسال و شنودگر در فاز دوم ارسال عمل می‌کند. در استراتژی دوم در فاز اول ارسال هواپیمای بدون سرنشین در نقش تداخل‌گر است و در فاز دوم بسته به کیفیت نسبی لینک‌های ارتباطی مشکوک و لینک شنود یکی از نقش‌های کمک‌کننده، شنودگر یا تداخل‌گر را خواهد داشت. نتایج شبیه‌سازی نشان می‌دهد که استراتژی‌های پیشنهادی در این مقاله به میزان زیادی نرخ استراق سمع[10] و در نتیجه امنیت لایه فیزیکی شبکه مشارکتی را در مقایسه با روش‌های رایج بهبود می‌دهند.

لازم به ذکر است که در میان مراجع موجود تنها مقاله [۲۳] به بحث دیده‌بانی در شبکه‌های رله کننده مشارکتی پرداخته است. اما مدل سیستم مورد بررسی در مقاله [۲۳] برای کاربران زمینی است و استفاده از UAV در آن در نظر گرفته نشده است. اما به طور مشخص، در این مقاله بر خلاف مقاله [۲۳]، برای نظارت بر ارتباطات مشکوک و در معرض تهدید شبکه‌های رله کننده مشارکتی، ایده استفاده از هواپیمای بدون سرنشین مطرح شده است. در شبکه های مبتنی بر هواپیمای بدون سرنشین، یکی از مهم‌ترین چالش‌ها، مدل سازی کانال‌های هوا به زمین یا زمین به هوا است که متفاوت با مدل‌سازی کانال‌های بیسیم زمینی مانند [۲۳] است. بنابراین مدل‌سازی کانال‌ها در این مقاله با مرجع [۲۳] کاملا متفاوت است و منجر به روابط تحلیلی کاملا متفاوت برای دو سیستم خواهد شد. از طرف دیگر با توجه به همه مزایای مهمی که برای سیستم‌های مبتنی بر هواپیمای بدون سرنشین اشاره شد، بررسی و تحلیل بازدهی سیستم نظارت قانونی مبتنی بر UAV ضروری به نظر می‌رسد. ضمن اینکه مدل سیستم نظارت قانونی مبتنی بر هواپیمای بدون سرنشین پیشنهادی در مقاله ما، دارای کاربردهای ویژه برای مکان‌های صعب‌العبور، شرایط وقوع بلایای طبیعی، دیده‌بانی‌های موقت در بسیاری از عملیات‌های نظامی و تغییر پویای مکان دیده‌بان دارد. از طرف دیگر تا آنجا که نویسندگان این مقاله مطلع هستند، سیستم رله‌کننده مشارکتی با دیده‌بان قانونی مبتنی بر هواپیمای بدون سرنشین تا قبل از این مقاله تاکنون در هیچ مرجعی بررسی نشده است و نتایج ارایه شده در این مقاله می‌تواند به عنوان یک مرجع برای تحلیل‌های بعدی بر روی امنیت سیستم‌های مبتنی بر UAV قرار گیرد.

۲- مدل سیستم

در این مقاله یک سیستم ارتباطات بی‌سیم شامل یک گره مبدأ (S)، یک گره مقصد (D)، یک گره رله (R) و یک هواپیمای بدون سرنشین (UAV) در نظر گرفته می‌شود. سیستم ارتباطی موردنظر در شکل ۱ نشان داده‌شده است. تمام گره‌ها مجهز به یک آنتن هستند. فرض شده است علاوه بر این‌که لینک مستقیمی از گره مبدأ (S) به گره مقصد (D) وجود دارد، گره مبدأ (S) با کمک یک گره رله (R) که پروتکل بازگشایی و ارسال DF را اتخاذ کرده است، با گره مقصد (D) ارتباط برقرار می‌کند. برای نظارت بر اطلاعات از UAV استفاده‌شده است که مانند یک دیده‌بان قانونی عمل می‌کند و سعی می‌کند پیام ارسالی از دو فرستنده مشکوک را شنود کند؛ بنابراین، UAV با استراق سمع کردن اطلاعات و با فرستادن سیگنال نویز و تداخل گیرنده غیرمجاز را به‌اشتباه وادار می‌کند. در این مقاله پروتکل اشتراک‌گذاری زمانی را در نظر می‌گیریم. به‌عبارتی کل زمان ارتباطی از دو بازه زمانی تشکیل‌شده است. در بازه زمانی اول منبع اطلاعات را می‌فرستد و رله گوش می‌دهد و سپس رله اطلاعات رمزگشایی‌شده را در بازه زمانی دوم به سمت مقصد می‌فرستد.

کانال‌های متناظر با لینک‌های زمین به زمین $S \to R$، $S \to D$و $R \to D$، به ترتیب با $h_{S,R}$، $h_{S,D}$ و $h_{R,D}$ نشان داده می‌شوند. همچنین فواصل اقلیدوسی بین زوج‌های لینک‌های $S \to R$، $S \to D$و $R \to D$، به ترتیب با نمادهای $d_{S,R}$، $d_{S,D}$، $d_{R,D}$، نشان داده می‌شوند. توجه کنید که برای مدل سازی دقیق‌تر کانال‌های زمین به زمین فرض می‌شود که کانال‌های زمینی هم تحت تاثیر تلفات مسیر مقیاس بزرگ و هم فیدینگ رایلی مقیاس کوچک هستند [۲۴]. به عنوان مثال کانال زمین به زمین $h_{S,R}$ به‌صورت $h_{S,R} = \frac{1}{\sqrt{A^{\alpha} d_{SR}^{\alpha}}} f_{S,R}$ مدل می‌شود که α ضریب تلفات مسیر است که در محیط‌های عملی مقدار آن بسته به جنس و نوع محیط انتشار در محدوده $2 \le \alpha \le 6$ است [24]. $f_{S,R}$ بیانگر اثر فیدینگ رایلی است که به صورت متغیر تصادفی گوسی مختلط با میانگین صفر و واریانس یک مدل می‌شود. در این فرمول $A = \left(\frac{4\pi f_c}{c}\right)$ و f_c فرکانس کریر و c سرعت نور است. لازم به ذکر است که با تغییر مناسب اندیس‌ها، سایر کانال‌های زمین به زمین نیز به همین صورت مدل می‌شوند.



شکل (۱): مدل یک سیستم رله کننده مشارکتی با حضور UAV به عنوان دیده‌بان قانونی

همچنین کانال‌های زمین به هوا یا هوا به زمین متناظر با لینک‌های $S \to UAV$، $R \to UAV$ و $UAV \to D$، به‌ترتیب با $G_{S,UAV}$ و $G_{R,UAV}$ و فواصل اقلیدوسی متناظر با این لینک ها به ترتیب با $d_{S,UAV}$ و $d_{R,UAV}$ نمایش داده می‌شوند. تذکر اینکه به دلیل تقارن فرض می‌شود که کانال‌های دو لینک $R \to UAV$ و $UAV \to R$ یعنی $G_{R,UAV}$ و $G_{R,UAV}$ با هم یکسان است.

در این مقاله برای مدل کردن کانال‌های هوا به زمین یا زمین به هوا از مدل کاربردی آماری استفاده می‌شود [25] و [26]. به طور مشخص در این مدل احتمال اینکه لینک ارتباطی بین UAV و کاربر زمینی در دید مستقیم باشد، بستگی به نوع محیط، ارتفاع پرواز UAV و زاویه فراز یا elevation angle بین UAV و کاربر زمینی دارد. به عنوان مثال تقریب احتمال LoS یعنی $\Pr_{LoS}$ برای لینک ارتباطی $S \to UAV$ به‌صورت زیر بدست می‌آید [25] و [26]:

$$\Pr_{LoS} = \frac{1}{1 + a\exp(-b[\theta_{S,UAV} - a])} \quad (۱)$$

$$d_{S,UAV} = \sqrt{(x_S - x_{UAV})^2 + (y_S - y_{UAV})^2 + (H)^2} \quad (۲)$$

$$\theta_{S,UAV} = \frac{180}{\pi} \sin^{-1}\left(\frac{H}{d_{S,UAV}}\right) \quad (۳)$$

در رابطه بالا a و b عدد ثابت می‌باشند که وابسته به نوع محیط ارتباطی و فرکانس ارتباطی هستند. $\theta_{S,UAV}$ زاویه فراز بین مبدا و UAV است. (x_S, y_S) بیانگر موقعیت مکانی مبدا است و (x_{UAV}, y_{UAV}, H) موقعیت مکانی UAV هستند که H ارتفاع پرواز UAV است. احتمال داشتن لینک دید غیر مستقیم NLoS یعنی $\Pr_{LoS}$ به‌صورت

$$\Pr_{NLOS} = 1 - \Pr_{LOS}$$

است؛ بنابراین رابطه نهایی کانال $S \to UAV$ به‌صورت زیر به دست می‌آید [25] و [26]:

$$G_{S,UAV} = \left(pr_{LoS} d_{S,UAV}^{\alpha} + pr_{NLoS}\ \eta d_{S,UAV}^{\alpha}\right)^{-\frac{1}{2}} \quad (۴)$$

که η ضریب تضعیف اضافی ناشی از اتصالات NLoS است. سایر کانال‌های هوا به زمین یا زمین به هوا یعنی $G_{R,UAV}$ و$G_{UAV,\ D}$به همین صورت با تغییر مناسب اندیس‌ها بر اساس روابط (۱) تا (۴) محاسبه می‌شوند.

۲-۱- تعریف نرخ استراق سمع

نرخ استراق سمع یک معیار مهم در بحث امنیت لایه فیزیکی می‌باشد که هر چقدر مقدار بالاتری داشته باشد نشان می‌دهد که عملیات دیده‌بانی برای لینک‌های مشکوک در شبکه با بازدهی بهتری انجام

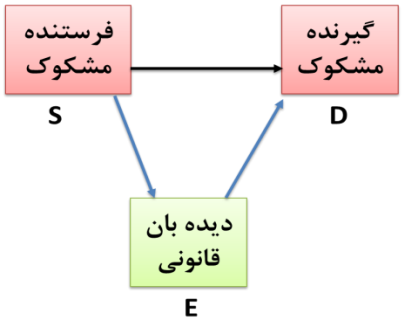
می‌شود. برای توضیح نرخ استراق سمع از شکل ۲ استفاده می‌کنیم. فرض کنید S یک فرستنده مشکوک و D یک گیرنده مشکوک باشد در حالی‌که E یک دیده‌بان قانونی است که بر سیستم نظارت می‌کند. حداکثر نرخ قابل حصول در لینک‌های مشکوک و لینک شنود یا دیده‌بانی به ترتیب عبارت است از

$$C_{SD}=\frac{1}{2}\min\left(\log(1+SINR_R),\log(1+SINR_D)\right)$$

و

$$C_{SE}=\frac{1}{2}\log(1+SNR_E)$$

دقت کنید که $SINR_D$ و $SINR_R$ به ترتیب نسبت سیگنال به نویز و تداخل[11] (SINR) در مقصد و رله می‌باشند که با توجه به نوع سناریو بکار گرفته شده برای دیده‌بانی روابط متفاوتی خواهند داشت که در بخش بعد استخراج می‌شوند. SNR_E هم نسبت سیگنال به نویز[12] (SNR) در دیده‌بان قانونی است. در این مقاله هواپیمای بدون سرنشین یا UAV نقش دیده‌بان قانونی را دارد و در بخش‌های بعدی این مقاله به جای نماد E از UAV استفاده خواهد شد. همچنین دقت کنید که فاکتور $\frac{1}{2}$ در روابط به این دلیل است که کل ارتباط در دو بازه زمانی صورت می‌گیرد.



شکل (۲): یک سیستم نظارت قانونی شامل یک فرستنده S و گیرنده D مشکوک و دیده‌بان قانونی E [۱۱].

اگر رابطه $C_{SE}\geq C_{SD}$ برقرار باشد مطمئن هستیم که دیده‌بان قانونی به‌خوبی اطلاعات را رمزگشایی می‌کند. بنابراین نرخ استراق سمع برابر خواهد بود با $\Re=C_{SD}$ [۲۳].
اگر $C_{SE}\leq C_{SD}$ برقرار باشد برای دیده‌بان قانونی امکان بازگشایی اطلاعات بدون خطا وجود ندارد و در این حالت نرخ استراق سمع موثر برابر با $\Re=0$ خواهد بود.

۳- بیان مسئله

در این مقاله پیشنهاد شده است که برای بهبود امنیت لایه فیزیکی و نظارت بر اطلاعات ارسالی از مبدأ به مقصد، مبدأ به رله و رله به مقصد از UAV استفاده‌شود. در حقیقت در طرح پیشنهادی UAV یا اطلاعات ارسالی از فرستنده‌های مشکوک را استراق سمع می‌کند و یا با فرستادن سیگنال نویز و تداخل کاربر غیرمجاز را به اشتباه وادار می‌کند و امنیت سیستم را بهبود می‌دهد. به طور مشخص در این مقاله بر اساس موقعیت قرارگیری و فاصله دیده‌بان قانونی UAV از فرستنده‌های مشکوک یعنی مبدأ و رله و کیفیت لینک‌های ارتباطی، برای هواپیمای بدون سرنشین دو استراتژی زیر با هدف بهبود نرخ استراق سمع پیشنهاد می‌شود:
۱) تداخل‌گر-شنودگر ، ۲) شنودگر-کمک‌کننده/ شنودگر-شنودگر/ شنودگر-تداخلگر. در استراتژی اول هواپیمای بدون سرنشین در نقش تداخل‌گر در فاز اول ارسال و شنودگر قانونی در فاز دوم ارسال عمل می‌کند. در استراتژی دوم در فاز اول UAV به‌عنوان شنودگر قانونی عمل می‌کند و در فاز دوم ارسال بسته به کیفیت نسبی لینک‌های ارتباطی مشکوک و لینک شنود، برای UAV یکی از نقش‌های کمک کننده، شنودگر یا تداخلگر در نظر گرفته می‌شود.
در ادامه این دو استراتژی به‌طور دقیق بررسی می‌شوند و روابط سیگنال به تداخل و نویز و نرخ استراق سمع استخراج می‌گردد.

۳-۱- سناریو اول: تداخل‌گر-شنودگر

این سناریو زمانی قابل‌استفاده است که UAV از S نسبتا دور است؛ بنابراین UAV در این سناریو نمی‌تواند استراق سمع کننده خوبی باشد؛ بنابراین در مرحله اول، S سیگنال اطلاعات را برای R و D ارسال می‌کند و به‌طور هم‌زمان UAV نویز مصنوعی را برای مختل کردن ارتباطات مشکوک می‌فرستد. سیگنال دریافتی در R به‌صورت زیر است:

$$y_{R}=\sqrt{P_S}h_{S,R}x+\sqrt{P_R}G_{UAV,R}x_J+n_R \qquad (۵)$$

که x و x_J به ترتیب نماد سیگنال اطلاعات و سیگنال تداخل با قدرت یک است و n_R نویز سفید جمع‌شونده[13] (AWGNs) با توزیع گوسی با میانگین صفر و واریانس یک در گره رله است. گره‌ی رله پروتکل بازگشایی و ارسال DF را اتخاذ می‌کند. بنابراین بعد از دریافت سیگنال، ابتدا سیگنال x را رمزگشایی کرده و سپس سیگنال را به گره‌ی مقصد می‌فرستد؛ بنابراین سیگنال دریافتی در مقصد به‌صورت زیر است.

$$y_{D_1}=\sqrt{P_S}h_{S,D}x+\sqrt{P_{UAV}}G_{UAV,D}x_J+n_{D_1} \qquad (۶)$$

دقت کنید که P_S و P_{UAV} به ترتیب قدرت سیگنال ارسالی از S و UAV است. n_{D_1} نویز سفید جمع‌شونده با توزیع گوسی با میانگین صفر و واریانس یک در گره مقصد است.

در مرحله دوم، R ابتدا اطلاعات را از S رمزگشایی می‌کند و سپس اطلاعات رمزگشایی‌شده را ارسال می‌کند، درحالی‌که UAV سعی می‌کند سیگنال را از فاصله دوری شنود کند؛ بنابراین سیگنال دریافتی در D و UAV عبارت است از:

$$y_{D_2=}\sqrt{P_R}h_{R,D}x+n_{D2} \quad (۷)$$

$$y_{UAV}=\sqrt{P_R}G_{R,UAV}x+n_{UAV} \quad (۸)$$

توجه کنید که P_R قدرت سیگنال ارسالی از رله است. n_{D2} و n_{UAV} نویز سفید جمع شونده با واریانس یک و میانگین صفر در گره مقصد و گره UAV است. گره مقصد دو نسخه از سیگنال ارسالی را دریافت می‌کند و برای افزایش کیفیت سیگنال از روش ماکزیمم نرخ ترکیبی[۱۴] (MRC) برای ترکیب نسخه‌های دریافتی استفاده می‌کند؛ بنابراین نسبت سیگنال به نویز و تداخل در رله و مقصد به ترتیب به‌صورت زیر به دست می‌آید:

$$SINR_R=\frac{P_S\left|h_{S,R}\right|^2}{P_R\left|G_{UAV,R}\right|^2+N_0} \quad (۹)$$

$$SINR_D=\frac{P_S\left|h_{S,D}\right|^2}{P_{UAV}\left|G_{UAV,D}\right|^2+N_0}+\frac{P_R}{N_0}\left|h_{R,D}\right|^2 \quad (۱۰)$$

و SNR در UAV برابر خواهد بود با:

$$SNR_{UAV}=\frac{P_R}{N_0}\left|G_{R,UAV}\right|^2 \quad (۱۱)$$

۳-۲- سناریو دوم: شنودگر-کمک‌کننده/ شنودگر-شنودگر/ شنودگر-تداخلگر

برخلاف سناریو اول، درصورتی‌که کیفیت کانال S-UAV خوب باشد، یعنی S به UAV نزدیک باشد بهتر است که در فاز اول، UAV عملیات استراق سمع یا شنود را انجام دهد. در این حالت، در فاز اول S اطلاعات را به R و D منتشر می‌کند، درحالی‌که UAV سعی می‌کند اطلاعات را شنود کند. سیگنال دریافتی در R، D و UAV به ترتیب به‌صورت زیر است:

$$y_R=\sqrt{P_S}h_{S,R}x+n_R \quad (۱۲)$$

$$y_{D_1}=\sqrt{P_S}h_{S,D}x+n_{D_1} \quad (۱۳)$$

$$y_{UAV}=\sqrt{P_S}G_{S,UAV}x+n_{UAV} \quad (۱۴)$$

سیگنال به نویز در R و UAV به صورت زیر نوشته می‌شود:

$$SNR_R=\frac{P_S}{N_0}\left|h_{S,R}\right|^2 \quad (۱۵)$$

$$SNR_{UAV}=\frac{P_S}{N_0}\left|G_{S,UAV}\right|^2 \quad (۱۶)$$

در فاز دوم ارسال اطلاعات، متناسب باکیفیت کانال مشکوک و کیفیت کانال استراق سمع، UAV می‌تواند برای بهبود نرخ استراق سمع یکی از نقش‌های کمک کننده/ شنودگر/ تداخلگر را داشته باشد. در ادامه به تفکیک هر کدام از این نقش‌ها توضیح داده می‌شود.

۳-۲-۱- عملیات اول- کمک‌کننده[۱۵]:

اگر رابطه $SNR_R \le SNR_{UAV}$ برقرار باشد، مطمئن هستیم که UAV به اطلاعات مشکوک دسترسی پیدا می‌کند و کانال مشکوک را به خوبی می‌تواند شنود کند. بنابراین به‌منظور بهبود نرخ استراق سمع، UAV به عنوان کمک کننده عمل می‌کند و تلاش می‌کند تا نرخ استراق سمع موثر را افزایش می‌دهد. سیگنال دریافتی در D به‌صورت زیر بیان می‌شود:

$$y_{D_2}=\sqrt{p_R}\,h_{R,D}x+\sqrt{p_{UAV}}G_{UAV,D}x+n_{D_2} \quad (۱۷)$$

برای داشتن یک مقایسه عادلانه[۱۶] بین سناریوهای مختلف، ماکزیمم قدرت ارسالی در سناریو ۱ را به صورت $0 \le P_{UAV} \le P$ محدود می‌کنیم. سیگنال به نویز متناظر در گره‌های D و R به ترتیب به صورت زیر به دست می‌آید:

$$SNR_D=\frac{P_S}{N_0}\left|h_{S,D}\right|^2+\frac{p_R}{N_0}\left|h_{R,D}\right|^2+\frac{P_{UAV}}{N_0}\left|G_{UAV,D}\right|^2 \quad (۱۸)$$

$$SNR_R=\frac{P_S}{N_0}\left|h_{S,R}\right|^2 \quad (۱۹)$$

۳-۲-۲- عملیات دوم: شنودگر

اگر رابطه $SNR_R > SNR_{UAV}$ را داشته باشیم، مطمئن هستیم که UAV اطلاعات مشکوک را نمی‌تواند با موفقیت در فاز اول رمزگشایی کند، بنابراین UAV می‌تواند در فاز دوم به عنوان یک استراق سمع کننده یا شنودگر عمل کند و شنود لینک‌ها را ادامه دهد یا به عنوان یک تداخل‌گر عمل کند. اگر UAV به عنوان شنودگر

رفتار کند، سیگنال دریافتی در D وUAV به ترتیب به‌صورت زیر خواهد بود:

$$y_{D_2} = \sqrt{P_R} h_{R,D} x + n_{D_2} \quad (۲۰)$$

و

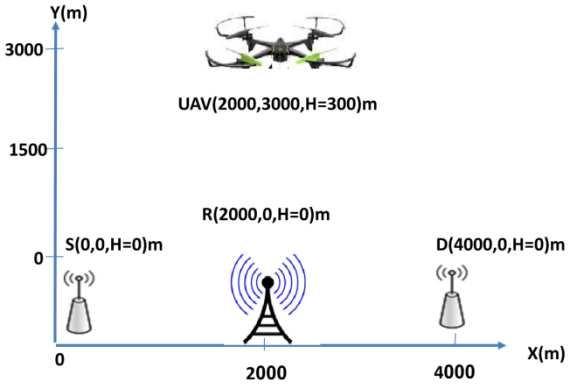
$$y_{UAV} = \sqrt{P_R} G_{R,UAV} x + n_{UAV} \quad (۲۱)$$

برای بهبود آشکارسازی سیگنال، UAV روش ترکیب سیگنال MRC را برای ترکیب دو سیگنال دریافتی در دو بازه زمانی به کار می‌گیرد. بنابراین سیگنال به نویز در رله، گره مقصد و UAV به ترتیب برابر خواهند بود با:

$$SNR_R = \frac{P_S}{N_0} |h_{S,R}|^2 \quad (۲۲)$$

$$SNR_D = \frac{P_S}{N_0} |h_{S,D}|^2 + \frac{P_R}{N_0} |h_{R,D}|^2 \quad (۲۳)$$

$$SNR_{UAV} = \frac{p_S}{N_0} |G_{S,UAV}|^2 + \frac{p_R}{N_0} |G_{R,UAV}|^2 \quad (۲۴)$$



شکل (۳): موقعیت قرارگیری S، R، D و UAV روی محور X-Y

۳-۲-۳- عملیات سوم: تداخل‌گر

در این حالت، UAV برای تخریب لینک مشکوک به عنوان تداخل‌گر عمل می‌کند و سیگنال تداخل می‌فرستد؛ بنابراین، احتمال استراق سمع موفق بهبود پیدا می‌کند. سیگنال دریافتی در گره مقصد مطابق زیر است:

$$y_{D_2} = \sqrt{P_R} h_{R,D} x + \sqrt{P_{UAV}} G_{UAV,D} s + n_{D_2} \quad (۲۵)$$

بنابراین سیگنال به نویز در رله، سیگنال به نویز و تداخل در گره مقصد و سیگنال به نویز در UAV به ترتیب برابر خواهند بود با:

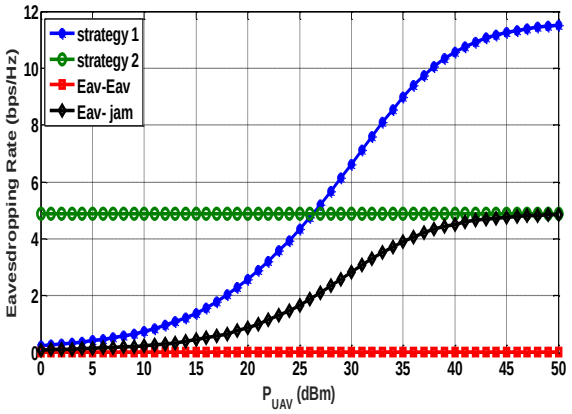
$$SNR_R = \frac{P_S}{N_0} |h_{S,R}|^2 \quad (۲۶)$$

$$SINR_D = \frac{P_S}{N_0} |h_{S,D}|^2 + \frac{P_R |h_{R,D}|^2}{P_{UAV} |G_{UAV,D}|^2 + N_0} \quad (۲۷)$$

$$SNR_{UAV} = \frac{P_S}{N_0} |G_{S,UAV}|^2 \quad (۲۸)$$

۴- نتایج شبیه‌سازی

در این بخش، نتایج شبیه‌سازی را برای ارزیابی عملکرد سناریوها ارایه می‌دهیم. مقادیر پارامترها براساس استاندار 3GPP LTE می‌باشند [27]. فرکانس کریر ۵GHZ، پهنای باند ۵MHZ، چگالی نویز سفید ۱۷۴dBm/HZ-، قدرت ارسالی S و R برابر ۴۰dBm و ضریب تلفات فضای آزاد α=۳ در نظر گرفته‌شده است. در این مقاله مقادیر پارامترهای a و b بر اساس مراجع [25] و [26] به ترتیب برابر با a=11/95 و b=0/136 تنظیم شده است. موقعیت قرارگیری مبدا، رله، مقصد و UAV در شکل ۳ نشان داده‌شده است، که بر اساس آنها



شکل (۴): مقایسه نرخ استراق سمع دو سناریو برحسب قدرت UAV

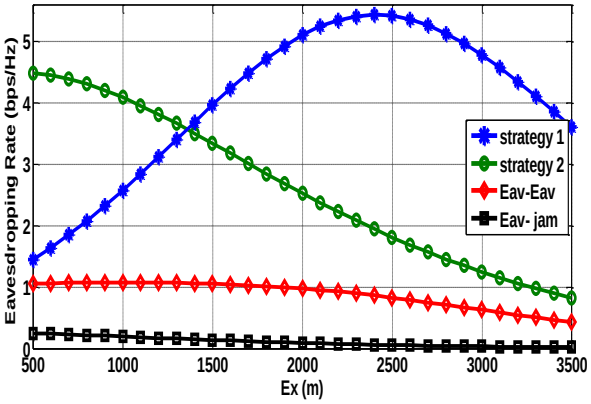
پارامترهای کانال و در نتیجه مقادیر سیگنال به نویز یا سیگنال به نویز و تداخل‌ها محاسبه می‌گردد.

برای مقایسه، بازدهی دو روش رایج و مرسوم در مقالات را به عنوان مرجع نیز بررسی کردیم. این دو روش عبارتند از شنود-تداخل(Jam-Eav) و شنود-شنود (Eav-Eav). در سناریو اول، UAV در فاز اول ارسال به عنوان تداخل‌گر و در فاز دوم به عنوان شنودگر عمل می‌کند. در سناریو دوم در هر دو فاز ارسال UAV به عنوان شنودگر عمل می‌کند.

شکل ۴ نرخ استراق سمع را بر حسب توانUAV نشان می‌دهد. تفاوت عملکرد بین سناریو اول و دوم به‌شدت به توپولوژی شبکه و پارامترهای عملیاتی وابسته است. برای سیستم در نظر گرفته شده در

این شبیه‌سازی، سناریو اول در مقایسه با سناریو دوم برای توان تداخل‌گر کم عملکرد بدتری دارد. در حالی‌که برای محدوده‌هایی که توان تداخلگر به اندازه کافی زیاد است سناریو اول عملکرد بهتری خواهد داشت.

در شکل ۵، نرخ استراق سمع سناریو اول و سناریو دوم و دو سناریو مرجع برحسب موقعیت محور x دیده‌بان قانونیUAV که با Ex نشان داده می‌شود، رسم شده‌است. همان‌طور که مشاهده می‌شود وقتی UAV از S دور می‌شود، نرخ استراق سمع سناریو دوم کاهش می‌یابد. این رفتار قابل پیش بینی است زیرا وقتی فاصله UAV و S زیاد می‌شود بازدهی استراق سمع کاهش می‌یابد (سیگنال شنود دریافتی در UAV ضعیف می‌شود). برعکس، بازدهی سناریو اول با افزایش Ex ابتدا افزایش می‌یابد و سپس کاهش پیدا می‌کند. یعنی یک نقطه بهینه برای مکان قرار گیری UAV از نظر بازدهی نرخ استراق سمع وجود دارد. این نقطه باید به رله نزدیک باشد. دلیل این امر این است که وقتی UAV به رله نزدیک است می‌تواند عملیات‌های شنود و تداخل را به صورت موثر و با بازدهی خوبی انجام دهد. بنابراین، به‌عنوان یک معیار مهم برای تصمیم‌گیری، UAV باید وقتی که نزدیک به مبدا است سناریو ۲ را اجرا کند و وقتی نزدیک به رله است سناریو ۱ را اجرا کند تا بهترین بازدهی را سیستم از نظر نرخ استراق سمع داشته باشد.



شکل (۵): نمودار نرخ استراق سمع در مقابل موقعیت Ex دیده‌بان قانونی (UAV)

۵- نتیجه‌گیری

در شبکه‌های بی‌سیم امکان نفوذ و برقراری ارتباط توسط افراد غیرمجاز و مخرب بسیار زیاد است. در سال‌های اخیر یک الگو جدید در بحث امنیت لایه فیزیکی برای شبکه‌های بی‌سیم پیشنهادشده است که در آن دیده‌بان قانونی نظارت بر ارسال اطلاعات را انجام می‌دهد. در این مقاله با توجه به پیشرفت‌ها و پتانسیل‌های زیادی که در زمینه هواپیماهای بدون سرنشین وجود دارد، پیشنهاد شد که از UAV برای دیده‌بانی شبکه مخابرات مشارکتی با ارتباطات مشکوک به‌منظور مقابله با تهدیدهای امنیتی استفاده شود. بر اساس موقعیت قرارگیری UAV و فاصله نسبی آن از فرستنده‌های مشکوک یعنی مبدا و رله، دو استراتژی تطبیقی با هدف بهبود امنیت سیستم پیشنهاد گردید. نرخ استراق سمع در محل دیده‌بان قانونی برای دو سناریو استخراج شد و نشان داده شد که این دو سناریوی پیشنهادی نسبت به روش‌های مرجع موجود بازدهی خیلی بهتری دارند. همچنین نشان داده شد که برای حصول بهترین نرخ استراق سمع، از موقعیت دیده‌بان قانونی می‌توان به‌عنوان یک معیار ساده برای تعیین سناریو مناسب استفاده کرد.

۶- مراجع

[1] Y. Zou, J. Zhu, X. Wang, and V. Leung, “Improving physical-layer security in wireless communications using diversity techniques,” IEEE Network, vol. 29, no. 1, pp. 42–48, Jan. 2015.

[2] F. Al-Qahtani, C. Zhong, and H. M. Alnuweiri, “Opportunistic relay selection for secrecy enhancement in cooperative networks,” IEEE Trans. Commun., vol. 63, no. 5, pp. 1756–1770, May 2015.

[3] S. Gong, C. Xing, Z. Fei, and J. Kuang, “Resource allocation for physical layer security in heterogeneous network with hidden eavesdropper,” China Commun., vol. 13, no. 3, pp. 82–95, Mar. 2016.

[4] X. Jiang, C. Zhong, X. Chen, T. Q. Duong, T. A. Tsiftsis, and Z. Zhang, “Secrecy performance of wirelessly powered wiretap channels,” IEEE Trans. Commun., vol. 64, no. 9, pp. 3858–3871, Sep. 2016.

[5] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, “A survey on wireless security: Technical challenges, recent advances, and future trends,” Proc. IEEE, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.

[6] J. Zhu, W. Xu, and N. Wang, “Secure massive MIMO systems with limited RF chains,” IEEE Trans. Veh. Technol., vol. 66, no. 6, pp. 5455–5460, Jun. 2017.

[۷] محسن ناصری، محمد جواد صابر، سید محمد سجاد صدوق، دکتر محمد ترابی **" ارزیابی عملکرد محرمانگی شبکه رله‌ای بافردار رادیوشناختی در کانال های محوشدگی رایلی"**، مجله مهندسی برق و الکترونیک ایران ، جلد ۱۶ شماره ۴ ، ۱۱۳-۱۲۱، ۱۳۹۸.

[۸] علیرضا بقائی پوری، محمد ترابی **" بهبود امنیت لایه فیزیکی در سیستم کدکننده زمان-فضا مبتنی بر مدل تعمیم یافته Alamouti"**، مجله مهندسی برق و الکترونیک ایران ، جلد ۱۷ شماره ۱ ، ۱-۹، ۱۳۹۹.

[9] D. Wang, P. Ren, Q. Du, Y. Wang, and L. Sun, “Secure cooperative transmission against jamming-aided eavesdropper for ARQ based wireless networks,” IEEE Access, vol. 5, pp. 3763–3776, 2017.

[10] J. Xu, L. Duan, and R. Zhang, “Surveillance and intervention of infrastructure-free mobile communications: A new wireless security paradigm,” IEEE Wireless Commun., vol. 24, no. 4, pp. 152–159, Aug. 2017.

[11] J. Xu, L. Duan, and R. Zhang, “Proactive eavesdropping via jamming for rate maximization over Rayleigh fading channels,” IEEE Wireless Commun. Lett., vol. 5, no. 1, pp. 80–83, Feb. 2016.

[12] J. Xu, L. Duan, and R. Zhang, “Proactive eavesdropping via cognitive jamming in fading channels,” in Proc. IEEE

Intl. Conf. Commun. (ICC), Kuala Lumpur, Malaysia, pp. 1–6, May 2016.

[13] J. Xu, L. Duan, and R. Zhang, "Fundamental rate limits of physical layer spoofing," IEEE Wireless Commun. Lett., vol. 6, pp. 154–157, Apr. 2017.

[14] C. Zhong, X. Jiang, F. Qu, and Z. Zhang, "Multi-antenna wireless legitimate surveillance systems: Design and performance analysis," IEEE Trans. Wireless Commun., vol. 16, pp. 4585–4599 July 2017.

[15] Y. Zeng and R. Zhang, "Wireless information surveillance via proactive eavesdropping with spoofing relay," IEEE J. Sel. Topics Signal Process., vol. 10, no. 8, pp. 1449–1461, Dec. 2016.

[16] A. Merwaday and I. Guvenc, "UAV assisted heterogeneous networks for public safety communications," in Proc. IEEE Wireless Commun .Netw. Conf. (WCNC), pp. 329–334, 9-12 Mar, 2015.

[17] B. Pearre and T. X. Brown, "Model-free trajectory optimization for wireless data ferries among multiple sources," in Proc. IEEE Global. Commun. Conf. (GLOBECOM), Miami, FL, pp. 1793–1798, Dec. 2010.

[18] Z. Zhang, "Routing in intermittently connected mobile ad hoc networks and delay tolerant networks: overview and challenges," IEEE Commun. Surv Tuts., vol. 8, no. 1, pp. 24–37, Jan. 2006.

[19] M. J. Khabbaz, C. M. Assi, and W. F. Fawaz, "Disruption-tolerant networking: A comprehensive survey on recent developments and persisting challenges," IEEE Commun. Surv. Tut., vol. 14, no. 2, pp. 607–640, 2012.

[20] I. Bucaille, S. Hethuin, A. Munari, R. Hermenier, T. Rasheed, and S. Allsopp, "Rapidly deployable network for tactical applications: Aerial base station with opportunistic links for unattended and temporary events absolute example," in Proc IEEE Military Commun. Conf. (MILCOM), San Diego, CA, USA, Nov. 2013.

[21] Z. Mobini, B. K. Chalise, M. Mohammadi, H. A. Suraweera, and Z. Ding "Proactive Eavesdropping Using UAV Systems with Full-Duplex Ground Terminal," in Proc. IEEE Intl conf. commun. (ICC), 2018.

[22] D. Hu, Q. Zhang, P. Yang, and J. Qin, "Proactive monitoring via jamming in amplify-and-forward relay networks," IEEE Signal Process. Lett., vol. 24, pp. 1714–1718, 2017.

[23] X. Jiang, H. Lin, C. Zhong, X. Chen, Z. Zhang, "Proactive eavesdropping in relaying systems," IEEE Signal Process. Lett., vol. 24, no. 6, pp. 917-921, Jun. 2017 .

[24] T. S. Rappaport, "Wireless Communications: Principles and Practice," 2nd ed. NJ: Prentice Hall, 2001.

[25] R. Yaliniz, A. El-Keyi, and H. Yanikomeroglu, "Efficient 3-D placement of an aerial base station in next generation cellular networks," in Proc. of IEEE Intl. Conf. Commun. (ICC), Kuala Lumpur, Malaysia, May. 2016.

[26] M. Mozaffari, W. Saad, M. Bennis and M. Debbah, "Mobile Unmanned Aerial Vehicles (UAVs) for Energy-Efficient Internet of Things Communications," IEEE Trans. Wireless Commun., vol. 16, no. 11, pp. 7574-7589, Nov. 2017.

[27] Z. Ding, Y. Liu, J. Choi, Q. Sun, M. Elkashlan, C.-L. I, and H. V. Poor, "Application of non-orthogonal multiple access in LTE and 5G networks," IEEE Commun. Mag., vol. 55, pp. 185–191, Feb. 2017.

زیرنویس‌ها

[1] Physical layer security
[2] Artificial Noise
[3] Monitoring
[4] Jammer
[5] Proactive Eavesdropping
[6] spoofing
[7] Unmanned Aerial Vehicle (UAV)
[8] Line-of-Sight (LoS)
[9] Decode and Forward (DF)
[10] Eavesdropping rate
[11] Signal to noise plus interference (SINR)
[12] Signal noise interference (SNR)
[13] Additive white Gaussian noises (AWGNs)
[14] Maximum ratio combining(MRC)
[15] helping
[16] fairness