تولید کلید مخفی برای ارتباطات پهبادها با کمک یک رله غیرقابل اعتماد

تاریخ دریافت: ۱۴۰۲/۰۷/۰۳
تاریخ پذیرش: ۱۴۰۲/۰۹/۰۲

محمدرضا کشاورزی[۱]، علی کوهستانی[۲]

۱- استادیار، پژوهشکده فناوری ارتباطات، پژوهشگاه ارتباطات و فناوری اطلاعات

۲- استادیار، دانشکده مهندسی برق و کامپیوتر، دانشگاه صنعتی قم، Kuhestani@qut.ac.ir

چکیده

در سال‌های اخیر، توسعه‌ی پهبادها[i] یک تغییر راهبردی اساسی و نوین در سیستم‌های ارتباطی بی‌سیم بوده است. این فناوری نوظهور، با بهره‌برداری از قدرت مانور بالا و نیز هزینه کم، قادر است ارتباطات فراگیر، به خصوص در نقاط حساس و مناطق دوردست، فراهم آورد. اخیراً یک راهکار امنیتی نوین و کارآمد به نام تولید کلید مخفی لایه فیزیکی بسیار مورد توجه محققان و صنعت‌گران قرار گرفته است. این روش، به دلیل سبک‌وزن[iii] بودن و مقیاس‌پذیری آسان برای کاربردهای پهباد جذاب است. با این حال، در ارتباطات پهباد به پهباد ایستا[iv]، تولید کلید مخفی با دو چالش مهم مواجه است: نرخ پایین تولید کلید و وجود نواحی آسیب‌پذیری[v]. برای مرتفع کردن ضعف اول، می‌توان از مولدهای تصادفی محلّی توسط خود پهبادها استفاده کرد. به طور خاص در این مقاله، سیگنال‌های کاوش کانال[vi] ارسالی توسط پهبادها، فاز تصادفی دارند. همچنین برای افزایش نرخ تولید کلید پیشنهاد شده است که یک گره خارجی به نام رله (که به آن اعتماد نداریم) در فرآیند تولید کلید شرکت کند. برای چنین مدل سیستمی، یک طرح تولید کلید امن پیشنهاد شده است. از آنجایی‌که کلید پیشنهادی مرکب از چندین فاز تصادفی می‌باشد، آنتروپی بالایی دارد. سپس، ضمن ارائه‌ی حمله برای شنودگر، طرح از منظر محرمانگی هندسی[vii] مورد ارزیابی قرار می‌گیرد. نتایج شبیه‌سازی نشان می‌دهد که طرح پیشنهادی در مقایسه با مرجع اخیر (بدون رله)، نواحی آسیب‌پذیری کمتری دارد.

واژه‌های کلیدی: *امنیت پهباد، تولید کلید مخفی لایه فیزیکی، رله غیرقابل اعتماد، محرمانگی هندسی.*

Secret key generation for UAV communications using an Untrusted Relay

Mohammadreza Keshavarzi[1], Ali Kuhestani[2]

1- Assistant Professor, ICT Research Institute, Iran Telecommunication Research Center (ITRC), Tehran, Iran
2- Assistant Professor, Faculty of Electrical and Computer Engineering, Qom University of Technology, Qom, Iran.

Abstract

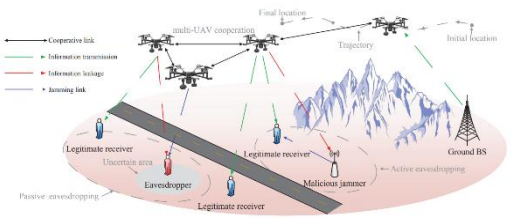
In recent years, the development of UAVs has been a fundamental and innovative strategic change in wireless communication systems. Recently, a new and efficient security solution called physical layer secret key generation has attracted the attention of researchers and industrialists. This method is attractive for UAV applications due to its lightweight and easy scalability. However, in static UAV communication, secret key generation faces two major challenges: low key generation rate and the existence of vulnerable areas. To overcome the first weakness, local random generators can be used by the UAVs themselves. Specifically, in this paper, the channel probe signals sent by UAVs have random phases. Also, to increase the key generation rate, it is suggested that an external node called relay (which is untrusted) cooperates in the key generation process. For this collaborative key generation scheme, while presenting possible attacks for eavesdroppers, it is evaluated from the perspective of geometric secrecy. The simulation results show that the proposed scheme has less vulnerable areas compared to the recent reference (without relay).

Keywords: *UAV security, Physical layer secret key generation, untrusted relay, geometric secrecy.*

۱. مقدمه

پهپادها با ارائه‌ی مزایایی مانند قابلیت مانور بالا، استقرار سریع برحسب نیاز، ارزان بودن، نرخ داده‌ی بالا، پوشش وسیع حتی نقاط دورافتاده و حساس و نیز پشتیبانی به دیگر فناوری‌های مخابراتی در ایام بحران، توجه بسیاری از پژوهشگران حوزه‌ی نظامی و تجاری را به خود جلب کرده است [۱] و [۲]. در مقایسه با ارتباطات سنتی زمینی، پهپادها به دلیل بهره‌وری از لینک دید مستقیم، کانال ارتباطی قوی فراهم می‌آورند. بنابراین، تأخیر بسیار کم و قابلیت اطمینان بسیار بالا از ویژگی‌های منحصر به فرد این فناوری نوظهور است [۳].

علیرغم ویژگی‌های برجسته و امیدوارکننده‌ی پهپادها، چالش‌های گوناگونی در راه‌اندازی آنها وجود دارد. در بین این چالش‌ها، امنیت به عنوان یک موضوع مهم در ارتباطات پهپادها محسوب می‌شود. به بیانی دیگر، وجود لینک قوی در ارتباطات پهپادها، اگرچه یک حسن بزرگ محسوب می‌شود، اما راه را برای حملات مهاجمان نیز باز می‌کند. شکل ۱، نمایی از انواع ارتباطات پهپادها و نیز حملات پرکاربرد شامل شنود اطلاعات و جمینگ را نشان می‌دهد. از آنجایی‌که لینک‌های حملات نیز غالباً دیدمستقیم و در نتیجه قوی هستند، لذا میزان نشت اطلاعات و نیز توان جمینگ در گیرنده‌ی هدف، زیاد است که این یک عیب بزرگ محسوب می‌شود.



شکل ۱. نمایی کلی از ارتباطات پهپادها و حملات محتمل بر آنها [۵]

در حوزه ارتباطات پهپاد، با افزایش حملات به لینک‌های مخابراتی، کنترلی و موقعیت‌یابی پهپاد، استفاده از الگوریتم‌های رمزنگاری قدرتمند ضروری است. اما الگوریتم‌های رمزنگاری مبتنی بر پیچیدگی محاسباتی هستند که با افزایش پیچیدگی آنها، هزینه و سربار محاسباتی دستگاه‌ها افزایش می‌یابد. این موضوع، برای پهپادها با ذخیره انرژی محدود، یک چالش محسوب می‌شود. اخیراً با پیدایش رایانه‌ها با پردازش‌های کوانتومی، امنیت سیستم‌های رمزنگاری زیر سوال رفته است [۴]. علاوه بر این، فرآیندهای اشتراک‌گذاری و مدیریت متمرکز کلید برای شبکه‌های توزیع شده مانند دسته‌ای از پهپادها چالش برانگیز است. برای غلبه بر چنین چالش‌هایی، اخیراً امنیت لایه فیزیکی[۱] (PLS) معرفی شده است [۵]. PLS به‌عنوان یک تکنیک قدرتمند و البته سبک‌وزن با مصرف انرژی کم و متکی بر نظریه اطلاعات، می‌تواند همراه با (یا مستقل از) تکنیک‌های رمزنگاری برای امن کردن ارتباطات پهپادها و نیز قابلیت اطمینان آنها به‌کار گرفته شود [۵]. بر خلاف روش‌های متداول پیشین، در PLS می‌توان فرض کرد که گره‌های غیرمجاز، توانایی محاسباتی نامحدودی داشته و در عین حال، امنیت تضمین شده داشته باشیم.

مبانی PLS اولین بار در مقاله معروف آقای واینر[۲] [۶] مطرح شد که در آن موضوع کانال شنود[۳] طرح گردید. در آن مقاله، با وارد کردن نویز به مدل ارتباطی، امنیت اطلاعات از زاویه‌ای جدید مورد بررسی قرار گرفت. اما واینر با وارد کردن شرایط کانال گیرنده قانونی[۴] و شنودگر[۵] در مدل ارتباطی و لحاظ‌کردن تفاوت‌های آن دو، ایده‌ی امکان انتقال امن اطلاعات با بهره‌گیری از راهکارهای مبتنی بر لایه فیزیکی را ارایه کرد. از جمله راهکارهای PLS

می‌توان به روش‌های مبتنی بر کدگذاری [۷]، روش‌های مبتنی بر آنتن‌های جهتی و پرتودهی[۶] [۸]،[۹]، انتشار نویز مصنوعی[۷] به منظور افزایش ظرفیت محرمانگی[۸] [۱۰]،[۱۱]، مخابرات مشارکتی[۹] [۱۲]،[۱۳] و تولید کلید مخفی[۱۰] (SKG) لایه فیزیکی [۱۴]-[۱۷] اشاره کرد. در بین این روش‌ها، SKG در حوزه‌ی صنعت بیشتر مورد توجه بوده است [۱۴].

SKG به دلایلی از قبیل سبک‌وزن[۱۳] بودن، توان مصرفی کمتر، کم بودن سربار پردازشی، نیازمندی تجهیزاتی ساده و نیز موجود بودن بستر پیاده‌سازی آن در غالب فناوری‌های مخابراتی، در مقایسه با سایر روش‌های PLS عملی‌تر و جذاب‌تر است [۱۴]. بنابراین، تولید کلید لایه فیزیکی برای تأمین امنیت در کاربردهایی نظیر اینترنت اشیاء و پهبادها که ممکن است قدرت محاسباتی و توان مصرفی آنها کم باشد، مناسب‌تر است [۱۴] و [۱۵]. در SKG، تولید کلید بر مبنای یکی از ویژگی‌های کانال مشترک طرفین ارتباط، صورت می‌گیرد. این ویژگی‌ها عبارتند از فاز کانال، شدت سیگنال دریافتی[۱۱](RSS)، اطلاعات حالت کانال[۱۲] (CSI) و غیره [۱۴].

خوب است ذکر شود که در مقالات [۹]-[۱۳]، امنیت ارتباطات بر پایه‌ی ارسال امن است. به طور خاص، در مرجع [۱۴] از بکارگیری توأم سیستم MIMO، مخابرات مشارکتی و تخصیص توان برای برقراری یک ارتباط امن استفاده شده است. در مرجع [۱۰] نویسندگان با طراحی پرتودهی در فرستنده MIMO و نیز بکارگیری یک جمر دوست، دو نیازمندی ارسال امن و مخابره پنهان را برآورده کرده‌اند. در مرجع [۱۱] نیز با طراحی توأم پرتودهی، سیگنال پیام و جمینگ، یک طرح امن برای ارتباطات موج میلیمتری مبتنی بر صفحات هوشمند بازتاب کننده امواج ارائه گردید. در کارهای [۱۲] و [۱۳] نیز یک طرح ارسال امن در حضور رله غیرقابل اعتماد ارائه گردید که در آنها، با استفاده از جمینگ دوستانه، رله غیرقابل اعتماد نمی‌تواند به پیام محرمانه منبع دست یابد. همچنین در این مراجع، با طرح مسائل بهینه‌سازی با هدف بیشینه‌سازی نرخ محرمانه قابل حصول، تخصیص توان برای گره‌ها صورت گرفت.

متفاوت با کارهای [۹]-[۱۳]، در کارهای [۱۵]-[۱۷] مبحث تولید کلید لایه فیزیکی برای سناریوهای مختلف مخابراتی مورد مطالعه قرار گرفته است. در مرجع [۱۵] نویسندگان یک طرح تولید کلید برای ارتباطات دستگاه به دستگاه شبکه موبایل ارائه کردند که در آن از CSI کانال برای تولید کلید استفاده می‌شد. سپس همان نویسندگان در مرجع [۱۶] یک طرح تولید کلید لایه فیزیکی برای سناریویی پیشنهاد دادند که در آن یک رله غیرقابل اعتماد بین منبع و مقصد قرار دارد و برای تولید کلید، استفاده از رله الزامی است. در مراجع [۱۵] و [۱۶]، تولید کلید برای یک محیط با پراکندگی زیاد (مرتبط با شبکه موبایل) و مبتنی بر CSI کانال می‌باشد. در مرجع اخیر [۱۷]، نویسندگان برای کانال‌های ایستا و بدون پراکنده‌ساز (معادل با کانال‌های AWGN) و به طور خاص ارتباطات بین پهبادها، یک طرح تولید کلید لایه فیزیکی مبتنی بر فاز کانال ارائه کردند. در این کار، ارتباطات پهباد به پهباد مطرح بود. ضمناً نویسندگان در این مرجع، مفهوم نواحی آسیب‌پذیری را مورد مطالعه قرار دادند.

در کار حاضر، مشابه مرجع [۱۷] از فاز کانال به عنوان یک منبع تصادفی مشترک برای تولید کلید لایه فیزیکی استفاده شده است. تفاوت آنجاست که متفاوت با [۱۷]، در این مقاله به منظور افزایش آنتروپی و نیز کاهش نواحی آسیب‌پذیری، از یک رله که در سطح زمین قرار دارد، در فرآیند تولید کلید استفاده می‌شود. پروتکل تولید کلید ارائه شده به گونه‌ای است که

رله هیچگونه اطلاعاتی در خصوص کلید بدست نخواهد آورد. به عبارت دیگر، رله غیرقابل اعتماد است. همچنین متفاوت با کار [۱۶] که رله در وسط منبع و مقصد قرار داشت و فسلفه حضوری آن یاری رساندن است، در این کار هدف از رله، صرفاً کمک به افزایش نرخ تولید کلید و کاهش نواحی آسیب‌پذیری می‌باشد. همچنین خوب است ذکر شود که در مرجع [۱۶] نواحی آسیب‌پذیری مورد مطالعه قرار نگرفته است.

در ارتباطات پهبادها، به‌دلیل وجود کانال دید مستقیم بین پهبادها و یا پهباد با کاربر زمینی، غالباً نسبت سیگنال به نویز[۱۴] (SNR) زیاد بوده و پدیده‌ی محوشدگی[۱۵] تجربه نمی‌گردد. در چنین ارتباطاتی که کانال آنها قابل مدل‌کردن با نویز سفید گوسی جمع شونده[۱۶] (AWGN) می‌باشد، ایجاد منبع با آنتروپی بالا یک ضرورت است؛ چرا که طرح‌های متداول SKG که صرفاً مبتنی بر آنتروپی کانال هستند، کلیدهای به اندازه‌ی کافی تصادفی تولید نمی‌کنند. به خصوص در کابرد پهباد که کانال بعضاً ایستا[۱۷] و نامتغیر بازمان است، تصادفی بودن کلید اساساً زیر سوال است. به بیانی دیگر، از منظر امنیتی نیز چالشی‌ترین وضعیت برای SKG، همین ارتباطات دید مستقیم می‌باشد که در آن، کانال قانونی و کانال شنود با AWGN مدل می‌شوند [۱۴] و [۱۷].

توجه شود که در طرح‌های لایه فیزیکی برای تولید کلید، استفاده از فاز کانال در مقایسه با دامنه‌ی کانال به لحاظ محرمانگی مزیت‌های قابل توجهی دارد که در ادامه به برخی از آنها اشاره شده است:

۱) در شرایط عملی، فاز کانال، یک متغیر تصادفی با توزیع یکنواخت در بازه صفر تا 2π است. بنابراین، اگر مهاجم به قدر کافی از گره‌های قانونی فاصله داشته باشد، فاز کانال قانونی و کانال شنود، ناهمبسته خواهد بود و در نتیجه مهاجم، با کمک مشاهدات خودش از فاز کانال، اطلاعاتی در مورد فاز کانال قانونی به دست نخواهد آورد. امّا مقدار دامنه‌ی کانال اینگونه نیست. در محیط‌های انتشاری مختلف، مقدار دامنه‌ی کانال برحسب طول موج و فاصله‌ی فرستنده و گیرنده، قابل مدل‌سازی است [۱۴]. در نتیجه مهاجم با دانستن فرکانس کاری و فاصله خودش تا گیرنده‌ی قانونی می‌تواند از روی قدرت سیگنال دریافتی خودش، برآورد خوبی از دامنه‌ی کانال قانونی بدست آورد. بنابراین برای مهاجم، برآورد دامنه‌ی کانال قانونی به مراتب ساده‌تر از برآورد فاز این کانال است.

۲) در کانال‌های بی‌سیم، حساسیت فاز کانال نسبت به تغییرات زمانی کانال در مقایسه با دامنه‌ی کانال، بیشتر است. به عنوان مثال، یک جابجایی کوچک در موقعیت فرستنده، گیرنده یا عوامل انتشاری، منجر به تغییرات زیادی در فاز کانال می‌شود؛ در حالی‌که ممکن است اندازه کانال بدون تغییر باقی بماند.

با توجه به توضیحات فوق، در ارتباطات پهبادها می‌توان از فاز کانال بی‌سیم به‌عنوان منبع تصادفی با آنتروپی بالا برای پیاده‌سازی تولید کلید استفاده کرد. بر این اساس، این پژوهش، بر روی تولید کلید از فاز کانال تمرکز دارد.

یکی از تکنیک‌های تقویت SKG، به‌کارگیری رله می‌باشد که در آن، رله کمک می کند تا سیگنال کاوش کانال با کیفیت بهتر در گره منبع و مقصد دریافت گردد [۱۲] و [۱۶]. در حوزه‌ی رله کردن مشارکتی، سناریوی رله‌ی غیرقابل اعتماد است [۱۲] و [۱۶] که در آن یک گره میانی به عنوان یک موجودیت قانونی به ارتباط منبع به مقصد کمک می کند، اما ممکن است آن رله در نقش یک شنودگر نیز رفتار کند. در این مقاله، با هدف افزایش آنتروپی کلید و نیز

افزایش نرخ تولید کلید، از رله به عنوان یک منبع تزریق سیگنال تصادفی استفاده می‌شود.

با توجه به توضیحات فوق، این پژوهش، به تولید کلید لایه فیزیکی برای یک لینک پهباد-به-پهباد در حضور رله‌ی غیرقابل اعتماد می‌پردازد. یک طرح تولید کلید مخفی ارائه می‌شود که در آن، رله غیرقابل اعتماد اگر چه در فرآیند تولید کلید نقش دارد ولی نمی‌تواند به کلید مخفی دست یابد. مشابه کارهای پیشین [۱۷] و [۱۹]، از فاز کانال به عنوان مؤلفه تصادفی مشترک بین آلیس، باب و رله برای تولید کلید استفاده می‌شود و ضمناً به منظور افزایش آنتروپی کلید، فاز تصادفی توسط آلیس و باب تزریق می‌گردد. کلید تولید شده مبتنی بر طرح پیشنهادی را می‌توان برای تولید الگوی پرش فرکانسی[۱۸]، جهت مقابله با حمله‌ی جمینگ به کار گرفت. متفاوت با کار پیشین [۱۷] که رله‌ای در شبکه حضور نداشت، در این پژوهش، یک رله غیرقابل اعتماد وجود دارد. همچنین با الهام از مرجع [۱۷]، نواحی آسیب‌پذیری برای طرح تولید کلید مشارکتی پیشنهادی محاسبه می‌شود. به منظور کاهش نواحی آسیب‌پذیری، طرح کاوش کانال بر روی چند فرکانس به جای یک فرکانس، پیشنهاد و اجرایی می‌گردد. همچنین خواهیم دید مصالحه‌ای بین نواحی آسیب‌پذیری (و در نتیجه امنیت طرح تولید کلید) و نیز نرخ خطای کلید (و در نتیجه کارآمدی طرح تولید کلید) برقرار است. نتایج شبیه‌سازی شهودهای مهندسی خوبی جهت بهبود محرمانگی هندسی ارائه می‌دهند.

بخش‌بندی مقاله به شرح زیر است: در بخش ۲ مدل سیستم، فرضیات و طرح پیشنهادی تولید کلید مبتنی بر فاز کانال ارایه می‌شود. بخش ۳ به تحلیل امنیتی طرح پیشنهادی با رویکرد محرمانگی هندسی می‌پردازد. نهایتاً، بخش ۴ این مقاله، به جمع‌بندی و ارائه کارهای آتی می‌پردازیم.

۲. مدل سیستم و پروتکل تولید کلید

در این بخش، مدل سیستم و فرضیات بیان می‌شود و سپس سیگنال‌های دریافتی در گره‌ها به‌دست می‌آید. در گام بعد، طرح تولید کلید لایه فیزیکی پیشنهادی تشریح می‌گردد.

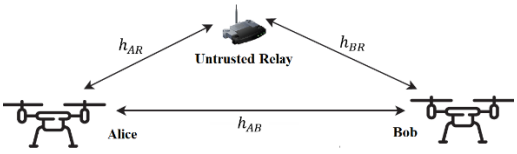
۲-۱- مدل سیستم و فرضیات:

سیستم مدل پیشنهادی، مطابق شکل ۲، شامل دو گرهٔ قانونی آلیس و باب (دو پهباد که می‌خواهند تبادل داده داشته باشند) می‌باشد که قصد دارند در فضای آزاد به تولید کلید بپردازند. همچنین یک رله‌ی غیرقابل اعتماد در شبکه حضور دارد که با هدف افزایش نرخ تولید کلید مخفی، در فرآیند تولید کلید، مشارکت دارد. این رله در سطح ارائه‌ی خدمت، مورد اعتماد بوده ولی در سطح داده، غیرقابل اعتماد است. لذا رله در اجرای پروتکل تولید کلید کاملاً همراه می‌باشد، ولی ممکن است کلید را استخراج کرده و از آن سوءاستفاده نماید. شنودگر غیرفعال نیز در شبکه حضور دارد (که برای سادگی، رسم نشده است) که با رصد کردن فرآیند تولید کلید مشارکتی، سعی دارد تا کلید مخفی را کشف کند.

فرضیات این پژوهش به‌صورت زیر است:

- تمام گره‌ها مجهز به یک آنتن هستند.
- تمام گره‌ها در وضعیت نیمه‌دوسویه[۱۹] عمل می‌کنند و در نتیجه، هیچ گره‌ای قادر به تبادل اطلاعات به‌صورت هم‌زمان و در یک باند فرکانسی نیست.
- کانال بین گره‌ها از نوع دید مستقیم و لذا AWGN بوده و ضمناً ایستا می‌باشد.
- زمان همدوسی[۲۰] کانال به اندازه‌ای است که یک دور کامل تبادل کلید را پوشش می‌دهد و ضمناً در این بازه زمانی، کانال هم‌پاسخ[۲۱] است.
- گره‌ها به‌طور کامل هم‌زمان‌سازی شده‌اند.

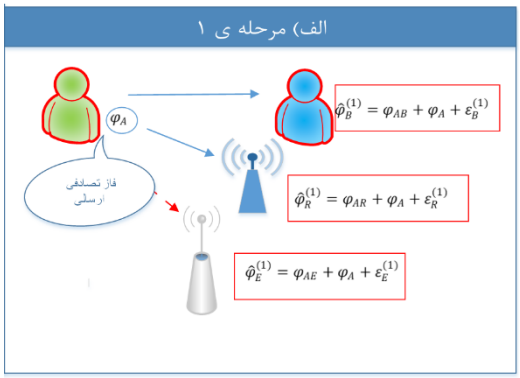
- شنودگر دارای توان محاسباتی نامحدود بوده و لذا قادر است فاز سیگنال‌های دریافتی خودش را دقیق تخمین بزند.

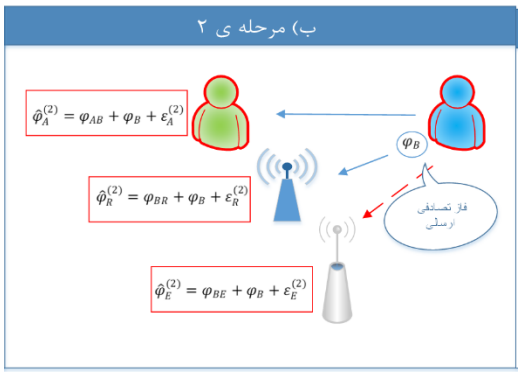


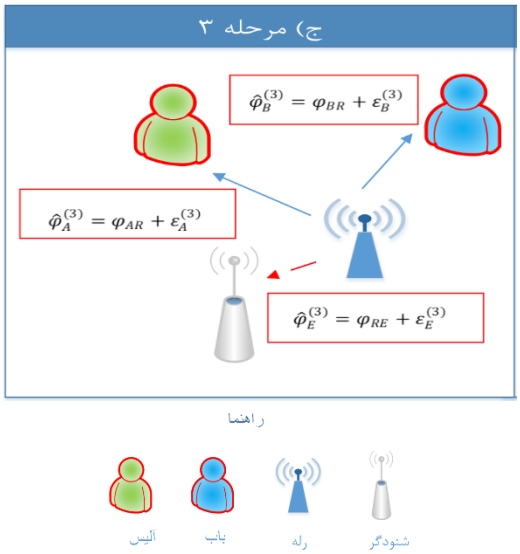
شکل ۲. مدل سیستم

۲-۲- پروتکل تولید کلید پیشنهادی:

مطابق شکل ۳، فرآیند تولید کلید مشارکتی در سه مرحله انجام می‌شود. در مرحله‌ی اول، آلیس سیگنال راهنما با فاز اولیه تصادفی φ_A را ارسال می‌کند (φ_A دارای توزیع یکنواخت در بازه‌ی $[0,2\pi)$ است). در اینجا، مدل باند پایه‌ی سیگنال دریافتی در باب، رله و شنودگر به‌ترتیب از روابط زیر محاسبه می‌شوند:







شکل ۳. طرح تولید کلید مشارکتی پیشنهادی

$$y_B^{(1)} = \sqrt{P_A}|h_{AB}|e^{j(\varphi_{AB}+\varphi_A)}x_A^P + n_B^{(1)} \quad (۱)$$

$$y_R^{(1)} = \sqrt{P_A}|h_{AR}|e^{j(\varphi_{AR}+\varphi_A)}x_A^P + n_R^{(1)} \quad (۲)$$

$$y_E^{(1)} = \sqrt{P_A}|h_{AE}|e^{j(\varphi_{AE}+\varphi_A)}x_A^P + n_E^{(1)} \quad (۳)$$

در روابط فوق $|h_{AB}|$، $|h_{AR}|$ و $|h_{AE}|$ به‌ترتیب اندازه‌ی کانال بین آلیس و باب، آلیس و رله و نیز آلیس و شنودگر هستند. φ_{AB}، φ_{AR} و φ_{AE} به‌ترتیب بیانگر فاز کانال بین آلیس و باب، آلیس و رله و نیز آلیس و شنودگر هستند. $n_i^{(1)}$ نویز حرارتی در گره $i \in \{B, R, E\}$ است. همچنین $x_A^P = 1$ و P_A نیز توان ارسال سیگنال راهنما توسط آلیس می‌باشد.

در مرحله‌ی دوم، باب سیگنال راهنما با فاز اولیه‌ی تصادفی φ_B که توزیع یکنواخت دارد، را ارسال می‌کند. در این حالت، مدل باند پایه‌ی سیگنال دریافتی در آلیس، رله و شنودگر به‌ترتیب از روابط زیر محاسبه می‌شود:

$$y_A^{(2)} = \sqrt{P_B}|h_{BA}|e^{j(\varphi_{BA}+\varphi_B)}x_B^P + n_A^{(2)} \quad (۴)$$

$$y_R^{(2)} = \sqrt{P_B}|h_{BR}|e^{j(\varphi_{BR}+\varphi_B)}x_B^P + n_R^{(2)} \quad (۵)$$

$$y_E^{(2)} = \sqrt{P_B}|h_{BE}|e^{j(\varphi_{BE}+\varphi_B)}x_B^P + n_E^{(2)} \quad (۶)$$

در روابط فوق $|h_{BA}|$، $|h_{BR}|$ و $|h_{BE}|$ به‌ترتیب اندازه‌ی کانال بین آلیس و باب، باب و رله

و نیز باب و شنودگر هستند. φ_{BA}، φ_{BR} و φ_{BE} به‌ترتیب بیانگر فاز کانال بین آلیس و باب، باب و رله و نیز باب و شنودگر هستند. $n_i^{(2)}$ نویز حرارتی در گره $i \in \{A, R, E\}$ است. همچنین $x_B^P = 1$ و P_B نیز توان ارسال سیگنال راهنما توسط باب است.

در مرحله‌ی سوم، رله سیگنال راهنما با فاز صفر را ارسال می‌کند. در این حالت، سیگنال دریافتی در آلیس، باب و شنودگر به‌ترتیب از روابط زیر محاسبه می‌شود:

$$y_A^{(3)} = \sqrt{P_R}|h_{RA}|e^{j(\varphi_{RA})}x_R^P + n_A^{(3)} \quad (۷)$$

$$y_B^{(3)} = \sqrt{P_R}|h_{RB}|e^{j(\varphi_{RB})}x_R^P + n_B^{(3)} \quad (۸)$$

$$y_E^{(3)} = \sqrt{P_R}|h_{RE}|e^{j(\varphi_{RE})}x_R^P + n_E^{(3)} \quad (۹)$$

در روابط فوق $|h_{RA}|$، $|h_{RB}|$ و $|h_{RE}|$ به‌ترتیب اندازه‌ی کانال بین رله و آلیس، رله و باب و نیز رله و شنودگر می‌باشد. φ_{RA}، φ_{RB} و φ_{RE} نیز به‌ترتیب بیانگر فاز کانال بین آلیس و رله، رله و باب و نیز رله و شنودگر می‌باشند. $n_i^{(2)}$ نویز حرارتی در گره‌ی $i \in \{A, B, E\}$ است. همچنین $x_R^P = 1$ و P_R نیز توان ارسال سیگنال راهنما توسط رله است.

در مرحله‌ی اول، باب، رله و شنودگر پس از دریافت سیگنال ارسالی توسط آلیس، فاز سیگنال دریافتی را تخمین می‌زنند که این تخمین‌ها، به ترتیب عبارتند از:

$$\hat{\varphi}_B^{(1)} = \varphi_{AB} + \varphi_A + \varepsilon_B^{(1)} \quad (۱۰)$$

$$\hat{\varphi}_R^{(1)} = \varphi_{AR} + \varphi_A + \varepsilon_R^{(1)} \quad (۱۱)$$

$$\hat{\varphi}_E^{(1)} = \varphi_{AE} + \varphi_A + \varepsilon_E^{(1)} \quad (۱۲)$$

در روابط فوق $\varepsilon_B^{(1)}$، $\varepsilon_R^{(1)}$ و $\varepsilon_E^{(1)}$ به‌ترتیب خطای تخمین فاز در باب، رله و شنودگر هستند.

در مرحله‌ی دوم آلیس، رله و شنودگر پس از دریافت سیگنال ارسالی توسط باب، فاز سیگنال دریافتی را تخمین می‌زنند:

$$\hat{\varphi}_A^{(2)} = \varphi_{AB} + \varphi_B + \varepsilon_A^{(2)} \quad (۱۳)$$

$$\hat{\varphi}_R^{(2)} = \varphi_{BR} + \varphi_B + \varepsilon_R^{(2)} \quad (۱۴)$$

$$\hat{\varphi}_E^{(2)} = \varphi_{BE} + \varphi_B + \varepsilon_E^{(2)} \quad (۱۵)$$

در روابط فوق $\varepsilon_A^{(2)}$، $\varepsilon_R^{(2)}$ و $\varepsilon_E^{(2)}$ به‌ترتیب خطای تخمین فاز در آلیس، رله و شنودگر هستند.

در مرحله‌ی سوم آلیس، باب و شنودگر پس از دریافت سیگنال ارسالی توسط رله، فاز سیگنال دریافتی را تخمین می‌زنند:

$$\hat{\varphi}_A^{(3)} = \varphi_{AR} + \varepsilon_A^{(3)} \quad (۱۶)$$

$$\hat{\varphi}_B^{(3)} = \varphi_{BR} + \varepsilon_B^{(3)} \quad (۱۷)$$

$$\hat{\varphi}_E^{(3)} = \varphi_{RE} + \varepsilon_E^{(3)} \quad (۱۸)$$

در روابط فوق $\varepsilon_A^{(3)}$، $\varepsilon_B^{(3)}$ و $\varepsilon_E^{(3)}$ به‌ترتیب خطای تخمین فاز در آلیس، باب و شنودگر هستند.

به منظور تولید کلید مشارکتی، هر یک از گره‌ها، پردازشی را بر روی فازهای دریافتی‌شان انجام می‌دهند. آلیس، فاز تخمینی در مرحله‌ی اول و سوم را با فاز تصادفی که در مرحله‌ی اول ارسال کرده است، جمع می‌زند و به $\hat{\theta}_A^{(2)}$ و $\hat{\theta}_A^{(3)}$ دست پیدا می‌کند:

$$\hat{\theta}_A^{(2)} = \hat{\varphi}_A^{(2)} + \varphi_A = \varphi_{AB} + \varphi_B + \varphi_A + \varepsilon_A^{(2)} \quad (۱۹)$$

$$\hat{\theta}_A^{(3)} = \hat{\varphi}_A^{(3)} + \varphi_A = \varphi_{AR} + \varphi_A + \varepsilon_A^{(3)} \quad (۲۰)$$

باب نیز فاز تخمینی در مرحله‌ی اول و سوم را با فاز تصادفی که در مرحله‌ی دوم ارسال کرده‌است، جمع می‌زند و به $\hat{\theta}_B^{(1)}$ و $\hat{\theta}_B^{(3)}$ دست پیدا می‌کند:

$$\hat{\theta}_B^{(1)} = \hat{\varphi}_B^{(1)} + \varphi_B = \varphi_{AB} + \varphi_B + \varphi_A + \varepsilon_B^{(1)} \quad (۲۱)$$

$$\hat{\theta}_B^{(3)} = \hat{\varphi}_B^{(3)} + \varphi_B = \varphi_{BR} + \varphi_B + \varepsilon_B^{(3)} \quad (۲۲)$$

رله تغییری در فاز تخمینی در مرحله‌ی اول و دوم اعمال نمی‌کند و همان مقدار را در نظر می‌گیرد:

$$\hat{\theta}_R^{(1)} = \hat{\varphi}_R^{(1)} = \varphi_{AR} + \varphi_A + \varepsilon_R^{(1)} \quad (۲۳)$$

$$\hat{\theta}_R^{(2)} = \hat{\varphi}_R^{(2)} = \varphi_{BR} + \varphi_B + \varepsilon_R^{(2)} \quad (۲۴)$$

آلیس و باب براساس $\hat{\theta}_{\mathrm{A}}^{(2)}$ و $\hat{\theta}_{\mathrm{B}}^{(1)}$ ، به تولید کلید $\mathbf{K}_1$ می‌پردازند. آلیس و رله نیز براساس $\hat{\theta}_{\mathrm{A}}^{(3)}$ و $\hat{\theta}_{\mathrm{R}}^{(1)}$ کلید $\mathbf{K}_2$ را تولید می‌کنند. باب و رله براساس $\hat{\theta}_{\mathrm{B}}^{(3)}$ و $\hat{\theta}_{\mathrm{R}}^{(2)}$ کلید $\mathbf{K}_3$ را تولید می‌کنند. نحوه‌ی تولید $\mathbf{K}_1$، $\mathbf{K}_2$ و $\mathbf{K}_3$ را در ادامه شرح می‌دهیم. هدف نهایی، تولید یک زوج کلید متقارن در آلیس و باب است، در حالی‌که کلید $\mathbf{K}_2$ و $\mathbf{K}_3$ به‌ترتیب بین آلیس و رله، و باب و رله ایجاد شده‌اند. در ادامه روشی آورده می‌شود تا هر سه کلید $\mathbf{K}_1$ ، $\mathbf{K}_2$ و $\mathbf{K}_3$ در آلیس و باب در دسترس باشند. رله $\mathbf{K} = \mathbf{K}_2 \oplus \mathbf{K}_3$ که xor بیت‌های کلید $\mathbf{K}_2$ و $\mathbf{K}_3$ می‌باشد را محاسبه می‌کند و از طریق کانال عمومی برای آلیس و باب ارسال می‌کند. پس از دریافت $\mathbf{K}$، آلیس $\mathbf{K} \oplus \mathbf{K}_2 = (\mathbf{K}_2 \oplus \mathbf{K}_3) \oplus \mathbf{K}_2 = \mathbf{K}_3$ را محاسبه می‌کند و به این ترتیب کلید $\mathbf{K}_3$ در آلیس به دست می‌آید. باب نیز حاصل $\mathbf{K} \oplus \mathbf{K}_3 = (\mathbf{K}_2 \oplus \mathbf{K}_3) \oplus \mathbf{K}_3 = \mathbf{K}_2$ را محاسبه می‌کند. به این ترتیب آلیس و باب، به هر سه کلید دسترسی دارند و از آنجایی‌که شنودگر $\mathbf{K}_2 \oplus \mathbf{K}_3$ را دریافت می‌کند، اطلاعاتی در خصوص کلیدهای $\mathbf{K}_2$ و $\mathbf{K}_3$ نخواهد داشت. باید این نکته را بیان نماییم که آلیس و باب نمی‌توانند هر دو کلید $\mathbf{K}_2$ و $\mathbf{K}_3$ را برای فرآیند تولید کلید به‌کار ببرند. علت این امر این است که شنودگر به $\mathbf{K}_2 \oplus \mathbf{K}_3$ دسترسی دارد. بنابراین، یکی از دو کلید $\mathbf{K}_2$ و $\mathbf{K}_3$ جهت تولید کلید مشارکتی به‌کار می‌رود. در انتها، کلید نهایی به‌صورت $\mathbf{K}_{\mathrm{Final}} = (\mathbf{K}_2 \text{ or } \mathbf{K}_3) \oplus \mathbf{K}_1$ به‌دست می‌آید. به این ترتیب که آلیس و باب یکی از کلیدهای $\mathbf{K}_2$ یا $\mathbf{K}_3$ را در $\mathbf{K}_1$، xor می‌کنند.

از دید شنودگر، او به دنبال دست‌یابی به قطعه کلید مشترک بین آلیس و باب است. برای تخمین $\mathbf{K}_1$، $\mathbf{K}_2$ و $\mathbf{K}_3$ از رابط (۲۵)، (۲۶) و (۲۷) استفاده می‌نماید:

$$\hat{\theta}_E^{\boldsymbol{K}_1} = \hat{\varphi}_E^{(1)} + \hat{\varphi}_E^{(2)} = \varphi_{AE} + \varphi_{BE} + \varphi_A + \varphi_B + \varepsilon_E^{(1)} + \varepsilon_E^{(2)} \quad (۲۵)$$

$$\hat{\theta}_E^{\boldsymbol{K}_2} = \hat{\varphi}_E^{(1)} + \hat{\varphi}_E^{(3)} = \varphi_{AE} + \varphi_{RE} + \varphi_A + \varepsilon_E^{(1)} + \varepsilon_E^{(3)} \quad (۲۶)$$

$$\hat{\theta}_E^{\boldsymbol{K}_3} = \hat{\varphi}_E^{(2)} + \hat{\varphi}_E^{(3)} = \varphi_{BE} + \varphi_{RE} + \varphi_B + \varepsilon_E^{(2)} + \varepsilon_E^{(3)} \quad (۲۷)$$

هر یک از گره‌ها جهت کوانتیزه کردن کلید، به طریقی که در ادامه می‌آوریم، عمل می‌کنند. اگر L تعداد سطوح کوانتیزاسیون باشد، تعداد بیت‌های مستخرج از هر نمونه کانال $\hat{\mathrm{L}} = \log_2 \mathrm{L}$ خواهد بود. اگر ψ بیانگر عرض نواحی محافظ باشد، گره‌ی $\mathrm{i} \in \{\mathrm{A}, \mathrm{B}, \mathrm{R}, \mathrm{E}\}$ با توجه به مقدار L و ψ مقادیر زیر را محاسبه می‌کند:

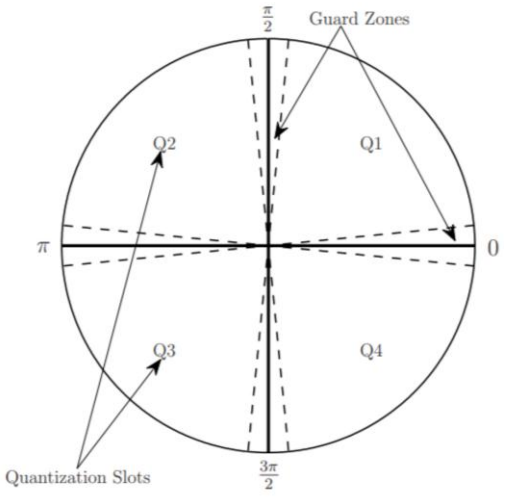
$$s_i = \left\lfloor \frac{\hat{\theta}_i}{\frac{2\pi}{L}} \right\rfloor,$$

$$s_i^+ = \left\lfloor \frac{\hat{\theta}_i + \psi/2}{2\pi/L} \right\rfloor, s_i^- = \left\lfloor \frac{\hat{\theta}_i - \psi/2}{2\pi/L} \right\rfloor \quad (۲۸)$$

سپس گره‌ی i قطعه کلید $\mathrm{k_i}$ را به‌صورت زیر محاسبه می‌کند:

$$k_i = \begin{cases} B(s_i) & if\ s_i^+ = s_i^- \\ \emptyset & Otherwise \end{cases} \quad (۲۹)$$

در رابطه‌ی فوق $B(x)$ دنباله‌ی باینری متناظر با x و به طول $\hat{\mathrm{L}}$ می‌باشد. $\emptyset$ نماد دور ریزی قطعه کلید مربوطه است. برای آشنایی با نحوه‌ی انجام نگاشت $\mathrm{B(x)}$، شکل ۴ برای $\mathrm{L} = 4$ و $\psi = \frac{\pi}{32}$ در نظر گرفته شده است.



شکل ٤. کوانتیزاسیون فاز با چهار ناحیه‌ی تصمیم و چهار ناحیه‌ی محافظ

۳. تحلیل امنیتی طرح پیشنهادی

در این قسمت می‌خواهیم به تحلیل امنیتی طرح ارائه شده بپردازیم. با مقایسه‌ی رابطه‌ی (۲۵) با (۱۹) و (۲۱) به این نتیجه می‌رسیم که زمانی $\hat{\theta}_{E}^{\mathbf{K}_1}$ به احتمال زیاد، به کلید $\mathbf{K}_1$ منجر می‌شود که $\Delta\varphi_1$ کمینه گردد. در این بخش، از اثر خطای تخمین فاز صرف‌نظر شده است که منجر به ارزیابی امنیت طرح، در بدترین شرایط ممکن می‌شود. $\Delta\varphi_1$ از رابطه‌ی زیر محاسبه می‌شود:

$$\Delta\varphi_1 \triangleq \left(\varphi_{E_1} - \varphi_{AB}\right) mod\ 2\pi \quad (۳۰)$$

یا

$$\Delta\varphi_1 \triangleq \left(\varphi_{AB} - \varphi_{E_1}\right) mod\ 2\pi$$

در رابطه‌ی فوق $\varphi_{E_1} \triangleq \varphi_{AE}+\varphi_{BE}$. با مقایسه‌ی رابطه‌ی (۲۶) با روابط (۲۰) و (۲۳) به این نتیجه می‌رسیم که زمانی $\hat{\theta}_{E}^{\mathbf{K}_2}$ به احتمال زیاد، به کلید $\mathbf{K}_2$ منجر می‌شود که $\Delta\varphi_2$ کمینه گردد. $\Delta\varphi_2$ عبارت است از:

$$\Delta\varphi_2 \triangleq \left(\varphi_{E_2} - \varphi_{AR}\right) mod\ 2\pi \quad (۳۱)$$

یا

$$\Delta\varphi_2 \triangleq \left(\varphi_{AR} - \varphi_{E_2}\right) mod\ 2\pi$$

در رابطه‌ی فوق $\varphi_{E_2} \triangleq \varphi_{AE}+\varphi_{RE}$. با مقایسه‌ی رابطه‌ی (۲۸) با روابط (۲۲) و (۲۴) به‌این نتیجه می‌رسیم که زمانی $\hat{\theta}_{E}^{\mathbf{K}_3}$ به احتمال زیاد به کلید $\mathbf{K}_3$ منجر می‌شود که $\Delta\varphi_3$ کمینه گردد. $\Delta\varphi_3$ از رابطه‌ی زیر محاسبه می‌گردد:

$$\Delta\varphi_3 \triangleq \left(\varphi_{E_3} - \varphi_{BR}\right) mod\ 2\pi \quad (۳۲)$$

یا

$$\Delta\varphi_3 \triangleq \left(\varphi_{BR} - \varphi_{E_3}\right) mod\ 2\pi$$

در رابطه‌ی فوق $\varphi_{E_3} \triangleq \varphi_{BE} + \varphi_{RE}$. ناحیه‌ی آسیب‌پذیری برای هر یک از کلیدهای $\mathbf{K}_1$، $\mathbf{K}_2$ و $\mathbf{K}_3$ به صورت زیر محاسبه می‌گردد:

$$\Delta\varphi_1 < \frac{2\pi}{L}, \Delta\varphi_2 < \frac{2\pi}{L}, \Delta\varphi_3 < \frac{2\pi}{L}, \quad (۳۳)$$

برای طرح تولید کلید در فضای آزاد، فازهای گوناگون به صورت زیر محاسبه می‌شوند:

$$\varphi_{AB} = \frac{2\pi d_{AB}}{\lambda}, \varphi_{AR} = \frac{2\pi d_{AR}}{\lambda},$$
$$\varphi_{BR} = \frac{2\pi d_{BR}}{\lambda}, \varphi_{AE} = \frac{2\pi d_{AE}}{\lambda},$$
$$\varphi_{BE} = \frac{2\pi d_{BE}}{\lambda}, \varphi_{RE} = \frac{2\pi d_{RE}}{\lambda}. \quad (۳۴)$$

با جایگذاری رابطه‌ی (۳۳) در رابطه‌ی (۳۴)، ناحیه‌ی آسیب‌پذیری کلیدهای $\mathbf{K}_1$، $\mathbf{K}_2$ و $\mathbf{K}_3$ به صورت زیر محاسبه می‌شوند:

$$\frac{d_{E_1} - d_{AB}}{\lambda} - \left\lfloor \frac{d_{E_1} - d_{AB}}{\lambda} \right\rfloor < \frac{1}{L}$$
$$\frac{d_{AB} - d_{E_1}}{\lambda} - \left\lfloor \frac{d_{AB} - d_{E_1}}{\lambda} \right\rfloor < \frac{1}{L} \quad (۳۵)$$

$$\frac{d_{E_2} - d_{AR}}{\lambda} - \left\lfloor \frac{d_{E_2} - d_{AR}}{\lambda} \right\rfloor < \frac{1}{L}$$
$$\frac{d_{AR} - d_{E_2}}{\lambda} - \left\lfloor \frac{d_{AR} - d_{E_2}}{\lambda} \right\rfloor < \frac{1}{L} \quad (۳۶)$$

$$\frac{d_{E_3} - d_{BR}}{\lambda} - \left\lfloor \frac{d_{E_3} - d_{BR}}{\lambda} \right\rfloor < \frac{1}{L}$$
$$\frac{d_{BR} - d_{E_3}}{\lambda} - \left\lfloor \frac{d_{BR} - d_{E_3}}{\lambda} \right\rfloor < \frac{1}{L} \quad (۳۷)$$

در روابط فوق d_{E_1}، d_{E_2} و d_{E_3} به ترتیب به‌صورت $d_{E_1} \triangleq d_{AE} + d_{BE}$، $d_{E_2} = d_{AE} + d_{RE}$ و $d_{E_3} = d_{BE} + d_{RE}$ تعریف می‌شوند. توجه شود از آنجایی‌که شنودگر به $\mathbf{K}_2 \oplus \mathbf{K}_3$

دسترسی دارد، ناحیه‌ی آسیب‌پذیری برای $\mathbf{K}_2$ و $\mathbf{K}_3$ اجتماع نواحی آسیب‌پذیری مطرح در روابط (۳۶) و (۳۷) خواهد بود که در ادامه توضیح می‌دهیم.

اکنون می‌خواهیم ناحیه‌ی آسیب‌پذیری مربوط به $\mathbf{K}_{\text{Final}}$ را تشریح کنیم. برای آنکه هر سه کلید در آلیس و باب در دسترس باشند، رله $\mathbf{K}_2 \oplus \mathbf{K}_3$ را در کانال عمومی برای آلیس و باب ارسال می‌کند. بنابراین شنودگر به $\mathbf{K}_2 \oplus \mathbf{K}_3$ دسترسی دارد. حال اگر شنودگر به هر یک از کلیدهای $\mathbf{K}_2$ یا $\mathbf{K}_3$ دست پیدا کند، توانایی دست‌یابی به دیگری را دارد. بنابراین ناحیه‌ی آسیب‌پذیری هر یک از کلیدهای $\mathbf{K}_2$ و $\mathbf{K}_3$ به‌طور دقیق اجتماع ناحیه‌های آسیب‌پذیری مطرح شده در روابط (۳۶) و (۳۷) است. ناحیه‌ی آسیب‌پذیری دقیق $\mathbf{K}_2$ و $\mathbf{K}_3$ به‌صورت زیر خواهد بود.

همانطور که بیان شد، کلید نهایی از رابطه‌ی $\mathbf{K}_{\text{Final}} = (\mathbf{K}_2 \text{ or } \mathbf{K}_3) \oplus \mathbf{K}_1$ محاسبه می‌شود. بنابراین ناحیه‌ی آسیب‌پذیری کلید نهایی، اشتراک ناحیه‌ی آسیب‌پذیری مطرح شده در رابطه (۳۵) و ناحیه‌ی آسیب‌پذیری مطرح شده در روابط (۳۶) و (۳۷) می‌باشد. چرا که زمانی شنودگر به $\mathbf{K}_{\text{Final}}$ دسترسی خواهد داشت که به $\mathbf{K}_1$ و هر یک از کلیدهای $\mathbf{K}_2$ یا $\mathbf{K}_3$ که در فرآیند تولید کلید استفاده می‌شوند، دسترسی داشته باشد. تنها با دسترسی به یکی از آن‌ها، توانایی دست‌یابی به $\mathbf{K}_{\text{Final}}$ را نخواهد داشت.

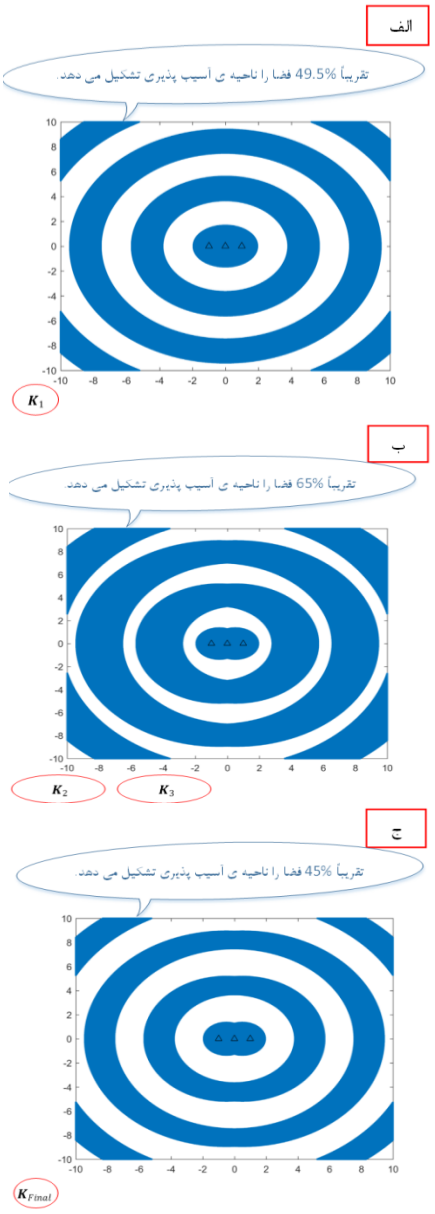
توجه ۱: در صورتی‌که رله در فرآیند SKG مشارکت نکند، ناحیه‌ی آسیب‌پذیری برابر ناحیه‌ی آسیب‌پذیری $\mathbf{K}_1$ خواهد بود که از رابطه‌ی (۳۵) محاسبه می‌شود. با مشارکت رله در فرآیند تولید کلید مشارکتی، ناحیه‌ی آسیب‌پذیری از اشتراک روابط (۳۵)-(۳۹) به‌دست می‌آید. بنابراین استفاده از رله سبب کاهش نواحی آسیب‌پذیری می‌گردد.

توجه ۲: اگر فرکانس نمونه‌برداری کانال برای دو پهباد f_S باشد، در اینصورت نرخ تولید کلید $\mathrm{R} = \mathrm{f_s}(1 - \mathrm{P_{KD}})$ خواهد شد که $\mathrm{P_{KD}}$ احتمال دور ریزی کلیدها می‌باشد که به ψ یعنی عرض نواحی محافظ ربط دارد. از آنجایی‌که افزایش ψ منجر به کاهش نرخ خطای کلید و نرخ تولید کلید می‌شود، انتخاب ψ برای برقراری تعادل بین نیازمندی‌های نرخ خطای کلید و نرخ تولید کلید بسیار مهم است. به‌عنوان مثال، اگر یک پهباد، قابلیت تصحیح خطای بالایی داشته باشد و نرخ تولید کلید بالا، مطلوب آن باشد، در اینصورت نرخ خطای کلید یک معیار مطلوب نیست و در عوض یک ψ کوچک ترجیح داده می‌شود.

۴. شبیه‌سازی و تفسیر نتایج

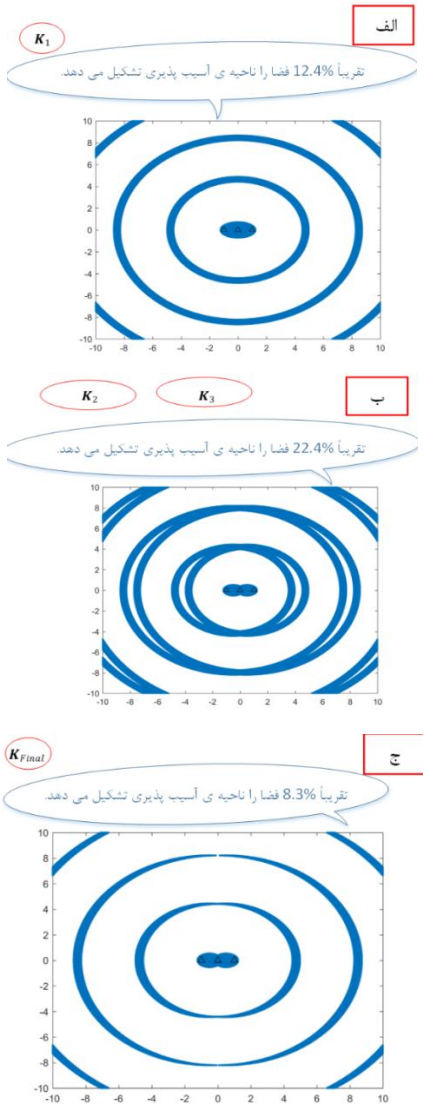
در این بخش به شبیه‌سازی نواحی آسیب‌پذیری طرح تولید کلید مشارکتی پیشنهادی می‌پردازیم. همچنین این طرح نوین را با طرح ارسال مستقیم و بدون استفاده از رله [۱۷] مقایسه می‌کنیم تا اهمیت حضور رله، هر چند غیرقابل اعتماد، مشخص شود.

برای شبیه‌سازی، موقعیت آلیس، رله و باب در فضای R^2 به‌ترتیب $(-1,0)$، $(0,0)$ و $(+1,0)$ در نظر گرفته می‌شود. فرکانس‌کاری و تعداد سطوح کوانتیزاسیون به ترتیب $\mathrm{f} = 40\mathrm{MHz}$ و $\mathrm{L} = 4$ فرض شده‌اند. در این حالت، نواحی آسیب‌پذیری مربوط به $\mathbf{K}_1$، هر کدام از $\mathbf{K}_2$ یا $\mathbf{K}_3$ و $\mathbf{K}_{\text{Final}}$ به‌ترتیب در شکل ۴ الف، ۴ ب و ۴ ج نمایش داده‌شده اند. رنگ آبی و سفید به ترتیب بیانگر ناحیه‌ی آسیب‌پذیری و ناحیه‌ی محرمانه هستند. ناحیه‌ی آسیب‌پذیری $\mathbf{K}_1$، هر کدام از $\mathbf{K}_2$ یا $\mathbf{K}_3$ و $\mathbf{K}_{\text{Final}}$ به ترتیب تقریباً حدود 50، 65 و 45 درصد از فضا را پوشش می‌دهند. همان‌طوری که نتیجه می‌گیریم حضور رله سبب شده است که حدود 5 درصد از ناحیه آسیب‌پذیری کاهش یابد.



شکل ٤. نواحی آسیب پذیری برای $f = 40MHz$ و $L = 4$: الف) ناحیه‌ی آسیب‌پذیری برای K_1، ب) ناحیه‌ی آسیب‌پذیری برای هر یک از کلیدهای K_2 و K_3، ج) ناحیه‌ی آسیب‌پذیری برای K_{Final}

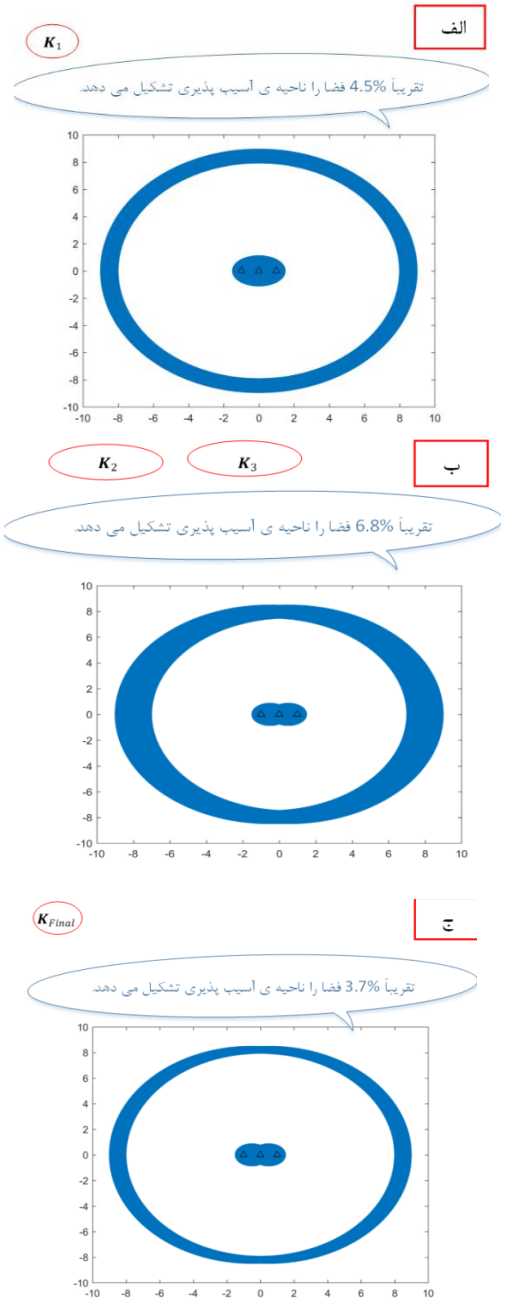
برای مشاهده‌ی تأثیر تعداد سطوح کوانتیزاسیون، $L = 16$ لحاظ می‌گردد و سایر پارامترها را تغییری نمی‌دهیم. نتایج شبیه‌سازی در شکل ۴ آورده شده است. ناحیه‌ی آسیب‌پذیری برای $\boldsymbol{K_1}$، هر کدام از $\boldsymbol{K_2}$ یا $\boldsymbol{K_3}$ و $\boldsymbol{K_{Final}}$ به‌ترتیب تقریباً حدود 12.4، 22.4 و 8.3 درصد از فضا را پوشش می‌دهد. با مقایسه شکل ۳ و ۴ نتیجه می‌گیریم که با افزایش تعداد سطوح کوانتیزاسیون، درصد نواحی آسیب‌پذیری کاهش می‌یابد. البته در این حالت، نرخ تولید کلید نیز افزایش می‌یابد؛ اما توجه شود که نرخ خطای تولید کلید نیز افزایش می‌یابد. لذا این مصالحه بین کاهش نواحی آسیب پذیری (و در نتیجه تقویت امنیتی طرح تولید کلید) و نیز افزایش نرخ خطای کلید (و در نتیجه تضعیف کارآمدی طرح تولید کلید) را باید در نظر گرفت.



شکل ۵. نواحی آسیب پذیری برای $f = 40MHz$ و $L = 16$: الف) ناحیه‌ی آسیب‌پذیری برای K_1، ب) ناحیه‌ی آسیب‌پذیری برای هر یک از کلیدهای K_2 و K_3، ج) ناحیه‌ی آسیب‌پذیری برای K_{Final}

تاکنون فرض بر این بود که برای تولید یک دنباله کلید، روال کاوش کانال همواره بر روی یک فرکانس انجام می‌شود. از آنجا که پارامتر طول موج (λ) بر میزان نواحی آسیب‌پذیری تاثیرگذار است، لذا هندسه‌ی این نواحی و نیز نواحی محرمانه با تغییر فرکانس سیگنال کاوش (پویاسازی فرکانسی)، قابل دستکاری است [۱۷]. با عنایت به این موضوع، پیشنهاد می‌دهیم برای تولید یک دنباله کلید، کاوش کانال بر روی یک مجموعه از فرکانس‌های مختلف $\mathbb{F} = \{f_1, f_2, \dots, f_F\}$ اجرا گردد. به‌عبارت دیگر، هر سیگنال کاوش بر روی یک فرکانس از مجموعه فرکانسی $\mathbb{F}$ ارسال می‌گردد و ضمناً الگوی فرکانسی کاوش کانال به‌صورت عمومی در دسترس همگان و بخصوص آلیس و باب است. در ادامه تأثیر این ایده را بر بهبود نواحی محرمانه مورد بررسی قرار می‌دهیم.

بر پایه ایده فوق (پویاسازی فرکانسی)، اگر شنودگر بخواهد کل دنباله کلید را بدست آورد باید در مکانی مستقر شود که این مکان به ازاء تمام فرکانس‌های موجود در مجموعه $\mathbb{F}$، جزو نواحی آسیب‌پذیری باشد. بنابراین، به طور شهودی می‌توان گفت که میزان نواحی آسیب‌پذیری در صورت استفاده از چندین فرکانس نسبت به حالت تک فرکانس کمتر است. به بیان دیگر، در طرح پویاسازی فرکانسی، برای هر فرکانس، یک مجموعه نواحی آسیب‌پذیری به‌دست می‌آید. اشتراک این نواحی آسیب‌پذیری به ازای فرکانس‌های مختلف، ناحیه‌ی آسیب‌پذیری کل را نتیجه خواهد داد. به عنوان مثال، برای $L = 4$ و سه فرکانس کاوش کانال $f = 40, 60, 80$ MHz نواحی آسیب‌پذیری مربوط به $\mathbf{K}_1$، هر کدام از $\mathbf{K}_2$ یا $\mathbf{K}_3$ و $\mathbf{K}_{\text{Final}}$ به‌ترتیب در شکل ۶ الف، ۶ ب و ۶ ج نمایش داده شده‌اند. ناحیه‌ی آسیب‌پذیری $\mathbf{K}_1$، هر کدام از $\mathbf{K}_2$ یا $\mathbf{K}_3$ و $\mathbf{K}_{\text{Final}}$ به‌ترتیب حدود 4.5، 6.8 و 3.7 درصد از فضا را پوشش می‌دهند. با مقایسه شکل‌های ۴ و ۶ مشاهده می‌شود که طرح پویاسازی کانال، درصد نواحی آسیب پذیری را به شدت کاهش می‌دهد و در نتیجه امنیت طرح را ارتقاء می‌دهد؛ بدون آنکه کارآمدی کلید (نرخ خطای کلید) افزایش یابد.



شکل ۶. نواحی آسیب پذیری برای $f = 40,60,80MHz$ و $L = 16$: الف) ناحیه‌ی آسیب‌پذیری برای K_1، ب) ناحیه‌ی آسیب‌پذیری برای هر یک از کلیدهای K_2 و K_3، ج) ناحیه‌ی آسیب‌پذیری برای K_{Final}

۵. نتیجه‌گیری

در این مقاله، یک طرح تولید کلید لایه فیزیکی مبتنی بر فاز کانال برای ارتباطات پهباد-به-پهباد ارائه گردید. علاوه بر مولدهای تصادفی محلی از یک رله‌ی غیرقابل اعتماد نیز برای تزریق سیگنال تصادفی استفاده شد. بر این اساس، یک طرح تولید کلید پیشنهاد گردید به طوری‌که رله‌ی غیرقابل اعتماد نتواند به کلید مخفی دست یابد. کلید تولید شده مبتنی بر طرح پیشنهادی، قابلیت استفاده برای تولید الگوی پرش فرکانسی، جهت مقابله با حمله‌ی جمینگ دارند. سپس طرح را از منظر نواحی آسیب‌پذیری مورد مطالعه قرار دادیم. مشاهده شد که طرح کاوش کانال بر روی چند فرکانس به جای یک فرکانس، نواحی آسیب‌پذیری را کاهش می‌دهد. همچنین نتایج شبیه‌سازی حاکی از مصالحه‌ای بین نواحی آسیب‌پذیری و نیز نرخ خطای کلید بودند.

برای ادامه کار، پیشنهاد می‌شود که طرح تولید کلید مشارکتی پیشنهادی، از منظر نرخ خطای کلید مورد ارزیابی قرار گیرد. همچنین به منظور عملیاتی‌کردن طرح پیشنهادی، پیشنهاد می‌شود که به جای تزریق فاز پیوسته توسط پهبادها، رویکرد عملی تزریق فاز تصادفی گسسته (مثلا مدولاسیون PSK)، طراحی و از منظر امنیتی تحلیل شود. به‌کارگیری روش‌های یادگیری عمیق و یادگیری ماشین نیز به کاهش نرخ خطای کلید کمک کننده هستند.

۶. مآخذ

[1]. Y. Zeng, R. Zhang, and T. J. Lim, Wireless Communications with Unmanned Aerial Vehicles: Opportunities and Challenges, IEEE Commun. Mag., vol. 54, no. 5, pp. 36–42, May 2016.

[2]. Shui Wang, Kehan Zhang, Bingcheng Zhu, Wei Wang, Zaichen Zhang, Visible Light Communications for Unmanned Aerial Vehicle: Channel Modeling and Experimental Validation, IEEE Commun. Lett., vol. 27, no. 6, pp.1530-1534, May 2023.

[3]. J. Liang, W. Liu, N. N. Xiong, A. Liu, and S. Zhang, An intelligent and trust uav-assisted code dissemination 5g system for industrial internetof-things, IEEE Trans. Industrial Informatics, vol. 18, no. 4, pp. 2877–2889, June 2022.

[4]. M. Ahmed, H. Shi, X. Chen, Y. Li, M. Waqas, and D. Jin, Socially aware secrecy-ensured resource allocation in d2d underlay communication: An overlapping coalitional game scheme, IEEE Trans. Wireless Commun., vol. 17, no. 6, pp. 4118–4133, Aug. 2018.

[5]. X. Sun, D. W. K. Ng, Z. Ding, Y. Xu, and Z. Zhong, Physical layer security in UAV systems: Challenges and opportunities, IEEE Wireless Commun., vol. 26, no. 5, pp. 40–47, Jan. 2019.

[6]. A. D. Wyner, The Wiretap Channel, J. Bell System Tech., vol. 54, pp. 1355–1387, 1975.

[7]. D. Abbasi-Moghadam, V. T. Vakili, and A. Falahati, Combination of turbo coding and cryptography in NONGEO satellite communication systems, International Symposium on Telecommunications (IST), 2008, pp. 666-670.

[8]. G. Noubir, On connectivity in Ad-hoc network under jamming using directional antennas and mobility, 2nd Int'l. Conf. Wired and Wireless Internet Commun. 2004.

[9]. A. Kuhestani, A. Mohammadi, and M. Mohammadi, Joint relay selection and power allocation in large-scale MIMO systems with untrusted relays and passive eavesdroppers, IEEE Trans. Inf. Forensics Security, vol 13, no. 2, pp. 341–355, Feb. 2018.

[10]. M. Forouzesh, F. Samsami Khodadad, P. Azmi, A. Kuhestani and H. Ahmadi, Simultaneous secure and covert transmissions against two attacks under practical assumptions, IEEE Internet of Things J., vol. 10, no. 12, pp. 10160-10171, June 2023.

[11] M. Ragheb, A. Kuhestani, M. Kazemi, H. Ahmadi and L. Hanzo, RIS-aided secure millimeter-wave communication under RF-chain impairments, IEEE Trans. Veh. Technol., doi: 10.1109/TVT.2023.330745.

[12]. M. Letafati, A. Kuhestani, and H. Behroozi, Three-hop untrusted relay networks with hardware imperfections and channel estimation errors for Internet of Things, IEEE Trans. Inf. Forensics Security, vol. 15, pp. 2856–2868, Mar. 2020.

[13]. M. Ragheb, S. M. S. Hemami, A. Kuhestani, D. W. K. Ng and L. Hanzo, On the physical layer security of untrusted millimeter wave relaying networks: A stochastic geometry Approach, IEEE Trans. Inf. Foren. Sec., vol. 17, pp. 53-68, Feb. 2022.
[14]. J. Zhang, G. Li, A. Marshall, A. Hu and L. Hanzo, A new frontier for IoT security emerging from three decades of key generation relying on wireless channels, IEEE Access, vol. 8, pp. 138406–138446, Jul. 2020.
[15] M. Letafati, A. Kuhestani, K. -K. Wong and M. J. Piran, A lightweight secure and resilient transmission scheme for the Internet of Things in the presence of a hostile jammer, IEEE Internet of Things Journal, vol. 8, no. 6, pp. 4373-4388, 15 Mar. 2021.
[16]. M. Letafati, A. Kuhestani, D. W. K. Ng, and H. Behroozi, A new frequency hopping-aided secure communication in the presence of an adversary jammer and an untrusted relay, IEEE ICC'20 Workshop, Dublin, Ireland, Jun. 2020.
[17]. A. H. Khalili Tirandaz and A. Kuhestani, Security evaluation of mutual random phase injection scheme for secret key generation over static point-to-point communications, Journal of Electronic & Cyber Defense, Oct. 2022.
[18]. K. Ren, H. Su, and Q. Wang, Secret key generation exploiting channel characteristics in wireless communications, IEEE Wireless Communications, vol. 18, pp. 6-12, 2011.
[19] Q. Wang, H. Su, K. Ren, and K. Kim, Fast and scalable secret key generation exploiting channel phase randomness in wireless networks, 2011 Proceedings IEEE INFOCOM, pp. 1422-1430.
[20] A. A. Hassan, W. E. Stark, J. E. Hershey, and S. Chennakeshu, Cryptographic key agreement for mobile radio, Digital Signal Processing, vol. 6, pp. 207-212, Apr. 1996.
[21] D. Rife and R. Boorstyn, Single-tone parameter estimation from discrete-time observations, IEEE Transactions on Information Theory, vol. 20, no. 5, pp. 591–598, Aug. 1974.
[22] S. Eberz, M. Strohmeier, M. Wilhelm and I. Martinovic, A Practical Man-In-The-Middle Attack on Signal-Based Key Generation Protocols, Computer Security – ESORICS, vol 7459, pp. 235-252, May 2012.
[23] C. Feng and L. Sun, Physical layer key generation from wireless channels with non-ideal channel reciprocity: A deep learning based approach, IEEE 95th Vehicular Technology Conference: (VTC2022-Spring), Helsinki, Finland, 2022, pp. 1-6.
[24] X. Guan, N. Ding, Y. Cai and W. Yang, Wireless key generation from imperfect channel state information: Performance analysis and improvements, IEEE International Conf. Commun. (ICC), Shanghai, China, 2019, pp. 1-6.

۸. پی‌نوشت

[i]. Unmanned air vehicle
[ii]. Line-of-Sight
[iii]. Lightweight
[iv]. Static
[v]. Vulnerability region
[vi]. Channel probing
[vi]. Geometric secrecy
1. PLS: Physical Layer Security
2. Wyner
3. Wiretap channel
4. Legitimate
5. Eavesdropper
6. Beamforming
7. Artificial Noise
8. Secrecy
9. Cooperative communication
10. SKG: Secret Key Generation
11. RSS: Received Signal Strength
12. CSI: Channel State Information
13. Lightweight
14. SNR: Signal-to-Noise-Ratio
15. Fading
16. AWGN: Additive White Gaussian Noise
17. Static
18. Frequency hopping
19. Half-duplex
20. Coherence time
21. Reciprocal