تولید کلید لایه فیزیکی برای ارتباطات پهبادها و سنجش پایداری آن در برابر حملات غیرفعال و فعال

تاریخ دریافت: ۱۴۰۲/۰۶/۲۹
تاریخ پذیرش: ۱۴۰۲/۰۸/۰۱

محمدرضا کشاورزی[۱]، بهمن مددی[۲]، علی رحمان‌پور[۳]، علی کوهستانی[٤]

۱- استادیار، پژوهشکده فناوری ارتباطات، پژوهشگاه ارتباطات و فناوری اطلاعات
۲- دانشجوی دکتری جنگ الکترونیک مخابراتی دانشگاه جامع امام حسین (ع)
۳- کارشناس ارشد، دانش آموخته مخابرات امن دانشگاه علم و صنعت ایران
٤- استادیار، دانشکده مهندسی برق و کامپیوتر، دانشگاه صنعتی قم، kuhestani@qut.ac.ir

چکیده

ارتباطات بی‌سیم پهبادها[i] به دلایلی از قبیل امکان تحرک بالا، هزینه کم، استقرار بر اساس نیاز و نیز بهره‌وری از کانال‌های دید مستقیم[ii] هوا به زمین، علاقه‌مندی بسیاری را در کاربردهای نظامی و تجاری جلب کرده است. با این حال، این مزایا سیستم‌های ارتباطی بی‌سیم پهپاد را در برابر حملات غیرفعال و حملات فعال آسیب‌پذیر می‌کند. اخیراً راهکار امنیتی نوین و کارآمدی به نام تولید کلید از ویژگی‌های کانال بی‌سیم بسیار مورد توجه قرار گرفته است. در این مقاله، با تمرکز بر روی روش‌های مبتنی بر فاز کانال، دو روش عملی تولید کلید از فاز کانال یعنی: ۱) روش اول، استفاده از اختلاف فاز یک سیگنال سینوسی با دو فرکانس و ۲) روش دوم، به‌کارگیری فاز اولیهٔ تصادفی برای سیگنال سینوسی با یک فرکانس، معرفی می‌شوند. نتایج شبیه‌سازی نشان می‌دهد تولید کلید مبتنی بر روش دوم از منظر حملات فعال (حملهٔ مرد در میان[iii] و حملهٔ پارازیت[iv])، عملکرد بهتری نسبت به روش اول داشته و به‌علاوه، با تولید کلید با آنتروپی بالا بر چالش ایستایی لینک‌های پهباد غلبه می‌کند. بر این اساس، روش به‌کارگیری فاز اولیهٔ تصادفی از حیث احتمال موفقیت در تولید کلید برای نسبت سیگنال به نویزهای مختلف، تأثیر پارامتر کوانتیزاسیون و سایر عوامل مورد ارزیابی قرار می‌گیرد. همچنین این روش از منظر نواحی افشای کلید[v] مطالعه خواهد شد.

واژه‌های کلیدی: *امنیت پهباد، امنیت لایه فیزیکی، تولید کلید مخفی، فاز کانال.*

Physical layer key generation for UAV communication and measuring its resilience against passive and active attacks

Mohammadreza Keshavarzi[1], Bahman Madadi[2], Ali Rahmanpour[3], Ali Kuhestani[4]

1- ICT Research Institute, Iran Telecommunication Research Center (ITRC), Tehran, Iran
2- Ph.D student, Imam Hossein University, Tehran, Iran.
3- Iran University of Science and Technology, Iran.
4- Assistant Professor, Faculty of Electrical and Computer Engineering, Qom University of Technology, Qom, Iran.

Abstract

The wireless communication of unmanned aerial vehicles (UAVs) has attracted a lot of interest for reasons such as the possibility of high mobility, low-cost, deployment based on needs, and the efficiency of direct air-to-ground channels. However, these advantages make UAV wireless communications vulnerable to both passive and active attacks. Recently, key generation from wireless channels has gained much attention. Here, by focusing on the key generation from the channel phase, two methods of generating the key from the channel phase are introduced: 1) the first method, using the phase difference of a sinusoidal signal with two frequencies and 2) the second method, choosing the random initial phase for a sinusoidal signal with one frequency. The simulation results show that key generation based on the second method performs better than the first method from the perspective of active attacks (man-in-the-middle attack and jammer attack). For this purpose, the second method is studied in terms of the probability of success in key generation and the key disclosure resion.

Keywords: *UAV security, physical layer security, secret key generation, channel phase.*

۱. مقدمه

در سال‌های اخیر، پهپادها به دلیلی از قبیل قابلیت تحرک بالا، استقرار منعطف، فراهم آوردن نرخ دادهٔ بالا، تسریع در انتقال اطلاعات، پوشش وسیع محیط جغرافیایی و یاری‌رسانی به دیگر فناوری‌های مخابراتی در ایام بحران، توجه بی‌نظیری از پژوهشگران حوزهٔ نظامی و تجاری را به خود جلب کرده است [۱] و [۲]. این وسایل نقلیهٔ هوایی بدون‌سرنشین می‌توانند نقشی حیاتی در پشتیبانی از ارتباطات مطمئن و امن ایفا کنند. به بیان دیگر، در مقایسه با ارتباطات سنتی زمینی، پهپادها به دلیل بهره‌وری از لینک‌های انتقال 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].

با وجود ویژگی‌های امیدوارکنندهٔ ذکر شده برای پهپادها، چالش‌های متعددی در راه‌اندازی پهپادها وجود دارد. در میان چالش‌های مختلف، امنیت به عنوان یک از چالش‌های اصلی در ارتباطات کارآمد پهپادها محسوب می‌شود. با افزایش حملات به لینک‌های مخابراتی، کنترلی و موقعیت‌یابی پهپاد، استفاده از الگوریتم‌های رمزنگاری مقاوم ضروری است. با این حال، الگوریتم‌های رمزنگاری پیچیده‌تر مستلزم سربار قابل توجهی هستند و بنابراین اندازهٔ بسته ارسالی افزایش می‌یابد. همچنین پهنای‌باند مورد نیاز را به میزان قابل توجهی افزایش می‌دهد و در نتیجه کارایی طیفی کاهش می‌یابد.

الگوریتم‌های رمزنگاری مبتنی بر پیچیدگی محاسباتی هستند که با افزایش پیچیدگی آنها، هزینه و سربار محاسباتی تجهیزات/دستگاه‌ها افزایش می‌یابد؛ از سوی دیگر، مهاجمان امروزی مجهز به منابع محاسباتی نامحدود (ابررایانه‌ها با پردازش‌های کوانتومی) هستند و لذا می‌توانند برای سیستم‌های رمزنگاری فاجعه‌بار باشند [۴]. علاوه بر این، فرآیندهای اشتراک‌گذاری و مدیریت متمرکز کلید برای شبکه‌های توزیع شده مانند اینترنت اشیاء و پهپادها چالش برانگیز هستند. برای غلبه بر چالش‌های پیش‌روی تکنیک‌های رمزنگاری سنتی، اخیراً امنیت لایه فیزیکی[۱] (PLS) معرفی شده است [۵]. PLS یک تکنیک نوظهور و قدرتمند است که متکی بر نظریه اطلاعات می‌باشد و می‌تواند همراه با تکنیک‌های رمزنگاری برای امن کردن ارتباطات پهپادها و نیز قابلیت اطمینان آنها به‌کار گرفته شود [۵]. PLS از تصادفی بودن ویژگی کانال بی‌سیم برای برقراری امنیت استفاده می‌کند.

اولین بار در مقاله شناخته شدهٔ آقای واینر[۲] [۶] بود که در آن موضوع کانال شنود[۳] به عنوان زیربنای PLS مطرح گردید. در این 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 لحاظ کردن تفاوت‌های آن دو، ایدهٔ 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 این بین روش‌های ذکر شده، SKG توجه بسیاری را در حوزه صنعت به خود جلب کرده است [۱۴].

یکی از چالش‌های اصلی در ارتباطات، چگونگی به اشتراک‌گذاری یک کلید مخفی بین گره‌های قانونی شبکه است، به طوری‌که گره‌های غیرمجاز از این کلید آگاه نشود. اگر چه روش‌هایی همچون دیفی-هلمان تا حدی این چالش را برطرف می‌کنند، اما بار محاسباتی زیاد آن‌ها از یک‌سو و متکی بودنشان بر پیچیدگی محاسباتی از سوی دیگر، موجب شده است تا تحقیقات پیرامون روش‌های جایگزین آن به طور جدی دنبال شود [۱۴]. در این راستا، SKG در لایه فیزیکی بسیار جذاب است [۱۴]. در این روش، 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]. در روش‌های مبتنی بر SKG، بر خلاف روش‌های متداول پیشین، می‌توان فرض کرد که گره‌های غیرمجاز، توانایی محاسباتی نامحدودی داشته و در عین حال، امنیت تضمین شده باشد. 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 در دسترس تجهیزات کم باشد مناسب‌تر است [۱۴] و [۱۵].

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 پدیدهٔ محوشدگی[۱۵] وجود نخواهد داشت. 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 اندازهٔ کافی تصادفی تولید نمی‌کنند. توجه شود که از منظر امنیت، چالشی‌ترین وضعیت برای SKG، مربوط به همین ارتباطات دید مستقیم می‌باشد که در آن، کانال قانونی و کانال شنود با AWGN مدل می‌شوند [۱۴] و [۱۷]. در این حوزه، مرجع اخیر [۱۷] از *فاز کانال* بی‌سیم به‌عنوان منبع تصادفی با آنتروپی بالا برای پیاده‌سازی تولید کلید در ارتباطات ایستا[۱۷] استفاده کرده است.

این پژوهش بر روی تولید کلید از فاز کانال تمرکز دارد و روش‌های تولید کلید از فاز کانال به‌طور کامل بررسی می‌گردد. بر این اساس، نوآوری‌های این کار به شرح زیر است:

- دو روش تولید کانال از فاز کانال یعنی: ۱) استفاده از اختلاف فاز یک سیگنال سینوسی با دو فرکانس و ۲) به‌کارگیری فاز اولیهٔ تصادفی در یک سیگنال سینوسی با یک فرکانس، مورد مطالعه قرار می‌گیرند. تحقیقات این کار نشان می‌دهد که تولید کلید مبتنی بر روش

دوم از منظر حملات فعال (حمله مرد در میان و حمله پارازیت)، عملکرد بهتری نسبت به روش اول دارد. روش دوم یعنی تزریق فاز اولیهٔ تصادفی از حیث احتمال موفقیت در تولید کلید برای SNRهای مختلف، تأثیر پارامتر کوانتیزاسیون، تأثیر فرکانس نمونه‌برداری و سایر عوامل مورد ارزیابی قرار می‌گیرد.

- همچنین با الهام از مرجع [۱۷]، نواحی افشای کلید برای حالت *تزریق فاز تصادفی گسسته* تعریف و محاسبه می‌شود. توجه شود که متفاوت با کار اخیر [۱۷] که در آن فاز تصادفی پیوسته توسط کاربران تزریق می‌شود، در این کار، فاز تصادفی تزریقی از جنس گسسته و مبتنی بر مدولاسیون PSK بوده و لذا عملی‌تر است.
- به منظور کاهش نواحی افشای کلید، طرح کاوش کانال بر روی چند فرکانس به جای یک فرکانس، پیشنهاد و اجرایی می‌گردد.

بخش‌بندی مقاله به شرح زیر است: در بخش۲ مدل سیستم و نیز فرآیند و راهکارهای تولید کلید مبتنی بر کانال، با تمرکز بر فاز کانال ارایه می‌شود. بخش۳ به بررسی تولید کلید مبتنی بر فاز اولیهٔ تصادفی تزریقی پرداخته و ویژگی‌های آن در شرایط مختلف با شبیه‌سازی ارزیابی می‌گردد. همچنین در بخش۴، اثر حملات فعال بر روش‌های تولید کلید مبتنی بر فاز مطالعه می‌شود. در بخش۵، روش تولید کلید مبتنی بر تزریق فاز تصادفی گسسته معرفی و ارزیابی می‌گردد. در نهایت، در بخش ۶ این مقاله، به جمع‌بندی و ارائه کارهای آتی می‌پردازیم.

۲. تولید کلید مبتنی بر کانال

در این بخش، مدل سیستم و فرضیات آن را به‌طور کامل تبیین می‌کنیم. در گام بعد، طرح کلی تولید کلید مبتنی بر لایه فیزیکی را تشریح می‌نماییم و در انتها، دو روش جهت تولید کلید مبتنی بر فاز (که مطلوب ما در این مقاله است) ارائه می‌گردد.

۲-۱- مدل سیستم و فرضیات:

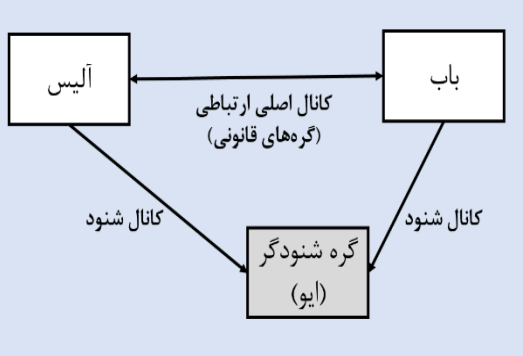
مدل کلی سیستم جهت تولید کلید، مطابق شکل ۱، شامل دو گرهٔ قانونی (این دو گرهٔ قانونی می‌توانند دو پهباد باشند که می‌خواهند تبادل داده داشته باشند و یا یک پهباد و یک کاربر زمینی باشند) به نام‌های آلیس و باب است که قصد دارند کلید مخفی K را با یکدیگر به اشتراک بگذارند. به‌علاوه در مدل سیستم، یک شنودگر داریم که قصد کشف کلید را دارد. فرضیات این کار پژوهشی به‌صورت زیر لیست می‌شود:

- تمام گره‌ها مجهز به یک آنتن هستند.
- ارتباطات در حالت نیمه‌دوسویه[۱۸] بوده و در نتیجه، هیچ گره‌ای قادر به تبادل اطلاعات به‌صورت هم‌زمان و در یک باند فرکانسی نیست.
- کانال بین گره‌ها از نوع دید مستقیم (AWGN) بوده و ضمناً ایستا می‌باشد.
- زمان همدوسی[۱۹] کانال به اندازه‌ای است که یک دور کامل تبادل کلید را پوشش می‌دهد

و ضمناً در این بازه زمانی، کانال هم‌پاسخ[20] است.

- از روش بیشینه شباهت[21] (ML) به منظور تخمین فرکانس و فاز استفاده می‌گردد.
- گره‌ها به‌طور کامل هم‌زمان‌سازی شده‌اند.
- شنودگر دارای توان محاسباتی نامحدود است و ضمناً می‌تواند فاز سیگنال‌های دریافتی خودش را به درستی تخمین بزند.

در بخش۴ این مقاله، مهاجم می‌خواهد به‌صورت فعالانه به فرآیند تبادل کلید ورود پیدا کرده و در کلید تغییر ایجاد کند و یا در فرآیند تولید کلید اخلال نماید. اما در بخش ۵ این مقاله، شنودگر قصد کشف کلید را دارد.



شکل ۱. نمایی کلی از مدل سیستم

۲-۲- فرآیند کلی تولید کلید از کانال:

مبنای غالب روش‌های تولید کلید از کانال فیزیکی، بر استفاده از مقادیر تصادفی کانال و خاصیت هم‌پاسخی آن برای استخراج یک رشته بیت مشخص و مشترک است. برای این کار، دامنه یا فاز سیگنال دریافتی توسط گره‌های کانال اندازه‌گیری شده و سپس اطلاعات لازم از آن استخراج می‌گردد. بنابراین به منظور اجرای فرآیند تولید کلید، می‌توانیم ۴ گام کلی زیر را در نظر بگیریم [۱۴]:

۱. **ارسال سیگنال‌های شناسایی (کاوش) بر روی کانال:**

از این سیگنال‌ها به منظور تولید کلید توسط آلیس و باب استفاده می‌گردد. توجه شود این سیگنال‌ها خود می‌توانند تحت شرایطی یکی از عوامل ایجاد حملهٔ فعال بر روی فرآیند تولید کلید و یا دخالت مهاجم در فرآیند آن باشند. در بخش۴ پیرامون این موضوع بحث می‌گردد.

۲. **پردازش بر روی سیگنال‌های کاوش دریافتی:**

سیگنال‌های کاوش توسط آلیس و باب دریافت می‌گردد. سپس ویژگی‌های موردنظر اندازه‌گیری شده و در نهایت با کمک یکی از روش‌های کوانتیزاسیون به بیت(ها) تبدیل می‌شوند.

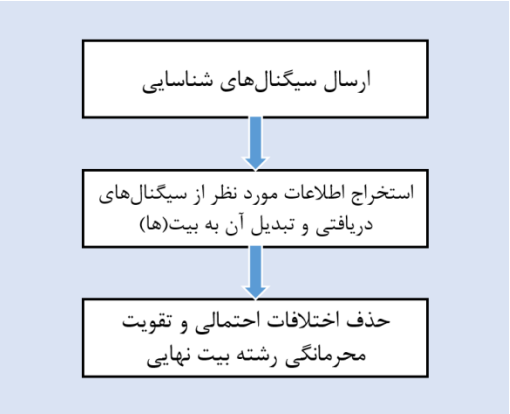
۳. **اصلاح[22] اختلافات احتمالی:**

ممکن است رشته بیت مخفی به‌دست آمده توسط هر یک از گره‌ها، در برخی بیت‌ها تفاوت داشته باشند. برای اصلاح این تفاوت‌ها از کدگذاری‌های مرسوم مانند Turbo و LDPC استفاده می‌شود [۱۴].

۴. **تقویت محرمانگی:**

در نهایت با کمک توابع چکیده‌ساز[23]، تقویت محرمانگی[24] رشته بیت نهایی انجام می‌گیرد.

نمایی از این مراحل در شکل ۲ آمده است. در این مقاله تمرکز ما بر دو بخش ابتدایی این فرآیند، یعنی تبادل سیگنال (کاوش کانال) و استخراج بیت‌های مخفی مشترک از آن می‌باشد.



شکل ۲. نمایی از مراحل کلی فرآیند تولید کلید از کانال

همان‌طور که اشاره شد، اگرچه کلیات این مراحل برای هر دو حالت استفاده از دامنه یا فاز کانال یکسان است، اما با توجه به تفاوت مشخصه‌های مورد استفاده، روش به‌کارگیری در هر یک برای تولید کلید، متفاوت می‌باشد. در ادامه جزئیات فرآیند تولید کلید مبتنی بر فاز کانال را مرور می‌کنیم.

۲-۳- تولید کلید از فاز کانال:

پیش از بررسی راهکار تولید کلید از فاز کانال، این پرسش مطرح است که با وجود روش‌های مبتنی بر دامنه، چرا باید به سراغ فاز رفت؟ در پاسخ باید گفت، روش‌هایی که از ویژگی تصادفی فاز کانال برای تولید کلید استفاده می‌کنند، نسبت به روش‌های مبتنی بر دامنه و توان، دارای برخی مزایای مهم هستند که ویژگی فاز را برای کاربرد پهباد بسیار ممتاز و ارزشمند می‌کند. برخی از مزایا عبارتند از:

- با کمک روش‌های پردازش سیگنال، امکان تخمین فاز سیگنال دریافتی با دقتی بالا وجود دارد و این امر، تولید کلید با نرخ بالا را امکان‌پذیر می‌سازد.
- در کانال بی‌سیم باند باریک، تغییرات فاز کانال را می‌توان با یک متغیر تصادفی با توزیع یکنواخت مدل کرد که این موضوع، به تولید یک کلید کاملاً تصادفی کمک به‌سزایی می‌کند.
- فاز کانال می‌تواند با ارسال‌های متوالی، در گره‌های مختلف انباشته شود. از این رو، برای تولید کلید گروهی (تولید کلید بین بیش از ۲ گره) بسیار ساده‌تر از روش‌های مبتنی بر دامنه است. برای نمونه می‌توان روش [۱۹] را برای تولید کلید گروهی مشاهده نمود.
- علاوه بر موارد فوق، یکی دیگر از ویژگی‌های مثبت فاز کانال که در بخش ۴ این مقاله به صورت دقیق‌تری بررسی خواهد شد، مقاومت مؤثرتر آن در مقابل حملهٔ مرد در میان، نسبت به روش‌های مبتنی بر دامنه و توان است.

حال به فرآیند تولید کلید از فاز کانال می‌پردازیم. مبنای روش‌های تولید کلید از فاز کانال، تبادل سیگنال‌های تک‌فرکانس (سینوسی) در کانال و سنجش فاز آن‌ها در سوی دیگر است. تاکنون دو روش اصلی برای تولید کلید از فاز ارائه شده است: روش اول که در آن از اختلاف فاز دو سیگنال سینوسی دریافتی از کانال بهره برده می‌شود ([۱۸]-[۲۰]) و روش دوم که راهکاری جدیدتر است، بر مبنای ارسال یک سیگنال سینوسی با فاز اولیهٔ تصادفی می‌باشد ([۱۷] و [۱۹]).

در ابتدا، روش اول که مبتنی بر سیگنال سینوسی با دو فرکانس است بیان می‌شود:

۱. ابتدا آلیس دو سیگنال سینوسی زیر را برای باب ارسال می‌کند.

$$S(t)=\cos(2\pi f_1 t+\Phi)+\cos(2\pi f_2 t+\Phi) \quad (۱)$$

در رابطهٔ فوق، f ها فرکانس‌های سیگنال سینوسی و Φ فاز اولیهٔ آن‌ها بوده که دلخواه می‌باشد.

۲. باب سیگنال‌ها را به صورت زیر، ولی با تضعیف متفاوت دریافت می‌کند؛ چرا که فرکانس‌های محتلف، کانال‌های مختلفی را تجربه می‌کنند. لذا داریم:

$$r(t)=\alpha_1(t)\cos(2\pi f_1 t+\Theta_1(t)) +\alpha_2(t)\cos(2\pi f_2 t+\Theta_2(t)) \quad (۲)$$

در رابطهٔ بالا به ازای $i=1,2$، $\alpha_i(t)$ بیانگر ضریب تضعیف انتشار سیگنال و $\Theta_i(t)$ فاز کانال است که به صورت یک فرآیند تصادفی با توزیع یکنواخت در $[0,2\pi]$ در نظر گرفته می‌شود.

۳. مشابه فرآیند فوق، باب نیز دو سیگنال سینوسی را در همان فرکانس برای آلیس ارسال کرده و سیگنال‌های تضعیف‌شده را دریافت می‌کند.

۴. نهایتاً اختلاف فاز بین دو سینوسی، یعنی $\Theta(t)=\Theta_1(t)-\Theta_2(t)$، توسط هر طرف ارتباطی اندازه‌گیری و برای کوانتیزاسیون استفاده می‌شود. از آنجایی‌که این فرآیند در زمان همدوسی کانال اجرا می‌شود، اختلاف فاز حاصل برای آلیس و باب مقداری تقریباً یکسان خواهد بود. به طور مشخص، به منظور کوانتیزاسیون، بازهٔ $[0,2\pi]$ به 2^N زیر بازهٔ مساوی تقسیم شده و عمل کوانتیزاسیون به این صورت تعریف می‌شود:

$$Q(\Phi_i)=q \quad if \quad \Phi_i\in\left[\frac{2\pi(q-1)}{2^N},\frac{2\pi q}{2^N}\right) \quad (۳)$$

که $q=1,2,\ldots,2^N$ است. به‌عنوان مثال، کوانتیزاسیون با $N=3$، بازهٔ $[0,2\pi]$ را به هشت زیربازه تقسیم کرده و هر زیربازه معادل سه بیت است. هر یک از گره‌های باب و آلیس پس از یک دور اجرای فرآیند فوق، دریافت سیگنال و محاسبهٔ $\Theta(t)$، بررسی می‌کنند که این مقدار در کدام زیربازه قرار گرفته و رشته بیت متناظر با آن را به‌دست می‌آورند. توجه شود که این نوع کوانتیزاسیون یکنواخت، بهینه است؛ چرا که فازهای تصادفی دریافتی درکاربران، توزیع یکنواخت دارد.

اما در روش دوم که مبتنی بر سیگنال سینوسی با یک فرکانس و تزریق فاز تصادفی است، مراحل تولید کلید به شرح زیر است:

۱. ابتدا آلیس سیگنال سینوسی زیر را برای باب ارسال می‌کند.

$$S(t)=\cos(2\pi f_1(t-t_0)+\Phi_1) \quad (۴)$$

در رابطهٔ بالا، f_1 فرکانس مورد نظر، t_0 زمان تأخیر انتشار ناشی از فاصلهٔ آلیس و باب و Φ_1 فاز اولیهٔ تصادفی در نظر گرفته‌شده توسط آلیس است که به صورت تصادفی انتخاب می‌شود.

۲. باب سیگنال زیر را دریافت می‌کند:

$$r(t)=\alpha_1(t)\cos(2\pi f_1 t+\Phi_1+\Theta_0) \quad (۵)$$

که در آن $\alpha_1(t)$ ضریب تضعیف و Θ_0 فاز تصادفی اضافه‌شده توسط کانال است که نتیجهٔ یک متغیر تصادفی یکنواخت می‌باشد.

۳. در ادامه، باب نیز سیگنال سینوسی زیر را برای آلیس ارسال می‌کند که در آن Φ_2 فاز اولیهٔ تصادفی در نظر گرفته‌شده توسط باب است.

$$S(t)=\cos\left(2\pi f_1(t-t_0)+\Phi_2\right) \qquad (۶)$$

و آلیس نیز سیگنال زیر را دریافت می‌کند:

$$r(t)=\alpha_1(t)\cos\left(2\pi f_1 t+\Phi_2+\Theta_0\right) \qquad (۷)$$

که با توجه به اینکه این فرآیند در زمان همدوسی کانال اجرا می‌شود، فاز کانال ثابت باقی مانده است.

۴. در نهایت، آلیس و باب هر یک فاز سیگنال دریافتی خود را با فاز اولیهٔ ارسالی‌شان جمع‌کرده و هر دو به مقدار یکسان زیر می‌رسند:

$$\Theta_t=\left(\Phi_1+\Phi_2+\Theta_0\right) \qquad (۸)$$

که مشابه روش اول، با محاسبهٔ $\Theta_t \mod 2\pi$ و کوانتیزاسیون آن، رشته بیت تصادفی یکسان در دو طرف قابل استخراج است.

توجه شود که تعمیم هر کدام از الگوریتم‌های فوق، برای ارتباطات گروهی قابل پیاده‌سازی خواهد بود [۱۹].

روش دوم نسبت به روش اول دارای یک مزیت اساسی است: با توجه به تولید فازهای تصادفی در آلیس و باب و سپس ارسال آن‌ها، با تغییر این فازهای اولیه، امکان اجرای مکرر الگوریتم در یک دورهٔ همدوسی وجود دارد. بنابراین در لینک‌های پهباد که ممکن است کانال ایستا باشد نیز نرخ تولید کلید محدود نخواهد بود. در ادامه با ارائه شبیه‌سازی‌هایی به بررسی دقیق‌تر این روش و تأثیر پارامترهای مختلف بر روی آن می‌پردازیم.

۳. بررسی تولید کلید از فاز اولیهٔ تصادفی یک سیگنال سینوسی

در این بخش با تمرکز بر روش به‌کارگیری یک سیگنال سینوسی با فاز تصادفی، با ارائه شبیه‌سازی‌ها، تأثیر پارامترهای مختلف را بر این راهکار بررسی خواهیم کرد. همچنین با مقایسهٔ روش تولید کلید مذکور با روش قدیمی (تولید کلید با استفاده از اختلاف فاز دو سیگنال سینوسی ارسالی)، کارآمدی طرح مورد نظر را در برابر حملات فعال مشخص می‌کنیم. در نهایت، برای نمونهٔ عملی تزریق فاز گسسته، طرح تولید کلید را از منظر نواحی افشای کلید بررسی می‌کنیم.

۳-۱- مفروضات شبیه‌سازی:

در شبیه‌سازی‌ها برای پیچیده‌تر کردن شرایط محیطی، کانال را محوشدگی باند باریک با مدل رایلی در نظر می گیریم، مگر اینکه خلاف آن ذکر گردد. از طرفی، همان‌طور که در مخابرات دیجیتال ضرورت دارد، سیگنال تک‌فرکانس پس از ارسال، با فرکانسی بزرگتر از دو برابر فرکانس آن، نمونه‌برداری شده و سپس از روی آن مشخصه‌های سیگنال اولیه تخمین زده می‌شود.

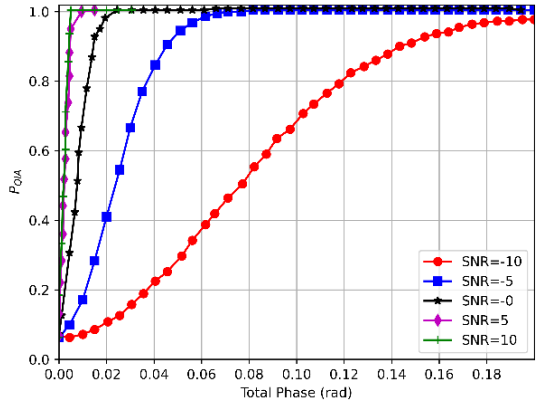
از این رو، برای مشاهدهٔ تأثیر خطای تخمین‌گر ML بر روی فاز استخراجی، از کران پایین Cramer-Rao استفاده می‌شود که برای مقادیر نسبتاً بالای SNR، مقادیر استخراجی از تخمین‌گرهای ML با این حد همخوانی بسیار خوبی دارد [۲۱] . بر این اساس، مقدار واریانس فاز برای سیگنال $b_0\cos(\omega t+\theta)$، به‌صورت ذیل استخراج می‌شود [۲۱]:

$$var\left\{\hat{\theta}\right\}\geq\begin{cases}\dfrac{\sigma^2}{b_0{}^2N}\\[2ex]\dfrac{12\sigma^2\left(n_0{}^2N+2n_0P+Q\right)}{b_0{}^2N^2\left(N^2-1\right)}\end{cases}\qquad(۹)$$

حالت نخست که در اینجا نیز صادق است، برای زمانی است که فرکانس سیگنال در گیرنده مشخص باشد و مورد دوم برای حالتی است که فرکانس نامعلوم باشد. همچنین در کلیه شبیه‌سازی‌ها پارامتر کوانتیزاسیون $Q=16$ فرض شده است.

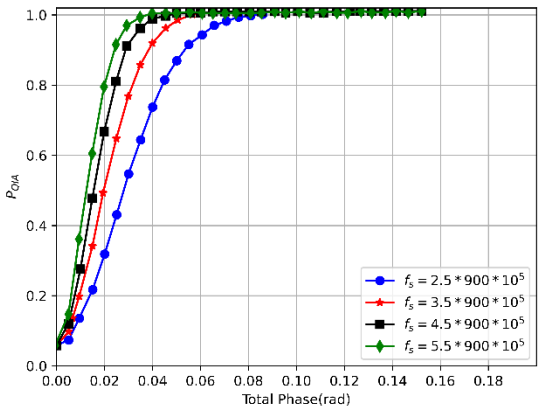
۳-۲- تأثیر SNR و فرکانس نمونه‌برداری

در ابتدا احتمال یکسانی ناحیه کوانتیزاسیون[۲۵] ($P_{QIA}(\phi)$) و توافق در رشته بیت تولیدی میان آلیس و باب به ازای SNRهای مختلف و برای مقادیر ذیل بررسی شده است؛ فرکانس سیگنال سینوسی $f_c=90\ MHz$، طول دورهٔ نمونه‌برداری $T_0=10^{-6}$ ثانیه، فرکانس نمونه‌برداری $f_s=270\ MHz$ و تعداد نمونه‌ها برابر با $N=T_0f_s$ می‌باشد. محور افقی در شکل ۳ نمایانگر فاز اولیهٔ انتخابی می‌باشد که با توجه به تقارن موجود، برای نیمی از یک ناحیه کوانتیزاسیون (π/Q) در نظر گرفته شده است.



شکل ۳. احتمال توافق کلید برای SNRهای مختلف

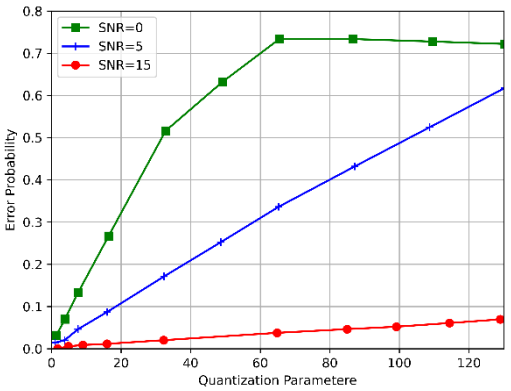
موضوع دیگر که لازم است مورد توجه قرار گیرد این است که انتظار می‌رود با افزایش تعداد نمونه‌ها، امکان صحت تبادل کلید حتی در SNRهای پایین‌تر نیز افزایش یابد. از این رو، بررسی تأثیر زمان یا فرکانس نمونه‌برداری و در نتیجه تعداد نمونه‌ها، مورد مهم دیگری است که می‌توان بررسی نمود. همان‌طور که در شکل ۴ مشاهده می‌شود نتایج شبیه‌سازی نیز مطابق انتظار می‌باشد. شکل ۴ احتمال توافق کلید را برای فرکانس‌های نمونه‌برداری متفاوت، به ازای $T_0=10^{-7}$ و $\mathrm{SNR}=5\ \mathrm{dB}$ نشان می‌دهد. البته مقادیر فرکانس به‌گونه‌ای انتخاب شده‌اند که حد نایکوئیست رعایت شود.



شکل ٤. احتمال توافق کلید میان آلیس و باب برای فرکانس‌های مختلف نمونه‌برداری

۳-۳- بررسی تأثیر پارامتر کوانتیزاسیون

یکی از موضوعات مهم در تولید کلید از فاز کانال، پارامتر کوانتیزاسیون فاز برای تولید کلید است. واضح است که هر چه این پارامتر (که به‌صورت توانی از ۲ است) بزرگتر باشد، تعداد بیت‌های قابل استخراج در هر دور تولید کلید و در نتیجه نرخ تولید کلید افزایش می‌یابد؛ اما از سوی دیگر، تأثیر خطا بر آن نیز بیشتر شده و در نتیجه احتمال عدم توافق کلید افزایش می‌یابد.



شکل ۵. نمودار خطا بر حسب پارامتر کوانتیزاسیون (Q) برای SNRهای مختلف

در شکل ۵، نمودار خطا بر حسب پارامتر کوانتیزاسیون (Q) و برای SNRهای مختلف رسم شده است. در این نمودار، فرکانس سیگنال سینوسی $f_c = 90\ MHz$، طول دوره نمونه‌برداری $T_0 = 10^{-7}$ ثانیه و فرکانس نمونه‌برداری $f_s = 270\ MHz$ می‌باشد. همان طوری‌که در این شکل مشخص است، با افزایش SNR، احتمال خطا کاهش قابل ملاحظه‌ای دارد.

۴. بررسی اجرای حملات فعال بر راهکارهای تولید کلید مبتنی بر فاز

در این بخش، به بررسی دو حملهٔ فعال اصلی بر روی راهکار تولید کلید از کانال می‌پردازیم. در حمله نخست، یعنی حملهٔ مرد در میان، مهاجم قصد دارد تا در روند تولید کلید وارد شده و تأثیر بگذارد. همان‌طور که خواهیم دید، یکی از مزایای مهم راهکار تولید کلید از فاز نسبت به راهکار تولید کلید از توان، مقاومت آن در برابر این نوع حملات است. حمله دوم که در اینجا مورد تأکید است، حالتی است که مهاجم صرفاً با ارسال پارازیت می‌خواهد تولید کلید یکسان در دو سوی ارتباط را خراب کند. این حمله به طور دقیق‌تر می‌شود.

۴-۱- حمله به منظور ورود به فرآیند تولید کلید

علی‌رغم امکان اجرای این حمله بر روش تولید کلید مبتنی بر توان [۲۲]، روش تولید کلید مبتنی بر فاز در مقابل این حمله مقاوم است. علت اصلی این مزیت، به تفاوت این راهکار با روش مبتنی بر توان بر می‌گردد. در راهکار مبتنی بر توان، دو طرف با ارسال سیگنال‌های کاوش این زمینه را به وجود می‌آورند تا ابتدا کانال را شناسایی کنند، مساله‌ای که می‌تواند منجر به شناسایی کانال توسط مهاجم نیز شود. اما در روش مبتنی بر فاز، فاز کانال می‌تواند حتی برای دو گره قانونی ارتباط نیز کاملاً ناشناخته باقی بماند و ضرورتی به آشکار شدن آن در فرآیند تولید کلید وجود ندارد. این یک نقطه قوت برای روش تولید کلید از فاز به حساب می‌آید که شاید برتر از سه نقطه قوت دیگر باشد که پیش‌تر مورد بررسی قرار گرفت. برای بررسی جزئیات اعمال

این حمله بر روش مبتنی بر توان می‌توان به [۲۲] مراجعه نمود.

بنابراین می‌توان گفت روش تولید کلید از فاز، در مقابل دخالت فعال مهاجم به منظور ورود به فرآیند تولید کلید مقاوم است.

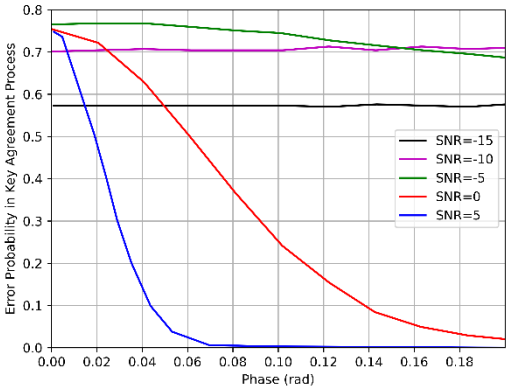
۴-۲- حمله به منظور ایجاد اخلال در فرآیند تولید کلید

دسته‌ای دیگر از حملات فعال که در تولید کلید مبتنی بر کانال می‌توان متصور شد، ارسال یک سیگنال از سوی مهاجم به منظور تخریب فرآیند تبادل کلید است (تزریق سیگنال پارازیت) [۱۵]. این روش زمانی مورد استفاده قرار می‌گیرد که امکانی برای نفوذ در فرآیند وجود ندارد و حداقل به این طریق می‌توان در ارتباط دو گرهٔ قانونی و تولید کلید میان آن دو اخلال ایجاد کرده و یا با ملزم‌کردن آن‌ها به تکرار فرآیند، هزینهٔ تولید کلید را برای آن‌ها بالا برد. البته از آنجایی‌که به‌کارگیری این نوع حمله در غالب روش‌های ارتباطی می‌تواند مؤثر باشد، روش چندان بهینه و مناسبی نیست و بنابراین قابلیت اعمال آن بر روش تولید کلید از فاز نیز چندان دور از ذهن نمی‌باشد. برای رفع این معضل، از طرح پیشنهادی در مرجع [۱۵] می‌توان بهره برد.

در ادامه و با فرض اینکه مهاجم با هدف طبیعی جلوه دادن حمله، سیگنالی با مقدار تصادفی را برای گره‌های قانونی ارسال می‌کند تا در آن‌ها صرفاً به تقویت اثر نویز بیانجامد، دو حالت را می‌توان در نظر گرفت: حالت اول زمانی است که در هر دورهٔ همدوسی کانال تنها یک دور تولید کلید میان گره‌های قانونی رخ دهد. در این حالت، از آنجایی که اندازه کانال مهاجم با آلیس (h_{MA}) و باب (h_{MB}) به صورت یک متغیر تصادفی گوسی است، کافی است مهاجم در هر دوره یک پالس ثابت ارسال کند و نهایتاً این پالس در گره‌های قانونی به صورت نویز گوسی ظاهر می‌شود. اما در حالتی‌که در هر دورهٔ همدوسی کانال، چند دوره فرآیند تولید کلید انجام شود، برای اطمینان از تأثیر حمله در گره‌های قانونی، باید یک سیگنال تصادفی (در اینجا گوسی) توسط مهاجم ارسال شود تا ثبات کانال در زمان همدوسی منجر به افزوده شدن یک مقدار ثابت و نهایتاً حذف احتمالی آن توسط گره‌های قانونی نگردد. توجه شود که پالس باید در فرکانس مورد نظر ارسال شود. در اینجا و با توجه به تک‌فرکانس بودن سیگنال اصلی، در حقیقت دامنهٔ یک سیگنال سینوسی مدنظر است.

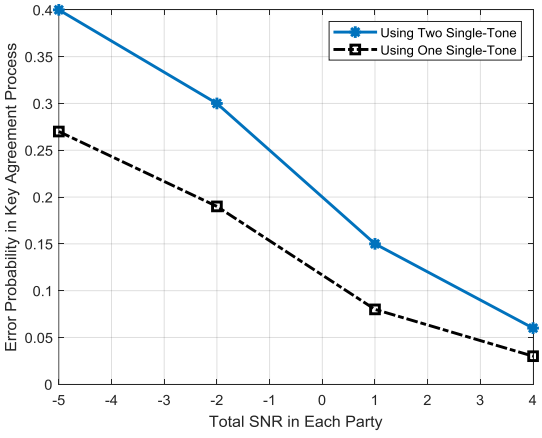
در ادامه و با این فرض که با رعایت موارد فوق، نهایتاً سیگنال دریافتی در گره‌های قانونی، به صورت یک نویز گوسی عمل کند، نمودار چگونگی تأثیر این حمله به ازای توان‌های مختلف ارسالی توسط مهاجم آمده است. در نمودارهای شکل ۶، فرکانس سیگنال سینوسی $f_c = 90\ MHz$، طول دورهٔ نمونه‌برداری $T_0 = 10^{-7}$ ثانیه، فرکانس نمونه‌برداری $f_s = 270\ MHz$ و پارامتر کوانتیزاسیون $Q = 16$ در نظر گرفته شده است.

البته باید توجه داشت (همان‌طور که پیش‌تر نیز اشاره شد) در SNRهای خیلی پایین عملاً استفاده از حد CRB برای تعیین خطای فاز دقت پائینی دارد.



شکل ۶. تأثیر حمله پارازیت برای توان‌های متفاوت مهاجم و در SNRهای مختلف

یکی از موارد مهم دیگر که می‌توان بررسی نمود، سنجش میزان مقاومت دو روش ذکر شده در بخش ۲-۳ در برابر سیگنال تخریبی اخلال‌گر است؛ یعنی روش قدیمی (کاوش توسط یک سیگنال سینوسی با دو فرکانس) و روش جدید (کاوش توسط یک سیگنال سینوسی تک‌فرکانس با فاز تصادفی) که در این مقاله از آن بهره بردیم. در شکل ۷، احتمال خطای این دو روش برحسب SNR مقایسه شده است. پارامترهای شبیه‌سازی همان پارامترهای به‌کارگرفته شده در شکل ۶ است. همان‌طور که مشاهده می‌شود روش جدید در شرایط بد SNR و همچنین نیز در حضور حملهٔ پارازیت از مقاومت بیشتری برخوردار است.



شکل ۷. مقایسه میزان مقاومت در برابر اخلال‌گر برای روش‌های مبتنی بر یک سینوسی و دو سینوسی

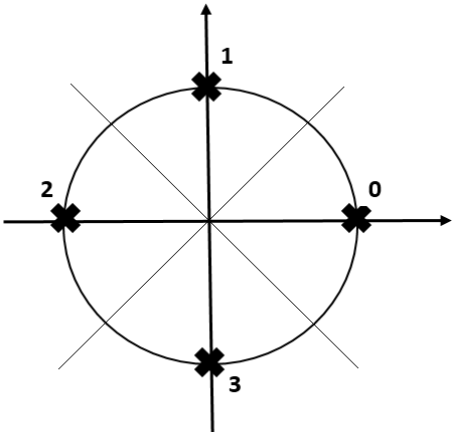
۵. بررسی محرمانگی هندسی[۲۶] برای طرح تولید کلید مبتنی بر تزریق فاز تصادفی گسسته

در این بخش، امنیت طرح تولید کلید فاز گسسته را با رویکرد محرمانگی هندسی مورد بررسی قرار می‌دهیم. همچنین برای بهبود امنیت این طرح پیشنهادی، ایدهٔ پویاسازی فرکانسی ارائه می‌گردد.

در اینجا، آلیس و باب سمبل‌ها با فاز تصادفی گسسته را از فضای منظومه M-PSK انتخاب و به طور متقابل برای یکدیگر ارسال می‌کنند. برای $u \in \{1,2\}$، فاز سمبل ارسالی توسط کاربر u عبارت است از:

$$\phi_u = \frac{2\pi}{M} i_u \qquad (۱۰)$$

که اندیس $i_u \in \{0, \dots, M-1\}$ به‌صورت تصادفی توسط گره‌ها انتخاب می‌شود. پیشنهاد ما این است که کاربران در وضعیت گیرندگی، از برچسب‌گذاری ترتیبی برای آشکارسازی فاز دریافتی‌شان بهره ببرند. به‌عنوان مثال، برای $M = 4$، مطابق شکل ۸، سمبل‌ها به ترتیب با اعداد ۰، ۱، ۲ و ۳ برچسب گذاری می‌شوند.



شکل ۸. برچسب‌گذاری ترتیبی برای منظومه 4-PSK. خطوط مورب، مرز نواحی تصمیم هستند.

برای تولید کلید، هر یک از گره‌ها، فاز سیگنال دریافتی از کاربر مقابل را آشکار کرده و با اندیس تصادفی متناظر با سمبل ارسالی خود، در پیمانهٔ M جمع می‌کند. در نتیجه آلیس و باب به ترتیب مقادیر زیر را به عنوان کلید، به‌دست می‌آورند:

$$K_1 \overset{M}{=} Q(\phi_2 + \Theta_0) + i_1$$
$$K_2 \overset{M}{=} Q(\phi_1 + \Theta_0) + i_2 \qquad (۱۱)$$

در رابطهٔ بالا، تابع $Q(.)$ بیانگر عملیات کوانتیزاسیون است که با $Q(x) = \left\lfloor \frac{x}{2\pi/M} + \frac{1}{2} \right\rfloor$ قابل بیان است. با قرار دادن $\phi_0 = \frac{2\pi d_{12}}{\lambda}$ و نیز رابطهٔ (۱۰) در رابطهٔ (۱۱) (که d_{12} فاصلهٔ بین آلیس و باب و λ طول موج سیگنال کاوش کانال است)، به نتیجهٔ زیر می‌رسیم:

$$K_1 \overset{M}{=} \left\lfloor \frac{\frac{2\pi}{M} i_2 + \Theta_0}{\frac{2\pi}{M}} + \frac{1}{2} \right\rfloor + i_1$$
$$= i_1 + i_2 + \left\lfloor \frac{M d_{12}}{\lambda} + \frac{1}{2} \right\rfloor \qquad (۱۲)$$

از نگاه شنودگر، در مرحله تبادل سیگنال‌های کاوش، شنودگر دو سیگنال با فازهای $\phi_1 + \phi_{1E}$ و $\phi_2 + \phi_{2E}$ دریافت می‌کند که ϕ_{1E} و ϕ_{2E} به ترتیب بیانگر فاز ناشی از کانال آلیس-شنودگر و کانال باب-شنودگر هستند. با فرض آنکه شنودگر از طرح SKG به طور کامل آگاهی دارد، تلاش می‌کند تا یک کپی از کلید را به‌دست آورد. بدین منظور، شنودگر نیز مشابه آلیس و باب با ترکیب مشاهداتش از دو کانال شنود، تخمینی از کلید مشترک آلیس و باب را به‌دست می‌آورد. با این توضیحات، بهترین پردازش برای شنودگر این است که فاز سیگنال‌های دریافتی از آلیس و باب را به طور جداگانه کوانتیزه کرده و سپس مقادیر به‌دست آمده را در پیمانه M با هم جمع کند. به عبارتی:

$$K_E \overset{M}{=} Q(\phi_1 + \phi_{1E}) + Q(\phi_2 + \phi_{2E}) \qquad (۱۳)$$

همچنین اگر فاصلهٔ شنودگر تا آلیس و باب به ترتیب برابر با d_{1E} و d_{2E} باشد، رابطهٔ (۱۳) به صورت زیر قابل بازنویسی است:

$$K_E \overset{M}{=} \left\lfloor \frac{\frac{2\pi}{M} i_1 + \frac{2\pi d_{1E}}{\lambda}}{\frac{2\pi}{M}} + \frac{1}{2} \right\rfloor + \left\lfloor \frac{\frac{2\pi}{M} i_2 + \frac{2\pi d_{2E}}{\lambda}}{\frac{2\pi}{M}} + \frac{1}{2} \right\rfloor$$
$$= i_1 + i_2 + \left\lfloor \frac{M d_{1E}}{\lambda} + \frac{1}{2} \right\rfloor + \left\lfloor \frac{M d_{2E}}{\lambda} + \frac{1}{2} \right\rfloor \qquad (۱۴)$$

تعریف (نواحی افشای کلید): صحت کلید شنودگر، منوط به برقراری رابطهٔ زیر است:

$$K_E \overset{M}{=} K_1 \qquad (۱۵)$$

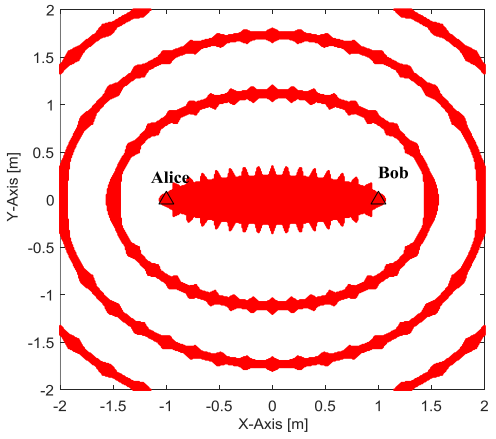
به‌عبارت دیگر، در هر مکانی که رابطهٔ (۱۵) برقرار باشد، شنودگر می‌تواند کلید مشترک آلیس و باب را به درستی بدست آورد. مکان هندسی این نقاط را اصطلاحاً *نواحی افشای کلید* می‌نامیم. در اینجا، با فرض ایستا بودن کانال و نیز برای فضای آزاد (برای ارتباطات پهبادها)، این نواحی را به‌دست می‌آوریم.

با جایگذاری روابط (۱۲) و (۱۴) در رابطهٔ (۱۵) و نیز اعمال عملیات پیمانه M، نواحی افشای کلید از تساوی زیر بدست خواهد آمد:

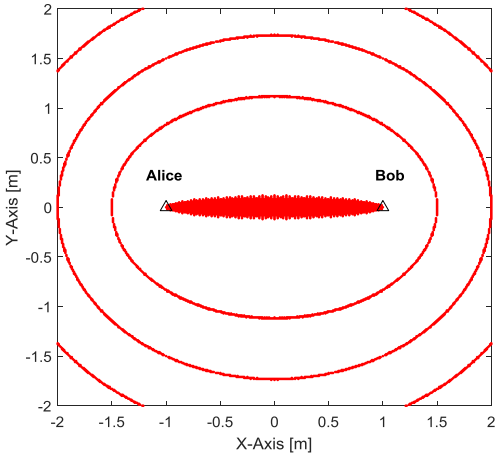
$$\left\lfloor \frac{M d_{12}}{\lambda} \right\rfloor + nM = \left\lfloor \frac{M d_{1E}}{\lambda} + \frac{1}{2} \right\rfloor + \left\lfloor \frac{M d_{2E}}{\lambda} + \frac{1}{2} \right\rfloor \qquad (۱۶)$$

در رابطه بالا، $n \in \{0,1,2,3,\dots\}$ است. برای وضعیتی که آلیس و باب در مکان (-1,0) و (+1,0) قرار گرفته‌اند، نواحی افشای کلید برای طرح فاز گسسته به ترتیب در شکل‌های ۹ و ۱۰ با رنگ قرمز نشان داده شده است. فرکانس کاوش کانال $f = 300\ MHz$ و مرتبه مدولاسیون به ترتیب $M = 8$ و $M = 64$ در نظر گرفته شده است.

توجه شود که در شکل‌های ارائه شده، بخش‌هایی که با رنگ سفید نشان داده شده‌اند، نواحی محرمانه هستند. نتایج شبیه‌سازی نشان می‌دهد که به ازاء $M = 8$ و $M = 64$ نواحی افشای کلید به ترتیب حدود 18.7% و 3.6% از کل فضا بوده و سایر نقاط فضا، نواحی محرمانه می‌باشند. از مقایسه این دو، نتیجه می‌گیریم که با افزایش مرتبه مدولاسیون درصد نواحی محرمانه افزایش می‌یابد. همچنین مشخص است که با افزایش M، ضخامت نواحی افشای کلید و به‌خصوص مساحت ناحیهٔ افشای کلید حول خط دید مستقیم، به میزان قابل توجهی کاهش پیدا می‌کند. در این وضعیت، کار شنودگر جهت استقرار در ناحیه افشای کلید دشوارتر می‌گردد.



شکل ۹. نواحی افشای کلید به ازاء $M = 8$ و فرکانس‌کاری $f = 300\ MHz$.

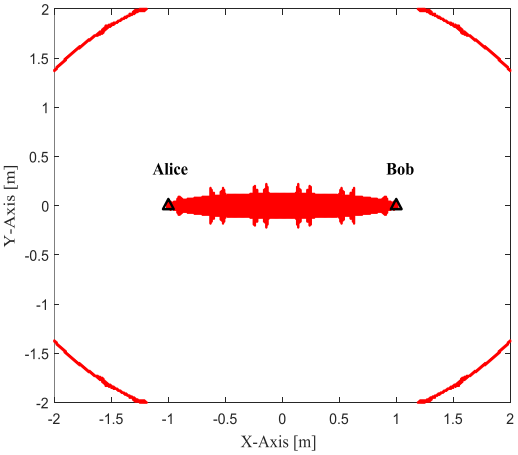


شکل ۱۰. نواحی افشای کلید به ازاء $M = 64$ و فرکانس‌کاری $f = 300\ MHz$.

با توجه به رابطهٔ (۱۶) پارامتر طول موج بر نواحی افشای کلید تأثیرگذار است. لذا هندسه‌ی نواحی محرمانه و نواحی افشای کلید با تغییر فرکانس سیگنال کاوش، قابل تغییر است. بر این اساس، پیشنهاد می‌شود که 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. به عبارت دیگر، هر سیگنال کاوش بر روی یک فرکانس از مجموعه فرکانسی $\mathbb{F}$ ارسال گردد و این الگوی فرکانسی کاوش کانال، در دسترس همگان است.

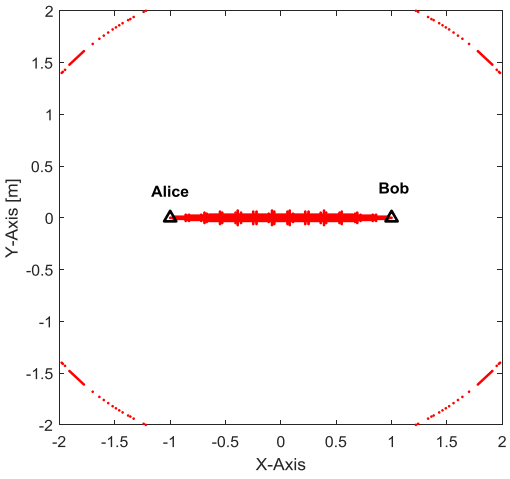
بر پایهٔ این ایده، اگر شنودگر بخواهد کل دنبالهٔ کلید را به‌دست آورد باید در مکانی مستقر شود که این مکان به ازاء تمام فرکانس‌های موجود در مجموعه $\mathbb{F}$، جزو نواحی افشای کلید باشد. بنابراین، به طور شهودی می‌توان گفت که میزان نواحی افشای کلید در صورت استفاده از چندین فرکانس نسبت به حالت تک فرکانس کمتر است. برای مثال، برای $M = 8$ و فرکانس‌های کاوش $f = 100, 200, 300, 400, 500\ MHz$،

نواحی افشای کلید در شکل ۱۱ ترسیم شده است. همان‌طوری‌که مشخص است در مقایسه با شکل ۹ (استفاده از یک فرکانس برای کاوش کانال)، نواحی افشای کلید به مراتب کمتر است؛ به طوری‌که در این حالت، نواحی افشای کلید حدود 3% از کل فضا است. همچنین در شکل ۱۲ برای دنبالهٔ فرکانسی مذکور و به ازاء $M = 64$، نواحی افشای کلید ترسیم شده است. در این حالت، حدود 0.8% از کل فضا، نواحی افشای کلید است که در مقایسه با حالت تک فرکانس، تقریباً $\frac{1}{4}$ برابر شده است.



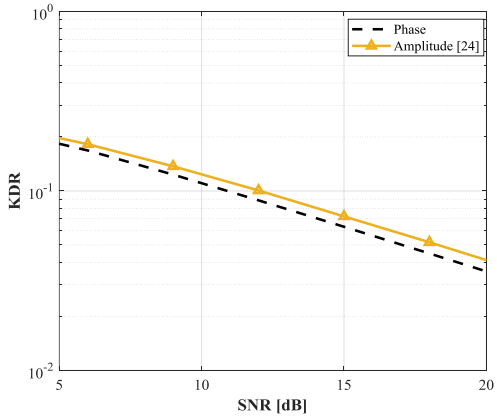
شکل ۱۱. نواحی افشای کلید برای تعداد سطوح کوانتیزاسیون $\boldsymbol{M = 8}$ و فرکانس‌های کاوش $\boldsymbol{f = 100, 200, 300, 400, 500\ MHz}$.

نتایج شبیه‌سازی‌ها در شکل‌های ۱۱ و ۱۲ نشان می‌دهد که وقتی در مرحله کاوش کانال به جای یک فرکانس، از چند فرکانس استفاده شود، نواحی افشای کلید به مقدار قابل ملاحظه‌ای کاهش می‌یابد.



شکل ۱۲. نواحی افشای کلید برای تعداد سطوح کوانتیزاسیون $\boldsymbol{M = 64}$ و فرکانس‌های کاوش $\boldsymbol{f = 100, 200, 300, 400, 500\ MHz}$

برای مشاهدهٔ اهمیت تولید کلید فاز گسسته، نرخ عدم تطابق کلید[۲۷] (KDR) آن را با تولید کلید مبتنی بر دامنه مقایسه می‌کنیم. برای سادگی، در گیرنده، از الگوریتم متداول کوانتیزاسیون تک بیتی [۲۳] و [۲۴] استفاده می‌کنیم. لذا آلیس و باب از BPSK برای ارسال فازهای تصادفی گسسته خود بهره می‌برند. توجه شود که عدم تطبیق قطعه کلید $K_1 \neq K_2$، وقتی رخ می‌دهد که $(K_1 = 0, K_2 = 1)$ یا $(K_1 = 1, K_2 = 0)$ باشد. در شکل ۱۳، طرح پیشنهادی در این مقاله (که مبتنی بر فاز کانال است) را با طرح پیشنهادی در مرجع [۲۴] (که مبتنی بر دامنهٔ سمبل‌های کاوش است) مقایسه می‌کنیم. همان‌طوری‌که در این شکل مشخص است، طرح پیشنهادی فاز گسسته در مقایسه با طرح مرجع [۲۴]، به ازای یک KDR ثابت، حدود 1 dB در SNR کاوش کانال صرفه‌جویی می‌کند.



شکل ۱۳. نرخ عدم تطابق کلید برحسب SNR کاوش کانال.

۶. جمع‌بندی و کارهای آینده

این مقاله، بر روی تولید کلید مبتنی فاز کانال برای ارتباطات پهبادها متمرکز شده است. ضمن معرفی دو روش در این حوزه، روش تولید کلید مبتنی بر یک سیگنال تک‌فرکانس با فاز ابتدایی تصادفی ارزیابی گردید. به‌طور خاص، تأثیر SNR و پارامتر کوانتیزاسیون در عملکرد این روش مورد بررسی قرار گرفت. همچنین اثر حملات فعال مورد تحلیل و بررسی قرار گرفت. همان‌طور که مشاهده شد، روش تزریق فاز تصادفی اولیه نسبت به روش‌های مبتنی بر توان در مقابل حملات فعال، مقاوم‌تر هستند. همچنین به مطالعهٔ حالت خاص و عملی تزریق فاز تصادفی گسسته و نواحی افشای کلید برای آن پرداخته شده است. مشاهده شد که طرح پیشنهادی کاوش کانال بر روی چند فرکانس، درصد نواحی افشای کلید را کاهش می‌دهد.

از جمله مواردی که می‌توان در آینده مطالعه کرد، تولید کلید مبتنی بر فاز در سناریوی مبتنی بر رله است. سپس، نرخ تولید کلید و احتمال موفقیت تولید کلید را برای آن ارزیابی نمود. همچنین پیشنهاد می‌شود طرح تولید کلید مبتنی بر فاز گسسته بر سناریوی تولید گروهی پهبادها مورد تحلیل و ارزیابی قرار گیرد.

توجه شود اگر کانال هم‌پاسخ نباشد پروتکل تولید کلید شکست خواهد خورد. در واقع یک اصل اساسی در SKG این است که کانال‌ها هم‌پاسخ باشند. البته اگر کانال‌ها هم‌پاسخی ضعیف داشته باشند، به جای هم‌پاسخی کامل، در این صورت روش‌هایی مانند در نظر گرفتن ناحیه محافظ و نیز به‌کارگیری کدینگ‌های مناسب مانند کد توربو به عنوان راهکارهای بسیار توانمند در مراجع [۲۴] و [۲۵] معرفی شده‌اند. همچنین در مرجع اخیر [۲۳] به‌کارگیری یادگیری عمیق توانسته است هم‌پاسخی ضعیف را جبران کند و نرخ عدم تطابق کلید (KDR) را کاهش دهد.

۷. 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, 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, 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, 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, 2018.

[5]. X. Sun, D. W. K. Ng, Z. Ding, Y. Xu, and Z. Zhong, Physical layer security in UAV systems: Challenges and opportunities,

Internet of Things in the presence of a hostile jammer, IEEE Internet of Things Journal, Vol. 8, No. 6, pp. 4373-4388, 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, in 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, 1996.

[21] D. Rife and R. Boorstyn, Single-tone parameter estimation from discrete-time observations, IEEE Trans. Inf. Theory, Vol. 20, No. 5, pp. 591–598, 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, 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 Conference on Communications Workshops (ICC Workshops), Shanghai, China, 2019, pp. 1-6.

[25] G. Epiphaniou, P. Karadimas, D. Kbaier Ben Ismail, H. Al-Khateeb, A. Dehghantanha and K. -K. R. Choo, Nonreciprocity Compensation Combined With Turbo Codes for Secret Key Generation in Vehicular Ad Hoc Social IoT Networks, IEEE Internet of Things Journal, Vol. 5, No. 4, pp. 2496-2505, 2018.

IEEE Wireless Commun., Vol. 26, No. 5, pp. 40–47, 2019.

[5] J. Bosbach, J. Pennecot, C. Wagner, M. Raffel, T.H. Lerche and S.T. Repp, Experimental and Numerical Simulations of Turbulent Ventilation in Aircraft Cabins, Energy, Vol. 31. No. 5, pp. 694-705, 2006.

[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, 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, 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, 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, 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

۸. پی‌نوشت

[i]. Unmanned air vehicle
[ii]. Line-of-Sight
[iii]. Man-in-The-Middle
[iv]. Jamming
[v]. Key disclosure region
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. Half-duplex
19. Coherence time
20. Reciprocal
21. ML: Maximum Likelihood
22. Reconciliation
23. Hash
24. Privacy amplification
25. QIA: Quantization Index Agreement
26. Geometric secrecy
27. KDR: Key Disagreement Rate