ارائه یک طرح لایه فیزیکی جهت تولید کلید مخفی مبتنی بر تزریق فاز تصادفی گسسته

امیرحسین خلیلی تیرانداز[1] **علی کوهستانی[2]**

۱- استادیار- دانشکده مهندسی برق و کامپیوتر- دانشگاه صنعتی قم - قم- ایران
khalili@qut.ac.ir

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

چکیده: در ارتباطات نقطه به نقطهٔ ایستا، تولید کلید مخفی با دو چالش مهم مواجه است: نرخ پایین تولید کلید و وجود نواحی افشای کلید. برای رفع چالش اول می‌توان از طرح‌های مبتنی بر مولدهای تصادفی محلی استفاده کرد. یکی از این طرح‌ها، طرح تزریق فاز تصادفی است که در آن سیگنال‌های کاوش کانال با فاز تصادفی بین طرفین ارتباط (آلیس و باب) مبادله می‌شود. در این مقاله، یک طرح تولید کلید نوین بر پایه‌ی ارسال سیگنال‌های کاوش کانال با فاز تصادفی "گسسته" ارائه می‌گردد. سپس ضمن تعریف نواحی افشای کلید، امنیت طرح پیشنهادی را با رویکرد محرمانگی هندسی مورد ارزیابی قرار می‌دهیم. نتایج شبیه‌سازی نشان می‌دهد که اگر در مرحله کاوش کانال به جای یک فرکانس، از چند فرکانس استفاده شود، نواحی محرمانه به میزان قابل ملاحظه‌ای افزایش می‌یابد. همچنین نشان داده می‌شود که ایده کاوش کانال بر روی چند فرکانس، آنتروپی کلید را افزایش می‌دهد. در انتهای مقاله، برخی از زمینه‌های تحقیقاتی جهت بررسی و افزایش امنیت طرح‌های تولید کلید ارائه می‌گردد.

.

واژه‌های کلیدی: تولید کلید مخفی، تزریق فاز تصادفی گسسته، محرمانگی هندسی و نواحی افشای کلید

نوع مقاله: پژوهشی

DOI: 10.61186/jiaeee.21.3.59

تاریخ ارسال مقاله: ۱۴۰۱/۰۵/۱۸

تاریخ پذیرش مشروط مقاله: ۱۴۰۳/۰۴/۰۶

تاریخ پذیرش مقاله: ۱۴۰۲/۰۶/۱۰

نام نویسنده‌ی مسئول: دکتر علی کوهستانی

نشانی نویسنده‌ی مسئول: ایران – قم - کیلومتر ۵ جاده تهران - دانشگاه صنعتی قم – دانشکده‌ی مهندسی برق و کامپیوتر

۱- مقدمه

با بهره‌برداری روزافزون از اینترنت اشیاء[۱] (IoT) [۱]، فناوری‌هایی از قبیل شبکه‌های حسگر بی‌سیم[۲] (WSN)، ارتباطات دستگاه به دستگاه[۳] (D2D)، ارتباطات بُرد کوتاه[۴] (SRC) [۲] نظیر تگ‌های RFID[۵] [۳] و استاندارد *ZigBee* توسعه و کاربرد بیشتری پیدا کرده‌اند. این فناوری‌ها با تشکیل یک جهان تماماً متصل، کیفیت زندگی را بهبود می‌دهد. در مدل IoT، تجهیزات مختلفی نظیر حسگرها و محرّک‌ها در مقیاس زیاد مورد استفاده قرار می‌گیرند که باید قابلیت اتصال بی‌سیم دو به دو را دارا باشند. این مهم، نیازمند یک بستر ارتباطی غیرمتمرکز و مقیاس‌پذیر است. در چنین بستری، حجم زیادی از اطلاعات خصوصی و محرمانه مبادله می‌شود که با توجه به ماهیت همه پخشی ارتباطات بی‌سیم، در معرض تهدیدات امنیتی مختلفی نظیر شنود و اختلال می‌باشند. در طراحی سیستم‌های مخابراتی امن، برای جلوگیری از شنود، غالباً از روش‌های رمزنگاری استفاده می‌شود. روش‌های رمزنگاری، مبتنی بر پیچیدگی محاسبات بوده و عموماً در لایه‌های بالای شبکه مورد استفاده قرار می‌گیرند. همچنین این روش‌ها بواسطهٔ نیاز به طرح‌های مدیریت کلید، برای استفاده در بسترهای نامتمرکز نظیر IoT با چالش عدم مقیاس‌پذیری مواجه‌اند.

در سال‌های اخیر، حوزهٔ جدیدی تحت عنوان امنیت لایه فیزیکی[۶] - یا به اختصار PLS - ارائه شده است [۴]-[۷]. در طرح‌های PLS، از ویژگی‌های کانال فیزیکی برای تأمین امنیت ارتباطات استفاده می‌شود و امنیت آنها نیز عمدتاً بر پایه‌ی نظریه اطلاعات است. پیچیدگی محاسباتی کم، توان مصرفی پایین، مقیاس‌پذیری و عدم نیاز به گره ثالث جهت مدیریت کلید (نامتمرکز بودن) از مزایای طرح‌های PLS در مقایسه با روش‌های رمزنگاری است. لذا این طرح‌ها گزینه‌های جذاب و مناسبی جهت بکارگیری در IoT می‌باشند. بطور کلی، طرح‌های PLS به سه دسته قابل تقسیم هستند: ۱) مخابره محرمانه در لایه فیزیکی[۷] (PLST) [۴]، ۲) تولید کلید مخفی لایه فیزیکی[۸] (SKG) [۵] و [۶] و ۳) احراز هویت لایه فیزیکی[۹] (PLA) [۷]؛ که در بین آنها، طرح‌های SKG نسبت به بقیه عملی‌تر هستند [۵]. در طرح‌های SKG، طرفین ارتباط بعد از تبادل سیگنال‌های راهنما[۱۰] و انجام پردازش‌های لازم، به یک کلید محرمانهٔ مشترک دست می‌یابند. سپس آلیس و باب می‌توانند از این کلید جهت رمزنگاری در لایه‌های مختلف شبکه استفاده کنند.

تجهیزات مورد استفاده در کاربردهای IoT معمولاً از نظر منابع پردازشی و توان مصرفی با محدودیت‌های زیادی مواجه‌اند که باعث می‌شود تا استفاده از طرح‌های PLS و به ویژه SKG مورد توجه قرار گیرد [۵]. جهت اجرای طرح‌های SKG به یک منبع آنتروپیِ هم‌پاسخ در کانال ارتباطی نیاز است؛ اما در برخی از سیستم‌های ارتباطی چنین منبعی وجود ندارد. به‌عنوان مثال، در سیستم‌های SRC به دلیل مخابره پیام در مسافت‌های کوتاه و یا ارتباطات موج میلیمتری، نسبت سیگنال به نویز[۱۱] (SNR) نسبتاً زیاد بوده و پدیده محوشدگی هم وجود ندارد. همچنین در ارتباطات دید مستقیم[۱۲] (LoS) بین ماهواره‌ها [۷] و یا ارتباطات پرنده‌های بدون سرنشین[۱۳] (UAV) [۸]، و به طور کلی در هر مخابره‌ای که کانال آن قابل مدل کردن با نویز سفید گوسی جمع شونده[۱۴] (AWGN) باشد، ایجاد منبع با آنتروپی بالا یک ضرورت است؛ چرا که طرح‌های متداول SKG که صرفاً مبتنی بر آنتروپی کانال هستند، کلید به اندازه کافی تصادفی تولید نمی‌کنند. توجه شود که از منظر امنیت، چالشی‌ترین سناریو در طرح‌های SKG، همین سناریوی اصطلاحاً ارتباطات فضای-آزاد[۱۵] است [۹] و [۱۰] که در آن، تمام لینک‌های ارتباطی - اعم از لینک‌های قانونی و لینک‌های شنود - از نوع LoS بوده و همگی بصورت AWGN مدل‌سازی می‌شوند[۱۶]. با توجه به این توضیحات، در این مقاله، سناریوی ارتباطاتی LoS در فضای آزاد مورد مطالعه قرار می‌گیرد.

در بین مشخصه‌های مختلف کانال‌های بی‌سیم، معمولاً از یکی از دو پارامتر زیر برای مقاصد تولید کلید استفاده می‌شود [۵] و [۶]:

- قدرت سیگنال دریافتی[۱۷] (RSS)
- اطلاعات حالت کانال[۱۸] (CSI)

مشخصهٔ RSS بیشتر مورد استفاده قرار می‌گیرد زیرا این پارامتر، در بسیاری از رادیوها به صورت پیش فرض اندازه‌گیری می‌شود و بدون هرگونه سربار اضافه، همواره موجود است [۵]. با این وجود، مشکل روش‌های مبتنی بر RSS این است که معمولاً نرخ تولید کلید پایینی دارند چون در هر بازهٔ همدوسی کانال ، فقط یک مقدار RSS اندازه‌گیری می‌شود. مشخصهٔ CSI نیز شامل پاسخ ضربه کانال[۱۹] (CIR) در حوزه زمان یا پاسخ فرکانسی کانال[۲۰] (CFR) در حوزه فرکانس است. در طرح‌های مبتنی بر CSI برخلاف طرح‌های مبتنی بر RSS چالش نرخ تولید کلید خیلی جدّی نیست. توجه شود که از CSI کانال، هم دامنه کانال و هم فاز کانال قابل استخراج است؛ لیکن در طرح‌های لایه فیزیکی برای تولید کلید، استفاده از فاز کانال در مقایسه با دامنهٔ 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 [۱۰]. 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 دامنهٔ کانال اینگونه نیست. در محیط‌های انتشاری مختلف مقدار دامنهٔ کانال بر حسب طول موج و فاصلهٔ فرستنده و گیرنده، قابل مدل‌سازی است [۵] درنتیجه مهاجم با دانستن فرکانس کاری و فاصله خودش تا گیرندهٔ قانونی می‌تواند از روی قدرت سیگنال دریافتی خودش، برآورد خوبی از دامنهٔ کانال قانونی بدست آورد. بنابراین برای

مهاجم، برآورد دامنهٔ 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 دامنهٔ 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، از آنجایی‌که در ارتباطات فضای آزاد، تلف مسیر به عنوان تنها مؤلفه کانال بی‌سیم مطرح است، روش‌های تولید کلید مخفی مبتنی بر RSS و دامنه CSI برای چنین شبکه‌های مخابراتی قابل استفاده نیست [۹]-[۱۱]. بر این اساس، در مرجع [۹] با توجه به تحرک فضاپیماها از شیفت فرکانس داپلر برای تولید کلید الهام گرفته شده است. در مراجع [۱۰]-[۱۳] با فرض ایستایی محیط و گره‌ها، راهکارهایی ارائه شده است. برخلاف مرجع [۱۲] که یکی از گره‌ها را مجهز به چند آنتن در نظر گرفته و یک طرح SKG متکی بر انتخاب آنتن پیشنهاد داده است، در مراجع [۱۰] و [۱۱] و [۱۳] برای یک سیستم ساده متکی بر گره‌های تک آنتن، از فاز کانال بی‌سیم برای پیاده‌سازی SKG بهره برده‌اند. به طور خاص در مرجع [۱۳]، با تکیه بر تئوری اطلاعات و نتایج عملی نشان داده شده است که هرگاه از سمبل‌های مدولاتور کلیدزنی فاز[۲۱] (PSK) برای کاوش کانال استفاده شود، میزان نشت اطلاعات به شنودگر صفر خواهد بود.

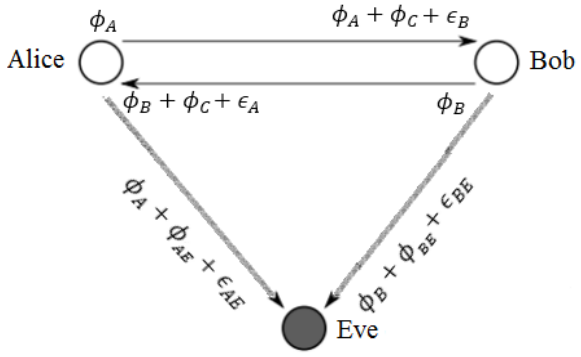
در مقاله حاضر نیز از فاز کانال بی‌سیم به عنوان مؤلفه مشترک جهت تولید کلید استفاده می‌شود. همچنین به منظور افزایش آنتروپی کلید، از تکنیک تزریق فاز تصادفی[۲۲] [۱۰] بهره می‌بریم. تفاوت کار ما در این مقاله با مراجع [۹]-[۱۲] در این است که فاز تصادفی تزریقی در طرح پیشنهادی، از جنس گسسته (مبتنی بر PSK) است. پر واضح است که فاز گسسته نسبت به فاز پیوسته عملیاتی‌تر و از منظر پیاده‌سازی نیز ساده‌تر است. همچنین تفاوت این مقاله با کار [۱۳] در این است که در این مقاله ضمن ارائه جامع یک طرح تولید کلید مبتنی بر فاز کانال، آن را از منظر محرمانگی هندسی[۲۳] در یک کانال مخابراتی ایستا[۲۴] مورد بررسی قرار می‌دهیم. بدین منظور، نواحی افشای کلید[۲۵] (مناطقی که شنودگران با استقرار در آن، شنود سیگنال‌های کاوش[۲۶] و اجرای پروتکل SKG، می‌توانند به کلید مشترک آلیس و باب دست یابد) را بصورت تحلیلی بدست آورده و سپس از طریق شبیه‌سازی نواحی محرمانه[۲۷] (مناطقی که شنودگران نمی‌توانند کلید مشترک آلیس و باب را به درستی بدست آورند) را نیز تعیین می‌کنیم. در شبیه‌سازی‌ها با مشاهده تأثیر طول موج سیگنال کاوش و تعداد سطوح کوانتیزاسیون، نتایج مفیدی ارائه شده است. همچنین در این مقاله، ایدهٔ اجرای روال کاوش کانال، روی چندین فرکانس حامل - به جای یک فرکانس - پیشنهاد شده است. هدف از این ایده، پویاسازی فاز کانالِ معادل است که منجر به افزایش قابل توجه آنتروپی کلید می‌گردد. نتایج این کار تحقیقاتی مؤید این واقعیت است که با اجرای روال کاوش بر روی چند کانال مختلف، درصد نواحی افشای کلید به شدت کاهش یافته و به خصوص محرمانگی نواحی اطراف لینک LoS به مقدار قابل ملاحظه‌ای افزایش می‌یابد. در انتهای مقاله، برخی موضوعات عملی و توسعه‌ای بیان شده است.

۲- طرح پیشنهادی

در این بخش مدل سیستم و سناریوهای شنود ارائه می‌گردد.

۲-۱- مدل سیستم

مطابق شکل ۱، مدل سیستم شامل یک جفت کاربر قانونی (آلیس و باب) و یک شنودگر (ایو) است که همگی یک آنتن دارند.

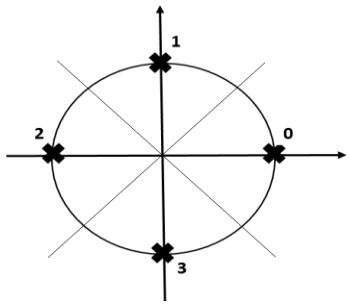


شکل (۱): مدل سیستم

فرض می‌شود کانال بین آلیس و باب هم‌پاسخ[۲۸] بوده و در طول تبادل سیگنال‌های کاوش، ثابت است. در اینجا، فاز کانال با ϕ_C معرفی می‌شود. آلیس و باب سمبل‌های دارای فاز تصادفی گسسته را از فضای منظومه[۲۹] M-PSK انتخاب و به طور متقابل برای یکدیگر ارسال می‌کنند. برای $u \in \{A, B\}$، فاز سمبل ارسالی توسط کاربر u عبارت است از:

$$\phi_u = \frac{2\pi}{M} i_u \qquad (۱)$$

که اندیس $i_u \in \{0, \dots, M-1\}$ به صورت تصادفی توسط کاربران انتخاب می‌شود. پیشنهاد ما این است که کاربران در وضعیت گیرندگی، از برچسب‌گذاری ترتیبی[۳۰] برای آشکارسازی فاز دریافتی‌شان بهره ببرند. به عنوان مثال، برای $M = 4$، مطابق شکل۲، سمبل‌ها به ترتیب با اعداد ۰، ۱، ۲ و ۳ برچسب گذاری می‌شوند. توجه شود که نیازی نیست تا کاربران، فاز کانال یا فاز تصادفی تزریقی گره مقابل را تخمین بزنند، بلکه فقط کافی است تا فاز دریافتی‌شان را تخمین بزنند.



شکل (۲): برچسب‌گذاری ترتیبی برای منظومه 4-PSK. (در این شکل، خطوط مورب، مرز نواحی تصمیم هستند)

پس از مرحله کاوش کانال، روال استخراج کلید به صورت زیر است: هر یک از کاربران، ابتدا فاز دریافتی[۳۱] 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 قطعه کلید مشترک، به‌دست می‌آورند:

$$\hat{k}_A \overset{M}{=} Q(\phi_B + \phi_C + \epsilon_A) + i_A \qquad (۲)$$

$$\hat{k}_B \overset{M}{=} Q(\phi_A + \phi_C + \epsilon_B) + i_B \qquad (۳)$$

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. همچنین نماد $\lfloor . \rfloor$ بیانگر عملگر جزء صحیح است. توجه شود که در دو رابطهٔ اخیر، پارامترهای ϵ_A و ϵ_B ناشی از عوامل مخربی همچون نویز و نقیصه‌های سخت‌افزاری است. از بین تمام نقیصه‌های سخت‌افزاری، عدم همزمان‌سازی بین آلیس و باب بیشترین تأثیر را بر روی فاز دارد. در عمل، کانال‌های آلیس و باب متأثر از آفست فاز (که خود ناشی از اسیلاتورهای محلی آلیس و باب است) می‌باشند. از آنجایی‌که همزمان‌سازی فاز، به صورت ایده‌آل محقق نمی‌شود، در هر بار کاوش کانال، یک آفست فاز تجربه می‌شود. همچنین، فرکانس تولید شده توسط اسیلاتورهای محلی بطور پیوسته حوالی فرکانس مرکزی نوسان نموده که نتیجتاً یک انحراف فاز وابسته به زمان را ایجاد می‌کند. برای کاهش چنین آفست فاز، روش‌های بسیار زیادی ارائه گردیده است [۱۳] و [۱۴].

حال می‌خواهیم نشان دهیم در شرایط ایده‌آل ($\epsilon_A = \epsilon_B = 0$) کلید آلیس و باب که در روابط (۲) و (۳) محاسبه شد، با هم برابرند. به‌عبارت دیگر، می‌خواهیم مطمئن شویم آلیس و باب به یک قطعه کلید مشترک خواهند رسید. با قرار دادن (۱) در (۲) و همچنین با توجه به اینکه $\phi_C = \frac{2\pi d_{AB}}{\lambda}$ (که d_{AB} فاصله بین آلیس و باب و λ طول موج سیگنال کاوش کانال است)، به نتیجه زیر می‌رسیم:

$$\hat{k}_A \overset{M}{=} \left\lfloor \frac{\frac{2\pi}{M} i_B + \phi_C}{\frac{2\pi}{M}} + \frac{1}{2} \right\rfloor + i_A = i_A + i_B + \left\lfloor \frac{M d_{AB}}{\lambda} + \frac{1}{2} \right\rfloor \qquad (۴)$$

اگر همین روند را برای $\hat{k}_B$ در (۳) بنویسیم، به نتیجهٔ یکسانی می‌رسیم. در نتیجه اثبات می‌شود که آلیس و باب، به یک قطعه کلید مشترک دست خواهند یافت. در ادامه، آلیس را به عنوان گره مرجع در نظر می‌گیریم و $\hat{k}_A$ را به عنوان قطعه کلید مشترک لحاظ می‌کنیم.

توجه شود که آلیس و باب با اجرای چندین بار تزریق فاز تصادفی، به چندین $\hat{k}_A$ و $\hat{k}_B$ دست می‌یابند. با قرار دادن این قطعه کلیدها کنار یکدیگر، کلید خام هر کاربر حاصل می‌گردد. این کلیدهای خام وارد گام‌های بعدی پروتکل SKG می‌شوند تا در نهایت کلید مخفی توافق گردد.

توجه۱: در عمل به دلیل وجود نویز و نقیصه‌های سخت‌افزاری، مقادیر ϵ_A و ϵ_B قابل صرفنظر کردن نیستند؛ لذا در عمل، برای آشکارسازی فاز سیگنال دریافتی، از ایدهٔ نواحی محافظ[۳۲] استفاده می‌شود. ایده نواحی محافظ به زبان ساده به این صورت است که اگر فاز سیگنال دریافتی، در مجاورت مرز نواحی تصمیم قرار بگیرد، با توجه به اینکه احتمال عدم برابری کلید آلیس و باب زیاد است، در این وضعیت طرفین اقدام به استخراج کلید نمی‌کنند و سیگنال‌های دریافتی را دور می‌ریزند. البته در این مقاله، از نویز و نقیصه‌های سخت‌افزاری صرفنظر می‌شود تا به موجب آن، تحلیل‌ها ساده شود و ضمناً بتوان شهودهای طراحی خوبی ارائه کرد. در کارهای آتی، می‌توان اثر نواحی محافظ را بر تحلیل‌ها بررسی کرد.

توجه۲: افزایش تعداد سطوح کوانتیزاسیون M، باعث می‌شود تعداد بیت‌های متناظر با کلید مستخرج از کانال افزایش یابد؛ در نتیجه نرخ تولید کلید بیشتر خواهد شد. اما بدلیل افزایش نواحی مرزی، احتمال عدم تطابق کلیدها افزایش می‌یابد و اگر از ایده نواحی محافظ استفاده شود، به دلیل زیاد شدن نواحی محافظ، نرخ دور ریزی کلیدها زیاد می‌شود.

۲-۲- سناریوهای شنود

در مرحله تبادل سیگنال‌های کاوش، شنودگر نیز دو سیگنال با فازهای $\phi_A + \phi_{AE} + \epsilon_{AE}$ و $\phi_B + \phi_{BE} + \epsilon_{BE}$ دریافت می‌کند که ϕ_{AE} و ϕ_{BE} به ترتیب بیانگر فاز ناشی از کانال آلیس-شنودگر و کانال باب-شنودگر هستند. ضمناً ϵ_{AE} و ϵ_{BE} مقادیر جابجایی فاز ناشی از نویز و نقیصه‌های سخت‌افزاری است.

با فرض آنکه شنودگر از طرح SKG به طور کامل آگاهی دارد، تلاش می‌کند تا یک کپی از کلید را بدست آورد. بدین منظور، شنودگر با ترکیب مشاهداتش از دو کانال شنود، تخمینی از کلید مشترک آلیس و باب را بدست می‌آورد. با این توضیحات، در ادامه دو سناریوی پردازشی برای شنودگر ارائه می‌شود. این دو سناریو، بیشترین شباهت را به عملیات پردازشی آلیس و باب دارد.

- **سناریوی شنود اول:** شنودگر فاز سیگنال دریافتی از آلیس و باب را با هم جمع کرده و سپس عملیات آشکارسازی (کوانتیزاسیون) را انجام می‌دهد. به عبارت دیگر:

$$\hat{k}_1 = Q(\phi_A + \phi_B + \phi_{AE} + \phi_{BE} + \epsilon_{AE} + \epsilon_{BE}) \qquad (۵)$$

➢ **سناریوی شنود دوم:** شنودگر فاز سیگنال‌های دریافتی از آلیس و باب را بطور جداگانه کوانتیزه کرده و سپس مقادیر بدست آمده را در پیمانه M با هم جمع می‌کند. به عبارتی:

$$\hat{k}_2 \overset{M}{=} Q(\phi_A + \phi_{AE} + \epsilon_{AE}) + Q(\phi_B + \phi_{BE} + \epsilon_{BE}) \quad (۶)$$

با مقایسه روابط (۵) و (۶) با رابطه (۲) و (۳) متوجه می‌شویم که کلیدهای بدست آمده در شنودگر با کلیدهای آلیس و باب تفاوت زیادی دارند که ناشی از تفاوت مکانی آنهاست.

۳- تحلیل امنیتی

در این بخش، امنیت طرح پیشنهادی را با رویکرد محرمانگی هندسی مورد بررسی قرار می‌دهیم. همچنین برای بهبود امنیت طرح پیشنهادی، ایدهٔ پویاسازی فرکانسی را ارائه می‌کنیم. همانطور که پیش‌تر هم اشاره شد، برای سادگی تحلیل‌ها، از تأثیر نویز و نقیصه‌های سخت‌افزاری صرفنظر می‌شود. در پایان، پیچیدگی شنود در شرایط عملی مورد بررسی قرار می‌گیرد.

۳-۱- ارزیابی نواحی افشای کلید

تعریف ۱ (نواحی افشای کلید): صحت کلید شنودگر، منوط به برقراری رابطه زیر است:

$$\forall e \in \{1,2\} \ , \ \hat{k}_e \overset{M}{=} \hat{k}_A \quad (۷)$$

به‌عبارت دیگر، در هر نقطه‌ای که رابطه (۷) 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 این بخش، نواحی افشای کلید را با فرض ایستا بودن کانال، در فضای آزاد بدست می‌آوریم. به این منظور، ابتدا نواحی افشای کلید را برای دو سناریوی ذکر شده در بخش ۲-۲، به طور مجزا بدست می‌آوریم. سپس اجتماع این دو ناحیه را به عنوان ناحیه افشای کلید برای طرح پیشنهادی در نظر می‌گیریم[۳۳].

اگر فاصله شنودگر تا آلیس و باب به ترتیب برابر با d_{AE} و d_{BE} باشد، با تعریف $d_E = d_{AE} + d_{BE}$، نواحی افشای کلید برای هر یک از دو سناریوی شنود به شرح زیر است:

➢ **نواحی افشای کلید در سناریوی شنود اول:**

با نادیده گرفتن نویز و نقیصه‌های سخت‌افزاری رابطه (۵) به صورت زیر قابل بازنویسی است:

$$\hat{k}_1 \overset{M}{=} \left\lfloor \frac{\frac{2\pi}{M} i_A + \frac{2\pi}{M} i_B + \frac{2\pi d_{AE}}{\lambda} + \frac{2\pi d_{BE}}{\lambda}}{\frac{2\pi}{M}} + \frac{1}{2} \right\rfloor = i_A + i_B + \left\lfloor \frac{M d_E}{\lambda} + \frac{1}{2} \right\rfloor \quad (۸)$$

که $d_E = d_{AE} + d_{BE}$. با جایگذاری روابط (۴) و (۸) در رابطه (۷) و نیز اعمال عملیات پیمانه M، نواحی افشای کلید از تساوی زیر بدست خواهد آمد:

$$\left\lfloor \frac{\mathrm{Md_{AB}}}{\lambda} + \frac{1}{2} \right\rfloor + \mathrm{nM} = \left\lfloor \frac{\mathrm{Md_E}}{\lambda} + \frac{1}{2} \right\rfloor \quad (۹)$$

که در آن $n \in \{0,1,2,3,\dots\}$ است. به عنوان مثال در باند فرکانسی $f = 300\ MHz$ (معادل با $\lambda = 1$) و به ازاء $M = 4$، نواحی افشای کلید از حل تساوی زیر بدست می‌آید:

$$\left\lfloor 4d_{AB} + \frac{1}{2} \right\rfloor + 4n = \left\lfloor 4d_E + \frac{1}{2} \right\rfloor \quad (۱۰)$$

با توجه به این رابطه، خط واصل بین آلیس و باب، همواره جزء نواحی افشای کلید است؛ یعنی شنودگر با استقرار در هر نقطه دلخواهی روی این خط، می‌تواند کلید را بدست آورد.

➢ **نواحی افشای کلید در سناریوی شنود دوم:**

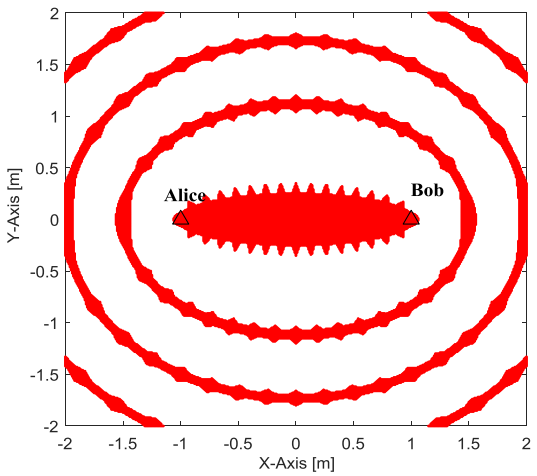
با نادیده گرفتن نویز و نقیصه‌های سخت‌افزاری رابطه (۶) به صورت زیر قابل بازنویسی است:

$$\hat{k}_2 \overset{M}{=} \left\lfloor \frac{\frac{2\pi}{M} i_A + \frac{2\pi d_{AE}}{\lambda}}{\frac{2\pi}{M}} + \frac{1}{2} \right\rfloor + \left\lfloor \frac{\frac{2\pi}{M} i_B + \frac{2\pi d_{BE}}{\lambda}}{\frac{2\pi}{M}} + \frac{1}{2} \right\rfloor = i_A + i_B + \left\lfloor \frac{M d_{AE}}{\lambda} + \frac{1}{2} \right\rfloor + \left\lfloor \frac{M d_{BE}}{\lambda} + \frac{1}{2} \right\rfloor \quad (۱۱)$$

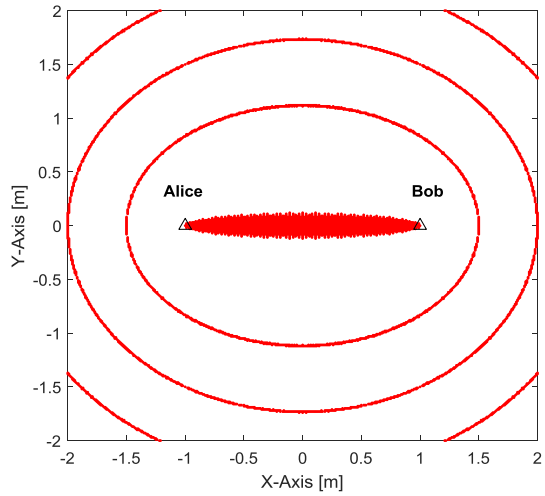
با جایگذاری روابط (۴) و (۱۱) در رابطه (۷)، و نیز اعمال عملیات پیمانه M، نواحی افشای کلید از تساوی زیر بدست خواهد آمد:

$$\left\lfloor \frac{M d_{AB}}{\lambda} \right\rfloor + nM = \left\lfloor \frac{M d_{AE}}{\lambda} + \frac{1}{2} \right\rfloor + \left\lfloor \frac{M d_{BE}}{\lambda} + \frac{1}{2} \right\rfloor \quad (۱۲)$$

در وضعیتی که آلیس و باب در مکان (-1,0) و (+1,0) قرار گرفته‌اند نواحی افشای کلید برای طرح پیشنهادی[۳۴] به ترتیب در شکل‌های ۳ و ۴ 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.



شکل (۳): نواحی افشای کلید برای یک طرح SKG مبتنی بر فاز گسسته به ازاء $M = 8$ و فرکانس‌کاری $f = 300\ MHz$



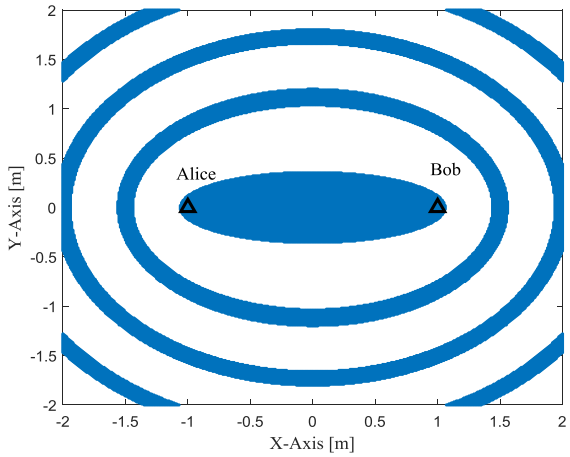
شکل (۴): نواحی افشای کلید برای یک طرح SKG مبتنی بر فاز گسسته به ازاء $M = 64$ و فرکانس‌کاری $f = 300\ MHz$

توجه شود که در تمامی 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 می‌باشد. 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 بخصوص مساحت ناحیه 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.

به منظور روشن شدن تفاوت بین طرح پیشنهادی در این مقاله با طرح فاز پیوسته در مرجع [۱۰]، نواحی محرمانه برای طرح فاز پیوسته را در شکل ۵ بازتولید کردیم. در این شکل، نواحی محرمانه به رنگ سفید و نواحی آسیب‌پذیر با رنگ آبی مشخص شده‌اند. به منظور مقایسه منصفانه بین طرح‌های فاز گسسته و فاز پیوسته، دقیقاً از پارامترهای مورد استفاده در شکل ۳ استفاده نموده‌ایم.

براساس نتایج شبیه‌سازی، در طرح فاز پیوسته (شکل ۵) حدود 72% از کل صفحه را نواحی محرمانه تشکیل می‌دهد؛ درحالی‌که در طرح پیشنهادی فاز گسسته، نواحی محرمانه حدود 82% از کل فضا است. بنابراین، می‌توان نتیجه گرفت که در طرح پیشنهادی، نواحی محرمانه حدود 10% از طرح فاز پیوسته بیشتر است. همچنین مشاهده می‌کنیم که الگوی نواحی افشای کلید برای حالت فاز گسسته، مشابه حالت فاز پیوسته، بصورت بیضی‌هایی می‌باشد. توجه شود که برای حالت فاز گسسته به دلیل وجود پردازش جزء صحیح در گیرنده، هندسه‌ی حلقه‌ها قدری متفاوت خواهد بود.

همچنین متذکر می‌شویم که خود مکان آلیس و باب و نیز حوالی این مکان‌ها می‌بایست جزء نواحی افشای کلید باشند؛ چرا که اگر شنودگر مثلاً در حوالی آلیس مستقر شود آنگاه فاز تزریقی توسط آلیس و نیز جمع فاز تزریقی توسط باب و فاز کانال قانونی را به خوبی تخمین می‌زند و لذا با اجرای پردازشی مشابه آلیس و باب، به کلید مشترک آنها دست می‌یابد. نتایج شبیه‌سازی در شکل ۵، حقیقت ذکر شده در بالا را نشان می‌دهد که خود تأییدی بر اعتبار طرح پیشنهادی و تحلیل‌های امنیتی آن می‌باشد.



شکل (۵): نواحی آسیب‌پذیری برای طرح SKG مبتنی بر فاز پیوسته به ازاء $M = 8$ و فرکانس‌کاری $f = 300\ MHz$

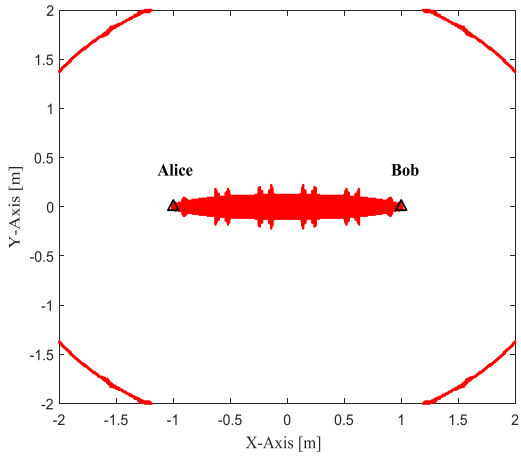
۳-۲- ایده پویاسازی فرکانسی

تاکنون فرض بر این بود که برای تولید یک دنباله کلید، روال کاوش کانال همواره بر روی یک فرکانس انجام می‌شود. با توجه به روابط (۹) و (۱۲) پارامتر طول موج (λ) بر نواحی افشای کلید تاثیرگذار است. لذا هندسه‌ی نواحی محرمانه و نواحی افشای کلید با تغییر فرکانس سیگنال کاوش، قابل دستکاری است. 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. به عبارت دیگر، هر سیگنال کاوش بر روی یک فرکانس از مجموعه فرکانسی $\mathbb{F}$ ارسال می‌گردد و ضمناً الگوی فرکانسی کاوش کانال بصورت عمومی در دسترس همگان و بخصوص آلیس و باب است. در ادامه تأثیر این ایده را بر بهبود نواحی محرمانه و آنتروپی کلید مورد بررسی قرار می‌دهیم.

۳-۲-۱- افزایش نواحی محرمانه

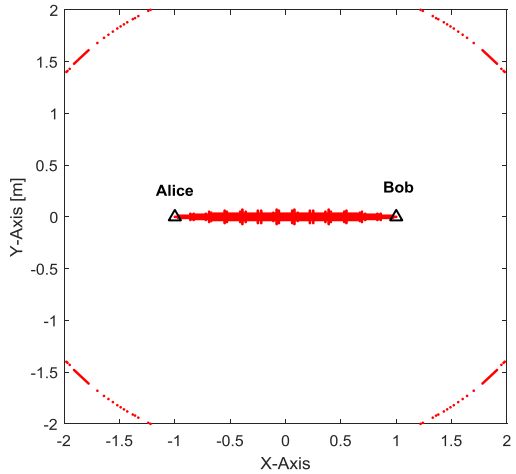
بر پایه این ایده، اگر شنودگر بخواهد کل دنباله کلید را بدست آورد باید در مکانی مستقر شود که این مکان به ازاء تمام فرکانس‌های موجود در مجموعه $\mathbb{F}$، جزو نواحی افشای کلید باشد. بنابراین، به طور شهودی می‌توان گفت که میزان نواحی افشای کلید در صورت استفاده از چندین فرکانس نسبت به حالت تک فرکانس کمتر است. برای مثال، برای $M = 8$ و فرکانس‌های کاوش $f = 100, 200, 300, 400, 500\ MHz$، نواحی افشای کلید در شکل ۶ ترسیم شده است. همان‌طوری‌که مشخص است در مقایسه با

شکل ۳ (استفاده از یک فرکانس)، نواحی افشای کلید به مراتب کمتر است؛ به طوری‌که در این حالت نواحی افشای کلید حدود 3% از کل فضا است. همچنین در شکل ۷ برای دنباله 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 (۶): نواحی افشای کلید برای تعداد سطوح کوانتیزاسیون $M = 8$ و فرکانس‌های کاوش $f = 100, 200, 300, 400, 500\ MHz$

نتایج شبیه‌سازی‌ها در شکل‌های ۶ و ۷ 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 (۷): نواحی افشای کلید برای تعداد سطوح کوانتیزاسیون $M = 64$ و فرکانس‌های کاوش $f = 100, 200, 300, 400, 500\ MHz$

۳-۲-۲- بهبود آنتروپی کلید

ایده پویاسازی فرکانسی، از منظر افزایش آنتروپی کلید نیز مفید است. در صورت استفاده از این ایدهٔ با F فرکانس مختلف، با یک کانال متغیر مواجه خواهیم بود که فاز آن می‌تواند F وضعیت متفاوت را تجربه کند. در این حالت، اگر تعداد دفعات کاوش کانال برای تولید دنباله کلید برابر با L باشد، در این‌صورت آنتروپی دنبالهٔ کلید برابر با $\min(L, F) \times \log_2 M$ خواهد بود. به عنوان مثال، در حالت $M = 2$ و با فرض $F \geq L$ آنتروپی دنباله کلید، کامل بوده و در نتیجه کل فضا محرمانه بوده و ناحیه افشای کلید تهی است؛ اما اگر $F = 1$ باشد (حالت تک فرکانس)، آنتروپی دنباله کلید، فارغ از طول آن، همواره برابر با ۱ بیت خواهد بود؛ زیرا در این مورد، دنباله کلید بدست آمده توسط شنودگر، یا همان دنباله کلید بدست آمده توسط آلیس و باب است و یا متمم[۳۵] آن می‌باشد.

۳-۲-۳- پیچیدگی شنود در شرایط عملی

تحلیل‌های انجام شده در بخش ۳-۱ در شرایط ایده‌آل با فرض ایستایی کانال در فضای آزاد انجام شده است. اما در عمل به واسطه پویایی کانال و وجود پدیده چندمسیرگی، چنین شرایط ایده‌آلی وجود ندارد؛ بدیهی است که در صورت پویا بودن کانال (که ناشی از تحرک آلیس، باب و یا عوامل محیطی است) الگوی نواحی افشای کلید، متغیر خواهد بود. همچنین در صورت وجود پدیده چندمسیرگی، روابط تحلیلی جهت محاسبه نواحی افشای کلید بسیار دشوار شده و در چنین شرایطی، این نواحی برخلاف سناریوی ارتباطی فضای آزاد، فاقد تقارن خواهد بود. متذکر می‌شویم که گذشته از موارد فوق، در شرایط عملی محدودیت‌های شنودگر نیز مزید بر علت شده و باعث می‌شود کار تعیین نواحی افشای کلید برای شنودگر دشوارتر گردد. به عنوان مثال، می‌توان به مواردی همچون خطای موقعیت‌یابی شنودگر در تعیین محل استقرار آلیس و باب، و غیرقابل پیش‌بینی بودن کانال آلیس-باب در محیط‌های با پراکندگی زیاد اشاره کرد (بدلیل ناهمبستگی فضایی).

با توجه به روابط (۲) و (۳)، کلید آلیس و باب تابعی از فاز کانال قانونی (ϕ_C) است. در محیط‌های با پراکندگی زیاد، فاز کانال‌های شنود (ϕ_{AE} و ϕ_{BE}) و فاز کانال قانونی ناهمبسته بوده و بنابراین شنودگر به هیچ طریقی نمی‌تواند فاز کانال قانونی را بدست آورد تا به وسیله آن، کلید را استخراج کند. اما با توجه به تعریف۱، نواحی افشای کلید از رابطه (۷) بدست می‌آید. بدیهی است که در محیط‌های با پراکندگی زیاد نیز می‌توان نقاطی را در محیط انتشار پیدا کرد که این رابطه برقرار باشد. لذا اگر شنودگر تعداد زیادی آنتن را بصورت تصادفی در محیط انتشاری پخش کند با احتمال بالایی حداقل یکی از آنتن‌ها در ناحیه افشای کلید قرار خواهد گرفت و شنودگر می‌تواند کلید را بدست آورد. در این سناریو، سیستم شنود نیازی به دانستن نواحی افشای کلید ندارد، بلکه فقط کافیست بداند نواحی افشای کلید چه درصدی از کل

فضا را تشکیل می‌دهند تا بتواند، تعداد آنتن‌های لازم جهت توزیع در محیط انتشار جهت افشای کلید را محاسبه کند.

۴- ارزیابی عملکردی

در این کار تحقیقاتی، ما صرفاً از منظر امنیتی (نواحی افشاء کلید) به مطالعه طرح پیشنهادی پرداختیم. مطالعه کارایی طرح پیشنهادی یعنی محاسبه نرخ تولید کلید[۳۶] و نیز نرخ عدم تطابق کلید[۳۷] (KDR) نیز موضوع مهمی است. واضح است که خطای کلید عمدتاً زمانی اتفاق می‌افتد که فاز برآیند مقداری نزدیک به مرز نواحی تصمیم داشته باشد. بنابراین می‌توان با تعریف نواحی مرزی کوچک، نواحی تصمیم را تفکیک کرد تا آن مقادیری از کانال را که سبب اختلاف بین نمونه‌های دریافتی آلیس و باب می‌شوند، کنار گذاشت [۱۵]. توجه شود در حالتی‌که با فاز سروکار داریم نواحی محافظ به گونه‌ای تعریف می‌شود که اگر فاز بدست آمده در گره‌ها در هر کدام از این نواحی قرار گرفت، به سادگی آن فاز دور ریخته می‌شود. بر این اساس، متوسط تعداد بیت‌ها در هر بار کاوش کانال، $N_{av} \leq \left(1-\frac{\psi M}{2\pi}\right) log_2 M$ خواهد شد که M و ψ به ترتیب تعداد نواحی تصمیم و عرض ناحیه محافظ هستند.

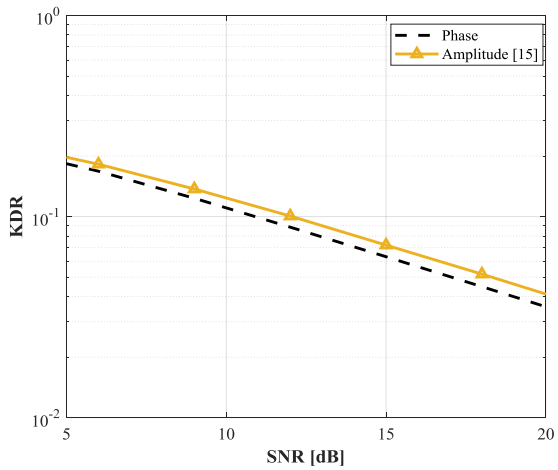
در این مقاله، از رویکرد کوانتیزاسیون مستقیم و بدون استفاده از ناحیه محافظ برای استخراج کلید استفاده کرده‌ایم. بر مبنای مرجع [۱۵]، این رویکرد منجر به نرخ خطای بالا برای کلید می‌شود و در نتیجه به کدهای تصحیح خطای قوی در فاز اصلاح اطلاعات نیاز دارد. در کارهای آینده، رویکرد کوانتیزاسیون با نواحی محافظ را برای طرح تولید کلید فاز گسسته پیشنهادی بررسی خواهیم کرد.

بدیهی است که نتیجه مرحله کوانتیزاسیون برای هر نمونه کاوش کانال، یکی از دو پیشامد زیر خواهد شد:

- پیشامد ۱: $\hat{k}_A$ و $\hat{k}_B$ بیت‌های یکسان داشته باشند.
- پیشامد ۲: $\hat{k}_A$ و $\hat{k}_B$ بیت‌های غیریکسان داشته باشند.

در این بخش، برای سادگی، از الگوریتم متداول کوانتیزاسیون تک بیتی[۳۸] [۱۵] استفاده می‌کنیم. لذا آلیس و باب از BPSK برای ارسال فازهای تصادفی گسسته خود بهره می‌برند. خروجی کوانتیزه کننده تک بیتی، برای آلیس و باب به ترتیب، بیت‌های $\hat{k}_A$ و $\hat{k}_B$ خواهد بود. بعد از L بار کاوش کانال، با قرار دادن قطعه کلیدها کنار یکدیگر، کلید خام حاصل شده برای هر کدام K_A و K_B خواهد بود.

توجه شود که عدم تطبیق قطعه کلید $\hat{k}_A \neq \hat{k}_B$، وقتی رخ می‌دهد که $(\hat{k}_A = 0, \hat{k}_B = 1)$ یا $(\hat{k}_A = 1, \hat{k}_B = 0)$ باشد. در شکل ۸، طرح پیشنهادی در این مقاله (که مبتنی بر فاز کانال است) را با طرح پیشنهادی در مرجع [۱۵] (که مبتنی بر دامنه سمبل‌های کاوش است) مقایسه می‌کنیم. همان‌طوری‌که در این شکل مشخص است، طرح پیشنهادی ما در مقایسه با طرح مرجع [۱۵]، به ازای یک KDR ثابت، حدود 1 dB در SNR کاوش کانال صرفه‌جویی می‌کند.



شکل (۸): نرخ عدم تطابق کلید برحسب SNR کاوش کانال

۵- نتیجه‌گیری و کارهای آتی

در این مقاله، به بررسی چالش تولید کلید مخفی در سیستم‌های ارتباطی نقطه به نقطهٔ ایستا پرداخته شد. دیده شد که بکارگیری تزریق فاز تصادفی گسسته با کمک مدولاسیون فاز PSK توسط آلیس و باب، به محرمانگی هندسی سیستم مخابراتی کمک می‌کند. برخلاف تزریق فاز پیوسته، دیده شد که طرح فاز گسسته، علاوه بر سهولت در پیاده‌سازی، محرمانگی بیشتری به همراه دارد؛ زیرا درصد نواحی افشای کلید، کمتر است. همچنین نواحی افشای کلید در طرح پیشنهادی، هندسه متفاوتی نسبت به نواحی آسیب‌پذیری در طرح‌های فاز پیوسته خواهد داشت.

نتایج شبیه‌سازی نشان می‌دهد که نواحی افشای کلید به فرکانس‌کاری و نیز مرتبه مدولاسیون مربوط است به طوری‌که با افزایش M، درصد نواحی افشای کلید کاهش می‌یابد. نتیجه جالب این مقاله این بود که اگر در کاوش کانال به جای یک فرکانس، چند فرکانس بکار گرفته شود، نواحی افشای کلید به میزان قابل توجهی کاهش می‌یابد.

حال به منظور کاهش نواحی افشای کلید و نیز توسعه طرح پیشنهادی، برخی از زمینه‌های تحقیقاتی جهت افزایش امنیت طرح‌های تولید کلید ارائه شده است. هر کدام از موارد زیر، می‌توانند به عنوان کارهای آتی مورد مطالعه قرار گیرند:

- در این مقاله، از مدولاتور PSK برای ارسال سیگنال‌های تصادفی آلیس و باب بهره برده شد. تعیین فاز اولیه مدولاتور با هدف کمینه‌سازی میزان نواحی افشای کلید، برای کارهای آتی پیشنهاد می‌شود.
- در این کار پژوهشی فقط به بررسی و مشاهده تأثیر SKG مبتنی بر چند فرکانس بر روی ناحیه افشای کلید پرداختیم. بهینه‌سازی محرمانگی هندسی به ارتقاء امنیت سیستم کمک می‌کند. به‌عبارت دیگر، از یک مجموعه بزرگ از فرکانس‌ها، بهتر است

تعدادی فرکانس برای کاوش کانال به‌گونه‌ای برگزیده شود تا مساحت اولین ناحیه محرمانه بیشینه گردد[۳۹].

- پیشنهاد می‌شود تأثیر نقیصه‌های سخت افزاری [۱۶] بخصوص نویز فاز اسیلاتور و عدم تعادل I/Q که تأثیر جدی بر مولفه فاز سیگنال دارند در طرح SKG مورد مطالعه و تحلیل قرار گیرد. به‌عبارت دیگر، نتیجه تأثیر نقیصه‌های سخت‌افزاری بر روی نواحی افشای کلید و نیز عدم تطابق کلید قابل تأمل خواهد بود.

- در شرایط نویز محدود[۴۰]، سناریویی که به بهبود کارایی SKG کمک می‌کند بکارگیری رله در ارتباطات است [۱۶]-[۱۸]. چرا که بدلیل فاصله زیاد بین آلیس و باب و یا توان ارسالی محدود این دو، ممکن است سیگنال کاوش دریافتی ضعیف بوده و در نتیجه فرآیند SKG با شکست مواجه شود. در چنین وضعیتی استفاده از رله، بسیار مفید خواهد بود. در چنین سناریویی، می بایست یک پروتکل SKG مناسب طراحی و تحلیل گردد. به خصوص وقتی با یک رله غیرقابل اعتماد سروکار داریم، طراحی یک پروتکل SKG به گونه‌ای که رله‌ی غیر قابل اعتماد نتواند کلید مشترک بین آلیس و باب را دریافت کند یک چالش مهم محسوب می‌شود.

- در توسعه بند قبلی، می‌توان یک سیستم مخابراتی مبتنی بر چندین رله متوالی را مورد مطالعه قرار داد [۱۹]. چنین سناریویی در برخی شبکه‌ها مانند شبکه های اقتضایی و IoT موجود است. ارائه‌ی یک طرح SKG کارا از منظر انرژی و زمان اجرا، در این سناریو حائز اهمیت است. چالش وقتی بیشتر می‌شود که رله‌های بکار گرفته شده غیرقابل اعتماد باشند.

- ممکن است در یک شبکه ارتباطی، یک تداخل‌گر و یا جمر وجود داشته باشد [۱۹] و [۲۰] که نتیجتاً به فرآیند SKG اجرا شده، آسیب خواهد زد. به‌عبارت دیگر، مقادیر تصادفی مشترک بین آلیس و باب با تزریق نویز تصادفی توسط جمر، عدم انطباق بیشتری خواهند داشت. در چنین شرایطی طرح‌های SKG مرسوم عملاً شکست خواهد خورد. بنابراین می‌بایست یک طرح SKG مقاوم در برابر تداخل یا جمینگ طراحی شود.

- در این مقاله، به عنوان یک کار ابتدایی و پایه‌ای، نواحی افشای کلید برای کلیدهای خام تعیین گردید. بهتر است نواحی افشای کلید برای کلیدی که بعد از مرحله اصلاح اطلاعات به‌دست می‌آید، محاسبه شود [۲۱]. چرا که در فرآیند اصلاح اطلاعات، بخشی از کلید نشت پیدا خواهد کرد و لذا احتمالاً نواحی افشای کلید، افزایش خواهد یافت.

مراجع

[1] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications", IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1125–1142, Oct 2017.

[2] P. Neelakanta, "Designing robust wireless communications for factory floors", in 2006 IEEE International Conference on Industrial Informatics, Aug. 2006.

[3] S. K. Timalsina, R. Bhusal, and S. Moh, "NFC and its application to mobile payment: Overview and comparison", in 2012 8th International Conference on Information Science and Digital Content Technology (ICIDT), pp. 203– 206.

[4] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao and K. Zeng, "Physical layer security of 5G wireless networks for IoT: Challenges and opportunities", IEEE Internet Things J., vol. 6, no. 5, pp. 8169-8181, Oct. 2019.

[5] 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, Aug. 2020.

[6] G. Li, C. Sun, J. Zhang, E. Jorswieck, B. Xiao, and A. Hu, "Physical layer key generation in 5G and beyond wireless communications: Challenges and opportunities", Entropy, vol. 21, p. 497, 2019.

[7] O. A. Topal and G. Karabulut Kurt, "Physical layer authentication for LEO satellite constellations", in 2022 IEEE Wireless Communications and Networking Conference (WCNC), pp. 1952-1957.

[8] K. Lin, Z. Ji, Y. Zhang, G. Chen, P. L. Yeoh and Z. He, "Secret key generation based on 3D spatial angles for UAV communications", in 2021 IEEE Wireless Communications and Networking Conference (WCNC), 2021, pp. 1-6.

[9] O. A. Topal, G. K. Kurt and H. Yanikomeroglu, "Securing the inter-spacecraft links: Physical layer key generation from doppler frequency shift", IEEE Journal of Radio Frequency Identification, vol. 5, no. 3, pp. 232-243, Sept. 2021.

[10] A. K. Tirandaz and A. Kuhestani, "Security analysis of a mutual random phase injection scheme to generate a secret key in static point-to-point communications", Electronic and Cyber Defense, vol. 10, no. 2, pp. 19-30, Oct. 2022

[11] T. M. Pham, A. N. Barreto, M. Mitev, M. Matthé and G. Fettweis, "Secure communications in line-of-sight scenarios by rotation-based secret key generation", in 2022 IEEE International Conference on Communications Workshops (ICC Workshops), pp. 1101-1105.

[12] G. Li, H. Yang, J. Zhang, H. Liu and A. Hu, "Fast and secure key generation with channel obfuscation in slowly varying environments", in 2022 IEEE INFOCOM, IEEE Conference on Computer Communications, pp. 1-10.

[13] S. Mohajer Hamidi, A. K. Khandani, and E. Bateni, "A secure key sharing algorithm exploiting phase reciprocity in wireless channels", arXiv:2111.15046v1, Nov. 2021.

[14] Y. Liu, S. C. Draper, and A. M. Sayeed, "Exploiting channel diversity in secret key generation from multipath fading randomness", IEEE Trans. Inf. Foren. Sec., vol. 7, no. 5, pp. 1484–1497, Oct. 2012.

[15] X. Guan, N. Ding, Y. Cai and W. Yang, "Wireless key generation from imperfect channel state information: Performance analysis and improvements", in IEEE International Conference on Communications Workshops (ICC Workshops), Shanghai, China, 2019, pp. 1-6.

[16] A. Kuhestani, A. Mohammadi and K.-K. Wong, "Optimal power allocation by imperfect hardware

analysis in untrusted relaying networks", IEEE Trans. Wireless Commun., vol. 17, pp. 4302-4314, July 2018.

[17] V. Shahiri, A. Kuhestani and L. Hanzo, "Short-packet amplify-and-forward relaying for the internet-of-things in the face of imperfect channel estimation and hardware impairments", IEEE Trans. Green Commun. Netw., vol. 6, no. 1, pp. 20-36, Mar. 2022.

[۱۸] دزفولی‌زاده، سمانه، مبینی، زهرا، "استراق سمع فعال با کمک UAV برای بهبود امنیت شبکه های مخابرات مشارکتی"، مجله مهندسی برق و الکترونیک ایران، جلد ۱۸، شماره ۳، ۱۴۳-۱۵۱، پاییز ۱۴۰۰.

[19] M. T. Mamaghani, A. Kuhestani, and H. Behroozi, "Can a multi-hop link relying on untrusted amplify-and-forward relays render security?", Wireless Netw., vol. 27, no. 1, pp. 795–807, Jan. 2021.

[20] H. Saedi, A. Mohammadi, and A. Kuhestani, "Characterization of untrusted relaying networks in the presence of an adversary jammer", Wireless Networks, Jun. 2019.

[21] 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 Int. Conf. Commun. Workshop (ICCW), Ireland, Jun. 2020.

[22] Z. Zhang, G. Li, and A. Hu, "An adaptive information reconciliation protocol for physical-layer based sewcret key generation", in 2019 IEEE 89th Veh. Technol. Conf. (VTC2019-Spring), 2019, pp. 1-5.

زیرنویس‌ها

[1] Internet-of-Things (IoT)
[2] Wireless Sensor Network
[3] Device-to-Device
[4] Short Range Communication
[5] Radio Frequency Identification
[6] Physical Layer Security
[7] Physical Layer Secrecy Transmission
[8] Secret Key Generation
[9] Physical Layer Authentication (PLA)
[10] Pilot
[11] Signal-to-Noise-Ratio (SNR)
[12] Line-of-Sight

[13] Unmanned Aerial Vehicle (UAV)
[14] Additive White Gaussian Noise (AWGN)
[15] Free Space

[۱۶] توجه شود که در محیط‌های انتشار چندمسیره، به دلیل رخداد محوشدگی کانال، تولید کلید با میزان تصادفی بودن بالا، امکان پذیر است و لذا امنیت کلید برقرار خواهد بود. بنابراین سناریوی مورد مطالعه در این مقاله (ارتباط در فضای آزاد) را می‌توان به عنوان سناریوی بدبینانه در حوزه SKG در نظر گرفت.

[17] Received Signal Strength
[18] Channel State Information
[19] Channel Impulse Response
[20] Channel Frequency Response
[21] Phase Shift Keying
[22] Mutual Random Phase Injection
[23] Geometric Secrecy
[24] Static
[25] Key Disclosure Region
[26] Probing Signal
[27] Secrecy Regions
[28] Reciprocal
[29] Constellation
[30] Sequential

[۳۱] فاز دریافتی حاصل جمع فاز سمبل ارسالی و فاز کانال است

[32] Guard Zone

[۳۳] یادآور می‌شود که نواحی افشای کلید مجموعه نقاطی در فضا هستند که اگر شنودگر در آن نقاط مستقر شود می‌تواند کلید را بدست آورد. با توجه به اینکه مهم نیست شنود با چه پردازشی به کلید مشترک بین آلیس و باب می‌رسد؛ برای تعیین نواحی افشای کلید، هر دو سناریوی شنود، مورد بررسی قرار می‌گیرد.

[۳۴] نواحی افشای کلید در سناریوی شنود اول، مجموعه نقاطی در فضای $\mathbb{R}^2$ است که در رابطه (۹) صدق می‌کنند و در سناریوی شنود دوم، مجموعه نقاطی در فضای $\mathbb{R}^2$ است که در رابطه (۱۲) صدق می‌کنند. اجتماع این دو ناحیه، نواحی افشای کلید برای طرح پیشنهادی است.

[35] Complement
[36] Key Generation Rate
[37] Key Disagreement Rate
[38] One Bit Quantizer

[۳۹] همانطورکه پیش‌تر گفتیم در مجاورت آلیس و باب، یک ناحیه افشای کلید غیرقابل اجتناب حول خط واصل بین آلیس و باب وجود دارد که با افزایش تعداد کانال‌های مورد استفاده در مرحله کاوش کانال، این ناحیه به خط واصل بین آلیس و باب تقلیل می‌یابد. اگر سیستم مخابراتی مدنظر SRC باشد، شنودگر نمی‌تواند روی خط واصل مستقر شود؛ زیرا این ناحیه جزو نواحی حفاظت شده بوده و در صورت استقرار شنودگر در آن ناحیه، حضور شنودگر توسط آلیس و باب قابل کشف خواهد بود. لذا در کاربردهای SRC نسبت به این ناحیه، نگرانی نداریم.

[40] Noise Limited