یک طرح نوین تولید کلید لایه فیزیکی مبتنی بر فاز کانال برای ارتباطات همتا به همتا

محمدرضا کشاورزی[1] علی کوهستانی[2]

۱- استادیار- پژوهشکده فناوری ارتباطات- پژوهشگاه ارتباطات و فناوری اطلاعات – تهران – ایران
mrkeshavarzi@itrc.ac.ir

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

چکیده: در بین روش‌های برقراری امنیت لایه فیزیکی، تولید کلید مخفی به‌دلیل ویژگی‌ها و قابلیت‌های مطلوبی که دارد، برای شبکه‌های نسل ششم (6G) کارآمد است. به طور خاص، می‌توان از طرح‌های مبتنی بر مولدهای تصادفی محلّی برای تولید کلید مخفی با نرخ بالا 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 نوین تولید کلید مبتنی بر ارسال سیگنال‌های کاوش کانال با فاز تصادفی گسسته و برای ارتباطات همتا به همتا پیشنهاد می‌دهیم. بدین منظور، ضمن معرفی روش‌های کوانتیزاسیون، در طرح پیشنهادی، از روش ساده و کاربردی "کوانتیزاسیون با نواحی محافظ (GB)" برای استخراج کلید استفاده می‌شود. همچنین برخلاف بسیاری از مطالعات صورت گرفته شده، فرض می‌کنیم که کانال قانونی از هم‌پاسخی ضعیف رنج می‌برد و نویز نیز بر فاز دریافتی آلیس و باب اثرگذار است. برای چنین سناریویی، روابطی برای نرخ عدم تطبیق کلید (KMR) و نیز نرخ دور ریزی کلید (KDR) به ازای هر کاوش کانال ارائه می‌دهیم. اگرچه افزایش محدوده GB، معیار KMR را کاهش می‌دهد، اما طول دنباله کلید خام نیز کوتاه می‌گردد. به منظور ارزیابی تأثیر GB بر روی کارایی طرح تولید کلید پیشنهادی، در این مقاله، نرخ تولید کلید خام تعریف شده و محاسبه می‌گردد. نتایج شبیه‌سازی موید روابط تحلیلی بوده و برای تعیین توان سیگنال کاوش و محدود GB مفید است.

واژه‌های کلیدی: تولید کلید لایه فیزیکی، تزریق فاز تصادفی گسسته، نواحی محافظ، نرخ عدم تطبیق کلید، نرخ دور ریزی کلید.

نوع مقاله: پژوهشی

DOI: 10.61186/jiaeee.21.3.47

تاریخ ارسال مقاله :۱۴۰۲/۶/۲۲

تاریخ پذیرش مشروط مقاله: ۱۴۰۲/۰۴/۱۳

تاریخ پذیرش مقاله : ۱۴۰۲/۸/۱۵

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

به طور مرسوم، جهت برآورده کردن الزامات محرمانگی و احراز هویت در شبکه‌ها، از سازوکارهای امنیتی مبتنی بر رمزنگاری استفاده می‌شود. با این حال، نسل ششم شبکه‌های سلولی (6G) با تعداد قابل ملاحظه‌ای از ارتباطات همتا به همتا[۱] قابل پیاده‌سازی است که براساس آن، راه‌حل‌های مرسوم امنیتی می‌بایست مورد بازنگری قرار گیرد [۱]، [۲]. به عنوان یک راهکار امیدبخش و تحول‌ساز، به جای استفاده از راه‌حل‌های امنیتی مبتنی بر پیچیدگی محاسباتی می‌توان از تکنیک‌های امنیتی سبک وزن[۲] نظیر *تولید کلید مخفی لایه فیزیکی*[۳] (PLSKG)در شبکه‌های 6G [۳]، به صورت یک سازوکار امنیتی مستقل و یا مکمل روش‌های موجود [۴] بهره برد. قابل توجه است که اخیراً بسیاری از محققان دانشگاهی [۴]، [۵] و صنعتی [۶]، [۷] به تحقیق در زمینهٔ PLSKG پرداخته‌اند.

طرح‌های PLSKG مزایای قابل توجهی برای شبکه‌های بی‌سیم دارد [۳]. به طور خاص، توزیع و مدیریت کلید برپایه‌ی PLSKG نیازی به زیرساخت متمرکز ندارد؛ زیرا کلید مخفی بدون نیاز به همکاری شخص ثالث به دست می‌آید. این موضوع، زمان مورد نیاز برای توافق کلید را به طور قابل توجهی کاهش می‌دهد. علاوه بر این، به دلیل تغییرات کانال بی‌سیم، می‌توان کلید مخفی به‌دست‌آمده از روش PLSKG را به طور مداوم به‌روز رسانی کرد [۵]. لازم به ذکر است که PLSKG از طریق پیاده‌سازی سازوکارهای سبک و با حداقل تغییرات مورد نیاز تحقق می‌یابد؛ در حالی‌که از منظر نظریه اطلاعات، تضمین‌های امنیتی نیز ارائه می‌دهد. از این رو، این رویکرد به عنوان یک راه حل امیدوارکننده برای سیستم‌های فراتر از نسل پنجم[۴] (B5G) مانند اینترنت اشیاء[۵] (IoT) و ارتباطات با تأخیر کم و با قابلیت اطمینان بسیار زیاد[۶] (URLLC) مطرح است.

PLSKG از کانال بی‌سیم به عنوان منبع مشترک تصادفی[۷] بین گره‌های قانونی، بهره‌برداری می‌کند. به طور خاص، طرفین ارتباط بعد از تبادل سیگنال‌های راهنما[۸] و انجام پردازش‌های لازم، به یک کلید محرمانهٔ[۹] مشترک دست می‌یابند. در طرح‌های PLSKG، از مشخصاتی نظیر فاز کانال، توان سیگنال دریافتی[۱۰] (RSS)، اطلاعات حالت کانال[۱۱] (CSI) و سایر ویژگی‌های کانال جهت تولید کلید مخفی استفاده می‌شود [۳] و [۸] و [۹]. طرح های PLSKG در مرحلهٔ استخراج مقدار تصادفی مشترک (مرحله کاوش[۱۲] کانال)، ممکن است تحت تأثیر حملاتی از قبیل حملهٔ مرد در میان[۱۳] (MiM) یا حملهٔ منع سرویس[۱۴] (DoS) قرار گیرند [۱۰] و یا نقص‌های عملی و اجتناب‌ناپذیر مانند نویز حرارتی، ناقص بودن اطلاعات حالت کانال[۱۵](CSI) ناقص و نقیصه‌های سخت‌افزاری[۱۶] [۱۱] ،[۱۲] و نیز هم‌پاسخی ضعیف[۱۷] [۱۳] بر روی مقدا تصادفی مشترک تأثیر گذارد. این نقص‌ها و موارد عملی بخصوص در کاربردهای IoT که تجهیزات مورد استفاده معمولاً از نظر منابع پردازشی و توان مصرفی، محدودیت‌های زیادی دارند، ظهور پیدا می‌کند.

بدلیل موجود بودن RSS در بسیاری از دستگاه‌های تجاری، کارهای تحقیقاتی متعددی بر روی آن صورت گرفته است [۳] و [۱۴]. با این وجود، RSS جزو مشخصه‌های مقیاس بزرگ[۱۸] محسوب می‌شود که نرخ تولید کلید حاصل از آن، بخصوص در محیط‌های ایستا[۱۹]، کم است. بعلاوه، RSS به بسیاری از حملات از قبیل حمله شنود[۲۰] [۱۵]، حمله MiM [۱۶]، [۱۷] و حمله کانال قابل‌پیش‌بینی[۲۱] [۱۸] آسیب‌پذیر است. در ادامه، با تمرکز بر CSI کانال به عنوان یک ویژگی مقیاس کوچک[۲۲] کانال، تحقیقات بیشتری در حوزه تولید کلید صورت گرفت به طوری‌که توسط برخی NICهای تجاری قابل بهره‌برداری است[۲۳] [۳] و [۶]. در مطالعه اخیر [۱۹] تصریح شده است که CSI در مقایسه با RSS در سیستم تولید کلید، مزیت دارد. در این حوزه، کارهای مبتنی بر دامنه‌ی CSI عملی‌تر هستند [۲۰] و [۲۱]. با این وجود، دامنه به عنوان بهره‌ی سیگنال می‌تواند توسط سیگنال‌های قوی‌تر پوشانده شود. همچنین دامنه از نویز تأثیر زیادی می‌پذیرد و در نتیجه، نرخ تطبیق بیت[۲۴] پایین خواهد بود. یک ویژگی دیگر کانال که نواقص دامنه‌ی کانال را مرتفع می‌کند، اطلاعات فاز کانال است. فاز کانال در مقایسه با دامنه کانال نسبت به نویز حساس نیست و ضمناً به اندازه کافی تغییرات دارد. لذا به عنوان یک منبع تصادفی با آنتروپی بالا محسوب می‌شود.

در ارتباطات بُرد کوتاه و یا ارتباطات موج میلیمتری، نسبت سیگنال به نویز[۲۵] (SNR) نسبتاً زیاد بوده و پدیده محوشدگی وجود نخواهد داشت. همچنین در ارتباطات دید مستقیم[۲۶] (LoS) بین ماهواره‌ها [۲۲] و یا ارتباطات پرنده‌های بدون سرنشین[۲۷] (UAV) [۲۳] که در شبکه 6G حضور دارند، و به طور کلی در هر مخابره‌ای که کانال آن قابل مدل کردن با نویز سفید گوسی جمع شونده[۲۸] (AWGN) باشد، ایجاد منبع با آنتروپی بالا یک ضرورت است؛ چرا که طرح‌های متداول PLSKG که صرفاً مبتنی بر آنتروپی کانال هستند، کلیدهای به اندازه کافی تصادفی تولید نمی‌کنند. ذکر این نکته حائز اهمیت است که از منظر امنیت، چالشی‌ترین وضعیت برای تولید کلید مخفی، مربوط به ارتباطات فضای-آزاد[۲۹] می‌باشد [۲۴] و [۲۵] که در آن، کانال قانونی و کانال شنود از نوع LoS بوده و با AWGN مدل می‌شوند[۳۰]. در این حوزه، مرجع [۲۴] با الهام از تحرک فضاپیماها از شیفت فرکانس داپلر به منظور تولید کلید بهره برده است. در مراجع [۲۵]-[۲۸] نیز با فرض ایستایی محیط و گره‌ها، راهکارهایی برای تولید کلید ارائه شده است. برخلاف مرجع [۲۷] که یکی از گره‌ها مجهز به چندین آنتن است، در مراجع [۲۵] و [۲۶] و [۲۸] برای یک سیستم ساده متکی بر گره‌های تک آنتن، از فاز کانال بی‌سیم برای پیاده‌سازی PLSKG بهره برده شده است. به طور خاص، در مرجع [۲۸] با ارائه‌ی یک پیش‌پردازش بر روی داده‌های فاز و سپس فیلتر کردن آن، داده‌های فاز دو کاربر دارای

تغییرات آرام و بسیار منطبق گردید[۳۱]. در همین کار، نگاشتی بهتر از نگاشت Gray ارائه گردید که تصادفی بودن کلید را افزایش می‌دهد.
در این مقاله، مشابه کار [۲۵]، تولید کلید مخفی در یک ارتباط همتا به همتای LoS و در فضای آزاد مورد مطالعه قرار می‌گیرد. در این کار نیز، از فاز کانال به عنوان مؤلفه تصادفی مشترک بین آلیس و باب برای تولید کلید استفاده می‌کنیم و ضمناً به منظور افزایش آنتروپی کلید، فاز تصادفی[۳۲] توسط گره‌های قانونی تزریق می‌شود. اما متفاوت با کار پیشین [۲۵] که فاز تصادفی تزریقی توسط کاربران پیوسته بود، در این پژوهش، فاز تصادفی تزریقی از جنس گسسته بوده و لذا هم عملیاتی‌تر و هم از منظر پیاده‌سازی ساده‌تر است. به طور خاص، در این مقاله از مدولاسیون فاز BPSK برای ارسال فاز تصادفی گسسته استفاده می‌شود.
همان‌طوری‌که می‌دانیم اساس تولید کلید مخفی از کانال بی‌سیم بر اصل هم‌پاسخی کانال استوار است؛ حال آنکه در فاز کاوش کانال، وجود عواملی نظیر نویز، خطای تخمین کانال و وجود نقیصه‌های سخت‌افزاری، باعث عدم تطبیق کلیدها می‌شود. به منظور کاهش این نرخ اختلاف، تکنیک‌های کوانتیزاسیون گوناگونی بکار گرفته می‌شود [۲۹] -[۳۲]. در این مقاله، ضمن معرفی و مقایسه این روش‌ها، از روش مبتنی بر ناحیه محافظ[۳۳] (GB) و نیز کوانتیزه کننده تک‌بیتی استفاده کرده و نرخ عدم تطبیق کلید[۳۴] (KMR) را محاسبه می‌کنیم. همچنین متفاوت با تمام کارهای قبلی، اثر انحراف فرکانسی حامل[۳۵] (CFO) در عملکرد طرح PLSKG پیشنهادی، مورد مطالعه قرار می‌گیرد. توجه شود که در رویکرد مبتنی بر GB، تنها زمانی نمونه‌ی مستخرج از کاوش کانال برای تولید کلید مخفی استفاده می‌شود که کمیت تخمین زده شده در یک ناحیه کوانتیزاسیون[۳۶] (QR) یا ناحیه تصمیم قرار گرفته و در GBها قرار نگیرد. بر این اساس، معیار نرخ دور ریزی کلید[۳۷] (KDR) نیز برای طرح پیشنهادی محاسبه می‌گردد. به منظور ارزیابی تأثیر منفی افزایش اندازه GB، نرخ تولید کلید خام[۳۸] (RKGR) معرفی و محاسبه می‌شود. نتایج عددی ارائه شده، صحت روابط تحلیلی بدست آمده را تأیید کرده و ضمناً در خصوص مقدار توان سیگنال کاوش کانال و اندازه GB شهود خوبی ارائه می‌دهند.

۲- مقدمات و مدل سیستم

در این بخش در ابتدا، به معرفی انواع کوانتیزه کننده‌ها پرداخته و تأثیر آنها را بر روی کارایی کلید استخراج شده مطالعه می‌کنیم. در این خصوص، روش کوانتیزه مستقیم[۳۹] (صرفاً دمدولاسیون – بدون باند محافظ)، کوانتیزه با ناحیه محافظ و کوانتیزه با جابجایی فاز[۴۰]، مورد مطالعه قرار گیرد. در ادامه، مدل سیستم و مفروضات بیان می‌گردند.

۲-۱- روش‌های کوانتیزاسیون فاز

در این بخش، بر مبنای مرجع [۳۰] روش‌های کوانتیزاسیون و استخراج بیت از کمیت فاز کانال را ارائه می‌دهیم. البته این روش‌ها، با اندکی تغییر برای استخراج کلید از سایر ویژگی‌های کانال نیز قابل پیاده‌سازی هستند. در این راستا، در ابتدا رویکرد کوانتیزاسیون مستقیم را ارائه می‌کنیم و خواهیم گفت که چرا این رویکرد منجر به نرخ خطای بالا می‌شود و در نتیجه به کدهای تصحیح خطای قوی در فاز اصلاح اطلاعات نیاز دارد. سپس دو روش کوانتیزاسیون با نواحی محافظ و کوانتیزاسیون با جابجایی فاز را معرفی خواهیم کرد که نرخ خطای کلید کمتری دارند.

۱) کوانتیزاسیون مستقیم: در این روش، فازهای بدست آمده در هر گره قانونی مستقیماً کوانتیزه می‌شوند. این موضوع توسط یک دمدولاتور PSK تحقق می‌یابد. در شکل ۱، نمایشی از تعداد زیادی مشاهدات کانال در یک صفحه مختلط و تخمین‌های نویزی آنها ارائه شده است. با در نظر گرفتن چهار ناحیه در صفحه مختصات به عنوان نواحی کوانتیزاسیون[۴۱] (QR) یا نواحی تصمیم، واضح است که مقادیر در نواحی مرزی، مستعدترین مقادیر به تصمیم‌گیری اشتباه هستند. بنابراین یک رویکرد کوانتیزه کردن هوشمند می‌تواند نمونه‌های واقع شده در نواحی مرزی را دور بریزد (با تعریف GB، فاصله‌ی بین QRها افزایش می‌یابد) یا این مقادیر را جابجا کند تا در میانه‌ی QR قرار گیرند.

۲) کوانتیزاسیون با نواحی محافظ: مشخص است که نرخ خطای بیت عمدتاً به دلیل مقادیر کانال نزدیک به نواحی مرزی است. بنابراین با تعریف نواحی مرزی، نواحی کوانتیزاسیون یا QRها را تفکیک می‌کنیم تا آن مقادیری از کانال را که سبب اختلاف بین نمونه‌های دریافتی آلیس و باب می‌شوند، کاهش داده شوند. متذکر می‌شویم در حالتی‌که با فاز سروکار داریم GBها 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، $N_{av} \le \left(1-\frac{\psi M}{2\pi}\right)\log_2 M$ خواهد شد که M و ψ به ترتیب تعداد QRها و عرض ناحیه محافظ هستند.
از نقطه نظر امنیت، این سؤال مطرح می‌شود که هر گره چگونه می‌تواند گره دیگر را مطلع کند که یک کاوش کانال می بایست دور ریخته شود، بدون آنکه محرمانگی کاهش یابد؟ در واقع، همان‌طوری‌که QRها هم احتمال هستند، GBها نیز هم احتمال هستند. در این مورد، در فاز گفتگوی عمومی، هر گره می‌تواند اعلام کند که کدام کاوش، کوانتیزه شود و کدامیک دور ریخته شود. در طرح ارائه شده در این مقاله، در ابتدا، گره‌ی مرجع، کاوش‌های مورد قبول را با ارسال اندیس‌های مربوطه اعلام می‌کند و سپس گره مقابل نیز چنین انجام می‌دهد. بدین طریق، بر روی آن کاوش‌هایی که در فرآیند استخراج بیت‌های مخفی مورد استفاده قرار می‌گیرد، توافق می‌کنند. از منظر عملکرد، واضح است که که GBهای بزرگتر، احتمال اختلاف کلید (P_{SKD}) کمتری را نتیجه می‌دهد؛ چرا که کاوش‌های کانال مشکوک بیشتری دور ریخته می‌شوند. بنابراین در این مورد، یک مصالحه بین کارایی و کارآمدی[۴۲] وجود دارد. بنابراین، این ایده مطرح می‌شود که

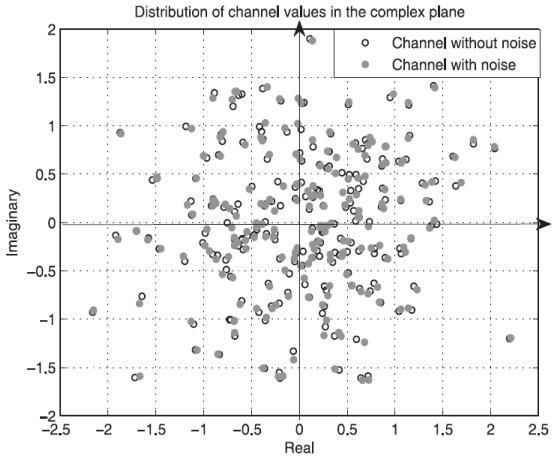
یک P_{SKD} هدف در نظر گرفته شود و سپس دستیابی به بیشترین تعداد بیت‌های مخفی مدنظر باشد. به عنوان مثال، می‌توان P_{SKD} هدف برای هر نمونه مستخرج از کاوش کانال 10^{-3} تعیین کرد و سپس بهینه مقدار زاویه GB و نیز تعداد سطوح کوانتیزاسیون را به گونه‌ای تعیین کرد که بیشترین تعداد بیت‌های مخفی بدست آید.

۳) کوانتیزاسیون با جابجایی فاز: بطور شهودی قابل استنتاج است که روش کوانتیزاسیون با GB از منظر کارآمدی استخراج کلید، بهینه نیست. در واقع، در این رویکرد، آن مقادیر از کانال که در GBها قرار می‌گیرند به سادگی نادیده گرفته شده و در فرآیند کوانتیزاسیون لحاظ نمی‌شوند. این موضوع، منجر به کاهش میانگین تعداد بیت‌های مخفی استخراج شده می‌گردد. بنابراین به منظور دستیابی به کارآمدی بالا در استخراج کلید، نباید کانال‌ها با بهره کافی را دور بریزیم. بر این اساس، یک رویکرد جدید برای کاهش خطا در کوانتیزاسیون کانال پیشنهاد می‌شود. ایده به این صورت است که مسئله کوانتیزاسیون به یک مسئله دمدولاسیون معمولی تبدیل می‌شود به طوری‌که در آن، مقادیر کانال‌ها به جای پراکندگی تصادفی، در اطراف نقاط فضای منظومه پخش می‌شوند. از این رو، بدون نیاز به GB می‌توان کوانتیزاسیون مستقیم را پیاده کرد. به منظور فهم بهتر این روش، فرض کنید θ_1 و θ_2 به ترتیب فاز کانال قانونی تخمین زده شده در آلیس و باب باشند. همچنین $\hat{\theta}$ فاز بدست آمده پس از دمدولاسیون PSK باشد (در واقع $\hat{\theta}$ یک نقطه در فضای منظومه است). در این روش، ابتدا آلیس پس از محاسبه θ_1 و $\hat{\theta}$، فاز تفاضلی $\mu = \theta_1 - \hat{\theta}$ را در فاز گفتگوی عمومی برای باب ارسال می‌کند. همیشه فرض می‌شود که یک کانال عاری از خطا[۴۳] برای ارسال μ به باب وجود دارد. متعاقباً باب، بعد از تخمین کانال قانونی، فاز خودش را به صورت زیر اصلاح می‌کند:

$$\theta_2' = \theta_2 - \mu = \Delta\theta + \hat{\theta} \qquad (۱)$$

که $\Delta\theta = \theta_2 - \theta_1$ معرف خطای مرکب از تخمین فاز در آلیس و باب است. از نقطه نظر امنیتی، ممکن است این سوال ایجاد شود که این روش، چقدر امن است؟ پاسخ این است از آنجایی‌که فاز کانال، تصادفی با توزیع یکنواخت است، ارسال کمیت تفاضل فاز بر روی کانال عمومی هیچ اطلاعاتی را در مورد فاز مربوطه افشا نمی‌کند. در واقع، تنها این اطلاعات در اختیار شنوگر قرار می‌گیرد که فاز کانال به اندازه‌ی μ از یک نقطه در فضای منظومه فاصله دارد. اما، چون نقاط فضای منظومه هم‌احتمال هستند، هیچ اطلاعات اضافی در اختیار شنودگر قرار نمی‌گیرد. از این رو، در فاز گفتگوی عمومی، تفاضل فاز μ و اندیس‌های کانال‌هایی که به واسطه بهره بالا کوانتیزه می شوند، ارسال می‌گردند.

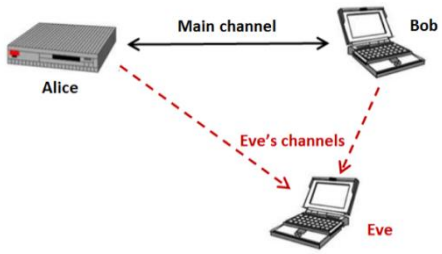
از منظر عملکرد، زمانی در فرآیند استخراج کلید خطا رخ می‌دهد که $|\Delta\theta| > \frac{\pi}{M}$ باشد که M تعداد سطوح کوانتیزاسیون (تعداد QRها) است. مشابه کوانتیزاسیون با GB، می‌توان یک الگوریتم کوانتیزاسیون تطبیقی ارائه داد که در آن تعداد QRها بسته به بهره کانال تغییر کند. در واقع، برای یک P_{SKD} هدف (مثلاً 10^{-3}) به ازای هر مشاهده کانال، می‌توان تعداد بهینه QRها را یافت.



شکل (۱): نمایشی از چندین تحقق کانال و تخمین نویزی آنها در فضای مختلط

۲-۲- مدل سیستم و کاوش کانال

مطابق شکل ۲، مدل سیستم مورد مطالعه، شامل یک جفت کاربر قانونی (آلیس و باب) و یک شنودگر (ایو) است که همگی یک آنتن دارند.



شکل (۲): مدل سیستم

همان‌طوری‌که می‌دانیم آنتروپی بیت‌های مستخرج از کوانتیزاسیون CSI زمانی به مقدار بیشینه خود می‌رسد که توزیع یکنواخت داشته باشد [۲۹]. از این جهت، روش‌های مبتنی بر دامنه (شامل RSS، پوش سیگنال و فاصله) که از کوانتیزه کننده یکنواخت بهره می‌برند، آنتروپی محرمانگی[۴۴] کمتری خواهند داشت؛ چرا که توزیع تخمین دامنه، یکنواخت نیست. در نتیجه، بعد از کوانتیزاسیون یکنواخت، بیت‌ها غیر هم‌احتمال خواهند شد. از منظر مقایسه، فاز کانال به طور کلی توزیع یکنواخت دارد و لذا کلیدهای تولید شده، آنتروپی محرمانگی بالاتری دارند (کلیدهای تولید شده، میزان تصادفی بودن بالاتری دارند). بنابراین روش‌های مبتنی بر فاز از نقطه نظر آنتروپی محرمانگی، ترجیح داده می‌شوند[۴۵]. بر این اساس در این مقاله، بر تولید کلید مبتنی بر فاز تمرکز داریم. بدین صورت که آلیس و باب سمبل‌ها با فاز تصادفی گسسته را از فضای منظومه[۴۶] BPSK انتخاب و به طور متقابل برای یکدیگر ارسال می‌کنند. برای $u \in \{A, B\}$، فاز سمبل ارسالی توسط کاربر u عبارت است از:

$$\phi_u = \pi\, i_u \qquad (۲)$$

که اندیس $i_u \in \{0,1\}$ به صورت تصادفی توسط کاربران انتخاب می‌شود.

فرض می‌کنیم L بار کاوش کانال صورت گیرد تا در نهایت، کلید خام حاصل شده برای آلیس (K_A) و برای باب (K_B) طول دلخواه L بیت داشته باشد. همچنین، اگر کانال آلیس-باب با ϕ_{AB} و فاز کانال باب-آلیس با ϕ_{BA} نمایش داده شود، با در نظر گرفتن زمان سوئیچینگ بین آلیس و باب و پویایی کانال، برای سادگی می‌توان $\phi_{BA} = \phi_{AB} + \Delta\phi$ را در نظر گرفت.

توجه۱ (هم‌پاسخی ضعیف کانال قانونی): در عمل، CSI تخمین زده شده توسط آلیس و باب با یکدیگر تفاوت دارد و در نتیجه هم‌پاسخی ضعیف کانال قانونی رخ خواهد داد. دلایل این موضوع عبارتند از: ۱) عملکرد نیمه دوطرفه[۴۷] گره‌ها که به موجب آن، CSI با یک تأخیر زمانی توسط آلیس و باب تخمین زده می‌شود. در اینجا، تحرک محیط، منجر به تغییرات کانال می‌شود، ۲) وجود خطای تخمین غیرقابل اجتناب، ۳) تفاوت در سخت‌افزار گره‌ها که به موجب آن، انحرافات سخت‌افزاری آنها متفاوت خواهد بود. به عنوان مثال، در سیستم‌های مخابراتی، اختلاف در اسیلاتور گره‌ها، CFO را به همراه دارد.

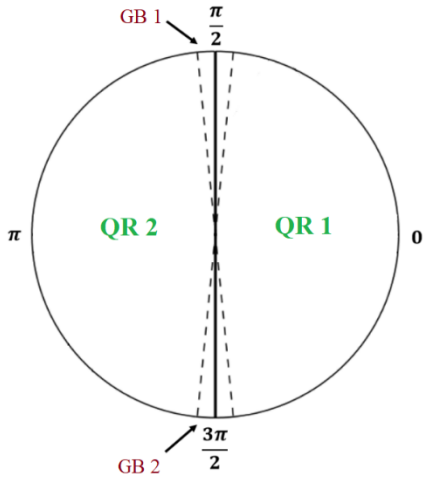
توجه۲ (اثر CFO): بدلیل شرایط محیطی مانند دما و ...، اسیلاتورهای فرستنده و گیرنده، انحراف فرکانسی از فرکانس مرکزی f_c را تجربه می‌کنند. اگر دقت اسیلاتور α [ppm] باشد، در اینصورت حداکثر انحراف فرکانسی برابر خواهد شد با:

بعنوان مثال برای $f_c = 500\ MHz$ و $\alpha = 1.5\ [ppm]$، بیشترین انحراف فرکانسی برابر با $f_\Delta = 750$ Hz خواهد شد که مشاهده می‌شود در مقایسه با f_c ناچیز است. این بدان معناست که خروجی مخلوط کننده[۴۸] دارای فرکانسی در بازه $f_c \pm f_\Delta$ خواهد بود. با این توضیح، اگر انحراف فرکانس‌های اسیلاتورهای آلیس و باب از فرکانس مرکزی به ترتیب با Δf_A و Δf_B نمایش داده شود، در اینصورت با عنایت به رابطه فاز $\phi = 2\pi\left(\frac{df}{c} - \left\lfloor\frac{df}{c}\right\rfloor\right)$، فاز کانال دیده شده در آلیس (ϕ_{BA}) و باب (ϕ_{AB}) قابل محاسبه خواهد بود. حال می‌خواهیم ببینیم با وجود آنکه $f_c \gg \Delta f_A, \Delta f_B$، آیا می‌توان گفت ϕ_{AB} و ϕ_{BA} بسیار نزدیک هستند یا خیر؟ با دو مثال، این موضوع را بررسی می‌کنیم. فرض می‌کنیم $\alpha = 1.5\ [ppm]$ و فاصله آلیس و باب $d = 10\ km$ باشد:

۱- اگر $f_c = 300\ MHz$ باشد: در این شرایط، $f_\Delta = 450$ Hz خواهد شد. حال بدترین شرایط را برای انحراف فرکانسی اسیلاتورها در نظر بگیریم، یعنی $\Delta f_A = 450$ Hz و $\Delta f_B = -450$ Hz. با این کمیت‌ها، داریم $\phi_{BA} = 5.4^o$ و $\phi_{AB} = 360^o - 5.4^o$. لذا خواهیم داشت $\Delta\phi = \phi_{BA} - \phi_{AB} = 10.8^o$.

۲- اگر $f_c = 500\ MHz$ باشد: در این شرایط، $f_\Delta = 750$ Hz شده و نیز برای بدترین حالت، $\Delta f_A = 750$ Hz و $\Delta f_B = -750$ Hz خواهد شد. با این کمیت‌ها، $\phi_{BA} = 249^o$ و $\phi_{AB} = 231^o$. لذا خواهیم داشت $\Delta\phi = \phi_{BA} - \phi_{AB} = 18^o$.

دو مثال فوق بیان می‌کنند که برای فرکانس کاری زیاد، بیشینه اختلاف فاز بین ϕ_{AB} و ϕ_{BA} (وقتی انحراف فرکانسی دو اسیلاتور در بدترین حالت ممکن باشد) در حدود 20^o خواهد بود و برای فرکانس‌های کاری پایین‌تر، این مقدار کمتر خواهد شد. همچنین می‌توان دید که برای فواصل کمتر بین آلیس و باب مثلا $d = 1\ km$، اختلاف فاز $\Delta\phi$ برای هر دو فرکانس مرکزی ذکر شده، در حدود 1^o خواهد شد. بنابراین فاز کانال آلیس و باب یعنی ϕ_{BA} و ϕ_{AB} اگر چه به یکدیگر نزدیک خواهند بود ولی اختلاف فاز $\Delta\phi$ ثابتی را تجربه خواهیم کرد. اثر این مؤلفه را بر روی کارایی کلید تولید شده خواهیم دید. خوب است ذکر شود که پدیده داپلر نیز بر روی CFO اثر می‌گذارد.



شکل (۳): کوانتیزه کننده تک بیتی با نواحی محافظ

۲-۳- کوانتیزاسیون فاز

در گیرنده، مشاهدات همبسته، کوانتیزه می‌شوند تا دنباله‌های باینری تولید شوند. انتخاب یک الگوریتم کوانتیزه کننده مناسب می‌تواند KMR را بیشتر کاهش دهد. به عبارت دیگر، بسته به تعداد QRها (مرتبه کوانتیزاسیون)، کیفیت و کمیت کلید مخفی خام تعیین می‌شود. هر چه تعداد QRها بیشتر باشد، نرخ تولید کلید بیشتر می‌شود. با این حال، برای تعداد نواحی بسیار زیاد، اختلاف کلید قابل ملاحظه خواهد بود. یک مصالحه برای برقراری تعادل بین نرخ تولید کلید و KMR، بکارگیری GB برای کوانتیزاسیون است. در این مقاله، از الگوریتم متداول کوانتیزاسیون تک بیتی[۴۹] با GB [۳۱] و [۳۲] استفاده استفاده می‌کنیم که عرض باند آن ψ در نظر گرفته می‌شود[۵۰]. شکل ۳، کوانتیزه کننده تک بیتی مدنظر را به تصویر کشیده است. همانطوری که مشخص است، علاوه بر دو ناحیه کوانتیزاسیون QR 1 و QR 2، دو ناحیه محافظ GB1 و GB 2 به ترتیب حوالی $\frac{\pi}{2}$ و $\frac{3\pi}{2}$ وجود دارد. در خروجی این کوانتیزه کننده، برای آلیس و باب به ترتیب، بیت

(قطعه کلید) k_A و k_B تولید می‌شود. 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.

قرارداد می‌کنیم که در هر بار کاوش کانال، اگر فاز بدست آمده در آلیس ($\hat{\theta}_A$) یا باب ($\hat{\theta}_B$) در QR 1 قرار گیرد بیت صفر و اگر در QR 2 واقع شود، بیت یک آشکار می‌گردد. توجه شود که اطلاعات مربوط به کوانتیزاسیون شامل مرتبه و بازه‌ی GBها، به صورت عمومی بین کاربران قانونی به اشتراک گذاشته می‌شود.

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

- پیشامد ۱: $\hat{\theta}_A$ و $\hat{\theta}_B$ به یک بیت یکسان کوانتیزه شوند.
- پیشامد ۲: $\hat{\theta}_A$ و $\hat{\theta}_B$ به بیتهای غیریکسان کوانتیزه شوند.
- پیشامد ۳: هر کدام از $\hat{\theta}_A$ یا $\hat{\theta}_B$ در GB قرار گیرد.

توجه شود که تنها آن نمونه‌هایی که در پیشامد ۱ یا ۲ قرار گیرند، قابل استفاده خواهند بود. اگر در مرحله‌ای از کاوش کانال، پیشامد ۳ واقع شود، $\hat{\theta}_A$ و $\hat{\theta}_B$ متناظر می‌بایست دور ریخته شود تا کلیدهای بدست آمده جهت تحویل به مرحله اصلاح اطلاعات (یعنی کلیدهای خام K_a و K_b)، طول یکسانی داشته باشند. جهت تحقق این موضوع، در یک گفتگوی عمومی، اندیس‌های مربوط به نمونه‌های غیرمفید، بین آلیس و باب مبادله می‌شود. از منظر ریاضیاتی، احتمالات پیشامدهای فوق بصورت زیر قابل بیان هستند:

$$\begin{aligned} P_1 &= P_r\{\hat{\theta}_A, \hat{\theta}_B \in \text{QR } 1\} \\ &\quad + P_r\{\hat{\theta}_A, \hat{\theta}_B \in \text{QR } 2\} \\ &= 2P_r\{\hat{\theta}_A, \hat{\theta}_B \in \text{QR } 1\} \end{aligned} \quad (۳)$$

که تساوی دوم به دلیل یکنواختی فازهای تزریقی توسط آلیس و باب و نیز فاز کانال برقرار است. به طور مشابه داریم:

$$\begin{aligned} P_2 &= P_r\{\hat{\theta}_A \in \text{QR } 1\,, \hat{\theta}_B \in \text{QR } 2\} \\ &\quad + P_r\{\hat{\theta}_A \in \text{QR } 2\,, \hat{\theta}_B \in \text{QR } 1\} \\ &= 2P_r\{\hat{\theta}_A \in \text{QR } 1\,, \hat{\theta}_B \in \text{QR } 2\} \end{aligned} \quad (۴)$$

و در نهایت، با استدلالی مشابه، می‌توان بیان کرد:

$$\begin{aligned} P_3 &= P_r\{\hat{\theta}_A \in GB\} + P_r\{\hat{\theta}_B \in GB\} \\ &\quad - P_r\{\hat{\theta}_A \in GB\,, \hat{\theta}_B \in GB\} \\ &= 2\,P_r\{\hat{\theta}_A \in GB\} \\ &\quad - P_r\{\hat{\theta}_A \in GB\,, \hat{\theta}_B \in GB\} \end{aligned} \quad (۵)$$

که GB بیانگر اجتماع GB 1 و GB 2 است. توجه شود که $P_3 = 1 - P_1 - P_2$. می‌توان به سادگی نتیجه‌گیری کرد که P_1 بیانگر احتمال تولید یک بیت قطعه‌کلید یکسان در آلیس و باب، با استفاده از یک نمونه کاوش کانال است؛ اما توجه شود که $P_{1,2} = P_1 + P_2$ برای ما مهم است چرا که $P_{1,2}$ بیانگر میزان نمونه‌های قابل بهره‌برداری از بین تمام نمونه‌ها، جهت استخراج کلید می‌باشد. بنابراین، رابطه دقیق و به شکل بسته برای KMR بصورت زیر قابل بیان است:

$$P_{KM} = \frac{P_2}{P_1 + P_2} \quad (۶)$$

در واقع، اگر P_{KM} از یک آستانه‌ی مشخص (قدرت تصحیح خطای کدینگ) کمتر باشد، بیت‌های خطا در مرحله اصلاح اطلاعات تصحیح می‌شوند که این به آن معناست که کل کلید خام، قابل بهره‌برداری خواهد بود. بنابراین، $P_{1,2}$ زیاد و در نتیجه KMR کم، مطلوب است.

همان‌طوری‌که در ادامه خواهیم دید، موارد ذکر شده در توجه ۱و ۲، KMR را افزایش می‌دهد. در این بین، بکارگیری GB ایده‌ی مناسبی است که تأثیر مخرب هم‌پاسخی ضعیف را کاهش می‌دهد.

۲-۴- طرح استخراج کلید

به منظور استخراج کلید، هر یک از کاربران، ابتدا فاز دریافتی از کاربر مقابل (مجموع فاز سمبل ارسالی و فاز کانال) را با فاز سمبل انتخابی خودش، جمع کرده و بعد از کوانتیزه کردن، پیمانه‌ی دو آن را بدست می‌آورد. در نتیجه آلیس و باب به ترتیب با تخمین فازهای $\hat{\theta}_A = \phi_A + \phi_B + \phi_{BA} + \epsilon_A$ و $\hat{\theta}_A = \phi_A + \phi_B + \phi_{BA} + \epsilon_A$ به قطعه کلیدهای زیر دست خواهند یافت:

$$k_A \overset{2}{=} Q(\hat{\theta}_A) \quad (۷)$$

$$k_B \overset{2}{=} Q(\hat{\theta}_B) \quad (۸)$$

که $k_A, k_B \in \{0,1\}$ و تابع $Q(x) = \left\lfloor \frac{x}{\pi} + \frac{1}{2} \right\rfloor$ و $\theta = \phi_A + \phi_B + \phi_{AB}$ بیانگر عملیات کوانتیزاسیون است. $\lfloor . \rfloor$ نیز نماد 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. پر واضح است که در شرایط ایده‌آل ($\epsilon_A = \epsilon_B = 0$) و نیز هم‌پاسخی کامل کانال، طبق روابط (۷) و (۸)، آلیس و باب به قطعه کلید برابر می‌رسند. حال آلیس و باب مقادیر زیر را محاسبه می‌کنند (در پیمانه ۲):

$$\begin{aligned} k_m &\triangleq \left\lfloor \frac{\hat{\theta}_m}{\pi} + \frac{1}{2} \right\rfloor, k_m^+ \triangleq \left\lfloor \frac{\hat{\theta}_m + \frac{\psi}{2}}{\pi} + \frac{1}{2} \right\rfloor, \\ k_m^- &\triangleq \left\lfloor \frac{\hat{\theta}_m - \psi/2}{\pi} + \frac{1}{2} \right\rfloor \end{aligned} \quad (۹)$$

سپس آلیس و باب، قطعات کلید یک بیتی خود را به‌صورت زیر محاسبه می‌کنند:

$$k_m = \begin{cases} k_m & if \quad k_m^+ = k_m^- \\ \emptyset & Otherwise, \end{cases} \quad (۱۰)$$

در این رابطه، $\emptyset$ بیانگر دور ریختن نمونه مربوطه است. همان‌طوری‌که پیش‌تر شرح دادیم برای وضعیت $\emptyset$، کاربر مورد نظر طی یک پروتکل به کاربر مقابل اطلاع می‌دهد که او هم مقدار k_m خودش را برابر با $\emptyset$ قرار دهد. به این ترتیب، وقتی مقدار $\hat{\theta}_A$ یا $\hat{\theta}_B$ در نواحی محافظ قرار داشته باشد، از این مقادیر برای تولید کلید استفاده نمی‌شود. در رابطه فوق مشخص است که به واسطه پیمانه ۲ بودن، $k_m \in \{0,1\}$ و لذا در حوزه باینری خواهد بود.

۳- تحلیل عملکردی کلید اخذ شده بین آلیس و باب

در این بخش، در ابتدا، معیارهای ارزیابی طرح تولید کلید را معرفی کرده و سپس انها را برای طرح SKG پیشنهادی در این مقاله مورد تجزیه و تحلیل قرار می‌دهیم.

۳-۱- تحلیل کارایی طرح تولید کلید پیشنهادی:

در این بخش، یک رابطه‌ی بسته برای KMR و KDR به دست می‌آوریم. با کمک معیار KMR، میزان اختلاف کلیدهای خام و با کمک KDR، نرخ تولید کلید خام به سادگی قابل محاسبه خواهد بود. برای نیل به این هدف، ابتدا قضیه زیر را مطرح می‌کنیم.

قضیه: اگر $\phi \sim U[0,2\pi)$ باشد، در اینصورت برای مقادیر ثابت ϕ_L و ϕ_U، احتمال $P_r\{\phi_L < \phi < \phi_U\}$ برابر خواهد شد با:

$$P_r\{\phi_L < \phi < \phi_U\} = \begin{cases} F(\phi_U) - F(\phi_L) & ;\phi_U > \phi_L \\ 1 - F(\phi_L) + F(\phi_U) & ;\phi_L > \phi_U \end{cases} \quad (۱۱)$$

که $F(.)$ بیانگر تابع توزیع تجمعی متغیر تصادفی ϕ است.

اثبات: برای $\phi_L > \phi_U$ که بدیهی است. برای $\phi_L > \phi_U$، می‌توان این پیشامد را به صورت اجتماع دو پیشامد $\phi_L < \phi < 2\pi$ و $0 < \phi < \phi_U$ نوشت. در این صورت،

$$P_r\{\phi_L < \phi < \phi_U = F(2\pi) - F(\phi_L) + F(\phi_U) - F(0) \quad (۱۲)$$

که در آن $F(2\pi) = 1$ و $F(0) = 0$ است. □

برمبنای مرجع [۲۵]، گفتیم که آلیس و باب فاز $\hat{\theta}_m = \theta_m + \epsilon_m$ را بدست خواهند آورد که در آن ϵ خطای تخمین است. اگر SNR کاوش کانال پایین و متوسط باشد، خطای فاز دارای توزیع Tikhonov و برای SNR بالا، خطای فاز توزیع نرمال خواهد داشت [۲۵]. در این مقاله، ما بر روی SNRهای بالا تمرکز می‌کنیم و همانطوری که در شبیه‌سازی‌ها خواهیم دید، در SNRهای پایین‌تر نیز، تحلیل‌های ارائه شده دقت خوبی خواهند داشت. بنابراین، برای مقادیر زیاد SNR کاوش کانال ($\gamma \gg 1$) و با فرض اینکه کاوش‌ها توسط دو گره با توان برابر اتفاق بیفتد و نویز نیز در آنها برابر است، تابع چگالی احتمال[۵۱] (PDF) متغیر تصادفی $\hat{\theta}_m$ آن برابر خواهد بود با:

$$f_{\hat{\theta}_m}(t) = \frac{1}{\sigma(\gamma)\sqrt{2\pi}} e^{-\frac{(t-\theta_m)^2}{2\,\sigma^2(\gamma)}} \quad (۱۳)$$

که واریانس $\sigma(\gamma)$ تابعی از SNR کاوش کانال بوده و با دقت بسیار بالایی می‌توان انحراف معیار $\sigma(\gamma)$ را با $\sigma(\gamma) \approx \sqrt{\frac{2}{2\gamma+1}}$ تقریب زد [۲۵]. توجه شود که γ به توان سیگنال کاوش کانال و نویز در گیرنده ربط دارد.

۳-۱-۱- نرخ عدم تطبیق قطعه کلید:

عدم تطبیق قطعه کلید $k_A \neq k_B$، وقتی رخ می‌دهد که $(k_A = 0, k_B = 1)$ یا $(k_A = 1, k_B = 0)$ باشد. بدلیل برابری توزیع احتمال خطای فاز در آلیس و باب و نیز هم پاسخی کانال قانونی، می‌توان KMR را بصورت زیر محاسبه کرد:

$$\begin{aligned} P_{KM} &= 2\,P_r\{k_A = 0, k_B = 1\} \\ &= 2P_r\{GB_{2U} \le \phi_{BA} + \varepsilon_A \\ &< GB_{1L}, GB_{1U} \le \phi_{AB} + \varepsilon_B \\ &< GB_{2L}\} \end{aligned} \quad (۱۴)$$

که در آن کران‌های پایین و بالا برای GBهای ۱ و ۲ به ترتیب عبارتند از: $GB_{1L} = \frac{\pi}{2} - \frac{\psi}{2}$، $GB_{1U} = \frac{\pi}{2} + \frac{\psi}{2}$ و نیز $GB_{2L} = \frac{3\pi}{2} - \frac{\psi}{2}$ و $GB_{2U} = \frac{3\pi}{2} + \frac{\psi}{2}$. برای محاسبه احتمال بالا، ابتدا بر روی ϕ_{AB} شرطی کرده و سپس بر روی آن متوسط‌گیری می‌کنیم. با این توضیح، با توجه به آنکه ϕ_{AB} دارای توزیع یکنواخت $U[0,2\pi)$ است، داریم:

$$\begin{aligned} P_{KM} = 2\,\mathrm{E}_{\phi_{AB}}(&P_r\{GB_{2U} \le \phi_{BA} + \varepsilon_A \\ &< GB_{1L}|\phi_{AB}\}.P_r\{GB_{1U} \\ &\le \phi_{AB} + \varepsilon_B < GB_{2L}|\phi_{AB}\}) \end{aligned} \quad (۱۵)$$

که تجزیه شدن احتمال فوق، به‌دلیل استقلال دو پیشامد است که آن نیز به دلیل استقلال خطاهای فاز ε_A و ε_B می‌باشد. با کمک قضیه ۱ و با عنایت به آنکه $\phi_{BA} = \phi_{AB} + \Delta\phi$ (که $\Delta\phi$ ثابت است)، احتمال اول در رابطه (۱۵) به صورت زیر محاسبه می‌شود:

$$\begin{aligned} &P_r\{GB_{2U} \le \phi_{BA} + \varepsilon_1 < GB_{1L}|\phi_{AB}\} = \\ &\int_{GB_{2U}}^{2\pi} \frac{1}{\sigma(\gamma)\sqrt{2\pi}} e^{-\frac{(p-\phi_{BA})^2}{2\,\sigma^2(\gamma)}}\,dp \\ &\quad + \int_{0}^{GB_{1L}} \frac{1}{\sigma(\gamma)\sqrt{2\pi}} e^{-\frac{(p-\phi_{BA})^2}{2\,\sigma^2(\gamma)}}\,dp \\ &= \frac{1}{2}\left(\mathrm{erf}\left(\frac{\phi_{BA} - GB_{2U}}{\sigma(\gamma)\sqrt{2}}\right)\right. \\ &\quad - \mathrm{erf}\left(\frac{\phi_{BA} - 2\pi}{\sigma(\gamma)\sqrt{2}}\right) \\ &\quad + \mathrm{erf}\left(\frac{\phi_{BA}}{\sigma(\gamma)\sqrt{2}}\right) \\ &\quad \left. - \mathrm{erf}\left(\frac{\phi_{BA} - GB_{1L}}{\sigma(\gamma)\sqrt{2}}\right)\right) \end{aligned} \quad (۱۶)$$

که $\mathrm{erf}(x) = \frac{2}{\sqrt{\pi}}\int_0^x e^{-t^2}\,dt$. همچنین احتمال دوم به صورت زیر خواهد بود:

$$\begin{aligned} &P_r\{GB_{1U} \le \phi_{AB} + \varepsilon_B < GB_{2L}|\phi_{AB}\} = \\ &\int_{GB_{1U}}^{GB_{2L}} \frac{1}{\sigma(\gamma)\sqrt{2\pi}} e^{-\frac{(p-\phi_{AB})^2}{2\,\sigma^2(\gamma)}}\,dp \\ &= \frac{1}{2}\left(\mathrm{erf}\left(\frac{\phi_{AB} - GB_{1U}}{\sigma(\gamma)\sqrt{2}}\right)\right. \\ &\quad \left. - \mathrm{erf}\left(\frac{\phi_{AB} - GB_{2L}}{\sigma(\gamma)\sqrt{2}}\right)\right) \end{aligned} \quad (۱۷)$$

با قرار دادن (۱۶) و (۱۷) در (۱۵) و سپس انتگرال‌گیری بر روی ϕ_{AB} که دارای توزیع U[0,2π] است، به یک رابطه انتگرالی برای P_{KM} دست می‌یابیم که برای اختصار، از بیان آن در اینجا صرف‌نظر می‌کنیم.

۳-۱-۲- ارزیابی احتمال دور ریزی کلید:

بعد از آنکه $\hat{\theta}_A$ و $\hat{\theta}_B$ به بیت‌های خام کوانتیزه شدند، چندین مرحله گفتگو نیاز است تا بیت‌های اختلافی حذف گردند و در نتیجه آلیس و باب به کلید یکسانی برسند. برای کوتاه شدن فرآیند گفتگو، می‌توان محدوده GB را افزایش داد تا KMR کاهش یابد. با این حال، طول دنباله بیت خام نیز کاهش می‌یابد. دلیل اینست که با افزایش ψ، نمونه‌های کاوش بیشتری دور ریخته می‌شوند. با توجه به اینکه GB 1 دارای بازه زاویه‌ای با کران پایین LB_1 و کران بالای UB_1 و نیز GB 2 دارای بازه زاویه‌ای با کران پایین LB_1 و کران بالای UB_1 می‌باشد، در اینصورت KDR برابر می‌شود با:

$$P_{KD} = P_r\{\hat{\theta}_A \in GB \quad or \quad \hat{\theta}_B \in GB\} = 2\,(P_1 + P_2 - P_3 - P_4) \tag{۱۸}$$

که $P_1 = P_r\{\hat{\theta}_A \in GB_1\}$، $P_2 = P_r\{\hat{\theta}_B \in GB_1\}$، $P_3 = P_r\{\hat{\theta}_A, \hat{\theta}_B \in GB_1\}$ و $P_4 = P_r\{\hat{\theta}_A \in GB_1, \hat{\theta}_B \in GB_2\}$. با عنایت به اینکه $\hat{\theta}_A$ و $\hat{\theta}_B$ توزیع فاز یکسانی دارند، در محاسبه احتمال فوق از حقایق زیر استفاده شده است:

۱) $P_r\{\hat{\theta}_A \in GB\} = P_r\{\hat{\theta}_B \in GB\} = 2\,P_r\{\hat{\theta}_A \in GB_1\} = 2P_1$.

۲) $P_r\{\hat{\theta}_A, \hat{\theta}_B \in GB\} = P_r\{\hat{\theta}_A, \hat{\theta}_B \in GB_1\} + P_r\{\hat{\theta}_A, \hat{\theta}_B \in GB_2\} + P_r\{\hat{\theta}_A \in GB_1, \hat{\theta}_B \in GB_2\} + P_r\{\hat{\theta}_A \in GB_2, \hat{\theta}_B \in GB_1\}$

و بعلاوه $P_r\{\hat{\theta}_A, \hat{\theta}_B \in GB_1\} = P_r\{\hat{\theta}_A, \hat{\theta}_B \in GB_2\}$ و نیز $P_r\{\hat{\theta}_A \in GB_1, \hat{\theta}_B \in GB_2\} = P_r\{\hat{\theta}_A \in GB_2, \hat{\theta}_B \in GB_1\}$.

محاسبه P_1، P_2، P_3 و P_4 مشابه قبل است.

۳-۱-۳- نرخ تولید کلید خام:

فرض کنید فرکانس نمونه برداری کانال در دو کابر f_S باشد. در این صورت RKGR بصورت زیر تعریف می‌شود:

$$R_{raw} = f_S(1 - P_{KD}) \tag{۱۹}$$

از آنجایی‌که افزایش ψ منجر به کاهش هر دوی KMR و R_{raw} می‌شود، انتخاب ψ برای برقراری تعادل بین نیازمندی‌های KMR و RKGR بسیار مهم است. اگر سیستم، به عنوان مثال یک ایستگاه پایه، قابلیت تصحیح خطای بالایی داشته باشد و نرخ تولید کلید بالا، مطلوب آن باشد، در اینصورت KMR یک معیار مطلوب نیست و در عوض یک ψ کوچک ترجیح داده می‌شود. در کاربردهای دیگر، به عنوان مثال، یک شبکه حسگر بی‌سیم، با توانایی پردازش داده پایین و الزامات نرخ کلید پایین، ابتدا باید کارایی KMR برآورده شود و بنابراین مقدار ψ باید به درستی افزایش یابد.

۴- نتایج شبیه‌سازی

در این بخش، با ارائه نمودارهایی، به راستی آزمایی روابط تحلیل ارائه شده در این مقاله برای KMR و KDR می پردازیم. بدین منظور، نتایج تحلیلی همراه با نتایج شبیه‌سازی رسم می‌گردند. همچنین بینش‌های مهندسی خوبی برای طراحی PLSKG پیشنهادی ارائه می‌گردد.

در شکل ۴، تأثیر عرض GB (به ازای $\psi = 0, \frac{\pi}{64}, \frac{\pi}{16}$) و نیز تأثیر میزان هم‌پاسخی کانال قانونی ($\Delta\phi = 0$ برای هم‌پاسخی ایده‌آل و $\Delta\phi = \frac{\pi}{16}$ برای هم‌پاسخی ضعیف) بر روی احتمال نابرابری کلیدها (KMR) نشان داده شده است. همان طوری‌که مشخص است برای SNRهای بیشتر از 10 dB، نمودارهای تحلیلی با نمودارهای حاصل از شبیه‌سازی طرح تولید کلید پیشنهادی، در تطابق خوبی هستند که این مشاهده، اعتبار تحلیل‌های ارائه شده را برای SNRهای متوسط و پایین نیز بیان می‌کند.

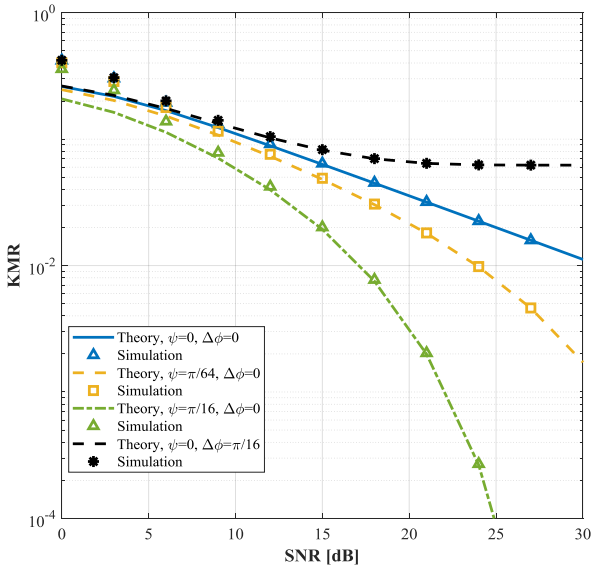
همچنین از این شکل متوجه می‌شویم که:

۱) با افزایش SNR کاوش کانال (و در نتیجه کاهش خطای تخمین کانال)، معیار KMR کاهش می‌یابد که یک نتیجه بدیهی است.

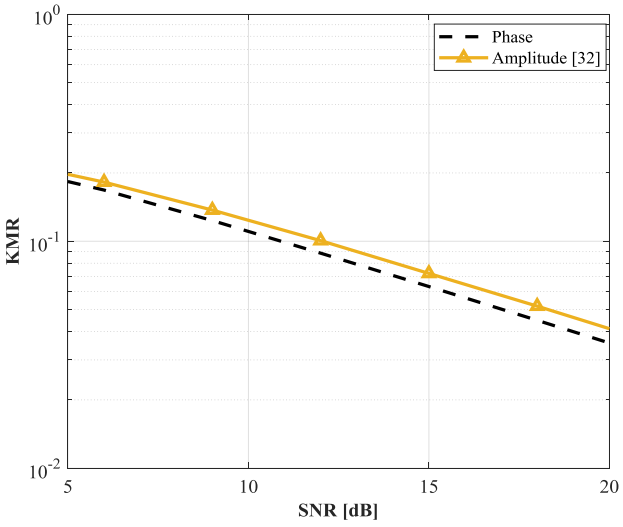
۲) با افزایش مقدار عرض باند ψ، معیار KMR سریعتر کاهش می‌یابد. دلیل اینست که با یک احتمالی، برخی نمونه‌های کاوش کانال در مجاورت مرزهای نواحی کوانتیزاسیون قرار می‌گیرند که این نمونه‌ها، ممکن است به خاطر وجود نویز، در نواحی متفاوتی بیفتند و لذا خطای عدم برابری بیت داشته باشیم. وجود GB، این نمونه‌های محتمل به خطا را دور می‌ریزد. توجه شود که $\psi = 0$ معادل با شرایطی است که باند محافظ ناپدید می‌گردد.

۳) برخلاف کانال هم‌پاسخ که با افزایش SNR میزان خطای کلید کمتر می‌شود، وجود هم‌پاسخی ضعیف (با $\Delta\phi = \frac{\pi}{16}$)، معیار KMR را افزایش داده و ضمناً یک وضعیت اشباع رخ می‌دهد. البته توجه شود که همچنان خطا زیر ۱۰٪ هست و این یک حسن است. به عبارت دیگر با کدینگ‌های متداول می‌توان چنین هم‌پاسخی ضعیفی را جبران کرد و به کلید رسید.

در شکل ۵، طرح پیشنهادی در این مقاله (که مبتنی بر فاز کانال است) را با طرح پیشنهادی در مرجع [۳۲] (که مبتنی بر دامنه سمبل‌های کاوش است) مقایسه می‌کنیم. جهت مقایسه منصفانه، عرض باند محافظ $\psi = 0$ قرار داده شده است. همان‌طوری‌که در این شکل مشخص است، طرح پیشنهادی در مقایسه با طرح مرجع [۳۲]، به ازای یک KMR ثابت، حدود 1 dB در SNR کاوش کانال صرفه‌جویی می‌کند.



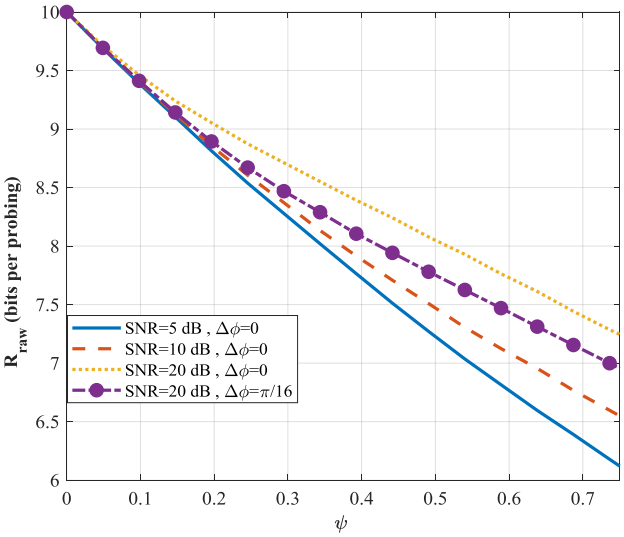
شکل (۴): معیار KMR در برابر SNR سمبل کاوش کانال برای مقادیر مختلف عرض باند محافظ $\psi = 0, \frac{\pi}{64}, \frac{\pi}{16}$ و نیز میزان هم‌پاسخی‌های $\Delta\phi = 0, \frac{\pi}{16}$.



شکل (۵): معیار KMR در برابر SNR سمبل کاوش کانال برای عرض باند محافظ $\psi = 0$ و برای هم‌پاسخی کامل کانال قانونی

شکل ۶، نرخ تولید کلید خام R_{raw} را برحسب عرض باند محافظ ψ نشان می‌دهد. در این شکل، نرخ کاوش کانال $f_s = 10$ و SNR کاوش کانال برابر با مقادیر SNR=5, 10, 20 dB اختیار شده است. این شکل تصدیق می‌کند که با افزایش عرض GB، نرخ تولید کلید کاهش می‌یابد؛ نتیجه‌ای که با مشاهدات در شکل ۴ تفاوت دارد. به عبارت دیگر، از یک طرف می‌بینیم که با افزایش ψ، کارایی KMR بهبود می‌یابد؛ چرا که آن کاوش‌های کانالی که به طور بالقوه، بیت‌های کلید متفاوتی را منجر می‌شوند، قبل از فرآیند کوانتیزاسیون، حذف می‌گردند. از طرف دیگر، برخی نمونه‌های کاوش مفید به اشتباه دور ریخته می‌شوند و متعاقباً طول دنباله کلید به شدت کوتاه می‌شود.

بنابراین متوجه می‌شویم که یک مصالحه بین KMR و RKGR برقرار است. در نتیجه، می‌بایست یک مقدار مناسب برای ψ انتخاب شود تا توازنی بین نیازمندی‌های KMR و RKGR برقرار گردد. این شکل، همچنین بیان می‌کند که با افزایش SNR کاوش کانال، R_{raw} افزایش می‌یابد. حال آنکه، وضعیت هم‌پاسخی ضعیف ($\Delta\phi = \frac{\pi}{16}$) نسبت به هم‌پاسخی ایده‌آل ($\Delta\phi = \frac{\pi}{16}$) نرخ تولید کلید کمتری دارد که البته بدیهی است. نکته دیگری که از این شکل، قابل استنتاج می‌باشد این است که در وضعیت بدون GB ($\psi = 0$)، برای تمام SNRها و تمام شرایط هم‌پاسخی کانال، $R_{raw} = f_s = 10$. دلیل این است که در وضعیت بدون GB، از تمام نمونه‌های کاوش کانال برای تولید کلید استفاده می‌شود و در نتیجه نرخ تولید کلید با نرخ کاوش کانال برابر می‌شود.



شکل (۶): معیار R_{raw} برحسب عرض باند محافظ ψ به ازای SNRهای مختلف کاوش کانال و برای هم‌پاسخی‌های مختلف $\Delta\phi = 0, \frac{\pi}{16}$

۵- نتیجه‌گیری

در این مقاله، یک طرح نوین تولید کلید مبتنی بر تزریق فاز گسسته ارائه گردید که در گیرنده، از کوانتیزه کنندهٔ ساده تک‌بیتی با GB برای استخراج کلید استفاده می‌شود. برخلاف بسیاری از مطالعات صورت گرفته شده، فرض گردید که کانال قانونی از هم‌پاسخی ضعیف رنج برده و نویز نیز بر فاز دریافتی آلیس و باب اثرگذار است. برای چنین سناریویی، روابطی برای KMR و KDR به ازای هر کاوش کانال ارائه شد. همچنین به منظور ارزیابی تأثیر GB بر روی کارایی طرح تولید کلید پیشنهادی، معیار RKGR تعریف شده و محاسبه گردید. نتایج شبیه‌سازی نشان می‌دهند که وجود هم‌پاسخی ضعیف کانال، نرخ خطای بیت را در SNR بالا به وضعیت اشباع می رساند. همچنین مشاهده شد که طرح تولید کلید پیشنهادی مبتنی بر فاز در مقایسه با دامنه حدود 1 dB در SNR صرفه‌جویی می‌کند. نتایج شبیه‌سازی، بینش‌های مهندسی خوبی در جهت بهینه‌سازی پارامترهای طرح تولید کلید ارائه می‌کنند.

حال به منظور توسعه و بهبود طرح پیشنهادی، برخی ایده‌ها جهت ادامه‌ی کار حاضر، ارائه شده است:

- به‌کارگیری رله و نیز صفحات هوشمند بازتاب کننده[۵۲] (IRS) در ارتباطات به بهبود کارایی SKG کمک می‌کند [۳۳]- [۳۵]. 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 یا IRS، بسیار مفید خواهد بود. در چنین سناریویی، می‌بایست یک پروتکل SKG مناسب طراحی و تحلیل گردد. به خصوص وقتی با یک رله یا IRS 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.
- ممکن است در یک شبکه ارتباطی، یک تداخل‌گر و یا جمر وجود داشته باشد [۸] 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. لذا طرح SKG مرسوم عملاً شکست خواهد خورد. بنابراین می‌بایست یک طرح SKG مقاوم در برابر تداخل یا جمینگ طراحی شود.
- پیشنهاد می‌شود نواحی آسیب‌پذیری [۲۵] برای طرح تولید کلید پیشنهادی در این مقاله، با در نظر گرفتن مرحله اصلاح اطلاعات محاسبه شود. چرا که در فاز اصلاح اطلاعات، بخشی از کلید نشت پیدا خواهد کرد و لذا احتمالاً نواحی آسیب‌پذیری، افزایش خواهد یافت.
- در مقاله [۳۱]، ایده‌ی ناحیه محافظ وفقی با تکیه بر یادگیری عمیق ارائه شده است که می‌تواند به عنوان کار آتی برای طرح پیشنهادی در این مقاله، مورد استفاده قرار گیرد.
- روش کوانتیزاسیون با جابجایی فاز، بدلیل کاهش دور ریزی قطعه کلید، نرخ تولید کلید بالاتری ارائه می‌دهد. پیشنهاد می‌شود طرح تزریق فاز گسسته ارائه شده در این مقاله با روش کوانتیزاسیون مذکور مورد بررسی و تحلیل قرار گیرد.
- در این مقاله برای هم‌پاسخی ضعیف کانال قانونی، از مدل ساده‌ای استفاده کرده‌ایم. برای توصیف دقیق‌تر، با کمک مدل Jake داریم [۳۲]:

$$h_{BA} = \rho h_{AB} + \sqrt{1-\rho^2} n_{AB} \qquad (۲۰)$$

که $n_{AB} \sim CN(0, \sigma^2_{h_{AB}})$ معرف خطای معادل ناشی از تأخیر زمانی بوده و مستقل از کانال قانونی است که در آن $\sigma^2_{h_{AB}} = d^{-n}$ با d فاصله بین آلیس و باب، و n مولفه تلف مسیر است. همچنین $0 < \rho \leq 1$ بیانگر ضریب همبستگی بین کانال h_{AB} و h_{BA} است. برای $\rho = 1$ هم پاسخی کامل (ایده‌آل) حاصل خواهد شد. حال اگر هر کدام از گره ها، با خطایی تخمین کانالشان را داشته باشند در این صورت، داریم $\hat{h}_{AB} = h_{AB} + e$ که $e \sim CN(0, \frac{1}{\gamma_{pilot}})$. توجه شود که $\gamma_{pilot} = \frac{P_{pilot}}{\sigma_n^2}$ بیانگر SNR سمبل‌های ارسالی در فاز کاوش کانال است. به طور مشابه $\hat{h}_{BA} = h_{BA} + e$. برای توضیح بیشتر به مرجع [۳۲] مراجعه نمایید.

با جایگذاری رابطه Jake در روابط تخمین کانال، بدست می‌آوریم:

$$\hat{h}_{BA} = \rho' \hat{h}_{AB} + n_e \qquad (۲۱)$$

که در آن $\sigma^2_{n_e} = (1-\rho^2)\left(\sigma^2_{h_{AB}} + \frac{1}{\gamma_{pilot}}\right)$ و نیز $\rho' = \rho \frac{\gamma_{pilot}\sigma^2_{h_{AB}}}{\gamma_{pilot}\sigma^2_{h_{AB}}+1}$.

مراجع

[1] W. Saad, M. Bennis and M. Chen, "A vision of 6G wireless systems: Applications, trends, technologies, and open research problems, IEEE Network, vol. 34, no. 3, pp. 134–142, May/Jun. 2020.

[2] M. Forouzesh *et al.*, "Simultaneous secure and covert transmissions against two attacks under practical assumptions", IEEE Internet of Things Journal, vol. 10, no. 12, pp. 10160-10171, June 2023.

[3] A. Chorti *et al.*, "Context-aware security for 6G wireless: the role of physical layer security", IEEE Communications Standards Magazine, vol. 6, no. 1, pp. 102-108, Mar. 2022.

[4] 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.

[5] T. Lu, L. Chen, J. Zhang, C. Chen, A. Hu, "Joint precoding and phase shift design in reconfigurable intelligent surfaces-assisted secret key generation", IEEE Trans. Inf. Forensics & Security, vol.18, pp.3251-3266, May 2023.

[6] G. Li, C. Sun, J. Zhang, E. Jorswieck, B. Xiao, A. Hu, "Physical layer key generation in 5G and beyond wireless communications: Challenges and opportunities", Entropy, vol. 21, no. 5, pp. 1–16, May. 2019.

[7] A. K. Junejo, F. Benkhelifa, B. Wong, J. A. Mccann, "LoRa-LiSK: a lightweight shared secret key generation scheme for loRa networks", *IEEE* Internet of Things Journal, vol. 9, no. 6, pp. 4110-4124, Aug. 2022.

[8] 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, Mar. 2021.

[9] M. Mitev, A. Chorti, M. Reed, and L. Musavian, "Authenticated secret key generation in delay-constrained wireless systems", EURASIP J. Wireless Commun. Netw., pp. 1–29, Jun. 2020.

[10] M. Mitev, A. Chorti, E. V. Belmega and M. Reed, "Man-in-the-middle and denial of service attacks in wireless secret key generation", in 2019 IEEE Global Communications Conference (GLOBECOM), 2019, pp. 1-6.

[11] M. Letafati, H. Behroozi, B. H. Khalaj and E. A. Jorswieck, "Hardware-impaired PHY secret key generation with man-in-the-middle adversaries", IEEE Wireless Communications Letters, vol. 11, no. 4, pp. 856-860, Apr. 2022.

[12] M. Letafati, H. Behroozi, B. H. Khalaj and E. A. Jorswieck, "Deep learning for hardware-impaired wireless secret key generation with man-in-the-middle attacks", in 2021 IEEE Global Communications Conference (GLOBECOM), 2021, pp. 1-6.

[13] M. Bottarelli, P. Karadimas, G. Epiphaniou, D. K. B. Ismail, C. Maple, "Adaptive and optimum secret key establishment for secure vehicular communications", IEEE Trans. Veh. Tech., vol.70, no.3, pp.2310-2321, Jan. 2021.

[14] Z. Li, Q. Pei, I. Markwood, Y. Liu, and H. Zhu, "Secret key establishment via RSS trajectory matching between wearable devices", IEEE Trans. Inf. Foren. Sec., vol. 13, no. 3, pp. 802–817, Mar. 2018.

[15] M. Letafati, H. Behroozi, B. H. Khalaj and E. A. Jorswieck, "Learning-based secret key generation in relay channels under adversarial Attacks", IEEE Open J. Veh. Tech., vol. 4, pp. 749-764, June 2023.

[16] M. Letafati, H. Behroozi, B. H. Khalaj and E. A. Jorswieck, "Hardware-impaired PHY secret key generation with man-in-the-middle adversaries", IEEE Wireless Commun. Lett., vol. 11, no. 4, pp. 856-860, April 2022.

[17] N. Patwari, J. Croft, S. Jana, and S. K. Kasera, "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements", IEEE Trans. Mobile Comput., vol. 9, no. 1, pp. 17–30, Jan. 2010.

[18] S. Jana, S. Premnath, M. Clark, S. Kasera, and N. Patwari, "On the effectiveness of secret key extraction from wireless signal strength in real environments", in *Proc.* ACM MOBICOM, 2009, pp. 321–332.

[19] 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.

[20] H. Liu, W. Yang, Y. Jie, and Y. Chen, "Fast and practical secret key extraction by exploiting channel response", in Proc. IEEE INFOCOM, 2013, pp. 3048–3056.

[21] X. Wei, X. Y. Li, Q. Chen, J. Han, and K. Zhao, "Keep: Fast secret key extraction protocol for D2D communication", in Proc. IEEE Int. Workshop Qual. Service (IWQoS), 2014, pp. 350–359.

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

[23] 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.

[24] 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.

[25] 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.

[26] 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.

[27] 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.

[28] L. Wang, H. An, H. Zhu and W. Liu, "MobiKey: Mobility-based secret key generation in smart home", IEEE Internet of Things J., vol. 7, no. 8, pp. 7590-7600, Aug. 2020.

[29] Y. Peng, P. Wang, W. Xiang, and Y. Li, "Secret key generation based on estimated channel state information for TDD-OFDM systems over fading channels", IEEE Trans. Wireless Commun., 2017.

[30] Y. Shehadeh, O. Alfandi, and D. Hogrefe, "Towards robust key extraction from multipath wireless channels", J. Commun. Net., vol. 14, no. 4, Aug. 2012.

[31] C. Feng and L. Sun, "Physical layer key generation from wireless channels with non-ideal channel reciprocity: A deep learning based approach", in IEEE 95th Vehicular Technology Conference: (VTC2022-Spring), Helsinki, Finland, 2022, pp. 1-6.

[32] 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.

[33] 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.

[۳۴] 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.

[۳۵] راغب، محمد. کوهستانی، علی. صفوی همامی، سید مصطفی. "طراحی توأم پرتودهی و نویز مصنوعی در ارتباطات موج میلیمتری محرمانه با کمک صفحات انعکاس دهنده هوشمند"، نشریه مهندسی برق و الکترونیک ایران، جلد ۱۹، شماره ۳، ۵۵-۶۲، زمستان ۱۴۰۱.

[36] M. Ragheb, A. Kuhestani, M. Kazemi, H. Ahmadi and L. Hanzo, "RIS-aided secure millimeter-wave communication under RF-chain impairment,s", IEEE Trans. Veh. Tech., pp. 1-13, Aug. 2023.

زیرنویس‌ها

[1] Peer-to-peer
[2] Lightweight
[3] Physical layer secret key generation
[4] Beyond 5G
[5] Internet-of-Things
[6] Ultra reliable low latency communications
[7] Common randomness
[8] Pilot
[9] Secret key
[10] Received Signal Strength
[11] Channel State Information
[12] Probing
[13] Man-in-the-middle
[14] Denial of service
[15] Channel State Information
[16] Hardware impairments
[17] Weak reciprocity
[18] Large-scale
[19] Static
[20] Eavesdropping
[21] Predictable channel attack
[22] Small-scale
[۲۳] توجه شود که CSI استخراج شده از دستگاه‌های تجاری، هم دامنه و هم فاز را شامل می‌شود.
[24] Bit matching rate
[25] Signal-to-Noise-Ratio (SNR)
[26] Line-of-Sight
[27] Unmanned Aerial Vehicle (UAV)
[28] Additive White Gaussian Noise (AWGN)
[29] Free space
[۳۰] 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.
[۳۱] بدلیل وجود نقیصه‌های سخت‌افزاری و ناهمزمانی کلاک زمانی بین فرستنده و گیرنده، نمی‌توان فاز واقعی کانال را بصورت مستقیم از طریق دستگاه‌های تجاری محاسبه کرد [۲۸].
[32] Mutual Random Phase Injection
[33] Guard Band
[34] Key Mismatch Rate
[35] Carrier Frequency Offset
[36] Quantization Region
[37] Key Discarding Rate
[38] Raw Key Generation Rate
[39] Direct quantization
[40] Phase shift
[41] Quantization region
[42] Performance and efficiency
[43] Error-free
[44] Secrecy entropy
[۴۵] متذکر می‌شویم که فاز و دامنه کانال، همیشه از هم مستقل نیستند، بلکه تنها در کانال با محوشدگی رایلی این استقلال برقرار است. هرگاه از هردوی دامنه و فاز برای SKG استفاده شود، میزان تصادفی بودن کلید مخفی کاهش می‌یابد [۲۹].
[46] Constellation
[47] Half-duplex
[48] Mixer
[49] One bit quantizer
[۵۰] در این مقاله، برای سادگی تحلیل‌ها و فهم بهتر، کوانتیزه کننده تک‌بیتی بکار گرفته شده است. توسعه به کوانتیزه کننده چند بیتی با M سطح سر راست است. در این سناریو، آلیس و باب از سیگنال‌های M-PSK برای تولید کاوش کانال استفاده می‌کنند و در گیرنده، M ناحیه کوانتیزاسیون QR i ($i \in \{1,2,\dots,M\}$) با M ناحیه محافظ خواهیم داشت. متذکر می‌شویم که افزایش تعداد سطوح کوانتیزاسیون M، باعث می‌شود تعداد بیت‌های متناظر با کلید مستخرج از کانال، افزایش یافته و در نتیجه نرخ تولید
[51] Probability Density Function