Scientific Journal of Electronical & Cyber Defence
Vol. 12, No. 3, Autumn2024, Serial No. 47

A Novel Secret Key Generation Scheme in the Presence of an Untrusted Relay

A. Kuhestani ,M.R.Keshavarzi,

*Assistant Professor, Qom University of Technology, Qom, Iran

Received:2024 /07/28, Revised: 2024/09/14, Accepted: 2024/10/14, Published: 2024/10/22

DOR: https://dor.isc.ac/dor/20.1001.1.23224347.1403.12.3.8.0

ABSTRACT

Compared to conventional cryptography methods, physical layer secret key generation (SKG) is more efficient and suitable for sixth generation (6G) networks due to features such as lightweight and scalability. In the field of SKG, schemes based on local random generators are used for high-rate key generation. One of these schemes is random phase injection, where the channel probing signals with random phase are exchanged between communication parties (Alice and Bob). In this research work, an SKG scheme is presented in the presence of an untrusted relay, where the relay cannot obtain the key. In order to make the scheme practical, for the first time, the channel probing signals are considered discrete random phase and a single-bit quantizer is used in reception. In addition, in order to reduce the key error rate, quantization with guard bands (GB) is used for key extraction. For such a scenario, we provide expressions for key matching rate, key mismatch rate (KMR), and key discarding rate (KDR) per channel probe. Although increasing the GB range decreases the KMR metric, the key length also shortens. In order to evaluate the effect of GB on the efficiency of the proposed key generation scheme, the raw key generation rate is defined and calculated. In the simulation section, useful engineering insights are provided into determining the probing signal power, the GB size as well as the required coding correction capability. It is also discussed the security evaluation of the proposed scheme in this article. While calculating the secret key capacity, it will be observed that the untrusted relay and external eavesdropper cannot discover the key by intercepting the channel probing steps.

Keywords: Physical layer secret key generation, Untrusted relay, Discrete random phase injection, Guard band.

❖ Corresponding Author Email: kuhestani@qut.ac.ir

«پدافند الکترونیکی و سایبری»
سال دوازدهم، شماره ۳، فصل پاییز ۱۴۰۳؛ ص ۸۴-۷۳

علمی – پژوهشی

یک طرح نوین تولید کلید مخفی در حضور رلهٔ غیرقابل‌اعتماد

علی کوهستانی [۱]، محمدرضا کشاورز [۲*]

۱- استادیار،دانشگاه صنعتی قم،قم، ایران ، ۲- استادیار، پژوهشگاه ارتباطات و فناوری اطلاعات، تهران ، ایران

(دریافت: ۱۴۰۳/۰۵/۰۷، بازنگری: ۱۴۰۳/۰۶/۲۴، پذیرش: ۱۴۰۳/۰۷/۲۳، انتشار: ۱۴۰۳/۰۸/۰۱)

DOR: https://dor.isc.ac/dor/20.1001.1.23224347.1403.12.3.8.0

ناشر: دانشگاه جامع امام حسین (ع) نویسندگان

چکیده

در مقایسه با روش‌های مرسوم رمزنگاری، تولید کلید مخفی (SKG) لایه فیزیکی به دلیل ویژگی‌هایی از قبیل سبک‌وزن بودن و مقیاس‌پذیری برای شبکه‌های نسل ششم (G۶) کارآمدتر و مناسب‌تر است. در حوزهٔ SKG، طرح‌های مبتنی بر مولدهای تصادفی محلّی برای تولید کلید با نرخ بالا، استفاده می‌شوند. یکی از این طرح‌ها، تزریق فاز تصادفی است که در آن سیگنال‌های کاوش کانال با فاز تصادفی بین طرفین ارتباط (آلیس و باب) مبادله می‌شود. در این کار تحقیقاتی، یک طرح SKG در حضور یک رلهٔ غیرقابل‌اعتماد ارائه می‌شود که در آن، رله نمی‌تواند به کلید دست یابد. به‌منظور عملیاتی بودن طرح، برای اولین‌بار، سیگنال‌های کاوش کانال از جنس فاز تصادفی گسسته در نظر گرفته شده و در گیرندگی نیز از کوانتیزه کننده تک‌بیتی استفاده می‌شود. به‌علاوه، به‌منظور کاهش نرخ خطای کلید، از کوانتیزاسیون با نواحی محافظ (GB) برای استخراج کلید استفاده می‌گردد. برای چنین سناریویی، روابطی برای نرخ تطبیق کلید، نرخ عدم تطبیق کلید (KMR) و نیز نرخ دور ریزی کلیدها (KDR) به‌ازای هر کاوش کانال ارائه می‌شود. اگرچه افزایش محدوده GB، معیار KMR را کاهش می‌دهد، اما طول دنباله کلید نیز کوتاه می‌گردد. به‌منظور ارزیابی تأثیر GB بر روی کارایی طرح تولید کلید پیشنهادی، نرخ تولید کلید خام تعریف شده و محاسبه می‌گردد. در بخش شبیه‌سازی، بینش‌های مهندسی مفیدی در خصوص تعیین توان سیگنال کاوش، محدود GB و نیز قدرت تصحیح کدینگ مورد نیاز، ارائه می‌شود. همچنین در این مقاله، طرح پیشنهادی از منظر امنیتی مطالعه می‌گردد. ضمن محاسبهٔ ظرفیت کلید مخفی، مشاهده می‌گردد که رلهٔ غیرقابل‌اعتماد و شنودگر خارجی با رهگیری مراحل کاوش کانال نمی‌توانند کلید را کشف کند.

کلیدواژه‌ها: تولید کلید مخفی لایه فیزیکی، رله غیرقابل‌اعتماد، تزریق فاز تصادفی گسسته، نواحی محافظ

۱- مقدمه

معمولاً برای برآورده‌کردن الزامات امنیتی در شبکه‌ها، از رمزنگاری استفاده می‌شود. به دلیل وجود تعداد قابل‌ملاحظه‌ای ارتباطات همتا به همتا[۲] در نسل ششم شبکه‌های سلولی (6G)، راه‌حل‌های مرسوم امنیتی سنتی قابل‌استفاده نیست [۱]. می‌توان از تکنیک‌های امنیتی سبک‌وزن[۳] نظیر *تولید کلید مخفی*[۴] (SKG)لایه فیزیکی به‌عنوان یک راهکار امیدبخش، به جای استفاده از راه‌حل‌های امنیتی مبتنی بر پیچیدگی محاسباتی، در شبکه‌های 6G [۲]، [۳] بهره برد. به‌خصوص که اخیراً بسیاری از محققان دانشگاهی [۳-۵] و صنعتی [۶]، [۷] به تحقیق در زمینهٔ SKG پرداخته‌اند.

طرح‌های SKG مزایای قابل‌توجهی برای شبکه‌های بی‌سیم دارند [۳]. به طور خاص، توزیع و مدیریت کلید برپایه‌ی این روش‌ها نیازی به زیرساخت متمرکز ندارد؛ زیرا کلید مخفی بدون نیاز به همکاری شخص ثالث به دست می‌آید. این موضوع، زمان موردنیاز برای توافق کلید را به طور قابل‌توجهی کاهش می‌دهد. علاوه بر این، به دلیل تغییرات کانال بی‌سیم، می‌توان کلید مخفی به‌دست‌آمده از روش SKG را به طور مداوم به‌روز رسانی کرد [۵]. لازم به ذکر است که این روش تولید کلید از طریق پیاده‌سازی سازوکارهای سبک و با حداقل تغییرات موردنیاز تحقق می‌یابد؛ در حالی‌که از منظر نظریه اطلاعات، تضمین‌های امنیتی نیز ارائه می‌دهد [۸]. از این رو، این رویکرد به‌عنوان یک راه حل امیدوارکننده برای سیستم‌های فراتر از نسل پنجم مانند اینترنت اشیاء و ارتباطات با تأخیر کم و با قابلیت اطمینان بسیار زیاد[۵] (URLLC) مطرح است.

در تولید کلیدلایه فیزیکی از منبع تصادفی مشترک بین گره‌های قانونی برای استخراج کلید بهره‌برداری می‌شود. به طور خاص،

* رایانامه نویسنده مسئول: kuhestani@qut.ac.ir

[2] Peer-to-peer
[3] Lightweight
[4] Secret key generation
[5] Ultra reliable low latency communications

طرفین ارتباط بعد از تبادل سیگنال‌های راهنما[1] و انجام پردازش‌های لازم، به یک کلید مخفی مشترک دست می‌یابند. در طرح‌های SKG، از مشخصاتی نظیر فاز کانال، توان سیگنال دریافتی[2] (RSS)، اطلاعات حالت کانال[3] (CSI) و سایر ویژگی‌های کانال جهت تولید کلید مخفی استفاده می‌شود [۳] و [۹-۱۳]. به دلیل موجود بودن RSS در بسیاری از دستگاه‌های تجاری، کارهای تحقیقاتی متعددی بر روی آن صورت‌گرفته است [۳] و [۱۴]. بااین‌وجود، نرخ تولید کلید حاصل از RSS بخصوص در محیط‌های ایستا، کم است. به‌علاوه، RSS به بسیاری از حملات از قبیل حمله شنود [۱۵]، حمله مرد در میان[4] [۱۶] و حمله کانال قابل‌پیش‌بینی[5] [۱۷] و [۱۸] آسیب‌پذیر است. در کارهای تحقیقاتی بعدی، با تمرکز بر CSI کانال، مطالعات بیشتری در حوزه SKG صورت گرفت به‌طوری‌که توسط برخی NICهای تجاری قابل‌بهره‌برداری است[6] [۳] و [۶]. در مطالعهٔ اخیر [۱۹] تصریح شده است که CSI در مقایسه با RSS در سیستم تولید کلید، مزیت دارد. در این حوزه، کارهای مبتنی بر دامنهٔ CSI عملی‌تر هستند [۲۰] و [۲۱]. بااین‌وجود، دامنه به‌عنوان بهرهٔ سیگنال دریافتی می‌تواند توسط سیگنال‌های قوی‌تر پوشانده شود. همچنین دامنه از نویز تأثیر زیادی می‌پذیرد و در نتیجه، نرخ تطبیق بیت[7] پایین خواهد بود. یک ویژگی دیگر کانال که نواقص دامنهٔ کانال را مرتفع می‌کند، *اطلاعات فاز کانال* است. فاز کانال در مقایسه با دامنهٔ کانال نسبت به نویز حساس نیست و ضمناً به اندازهٔ کافی تغییرات دارد؛ لذا به‌عنوان یک منبع تصادفی با *آنتروپی بالا* محسوب می‌شود.

در ارتباطات بُرد کوتاه و یا ارتباطات موج میلیمتری، نسبت سیگنال به نویز[8] (SNR) نسبتاً زیاد بوده و پدیدهٔ محوشدگی وجود نخواهد داشت. همچنین در ارتباطات دید مستقیم[9] (LoS) بین ماهواره‌ها [۲۲] و یا ارتباطات پرنده‌های بدون سرنشین[10] (UAV) [۲۳] که در شبکه 6G حضور دارند، و به‌طورکلی در هر مخابره‌ای که کانال آن قابل مدل‌کردن با نویز سفید گوسی جمع‌شونده[11] (AWGN) باشد، 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 است که از منظر امنیت، چالشی‌ترین وضعیت برای تولید کلید مخفی، مربوط به ارتباطات فضای - آزاد می‌باشد [۲۴] و [۲۵] که در آن، کانال قانونی و کانال شنود از نوع LoS بوده و با AWGN مدل می‌شوند[12]. در این حوزه، مرجع [۲۴] با الهام از تحرک فضاپیماها از شیفت فرکانس داپلر به‌منظور تولید کلید بهره برده است. در مراجع [۲۵] و [۲۶] نیز با فرض ایستایی محیط و گره‌ها، راهکارهایی برای تولید کلید ارائه شده است. برخلاف مرجع [۲۶] که یکی از گره‌ها مجهز به چندین آنتن است، در مرجع [۲۵] برای یک سیستم سادهٔ متکی بر گره‌های تک آنتن، از *فاز کانال* بی‌سیم برای پیاده‌سازی SKG استفاده شده است.

یکی از تکنیک‌های تقویت SKG، رله کردن مشارکتی[13] است که به‌خصوص برای مواردی که فاصله بین فرستنده و گیرنده زیاد است، بسیار مفید است [۲۷] و [۲۸]. در حوزهٔ رله کردن مشارکتی، یک حوزهٔ کاربردی و جذاب، سناریوی رلهٔ غیرقابل‌اعتماد است که در آن یک رله به‌عنوان یک موجودیت قانونی به ارتباط منبع به مقصد کمک می‌کند، اما ممکن است آن رله در نقش یک شنو دگر غیرفعال[14] نیز رفتار کند [۲۷] و [۲۸]. این سناریو برای شبکه‌های بی‌سیم در مقیاس بزرگ مانند اینترنت اشیاء[15] (IoT) و شبکه‌های حسگر بی‌سیم[16] (WSN) محتمل است. به‌عنوان‌مثال، نویسندگان در مراجع [۲۷] و [۲۸] یک طرح مشابه SKG مبتنی بر CSI کانال‌های آلیس - رله و باب - رله پیشنهاد کردند. بااین‌حال، نویسندگان این مراجع، پروتکل تولید کلید را به طور جامع مورد تحلیل و بررسی قرار ندادند. به‌عنوان‌مثال، معیارهای عملکردی مانند نرخ عدم تطبیق کلید[17] (KMR) و نرخ دور ریزی کلید[18] (KDR) در مراجع [۲۷] و [۲۸] مطالعه نشده است.

براین‌اساس، در این مقاله، تولید کلیدلایه فیزیکی برای یک ارتباط مشارکتی در حضور یک *رلهٔ غیرقابل‌اعتماد* و در فضای آزاد موردمطالعه جامع قرار می‌گیرد. مشابه کار پیشین [۲۵] و متفاوت با کارهای [۲۷] و [۲۸]، از *فاز کانال* به‌عنوان مؤلفه تصادفی مشترک بین آلیس، باب و رله برای تولید کلید استفاده می‌شود و ضمناً به‌منظور افزایش آنتروپی کلید، فاز تصادفی[19] توسط آلیس و باب تزریق می‌شود. متفاوت با کار پیشین [۲۵]

[1] Pilot
[2] Received Signal Strength
[3] Channel State Information
[4] Man-in-the-Middle
[5] Predictable channel attack
[6] توجه شود که CSI استخراج شده از دستگاه‌های تجاری، هم دامنه و هم فاز را شامل می‌شود.
[7] Bit matching rate
[8] Signal-to-Noise-Ratio
[9] Line-of-Sight
[10] Unmanned Aerial Vehicle
[11] Additive White Gaussian Noise
[12] 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.
[13] Cooperative relaying
[14] Passive
[15] Internet-of-Things
[16] Wireless Sensor Networks
[17] Key Mismatch Rate
[18] Key Discarding Rate
[19] Mutual Random Phase Injection

که رله‌ای در شبکه حضور نداشت و ضمناً 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.

همان‌طوری که می‌دانیم وجود هم پاسخی بالا برای کانال بی‌سیم، از اصول SKG می‌باشد؛ حال‌آنکه در مرحلهٔ کاوش کانال، وجود عواملی نظیر نویز، خطای تخمین کانال و وجود نقیصه‌های سخت‌افزاری، باعث عدم تطبیق کلیدها می‌شود. به‌منظور کاهش این نرخ اختلاف، تکنیک‌های کوانتیزاسیون گوناگونی بکار گرفته می‌شود [۲۹-۳۲]. در این مقاله، ضمن معرفی و مقایسهٔ این روش‌ها، از روش مبتنی بر باند محافظ[1] (GB) و نیز کوانتیزه کننده تک‌بیتی استفاده شده و KMR را محاسبه می‌کنیم. توجه شود که در رویکرد مبتنی بر GB، تنها زمانی نمونهٔ مستخرج از کاوش کانال برای تولید کلید استفاده می‌شود که کمیت تخمین زده شده در یک ناحیه کوانتیزاسیون[2] (QR) یا ناحیه تصمیم قرار گرفته و در GBها قرار نگیرد. براین‌اساس، معیار KDR نیز برای طرح پیشنهادی محاسبه می‌گردد. به‌منظور ارزیابی تأثیر منفی افزایش اندازه GB، نرخ تولید کلید خام[3] (KGR) معرفی و ارزیابی می‌شود. نتایج عددی ارائه شده، شهود مهندسی مفیدی در خصوص مقدار توان سیگنال کاوش کانال و اندازه GB ارائه می‌دهند. همچنین به ارزیابی امنیتی طرح پیشنهادی می‌پردازیم. ضمن محاسبهٔ ظرفیت کلید مخفی، خواهیم دید که رلهٔ غیرقابل‌اعتماد و شنو دگر خارجی با رهگیری مراحل کاوش کانال نمی‌توانند به کلید دست یابند. توجه شود که در مقالات [۳۱] و [۳۲]، محققین یک ارتباط نقطه‌به‌نقطه (بدون حضور رله) را مورد مطالعه قرار داده و برای آن، پروتکل تولید کلید ارائه دادند. درحالی‌که در این مقاله، یک سناریوی پیچیده‌تر بررسی می‌گردد که در آن، یک رله غیرقابل‌اعتماد در مدل سیستم حضور دارد. چون رلهٔ غیرقابل‌اعتماد، چون خود یک شنو دگر است، طراحی پروتکل تولید کلید آن چالشی خواهد بود. در این مقاله، با ارائه یک پروتکل تولید کلید، مسئله تولید کلید در حضور رله غیرقابل‌اعتماد پاسخ داده می‌شود. همچنین در مرجع [۳۱] از CSI کانال و در مرجع [۳۲] از دامنهٔ کانال، برای تولید کلید استفاده شده است. در این کار تحقیقاتی، از فاز کانال استفاده می‌شود که مزایای خودش را دارد. همچنین توجه شود که در مرجع [۳۱] تحلیل KGR و نیز KMR انجام نشده است و صرفاً با ارائه شبیه‌سازی‌هایی در خصوص آنها بحث شده است. اما در این کار پژوهشی، روابط تحلیلی ارائه می‌گردد. به‌علاوه، تحلیل امنیتی کلید از منظر شنودگر و نیز ظرفیت تولید کلید از مواردی است که صرفاً در کار تحقیقاتی پیشرو انجام شده و در [۳۱] و [۳۲] انجام نشده است.

ادامه این مقاله به شرح زیر است: در بخش ۲، مدل سیستم مطالعاتی و سیگنال های مربوطه نوشته می‌شود. همچنین روش‌های کوانتیزاسیون فاز تشریح می‌گردند. در بخش بعدی یعنی بخش ۳، طرح تولید کلید پیشنهادی در این مقاله که مبتنی بر فاز و در حضور رلهٔ غیرقابل‌اعتماد می‌باشد، تبیین می‌گردد. در بخش ۴، عملکرد طرح پیشنهادی با محاسبهٔ نرخ عدم تطابق کلید، نرخ دور ریزی کلید و نرخ تولید کلید خام مطالعه می‌گردد. سپس در بخش ۵، طرح پیشنهادی را از منظر امنیتی بررسی می‌کنیم. بدین منظور، تلاش شنودگر ارزیابی می‌گردد و همچنین ظرفیت تولید کلید محاسبه می‌شود. بخش ۶، به شبیه‌سازی و استخراج نتایج تخصیص داده شده است. در نهایت، در بخش ۷ نتیجه‌گیری ارائه می‌گردد.

۱- مدل سیستم و سیگنال‌ها

در این بخش در ابتدا، به معرفی انواع کوانتیزه کننده‌ها پرداخته و تأثیر آنها را بر روی کارایی تولید کلید مطالعه می‌کنیم. دراین‌خصوص، روش کوانتیزه مستقیم[4] (صرفاً دمدولاسیون – بدون GB)، کوانتیزه با GB و کوانتیزه با جابه‌جایی فاز[5]، موردمطالعه قرار می‌گیرد. 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 به‌دست آمده در هر گرهٔ 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

[1] Guard Band
[2] Quantization Region
[3] Key Generation Rate
[4] Direct quantization
[5] Phase shift

تخمین‌های نویزی آنها ارائه شده است. با در نظر گرفتن چهار ناحیه در صفحه مختصات به‌عنوان نواحی کوانتیزاسیون[1] (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: همان‌طوری‌که در بالا مشاهده کردیم، واضح است که نرخ خطای بالا عمدتاً به دلیل مقادیر کانال نزدیک به نواحی مرزی است. بنابراین با تعریف نواحی مرزی کوچک، QRها را تفکیک می‌کنیم تا آن مقادیری از کانال را که سبب اختلاف بین نمونه‌های دریافتی آلیس و باب می‌شوند، کاهش داده شوند. توجه شود 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. براین‌اساس، 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 QRها و عرض ناحیه محافظ هستند.

ازنقطه‌نظر امنیت، این سؤال مطرح می‌شود که هر گره چگونه می‌تواند گره دیگر را مطلع کند که یک کاوش کانال می‌بایست دور ریخته شود، بدون آنکه محرمانگی کاهش یابد؟ در واقع، همان‌طوری که 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، گرهٔ مرجع، کاوش‌های مورد قبول را با ارسال نمایه‌های مربوطه اعلام می‌کند و سپس گره مقابل نیز چنین انجام می‌دهد. بدین‌طریق، بر روی آن کاوش‌هایی که در فرآیند استخراج بیت‌های مخفی مورداستفاده قرار می‌گیرد، توافق می‌کنند. از منظر عملکرد، واضح است 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[2] 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. به‌عنوان 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.

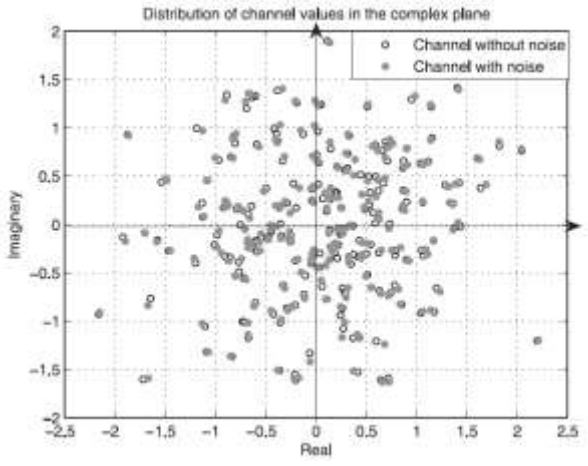
۳) کوانتیزاسیون با جابجایی فاز: بطور شهودی قابل استنتاج است که روش کوانتیزاسیون با GB از منظر کارآمدی استخراج کلید، بهینه نیست. در واقع، در این رویکرد، آن مقادیر از کانال که در GBها قرار می‌گیرند به سادگی نادیده گرفته شده و در فرآیند کوانتیزاسیون لحاظ نمی‌شوند. این موضوع، منجر به کاهش میانگین تعداد بیت‌های مخفی استخراج شده می‌گردد. بنابراین به‌منظور دستیابی به کارآمدی بالا در استخراج کلید، نباید کانال‌ها با بهره کافی را دور بریزیم. براین‌اساس، 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 به‌طوری‌که 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. به‌منظور 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، ابتداً 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[3] برای ارسال μ به باب وجود دارد. متعاقباً باب، بعد از تخمین کانال قانونی، فاز خودش را به صورت زیر اصلاح می‌کند:

$$\theta_2' = \theta_2 - \mu = \Delta\theta + \hat{\theta} \quad (1)$$

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}) به‌ازای هر مشاهده کانال، می‌توان تعداد بهینه QRها را یافت.

[1] Quantization region
[2] Performance and efficiency
[3] Error-free



شکل (۱): نمایشی از چندین تحقق کانال و تخمین نویزی آنها در فضای مختلط [۳۰].

۲-۲- مدل سیستم و کاوش کانال

مطابق شکل (۲)، مدل سیستم مورد مطالعه، شامل ۳ کاربر قانونی (منبع، مقصد و رله) است که همگی یک آنتن دارند به‌طوری‌که منبع و مقصد می‌خواهند با کمک رله غیرقابل‌اعتماد، به یک کلید مشترک برسند. رله موجود در سیستم مورد مطالعه، رله با عملکرد تقویت و ارسال[1] (AF) و با بهرهٔ ثابت بوده که در سطح ارائه سرویس، مورد اعتماد ولی در سطح داده، غیرقابل‌اعتماد است. لذا رله در اجرای پروتکل تولید کلید کاملاً همراه می‌باشد، ولی ممکن است کلید را استخراج کرده و از آن سوءاستفاده نماید.

شکل (۲): مدل سیستم

ازآنجایی‌که توزیع نمونه‌های مستخرج از روش‌های مبتنی بر دامنه (شامل RSS، پوش سیگنال و فاصله)، یکنواخت نیست، بنابراین بعد از کوانتیزاسیون یکنواخت، بیت‌ها غیر هم احتمال خواهند شد. در نتیجه، آنتروپی کلید ناشی از به‌کارگیری این ویژگی‌ها، کامل نیست. از منظر مقایسه، فاز کانال به‌طورکلی توزیع یکنواخت دارد و لذا کلیدهای تولید شده، آنتروپی محرمانگی[2] بالاتری دارند (کلیدهای تولید شده، میزان تصادفی بودن بالاتری دارند)؛ بنابراین روش‌های مبتنی بر فاز ازنقطه‌نظر آنتروپی محرمانگی، ترجیح داده می‌شوند. 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 هر دوی دامنه و فاز برای SKG استفاده شود، میزان تصادفی بودن کلید مخفی کاهش می‌یابد [۲۹]. براین‌اساس در این مقاله، تولید کلید مبتنی بر فاز کانال است. بدین صورت که منبع و مقصد نمادهای با فاز تصادفی گسسته را از فضای منظومه[3] BPSK انتخاب و به طور متقابل برای یکدیگر می‌فرستند. برای $u \in \{S, D\}$، فاز سمبل ارسالی توسط کاربر u عبارت است از:

$$\phi_u = \pi\, i_u \qquad (۱)$$

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

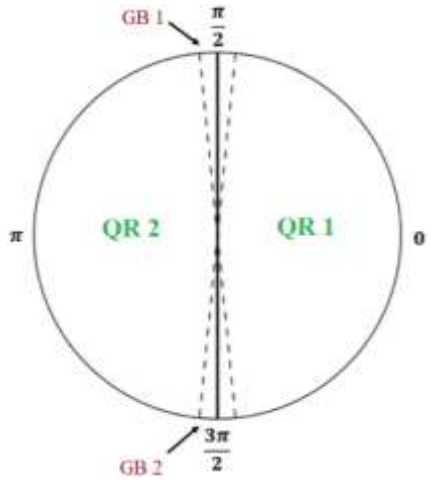
کانال را ایستا و ارتباطات را LoS در نظر می‌گیریم. براین‌اساس، ضریب تضعیف و فاز کانال منبع - رله به ترتیب با α_{sr} و ϕ_{sr}، برای کانال مقصد رله نیز با α_{rd} و ϕ_{rd} و برای منبع/مقصد/رله-شنودگر با $\alpha_{es/d/r}$ و $\phi_{es/d/r}$ نمایش داده شود. نویز حرارتی، سفید بوده و توزیع گوسی دارد و بعلاوه در تمام گره‌ها، توان آن σ_n^2 لحاظ می‌شود. توجه شود که در اجرای مراحل کاوش کانال، به‌دلایلی از قبیل خطای تخمین و نویز حرارتی در گیرنده‌ها، فرآیند تولید کلید با خطا خطا مواجه می‌شود.

۲- طرح تولید کلید مخفی پیشنهادی با رلهٔ غیرقابل‌اعتماد

در منبع و مقصد، مشاهدات همبسته، کوانتیزه می‌شوند تا دنباله‌های باینری تولید شوند. انتخاب یک الگوریتم کوانتیزه کننده مناسب می‌تواند KMR را کمتر دهد. به‌عبارت‌دیگر، 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. بااین‌حال، برای تعداد نواحی بسیار زیاد، اختلاف کلید قابل‌ملاحظه خواهد بود. یک مصالحه برای برقراری تعادل بین نرخ تولید کلید و KMR، به‌کارگیری GB برای کوانتیزاسیون است. در این مقاله، از الگوریتم متداول کوانتیزاسیون تک‌بیتی[4] با GB [۳۱] و [۳۲] استفاده می‌کنیم که عرض باند آن ψ در نظر گرفته می‌شود[5]. شکل (۳)، کوانتیزه کنندهٔ تک‌بیتی مدنظر را به تصویر کشیده است. همان‌طوری‌که

[1] Amplify-and-Forward
[2] Secrecy Entropy
[3] Constellation
[4] One bit quantizer
[5] 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 کلید بیشتر گردد. اما در عوض، احتمال اختلاف کلیدها افزایش می‌یابد و اگر از ایده GB استفاده شود، به دلیل زیاد شدن GBها، نرخ دور ریزی کلیدها زیاد می‌شود.

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. کران‌های پایین و بالا برای GBهای ۱ و ۲ به ترتیب به‌صورت: $GB_{1L}=\frac{\pi}{2}-\frac{\psi}{2}$، $GB_{1U}=\frac{\pi}{2}+\frac{\psi}{2}$ و نیز $GB_{2L}=\frac{3\pi}{2}-\frac{\psi}{2}$ و $GB_{2U}=\frac{3\pi}{2}+\frac{\psi}{2}$ خواهند بود. در خروجی کوانتیزه کننده، برای منبع و مقصد به ترتیب، قطعه کلید k_S و k_D تولید می‌شود. بعد از L بار کاوش کانال، با قرار دادن قطعه کلیدها کنار یکدیگر، کلید خام حاصل شده برای هر کدام K_S و K_D با طول L بیت خواهد بود.



شکل (۳): کوانتیزه کننده تک‌بیتی با نواحی محافظ.

توجه شود که برای تولید کلید مخفی مشترک از کانال بدون سیم، ابتدا می‌بایست تخمین کانال اجرا شود. این مورد برای هر نوع ارتباطاتی ضروری و پیش‌فرض محسوب می‌شود و هیچ سربار اضافی به همراه ندارد. در این کار، صرفاً نیاز است تا آلیس و باب کانال خودشان تا رله را بدانند. بدین منظور، صرفاً کافی است تا رله یک دنباله آزمونه مشخص را ارسال می‌کنند. با این فرض که کانال بین رله تا هر کاربر به طور ایده‌آل تخمین زده شده است، مراحل استخراج کلید بیان می‌گردد.

۱) <u>مرحله اول کاوش کانال</u>: منبع و مقصد همزمان به ترتیب سیگنال‌هایی با توان‌های $\sqrt{P_S}$ و $\sqrt{P_D}$ و نیز فاز تصادفی ϕ_S و ϕ_D تزریق می‌کنند. یعنی در باند پایه داریم: $x_S=$ $\sqrt{P_S}\,e^{j\phi_S}$ و $x_D=\sqrt{P_D}\,e^{j\phi_D}$ در نتیجه، سیگنال دریافتی در رله برابر خواهد شد با:

$$y_R=\sqrt{P_S}\alpha_{sr}\,e^{j(\phi_S+\phi_{sr})}+\sqrt{P_D}\alpha_{rd}\,e^{j(\phi_D+\phi_{rd})}+n_R \qquad (۲)$$

مشخص است که به دلیل تصادفی بودن فازها، رله هیچ اطلاعی از فازها کسب نخواهد کرد.

۲) <u>مرحله دوم کاوش کانال</u>: با در نظر گرفتن رله AF با بهره ثابت G، سیگنال ارسالی از آن $x_R=Gy_R$ خواهد شد. بنابراین سیگنال دریافتی در منبع برابر خواهد شد با:

$$y_S=G\sqrt{P_S}\alpha_{sr}^2\,e^{j(\phi_S+2\phi_{sr})}+G\sqrt{P_D}\alpha_{sr}\alpha_{rd}\,e^{j(\phi_D+\phi_{sr}+\phi_{rd})}+G\alpha_{sr}e^{j\phi_{sr}}n_R+n_S \qquad (۳)$$

منبع با اطلاعی که از پارامترهای خودش دارد، عبارت اول در رابطه فوق را حذف می‌کند (حذف سیگنال خود تداخلی). در نتیجه:

$$\tilde{y}_S=G\sqrt{P_D}\alpha_{sr}\alpha_{rd}\,e^{j(\phi_D+\phi_{sr}+\phi_{rd})}+n_T \qquad (۴)$$

که $n_T=G\alpha_{sr}e^{j\phi_{sr}}n_R+n_S$ نویز حرارتی برآیند بوده که خود نیز گوسی با توان $\sigma_{T,S}^2=\sigma_n^2(1+G^2\alpha_{sr}^2)$ خواهد بود. حال اگر بخواهیم SNR سیگنال دریافتی در منبع را بیابیم داریم:

$$\gamma_S=\frac{G^2\alpha_{sr}^2\alpha_{rd}^2P_D}{\sigma_{T,S}^2} \qquad (۵)$$

باتوجه‌به رابطه (۴) و با کمک مرجع [۲۵]، فاز تخمینی در منبع برابر می‌شود با:

$$\hat{\phi}_S=\phi_D+\phi_{sr}+\phi_{rd}+\epsilon_S \qquad (۶)$$

که ϵ_S توزیع نرمال با میانگین صفر و واریانس $\sigma_{\epsilon_S}^2=\sqrt{\frac{2}{2\gamma_S+1}}$ دارد. توجه شود که بر مبنای مرجع [۲۵]، ϵ_m خطای تخمین فاز، بسته به SNR کاوش کانال دارای توزیع Tikhonov (برای SNR پایین و متوسط) یا توزیع نرمال (برای SNR بالا) خواهد داشت.

توجه شود که منبع با آگاهی از ϕ_{sr}، کمیت $\phi_D+\phi_{rd}+\epsilon_S$ را در اختیار خواهد داشت. پس منبع دو کمیت $\phi_S+\phi_{Sr}$ و $\phi_D+\phi_{rd}+\epsilon_S$ را در اختیار دارد. مشابه تحلیل‌ها و مطالعات فوق، برای گره مقصد نیز قابل حصول است. یعنی مقصد دو کمیت $\phi_S+\phi_{Sr}+\epsilon_D$ و $\phi_D+\phi_{rd}$ را در اختیار خواهد داشت که که ϵ_D توزیع نرمال با میانگین صفر و واریانس $\sigma_{\epsilon_D}^2=\sqrt{\frac{2}{2\gamma_D+1}}$ و $\gamma_D=\frac{G^2\alpha_{sr}^2\alpha_{rd}^2P_S}{\sigma_{T,D}^2}$ که $\sigma_{T,D}^2=\sigma_n^2(1+G^2\alpha_{rd}^2)$.

بعد از کوانتیزه‌کردن دو کمیت فوق و سپس الحاق آنها به یکدیگر، می‌توان آن را به‌عنوان قطعه کلید خام مشترک برای منبع و مقصد در نظر گرفت. به عبارت ریاضی:

$$k_S=Q\left(\phi_S^{(1)}\right)||\,Q\left(\phi_S^{(2)}\right)\triangleq k_S^{(1)}||k_S^{(2)}$$
$$k_D=Q\left(\phi_D^{(1)}\right)||Q\left(\phi_D^{(2)}\right)\triangleq k_D^{(1)}||k_D^{(2)} \qquad (۷)$$

که $\phi_S^{(1)}=\phi_S+\phi_{Sr}$، $\phi_S^{(2)}=\phi_D+\phi_{rd}+\epsilon_S$، $\phi_D^{(1)}=\phi_S+\phi_{Sr}+\epsilon_D$، $\phi_D^{(2)}=\phi_D+\phi_{rd}$. تابع کوانتیزاسیون $Q(x)=\left\lfloor\frac{x}{\pi}+\frac{1}{2}\right\rfloor$ بوده و در پیمانه ۲ محاسبه می‌گردد. لذا $k_S^{(1)},k_S^{(2)},k_D^{(1)},k_D^{(2)}\in\{0,1\}$ پر واضح است که در شرایط ایده‌آل یعنی $\epsilon_S=\epsilon_D=0$، منبع و مقصد به قطعه کلید برابر می‌رسند. نکته قابل توجه در طرح پیشنهادی فوق در مقایسه با طرح بدون رله [۲۵] این است که در هر بار کاوش کانال، طرح ما یک دنباله باینری دو بیتی استخراج می‌کند در حالی‌که در طرح

بدون رله [۲۵]، یک بیت استخراج می‌گردد.

در حضور GB، منبع و مقصد می‌بایست مقادیر زیر را محاسبه کنند (در پیمانه ۲):

$$k_m^{(i)} \triangleq \left\lfloor \frac{\phi_m^{(i)}}{\pi} + \frac{1}{2} \right\rfloor, k_m^{+(i)} \triangleq \left\lfloor \frac{\phi_m^{(i)} + \frac{\psi}{2}}{\pi} + \frac{1}{2} \right\rfloor, \quad k_m^{-(i)} \triangleq \left\lfloor \frac{\phi_m^{(i)} - \psi/2}{\pi} + \frac{1}{2} \right\rfloor \tag{۸}$$

که $i \in \{1,2\}$ و $m \in \{S, D\}$. سپس منبع و مقصد، هر بیت از کلید دو بیتی خود را به‌صورت زیر محاسبه می‌کنند:

$$k_m^{(i)} = \begin{cases} k_m^{(i)} & if \quad k_m^{+(i)} = k_m^{-(i)} \\ \emptyset & Otherwise, \end{cases} \tag{۹}$$

در رابطهٔ فوق، $\emptyset$ بیانگر دورریختن بیت مربوطه است. همان‌طوری که پیش‌تر شرح دادیم برای وضعیت $\emptyset$، کاربر موردنظر، طی یک پروتکل به کاربر مقابل اطلاع می‌دهد که او هم $k_m^{(i)}$ خودش را برابر با $\emptyset$ قرار دهد. به این ترتیب، وقتی مقداری در GBها قرار داشته باشد، از این مقدار برای تولید کلید استفاده نمی‌شود. توجه شود که در اینجا، ممکن است تنها یک بیت از دو بیت دور ریخته شود نه لزوماً هر دو بیت استخراج شده از یکبار کاوش کانال. اما برای کاهش سربار طیفی، دو بیت مربوط به آن کاوش دور ریخته می‌شود.

۳- تحلیل کارایی طرح تولید کلید پیشنهادی:

در این بخش، روابط مفیدی برای احتمال تطابق کلید (P_{KA}) و احتمال دور ریزی کلید (P_{KDS}) به دست می‌آوریم. با کمک این معیارها، KMR و نیز نرخ تولید کلید خام را محاسبه خواهیم کرد.

بدیهی است که نتیجه مرحلهٔ کوانتیزاسیون، یکی از سه پیشامد زیر خواهد شد:

- پیشامد ۱: به دوبیتی یکسان کوانتیزه شوند. در این حالت اصطلاحاً تطابق قطعه‌کلیدها را داریم.
- پیشامد ۲: به دوبیتی‌های غیریکسان کوانتیزه شوند. در این حالت اصطلاحاً عدم تطابق قطعه‌کلیدها داریم.
- پیشامد ۳: هر کدام از $\phi_m^{(1)}$ها در GB قرار گیرد.

توجه شود که تنها آن نمونه‌هایی که در پیشامد ۱ یا ۲ قرار گیرند، قابل‌استفاده خواهند بود. اگر در مرحله‌ای از کاوش کانال، پیشامد ۳ واقع شود، نمونه‌های متناظر می‌بایست دور ریخته شود تا کلیدهای بدست آمده جهت تحویل به مرحله اصلاح اطلاعات (یعنی کلیدهای خام K_S و K_D)، 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، احتمال وقوع پیشامد ۱ همان احتمال تطابق کلید بوده و برابر است با:

$$\begin{aligned} &P_{KA} \\ &= P_r\left\{\phi_S^{(1)}, \phi_D^{(1)} \in (\text{QR 1 or QR 2}) \& \ \phi_S^{(2)}, \phi_D^{(2)} \in (\text{QR 1 or QR 2})\right\} \\ &= \sum_{i=1}^{2}\sum_{j=1}^{2} P_r\left\{\phi_S^{(1)}, \phi_D^{(1)} \in \text{QR } i \ \& \ \phi_S^{(2)}, \phi_D^{(2)} \in \text{QR } j\right\} = 4P_{KA,0}^2 \end{aligned} \tag{۱۰}$$

که در رابطهٔ بالا $P_{KA,0} = P_r\left\{\phi_S^{(1)}, \phi_D^{(1)} \in \text{QR 1}\right\}$. تساوی آخر به دلیل یکنواختی فازهای تزریقی توسط منبع و مقصد و یکنواختی فاز کانال، و نیز استقلال $\phi_m^{(1)}$ و $\phi_m^{(2)}$ که $m \in \{S, D\}$ است، برقرار می‌باشد. به طور مشابه، احتمال وقوع پیشامد ۳ همان نرخ دور ریزی قطعه‌کلیدها بوده و برابر است با:

$$P_{KDS} = P_r\left\{\left(\phi_S^{(1)} \text{or } \phi_D^{(1)} \in \text{GB}\right) \text{or } \left(\phi_S^{(2)} \text{or } \phi_D^{(2)} \in \text{GB}\right)\right\} \tag{۱۱}$$

که GB بیانگر اجتماع GB 1 و GB 2 است.

توجه شود احتمال پیشامد ۲ همان نرخ عدم تطابق کلید (KMR) بوده که به‌صورت $P_{KM} = 1 - P_{KA} - P_{KDS}$ قبل ارزیابی است. همچنین متذکر می‌شویم که احتمال تولید کلید $P_{KG} = P_{KA} + P_{KM}$ مهم است؛ چرا که P_{KG} بیانگر میزان نمونه‌های قابل‌بهره‌برداری از بین تمام نمونه‌ها، جهت استخراج کلید می‌باشد. بنابراین، رابطهٔ دقیق برای KMR به‌صورت زیر قابل بیان است:

$$P_{KM}^{\text{Exat}} = \frac{P_{KM}}{P_{KA} + P_{KM}} \tag{۱۲}$$

در حقیقت، اگر P_{KM}^{Exat} از یک آستانهٔ مشخص (میزان قدرت تصحیح خطای کدینگ) کمتر باشد، بیت‌های خطا در مرحله اصلاح اطلاعات تصحیح می‌شوند که این به آن معناست که کل کلید خام، قابل‌بهره‌برداری خواهد بود. بنابراین، P_{KG} زیاد و در نتیجه KMR کم، مطلوب است. همان‌طوری‌که در ادامه خواهیم دید، به‌کارگیری GB ایدهٔ خوبی است که میزان خطای کلید را کاهش داده و در نتیجه می‌تواند احتمال موفقیت پروتکل تولید کلید را افزایش دهد.

خوب است ذکر شود که اگر کانال از هم پاسخی خوبی برخوردار باشد و نیز SNR بالا باشد، با عنایت به اینکه P_{KM}^{Exat} به میزان قابل‌توجهی کم خواهد بود، می توان پروتکل تولید کلید را به حالت بدون GB تغییر داد. به عبارت دیگر، یک پروتکل تولید کلید وفقی داشته باشیم به‌طوری‌که بسته به شرایط سیستمی، بین دو وضعیت "گیرندگی با GB" و "گیرندگی بدون GB" سوئیچ کند. در اینجا بر روی پروتکل تولید کلید با GB تاکید می‌شود. بدیهی است که با قراردادن $\psi = 0$، حالت بدون GB حاصل می‌گردد.

در ادامه، روابط مفیدی برای P_{KA} و P_{KDS} به‌دست می‌آید. یادآوری می‌شود که KMR با عنایت به $P_{KM} = 1 - P_{KA} -$ P_{KDS} و سپس به‌کارگیری رابطهٔ (۱۲) قابل ارزیابی است.

۳-۱- نرخ تطابق کلید:

با عنایت به رابطهٔ (۱۰) و اینکه $\phi_m^{(1)}$ و $\phi_m^{(2)}$ مستقل هستند، می‌توان نوشت:

$$P_{KA} = \sum_{i=1}^{2}\sum_{j=1}^{2} P_r\{(\phi_S^{(1)},\phi_D^{(1)}) \in \text{QR } i \;\&(\phi_S^{(2)},\phi_D^{(2)}) \in \text{QR } j\} \\ = \sum_{i=1}^{2}\sum_{j=1}^{2} P_r\{(\phi_S^{(1)},\phi_D^{(1)}) \in \text{QR } i\}\, P_r\{(\phi_S^{(2)},\phi_D^{(2)}) \in \text{QR } j\} \quad (۱۳)$$

ازآنجایی‌که جفت‌های $(\phi_S^{(1)},\phi_D^{(1)})$ و $(\phi_S^{(2)},\phi_D^{(2)})$ توابع چگالی احتمال توأم یکسانی دارند، لذا تنها نیاز است که احتمال‌های $P_1 = P_r\{(\phi_S^{(1)},\phi_D^{(1)}) \in \text{QR } 1\}$ و $P_2 = P_r\{(\phi_S^{(1)},\phi_D^{(1)}) \in \text{QR } 2\}$ را محاسبه کنیم. در نهایت خواهیم داشت: $P_{KA} = P_1^2 + P_2^2 + 2P_1P_2$.

با تجزیهٔ QR 1 به دو ناحیهٔ QR 11 (معرف ربع اول صفحه مختصات) و QR 12 (معرف ربع چهارم صفحه مختصات)، برای P_1 می‌توان نوشت:

$$P_1 = P_r\{\phi_S^{(1)} \in \text{QR } 1\,, \phi_D^{(1)} \in \text{QR } 1\} \\ = P_r\{\left(\underbrace{\phi_S^{(1)} \in \text{QR } 11}_{A_1} \text{ or } \underbrace{\phi_S^{(1)} \in \text{QR } 12}_{A_2}\right), \\ \left(\underbrace{\phi_D^{(1)} \in \text{QR } 11}_{B_1} \text{ or } \underbrace{\phi_D^{(1)} \in \text{QR } 12}_{B_2}\right)\} \\ = P_r\{A_1,B_1\} + P_r\{A_1,B_2\} + P_r\{A_2,B_1\} \\ + P_r\{A_2,B_2\}$$

در توجهات ۱ و ۲ (در ادامه)، تابع CDF برای متغیر تصادفی $\phi_D^{(1)}$ و نیز برای نیز تابع CDF مشترک $\phi_S^{(1)}$ و $\phi_D^{(1)}$ محاسبه شده است. با کمک این توجهات و نیز تعریف $\Psi(\alpha,\beta) = \frac{1}{2\pi}\int_0^{\alpha} \text{G}(\beta - x)\,dx$ که $\text{G}(.)$ تابع CDF متغیر تصادفی نرمال است، احتمالات P_1 و P_2 و در نتیجه P_{KA} قابل ارزیابی بصورت رابطه ریاضی خواهد بود.

توجه ۱: با عنایت به آنکه $\phi_D^{(1)} = \phi_S + \phi_{sr} + \epsilon_D$، تعریف می‌کنیم $X = \phi_S + \phi_{sr}$ و $Y = \epsilon_D$. لذا $\phi_D^{(1)} = X + Y$ که در آن $X \sim U[0,2\pi]$ و $Y \sim N(0,\sigma^2(\gamma))$ است. بنابراین، با توجه به استقلال X و Y داریم:

$$F_{\phi_D^{(1)}}(\alpha) = P_r\{X + Y \le \alpha\} \\ = \int_{-\infty}^{+\infty}\int_{-\infty}^{\alpha-x} f_X(x')f_Y(y')dy'dx' \\ = \int_{0}^{2\pi}\int_{-\infty}^{\alpha-x} \frac{1}{2\pi} \times \frac{1}{\sqrt{2\pi\sigma^2(\gamma)}} e^{-\frac{y'^2}{2\,\sigma^2(\gamma)}} dy'dx' \\ = \frac{1}{2\pi}\int_0^{2\pi} \text{G}(\alpha - x')\,dx' = \Psi(2\pi,\alpha)$$

که تابع $\text{G}(x)$ به تابع CDF متغیر تصادفی نرمال مشهور است. همچنین تعریف کرده‌ایم $\Psi(\alpha,\beta) = \frac{1}{2\pi}\int_0^{\alpha} \text{G}(\beta - x)\,dx$.

توجه ۲: با تعریف $X = \phi_S + \phi_{sr}$ و $Y = \epsilon_D$ داریم $\phi_S^{(1)} = X$، $\phi_D^{(1)} = X + Y$. همچنین چون $Z = \phi_D^{(1)}$، برای سادگی تعریف می‌کنیم. لذا می‌بایست احتمال $P_r\{GB_{1L} \le X \le GB_{1U}, GB_{1L} \le Z \le GB_{1U}\}$ را محاسبه کنیم. اگر در صفحه دو بعدی x و z ناحیه فوق را رسم کنیم، به همان نتیجه در تساوی آخر رابطه (۱۸) یعنی $F_{X,Z}(GB_{1U},GB_{1U}) - F_{X,Z}(GB_{1L},GB_{1U}) - F_{X,Z}(GB_{1U},GB_{1L}) + F_{X,Z}(GB_{1L},GB_{1L})$ خواهیم رسید. لذا مسئله کنونی محاسبه CDF مشترک X و Z یعنی $F_{X,Z}(u_1,u_2)$ می‌باشد. لذا چون $Z = X + Y$ است، می‌توان نوشت:

$$F_{X,Z}(u_1,u_2) = P_r\{X \le u_1, Y \le u_2 - X\} \\ = \int_{-\infty}^{u_1}\int_{-\infty}^{u_2-x} f_{X,Y}(x',y')dy'dx' \\ = \int_{0}^{u_1}\int_{-\infty}^{u_2-x} \frac{1}{2\pi} \times \frac{1}{\sqrt{2\pi\sigma^2(\gamma)}} e^{-\frac{y'^2}{2\,\sigma^2(\gamma)}} dy'dx' \\ = \frac{1}{2\pi}\int_0^{u_1} \text{G}(u_2 - x')\,dx' = \Psi(u_1,u_2)$$

در اثبات بالا از این حقیقت که X و Y مستقل بوده و لذا PDF مشترک آنها به ضرب PDFها منجر می‌شود، استفاده شده است. همچنین در سطر آخر تعریف شده است $\Psi(\alpha,\beta) = \frac{1}{2\pi}\int_0^{\alpha} \text{G}(\beta - x)\,dx$.

۳-۲- نرخ دور ریزی کلید:

همان‌طوری که گفته شد، بعد از آنکه فازهای موجود در هر گره 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 کوتاه‌شدن فرآیند گفتگو، می‌توان محدوده GB را افزایش داد تا KMR کاهش یابد. بااین‌حال، طول دنباله بیت خام نیز کاهش می‌یابد. دلیل این است که با افزایش ψ، نمونه‌های کاوش بیشتری دور ریخته می‌شوند. باتوجه‌به رابطهٔ (۱۱)، P_{KDS} برابر می‌شود با:

$$P_{KDS} = P_r\{\phi_S^{(1)} \text{or } \phi_D^{(1)} \in \text{GB}\} \\ + P_r\{\phi_S^{(2)} \text{or } \phi_D^{(2)} \in \text{GB}\} \\ - P_r\{(\phi_S^{(1)} \text{or } \phi_D^{(1)} \in \text{GB}) \,\&(\phi_S^{(2)} \text{or } \phi_D^{(2)} \in \text{GB})\} \quad (۱۴) \\ = 2\,P_{KDS,0} - P_{KDS,0}^2$$

که $P_{KDS,0} = P_r\{\phi_S^{(1)} \text{or } \phi_D^{(1)} \in \text{GB}\}$ بوده و ضمناً تساوی آخر به علت تقارن در متغیرهای تصادفی و نیز استقلال فازهای $\phi_m^{(1)}$ و $\phi_m^{(2)}$ برقرار است. حال می‌بایست محاسبه گردد:

$$P_{KDS,0} = P_r\{\phi_S^{(1)} \in \text{GB}\} + P_r\{\phi_D^{(1)} \in \text{GB}\} \\ - P_r\{(\phi_S^{(1)},\phi_D^{(1)}) \in \text{GB}\} \quad (۱۵)$$

اکنون می‌خواهیم سه جملهٔ موجود در رابطه بالا را محاسبه کنیم.

باتکیه‌بر یکنواختی فازها، جمله اول برابر می‌شود با:

$$\begin{aligned} P_r\left\{\phi_S^{(1)} \in \text{GB}\right\} &= P_r\left\{\phi_S^{(1)} \in \text{GB 1 or } \phi_S^{(1)} \in \text{GB 2}\right\} \\ &= P_r\left\{\phi_S^{(1)} \in \text{GB 1}\right\} + P_r\left\{\phi_S^{(1)} \in \text{GB 2}\right\} \\ &- P_r\left\{\phi_S^{(1)} \in \text{GB 1 \& } \phi_S^{(1)} \in \text{GB 2}\right\} \\ &= 2P_r\left\{\phi_S^{(1)} \in \text{GB 1}\right\} = \frac{\psi}{\pi} \end{aligned} \quad (۱۶)$$

همچنین با تعریف کران‌های پایین و بالا برای GBهای ۱ و ۲ به ترتیب به‌صورت: $GB_{1L} = \frac{\pi}{2} - \frac{\psi}{2}$، $GB_{1U} = \frac{\pi}{2} + \frac{\psi}{2}$ و نیز $GB_{2L} = \frac{3\pi}{2} - \frac{\psi}{2}$ و $GB_{2U} = \frac{3\pi}{2} + \frac{\psi}{2}$، جمله دوم برابر می‌شود با:

$$\begin{aligned} &P_r\left\{\phi_D^{(1)} \in \text{GB}\right\} = P_r\left\{\phi_D^{(1)} \in \text{GB 1 or } \phi_D^{(1)} \in \text{GB 2}\right\} \\ &= P_r\left\{\phi_D^{(1)} \in \text{GB 1}\right\} + P_r\left\{\phi_D^{(1)} \in \text{GB 2}\right\} \\ &- P_r\left\{\phi_D^{(1)} \in \text{GB 1 \& } \phi_D^{(1)} \in \text{GB 2}\right\} \\ &= 2P_r\left\{\phi_D^{(1)} \in \text{GB 1}\right\} = 2\,P_r\left\{GB_{1L} < \phi_D^{(1)} < GB_{1U}\right\} \\ &= 2\left[F_{\phi_D^{(1)}}(GB_{1U}) - F_{\phi_D^{(1)}}(GB_{1L})\right] \end{aligned} \quad (۱۷)$$

در رابطهٔ فوق، تابع CDF برای $\phi_D^{(1)}$ یعنی $F_{\phi_D^{(1)}}(x)$ در توجه ۱ محاسبه شده است.

در نهایت جمله سوم به‌صورت زیر محاسبه می‌شود:

$$\begin{aligned} &P_r\left\{\left(\phi_S^{(1)}, \phi_D^{(1)}\right) \in \text{GB}\right\} \\ &= P_r\left\{\left(\phi_S^{(1)}, \phi_D^{(1)}\right) \in \text{GB 1}\right\} \\ &+ P_r\left\{\left(\phi_S^{(1)}, \phi_D^{(1)}\right) \in \text{GB 2}\right\} \overset{(*)}{=} 2P_r\left\{\left(\phi_S^{(1)}, \phi_D^{(1)}\right) \in \text{GB 1}\right\} \\ &= 2P_r\{GB_{1L} \le \phi_S + \phi_{sr} \le GB_{1U}, GB_{1L} \\ &\le \phi_S + \phi_{sr} + \epsilon_D \le GB_{1U}\} \\ &= 2\left[F_{\phi_S^{(1)},\phi_D^{(1)}}(GB_{1U}, GB_{1U})\right. \\ &- F_{\phi_S^{(1)},\phi_D^{(1)}}(GB_{1U}, GB_{1L}) - F_{\phi_S^{(1)},\phi_D^{(1)}}(GB_{1L}, GB_{1U}) \\ &\left.+ F_{\phi_S^{(1)},\phi_D^{(1)}}(GB_{1L}, GB_{1L})\right] \end{aligned} \quad (۱۸)$$

که (*) به‌خاطر تقارن GB 1 و GB 2 و نیز یکنواختی فازها برقرار است. در رابطهٔ فوق $F_{\phi_S^{(1)},\phi_D^{(1)}}(x,y)$ تابع CDF مشترک بوده که در توجه ۲ ارائه شده است. همچنین در این توجه، در خصوص چرایی تساوی آخر صحبت شده است.

در نهایت با قراردادن روابط (۱۶)-(۱۸) در رابطه (۱۵) و سپس نتیجه آن در رابطهٔ (۱۴)، احتمال دور ریزی کلیدها (P_{KDS}) محاسبه می‌شود.

۳-۳- نرخ تولید کلید خام:

اگر فرکانس نمونه‌برداری از کانال f_S باشد (برای هر دو کاربر)، در اینصوت، نرخ تولید کلید خام را می‌توان به صورت زیر تعریف کرد:

$$R_{raw} = f_s(1 - P_{KDS}) \quad (۱۹)$$

ازآنجایی‌که افزایش عرض باند ψ، کاهش هر دو ضرورت KMR و R_{raw} را به همراه دارد، انتخاب مناسب ψ برای برقراری تعادل بین این دو ضرورت بسیار مهم است. به‌عنوان مثال، ممکن است یک ایستگاه پایه در یک سیستم سلولی قابلیت تصحیح خطای بالایی داشته باشد و ضمناً نرخ تولید کلید بالا را بطلبد. در اینصورت KMR یک معیار مطلوب نیست و این یعنی یک ψ کوچک ترجیح داده می‌شود. در کاربردهای دیگر، به‌عنوان مثال، یک شبکه WSN، با توانایی پردازش داده پایین و الزامات نرخ کلید پایین، ابتدا باید کارایی KMR برآورده شود. بنابراین مقدار ψ باید به درستی افزایش یابد.

۴- تحلیل امنیتی طرح تولید کلید پیشنهادی

در این قسمت، از منظر تلاش شنودگر برای کشف کلید و نیز ظرفیت تولید کلید، امنیت طرح مورد ارزیابی قرار می‌گیرد.

۴-۱- تلاش شنودگر خارجی جهت کشف کلید:

حال می‌خواهیم ببینیم اگر شنودگری در شبکه وجود داشته باشد (حتی خود رله که یک شنودگر داخلی محسوب می‌شود)، آیا می‌تواند با شنود مراحل کاوش کانال، به کلید دست یابد؟ باتوجه‌به مراحل کاوش کانال، داشته‌های شنودگر به شرح زیر است:

۱) در مرحله اول کاوش کانال: ترکیبی از $\phi_S + \phi_{se}$ با $\phi_D + \phi_{de}$ در شنودگر دریافت می‌شود که قابل تفکیک از هم نیستند.

۲) در مرحله دوم کاوش کانال: در این مرحله، چون فاز ترکیبی در مرحله پیشین با فاز ϕ_{re} جمع می‌شود، شنودگر هیچ اطلاعی از فازهای تصادفی تزریقی و کانال قانونی بدست نمی‌آورد.

با عنایت به توضیحات فوق، شنودگر به‌هیچ‌وجه نمی‌تواند به کلیدی مشابه کلید آلیس (k_S) دست یابد. لذا می‌توان گفت که طرح تولید کلید پیشنهادی از منظر تلاش شنودگر، امن خواهد بود.

توجه شود که با راهکارهایی از قبیل توان متغیر برای آلیس و باب (وابسته به شرایط کانال‌های پرش اول و دوم)، می‌توان امنیت طرح را ارتقاء داد. حتی برای وقتی‌که رله بسیار نزدیک به منبع باشد، این تکنیک تخصیص توان متغیر، می‌تواند افزایش توان بیشتر به مقصد در مقایسه با منبع، ناحیه آسیب‌پذیری را سفر کند

.

۴-۲- ظرفیت تولید کلید:

طبق روابط موجود در [۳۳]، ظرفیت تولید کلید را می‌توان بصورت زیر بیان کرد:

$$I(h_{ab}; h_{ba}) - h(h_{ab}; h_{ae}) \le C_s \le I(h_{ab}; h_{ba}) \quad (۲۰)$$

که h_{ab}، h_{ba} و h_{ae} به ترتیب کانال‌های قانونی رفت، برگشت و

کانال شنود را معرفی می‌کنند. در سناریوی مورد مطالعه، می‌توان کران بالا برای ظرفیت را بصورت زیر معرفی کرد:

$$C_s^{Upper} = I(\underline{\phi_S};\underline{\phi_D}) \quad (۲۱)$$

که در آن $\underline{\phi_S} = [\phi_S^{(1)}, \phi_S^{(2)}]$ و نیز $\underline{\phi_D} = [\phi_D^{(1)}, \phi_D^{(2)}]$ می‌باشد. همچنین برای کران پایین می‌توان نوشت:

$$C_s^{Lower} = I\left(\underline{\phi_S};\underline{\phi_D}\right) - I\left(\underline{\phi_S};\underline{\phi_R},\underline{\phi_E}\right) \quad (۲۲)$$

در اینجا کران بالا محاسبه می‌گردد؛ چرا که به دلایل ذکر شده در بالا، رله و شنودگر خارجی، فازی با همبستگی پایین با کانال قانونی را تجربه خواهند کرد. در آینده، به محاسبهٔ کران پایین نیز خواهیم پرداخت.

با عنایت به آنکه آنتروپی یک متغیر تصادفی یکنواخت بر روی [a,b] به‌صورت $h(X) = \ln(b-a)$ و نیز آنتروپی یک متغیرتصادفی نرمال با واریانس σ^2 بصورت $h(X) = \ln(\sigma\sqrt{2\pi e})$ می‌باشد، لذا C_s^{Upper} به شرح زیر محاسبه می‌گردد:

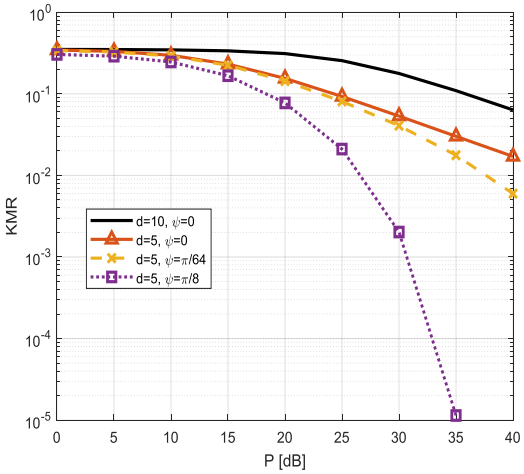
$$\begin{aligned}
C_s^{Upper} &= I\left(\underline{\phi_S};\underline{\phi_D}\right) = h\left(\underline{\phi_S}\right) - h\left(\underline{\phi_S}|\underline{\phi_D}\right) = \\
&[h(\phi_S^{(1)}) + h(\phi_S^{(2)}|\phi_S^{(2)})] - [h(\phi_S^{(1)},\phi_S^{(2)}|\phi_D^{(1)},\phi_D^{(2)})] \\
&= [h(\phi_S^{(1)}) + h(\phi_S^{(2)})] \\
&- [h(\phi_S^{(1)}|\phi_D^{(1)},\phi_D^{(2)}) \\
&+ h(\phi_S^{(2)}|\phi_D^{(1)},\phi_D^{(2)},\phi_S^{(1)})] \\
= [h(\phi_S^{(1)}) + h(\phi_S^{(2)})] &- [h(\phi_S^{(1)}|\phi_D^{(1)}) + h(\phi_S^{(2)}|\phi_D^{(2)})] \\
&= 2\ln(2\pi) - [h(\epsilon_S) + h(\epsilon_D)] \\
&= 2\ln(2\pi) - \ln\left(\sqrt{2\pi e}\,\sigma(\gamma_S)\right) \\
&- \ln\left(\sqrt{2\pi e}\,\sigma(\gamma_D)\right)
\end{aligned} \quad (۲۳)$$

می‌دانیم با افزایش SNR یا توان ارسالی، طبق رابطهٔ $\sigma(\gamma) = \sqrt{\frac{2}{2\gamma+1}}$ انحراف معیار کاهش می‌یابد. لذا طبق رابطهٔ به‌دست آمده در (۲۳)، ظرفیت تولید کلید افزایش خواهد یافت.

۵- شبیه‌سازی

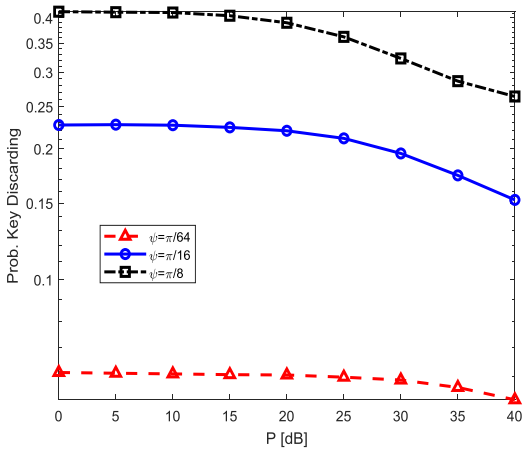
در این بخش، با ارائه نمودارهایی مبتنی بر روابط تحلیل ارائه شده، بینش‌های مهندسی خوبی پیرامون طرح تولید کلید پیشنهادی ارائه می‌گردد. در تمام شبیه‌سازی‌ها، توان نویز $\sigma_n^2 = 1$ و بهرهٔ رله $G = 1$ لحاظ شده است. همچنین همواره فرض شده است که رله در وسط مکان‌های آلیس و باب مستقر است.

در شکل (۴)، معیار KMR برحسب توان ارسالی توسط آلیس و باب (P) رسم شده است. معیار KMR همان P_{KM}^{Exact} می‌باشد. در این شکل، فاصله آلیس و باب $d = 10,5$ لحاظ شده است. همان‌طوری‌که مشاهده می‌شود با افزایش فاصله بین آلیس و باب، KMR افزایش می‌یابد که دلیل آن کاهش SNR دریافتی در گره‌ها است و در نتیجه افزایش خطای کلید را به همراه خواهد داشت. همچنین در این شکل، تأثیر باند محافظ ψ دیده می‌شود. واضح است که با حضور ψ در پروتکل تولید کلید، به دلیل دور ریختن نمونه‌های موجود در حوالی مرزهای تصمیم، معیار KMR کاهش می‌یابد. اما می‌دانیم که به دلیل دور ریختن نمونه‌های بیشتر، KGR کاهش می‌یابد. نکته طراحی خوبی که از این شکل می‌توان استنتاج کرد این است که اگر کدینگ به‌کارگرفته شده در پروتکل تولید کلید، قابلیت تصحیح خطای مثلاً ۱۰٪ داشته باشد و ضمناً گره‌ها بتوانند تا $P = 23$ dBW را مصرف کنند، شکل (۴) می‌گوید که گیرنده با GB برابر با $\psi = \frac{\pi}{64}$ بهترین گزینه است (در مقایسه با $\psi = \frac{\pi}{8}$). زیرا هم KGR بیشتر و هم نرخ خطای بیت کمتر از ۱۰٪ دارد که با کدینگ قابل جبران است.



شکل (۴): نرخ عدم تطابق کلید برحسب توان ارسالی آلیس و باب

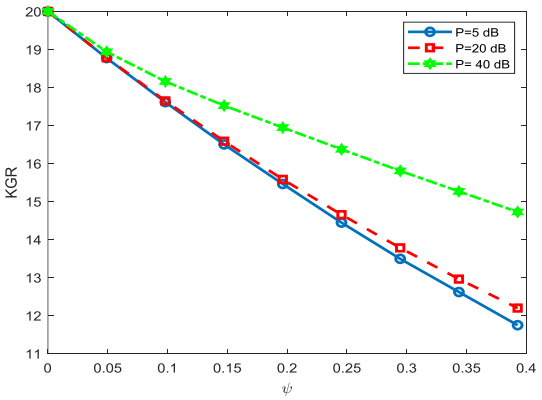
در شکل (۵)، احتمال دور ریزی کلید برحسب P برای ψهای مختلف رسم شده است. همان‌طوری‌که قابل پیش‌بینی بود با افزایش GB، نرخ دور ریزی افزایش می‌یابد. نکته قابل توجه در این شکل‌ها این است که با افزایش توان P، این نرخ دور ریزی کاهش چشمگیری نمی‌کند.



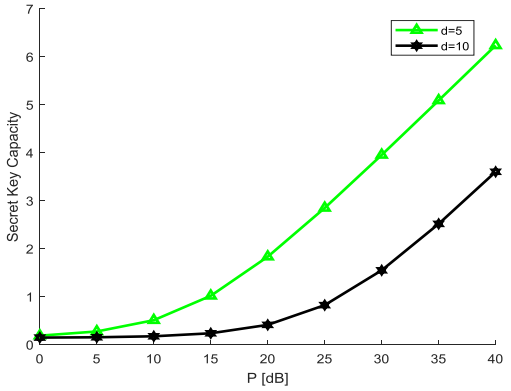
شکل (۵): احتمال دور ریزی کلید برحسب توان ارسالی آلیس و باب

حال می‌خواهیم ببینیم نرخ تولید کلید برحسب عرض باند محافظ ψ چگونه رفتاری دارد. در شکل (۶)، KGR رسم شده است. در این شکل $d = 5$ و ضمناً نرخ نمونه‌برداری از کانال $f_s = 10$ لحاظ گردیده است. توان‌های ارسالی آلیس و باب $P = 5\,,20\,,40\,dB$ لحاظ شده‌اند. در این شکل مشاهده می‌شود که برای $\psi = 0$ یعنی وقتی GB وجود نداشته باشد، حداکثر نرخ تولید کلید خام، یعنی ۲۰ بیت در ثانیه حاصل می‌گردد. با افزایش GB، از آنجایی‌که دور ریزی بیت‌ها بیشتر می‌شود، KGR نیز کاهش می‌یابد. یک راه جبران چنین موردی، افزایش توان ارسالی توسط گره‌ها است. توجه شود که با مقایسه شکل (۶) و شکل (۴) نتایج خوبی قابل استخراج است. مثلاً اگر کدینگ با قابلیت خطای حدود ۱۰٪ داشته باشیم، صرف توان 20 dB می‌توان به نرخ تولید کلید واقعی (نه خام) نزدیک به کران بالا یعنی ۲۰ بیت در ثانیه دست یافت.

در شکل (۷) نیز ظرفیت کلید مخفی بر اساس رابطه تحلیلی به‌دست آمده، رسم گردیده است. در این شکل، فاصله آلیس و باب برابر با $d = 10$ و $d = 5$ بوده و رله دقیقاً در وسط قرار گفته است. مشخص است که با افزایش توان ارسالی، ظرفیت روندی صعودی دارد. همچنین مشاهده می‌کنیم که با افزایش فاصله گره‌ها، ظرفیت کاهش می‌یابد.



شکل (۶): نرخ تولید کلید برحسب عرض باند ψ



شکل (۷): کران بالای ظرفیت تولید کلید برای طرح پیشنهادی

۶- نتیجه‌گیری

در این مقاله، یک طرح SKG نوین مبتنی بر استخراج کلید از فاز کانال و در حضور یک رلهٔ غیرقابل‌اعتماد ارائه گردید. سیگنال‌های کاوش کانال از جنس فاز تصادفی گسسته BPSK بوده و در گیرنده نیز از کوانتیزه کننده تک‌بیتی استفاده می‌شود. به‌منظور کاهش نرخ خطای کلید، از کوانتیزاسیون با GB استفاده گردید. برای چنین سناریویی، روابطی برای نرخ تطبیق کلید، KMR، KDR به‌ازای هر کاوش کانال و نیز KGR ارائه گردید. همچنین ظرفیت کلید مخفی ارزیابی شد و دیدیم که شنودگر خارجی با رهگیری مراحل کاوش کانال نمی‌تواند کلید را کشف کند.

۶. 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] A. Chorti, A. N. Barreto, S. Kopsell, M. Zoli, M. Chafii, P. Sehier, G. Fettweis, and H. V. Poor, "Context-aware security for 6G wireless The role of physical layer security," 2021, arXiv:2101.01536. [Online]. Available: https://arxiv.org/abs/2101.01536.

[3] 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.

[4] J. Zhang, S. Rajendran, Z. Sun, R. Woods and L. Hanzo, "Physical layer security for the Internet of Things: Authentication and key generation," IEEE Wireless Commun., vol. 26, no. 5, pp. 92–98, Oct. 2019.

[5] 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.

[6] J. Zhang, A. Marshall and L. Hanzo, "Channel-envelope differencing eliminates secret key correlation: LoRa-based key generation in low power wide area networks," IEEE Trans. Veh. Technol., vol. 67, no. 12, pp. 12462–12466, Dec. 2018.

[7] C. Zenger, H. Vogt, J. Zimmer, A. Sezgin and C. Paar, "The passive eavesdropper affects my channel: Secret-key rates under real-world conditions," in 2016 IEEE GLOBECOM Workshops (GC Wkshps), Washington, DC, USA, Dec. 2016, pp. 1–6.

[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] G. Epiphaniou, P. Karadimas, D. Kbaier Ben Ismail, H. Al-Khateeb, A. Dehghantanha and K. -K. R. Choo, "Non-reciprocity 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, Aug. 2018.
[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. Edman and A. Kiayias, "On passive inference attacks against physical-layer key extraction?" in Proc. 4th Eur. Workshop Syst. Security, 2011, p. 8.
[16] S. Eberz, M. Strohmeier, M. Wilhelm, and I. Martinovic, "A practical man-in-the-middle attack on signal-based key generation protocols," in Proc. Eur. Symp. Res. Comput. Security, 2012, pp. 235–252.
[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. (In Persian) https://dor.isc.ac/dor/20.1001.1.23224347.1401.10.2.3.9
[26] 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.
[27] C. D. T. Thai, J. Lee and T. Q. S. Quek, "Physical-layer secret key generation with colluding untrusted relays," IEEE Trans. Wireless Commun., vol. 15, no. 2, pp. 1517-1530, Feb. 2016.
[28] M. Letafati, A. Kuhestani, H. Behroozi, and D. W. K. Ng, "Jammingresilient frequency hopping-aided secure communication for Internet-of-Things in the presence of an untrusted relay," IEEE Trans. Wireless Commun., vol. 19, no. 10, pp. 6771–6785, Oct. 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] J. Zhang, B. He, T. Q. Duong, and R. Woods, On the Key Generation from Correlated Wireless Channels, IEEE Commun., Lett., 2007.