Scientific Journal of Electronical & Cyber Defence
Vol. 10, No. 2, Summer 2022, Serial No. 38

Security Evaluation of the Mutual Random Phase Injection Scheme for Secret Key Generation over Static Point-to-Point Communications

A. Khalili Tirandaz*, A. Koohestani

* Instructor, Computer Department, Qom University of Technology, Qom, Iran

(Received: 03/04/2021, Accepted: 18/01/2022)

ABSTRACT

The physical layer secret key generation schemes, usually have two serious challenges in static point-to-point communications: 1) low key generation rate due to the low entropy of channel state information and 2) security vulnerability at non-proximity regions due to spatial correlation. To solve the first challenge, the local random generator-based schemes can be used. One of these schemes is mutual random phase injection, in which the channel probing signals with random phase are exchanged between the legitimate parties. In this paper, the security of the aforementioned scheme is reviewed in a static point-to-point link with a geometric secrecy approach. For this purpose, the vulnerability regions and secrecy regions are determined, and then a closed expression is provided for the key error probability. Moreover, based on the entropy analysis, the amount of eavesdropper's equivocation about the key is calculated. The analytical results show that the eavesdropper's equivocation is very low in static environments. In order to eliminate this weakness, we propose the idea of probing over multiple carrier frequencies instead of just one frequency. The aim of this idea is to alter the equivalent channel phase, which leads to a significant increase in the key entropy. As an example, the analytical results show that in static environments if single-bit quantization is utilized, the eavesdropper's equivocation about the key equals the number of different carrier frequencies which are used in the probing phase; so if the channel probing is performed on a single frequency, the eavesdropper's equivocation would be only one bit, while, using the suggested idea, the eavesdropper's equivocation would be multifold. The simulation results show that if the probing process is performed on several frequencies, the vulnerability regions will decrease and the secrecy regions will increase. Finally, some suggestions are provided for further research in this field.

Keywords: Physical layer security, Secret key generation, Geometric secrecy.

* Corresponding Author Email: Tirandaz@chmail.ir

نشریه علمی "پدافند الکترونیکی و سایبری"
سال دهم، شماره ۲، تابستان ۱۴۰۱، ص ۳۰-۱۹

علمی-پژوهشی

ارزیابی امنیت طرح تزریق متقابل فاز تصادفی جهت تولید کلید مخفی در ارتباطات نقطه به نقطه ایستا

امیرحسین خلیلی تیرانداز[1*]، علی کوهستانی[2]
۱- مربی، گروه کامپیوتر، ۲- استادیار، گروه مخابرات و الکترونیک، دانشگاه صنعتی قم، قم، ایران
(دریافت: ۱۴۰۰/۰۱/۱۴، پذیرش: ۱۴۰۰/۱۰/۲۸)

چکیده

طرح‌های تولید کلید مخفی لایه فیزیکی، در ارتباطات نقطه به نقطه ایستا، معمولاً دو چالش جدی دارند: ۱) نرخ پایین تولید کلید، به دلیل کم بودن آنتروپی اطلاعات حالت کانال و ۲) آسیب‌پذیری امنیتی در نواحی غیر مجاور، به دلیل همبستگی فضایی. برای رفع چالش اول می‌توان از طرح‌های مبتنی بر مولدهای تصادفی محلی استفاده کرد. یکی از این طرح‌ها، طرح تزریق متقابل فاز تصادفی است که در آن، سیگنال‌های کاوش کانال با فاز تصادفی، بین طرفین مبادله می‌شود. در این مقاله، امنیت طرح مذکور در یک پیوند نقطه به نقطه ایستا با رویکرد محرمانگی هندسی مورد بازنگری قرار می‌گیرد. بدین منظور، نواحی آسیب‌پذیر و نواحی محرمانه مشخص شده و سپس یک رابطه بسته برای احتمال خطای کلید ارائه می‌شود. همچنین با تحلیل آنتروپی، میزان ابهام شنودگر در مورد کلید محاسبه شده است که نتایج تحلیلی نشان می‌دهد در محیط‌های ایستا، این معیار بسیار کم است. به‌منظور رفع این نقطه ضعف، در این مقاله ایده کاوش کانال روی چندین فرکانس حامل - به جای یک فرکانس- پیشنهاد شده است. هدف از این ایده، پویاسازی فاز کانال معادل است که منجر به افزایش قابل توجه آنتروپی کلید می‌گردد. به‌عنوان مثال، نتایج تحلیلی نشان می‌دهد که در محیط‌های ایستا اگر از کوانتیزاسیون تک بیت استفاده شود، ابهام شنودگر در خصوص کلید، برابر است با تعداد فرکانس‌های حامل متفاوتی که در مرحله کاوش کانال استفاده می‌شود؛ بنابراین اگر کاوش کانال بر روی یک فرکانس انجام شود، ابهام شنودگر در مورد کلید، فقط یک بیت خواهد بود در حالی که اگر از ایده پیشنهادی استفاده شود، ابهام شنودگر چندین برابر خواهد شد. همچنین نتایج شبیه‌سازی نشان می‌دهد در صورت کاوش کانال روی چند فرکانس حامل، نواحی آسیب‌پذیر کاهش و نواحی محرمانه افزایش می‌یابد. در انتهای مقاله، پیشنهاداتی جهت ادامه فعالیت‌های تحقیقاتی در این زمینه ارائه شده است.

کلیدواژه‌ها: امنیت لایه فیزیکی، تولید کلید مخفی، محرمانگی هندسی

۱- مقدمه

یکی از فناوری‌های مهم در نسل پنجم شبکه‌های سیار (5G)، اینترنت اشیاء[1] (IoT) است [۱]. این فناوری شامل شبکه‌های حسگر بی‌سیم[2] (WSN)، سامانه‌های فیزیکی - سایبری[3] (CPS) و و به ویژه ارتباطات برد کوتاه[4] (SRC) [۲] نظیر تگ‌های RFID[5] [۳]، ارتباطات برد کوتاه اختصاصی [۴]، ارتباطات دستگاه به دستگاه[6] (D2D) و استاندارد *ZigBee* است. از این فناوری، در شهرهای هوشمند، ترافیک هوشمند، حوزه سلامت و اتوماسیون صنعتی استفاده می‌شود.

در فناوری IoT، تجهیزات مختلفی نظیر حسگرها و محرک‌ها در مقیاس زیاد مورد استفاده قرار می‌گیرند. این تجهیزات باید قابلیت اتصال بی‌سیم دو به دو را داشته باشند. این مهم، نیازمند یک بستر ارتباطی بی‌سیم، غیر متمرکز و مقیاس‌پذیر است. در چنین بستری حجم زیادی از اطلاعات خصوصی و محرمانه مبادله می‌شود که با توجه به ماهیت پخش همگانی ارتباطات بی‌سیم، در معرض تهدیدات امنیتی مختلفی نظیر شنود و اختلال است.

برای جلوگیری از شنود، معمولاً از روش‌های رمزنگاری استفاده می‌شود. روش‌های رمزنگاری، غالباً مبتنی بر پیچیدگی محاسبات هستند و در لایه‌های بالای شبکه (بالاتر از لایه فیزیکی) استفاده می‌شوند. همچنین این روش‌ها به واسطه نیاز به طرح‌های مدیریت کلید، برای استفاده در بسترهای نامتمرکزی نظیر IoT با چالش جدی عدم مقیاس‌پذیری مواجه‌اند.

در سال‌های اخیر، حوزه جدیدی تحت عنوان امنیت لایه

* رایانامه نویسنده مسئول: Tirandaz@chmail.ir
[1] Internet-of-Things (IoT)
[2] Wireless Sensor Networks (WSN)
[3] Cyber-Physical System (CPS)
[4] Short Range Communication (SRC)
[5] Radio Frequency Identification
[6] Device-to-Device

ناشر: دانشگاه جامع امام حسین (ع)

فیزیکی[1] - یا به اختصار PLS - ارائه شده است [۵ و ۶]. در طرح‌های PLS، از ویژگی‌های کانال فیزیکی برای تأمین امنیت ارتباطات استفاده می‌شود و امنیت آن‌ها عمدتاً مبتنی بر نظریه اطلاعات است.

طرح‌های PLS در مقایسه با روش‌های رمزنگاری، سربار کمتری دارند و بنابراین برای استفاده در بسترهای دارای قدرت پردازشی و توان مصرفی پایین نظیر IoT مناسب هستند [۷]. همچنین، طرح‌های PLS در مقایسه با طرح‌های رمزنگاری قابلیت مقیاس پذیری بسیار بالاتری دارند، در نتیجه علاوه بر بسترهای متمرکز، در بسترهای ارتباطی نامتمرکز نیز به سادگی قابل استفاده‌اند. دلیل این موضوع این است که طرح‌های PLS عمدتاً فاقد کلیدند و بنابرین به طرح‌های مدیریت کلید نیاز ندارند اما طرح‌های رمزنگاری مبتنی بر کلید و نیازمند مدیریت کلید هستند.

طرح‌های PLS به سه دسته قابل تقسیم‌اند:
۱. مخابره محرمانه در لایه فیزیکی[2] (PLST)
۲. تولید کلید مخفی در لایه فیزیکی[3] (SKG)
۳. احراز هویت لایه فیزیکی[4] (PLA)

در بین این طرح‌ها، طرح‌های SKG کاربردی‌ترند. در طرح‌های SKG، طرفین ارتباط به یک کلید محرمانه مشترک دست می‌یابند و می‌توانند از آن در رمز کننده‌های لایه‌های مختلف شبکه استفاده کنند. در طرح‌های SKG، از مشخصاتی نظیر فاز کانال، قدرت سیگنال دریافتی[5]، اطلاعات حالت کانال[6] و سایر ویژگی‌های کانال جهت تولید کلید مخفی استفاده می‌شود [۸].

در مرجع [۹] یک طرح SKG کارآمد و عملی برای ارتباطات IoT و WSN پیشنهاد شده است. نتایج تجربی مرجع [۹] نشان می‌دهد که طرح LiSK در محیط‌های درون و بیرون ساختمان و نیز برای پیوندهای برد بلند، هم از منظر برابری کلید در طرفین مجاز و هم از منظر میزان نشت کلید به شنودگر از طرح‌های پیشین کارآمدتر است. نویسندگان [۱۰]، برای اولین بار یک طرح SKG با نرخ بالا برای سامانه LoRa[7] ارائه دادند. در مرجع [۱۰]، متفاوت با کارهای مرسوم، یک طرح اصلاح اطلاعات مبتنی بر حسگری فشرده ارائه شده است. با هدف بهبود طرح ارائه شده در مرجع [۱۰]، پژوهشگران در مرجع [۱۱] با به‌کارگیری آنتن‌های قابل تنظیم و نیز پردازش بر روی RSS[8] دریافتی توانستند طرح‌هایی برای تولید کلید پیشنهاد دهند که بر تأخیر زیاد در فاز کاوش کانال فائق آمده و به خوبی بتواند کلید رمزنگاری را بروز نماید. توجه شود که در طرح‌های ارائه شده در مراجع [۱۱–۹] از RSS سیگنال دریافتی به‌منظور تولید کلید استفاده می‌شود.

همچنین در مرجع [۱۲] نویسندگان، به ارائه یک طرح مقاوم در برابر جمینگ و شنود برای ارتباطات D2D پرداخته‌اند. در این مرجع، با تکیه بر تخمین اطلاعات حالت کانال[9] (CSI)، یک کلید محرمانه به‌دست می‌آید که این کلید هم به‌منظور رمز کردن داده‌ها و هم تولید الگوی پرش فرکانسی به‌کار گرفته شده است. در توسعه مرجع [۱۲]، پژوهشگران در مرجع [۱۳] یک طرح تولید کلید لایه فیزیکی برای شبکه‌های مشارکتی مبتنی بر رله غیر قابل اعتماد پیشنهاد داده‌اند. در این مرجع، به‌منظور ارزیابی طرح تولید کلید پیشنهادی، نرخ تولید کلید و نیز نرخ محرمانه ارگادیک به‌صورت روابط ریاضی ارائه شده‌اند.

بر خلاف ارتباطات برد بلند، در ارتباطات برد کوتاه، تجهیزات مورد استفاده معمولاً از نظر منابع پردازشی و توان مصرفی با محدودیت‌های زیادی مواجه‌اند. این مسئله باعث می‌شود که استفاده از روش‌های متداول رمزنگاری در ارتباطات برد کوتاه با چالش‌های زیادی همراه باشد. با ظهور فناوری PLS و به ویژه طرح‌های SKG امید می‌رود که بسیاری از این چالش‌ها مرتفع گردد [۷ و ۸]. با این حال، استفاده از طرح‌های SKG نیازمند وجود یک منبع آنتروپی هم پاسخ در کانال ارتباطی است اما در سامانه‌های ارتباطاتی برد کوتاه چنین منبعی وجود ندارد. در این سامانه‌ها، مخابره پیام در مسافت‌های کوتاه انجام می‌شود و در نتیجه SNR[10] دریافتی نسبتاً زیاد بوده و پدیده محوشدگی وجود ندارد. این ویژگی‌ها باعث می‌شود که امکان استفاده از طرح‌های متداول SKG که صرفاً مبتنی بر آنتروپی کانال هستند، وجود نداشته باشد. البته این مشکل منحصر به ارتباطات برد کوتاه نیست بلکه در هر کانالی که به‌صورت AWGN قابل مدل‌سازی باشد مطرح است.

از منظر امنیت، چالشی‌ترین سناریو در طرح‌های SKG، سناریوی ارتباطات فضای - آزاد[11] است که در آن تمام پیوندهای ارتباطی اعم از پیوند قانونی و پیوندهای شنود از نوع دید مستقیم[12] هستند و همگی به‌صورت AWGN مدل‌سازی می‌شوند. بر این اساس، در این مقاله، سناریوی ارتباطاتی دید مستقیم در فضای آزاد مورد بررسی قرار گرفته است.

[1] Physical Layer Security
[2] Physical Layer Secrecy Transmission (PLST)
[3] Secret Key Generation (SKG)
[4] Physical Layer Authentication (PLA)
[5] Received Signal Strength (RSS)
[6] Channel State Information (CSI)
[7] Long-Range
[8] Received Signal Strength
[9] Channel State Information
[10] Signal-to-Noise-Ratio (SNR)
[11] Free Space
[12] Line-of-Sight (LoS)

در این مقاله، با تمرکز بر طرح ارائه شده در مرجع [۱۴] و با هدف اصلاح و تکمیل تحلیل‌های آن، امنیت این طرح با رویکرد محرمانگی هندسی[1] در یک کانال مخابراتی ایستا[2] مورد بازنگری قرار گرفته است. مشابه مرجع [۱۴]، فرض می‌شود که مخابره در فضای آزاد صورت می‌پذیرد. در طرح مذکور که مبتنی بر فاز است، طرفین ارتباط (آلیس و باب) سیگنال‌هایی با فاز تصادفی را تولید و متقابلاً برای یکدیگر ارسال می‌کنند.

در این مقاله، پس از مرور طرح ارائه شده در مرجع [۱۴]، نواحی آسیب‌پذیر[3] را به‌صورت تحلیلی به‌دست آورده و با کمک شبیه‌سازی، نواحی محرمانه[4] مشخص می‌شود. در این مقاله نشان داده می‌شود که برخی از تحلیل‌ها و نتایج ارائه شده در مرجع [۱۴]، ایراد اساسی دارد.

در این پژوهش، برای اولین بار با تحلیل آنتروپی، میزان ابهام[5] شنودگر در مورد کلید به‌دست آمده است. نتایج تحلیلی ارائه شده در این مقاله نشان می‌دهد در محیط‌های ایستا، آنتروپی کلید از منظر شنودگر بسیار کم است. به‌منظور رفع این نقطه ضعف، ایده اجرای روال کاوش کانال، روی چندین فرکانس حامل - به جای یک فرکانس - پیشنهاد شده است. هدف از این ایده، پویاسازی فاز کانال معادل و در نتیجه افزایش قابل توجه آنتروپی کلید است. به‌عنوان مثال، در صورت استفاده از کوانتیزاسیون تک بیت، نتایج تحلیلی نشان می‌دهد که در شرایط ایستا اگر کاوش کانال بر روی یک فرکانس انجام شود، ابهام شنودگر در مورد کلید تنها یک بیت خواهد بود؛ حال آنکه با استفاده از ایده پیشنهاد شده در این مقاله، ابهام شنودگر از کلید به اندازه تعداد فرکانس‌های متفاوت مورد استفاده در مرحله کاوش کانال است.

نتایج شبیه‌سازی مؤید این واقعیت است که اجرای کاوش کانال بر روی چند فرکانس حامل، باعث کاهش نواحی آسیب‌پذیر و افزایش نواحی محرمانه می‌شود. بر این اساس، برخی شهودهای مهندسی برای طراحی ارائه شده است.

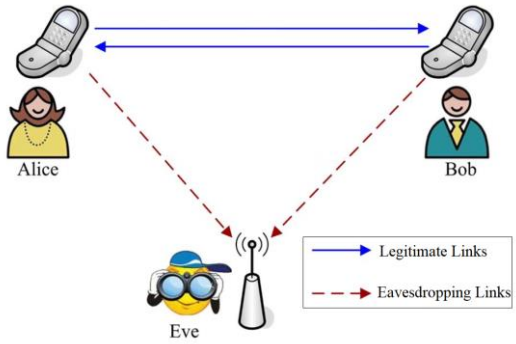
همچنین در این مقاله، کارایی طرح از منظر عملکردی با استفاده از معیار احتمال خطای کلید، مورد ارزیابی قرار گرفته است. با توجه به توضیحات فوق، مقاله پیش رو می‌تواند به‌عنوان مبنایی جهت ارزیابی طرح‌های SKG مورد استفاده قرار بگیرد.

در انتهای مقاله، پیشنهاداتی جهت ادامه فعالیت‌های تحقیقاتی در این زمینه ارائه شده است.

[1] Geometric Secrecy
[2] Static
[3] Vulnerability Regions
[4] Secrecy Regions
[5] Equivocation

۲- تولید کلید مبتنی بر تزریق متقابل فاز تصادفی

در این بخش، پس از مرور طرح ارائه شده در مرجع [۱۴]، این طرح را از نظر محرمانگی هندسی مورد تحلیل و بررسی قرار داده می‌شود و در ادامه نواحی آسیب‌پذیر و نواحی محرمانه برای این طرح مشخص می‌شود.



شکل (۱): مدل سامانه

۲-۱- بیان طرح

مطابق شکل (۱)، مدل سامانه شامل یک جفت کاربر مجاز (آلیس و باب) و یک شنودگر (ایو) است. در مرحله کاوش کانال، آلیس و باب، به‌طور جداگانه سیگنال‌هایی با فاز تصادفی یکنواخت در بازه $[0,2\pi)$ را تولید کرده و برای طرف مقابل مخابره می‌کنند. فاز سیگنال ارسالی آلیس و باب به ترتیب با ϕ_A و ϕ_B نشان داده می‌شود و فاز کانال قانونی با ϕ_{AB} مشخص می‌شود. به این ترتیب فاز سیگنال دریافتی آلیس و باب به ترتیب برابر است با:

$$\hat{\phi}_A = \phi_B + \phi_{AB} + \epsilon_A \mod 2\pi \quad (۱)$$

$$\hat{\phi}_B = \phi_A + \phi_{AB} + \epsilon_B \mod 2\pi \quad (۲)$$

که در آن، ϵ_A و ϵ_B، خطاهای ناشی از عوامل مخربی نظیر نویز، تداخل[6] و نقیصه‌های سخت‌افزاری[7] هستند.

فاز سیگنال‌های دریافتی شنودگر از آلیس و باب به ترتیب برابر است با:

$$\hat{\phi}_{AE} = \phi_A + \phi_{AE} + \epsilon_{AE} \mod 2\pi \quad (۳)$$

$$\hat{\phi}_{BE} = \phi_B + \phi_{BE} + \epsilon_{BE} \mod 2\pi \quad (۴)$$

[6] در این مقاله فرض می‌شود که مجموع توان تداخل‌های دریافتی در مقایسه با توان سیگنال دریافتی، ناچیز است. بنابراین تداخل صرفاً باعث افزایش کف نویز می‌شود.

[7] Hardware Impairment

که در آن، ϕ_{AE} و ϕ_{BE} به ترتیب بیانگر فاز کانال آلیس – شنودگر و باب – شنودگر هستند. در ضمن ϵ_{AE} و ϵ_{BE} خطاهای ناشی از عوامل مخربی همچون نویز حرارتی، تداخل و عیوب سخت‌افزاری هستند. برای تولید کلید، هر کدام از کاربران مجاز (آلیس و باب)، سیگنال ارسالی خود را و در سیگنال دریافتی از طرف مقابل، ضرب کرده و فاز حاصل‌ضرب[1] را به‌عنوان یک مقدار همبسته برای تولید کلید مورد استفاده می‌دهند. این مقادیر در آلیس و باب به ترتیب برابرند با:

$$\hat{\theta}_A = \phi_A + \phi_B + \phi_{AB} + \epsilon_A \mod 2\pi \quad (۵)$$

$$\hat{\theta}_B = \phi_A + \phi_B + \phi_{AB} + \epsilon_B \mod 2\pi \quad (۶)$$

مقادیر $\hat{\theta}_A$ و $\hat{\theta}_B$ یک ترم مشترک دارند. این ترم مشترک که با θ نشان داده می‌شود برابر با $\phi_A + \phi_B + \phi_{AB}$ است. این مقدار مشترک، یک متغیر تصادفی با توزیع یکنواخت در بازه $[0,2\pi)$ است. با افراز بازه $[0,2\pi)$ به تعدادی زیر بازه (کوانتیزاسیون فاز) و استفاده از یک نگاشت (نظیر نگاشت Gray)، آلیس و باب از روی مقادیر $\hat{\theta}_A$ و $\hat{\theta}_B$ به یک قطعه کلید باینری می‌رسند. وجود نویز و نقیصه‌های سخت‌افزاری باعث عدم برابری ϵ_A و ϵ_B و در نتیجه اختلاف $\hat{\theta}_A$ و $\hat{\theta}_B$ می‌شود. بنابراین مطابق شکل (۲) تعدادی ناحیه محافظ[2] در بازه $[0,2\pi)$ درنظر گرفته می‌شود. اگر $\hat{\theta}_A$ یا $\hat{\theta}_B$، در نواحی محافظ قرار داشته باشند، مقادیر مذکور دور ریخته می‌شود و از آن‌ها برای تولید کلید استفاده نمی‌شود. در چنین شرایطی به دلیل نزدیک بودن مقادیر $\hat{\theta}_A$ یا $\hat{\theta}_B$ به مرز نواحی کوانتیزاسیون، احتمال عدم برابری کلید بالاست.

در ادامه سایر مراحل استخراج کلید تشریح شده است. فرض کنید L تعداد سطوح کوانتیزاسیون و در نتیجه تعداد بیت‌های مستخرج از هر سمبل $\hat{L} = \log L$ بیت باشد[3]. همچنین ψ بیانگر عرض نواحی محافظ باشد. مثلاً در شکل (۲) دارید: $L = 4$ و $\psi = \frac{\pi}{32}$. حال هر کدام از کاربران مجاز یعنی آلیس و باب، با توجه به مقادیر L و ψ مقادیر زیر را محاسبه می‌کنند:

$$s_m \triangleq \left\lfloor \frac{\hat{\theta}_m}{2\pi/L} \right\rfloor, s_m^+ \triangleq \left\lfloor \frac{\hat{\theta}_m + \psi/2}{2\pi/L} \right\rfloor, s_m^- \triangleq \left\lfloor \frac{\hat{\theta}_m - \psi/2}{2\pi/L} \right\rfloor \quad (۷)$$

که نماد $\lfloor . \rfloor$ بیانگر جزء صحیح x و $m \in \{A, B\}$ است. سپس آلیس و باب، قطعات کلید خود را به‌صورت زیر محاسبه می‌کنند:

$$k_m = \begin{cases} B(s_m) & if \quad s_m^+ = s_m^- \\ \emptyset & Otherwise, \end{cases} \quad (۸)$$

در این رابطه، $B(x)$ دنباله باینری متناظر با x با طول $\hat{L}$ است و همچنین $\emptyset$، نماد یک دنباله باینری به طول صفر است. به‌عنوان مثال در شکل (۲)، در صورتی که از نگاشت Gray استفاده شود آنگاه

$B(s_m) \in \{00,01,10,11\}$ خواهد بود.

توجه ۱: وقتی مقدار k_m به‌دست آمده در آلیس یا باب برابر با $\emptyset$ شود، کاربر مورد نظر 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 و این طرح باید دوباره از ابتدا تکرار شود.

توجه ۲: با افزایش تعداد سطوح کوانتیزاسیون (L)، تعداد بیت‌های قابل استخراج $(\hat{L})$ افزایش می‌یابد و در نتیجه نرخ تولید کلید، زیاد خواهد شد. ولی به دلیل کوچک شدن نواحی تصمیم، اثر نویز روی عدم تطابق کلیدها بیشتر می‌شود و به دلیل بیشتر شدن تعداد نواحی محافظ، نرخ دور ریزی کلید نیز افزایش می‌یابد.

توجه ۳: با هر بار اجرای طرح فوق، دو رشته بیت همبسته با طول کوتاه (مثلاً ۲ بیت) در آلیس و باب به‌دست می‌آید که به آن‌ها *قطعه کلید*[4] گفته می‌شود. با اجرای مکرر این روال و کنار هم قرار دادن قطعات کلید، رشته بیت‌های همبسته با طول زیاد (K_A برای آلیس و K_B برای باب) در طرفین حاصل می‌گردد که به آن‌ها *کلید خام*[5] گفته می‌شود. *کلید نهایی*[6] پس از اجرای رویه‌های اصلاح اطلاعات[7]، بررسی سازگاری[8] و ارتقای محرمانگی[9] به‌دست می‌آید. این موارد خارج از حیطه این مقاله است. برای کسب اطلاعات بیشتر در این زمینه می‌توان به مرجع [۸] مراجعه کرد.

توجه ۴: در طرح‌های SKG، در مرحله بررسی سازگاری کلیدها، آلیس چکیده‌ای از کلید خام خود را برای باب ارسال می‌کند و باب مقدار دریافتی را با چکیده کلید خام خودش مقایسه کرده و یک پیام ACK (در صورت برابری) یا NACK (در صورت نابرابری) برای آلیس می‌فرستد. اگر فرآیند SKG به هر دلیلی ناموفق باشد (یعنی آلیس و باب به کلید یکسان دست نیابند)، با توجه به عمومی بودن سیگنال‌های ACK و NACK، شنودگر نیز از این موضوع مطلع شده و در نتیجه کلید مورد نظر را دور می‌ریزد.

---

[1] توجه شود که فاز حاصل‌ضرب دو سیگنال، برابر است با حاصل‌جمع فاز آن‌ها در پیمانه 2π.

[2] Guard Zone

[3] در این مقاله، پایه لگاریتم برابر با ۲ است.

[4] Partial Key

[5] Raw Key

[6] Final Key

[7] Information Reconciliation

[8] Consistency Check

[9] Privacy Amplification

۲-۲- سناریوی شنود

فرض کنید تعدادی شنودگر در محیط توزیع شده‌اند. هر یک از شنودگرها، به‌طور جداگانه اقدام به شنود سیگنال کاوش کانال ارسال شده توسط آلیس و باب می‌کنند و فاز حاصل‌ضرب این دو سیگنال را به‌عنوان تخمین θ درنظر می‌گیرد. تخمین شنودگر از θ را با $\hat{\theta}_E$ نشان داده می‌شود. با توجه به روابط (۳ و ۴)، دارید:

$$\hat{\theta}_E = \phi_A + \phi_B + \phi_E + \epsilon_{AE} + \epsilon_{BE} \mod 2\pi \qquad (۹)$$

در رابطه (۹) $\phi_E = \phi_{AE} + \phi_{BE}$ است. مقایسه رابطه (۹) و روابط (۵ و ۶) نشان می‌دهد که هر گاه رابطه $\phi_{AB} = \phi_E$ برقرار باشد - یعنی مجموع فاز کانال‌های شنود با فاز کانال قانونی برابر باشد - مقدار $\hat{\theta}_E$ و مقادیر $\hat{\theta}_A$ و $\hat{\theta}_B$ همبستگی بالایی خواهند داشت و بنابراین در چنین شرایطی، شنودگر با کوانتیزه کردن $\hat{\theta}_E$، با احتمال زیاد، به کلید مشترک آلیس و باب منجر می‌شود. در نتیجه شنودگر می‌تواند کلید را به‌دست آورد.

به‌منظور تحلیل امنیت این طرح، از اثر نویز حرارتی صرف نظر می‌شود[۱]. در این صورت، همبستگی $\hat{\theta}_E$ و $\hat{\theta}_A$ به اختلاف فاز کانال قانونی و شنود، بستگی دارد. اختلاف فاز کانال قانونی و شنود با نماد $\Delta\phi$ نشان داده می‌شود و برابر است با:

$$\Delta\phi = \min\big((\phi_E - \phi_{AB}) \bmod 2\pi\,, (\phi_{AB} - \phi_E) \bmod 2\pi\big) \qquad (۱۰)$$

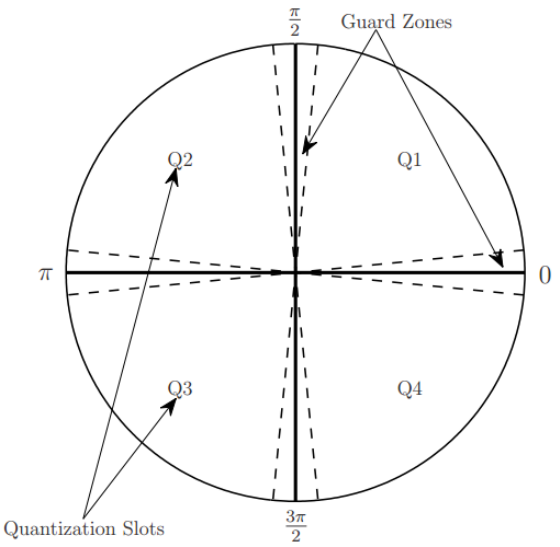
مقدار $\Delta\phi$ با همبستگی فاز بین کانال قانونی و کانال شنود رابطه عکس دارد. بنابراین در مناطقی که $\Delta\phi$ بسیار کوچک باشد، همبستگی فاز کانال قانونی و شنود زیاد است در نتیجه شنودگر با کوانتیزه کردن $\hat{\theta}_E$ می‌تواند کلید آلیس را استخراج کند. بر این اساس، کل فضا به دو زیرفضا قابل افراز است:

۱) *نواحی محرمانه:* مجموعه نقاطی در فضا که اگر شنودگر در یکی از این نقاط مستقر شود، کلیدی که شنودگر به‌دست می‌آورد قطعاً با کلید آلیس متفاوت خواهد بود (یعنی کلید شنودگر حداقل در یک بیت با کلید آلیس تفاوت خواهد داشت).
۲) *نواحی آسیب‌پذیر:* این نواحی، مکمل نواحی محرمانه هستند بنابراین کل فضا به جز نواحی محرمانه را شامل می‌شوند. اگر شنودگر در نواحی آسیب‌پذیر مستقر شود، کلیدی که شنودگر به‌دست می‌آورد لزوماً با کلید آلیس متفاوت نخواهد بود (یعنی ممکن است تمام بیت‌های کلید شنودگر با کلید آلیس برابر باشد).

[۱] با این فرض، امنیت طرح، در بدترین شرایط ممکن (Worst Case Senario) مورد ارزیابی قرار می‌گیرد.

۲-۳- محرمانگی هندسی

با توجه به تعریف نواحی محرمانه و آسیب‌پذیر، محیط پیرامون آلیس و باب، به این دو ناحیه قابل افزار است. آنالیز این نواحی و تعیین محدوده دقیق آن‌ها، اصطلاحاً محرمانگی هندسی نامیده می‌شود. توجه شود که اگر کمیت $\Delta\phi$ قابل کمینه‌سازی باشد، محرمانگی هندسی به لحاظ محاسباتی قابل انجام و دستیابی است اما در غیر این صورت، این آنالیز بسیار دشوار و برخی به لحاظ محاسباتی نشدنی خواهد بود. به‌عنوان یک مثال عملی، در محیط‌های با پراکندگی زیاد، فازهای ϕ_{AB}، ϕ_{AE} و ϕ_{BE} ناهمبسته بوده و بنابراین کمیت $\Delta\phi$ قابل کمینه‌سازی نیست. اما طبق رابطه (۱۰)، متغیر $\Delta\phi$ تابعی از فاز کانال‌های مختلف بوده و در محیط‌های با پراکندگی زیاد تصادفی است. بنابراین می‌توان نقاطی را در محیط انتشاری یافت که رابطه (۱۰) در آن نقاط برقرار باشد. به این منظور سامانه شنود می‌تواند تعداد به میزان کافی زیاد از آنتن‌ها را به‌صورت تصادفی در محیط انتشاری پخش کند تا با احتمال بالایی حداقل یکی از آنتن‌ها در موقعیت مناسب جهت استخراج کلید محرمانه قرار داشته باشد.



شکل (۲): کوانتیزاسیون فاز با $L = 4$ و نواحی محافظ با $\psi = \frac{\pi}{32}$

توجه ۵: در ارتباطات فضای آزاد، شنودگر ممکن است بتواند مکان آلیس و باب را با دقت خوبی تخمین بزند تا از نواحی آسیب‌پذیر آگاهی یابد. سپس با استقرار در نواحی آسیب‌پذیر، می‌تواند بخشی از کلید را به‌دست آورد[۲]. ذکر این نکته حائز

[۲] توجه شود اگر در پروتکل SKG هر سمبل در یک فرکانس ارسال گردد، نواحی آسیب‌پذیر برای فرکانس‌های مختلف متفاوت خواهد بود. بنابراین شنودگر می‌بایست ناحیه مشترک بین نواحی آسیب‌پذیر فرکانس‌های مختلف را (در صورت وجود) پیدا کند و سپس با استقرار در آن مکان، تمام کلید را

اهمیت است که محیط‌ها با پراکندگی فراوان نیز مانند محیط‌های فضای آزاد، نواحی آسیب‌پذیر دارند با این تفاوت که در این محیط‌ها، نواحی آسیب‌پذیر صرفاً بر اساس موقعیت فرستنده و گیرنده قابل تعیین نیست. به عبارت دیگر، موقعیت، تعداد عوامل انتشاری و جهت‌گیری آن‌ها نیز در شکل‌دهی نواحی آسیب‌پذیر مؤثر است.

با توجه به توضیحات فوق، بهترین وضعیت برای شنودگر در شرایط است که طرح SKG در فضای آزاد اجرا شود. در این وضعیت، فاز کانال قانونی و کانال‌های شنود، برابرند با:

$$\phi_{AB}=\frac{2\pi d_{AB}}{\lambda},\phi_{AE}=\frac{2\pi d_{AE}}{\lambda},\phi_{BE}=\frac{2\pi d_{BE}}{\lambda} \qquad (۱۱)$$

که در آن، d_{AB}، d_{AE} و d_{BE} به ترتیب بیانگر فاصله بین آلیس - باب، آلیس - شنودگر و باب - شنودگر است. همچنین λ طول موج متناظر با فرکانس حامل f است. با این فرض که شنودگر نمی‌تواند d_{AB} را به‌صورت دقیق به‌دست آورد، لازم است شنودگر تعداد زیادی آنتن را در محیط انتشاری توزیع کند تا احتمالاً یکی از گیرنده‌ها بتواند شرط زیر را برآورده کند (در سناریوی شنودگران غیر هم‌دست) [۱۴]:

$$\Delta\phi<\frac{2\pi}{L} \qquad (۱۲)$$

با جایگذاری رابطه (۱۰) در رابطه (۱۲)، نکات جالب و مهمی قابل استخراج است:

۱. نواحی آسیب‌پذیر به شکل تعدادی دیسک بیضی‌گون حول آلیس و باب هستند. همان‌طوری که مشخص است ضخامت این دیسک‌ها با افزایش L، کاهش می‌یابد.
۲. ناحیه آسیب‌پذیر گستره‌ای به عرض زاویه‌ای $4\pi/L$ دارد که ناحیه آشکارسازی کلید[۱] را شامل می‌شود. این بدان معناست که شنودگر با احتمال ۵۰٪ می‌تواند قطعه کلید ($\hat{L}$ بیت) را به‌دست آورد و با فرض به‌کارگیری کدینگ گری در مرحله کوانتیزاسیون، با احتمال ۵۰٪ می‌تواند تمام قطعه کلید به استثنای یک بیت ($\hat{L}-1$ بیت) را کشف کند[۲]. بر مبنای این استدلال، در بخش ۲-۴ به ارزیابی آنتروپی کلید خام پرداخته می‌شود.
۳. برای $L=2$ (کوانتیزاسیون تک بیت)، کل فضا آسیب‌پذیر خواهد بود. در این سناریو، از فاز دریافتی فقط یک بیت استخراج می‌گردد و آن یک بیت از منظر شنودگر با احتمال $\frac{1}{2}$ درست و با احتمال $\frac{1}{2}$ اشتباه است، بنابراین آنتروپی *قطعه کلید* برابر با $H\left(\frac{1}{2},\frac{1}{2}\right)=1\ bit$ است که $H(.)$ نماد آنتروپی است. توجه شود که در *کانال ایستا* به ازای $L=2$، آنتروپی *کلید خام* برابر با ۱ است (به اندازه آنتروپی یک قطعه کلید)؛ زیرا در این وضعیت، یا کلید شنودگر و یا متمم آن با کلید به‌دست آمده توسط آلیس برابر است. همچنین در یک کانال *شبه ایستا*[۳]، آنتروپی کلید خام، به اندازه حاصل‌ضرب آنتروپی یک قطعه کلید در تعداد قطعات کلید است. بنابراین در حالت $L=2$ آنتروپی کلید خام در کانال شبه ایستا، کامل است و کل فضا محرمانه خواهد بود. اگر چه چنین طرحی از منظر امنیتی ایده‌آل است ولی از منظر عملکردی به دلیل نرخ کلید پایین، کارآمد نیست.

توجه ۶: در تحلیل‌های امنیتی ذکر شده در این مقاله، ناحیه محافظ لحاظ نمی‌شود؛ هر چند که لحاظ کردن آن، کار شنودگر را دشوارتر می‌کند؛ زیرا در این شرایط، نه تنها شنودگر می‌بایست تخمین دقیقی از θ را داشته باشد، بلکه باید مطلع شود که آیا کلید استخراج شده توسط آلیس و باب دور ریخته شده است یا خیر.

حال ناحیه آسیب‌پذیر بر حسب فاصله مشخص می‌شود. با جایگذاری روابط (۱۱) در روابط (۱۰) و سپس قرار دادن نتیجه در نامساوی (۱۲)، درنهایت پس از قدری محاسبات، ناحیه آسیب‌پذیر برابر خواهد شد با مجموعه نقاطی در فضا که حداقل در یکی از دو محدوده زیر صادق باشد:

$$\frac{d_E-d_{AB}}{\lambda}-\left\lfloor\frac{d_E-d_{AB}}{\lambda}\right\rfloor<\frac{1}{L}$$
$$\frac{d_{AB}-d_E}{\lambda}-\left\lfloor\frac{d_{AB}-d_E}{\lambda}\right\rfloor<\frac{1}{L} \qquad (۱۳)$$

که $d_E\triangleq d_{AE}+d_{BE}$ است. از دو نامساوی مذکور قابل استنتاج است که تمام نقاط روی خط واصل آلیس - باب بخشی از نواحی آسیب‌پذیر است. همچنین تمام نقاطی که به ازای $k\in\{1,2,\dots\}$

به‌دست آورد.

[۱] ناحیه آشکارسازی کلید، ناحیه‌ای است با عرض زاویه‌ای $2\pi/L$ که اگر فاز سیگنال شنودگر $\hat{\theta}_E$ در آن ناحیه قرار گیرد، کلید به‌طور کامل قابل دستیابی است. به عبارت دیگر، ناحیه آشکارسازی کلید، همان ناحیه تصمیم کلید است.

[۲] به عبارت دیگر، اگر رابطه (۱۲) برقرار باشد (استقرار شنودگر در ناحیه آسیب‌پذیر)، در این صورت با احتمال ۵۰٪ نشت کامل کلید (full leakage) و با احتمال ۵۰٪ نشت جزئی کلید (partial leakage) وجود دارد.

[۳] در کانال شبه ایستا، در هر مرحله از کاوش کانال، فاز کانال رفت و برگشت بین آلیس و باب، هم‌پاسخ و ثابت است؛ اما از هر کاوش به کاوش دیگر، فاز کانال‌ها به‌صورت تصادفی و مستقل تغییر می‌کند.

رابطه $d_E = d_{AB} + k\lambda$ را برقرار می‌کنند[۱] جزء ناحیه آسیب‌پذیر هستند. همان‌طوری که مشاهده می‌شود، نواحی آسیب‌پذیر که با رابطه (۱۳) به‌دست می‌آید با رابطه نواحی آسیب‌پذیر در مرجع [۱۴] تفاوت اساسی دارد. دلیل چنین تفاوتی این است که بر اساس رابطه (۴) از مرجع [۱۴]، نواحی مجاور آلیس و باب، بخشی از ناحیه آسیب‌پذیر نیست؛ در حالی که طبق تحلیل‌های اصلاح شده و ارائه شده در این مقاله، نواحی مجاور آلیس و باب جزء نواحی آسیب‌پذیر است. البته این مسئله بدیهی است که نواحی مجاور آلیس و باب جزء نواحی آسیب‌پذیر می‌باشد.

در ادامه برای یک مورد خاص، نواحی آسیب‌پذیر مورد بررسی قرار گرفته است. موقعیت آلیس و باب در فضای R^2 به ترتیب (-1,0) و (+1,0) است. فرکانس کاری $f = 40\ MHz$ و تعداد سطوح کوانتیزاسیون $L = 4$ درنظر گرفته می‌شود. در این شرایط، نواحی آسیب‌پذیر و نواحی محرمانه در شکل (۳)، به ترتیب با رنگ تیره و روشن نشان داده شده است. همان‌طور که مشاهده می‌شود، ناحیه آسیب‌پذیر تقریباً نصف فضا را تشکیل می‌دهد. حال اگر تعداد سطوح کوانتیزاسیون به $L = 16$ تغییر داده شود (بدون تغییر سایر پارامترها)، نواحی آسیب‌پذیر مطابق با شکل (۴) خواهد بود که حدود ۱۳٪ از کل فضا را تشکیل می‌دهد. بر این اساس می‌توان گفت با افزایش تعداد سطوح کوانتیزاسیون، درصد نواحی آسیب‌پذیر کاهش یافته و نیز نرخ تولید کلید افزایش می‌یابد. البته توجه شود به دلیل افزایش تعداد سطوح کوانتیزاسیون، نرخ خطای کوانتیزاسیون افزایش یافته و در نتیجه نرخ عدم تطابق کلید[۲] (KMR) که بیانگر میزان عدم تطابق کلید آلیس و باب است، افزایش می‌یابد.

۲-۴- تحلیل آنتروپی کلید

در این بخش مقدار آنتروپی قطعه کلید برای شنودگری که در نواحی آسیب‌پذیر مستقر است، محاسبه می‌شود. به عبارت دیگر، به این سؤال پاسخ داده می‌شود که اگر شنودگر در نواحی آسیب‌پذیر قرار بگیرد، چه میزان ابهام در مورد قطعه کلید دارد؟

برای پاسخ به این سؤال، یک مثال ارائه می‌شود. فرض کنید $L = 8$ باشد، در این صورت طول قطعه کلید $\hat{L} = 3\ bits$ خواهد شد. بنابراین در صورت استقرار شنودگر در ناحیه آسیب‌پذیر، و با فرض استفاده از نگاشت Gray، قطعه کلید شنودگر یکی از حالت‌های زیر است:

۱) قطعه کلید آلیس با احتمال $\frac{1}{2}$؛
۲) قطعه کلید آلیس که بیت اول آن متمم شده با احتمال $\frac{1}{4}$؛
۳) قطعه کلید آلیس که بیت دوم آن متمم شده با احتمال $\frac{1}{8}$؛
۴) قطعه کلید آلیس که بیت سوم آن متمم شده با احتمال $\frac{1}{8}$؛

بنابراین آنتروپی قطعه کلید برابر خواهد بود با $H\left(\frac{1}{2},\frac{1}{4},\frac{1}{8},\frac{1}{8}\right) = \frac{bits}{partial\ key}$ ۱/۷۵. با الهام از مثال فوق، میزان ابهام شنودگر در مورد قطعه کلید آلیس[۳] برابر می‌شود با:

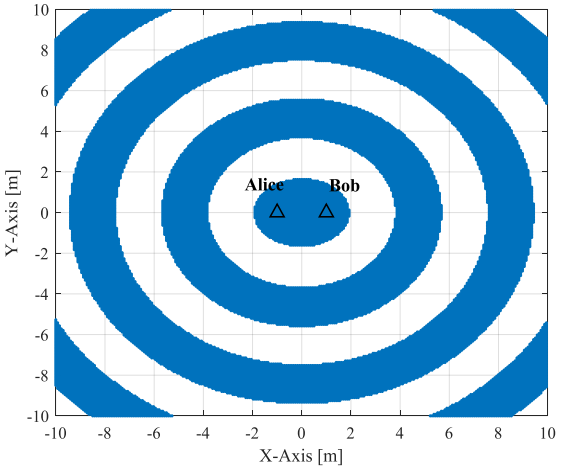
$$H(k_A|k_E) = 1 + \frac{1}{2}\log \hat{L} = 1 + \frac{1}{2}\log\log L \qquad (۱۴)$$

رابطه (۱۴) میزان ابهام شنودگر را بر حسب تعداد سطوح کوانتیزاسیون L نشان می‌دهد. همان‌طوری که مشخص است با افزایش تعداد سطوح کوانتیزاسیون، ابهام شنودگر افزایش می‌یابد ولی این افزایش بسیار ناچیز است. همان‌طور که پیش‌تر هم گفته شد و از رابطه (۱۴) نیز مشخص است، برای کوانتیزاسیون تک بیتی ($L = 2$)، آنتروپی کلید کامل است ($H((k_A|k_E) = 1$). بنابراین می‌توان گفت اگر L زیاد باشد، تهدید ناشی از نواحی آسیب‌پذیر بیشتر است؛ زیرا تعداد بیت‌های نشتی[۴] (LB) برابر است با اختلاف بین کل بیت‌ها و تعداد بیت‌های مبهم برای شنودگر. به عبارت دیگر دارید:

$$LB = \log L - \left(1 + \frac{1}{2}\log\log L\right) \qquad (۱۵)$$

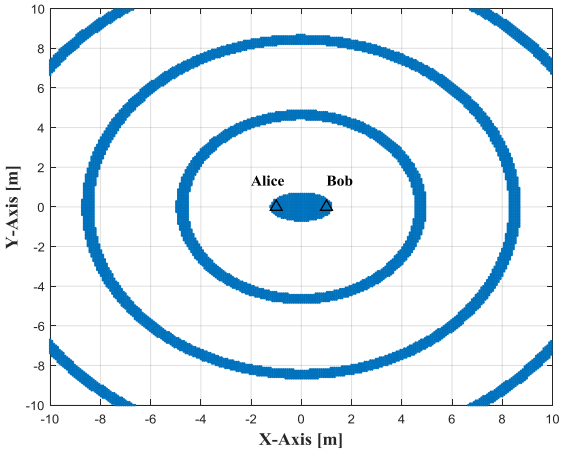
با توجه به رابطه (۱۵)، نرخ نشت کلید برابر است با:

$$R_{LB} = 1 - \frac{1 + \frac{1}{2}\log\log L}{\log L} \qquad (۱۶)$$



شکل (۳): نواحی آسیب‌پذیر برای طرح SKG مبتنی بر فاز با تعداد سطوح کوانتیزاسیون $L = 4$ و فرکانس کاوش $f = 40\ MHz$

[۱] این مجموعه نقاط، مرز نواحی فرنل زوج را تشکیل می‌دهند.
[2] Key Mismatch Rate
[۳] در اینجا فرض می‌شود که آلیس، گره مرجع است. یعنی کلید نهایی آلیس و باب از روی کلید خام آلیس به‌دست خواهد آمد.
[4] Leaked Bits



شکل (۴): نواحی آسیب‌پذیر برای طرح SKG مبتنی بر فاز با تعداد سطوح کوانتیزاسیو$L = 16$ن و فرکانس کاوش $f = 40\ MHz$

لازم به ذکر است که آنتروپی به‌دست آمده در رابطه (۱۴) برای یک قطعه کلید است و نه کل کلید خام. مطابق آنچه پیش‌تر گفته شد، در کانال‌های ایستا آنتروپی کلید خام نیز از رابطه (۱۴) به‌دست می‌آید در صورتی که در کانال‌های شبه ایستا، آنتروپی کلید خام برابر است با حاصل‌ضرب رابطه (۱۴) در تعداد قطعات کلید (تعداد کاوش‌های کانال برای تولید کلید خام).

توجه ۷ (مصالحه بین درصد نواحی آسیب‌پذیر و نشت کلید): همان‌طوری که در بخش ۲-۳ دیدید با افزایش تعداد سطوح کوانتیزاسیون (L)، درصد نواحی آسیب‌پذیر کاهش می‌یابد. اما در این بخش نشان داده شد که با افزایش L، میزان نشت قطعه کلید در نواحی آسیب‌پذیر افزایش پیدا می‌کند (به دلیل افزایش همبستگی بین قطعات کلید آلیس و شنودگر). بدین ترتیب بین درصد نواحی آسیب‌پذیر و میزان نشت اطلاعات یک مصالحه برقرار است.

۲-۵- احتمال خطای کلید خام

در این بخش، برابری کلید خام آلیس K_A و کلید خام باب K_B در طرح پیشنهادی، مورد بررسی قرار گرفته است. لازم به ذکر است که در هر بار کاوش کانال، یک قطعه کلید به طول $\hat{L}$ استخراج می‌شود و از کنار هم قرار دادن آن‌ها (در N بار کاوش کانال)، کلید خام $K_A = \left[k_A^{(1)}\ k_A^{(2)}\ \dots\ k_A^{(N)}\right]$ به طول $N\hat{L}$ به‌دست می‌آید.

همان‌طور که پیش‌تر ذکر شد، در ارسال هر سمبل یکی از سه وضعیت زیر تجربه خواهد شد: ۱) تطابق[1] سمبل دریافتی توسط آلیس و باب، ۲) عدم تطابق[2] سمبل و ۳) رد کردن[3] سمبل. هر کدام از این وضعیت‌های ممکن برای یک سمبل، با یک احتمال مشخص می‌شود: احتمال اولیه تطابق[4] (P_a')، احتمال اولیه عدم تطابق[5] (P_d') و احتمال رد[6] (P_r') که دارید $P_a' + P_d' + P_r' = 1$. احتمال تطابق یک سمبل که تنها بر روی ارسال‌های معتبر ارزیابی می‌گردد را با P_a نمایش داده و به‌صورت زیر محاسبه می‌گردد:

$$P_a = \frac{P_a'}{P_a' + P_d'} \qquad (۱۷)$$

به‌طور مشابه، احتمال عدم تطابق یا خطای سمبل (P_d) نیز به‌صورت زیر ارزیابی می‌گردد:

$$P_d = \frac{P_d'}{P_a' + P_d'} \qquad (۱۸)$$

توجه شود برای آنکه آلیس و باب بر روی کلید خام یکسان K تطابق داشته باشند می‌بایست بر روی تمام M سمبل تطابق داشته باشند. در نتیجه احتمال تطابق کلید خام (P_A) به‌صورت زیر تعیین می‌شود:

$$P_A = (P_a)^M \qquad (۱۹)$$

واضح است که احتمال خطای کلید خام نیز برابر خواهد بود با $P_E = 1 - P_A$. در ادامه احتمال خطای کلید خام برای طرح مذکور، در دو وضعیت SNR، به‌دست آمده است.

۲-۵-۱- محدوده SNR پایین و متوسط

برای محدوده SNR پایین و متوسط، فاز تخمینی $\hat{\theta}_m$ را می‌توان به شکل زیر مدل کرد:

$$\hat{\theta}_m = \theta + \epsilon \qquad (۲۰)$$

که در آن، ϵ خطای تخمین است. توزیع متغیر تصادفی ϵ را Tikhonov [۱۴] درنظر گرفته می‌شود. بنابراین فاز تخمین زده شده نیز از این توزیع تبعیت کرده، دارای متوسط θ بوده و بنابراین تابع چگالی احتمال[7] (PDF) آن برابر خواهد بود با:

$$f_{\hat{\theta}_m}(t) = \frac{\exp(\gamma \cos(t-\theta))}{2\,\pi\, I_0(\gamma)} \qquad (۲۱)$$

که در آن، γ بیانگر SNR سامانه و $I_j(.)$ بیانگر تابع بسل نوع اول و از مرتبه j است.

در قضیه زیر یک تابع احتمال مهم بیان می‌گردد. این تابع در ادامه، نقش کلیدی در محاسبه احتمال خطای کلید خام دارد.

قضیه ۱: فرض کنید فاز θ با SNR برابر با γ ارسال گردد و در

[1] Agreement
[2] Disagreement
[3] Rejection
[4] Primary Probability of Agreement
[5] Primary Probability of Disagreement
[6] Probability of Rejection
[7] Probability Density Function

گیرنده، تخمین آن یعنی $\hat{\theta}_m$ در بازه $[\phi_1,\phi_2]$ باشد. حال، تابع احتمال $D(\theta,\phi_1,\phi_2,\gamma)$ (که از انتگرال‌گیری بر روی PDF متغیر تصادفی Tikhonov در بازه ϕ_1 و ϕ_2 به‌دست می‌آید) محاسبه می‌شود. با کمک مرجع [۱۴] دارید:

$$\int f_{\hat{\theta}_m}(t)dt = \frac{1}{2\pi}\left(t+\frac{2}{I_0(\gamma)}\right)\sum_{j=1}^{\infty}\frac{I_j(\gamma)\sin[j(t-\theta)]}{j} \qquad (۲۲)$$

می‌توان تابع $D(\theta,\phi_1,\phi_2,\gamma)$ را به‌صورت زیر بیان کرد:

$$\begin{aligned} D(\theta,\phi_1,\phi_2,\gamma) &= \int_{\phi_1}^{\infty} f_{\hat{\theta}_m}(t)\,dt - \int_{\phi_2}^{\infty} f_{\hat{\theta}_m}(t)\,dt \\ &= \frac{\phi_2-\phi_1}{2\pi} + \frac{4}{I_0(\gamma)}\sum_{j=1}^{\infty}\frac{1}{j2\pi}I_j(\gamma) \\ &\times \cos\left(\frac{j}{2}(\phi_1+\phi_2-2\theta)\right)\sin\left(\frac{j}{2}(\phi_2-\phi_1)\right) \end{aligned} \qquad (۲۳)$$

وقتی مقادیر کوانتیزه شده سمبل‌های آلیس و باب برابر باشد، یعنی $Q(\hat{\theta}_A)=Q(\hat{\theta}_B)$، در این صورت سمبل‌ها با هم برابرند. برای یک جفت مشخص از (θ,γ)، احتمال تطابق سمبل‌ها برابر است با:

$$\sum_{i=1}^{L}\Pr\{Q(\hat{\theta}_A)=i|\theta\}.\Pr\{Q(\hat{\theta}_B)=i|\theta\} \qquad (۲۴)$$

برای محاسبه احتمال $\Pr\{Q(\hat{\theta}_A)=i|\theta\}$، می‌بایست از PDF متغیر تصادفی $\hat{\theta}_A$ بر روی کلیه نواحی کوانتیزاسیون انتگرال‌گیری شود. بدین منظور از قضیه ۱ بهره برده می‌شود. بنابراین با جایگذاری رابطه (۲۳) در رابطه (۲۴) و سپس با متوسط‌گیری بر روی θ (که به‌صورت یکنواخت بر بازه $[0,2\pi]$ توزیع شده است)، احتمال اولیه تطابق (P_a') به‌صورت زیر ارزیابی می‌شود:

$$P_a' = \frac{1}{2\pi}\sum_{i=1}^{L}\int_0^{2\pi} D^2\left(\theta,(i-1)\frac{2\pi}{L}+\frac{\psi}{2},i\frac{2\pi}{L}-\frac{\psi}{2},\gamma\right)d\theta \qquad (۲۵)$$

به‌طور مشابه، احتمال اولیه عدم تطابق (P_d') یعنی وضعیتی که $Q(\hat{\theta}_A)\neq Q(\hat{\theta}_B)$ باشد، به‌صورت زیر محاسبه می‌شود:

$$\begin{aligned} P_d' = \frac{1}{2\pi}\sum_{i=1}^{L}\sum_{\substack{j=1\\ j\neq i}}^{L}\int_0^{2\pi} & D\left(\theta,(i-1)\frac{2\pi}{L}+\frac{\psi}{2},i\frac{2\pi}{L}-\frac{\psi}{2},\gamma\right) \\ & \times\left(\theta,(j-1)\frac{2\pi}{L}+\frac{\psi}{2},j\frac{2\pi}{L}-\frac{\psi}{2},\gamma\right)\mathrm{d}\theta \end{aligned} \qquad (۲۶)$$

فرم بسته برای روابط (۲۵ و ۲۶) به سادگی قابل محاسبه است. در اینجا برای اختصار از بیان رابطه بسته صرف نظر شده است. با قرار دادن روابط (۲۵ و ۲۶) در روابط (۱۷ و ۱۸)، به ترتیب، احتمال تطابق سمبل و احتمال خطای سمبل قابل سنجش خواهد بود. سپس با کمک رابطه (۱۹) به راحتی می‌توان احتمال تطابق کلید خام و در نتیجه احتمال خطای کلید خام را محاسبه کرد.

۲-۵-۲- محدوده SNR بالا

برای مقادیر زیاد SNR، با دقت بالایی می‌شود توزیع احتمال Tikhonov را با توزیع گوسی تقریب زد [۱۴ و ۱۵]:

$$f_{\hat{\theta}_m}(t) = \frac{1}{\sigma(\gamma)\sqrt{2\pi}}e^{-\frac{(\hat{\theta}_m-\theta)^2}{2\,\sigma^2(\gamma)}} \qquad (۲۷)$$

که واریانس $\sigma(\gamma)$ تابعی از SNR سامانه بوده و برابر است با:

$$\sigma(\gamma) = \sqrt{2\left(1-\frac{I_1(\gamma)}{I_0(\gamma)}\right)} \qquad (۲۸)$$

با توجه به محدوده زیر برای نسبت توابع بسل [۱۲]:

$$\begin{aligned} \frac{\gamma}{i+\frac{1}{2}+\sqrt{\gamma^2+\left(i+\frac{3}{2}\right)^2}} &\leq \frac{I_{i+1}(\gamma)}{I_i(\gamma)} \\ &\leq \frac{\gamma}{i+\frac{1}{2}+\sqrt{\gamma^2+\left(i+\frac{1}{2}\right)^2}} \end{aligned} \qquad (۲۹)$$

در حالت SNR زیاد $(\gamma \gg 1)$، با دقت بسیار بالایی می‌توان واریانس $\sigma(\gamma)$ در رابطه (۲۸) را به‌صورت زیر تقریب زد:

$$\sigma(\gamma) \approx \sqrt{\frac{2}{2\gamma+1}} \qquad (۳۰)$$

با قرار دادن واریانس (۳۰) در تقریب گوسی (۲۷) و سپس محاسبه تابع $D(\theta,\phi_1,\phi_2,\gamma)$ در رابطه (۲۳)، نتیجه زیر حاصل می‌گردد:

$$\begin{aligned} & D(\theta,\phi_1,\phi_2,\gamma) = \\ & \frac{1}{2}\left[\mathrm{erfc}\left(\frac{\phi_1-\theta}{\sqrt{2\sigma^2(\gamma)}}\right)-\mathrm{erfc}\left(\frac{\phi_2-\theta}{\sqrt{2\sigma^2(\gamma)}}\right)\right. \\ & \left.+\mathrm{erfc}\left(\frac{\phi_2-\theta-2\pi}{\sqrt{2\sigma^2(\gamma)}}\right)-\mathrm{erfc}\left(\frac{\phi_1-\theta-2\pi}{\sqrt{2\sigma^2(\gamma)}}\right)\right] \end{aligned} \qquad (۳۱)$$

که در آن، $\mathrm{erfc}(.)$ بیانگر تابع خطای مکمل[1] است. لازم به ذکر است در SNRهای بالا نیز مشابه SNR پایین، احتمالات P_a' و P_d' به ترتیب با استفاده از روابط (۲۵ و ۲۶) محاسبه می‌شوند. با کمک این احتمالات، P_A و در نتیجه P_E قابل ارزیابی خواهد بود.

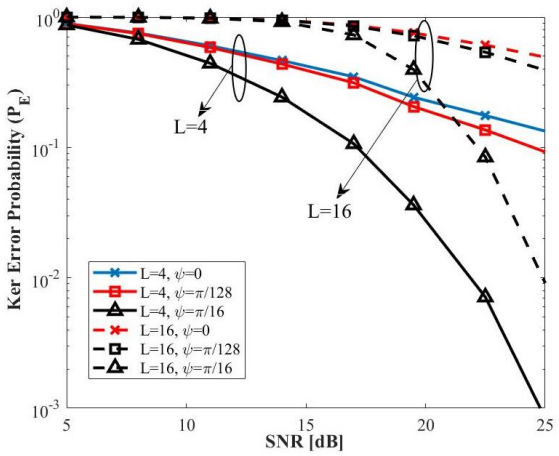
۳- نتایج عددی و تفسیر آن‌ها

در این بخش، کارایی طرح مورد مطالعه از منظر احتمال خطای کلید خام (P_E) بر حسب SNR دریافتی بررسی می‌شود. در شکل (۵)، احتمال خطای P_E به ازای $\psi = 0,\frac{\pi}{128},\frac{\pi}{16}$ و $L=4,16$ رسم شده است. به ازای $\mathrm{SNR} < 20\ \mathrm{dB}$ از رابطه (۲۳) و برای

[1] Complementary Error Function

SNRهای بیشتر، از رابطه (۳۱) استفاده شده است. همان‌طور که در شکل (۵) مشخص است، L، ψ و نیز مقدار SNR بر روی P_E اثر دارند. مشاهده می‌شود که در SNRهای پایین، عرض ناحیه محافظ تأثیر چندانی بر روی P_E ندارد و بنابراین نمی‌توان از این درجه آزادی در جهت ارتقای کارایی طرح، بهره برد. در چنین شرایطی، می‌بایست تعداد سطوح کوانتیزاسیون L کاهش یابد تا از P_E کاسته شود. توجه شود با کاهش L، طول کلید کاهش می‌یابد و بنابراین در ازای پذیرش کاهش نرخ کلید، ابهام در آشکارسازی سمبل‌ها کم شده و در نتیجه P_E کاهش می‌یابد. همچنین برای تعداد Lهای زیاد، با افزایش SNR می‌توان P_E را کاهش داد. ذکر این نکته حائز اهمیت است که در این وضعیت، به دلیل دور ریختن سمبل‌ها، تعداد کاوش‌های مورد نیاز، بسیار افزایش می‌یابد.

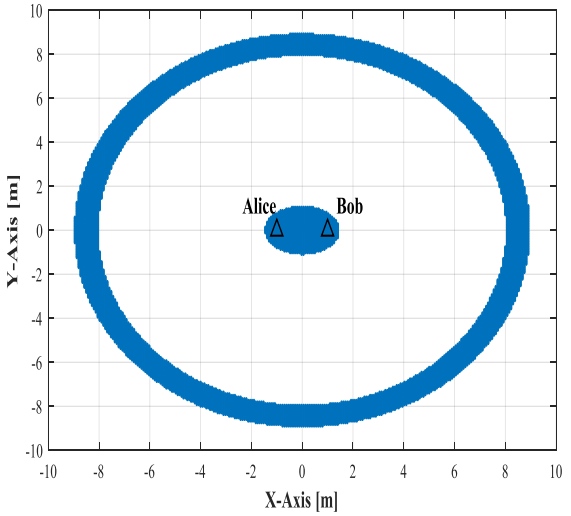
همچنین با توجه به شکل (۵) در $\mathrm{SNR} = 22\ \mathrm{dB}$، وضعیت $L = 4$ و $\psi = \frac{\pi}{128}$ با وضعیت $L = 16$ و $\psi = \frac{\pi}{16}$ کارایی یکسانی دارند و در هر دوی آن‌ها $P_E \approx 0.1$ است. توجه شود که سناریو با $L = 4$ نسبت به $L = 16$ میزان دور ریختگی سمبل‌های کمتری داشته و نرخ کلید کمتری ارائه می‌دهد.



شکل (۵): احتمال خطای کلید بر حسب SNR برای تعداد سطوح کوانتیزاسیون $L = 4, 16$ و مقادیر مختلف ناحیه محافظ (ψ)

تاکنون فرض بر این بود که کاوش کانال در یک فرکانس صورت می‌پذیرد. حال طرح پیشنهادی، در وضعیتی مورد مطالعه قرار می‌گیرد که در آن کاوش کانال مبتنی بر یک مجموعه فرکانسی $F = \{f_1, f_2, \dots, f_M\}$ اجرا می‌شود. توجه شود گاهی مهندسان و طراحان سامانه‌ای به دنبال بهینه‌سازی محرمانگی هندسی هستند. مثلاً می‌خواهند از یک مجموعه بزرگ از فرکانس‌ها، M فرکانس را به گونه‌ای انتخاب کنند که اولین ناحیه محرمانگی بیشینه گردد[۱]. در ادامه تأثیر استفاده از چند فرکانس کاوش (به جای یک فرکانس)، بر روی نواحی آسیب‌پذیر مورد بررسی قرار می‌گیرد.

در طرح SKG با چندین فرکانس کاوش، برای اینکه شنودگر بتواند کلید محرمانه را به‌دست آورد می‌بایست در مکانی مستقر شده باشد که این مکان، درون اشتراک نواحی آسیب‌پذیر مربوط به مجموعه فرکانس‌های F باشد. به‌عبارت دیگر، با کمک رابطه (۱۳)، برای هر فرکانس یک مجموعه نواحی آسیب‌پذیر به‌دست آورده می‌شود. اشتراک این نواحی به ازای فرکانس‌های مختلف، ناحیه آسیب‌پذیر طرح SKG مبتنی بر چند فرکانس کاوش را مشخص می‌کند. به‌عنوان مثال، برای $L = 4$ و سه فرکانس کاوش کانال $f = 40, 60, 80\ MHz$، نواحی آسیب‌پذیر در شکل (۶) ترسیم شده است. همان‌طوری که مشخص است در مقایسه با یک فرکانس کاوش (شکل ۳)، سه فرکانس کاوش کانال، نواحی آسیب‌پذیر به مراتب کمتری دارد به‌طوری که در این حالت حدود ۱۳٪ از کل فضا مشکوک به کشف کلید محرمانه است. بنابراین می‌توان نتیجه گرفت که به‌کارگیری چند فرکانس در مقایسه با یک فرکانس، درصد امنیت بالاتری را برای محرمانگی کلید فراهم می‌آورد.



شکل (۶): نواحی آسیب‌پذیر برای طرح SKG مبتنی بر سه فرکانس f=40,60,80 MHz با سطوح کوانتیزاسیون L=4

[۱] همان‌طور که پیش‌تر گفته شد در مجاورت آلیس و باب، یک ناحیه آسیب‌پذیر غیر قابل اجتناب وجود دارد و آن بیضی اولیه است. با افزایش فرکانس، این ناحیه آسیب‌پذیر به خط واصل بین آلیس و باب تقلیل می‌یابد. اگر سامانه مخابرات مد نظر SRC باشد، به دلیل واضح بودن لینک ارتباطی، شنودگر نمی‌تواند روی خط واصل مستقر شود چرا که به راحتی کنار زده می‌شود. بنابراین در کاربردهای SRC نسبت به بیضی اولیه، نگرانی ندارید. با عنایت به اینکه SNR دریافتی توسط شنودگر با دور شدن از آلیس و باب کاهش می‌یابد، علاوه بر بیضی اولیه، اولین حلقه بیضوی نیز اهمیت خاصی پیدا می‌کند.

۴- نتیجه‌گیری و کارهای تکمیلی

در این مقاله به بررسی چالش SKG در سامانه‌های مخابراتی نقطه به نقطه ایستا پرداخته شد. در طرح SKG مطالعه شده، از فاز کانال بین آلیس و باب جهت استخراج کلید مشترک بهره برده شد. در ضمن به‌منظور افزایش آنتروپی کلید، آلیس و باب فاز تصادفی پیوسته تزریق می‌کردند. با هدف ارزیابی امنیتی طرح مذکور، نواحی آسیب‌پذیر تعیین شد. سپس با به‌دست آوردن رابطه بسته‌ای برای احتمال خطای کلید خام مشترک بین آلیس و باب، کارایی طرح بررسی شد. درنهایت، با تحلیل آنتروپی روی کلید خام، میزان ابهام شنودگر در مورد کلید خام محاسبه گردید. نتایج شبیه‌سازی نیز نشان می‌دادند که اگر در مرحله کاوش کانال به جای یک فرکانس، چند فرکانس به‌کار گرفته شود (پویاسازی مجازی کانال مخابراتی)، نواحی آسیب‌پذیر کاهش می‌یابد. در چنین کانالی (کانال شبه ایستا) مشاهده می‌شود که یک مصالحه بین درصد نواحی آسیب‌پذیر و میزان نشت اطلاعات وجود دارد.

به‌عنوان کارهای آتی برای توسعه طرح‌های SKG مبتنی بر تزریق فاز تصادفی، موارد زیر پیشنهاد می‌شود:

- برای تزریق فاز تصادفی به جای ارسال فاز پیوسته، می‌توان از فاز گسسته نظیر نقاط فضای منظومه QAM و PSK استفاده کرد. این ایده، علاوه بر سادگی پیاده‌سازی، درصد نواحی آسیب‌پذیر نیز کاهش می‌یابد. ما این پیشنهاد را در قالب یک مقاله مجزا آماده کرده‌ایم که بزودی منتشر خواهد شد.
- پیشنهاد می‌شود تأثیر نقیصه‌های سخت‌افزاری [۱۶] بر طرح‌های SKG مورد مطالعه قرار بگیرد. به‌طور مشخص تأثیر نقیصه‌های سخت‌افزاری بر نواحی آسیب‌پذیر قابل تأمل است.
- سناریویی که به بهبود کارایی طرح‌های SKG کمک می‌کند، به‌کارگیری رله است. در صورتی که فاصله بین آلیس و باب زیاد یا توان ارسالی محدود باشد، ممکن است سیگنال کاوش دریافتی ضعیف بوده و در نتیجه فرآیند SKG با شکست مواجه شود. در چنین وضعیتی استفاده از رله، بسیار مفید خواهد بود. در چنین سناریویی می‌بایست یک طرح SKG مناسب، ارائه شود. به خصوص وقتی با یک رله غیر قابل اعتماد سروکار دارید، طراحی یک پروتکل SKG محرمانه به گونه‌ای که رله غیر قابل اعتماد، نتواند کلید مشترک بین آلیس و باب را به‌دست آورد، یک چالش مهم محسوب می‌شود.
- در توسعه بند قبلی، می‌توان یک سامانه مخابراتی مبتنی بر چند رله متوالی را مورد مطالعه و تحلیل قرار داد [۱۷ و ۱۸]. چنین سناریویی در برخی شبکه‌ها مانند شبکه‌های اقتضایی و IoT موجود است. ارائه یک طرح SKG کارا در این سناریو حائز اهمیت است. چالش چنین طرحی زمانی بیشتر می‌شود که رله‌های به‌کار گرفته شده غیر قابل اعتماد باشند.
- وجود تداخل‌گرها یا جمرهای پرتوان، می‌تواند به موفقیت فرآیند SKG، آسیب جدی بزند [۱۹]. همچنین، در شبکه‌های سلولار، ارائه یک طرح SKG مقاوم در برابر تداخل‌های بین سلولی اهمیت ویژه‌ای دارد زیرا با افزایش توان تداخل تجمعی در آلیس و باب، همبستگی مقادیر تصادفی مبنای تولید کلید کاهش پیدا می‌کند و نرخ عدم برابری کلید زیاد می‌شود.
- کلیدهای مستخرج از لایه فیزیکی در رمز کننده‌های لایه‌های بالاتر نظیر لایه کاربرد قابل استفاده هستند. ولی این مهم، نیازمند ذخیره‌سازی امن کلیدهاست. به این منظور می‌توان از طرح‌های بیومتریک (Biometric) نظیر مرجع [۲۰] به‌عنوان مکمل طرح‌های تولید کلید مخفی لایه فیزیکی استفاده کرد.

۵- مراجع

[1] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," *IEEE International Things*, vol. 4, no. 5, pp. 1125–1142, 2017.

[2] P. Neelakanta, "Designing Robust Wireless Communications for Factory Floors," in IEEE International Conference on Industrial Informatics, 2006.

[3] S. K. Timalsina, R. Bhusal, and S. Moh, "NFC and Its Application to Mobile Payment: Overview and Comparison," In International Conference on Information Science and Digital Content Technology (ICIDT), 2012, pp. 203–206.

[4] S. Biswas, R. Tatchikou, and F. Dion, "Vehicle-to-Vehicle Wireless Communication Protocols for Enhancing Highway Traffic Safety," IEEE Commun. Mag., vol. 44, no. 1, pp. 74–82, 2006.

[5] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey," IEEE Commun. Surveys Tuts., vol. 16, no. 3, pp. 1550–1573, 2014.

[6] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and Applications of Physical Layer Security Techniques for Confidentiality: A Comprehensive Survey," IEEE Commun Surveys Tuts., vol. 21, no. 2, pp. 1773–1828, 2018.

[7] G. Li, C. Sun, J. Zhang, E. Jorswieck, B. Xiao, and A. Hu, "Physical Layer Key Generation in 5G and Beyond Wireless Communications: Challenges and Opportunities," Entropy, vol. 21, p. 497, 2019.

[8] 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, 2020.

[9] A. K. Junejo, F. Benkhelifa, B. Wong, and J. A. McCann, "LoRa-LiSK: A Lightweight Shared Secret Key Generation Scheme for LoRa Networks," IEEE Int. Things J.

[10] W. Xu, S. Jha, and W. Hu, "LoRa-Key: Secure Key Generation System for LoRa-Based Network," IEEE Int. Things J., vol. 6, no. 4, pp. 6404–6416, 2019.

[11] H. Ruotsalainen, J. Zhang, and S. Grebeniuk, "Experimental Investigation on Wireless Key Generation for Low-Power Wide-Area Networks," IEEE Int. Things J., vol. 7, no. 3, pp. 1745–1755, 2020.

[12] 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 Int. Things J., vol. 8, no. 6, pp. 4373–4388, 2021.

[13] M. Letafati, A. Kuhestani, H. Behroozi, and D. W. K. Ng, "Jamming-Resilient 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, 2020.

[14] S. Severi, G. Abreu, G. Pasolini, and D. Dardari, "A Secret Key Exchange Scheme for Near Field Communication," In IEEE WCNC, 2014, pp. 428–433.

[15] H. Fu and P. Y. Kam, "Exact Phase Noise Model and Its Application to Linear Minimum Variance Estimation of Frequency and Phase of a Noisy Sinusoid," In IEEE PIMRC, 2008, pp. 1–5.

[16] A. Kuhestani, A. Mohammadi, and K. K. Wong, "Optimal Power Allocation by Imperfect Hardware Analysis in Untrusted Relaying Networks," IEEE Trans. Wireless Commun., vol. 17, no. 7, pp. 4302–4314, 2018.

[17] M. T. Mamaghani, A. Kuhestani, and H. Behroozi, "Can a Multi-Hop Link Relying on Untrusted Amplify-and-Forward Relays Render Security?," Wireless Net.., vol. 27, pp. 795–807, 2021.

[18] M. Letafati, A. Kuhestani, and H. Behroozi, "Three-Hop Untrusted Relay Networks with Hardware Imperfections and Channel Estimation Errors for Internet of Things," IEEE Trans. Inf. Foren. Sec., vol. 15, pp. 2856–2868, 2020.

[19] H. Saedi, A. Mohammadi, and A. Kuhestani, "Characterization of Untrusted Relaying Networks in the Presence of an Adversary Jammer," Wireless Net., vol. 26, pp. 2113–2124, 2020.

[20] A. Bidokhti, S. M. Pournaghei, and A. H. Khalili, "A Generalized Scheme for Extracting Biometric Keys from Keystroke Dynamics," Journal of Electronical & Cyber Defence, vol. 5, no. 1, pp. 9–18, 2017 (In Persian).