University of Qom
Engineering Management and Soft Computing
JEMSC.QOM
Online ISSN: 2538-2675

Design and Management of Group Key Generaation Based on Wireless Channel Phase

Mohammadreza Keshavarzi, Ali Kuhestani, Bahman Madadi
1. Corresponding author, Assistant Professor of ICT Research Institute, Iran Telecommunication Research Center (ITRC), Tehran, Iran, Email: mrkeshavarzi@itrc.ac.ir
2. Assistant Professor of Telecommunication Engineering at Qom University of Technology, Email: kuhestani@qut.ac.ir
3. Ph.D. Student of Telecommunication Engineering at Imam Hussain University. Email: ieee.madadi@gmail.com

Article Info

Article type:
Research Article

Article history:
Received 27 - 8 – 2024
Received in revised form
31 - 10 – 2024
Accepted 18 - 2 – 2025
Published online 18 - 3 – 2025

Keywords:
Security, group secret key generation, wireless channel phase

ABSTRACT

In this paper, a secret key generation scheme for a group of users based on wireless channel is presented in which legal nodes are connected under star topology. Instead of using the characteristics of the channel domain such as received signal strength (RSS), the channel phase is used in the proposed scheme; Because in channels with low mobility or channels with low dispersion that do not have a large entropy channel range, the channel phase can show significant changes. Based on this, in this article, a group key generation scheme based on channel phase is proposed. The proposed key generation scheme, compared to the similar scheme, needs less time intervals for execution and therefore has a high speed of the algorithm. As a result, the key production rate will be higher, which is very desirable. In the following, we will analyze and examine the proposed protocol in terms of some criteria such as the probability of generating the correct group key, scalability and vulnerable areas.

Cite this article: ……..

DOI: https://doi.org/

Publisher: University of Qom

JEMSC.QOM
شاپا الکترونیکی: ۲۶۷۵-۲۵۳۸

مدیریت مهندسی و رایانش نرم

دانشگاه قم

طراحی و مدیریت تولید کلید گروهی مبتنی بر فاز کانال بی‌سیم

محمدرضا کشاورزی، علی کوهستانی، بهمن مددی

1. نویسنده مسئول، استادیار پژوهشگاه فناوری اطلاعات و ارتباطات، مرکز تحقیقات مخابرات ایران، تهران، ایران، ایمیل: mrkeshavarzi@itrc.ac.ir

2. استادیار گروه مهندسی مخابرات دانشگاه صنعتی قم، ایمیل: kuhestani@qut.ac.ir

3. دانشجوی دکتری رشته مهندسی مخابرات دانشگاه امام حسین(ع) ایمیل: ieee.madadi@gmail.com

اطلاعات مقاله

نوع مقاله: مقاله پژوهشی

تاریخ دریافت: 1403/06/06

تاریخ بازنگری: 1403/08/10

تاریخ پذیرش: 1403/11/30

تاریخ انتشار1403/12/30

کلیدواژه‌ها:

امنیت، تولید کلید مخفی گروهی، تزریق فاز تصادفی، فاز کانال بی‌سیم

چکیده

در این مقاله، یک طرح تولید و مدیریت کلید مخفی برای گروهی از کابران شبکه ارائه می‌گردد که در آن کاربران تحت توپولوژی ستاره با هم در ارتباط هستند. به جای استفاده از ویژگی‌های دامنهٔ کانال مانند شدت سیگنال دریافتی، در طرح پیشنهادی از فاز کانال بی‌سیم استفاده شده است؛ چرا که در کانال‌های با تحرک کم یا کانال‌های با پراکندگی کم که دامنه کانال آنتروپی زیادی ندارند، فاز کانال می‌تواند تغییرات چشمگیری از خود نشان دهد. بر این اساس، در این مقاله یک طرح تولید کلید گروهی مبتنی بر فاز کانال پیشنهاد می‌گردد. طرح تولید کلید پیشنهادی، در مقایسه با طرح مشابه، بازه‌های زمانی کمتری برای اجرا نیاز داشته و بنابراین سرعت الگوریتم بالایی دارد. در نتیجه نرخ تولید کلید آن بیشتر خواهد بود که بسیار مطلوب است. در ادامه، پروتکل پیشنهادی را از نظر برخی معیارهای عملکردی و امنیتی مانند احتمال تولید کلید گروهی صحیح، مقیاس‌پذیری و نواحی آسیب‌پذیری مورد تحلیل و بررسی قرار می‌دهیم.

استناد: .....

ناشر: دانشگاه قم

Engineering Management and Soft Computing
JEMSC.QOM
Online ISSN: 2538-2675
University of Qom

1) مقدمه

تا پیش از حدود نیم قرن پیش، غالب روش‌های امنیت اطلاعات بر مبنای نظریه محرمانگی شانون (رمزنگاری در لایه‌های بالا) بودند؛ تا آنکه در سال 1975، آقای واینر [۱] با پیشنهاد تزریق نویز به مدل کانال ارتباطی، بحث امنیت اطلاعات را از زاویه‌ای جدید مورد بررسی قرار داد. واینر با در نظر گرفتن شرایط کانال گیرنده قانونی و شنودگر، ایدهٔ ارسال امن اطلاعات با بهره‌گیری از راهکارهای مبتنی بر لایه فیزیکی را ارایه کرد. اخیراً به دلیل رشد روزافزون قدرت محاسباتی رایانه‌ها و ظهور پردازشگرهای کوانتومی، الگوریتم‌های رایج مبتنی بر پیچیدگی محاسباتی در معرض آسیب جدی هستند. همچنین نیازمندی‌های پیاده‌سازی امن پروتکل‌های امنیتی و نیز مدیریت و تبادل کلید سبب شده است تا بحث امنیت لایه فیزیکی[۱] (PLS)، مجدداً به شدت مورد توجه قرار گیرد.

به‌طور کلی روش‌های PLS عبارتند از [2]-[5]: روش‌های سنتی طیف‌گسترده به منظور مقابله با حمله پارازیت، روش‌های مبتنی بر کدگذاری، روش‌های مبتنی بر آنتن‌های جهتی و پرتودهی، تزریق نویز مصنوعی، مخابرات مشارکتی و نیز تولید کلید مخفی[۲] (SKG) لایه فیزیکی. از بین روش‌های فوق، SKG به دلایل ذیل بیشتر مورد توجه پژوهشگران و اهل صنعت بوده است؛ چرا که در SKG، برخلاف روش‌های متداول پیشین، می‌توان فرض کرد که گره‌های غیرمجاز توانایی محاسباتی نامحدودی داشته باشند اما همچنان امنیت، تضمین شده باشد. همچنین SKG به‌دلیل سربار طیفی پایین، پردازش سبک و نیز توان مصرفی کمتری، از سایر روش‌های PLS عملی‌تر و جذاب‌تر است؛ از این رو برای تأمین امنیت در کاربردهایی نظیر اینترنت اشیاء[۳] (IoT) و یا ارتباطات پهبادها که سنسورها، قدرت محاسباتی کم و توان مصرفی پایینی دارند مناسب‌تر است. در SKG، استخراج کلید بر مبنای ویژگی‌های کانال مشترک طرفین ارتباط صورت می‌گیرد. این ویژگی ها شامل فاز کانال، قدرت سیگنال دریافتی[۴] (RSS)، اطلاعات حالت کانال[۵] (CSI) و دامنهٔ کانال می‌شوند [5].

در شبکه‌های مخابراتی گاهی نیاز است به‌جای دو کاربر، چندین کاربر به یک کلید مخفی مشترک دست یابند. اصطلاحاً گره‌های قانونی بتوانند یک کلید مخفی گروهی[۶] را با یکدیگر به اشتراک بگذارند. این توسعه از دو کاربر به چند کاربر، عملاً چالش برانگیز است. اولین دلیل این است که تولید کلید در لایه فیزیکی فقط با اتکاء بر هم‌پاسخی کانال بین دو کاربر صورت می‌گیرد. لذا دستیابی به اطلاعات کانال برای دو کاربر آسان است. حال آنکه، برای به اشتراک گذاشتن اطلاعات کانال با کاربران بیشتر، نیازمند تبادل بیشتر اطلاعات است که نتیجتاً خطر نشت اطلاعات به شنودگر وجود دارد. چالش دوم این است که اگر چه که با افزایش تعداد کاربران می‌توان به یک کلید گروهی طولانی‌تر دست یافت، با این حال می‌بایست زمان همدوسی کانال به اندازه کافی بزرگ باشد تا کانال ثابت بماند. توجه شود اگر همه‌ی گره‌های شبکه در محدوده ارسال یکدیگر باشند از توپولوژی ستاره استفاده

[1] Physical layer security
[2] Secret key generation
[3] Internet-of-Things
[4] Received signal strength
[5] Channel state information
[6] Group secret key

University of Qom
Engineering Management and Soft Computing
JEMSC.QOM
Online ISSN: 2538-2675

می‌شود (برای مثال افرادی که با یکدیگر سفر می‌کنند) و اگر همه‌ی گره‌های شبکه به طور مستقیم به هم متصل نباشند ولی از طریق چند گره واسط به هم لینک داشته باشند، از توپولوژی زنجیره‌ای کمک گرفته می‌شود.

2) پیشینه تحقیق

اخیراً برخی کارهای پژوهشی، پروتکل‌های تولید کلید گروهی ارائه داده‌اند [6]-[9]. در مقاله‌ی [6]، نویسندگان به مشکل پیچیدگی زیاد سیستم و نشت زیاد اطلاعات به شنودگر در حین مرحله‌ی توافق اطلاعات اشاره می‌کنند و سعی می‌کنند الگوریتمی ارائه دهند که این مشکل را تا حدودی برطرف کند. دو توپولوژی مورد مطالعه، ستاره و زنجیره بوده است. در مقاله‌ی [7] نویسندگان الگوریتم‌هایی برای تولید و به اشتراک‌گذاری کلید مخفی گروهی بین گروهی از گره‌ها و برای توپولوژی‌های مختلف حلقه و مش معرفی کرده و سپس ثابت می‌کنند که این الگوریتم‌ها می‌توانند به نرخ کلید گروهی بهینه دسترسی پیدا کنند. برخلاف کارهای بالا که در آنها گره‌های قانونی و شنودگر دارای یک آنتن هستند، در مقاله‌ی [8] مسأله برای حالتی که گره‌های اصلی و شنودگر همگی دارای چندین آنتن هستند بررسی شده است. با مجهز کردن گره‌ها به چندین آنتن، می‌توان از کانال‌های بیشتری برای تولید کلید استفاده کرد و نتیجتاً به نرخ کلید بالاتری دست یافت. متذکر می‌شویم اگر چه که در اکثر کارهای پژوهشی صورت گرفته شده، از مقادیر RSS برای تولید کلید استفاده شده است، اما نرخ تولید کلید آن پایین است. بخصوص اینکه، روش‌های مبتنی بر RSS در محیط‌های ایستا نمی‌توانند نرخ کلید خوبی ارائه دهند. با این دلایل، در مقاله‌ی [9]، SKG گروهی مبتنی بر خاصیت تصادفی فاز کانال مورد بررسی قرار گرفت. همچنین در مقاله‌ی اخیر [10]، چالش تولید کلید مبتنی بر فاز برای یک جفت کاربر، در ارتباطات خط دید[7] (LoS) و بُرد کوتاه بررسی گردید. نکته مهم اینست که در ارتباطات LoS، پدیده محوشوندگی وجود ندارد و لذا نمی‌توان از روش‌های مبتنی بر اندازه برای تولید کلید استفاده کرد. چرا که در نبود خاصیت تصادفی کافی، آنتروپی کلید کم است و در نتیجه امنیت کلید تولید شده به خطر می‌افتد.

در این مقاله، ما بر روی تولید کلید مخفی گروهی برای ارتباطات LoS و تحت توپولوژی ستاره متمرکز می‌شویم. لینک ارتباطاتی در ارتباطات ماهواره‌ای و برخی کاربردهای IoT از نوع LoS است. در این نوع ارتباطات، کانال میزان تصادفی بودن به مراتب کمتری در مقایسه با کانال‌های چندمسیری دارد. بنابراین نمی‌توان از RSS و اندازه کانال برای تولید کلید گروهی استفاده کرد. در این مقاله، از روش مبتنی بر فاز کانال برای تولید کلید گروهی استفاده خواهیم کرد. بدین منظور، یک پروتکل تولید کلید لایه فیزیکی مبتنی بر توپولوژی ستاره ارائه می‌گردد. سپس طرح را از منظر عملکردی (مانند احتمال تولید کلید صحیح) و امنیتی (نواحی آسیب‌پذیری[8]) مورد مطالعه قرار می‌دهیم. نتایج شبیه‌سازی ذکر شده در این مقاله، بینش‌های مهندسی مفیدی در جهت طراحی و بهینه‌سازی تولید کلید لایه فیزیکی گروهی ارائه می‌دهد.

[7] Line-of-sight
[8] Vulnerability

3) مدل سیستم و فرضیات

مدل کلی سیستم تحت مطالعه، شامل M گره است که می‌خواهند با یکدیگر بر روی یک کلید مشترک به توافق برسند و این تعداد، در مدت زمان تعامل آنها با یکدیگر برای تولید کلید، تغییر نمی‌کند (یعنی در وسط فرآیند، گره‌ای به شبکه اضافه یا کم نمی‌شود). به‌علاوه در این سیستم مدل، یک شنودگر وجود دارد که قصد دارد تا کلید را کشف کند. فرضیات این کار پژوهشی بصورت زیر لیست می شود:

- تمام گره‌ها مجهز به یک آنتن هستند.
- کانال بین گره‌ها هم پاسخ[9] بوده و در طول T شکاف زمانی، تقریباً ثابت است.
- ارتباطات در حالت نیمه‌دوسویه[10] بوده و در نتیجه، هیچ گره‌ای قادر به تبادل اطلاعات به‌صورت هم‌زمان و در یک باند فرکانسی نیست.
- کانال بین گره‌ها، نویز سفید گوسی جمع شونده[11] (AWGN) بوده و لذا پدیدهٔ محوشدگی چندمسیری تجربه نمی‌شود.
- شنودگر اطلاعی از مکان دقیق گره‌ها ندارد، حال آنکه دارای توان محاسباتی نامحدود است و می‌تواند فاز سیگنال‌های دریافتی را به درستی تخمین بزند.
- گره‌ها بطور کامل هم‌زمان‌سازی شده‌اند.

به این دلیل که پارامتر فاز کانال در مقایسه با اندازه‌ی کانال، حساسیت بیشتری به فاصله‌ی بین کاربرها دارد، لذا می‌تواند برای محیط‌هایی که کانال بی‌سیم آن خاصیت محوشوندگی ندارند، به عنوان منبع تصادفی مورد استفاده قرار گیرد. برای روشن‌تر شدن این موضوع، مثالی می‌زنیم تا نشان دهیم با تفاوت اندکی در فاصله‌ی بین دو کاربر، فاز سیگنال ارسالی می‌تواند به میزان قابل توجهی تغییر کند، حال آنکه حساسیت RSS به فاصله ناچیز است. فرض کنید که کاربر A میخواهد برای کاربر B سیگنالی را ارسال کند. اگر فرکانس‌کاری برابر ۳۰۰ مگاهرتز باشد، طول موج برابر خواهد بود با λ=1 m پس یعنی اگر A و B به اندازه یک متر از هم فاصله بگیرند سیگنال دریافتی در هر کدام از کاربران، به میزان 2π رادیان تغییر فاز خواهد داشت. حال اگر یکی از آنها حدود ۱۰ سانتی‌متر جابه‌جا شود، تغییر فازی برابر با حدوداً ۳۶ درجه اتفاق می‌افتد. لذا می‌بینیم که حساسیت فاز نسبت به اندکی جابه‌جایی، بسیار زیاد است. بنابراین از آنجایی‌که تخمین فاصله‌ی بین دو کاربر برای شنودگر همواره با مقداری خطا همراه است، این حساسیت موجب افزایش امنیت کلید خواهد شد. در حالی‌که کمیت RSS حساسیت زیادی به فاصله ندارد و لذا مهاجم که عموماً قادر به تخمین فاصله با دقت قابل قبولی می‌باشد، می‌تواند با احتمال بالایی کلید را کشف کند.

به منظور افزایش آنتروپی کلید و در نتیجه افزایش نرخ تولید کلید، پیشنهاد می‌شود تمامی گره‌ها سیگنالی با فاز تصادفی تولید کنند. در ادامه، پروتکل SKG گروهی پیشنهادی را بیان می‌کنیم.

---

[9] Reciprocal
[10] Half-duplex
[11] Additive White Guassian Noise

University of Qom
Engineering Management and Soft Computing
JEMSC.QOM
Online ISSN: 2538-2675

4) پروتکل تولید کلید گروهی پیشنهادی

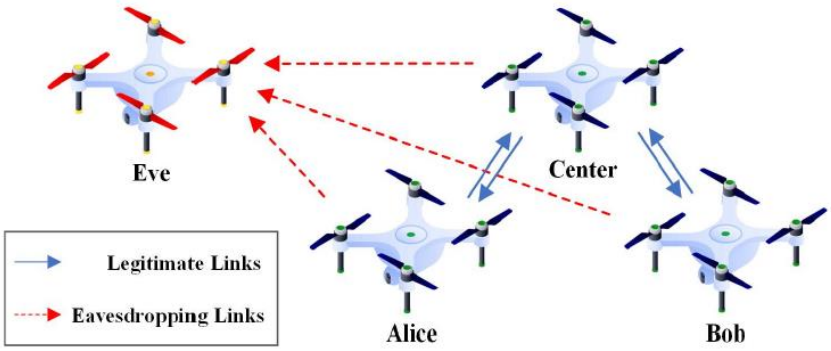
در این بخش، الگوریتم پیشنهادی برای SKG گروهی ارائه می‌گردد. الگوریتم پیشنهادی بر مبنای توپولوژی ستاره است که با اجرای چندباره‌ی الگوریتم، گره‌ها می‌توانند کلیدی به اندازه‌ی $|K|$ بین خودشان به اشتراک بگذارند. بعد از معرفی این پروتکل، نشان می‌دهیم که این پروتکل از پروتکل معرفی شده در [9]، از جهت تعداد شکاف‌های زمانی مورد نیاز بهتر عمل می‌کند.

مطابق شکل 1، ابتدا یک گره دلخواه را به عنوان گره مرکزی در نظر می‌گیریم و آنرا C می‌نامیم. سپس M-1 گره دیگر را به ترتیب از 1 تا M-1 شماره‌گذاری می‌کنیم. توجه شود که اگر سیستم تحرک نداشته باشد یا گره‌ها از موقعیت یکدیگر باخبر باشند، می‌توان گره مرکزی را به راحتی و با حل یک مسأله‌ی بهینه‌سازی ساده به نحوی انتخاب کرد که گره‌ها برای ارتباط با یکدیگر، در مجموع به کمترین توان ارسالی نیاز داشته باشند. اما با توجه به اینکه در سیستم‌های واقعی معمولاً اینگونه نیست، از مطرح کردن این موضوع صرف‌نظر کرده و گره مرکزی را بصورت تصادفی انتخاب می‌کنیم. حال به توضیح مراحل الگوریتم می‌پردازیم:

مرحله ۱: در شکاف زمانی شماره‌ی i که از این پس با $TS(i)$ نمایش می‌دهیم، گره غیرمرکزی i که $1 \le i \le M-1$، فاز تصادفی φ_i (که یکنواخت در بازهٔ 0 و 2π است) را انتخاب می‌کند و سیگنالی با این فاز برای گره C ارسال می‌کند. لذا گرهٔ C سیگنال زیر را دریافت می‌کند:

$$\varphi_{ic} = \varphi_i + \varphi_{Cic} + \varepsilon_{ic} \qquad (1)$$

که φ_{Cic} و ε_{iC} به ترتیب فاز کانال و خطای تخمین می‌باشند. بنابراین در پایان شکاف زمانی $TS(M-1)$، گره C فاز دریافت شده از همهٔ گره‌های غیرمرکزی را در اختیار دارد. شکل 1 این مرحله را به تصویر می‌کشد.



شکل 1. تولید کلید گروهی بر مبنای توپولوژی ستاره

مرحله ۲: در این مرحله، در شکاف زمانی $TS\ (M-1+i)$، گرهٔ C سیگنالی با فاز زیر را برای گرهٔ i ارسال می‌کند:

$$\sum_{\substack{j \neq i \\ j \in \{1,2,\dots,M-1\}}} \varphi_{jc} \qquad (2)$$

توجه شود که در واقع گرهٔ C مجموع فازهای دریافتی از تمام گره‌های دیگر به جز خود آن گرهٔ گیرنده را برای آن گره ارسال می‌کند. بنابراین فاز دریافتی در گرهٔ گیرنده i برابر است با:

$$\left(\sum_{\substack{j\neq i \\ j\in\{1,2,\dots,M-1\}}} \varphi_{jc}\right) + \varphi_{Cci} + \varepsilon_{ci} \tag{3}$$

حال کافی است گرهٔ i فاز φ_i را که در مرحلهٔ قبل تولید کرده بود را به این فاز دریافتی اضافه کند. لذا فاز نهایی برابر می‌شود با:

$$\left(\sum_{\substack{j\neq i \\ j\in\{1,2,\dots,M-1\}}} \varphi_{jc}\right) + \varphi_{Cci} + \varphi_i + \varepsilon_{ic} + (\varepsilon_{ci} - \varepsilon_{ic}) = \left(\sum_j \varphi_{jc}\right) + \varepsilon' \tag{4}$$

همچنین گرهٔ C با جمع کردن فازهایی که در شکاف‌های زمانی 1 تا M-1 دریافت کرده بود، به همین فاز خواهد رسید. بنابراین بدون در نظر گرفتن خطای تخمین، تمام گره‌ها به فاز مشترک زیر می‌رسند (تأثیر خطای تخمین را بعداً در آنالیز عملکرد الگوریتم خواهیم دید):

$$\left(\sum_i \varphi_i + \sum_i \varphi_{Cic}\right) \tag{5}$$

مرحله ۳: حال با کوانتیزه کردن این مقدار توسط یک کوانتیزه کنندهٔ q سطحی، گره‌ها به یک کلید مشترک $\log q$ بیتی می‌رسند و با اجرای این الگوریتم به تعداد $\frac{|K|}{\log q}$ بار می‌توانند به یک کلید مشترک $|K|$ بیتی برسند. برای کوانتیزه کردن، روش‌های بسیاری معرفی شده است که می‌توان از هر یک از آنها استفاده کرد [5]. ما از کوانتیزه کنندهٔ یکنواخت q سطحی استفاده می‌کنیم:

$$Q(x) = Bin(k), if\ x \in \left[\frac{2\pi(k-1)}{q} + \mu, \frac{2\pi k}{q} - \mu\right) \tag{6}$$

که در آن $k = 1, 2, \dots, q$ است. در این رابطه، منظور از $Bin(k)$ نمایش باینری عدد k می‌باشد. هم‌چنین μ ناحیه‌ی حفاظتی[14] می‌باشد که برای افزایش دقت کوانتیزاسیون، لحاظ شده است. اگر فازی در این ناحیه قرار بگیرد، دور ریخته می‌شود.

توجه 1 (مقایسه پروتکل پیشنهادی در این مقاله با مرجع [9]): اگر تعداد تکرار الگوریتم را برابر N_r در نظر بگیریم ($N_r = \frac{|K|}{\log q}$)، در مجموع در پروتکل پیشنهادی ما به $(2M-2)N_r + 1$ شکاف زمانی نیاز است که 1 در آن برای مرحله‌ی توافق اطلاعات است. توجه شود که می‌توان مرحله‌ی توافق اطلاعات را در یک شکاف زمانی انجام داد. هدف از توافق اطلاعات این است که گره‌ها مطمئن شوند تا کلید به اشتراک گذاشته شده برای همه یکسان است و نویز و خطای تخمین‌ها باعث تفاوت هیچ دو کلیدی با یکدیگر نشده است. اما در پروتکل ارائه شده در مرجع [9] به $(2M-1)N_r + 1$ شکاف زمانی نیاز دارد. همان‌طور که می‌بینیم روش پیشنهادی ما N_r شکاف زمانی کمتری نیاز دارد. به این معنا که برای کوانتیزه کننده با تعداد سطوح برابر، هر چه طول نهایی کلید خواسته شده بیشتر باشد، الگوریتم پیشنهادی ما از الگوریتم [9] بهتر عمل می‌کند.

توجه 2 (کلید با آنتروپی بالا): قطعه کلیدهای به‌دست آمده در دور از کاوش کانال، باید در زمان‌های همدوسی مستقل باشند تا کلید خام نهایی خاصیت تصادفی بیشتری داشته باشند. بنابراین داشتن تحرک کافی به تولید بیت‌ها با آنتروپی بالا کمک

Engineering Management and Soft Computing
JEMSC.QOM
Online ISSN: 2538-2675
University of Qom

می‌کند. با این وجود، در پروتکل ارائه شده این محدودیت وجود ندارد؛ چرا که برای یک زمان همدوسی به اندازهٔ کافی بزرگ، می‌توان الگوریتم فوق را به تعداد دلخواه تکرار کرد تا به تعداد بیت دلخواه رسید و ضمناً خاصیت تصادفی همچنان برقرار باشد؛ چرا که طبق طرح پیشنهادی، در هر بار کاوش کانال، فازهای تزریقی تصادفی انتخاب می‌شوند.

5) ارزیابی طرح تولید کلید پیشنهادی

در این بخش، طرح تولید کلید گروهی پیشنهادی را از منظر عملکردی و امنیتی مورد مطالعه قرار می دهیم.

5-1- ارزیابی عملکردی طرح پیشنهادی

در این بخش، احتمال اینکه کلیدهای تولید شده در گره‌ها در یک دور با هم برابر باشند محاسبه می‌گردد. برای این منظور احتمال موافقت اندیس کوانتیزاسیون (P_{QIA}) ارزیابی می‌گردد.

قضیه ۱ [10]: اگر $x, y \in [0, 2\pi]$ دو متغیر مستقل با توزیع یکنواخت در این بازه باشند، آنگاه $x+y$ به پیمانه 2π نیز یک متغیر تصادفی با توزیع یکنواخت در همین بازه است.

توجه شود که فازهای تصادفی تزریقی دارای توزیع یکنواخت در بازه‌ی $[0,2\pi)$ و فاز کانال نیز تصادفی یکنواخت در همین بازه است. بنابراین طبق قضیه ۱، فاز مجموع نیز توزیع یکنواخت دارد.

حال فرض کنیم بدون کم شدن از کلیت مسأله، داریم:

$$\varphi \in \left[\frac{2\pi i}{q}, \frac{2\pi(i+1)}{q}\right) \tag{7}$$

چون خطاهای تخمین برای نسبت سیگنال به نویز[12] (SNR) بالا دارای توزیع گوسی هستند [10]، لذا احتمال اینکه:

$$\varphi' = \varphi + \varepsilon \in \left[\frac{2\pi i'}{q}, \frac{2\pi(i'+1)}{q}\right) \tag{8}$$

برابر می‌شود با:

$$P_{i'}(\varphi) = \int_{\frac{2\pi i'}{q}}^{\frac{2\pi(i'+1)}{q}} \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(x-\varphi)^2}{2\sigma^2}} dx \tag{9}$$

که این احتمال برابر این است که فاز تخمین زده شده، در بازه‌ی i' کوانتیزاسیون بیفتد. بنابراین احتمال اینکه فاز تخمینی هر سه گره در بازه‌ی i' کوانتیزاسیون بیفتد برابر $P_{i'}(\varphi)^3$ می باشد و در نتیجه داریم:

[12] Signal-to-Noise-Ratio

$$P_{QIA}(\varphi) = \sum_{i'=0}^{q-1} P_{i'}(\varphi)^3 \quad (10)$$

پس توانستیم احتمال اینکه در یک دور، قطعه کلیدها با هم برابر باشند را به‌دست آوریم.

2-5- ارزیابی امنیتی طرح پیشنهادی

برای ارزیابی امنیتی طرح تولید کلید گروهی پیشنهادی، آن را از منظر نواحی آسیب‌پذیری [10] مورد مطالعه قرار می‌دهیم. برای این منظور، سناریوی شنود معرفی می‌گردد که بر مبنای آن، فرض می‌شود تعداد زیادی شنودگر در محیط توزیع شده‌اند. شنودگرها به طور جداگانه اقدام به شنود سیگنال‌های کاوش کانال می‌کنند و با انجام پردازش مناسب روی این سیگنال‌ها به دنبال یافتن قطعه کلید مشترک بین آلیس، باب و گره مرکزی هستند. برای این منظور، هر شنودگر فاز حاصل‌ضرب سیگنال‌های دریافتی از آلیس، باب و گره مرکزی را به عنوان $\hat{\theta}_E$ در نظر می‌گیرد که به صورت زیر قابل بیان است:

$$\hat{\theta}_E = \hat{\phi}_{AE} + \hat{\phi}_{BE} + 2\hat{\phi}_{CE} = 2(\phi_A + \phi_B) + \phi_{AC} + \phi_{BC} + \phi_E + \varepsilon_E \quad (11)$$

که در این رابطه $\phi_E = \phi_{AE} + \phi_{BE} + 2\phi_{CE}$ می‌باشد. با مقایسه این رابطه با روابط قبلی، پیداست که هرگاه رابطه $\frac{1}{2}(\phi_{AC} + \phi_{BC}) = \frac{1}{2}(\phi_{AE} + \phi_{BE}) + \phi_{CE}$ برقرار باشد، مقدار $\hat{\theta}_E$ و مقادیر به‌دست آمده در گره‌های قانونی همبستگی بالایی خواهند داشت. در چنین شرایطی، کوانتیزاسیون فاز شنودگر $\hat{\theta}_E$ با احتمال زیاد، به کلید مشترک بین آلیس، باب و گره مرکزی منجر می‌شود. در نتیجه شنودگر می‌تواند کلید را به دست آورد. به بیان ریاضی، می‌توان اختلاف فاز دریافتی در گره‌های قانونی و گره شنودگر را $\Delta\phi$ نامید و سعی کرد $\Delta\phi$ را کمینه نمود. بر این اساس نواحی محرمانه، مکان هندسی نقاطی در فضا می‌باشند که کلید تولید شده توسط شنودگر با کلید به‌دست آمده توسط آلیس، باب و گره مرکزی متفاوت است. همچنین کل فضا منهای نواحی محرمانه، اصطلاحاً نواحی آسیب‌پذیری نامیده می‌شود. به‌عبارت دیگر، نقطه‌ای از فضا آسیب‌پذیر است که در آن شرط $\Delta\phi < \frac{2\pi}{q}$ برقرار گردد [10]. شنودگر مستقر در ناحیه آسیب‌پذیری با احتمال بالایی می‌تواند کلید را به‌دست آورد.

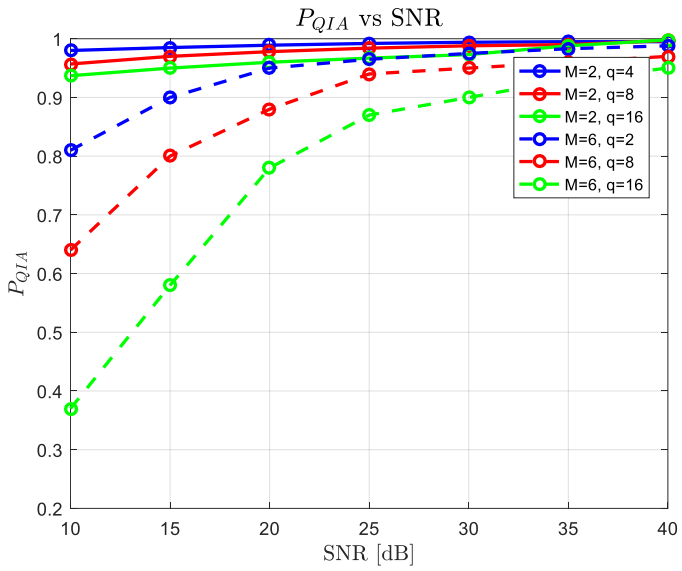
6) نتایج شبیه‌سازی

در این بخش با ارائه شبیه‌سازی‌هایی، طرح تولید کلید گروهی پیشنهاد شده را از منظر عملکرد و امنیت آن مورد مطالعه و بررسی قرار می‌دهیم.

در شکل 2 احتمال تولید کلید موفق بر حسب SNR و برای تعداد گره‌های مختلف در شبکه و همچنین تعداد سطوح مختلف کوانتیزاسیون رسم شده است. مشاهده می‌شود در حالتی که M=6 احتمال تولید کلید صحیح با افزایش SNR به میزان بیشتری افزایش می‌یابد. دلیل این امر این است که وقتی تعداد گره‌های شبکه افزایش می‌یابد، در کلید تولید شده خطاهای تخمین بیشتری با هم جمع می‌شوند و بنابراین نیاز است تا SNR به میزان بیشتری افزایش یابد تا تأثیر آن خطاهای تخمین از بین برود. همچنین مشاهده می‌کنیم که احتمال خطا با افزایش تعداد سطوح کوانتیزاسیون افزایش می‌یابد. به این دلیل که با افزایش سطوح کوانتیزاسیون، با مقدار کمتری خطا ممکن است ناحیه تصمیم جابجا شود و در نتیجه خطا رخ دهد. اما از سوی دیگر، هر چه تعداد سطوح کوانتیزاسیون کمتر باشد، تعداد بیت تولید شده در هر بار اجرای الگوریتم، کمتر خواهد بود که باعث می‌شود

University of Qom
Engineering Management and Soft Computing
JEMSC.QOM
Online ISSN: 2538-2675

برای رسیدن به تعداد بیت کلید مشخص، لازم باشد الگوریتم را به تعداد بیشتری اجرا کنیم. با آزمایش مقادیر مختلف به نظر می‌رسد $M = 16$ مناسب باشد.

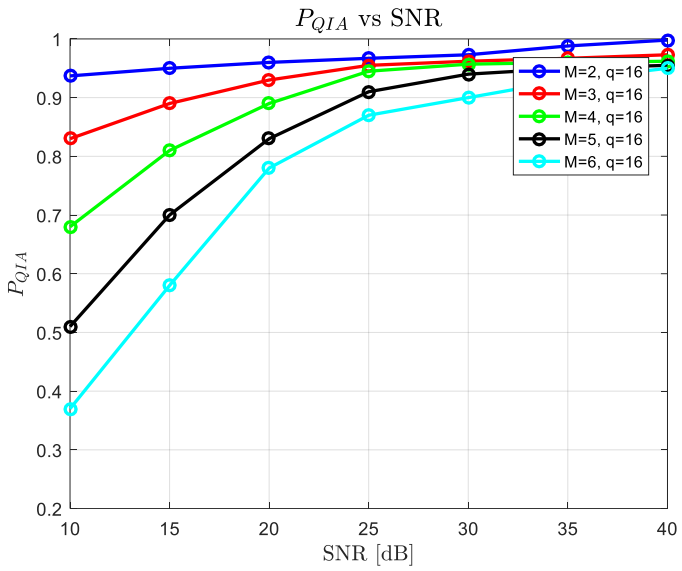


شکل 2. احتمال تولید کلید موفق بر حسب SNR

در شکل 3 احتمال تولید کلید صحیح را برای یک سطح کوانتیزاسیون خاص $q = 16$ و تعداد گره‌های مختلف، ۲ تا ۶ رسم می‌کنیم. مشاهده می‌شود که با افزایش M احتمال تولید کلید صحیح بین تمام گره‌ها کمتر می‌شود که به وضوح به این دلیل است که واریانس خطای تخمین گره‌ها با هم جمع می‌شود و در نتیجه احتمال خطا را بالا می‌برد.

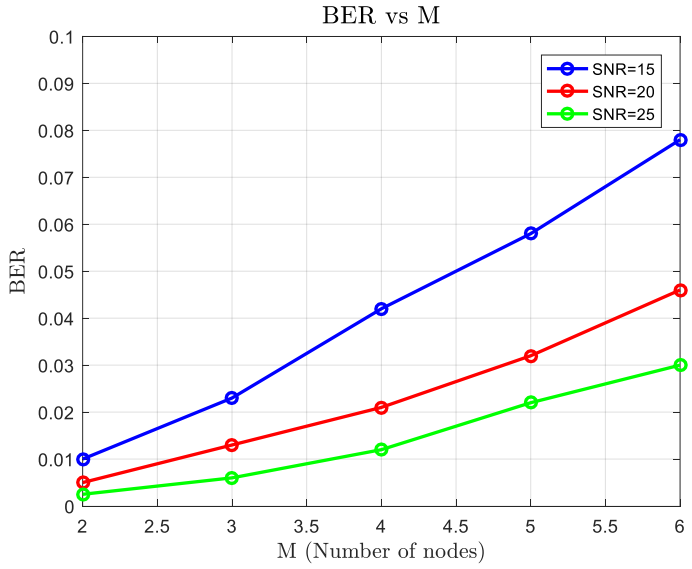
همان‌طور که در پیش‌تر هم اشاره کردیم به دلیل جمع‌شدن خطاهای تخمین با بالارفتن تعداد گره‌ها، اندازهٔ شبکه توسط نرخ خطای بیت[۱۳] (BER) کنترل می‌شود.

[13] Bit Error Rate



شکل 3. احتمال تولید کلید موفق بر حسب SNR (برای تعداد گره‌های مختلف)

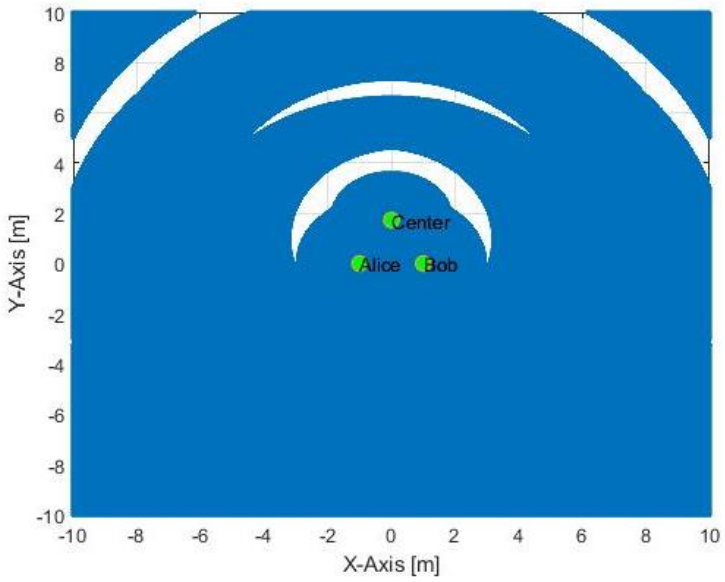
شکل 4 مشاهده می‌کنیم در SNRهای مختلف BER تقریباً به طور خطی با M افزایش می‌یابد (مقیاس‌پذیری طرح تولید کلید پیشنهادی). هر کد تصحیح خطا تا میزان مشخصی از خطا را می‌تواند اصلاح کند. برای مثال اگر از کد BCH با $[n,k,t] = [127,85,13]$ استفاده کنیم قدرت تصحیح خطا برای این کد $\frac{t}{n} = 4.72\%$ خواهد بود. بنابراین در شکل 4 برای مثال، اگر SNR را برابر ۲۰ در نظر بگیریم تعداد گره‌های شبکه از ۶ عدد نمی‌تواند بیشتر باشد. یک راه حل برای این موضوع این است که SNR را افزایش دهیم که چندان راه منطقی به نظر نمی‌رسد. راه دیگر این است که از کدهای تصحیح خطای قوی‌تر استفاده کنیم.



شکل 4. نرخ خطای بیت بر حسب تعداد گره (برای SNRهای مختلف)

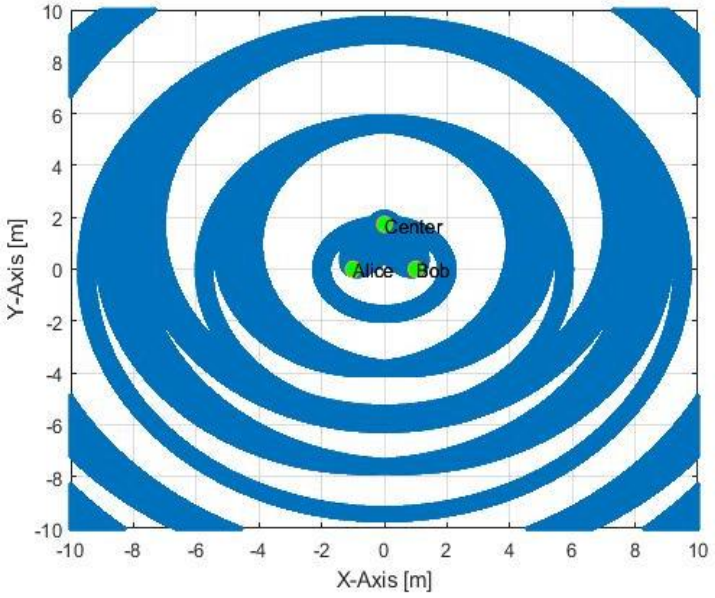
Engineering Management and Soft Computing
JEMSC.QOM
Online ISSN: 2538-2675
University of Qom

حال به منظور بررسی امنیت طرح تولید کلید پیشنهادی، نواحی آسیب‌پذیری آن را مطالعه می‌کنیم. موقعیت آلیس، باب و گره مرکزی در فضای دو بعدی به ترتیب $(-1,0)$، $(+1,0)$ و $\left(0,\sqrt{3}\right)$ در نظر گرفته می‌شود. ابتدا برای فرکانس‌کاری $f = 40$ MHz و تعداد سطوح کوانتیزاسیون $M = 4$ نواحی آسیب‌پذیری را مشخص می‌کنیم. نواحی آسیب‌پذیری و محرمانه مطابق شکل 5 می‌باشد که به ترتیب با رنگ آبی و سفید مشخص شده‌اند. با توجه به شکل زیر ٪92 از فضا را ناحیه آسیب‌پذیری تشکیل می‌دهد.



شکل 5: اشتراک نواحی آسیب‌پذیری برای $f = 40$ MHz و $M = 4$

حال اگر تعداد سطوح کوانتیزه را به $M = 16$ افزایش دهیم و تغییر در سایر پارامترها نداشته باشیم، نواحی آسیب‌پذیری مطابق شکل 6، حدوداً ٪44 از کل فضا را شامل می‌شود. بر این اساس، افزایش تعداد سطوح کوانتیزه موجب کاهش میزان نواحی آسیب‌پذیری می‌شود و از طرفی می‌توان در نظر داشت که نرخ تولید کلید افزایش می‌یابد؛ چرا که تعداد بیت بیشتری در هر بار کاوش کانال استخراج می‌شود. اما لازم به ذکر است که با افزایش تعداد سطوح کوانتیزه، نرخ خطای کوانتیزاسیون افزایش یافته و در نتیجه نرخ خطای کلید نیز افزایش می‌یابد.



شکل 5: نواحی آسیب‌پذیری برای $f = 40\ MHz$ و $M = 16$

7) نتیجه گیری

در این مقاله، با تکیه بر تولید کلید از کانال بی‌سیم، روشی جدیدی برای تولید کلید مخفی برای گروهی از گره‌ها ارائه گردید که در آن از فاز کانال‌ها استفاده کردیم. استفاده از فاز به جای مقدار RSS که در برخی از پژوهش‌های قبلی استفاده شده بود، این امکان را فراهم می‌کند که پروتکل پیشنهادی ما هم در محیط‌های چند مسیری و هم در محیط‌های باز که گره‌ها غالباً به هم نزدیک هستند و کانال‌ها نیز آنتروپی زیادی ندارند، قابل استفاده باشد. پروتکل پیشنهادی در این مقاله، بازه‌های زمانی کمتری برای اجرا نیاز داشته و بنابراین سرعت الگوریتم بالاتری دارد. در نتیجه نرخ تولید بیت کلید افزایش می‌یابد که بسیار مطلوب است. در ادامه، پروتکل پیشنهادی را از نظر برخی معیارهای عملکردی و امنیتی مورد تحلیل و بررسی قرار دادیم.

برای ادامه کار، پیشنهاد می‌شود که برای ارتقاء امنیت طرح پیشنهادی در این مقاله، بجای کاوش کانال بر روی یک فرکانس، کاوش کانال بر روی چندین فرکانس صورت گیرد تا نواحی آسیب‌پذیری کاهش داده شود [10]. همچنین برای ادامه کار پیشنهاد می‌شود از صفحات هوشمند بازتاب کننده امواج [11] یا رله‌ها [12] نیز در تولید کلید استفاده شود تا اهمیت آنها دیده شود. مخابره در باند موج میلیمتری [13] نیز مقوله‌ای است که احتمالاً می‌تواند به ارتقاء امنیت تولید کلید گروهی کمک کند. همچنین پیشنهاد می‌شود تأثیر جمینگ مخرب بر روی طرح تولید کلید پیشنهادی در این مقاله، با الهام از مرجع [14]، مورد مطالعه قرار گرفته و سپس عملکرد بهبود یابد. در نهایت بجای استفاده از سیگنال تک‌حامله جهت کاوش کانال، می‌توان از سیگنال چندحامله استفاده کرد (مشابه مرجع [15]). در نتیجه، ضمن افزایش بُعد منبع مولد متغیر تصادفی، بایاس فاز حذف شده و بعلاوه بخشی از تأثیر نویز نیز حذف گردد. با این تکنیک، ضمن افزایش نرخ تولید کلید، احتمال تطابق کلیدها نیز افزایش می‌یابد.

University of Qom
Engineering Management and Soft Computing
JEMSC.QOM
Online ISSN: 2538-2675

منابع

[1] A. D. Wyner, “The Wiretap Channel,” *J. Bell System Tech.*, vol. 54, pp. 1355–1387, 1975.

[2] M. Mitev, A. Chorti, H. V. Poor and G. P. Fettweis, “What physical layer security can do for 6G security,” *IEEE Open J. Veh. Technol.*, vol. 4, pp. 375-388, 2023.

[3] X. Chen *et al*., “Covert communications: a comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 2, pp. 1173-1198, 3rd Quart 2023.

[4] X. Chen, D. W. K. Ng, W. H. Gerstacker, and H.-H. Chen, “A survey on multiple-antenna techniques for physical layer security,” *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 1027–1053, 2nd Quart., 2017.

[5] J. Zhang, G. Li, A. Marshall, A. Hu and L. Hanzo, “A new frontier for IoT security emerging from three decades of key generation relying on wireless channels,” *IEEE Access*, vol. 8, pp. 138406–138446, Jul. 2020.

[6] G. Li, L. Hu and A. Hu, “Lightweight group secret key generation leveraging non-reconciled received signal strength in mobile wireless networks,” in *IEEE Int. Conf. Commun. (ICC Workshops)*, Shanghai, China, 2019.

[7] P. Xu, K. Cumanan, Z. Ding, X. Dai, and K. K. Leung, “Group secret key generation in wireless networks: algorithms and rate optimization,” *IEEE Trans. Inf. Foren. Sec.*, vol. 11, no. 8, pp. 1831–1846, Apr. 2016.

[8] C. D. T. Thai, J. Lee, J. Prakash and T. Q. S. Quek, “Secret group-key generation at physical layer for multi-antenna mesh topology,” *IEEE Trans. Inf. Foren. Sec.*, vol. 14, no. 1, pp. 18-33, Jan. 2019.

[9] Q. Wang, K. Xu and K. Ren, “Cooperative secret key generation from phase estimation in narrowband fading channels,” *IEEE J. Selected Areas in Commun.*, vol. 30, no. 9, pp. 1666-1674, Oct. 2012.

[10] A. K. Tirandaz and A. Kuhestani, “Security analysis of a mutual random phase injection scheme to generate a secret key in static point-to-point communications,” *Journal of Electronic & Cyber Defense*, Sept. 2022. (In Persian).

[11] M. Ragheb, A. Kuhestani, M. Kazemi, H. Ahmadi and L. Hanzo, “RIS-aided secure millimeter-wave communication under RF-chain impairments,” *IEEE Trans. Veh. Technol.*, doi: 10.1109/TVT.2023.330745.

[12] M. Letafati, A. Kuhestani, and H. Behroozi, “Three-hop untrusted relay networks with hardware imperfections and channel estimation errors for Internet of Things,” *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 2856–2868, Mar. 2020.

[13] M. Ragheb, S. M. S. Hemami, A. Kuhestani, D. W. K. Ng and L. Hanzo, “On the physical layer security of untrusted millimeter wave relaying networks: A stochastic geometry Approach,” *IEEE Trans. Inf. Foren. Sec.*, vol. 17, pp. 53-68, Feb. 2022.

[14] 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, 15 Mar. 2021.

[15] X. Yuan, Y. Jiang, G. Li and A. Hu, "Wireless Channel Key Generation Based on Multi-subcarrier Phase Difference," *IEEE Internet of Things Journal*, vol. 11, no. 20, pp. 32939-32955, Oct. 2024.