Scientific Journal of Electronic & Cyber Defense
Vol. 11, No. 4, Winter 2024, Serial No. 44
ISSN: 2322-4347 , E-ISSN: 2980-8979

Physical Layer Security with the Aid of Compressive Sensing in the Presence of Non-Ideal Relays by Removing the Effect of Hardware Impairments by Providing an Iterative Method

Maryam Baratian , Hadi zayyani * Ali Kuhestani

* .Associate Professor, Department of Telecommunications and Electronics, Qom University of Technology, Qom, Iran.

(Received: 2022/08/07, Revised: 2023/11/08, Accepted: 2023/12/16, Published: 2024/01/18)

DOR: https://dorl.net/dor/20.1001.1.23224347.1402.11.4.6.3

ABSTRACT

In wireless communications, the channel is available to everyone and therefore, any receiver in the telecommunication coverage area can receive the transmitted signal. In such cases, unauthorized users may use this feature to eavesdrop the information, disrupt data transmission, reduce network performance, and so on. Recently, using compressive sensing in physical layer security has attracted the attention of many researchers. Compressive sensing is very useful when the signals are sparse or compressible such as in image signal processing or image recognition. This is because it can be considered as an encryption system, sampling, compression and encryption, while maintaining a secret matrix. In this paper, we examine the physical layer security in a cooperative wireless communication based on several consecutive relays. In such a model system, the equivalent channel matrix is used as the secure measurement matrix. Since the majority of research work in this field consider relay hardware to be ideal and free of hardware impairments, in this research work, this practical assumption is made in the physical layer security with the help of compressive sensing. We consider a cooperative communication with multiple-hops. Finally, we will propose a solution to improve the secrecy performance of such a system. Simulation results show that in worst case, the screcy rate increases at least 10 percent and this would be increased to 120 percent in the best case. Moreover, computational complexity in terms of simulation run time is increased by 22 percent .

Keywords: Physical layer security, compressive sensing, Cooperative communication, Hardware impairments

This article is an open-access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

Publisher: Imam Hussein University © Authors

* Corresponding Author Email: zayyani@qut.ac.ir

نشریه علمی "پدافند الکترونیکی و سایبری"
سال یازدهم، شماره ۴، زمستان ۱۴۰۲، ص۷۵-۸۲
شاپا الکترونیکی: ۸۹۷۹-۲۹۸۰ شاپا چاپی: ۴۳۴۷-۲۳۲۲

علمی – پژوهشی

امنیت لایه فیزیکی با کمک حسگری فشرده در حضور رله‌های غیر ایده‌آل با رفع اثر نقیصه‌های سخت‌افزاری با ارائه‌ی یک روش تکراری

مریم براتیان [۱]، هادی زیانی *[۲]، علی کوهستانی [۳]

۱. کارشناسی ارشد دانشگاه صنعتی قم، ۲و۳. دانشیار گروه مخابرات و الکترونیک دانشگاه صنعتی قم، قم، ایران.

(دریافت: ۱۴۰۲/۰۵/۱۶، بازنگری: ۱۴۰۲/۰۸/۱۷، پذیرش: ۱۴۰۲/۰۹/۲۵، انتشار: ۱۴۰۲/۱۰/۲۸)
DOR: https://dorl.net/dor/20.1001.1.23224347.1402.11.4.6.3

* این مقاله یک مقاله با دسترسی آزاد است که تحت شرایط و ضوابط مجوز Creative Commons Attribution (CC BY) توزیع شده است.

ناشر: دانشگاه جامع امام حسین (ع)

نویسندگان

چکیده

در ارتباطات بی‌سیم، کانال ارتباطی در دسترس همگان است و لذا هر گیرنده در محدوده پوشش مخابراتی، می‌تواند سیگنال ارسالی را دریافت کند. در چنین شرایطی، کاربران غیرمجاز ممکن است از این ویژگی کانال بی‌سیم برای شنود اطلاعات، ایجاد اختلال در ارسال داده، کاهش عملکرد شبکه و ... استفاده کنند. اخیراً استفاده از حسگری فشرده در برقراری امنیت لایه فیزیکی توجه بسیاری از محققین را به خود جلب کرده است. روش حسگری فشرده در جاهایی که سیگنال‌ها تنک و یا قابل فشرده‌شدن در یک‌پایه باشند، مانند پردازش سیگنال تصویر و یا تشخیص تصویر، بسیار کاربرد دارد؛ چرا که می‌تواند به‌عنوان یک سیستم رمزنگاری در نظر گرفته شود تا ضمن حفظ ماتریس اندازه‌گیری مخفی، عملیات‌های نمونه‌برداری، فشرده‌سازی و رمزگذاری را محقق نماید. در این مقاله، امنیت لایه فیزیکی در یک ارتباط بی‌سیم مشارکتی مبتنی بر چند رله متوالی مورد بررسی قرار گرفته است. در چنین مدلی، ماتریس کانال معادل به‌عنوان ماتریس اندازه‌گیری امن، مورداستفاده قرار می‌گیرد. ازآنجایی‌که اکثریت کارهای پژوهشی صورت‌گرفته شده در این حوزه، سخت‌افزار رله ایده‌آل و عاری از نقیصه‌های سخت‌افزاری در نظر گرفته می‌شود، در این کار تحقیقاتی نیز، فرض عملی نقیصه سخت‌افزاری کوچک در امنیت لایه فیزیکی با کمک حسگری فشرده و در یک شبکه مشارکتی با چندین رله متوالی در نظر گرفته شده است. در نهایت راهکاری جهت بهبود کارایی محرمانگی چنین سیستمی پیشنهاد داده شده است. نتایج شبیه‌سازی روش ارائه شده نشان داد که در بدترین حالت، نرخ محرمانگی حداقل ۱۰ درصد و در بهترین حالت ۱۲۰ درصد افزایش می‌یابد. همچنین، پیچیدگی محاسباتی روش ارائه شده از نظر زمان شبیه‌سازی افزایش ۲۲ درصدی را نشان می‌دهد.

کلید واژه‌ها: امنیت لایه فیزیکی، حسگری فشرده، مخابرات مشارکتی، نقیصه‌های سخت‌افزاری.

۱- مقدمه

تأمین امنیت اطلاعات یکی از موضوعات حیاتی در بسیاری از سیستم‌های مخابراتی محسوب می‌شود. این موضوع، به‌خصوص در شبکه‌های مخابراتی بی‌سیم در مقایسه با ارتباطات سیمی، به دلیل انتشار امواج در محیط باز، چالش‌برانگیزتر است. هر گیرنده‌ای که در حیطهٔ پوشش فرستنده قرار داشته باشد، قادر است سیگنال ارسالی را دریافت کند و در نتیجه، این خطر وجود دارد که اطلاعات توسط شنو دگر رمزگشایی شده و مورد سوءاستفاده قرار گیرد. یکی از روش های برقراری امنیت در شبکه‌های مخابراتی بی‌سیم که اخیراً بسیار موردتوجه قرار گرفته است، امنیت لایه فیزیکی[۱] (*PLS*) است [۱]. *PLS* به‌عنوان یک راهکار امیدوارکننده جهت برقراری امنیت ارتباطات، به روشی هوشمندانه از ویژگی‌های ذاتی کانال ارتباطی بهره‌برداری می‌کند [۲].

ایده *PLS* جدید نیست و به سال ۱۹۴۹ برمی‌گردد؛ آن زمان که آقای شانون [۳] اصول بنیادین رمزنگاری مدرن را در کارهای اولیه خود مطرح کرد. در آن مقاله، شانون طرحی را ارائه می‌کند که در آن فرستنده، اطلاعات رمزگذاری شده را با استفاده از کلید یکبار مصرف[۲] بر روی کانال بدون نویز، در حضور یک شنودگر ارسال می‌کند. در این مقاله، او برای اولین‌بار یک سامانه رمزنگاری را از منظر نظریه اطلاعاتی تحلیل کرد. او این سامانه را به طور کامل امن در نظر گرفت، با این شرط که شنودگر نتواند با در اختیار داشتن متن رمز شده، اطلاعاتی در مورد متن اصلی به دست آورد. شانون نشان داد که برای دستیابی به امنیت کامل، بایستی کلیدی که برای رمزنگاری متن اصلی به کار می‌رود، دارای حداقل طولی برابر با طول متن اصلی باشد. ازآنجاکه متن

*Corresponding Author E-mail:zayyani@qut.ac.ir

[1] Physiacl layer security

[2] One-time pad

اصلی در کاربردهای عملی بسیار طولانی است، لذا طول کلید موردنیاز نیز متعاقباً طولانی خواهد بود و بنابراین مشکل مدیریت کلید وجود خواهد داشت. این مقاله، سرآغاز ارائه روش‌های تأمین امنیت با استفاده از کلید بود. سپس در سال ۱۹۷۵، آقای واینر [۴] روشی برای برقراری امنیت بدون استفاده از کلید، مطرح کرد. او با کمک نظریه اطلاعات، امکان برقراری یک ارتباط کاملاً امن و بدون اتکا به کلیدهای محرمانه و صرفاً با استفاده از خواص فیزیکی کانال را پایه‌گذاری کرد. بر مبنای مقاله آقای واینر، سال ۲۰۰۱، برای اولین‌بار امنیت در کانال‌های رله در مرجع [۵] مورد بررسی قرار گرفت. او در این مقاله، مدل کانال رله را برای سناریویی در نظر گرفت که در آن، رله نه‌تنها به‌عنوان یک یاری‌رسان، بلکه به‌عنوان یک شنودگر احتمالی تلاش دارد تا به پیام‌های محرمانه دسترسی پیدا کند. اخیراً، مطالعاتی در زمینه ارسال امن در شبکه‌های مشارکتی مبتنی بر رله‌های تقویت و ارسال[1] (*AF*) با چندین پرش صورت‌گرفته است [۶،۷] . در این مراجع، رله‌های متوالی کمک می‌کنند تا پیام به‌صورت محرمانه از فرستنده به گیرنده قانونی منتقل شود.

در بین تکنیک‌های *PLS*، حسگری فشرده[2] (*CS*) می‌تواند سیگنال تنک را با نرخ بسیار کمتری در مقایسه با نرخ نمونه‌برداری نایکوئیست فشرده کند. ابعاد سیگنال تنک، بسیار کوچک‌تر از سیگنال اصلی است. علاوه بر این، گیرنده قانونی می‌تواند به‌درستی سیگنال اصلی را با احتمال زیاد تحت شرایط خاص بازسازی کند [۸] . در سال‌های اخیر، *CS* در شبکه‌های نقطه‌به‌نقطه بی‌سیم نیز استفاده شده است که در آن ماتریس کانال به‌عنوان ماتریس اندازه‌گیری برای افزایش امنیت سیستم در نظر گرفته می‌شود [۹] . ترکیبی از ماتریس اندازه‌گیری فشرده‌سازی و ماتریس کانال یک شبکه مشارکتی مبتنی بر رله *AF* را می‌توان به‌عنوان یک ماتریس اندازه‌گیری کارآمد برای *PLS* در نظر گرفت [۱۰] . در چنین سناریویی، شنودگر به‌سختی می‌تواند داده‌های اصلی را استخراج کند. *CS* امکان بازسازی سیگنال را از اندازه‌گیری‌های بسیار کمتر می‌دهد، بنابراین به دلیل کاهش حجم سیگنال، سربار الگوریتمی را به حداقل می‌رساند [۱۱] . در مرجع [۱۲] محققین ظرفیت محرمانه یک شبکه بی‌سیم مشارکتی را با استفاده از تکنیک *CS* بررسی کرده‌اند و در [۱۳] از ماتریس اندازه‌گیری *CS* برای رمزنگاری مبتنی بر امنیت لایه فیزیکی استفاده شده است.

در عمل سیستم‌های مخابراتی از نقیصه‌های سخت‌افزاری مانند نویز فاز، غیرخطی‌بودن تقویت‌کننده، غیر ایده‌آل بودن فیلترها و ... رنج می‌برند [۱۴،۱۵] . هرکدام از این نقیصه‌ها به نحوی، سیگنال پیام را معوج می‌کنند و در نتیجه تأثیر مخربی بر عملکرد سیستم‌های ارتباطی، به‌ویژه برای سیستم‌های با نرخ ارسال بالا دارند. اخیراً برخی مقالات به مطالعه تأثیر نقیصه‌های سخت‌افزاری بر کارایی محرمانگی شبکه‌های مخابراتی محرمانه پرداخته‌اند [۱۶،۱۷] . به طور خاص، در مرجع [۱۵] پژوهشگران به مطالعه تأثیر نقیصه‌های سخت‌افزاری و نیز تخمین ناقص کانال در یک شبکه مشارکتی با یک رله *AF* و بدون قید محرمانگی مخابرات، پرداختند. همچنین محققین در مرجع [۱۶] یک شبکه مشارکتی را در حضور یک رله *AF* از منظر قابلیت اطمینان و امنیت مورد تحلیل قرار دادند. ازآنجاکه رله‌ها عناصر ارزان‌قیمت و پرکاربرد در اینترنت اشیا محسوب می‌شوند، در این کار تحقیقاتی، ما تنها نقیصه‌های سخت‌افزاری در این گره را در نظر می‌گیریم. در ادامه کار [۱۶] محققین در مرجع [۷] تأثیر نقیصه‌های سخت‌افزاری را بر کارایی محرمانگی یک شبکه مخابراتی با دو رله *AF* متوالی (با سه پرش) موردمطالعه قرار دادند. در [۱۷] نقیصه‌های سخت‌افزاری در اینترنت اشیا و در حضور تعداد دلخواه شنودگر مورد بررسی و شبیه‌سازی قرار گرفته است. همچنین در مرجع [۱۸] نویسندگان به ارائه یک طرح تولید کلید مخفی، به ارزیابی امنیت آن با رویکرد محرمانگی هندسی پرداختند.

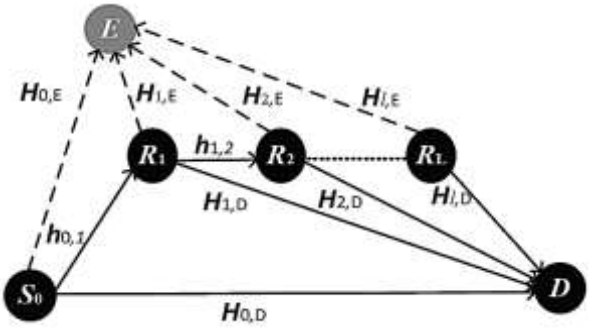
در این مقاله، مشابه مقاله [۱۱] ما با یک شبکه مشارکتی مبتنی بر چندین رله متوالی *AF* سروکار داریم که یک شنودگر در محیط حضور دارد. بر خلاف‌کار تحقیقاتی [۱۱] در سیستم مدل موردمطالعه، رله‌ها از نقیصه‌های سخت‌افزاری رنج می‌برند. ماتریس کانال که ماتریس اندازه‌گیری نامیده می‌شود از توزیع گاوسی پیروی می‌کند. تعداد شکاف‌های زمانی به‌عنوان بُعد اندازه‌گیری *CS* در نظر گرفته می‌شود. در اینجا، امنیت لایه فیزیکی شبکه با کمک *CS* محقق می‌شود. در نهایت، نرخ محرمانه[3] برای ارزیابی عملکرد امنیتی شبکه استفاده می‌شود [*19*]. با ارائه شبیه‌سازی‌های کامپیوتری تأثیر نقیصه‌های سخت‌افزاری بر کارایی محرمانگی شبکه مشارکتی بررسی خواهد شد. در ادامه، راهکاری جهت بهبود امنیت شبکه ارائه خواهد شد.

ادامه مقاله به این صورت است که در ادامه مقدمه، مدل سیستمی مسئله و مدل سیگنال‌های استفاده شده ارائه می‌شود. سپس، در بخش ۳ مدل سیستم در حضور نقیصه‌های سخت‌افزاری معرفی می‌شود. آنگاه، بخش ۴ روش پیشنهادی برای مساله را پیشنهاد می‌دهد در حالی که در بخش ۵ به ارزیابی عملکرد امنیت سیستم پرداخته خواهد شد. سپس، در بخش ۶ آنالیز خطای روش بحث خواهد شد و بعد از آن در بخش ۷ نتایج شبیه‌سازی خواهد آمد. در پایان هم به نتیجه‌گیری خواهیم پرداخت.

[1] Amplify and forward
[2] Compressive sensing
[3] Secrecy

۲- مدل سیستم و سیگنال‌ها

این مدل شامل یک منبع، یک مقصد، یک شنودگر و تعدادی رله AF می‌باشد که برای افزایش امنیت شبکه، از CS استفاده می‌شود. همچنین، نقیصه‌های سخت‌افزاری را برای رله‌ها، به‌عنوان عناصر ارزان‌قیمت و تجهیزات ساده [۱۶] در نظر می‌گیریم. همان‌طوری که در شکل (۱) نشان‌داده‌شده است، سیستم مدل موردمطالعه، یک شبکه رله‌ای بی‌سیم با $(L+1)$ پرش و متشکل از یک گره منبع S_0، L رله‌ی قابل اعتماد R_L، یک گره مقصد D و یک شنودگر E است، که در آن هر گره مجهز به یک آنتن و هر رله AF در حالت نیمه دو طرفه[1] کار می‌کند.



شکل (۱): مدل سیستم **[۱۱]**

در ادامه، بر پایه تکنیک CS، مراحل تولید سیگنال در منبع و استخراج سیگنال در مقصد را تشریح می‌کنیم.

۱) مرحله سنجش: فرض بر این است که سیگنال K-تنک X با طول N از طریق رله با $L+1$ بخش زمانی، از منبع به مقصد انتقال می‌یابد. به عبارت دیگر، در X فقط و فقط K موقعیت غیرصفر وجود دارد.

۲) مرحله برنامه‌ریزی: برای یک رله، سیگنالی که دریافت کرده است یک بردار $N\times 1$ است. در بخش زمانی mام، گره mام سیگنال تقویت شده را ارسال می‌کند، که توسط رله بعدی و نیز مقصد و شنودگر دریافت می‌شود. سیگنال‌های دریافت شده در بخش زمانی mام با $m=0,1...,L$ را می‌توان بصورت زیر بیان کرد:

(۱)
$$y_l(m)=\sqrt{P}h_{m,l}*X_m+Z_l(m)$$

(۲)
$$y_D(m)=\sqrt{P}H_{m,D}*X_m+Z_D(m)$$

(۳)
$$y_E(m)=\sqrt{P}H_{m,E}*X_m+Z_E(m)$$

که $l=m+1$ و علامت $*$ ضرب نقطه‌ای را نشان می‌دهد. P توان انتقال گره mام و $h_{m,l}$ یک بردار $N\times 1$ است که ماتریس انتقال کانال بین گره mام و گره lام را نشان می‌دهد. بردارهای $H_{m,D}$ و $H_{m,E}$ با ابعاد $N\times 1$ به ترتیب بهره‌های کانال از گره mام به مقصد و شنودگر را نشان می‌دهند. بردارهای $Z_D(m)$ و $Z_E(m)$ و $Z_l(m)$ نیز نویز گاوسی سفید با میانگین صفر و واریانس σ^2 هستند. هر رله، سیگنال نویز را تقویت و ارسال می‌کند. به عبارت دیگر، رله l نسخه مقیاس یافته $y_l(m)$ را در زمان l، به صورت زیر ارسال می‌کند:

(۴)
$$x_l=\beta_l y_l(m)\ ,\ \beta_l(i)=\sqrt{\frac{1}{h_{m,l}(i)^2+\sigma^2}}$$

در ادامه، بعد از $M=L+1$ بخش زمانی، سیگنال دریافتی در مقصد و شنودگر به ترتیب، به‌صورت زیر می‌باشد:

(۵)
$$Y_D=H_DX+Z_D=\Phi X+Z_D$$

(۶)
$$Y_E=H_EX+Z_E=\hat{\phi}X+Z_E$$

که $\Phi=H_D$ و $\hat{\phi}=H_E$ ماتریس $M\times 1$ هستند که به ترتیب ماتریس کانال معادل از هر گره به مقصد و شنودگر می‌باشند. Z_D و Z_E به ترتیب بردارهای ترکیبی از نویز انتقال ($Z_D(m)$ و $Z_E(m)$) و نویز اضافه شده از منبع و رله‌های مختلف به مقصد و شنودگر هستند. به طور خاص، ϕ و $\hat{\phi}$ عبارتند از:

(۷)
$$\Phi=\Big[H_{0,D},H_{1,D}*h_{0,1}*\beta_1,...,H_{L,D}\\ *h_{0,1}*\beta_1*...*\beta_{L-1}*h_{L-1,L}\Big]$$

(۸)
$$\hat{\phi}=\big[H_{0,E},H_{1,E}*h_{0,1}*\beta_1,\ ...\ ,\\ H_{L,E}*h_{0,1}*\beta_1*...\\ *\beta_{L-1}*h_{L-1,L}\big]$$

۳) مرحله بازسازی: هدف از بازسازی، بازیابی سیگنال تنک X از روی Y_D است. ابتدا ماتریس Φ به عنوان ماتریس اندازه‌گیری که RIP[2] *[۸]* را برآورده می‌کند را در نظر می‌گیریم. گیرنده مقصد، رابطه (۹) را که مساله بازیابی بردار تنک است [۸]، حل می‌کند:

(۹)
$$\min\left\|\hat{X}\right\|_1 s.t.\left\|Y_D-\Phi\hat{X}\right\|_2<\varepsilon$$

که ε حد بالایی برای مقدار نویز است و $\hat{X}$ سیگنالی است که توسط مقصد بازیابی می‌شود.

در مدل شبکه مدنظر در این مقاله، ماتریس Φ با ابعاد $M\times N$ نشان‌دهنده M بخش زمانی کانال معادل از منبع و رله‌ها به مقصد است. بردار $\Phi^{(m)}$، m ردیف از Y_D را نشان دهد. ماتریس حاوی تمام ضرایب کانال در مقصد $\Phi=\Big[\Phi^{(0)}\Phi^{(1)}...\Phi^{(M-1)}\Big]^T$ است. توجه شود که $\Phi^{(m)}(e.g,h_{m,l},H_{m,D},H_{m,E})$ یک توزیع گاوسی مختلط با میانگین صفر و واریانس $1/M$ دارد. بنابراین، مطابق معادلات، Φ و $\phi^{(0)},\phi^{(1)},....,\phi^{(M-1)},\hat{\phi}$ توزیع مستقل و یکسان دارند. از نظر CS ماتریس $M\times N$ را می‌توان یک ماتریس اندازه‌گیری در نظر گرفت. از طرف دیگر، تصادفی بودن کانال از ویژگی‌های کانال بی‌سیم است که بدست آوردن Φ برای شنودگر را سخت می‌کند. ماتریس کانال معادل در شنودگر $\hat{\phi}$ تقریباً مشابه با مقصد Φ است که می‌تواند به عنوان یک ماتریس اندازه‌گیری در نظر گرفته شود.

[1] Half-duplex

[2] Restricted Isometry Property

۳- مدل سیستم در حضور نقیصه‌های سخت‌افزاری

در عمل، فرستنده-گیرنده‌های فرکانس رادیویی[1] *(RF)* از نقیصه‌های مختلفی رنج می‌برند که باعث ایجاد عدم تطابق بین سیگنال تولید شده و سیگنال ساطع شده، می‌شود. از آنجایی‌که رله‌ها عناصر ارزان قیمتی هستند، در این کار، نقیصه‌های سخت‌افزاری را در این گره‌ها در نظر گرفته می شود. به این منظور، هم در قسمت دریافت پیام از گره قبلی و هم در قسمت ارسال پیام به گره بعدی، نقیصه سخت‌افزاری برای رله‌ها در نظر گرفته می‌شود. مدل سیستم پیشنهادی در شکل (۲) نشان داده شده‌است. برای مدل‌سازی نقیصه‌های سخت‌افزاری ζ و η را به صورت زیر تعریف می‌کنیم [۱۴]:

$$\zeta \sim CN(0,\sigma^2) \quad (۱۰)$$

$$\eta_i \sim CN(0,(\kappa_i)^2 P) \quad (۱۱)$$

توجه شود که مدل نقیصه سخت‌افزاری مورد استفاده در این مقاله، بر مبنای مرجع [۱۴] است. در این مرجع، کل نقیصه‌های سخت‌افزاری موجود در گره‌ها را بعد از اعمال جبران‌سازی، با یک متغیرتصادفی گوسی مدل کرده است. با الهام از مرجع [۱۴]، نویسندگان در مراجع [۱۵] و [۱۶] نیز در کاربردهای اینترنت اشیاء از این مدل استفاده کردند. در روابط فوق، پارامتر $\kappa_i > 0$ سطح نقیصه‌های موجود در کانال iام را توصیف می‌کند. بنابراین، پیام با توجه به اینکه از چند رله می‌گذرد نقیصه‌های سخت‌افزاری مختلفی را تجربه می‌کند. نقیصه‌های سخت‌افزاری موجود با توجه به رابطه نرخ محرمانه و ارتباط آن با Y_D و Y_E، بروی نرخ محرمانه سیستم تأثیر می‌گذارند. لذا، در ادامه راهکاری جهت بهبود امنیت سیستم در حضور نقیصه سخت‌افزاری، ارائه می‌شود.

۴- الگوریتم پیشنهادی جهت بهبود امنیت سیستم

همان‌طوری که در قسمت قبل گفته شد، نقیصه‌های سخت‌افزاری در رله درنظرگرفتن می‌شوند؛ بنابراین، خروجی سیگنال بعد از رله می‌شود:

$$X_l = (\sqrt{P}(h_{m,l}+\zeta_i) * X_m + Z_l(m)) * G_i + \eta_i \quad (۱۲)$$

که ζ_i نقیصه سخت‌افزاری در قسمت دریافت رله است که با ماتریس کانال جمع شده است. همچنین G_i بهره رله و η_i نقیصه سخت‌افزاری در قسمت ارسال رله می‌باشد. با توجه به اینکه تمام گره‌های شبکه، توان برابر دارند، رابطه G_i به صورت زیر می‌شود [۱۱] و [۱۵]:

$$G_i = \sqrt{\frac{1}{(1+\kappa_i^2)h_{m.l}^2+\sigma^2}} \quad (۱۳)$$

با ساده‌سازی رابطه (۱۲) داریم:

$$X_l = \sqrt{P}h_{m,l}X_m G_i + \sqrt{P}X_m G_i \zeta_i + Z_l(m)G_i + \eta_i \quad (۱۴)$$

[1] Radio frequency

همان‌طورکه از رابطه (۱۴) پیداست، فقط قسمت اول به سیگنال اصلی مربوط بوده و بقیه مؤلفه‌ها، نویز و نقیصه سخت‌افزاری هستند. البته باید به این نکته توجه داشت که خود X_m در قسمت اول رابطه نیز دارای نقیصه و نویز می‌باشد، چون از رله قبل گرفته شده است. بنابراین، X_m را دو بخش درنظر می‌گیریم: بخش اول، X_m^1 که بدون نویز و نقیصه سخت‌افزاری است. بخش دوم، X_m^2 که نویز و نقیصه سخت‌افزاری دارد. بدین ترتیب رابطه (۱۴) به رابطه زیر تبدیل می‌شود:

$$X_l = \sqrt{P}h_{m,l}X_m^1 G_i + \sqrt{P}h_{m,l}X_m^2 G_i + \sqrt{P}X_m G_i \zeta_i + Z_i(m)G_i + \eta_i \quad (۱۵)$$

حال، باتوجه‌به توضیحات فوق، برای رفع اثر نقیصه سخت‌افزاری و نویز به روش زیر عمل می‌کنیم:

- ابتدا تخمینی از X را با استفاده از رابطه (۹) به‌دست می‌آوریم.
- با استفاده از رابطه (۱۵) و $h_{m,l}$ و X تخمین زده شده X_m^1 (ایده‌آل) را به دست می‌آوریم.
- دو رابطه به‌دست‌آمده را از هم کم می‌کنیم و مجموع نویز و نقیصه‌ها به دست می‌آید.

این کار، رله به رله انجام می‌شود تا اثر نویز و نقیصه حذف شود.

اکنون با داشتن اختلاف X_m^1 و X می‌توان Y_D و Y_E را اصلاح کرد و نرخ محرمانه را به دست‌آورد. شکل (۳) بلوک دیاگرام روش پیشنهادی را نشان می‌دهد. نکته قابل ذکر درباره همگرایی روش تکراری بالا این است که نتایج شبیه‌سازی نشان داد که با بزرگ بودن نقیصه سخت‌افزاری همگرایی تضمین نمی‌شود و ممکن است واگرایی داشته باشیم. لذا، در شبیه‌سازی‌های مقاله از فرض کوچک بودن نقیصه سخت‌افزاری استفاده می‌کنیم.

۵- ارزیابی عملکرد امنیت سیستم

نرخ محرمانه برای کانال شنود به‌صورت زیر محاسبه می‌گردد [۱۸]

$$R_s = \left[I(X;Y_D) - I(X;Y_E)\right]^+ \quad (۱۶)$$

که $[u]^+ = \max(u,0)$. همچنین $I(X,Y_D)$ و $I(X,Y_E)$ به ترتیب اطلاعات متقابل بین سیگنال منبع X و سیگنال دریافت شده در مقصد Y_D و سیگنال در شنودگر Y_E را نشان می‌دهند که به ترتیب برابر هستند با:

$$I(X;Y_D) = \frac{1}{M}\sum_{j=1}^{M} log\left(1+\frac{[\phi]_j + [\phi]_j^T P}{[Z_D]_j^2}\right) \quad (۱۷)$$

$$I(X;Y_E)=\frac{1}{M}\sum_{j=1}^{M} log\left(1+\frac{[\hat{\phi}]_j+[\hat{\phi}]_j^T P}{[Z_E]_j^2}\right) \quad (۱۸)$$

که در آن $[.]_j$ بیانگر سطر j ام ماتریس یا مقدار j ام بردار است.

۶- آنالیز خطا برای الگوریتم پیشنهادی

اکنون برای الگوریتم پیشنهادی، میزان خطا محاسبه می‌شود. سیگنال دریافتی در رله m ام، از رابطه (۱۹) به دست می‌آید:

$$X_m=(\sqrt{P}(h_{m-1,m}+\zeta_m)*X_{m-1}+Z_m(m))*G_m+\eta_m \quad (۱۹)$$

همانطور که دربخش (۴) گفته شد X_{m-1} دارای دو بخش بدون نقیصه سخت‌افزاری X^1_{m-1} و با نقیصه سخت‌افزاری X^2_{m-1} می‌باشد. بنابراین با ساده‌سازی رابطه (۱۹) به رابطه زیر می‌رسیم:

$$\begin{aligned}X_m&=(\sqrt{P}(h_{m-1,m}+\zeta_m)(X^1_{m-1}+X^2_{m-1})+Z_m)G_m+\eta_m\\&=\sqrt{P}h_{m-1,m}\,X^1_{m-1}G_m+\sqrt{P}h_{m-1,m}\,X^2_{m-1}G_m\\&+\sqrt{P}\zeta_m X_{m-1}G_m+Z_mG_m+\eta_m\\&=X^*_m+X^e_m\end{aligned} \quad (۲۰)$$

سپس سیگنال در مقصد به‌صورت زیر درمی‌آید:

$$\begin{aligned}&Y_D(m)=\sqrt{P}H_{m,D}X_m+Z_D(m)\Rightarrow\\&Y_D(m)=\sqrt{P}H_{m,D}(X^*_m+X^e_m)+Z_D(m)\Rightarrow\\&Y_D(m)=\sqrt{P}H_{m,D}\,X^*_m+\sqrt{P}H_{m,D}X^e_m+Z_D(m)\\&\Rightarrow Y_D=H_DX+Z'_D\end{aligned} \quad (۲۱)$$

اکنون سیگنال $\hat{X}$ از رابطه (۹) به دست می‌آید و سپس سیگنال در هر رله:

$$\hat{X}_m=\sqrt{P}\,h_{m-1,m}\,\hat{X}^1_{m-1}G_m=\hat{X}^*_m \quad (۲۲)$$

سپس $\hat{X}^e_m$ به‌صورت زیر به دست می‌آید:

$$\hat{X}^e_m=Y_mG_m-\hat{X}_m=X_m-\hat{X}_m-\eta_m \quad (۲۳)$$

در ادامه Y_D اصلاح شده به‌صورت زیر است:

$$Y^C_D(m)=Y_D(m)-\sqrt{P}H_{m,D}\,\hat{X}^e_m \quad (۲۴)$$

$$Z^C_D(m)=Z'_D(m)-\sqrt{P}H_{m,D}\hat{X}^e_m=\hat{Z}_D(m) \quad (۲۵)$$

اکنون دو رابطه را مقایسه کرده که به‌صورت زیر نوشته می‌شود:

$$\left\|Z_D(m)-\hat{Z}_D(m)\right\|<\varepsilon'+\varepsilon''=\varepsilon'+\sqrt{P}H_{m,D}\,\eta_m \quad (۲۶)$$

درروش پیشنهادی η_mرا نمی‌توان تخمین زد؛ یعنی همه نقیصه‌های قبل از رله mام تخمین زده می‌شود، بجز رله آخرکه تأثیر خیلی کمی دارد. دلیل این است که درعمل سیگنال ارسال را کامل نمی‌توانیم بخوانیم. هرچه ε' و ε'' کوچکتر باشد اصلاح ضریب امنیت بهتر انجام می‌شود. توجه شود که دقت روش بهینه‌سازی بر روی ε' تاثیرگذار است.

به‌منظور مقایسه طرح *PLS* مبتنی *CS* در این مقاله با سایر روش‌ها، جدول ۱ طراحی شده است که در آن مزایا و معایب روش‌ها ذکر گردیده است. به علاوه، جنبه‌های پیچیدگی پیاده‌سازی و مصرف انرژی نیز مقایسه شده است. همچنین سناریوهای کاربردی بالقوه برای هر روش *PLS* ارائه شده است. جدول ۱ می‌تواند به عنوان راهنمای خوبی جهت انتخاب راهکار مناسب *PLS* برای کاربردهای مختلف اینترنت اشیا، مورد استفاده قرار گیرد.

جدول (۱). مقایسه روش های امنیت لایه فیزیکی

تکنیک *PLS*	مزایا	معایب	پیچیدگی پیاده‌سازی	مصرف انرژی	سناریوهای کاربردی بالقوه
تزریق نویز مصنوعی	تولید نویز مصنوعی، به‌سادگی تحقق می‌یابد.	مصرف انرژی اضافه	متوسط	بالا	پزشکی از راه دور (Telemedicine)
رمزنگاری لایه فیزیکی	به‌راحتی با پروتکل‌های امنیتی موجود قابل تلفیق است.	به کاوش کانال و توافق کلید مخفی نیاز دارد.	بالا	پایین	مربیگری از راه دور (Remote coaching)
چرخش فضای منظومه	درجه آزادی کانال‌ها می‌تواند به طور کامل مورد سوءاستفاده قرار گیرد.	نیاز است تا *CSI* در فرستنده موجود باشد	متوسط	متوسط	ارتباطات دستگاه به دستگاه (D2D)
رله کردن مشارکتی	انعطاف بالا و امنیت بهتر	سربار سیگنالینگ قابل‌توجه	بالا	متوسط	مخابرات وسیله نقلیه هوایی بدون سرنشین (UAV)
حسگری فشرده	عدم نیاز به توان اضافه	ماتریس اندازه‌گیری می‌بایست به اشتراک گذاشته شود	بالا	پایین	شبکه‌های حسگر بی‌سیم (WSN)

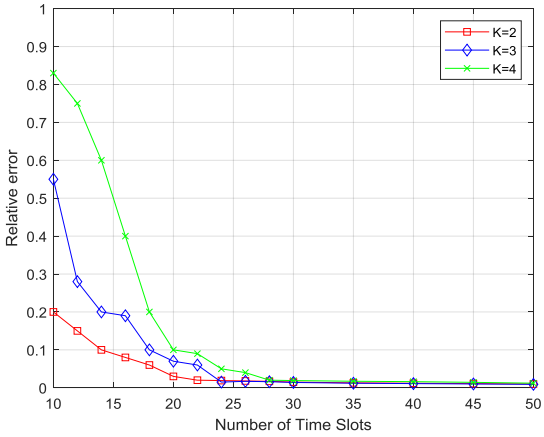
۷- شبیه‌سازی

در این بخش، مدل سیستم پیشنهادی در حضور نقیصه سخت‌افزاری و بهبود آن از طریق حسگری فشرده، شبیه‌سازی می‌شود. نتایج شبیه‌سازی شامل ۱۰۰ آزمایش مستقل برای به‌دست‌آوردن میانگین نتایج با استفاده از نرم‌افزار *MATLAB* می‌باشد. پارامترهای شبیه‌سازی در جدول (۱) ذکر شده‌اند.

جدول (۱) : پارامترهای شبیه‌سازی

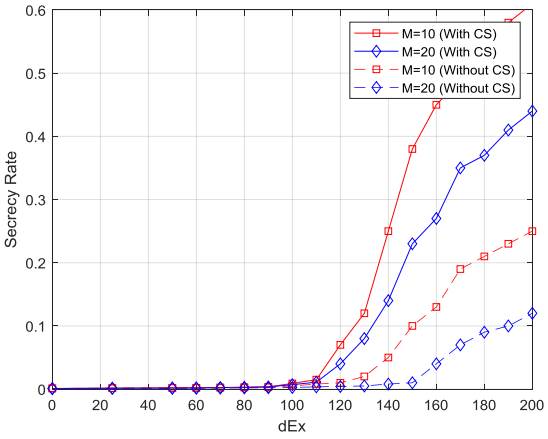
پارامتر	مقدار
$N=50$	ابعاد سیگنال ارسالی
$P=17dBm$	توان ارسالی
$\sigma^2=-70dBm$	توان نویز
$\alpha=1.5$	عامل محوشدگی
$d_{0,D}=100m$	فاصله منبع تا مقصد
$d_{Ex}=50m$ $\quad$ $d_E=20m$	فاصله افقی و عمودی شنودگر

در شبیه‌سازی‌ها، در ابتدا نرخ محرمانه قابل حصول بدون درنظرگرفتن نقیصه سخت‌افزاری را مشاهده می‌کنیم. سپس نقیصه‌های قسمت رله اضافه شده و در نهایت، الگوریتم پیشنهادی را شبیه‌سازی می‌کنیم. در شکل (۲)، خطای بازسازی نسبی در مقابل تعداد شکاف‌های زمانی M برای درجه تنکی مختلف K ارائه شده است. می‌توان مشاهده کرد که هرچه درجه تنکی بیشتر باشد، خطای بازسازی نسبی هم بیشتر می‌شود.



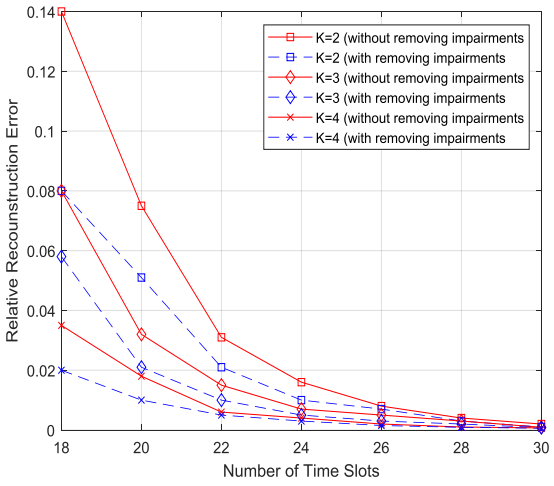
شکل (۲): خطای بازسازی نسبی نسبت به تعداد شکاف‌های زمانی

شکل (۳) نرخ محرمانه قابل حصول را بر حسب فاصله افقی از شنودگر نشان می‌دهد که برای $d_{Ex}<80$ و برای Mهای مختلف صفر می‌باشد که مشاهده می‌شود با افزایش d_{Ex} نرخ محرمانه افزایش می‌یابد. $L=M-1$ بیانگر تعداد رله‌ها بوده که با افزایش آن، نرخ محرمانه افزایش پیدا می‌کند.



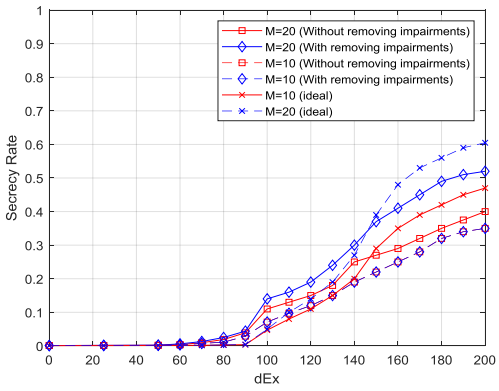
شکل (۳): نرخ محرمانه نسبت به فاصله افقی ازشنودگر در دوحالت حسگری فشرده و بدون آن

اکنون نقیصه‌های سخت‌افزاری به سیستم اعمال می‌کنیم و با الگوریتم پیشنهادی آن را بهبود می‌دهیم. در شکل (۴) خطای بازسازی نسبی مشاهده می‌شود که با درنظرگرفتن نقیصه‌های سخت‌افزاری و بهبود آن می‌باشد. در این شکل، مقدار درجه تنکی مختلف K مقایسه شده است و واضح است که با افزایش K خطای‌بازسازی‌نسبی بیشتر می‌گردد، ولی با بهبود و حذف تقریبی اثر نقیصه‌های سخت‌افزاری، مقدار خطای بازسازی نسبی کاهش پیدا کرده است.

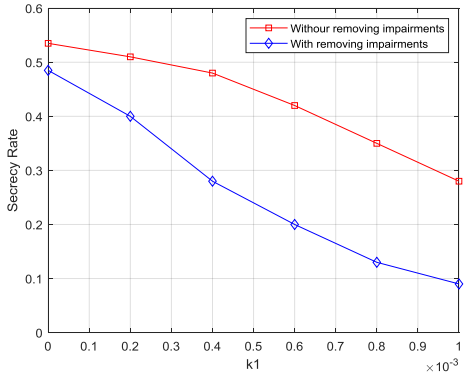


شکل (۴): خطای بازسازی نسبی با نقیصه‌های سخت‌افزاری و بهبود آن.

همان‌طور که در نمودار شکل (۵) مشخص است با وجود نقیصه‌های سخت‌افزاری، نرخ محرمانه نسبت به حالت ایده‌آل بدون نقیصه کمتر است و با رفع تقریبی اثر نقیصه‌های سخت‌افزاری، مقدار نرخ محرمانه افزایش پیداکرده است. این موضوع نشان می‌دهد که حذف اثر نقیصه‌های سخت افزاری تقریباً به خوبی انجام شده است.



شکل (۵): نرخ محرمانه در سه حالت: بدون نقیصه‌های سخت افزاری- با نقیصه‌های سخت‌افزاری- بهبود اثر نقیصه‌های سخت‌افزاری



شکل (۶) : نرخ محرمانه درحضور نقیصه‌ها و بهبود آن

شکل (۶) نرخ محرمانه را نسبت به سطح نقیصه سخت‌افزاری κ نشان می‌دهد. همان‌طوری‌که مشخص است با افزایش κ، نرخ محرمانه کاهش پیدا می‌کند، ولی با حذف تقریبی اثر نقیصه‌های سخت‌افزاری، نرخ محرمانه نسبت به حالت وجود نقیصه‌ها، افزایش می‌یابد که این نتیجه، دلیلی برای کیفیت روش پیشنهادی است. به طور کمی باید گفت که در بدترین حالت، نرخ محرمانگی از ۰٫۴۸ به مقدار ۰٫۵۳ افزایش پیدا کرده است که رشد حداقل قابل توجهی را نشان می‌دهد. البته باید توجه داشت که در بهترین حالت می‌تواند به افزایش ۱۲۰ درصدی نرخ محرمانگی هم منجر شود. این نکته هم قابل ذکر است که وقتی نقیصه‌های سخت‌افزاری افزایش پیدا می‌کند، دقت تخمین کاهش پیدا می‌کند. به همین دلیل، شیب منحنی قرمز بیشتر می‌باشد که این، بدان معنی می‌باشد که نرخ کاهش ضریب امنیت، شدیدتر می‌شود.

درباره پیچیدگی محاسباتی روش جبران نقیصه، باید گفت که یک اجرای شبیه‌سازی بدون جبران نقیصه در آزمایش آخر ذکر شده، حدود ۸٫۵ ثانیه به طول می‌انجامد که این زمان برای یک بار اجرای شبیه‌سازی با جبران نقیصه سخت‌افزاری حدود ۱۰٫۴ ثانیه به طول انجامد. بنابراین، اجرای روش تکراری جبران‌سازی نقیصه سخت‌افزاری حدود ۲۲ درصد پیچیدگی محاسباتی از نظر زمان شبیه‌سازی را افزایش می‌دهد.

۸- نتیجه‌گیری

امنیت لایه فیزیکی راهکاری برای مقابله با شنود مخابراتی و برقراری امنیت در شبکه مخابراتی است که به‌جای استفاده از روش سنتی رمزنگاری از خواص تصادفی کانال برای حصول امنیت استفاده می‌کند. همچنین، حسگری فشرده که به طور سنتی به‌عنوان ابزاری برای فشرده‌سازی و بازسازی سیگنال‌های تنک استفاده می‌شود، به‌عنوان ماتریس اندازه‌گیری مخفی در حصول امنیت هم به کار می‌رود. در این مقاله، به ایده کلی استفاده از حسگری فشرده در امنیت لایه فیزیکی پرداخته شد. در یک مدل شبکه‌های مشارکتی چند پرشه، به تحلیل تأثیر نقیصه‌های سخت‌افزاری پرداخته شد و سپس راهکاری تکراری جهت رفع اثر نقیصه و بهبود امنیت ارائه گردید. در این روش، به‌صورت تکراری، نقیصه را تخمین زده و سپس حذف می‌کنیم و این کار همین‌طور با تکرارهای بیشتر انجام می‌شود. در این مقاله، به طور تحلیلی نشان داده شد که هرچه درجه تنکی سیگنال K بیشتر باشد خطای بازسازی نسبی بیشتر می‌شود. همچنین با رفع تقریبی اثر نقیصه‌های سخت‌افزاری، نرخ محرمانه بهبود داده می‌شد؛ هر چند به حالت ایده‌آل نمی‌رسید. دلیل این است که همواره مقداری نویز و نقیصه در عمل در سیستم وجود خواهد داشت. نتایج شبیه‌سازی نشان داد که این بهبود محرمانگی بین ۱۰ درصد در بدترین حالت و تا ۱۲۰ درصد در بهترین حالت متغیر است. همچنین، این بهبود با افزایش حدود ۲۲ درصدی در محاسبات به‌دست‌آمده است.

۹. مراجع

[1] *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, 2022.*

[2] *M. Tarihi, "A survey on the physical layer security in wirless communication networks",* 4th conference on applicable research on computer engineering and signal processing, *Nov. 2016 (in Persian).*

[3] *C. E. Shannon, "Communication theory of secrecy systems,"* Bell Syst. Tech. J., *vol. 28, p. 656–715, 1949.*

[4] *A. D. Wyner, "The wire-tap channel,"* Bell Syst. Tech. J, *vol. 54, no. 8, pp. 1355-1387, 1975.*

[5] *Y. Oohama, "Coding for Relay Channels with Confidential Messages,"* Proceedings 2001 IEEE Information Theory Workshop, *2001.*

[6] *M. Tatar Mamaghani, A. Kuhestani, and H. Behroozi, "Can a multi-hop link relying on untrusted AF relays render security,"* Wireless Net., *Jan. 2021.*

[7] *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., Mar. 2020.*

[8] *R. G.Braunik, "Compressive Sensing,"* IEEE Sigal Process. Mag., *2007.*

[9] *Y. Zhang, Y. Xiang, L. Y. Zhang, "Secure Wireless Communications Based on Compressive Sensing: A Survey*", IEEE Commun. Surv. Tut., *vol. 21, pp. 1093-1111, 2019.*

[10] *G. Han, X. Fu, Q. Lyu, "Compressed Sensing for Physical Layer Security in Single Relay Cooperative System",* 2019 IEEE International Conference on Signal, Information and Data Processing (ICSIDP);*2019.*

[11] *L. Qing, H. Guangyao and F. Xiaomei, "Physical Layer Security in Multi-Hop AF Relay Network Based on Compressed Sensing,"* IEEE Commun. Lett., *vol. 22, no. 9, pp. 1882-1885, Sept. 2018.*

[12] *S. Chang, J. Li, X. Fu, and L. Zhang*, "*Energy harvesting for physical layer security in cooperative networks based on compressed sensing",* Entropy, *vol. 19, no. 9, p. 462, 2017.*

[13] *R. Dautov and G. R. Tsouri, "Establishing secure measurement matrix for compressed sensing using wireless physical layer security,"* in Int. Conf. Comput. Network. Commun. (ICNC), *pp. 354–358, 2013.*

[14] *E. Bjornson, M. Matthaiou and M. Debbah, "A New Look at Dual-Hop Relaying: Performance Limits with Hardware Impairments,"* IEEE Trans. Commun., *vol. 61, no. 11, pp. 4512-4525, Nov. 2013.*

[15] *V. Shahiri, A. Kuhestani and L. Hanzo, "Short-packet AF relaying for the IoT in the face of imperfect channel estimation and hardware impairments,"* IEEE Trans. Green Commun. Net., *vol. 6, no. 1, pp. 20-36, Mar. 2022.*

[16] *A. Kuhestani, A. Mohammadi and P. L. Yeoh, "Security-reliability trade-off in cyber-physical cooperative systems with non-ideal untrusted relaying," in* Proc. IEEE 4th World Forum on Internet of Things (WF-IoT), *2018, pp. 552-557.*

[17] *M. Fatehi, S. A. Mohajeran, J. Jahanshiri, "Investigation and simulation of hardware impairment on physical layer security in IoT Networks in presence of arbitrary number of eavesdroppers,"* Electronic and cyber defense Journal, *vol. 3, no. 10, 2023 (in Persian).*

[18] *A. Khalili Tirandaz, A. Kuhestani, "Security Evaluation of the Mutual Random Phase Injection Scheme for Secret Key Generation over Static Point-to-Point Communications,"* Electronic and cyber defense Journal, *vol. 10, no. 2, 2022 (in Persian).*

[19] *M. Bloch, J. Barros, M. R. D. Rodrigues and S. W. McLaughlin, "Wireless information-theoretic security,"* IEEE Trans. Inf. Theory, *vol. 54, no. 6, pp. 2515-2534, June 2008.*

[20] *L. Sun and Q. Du, "A review of physical layer security techniques for Internet of Things: Challenges and solutions,"* Entropy, *vol. 20, no. 10, p. 730, 2018*