Electronic & Cyber Defense
Vol. 13, No. 3, 2025 (Serial No. 51). pp. 41- 50
ISSN: 2322-4347, E-ISSN: 2980-8979

Analysis of Impact of Hardware Impairments on Cover Communication Using a Friendly Jammer

Mohammadreza Keshavarzi[1], Moslem Forouzesh[2], Ali Kuhestani[3*]

[1] Assistant Professor, Communication and Information Technology Research Institute, Tehran, Iran. mrkeshavarzi@itrc.ac.ir

[2] Assistant Professor, Amol University of New Technologies, Amol, Iran. m.forouzesh@ausmt.ac.ir
[3] Assistant Professor, Qom University of Technology, Qom, Iran. (Correspondence: Kuhestani@qut.ac.ir)

ARTICLE INFO

Article history:

Article Type: Research paper

Receive: 31 May 2025

Revise: 29 July 2025

Accept: 09 September 2025

Available online: 03 October 2025

Keywords:

Covert communication

Hardware impairments

Friendly jammer

ABSTRACT

The presence of hardware impairments in communication systems is one of the challenges that can impact system performance. In many presented articles, researchers do not consider this issue and ignore their effects, while in cases such as communication security, their role can be more prominent, and perhaps they can be used as a feature to enhance communication security. In this paper, a covert communication protocol for a network including a source, a destination, and a malicious node (observer) is presented. In order to deceive the observer, a friendly jammer is recruited in the network to continuously send jamming. For such a communication network, an optimization problem is designed with the aim of maximizing the covert rate. Since this problem is a non-convex optimization problem, Epigraph and DC methods are used to solve it, and an iterative algorithm is proposed. Simulation results show that the hardware impairments of the transmitter and receiver have the most significant impact on the covert rate, and the hardware impairments of the jammer also have the least impact on the covert rate, so that when the impairment value of the jammer, observer, receiver and transmitter are considered to be 0.5, the covert rate relatives to the case where there is no impairment in any of the nodes decreases by 4.2%, 8%, 62.2% and 62.8%, respectively. Therefore, designing a transmitter and receiver with the least hardware impairment compared to other nodes is essential and plays a significant role in improving covert communication performance.

Cite this article: Keshavarzi, M., forouzesh, M., & Kuhestani, A. (2025). Analysis of Impact of Hardware Impairments on Cover Communication Using a Friendly Jammer. *Electronic and Cyber Defense*, *13*(3), 41-50.

DOR: https://dor.isc.ac/dor/20.1001.1.23224347.1404.13.3.4.3

Publisher: Imam Hossein University

«پدافند الکترونیکی و سایبری»

سال سیزدهم، شماره ۳، پاییز ۱۴۰۴، ص ۴۱- ۵۰

شاپا الکترونیکی: 4347 -2322 شاپا چاپی: 8979- 2980

تحلیل تأثیر نقیصه‌های سخت‌افزاری بر مخابره پنهانِ مبتنی بر اختلال‌گر دوست

محمدرضا کشاورزی[1]، مسلم فروزش[2]، علی کوهستانی* [3]

[1] استادیار ،پژوهشگاه فناوری اطلاعات و ارتباطات کاربردی،تهران ، ایران. *mrkeshavarzi@itrc.ac.ir*

[2] استادیار، دانشگاه فناوری‌های نوین آمل، آمل، ایران. *m.forouzesh@ausmt.ac.ir*

[3] استادیار، دانشگاه صنعتی قم ، قم ، ایران. (نویسنده مسئول: *Kuhestani@qut.ac.ir*)

چکیده

وجود نقیصه‌های سخت‌افزاری در سیستم‌های مخابراتی یکی از چالش‌هایی است که می‌تواند عملکرد سیستم را تحت تأثیر قرار دهد. در بسیاری از مقاله‌های ارائه‌شده، محققین این موضوع را در نظر نمی‌گیرند و از اثر آن‌ها صرف‌نظر می‌کنند؛ درحالی‌که در مواردی مانند امنیت مخابرات، نقش این موارد می‌تواند پررنگ‌تر باشد و چه‌بسا بتوان از آن‌ها به‌عنوان یک ویژگی در جهت ارتقاء امنیت مخابرات بهره‌برداری کرد. در این مقاله، یک پروتکل مخابره پنهان برای یک شبکه شامل یک منبع، یک مقصد و یک گره متخاصم (ناظر) ارائه می‌شود. به‌منظور فریب دادن ناظر، یک اختلال‌گر دوست در شبکه به استخدام گرفته می‌شود تا به‌طور پیوسته سیگنال اختلال ارسال نماید. برای چنین شبکه مخابراتی، یک مسئله بهینه‌سازی باهدف بیشینه کردن نرخ پنهان طراحی می‌گردد. ازآنجایی‌که این مسئله یک مسئله بهینه‌سازی غیر محدب است، برای حل آن از روش Epigraph و DC استفاده نموده و یک الگوریتم تکراری پیشنهاد داده می‌شود. نتایج شبیه‌سازی نشان می‌دهد که نقیصه سخت‌افزاری فرستنده و گیرنده بیشترین تأثیر را بر نرخ پنهان و نقیصه سخت‌افزاری اختلال‌گر نیز کمترین تأثیر را بر نرخ پنهان دارد به صورتی که، وقتی مقدار نقیصه در اختلال‌گر، ناظر، گیرنده و فرستنده را برابر 0.5 در نظر گرفته می‌شود نرخ پنهان نسبت به حالتی که هیچ نقیصه‌ای در هیچ‌یک از گره‌ها وجود ندارد به ترتیب 4.2٪، 8٪، 62.2٪ و 62.8٪ کاهش می‌یابد. بر این اساس، طراحی فرستنده و گیرنده با کمترین نقیصه سخت‌افزاری نسبت به گره‌های دیگر یک امر ضروری بوده و در بهبود عملکرد مخابره پنهان نقش مؤثری خواهد داشت.

مشخصات مقاله

تاریخچه مقاله:

نوع مقاله: علمی- پژوهشی

دریافت: 10 خرداد 1404

بازنگری: 07 مرداد 1404

پذیرش: 18 شهریور 1404

ارائه آنلاین: 11 مهر 1404

کلیدواژه‌ها:

مخابره پنهان

نقیصه‌های سخت‌افزاری

اختلال‌گر دوست

استناد: کشاورزی، محمدرضا، فروزش، مسلم ،کوهستانی، علی. (۱۴۰۴). تحلیل تأثیر نقیصه‌های سخت‌افزاری بر مخابره پنهانِ مبتنی بر اختلال‌گر دوست .*پدافند الکترونیکی و سایبری*، ۱۳(۳)، ص ۴۱-۵۰. https://dor.isc.ac/dor/20.1001.1.23224347.1404.13.3.4.3

ناشر: دانشگاه جامع امام حسین(ع).

1- مقدمه

به دلیل انتشار سیگنال‌های بی‌سیم در هوا، امنیت و حریم خصوصی ارتباطات بی‌سیم به‌عنوان یک ملاحظه حیاتی برای اپراتورهای شبکه محسوب می‌شود. به‌طورکلی، راهکارهای امنیتی برای ارتباطات بی‌سیم بر پایهٔ رمزنگاری در لایه‌های بالای شبکه پیاده‌سازی می‌شوند [1]. اخیراً، محرمانگی نظریه اطلاعاتی[1] (ITS) به‌عنوان یک فن امیدوارکننده برای امن سازی ارتباطات بی‌سیم معرفی‌شده است که در آن هیچ روش پیچیده تبادل کلید بر روی شبکه تحمیل نمی‌شود [2]. در کار پیشگام [3]، واینر نشان می‌دهد که وقتی کانال شنود[2] یک نسخهٔ تنزل یافته از کانال قانونی است، فرستنده و گیرنده می‌توانند به نرخ محرمانگی مثبت دست یابند. برای این منظور، چندین فن برای تقویت ITS پیشنهادشده است: شکل‌دهی پرتو در ارسال [4-6]، انتخاب آنتن [7] و [8]، فن‌های مشارکتی [9] و [10] و به‌کارگیری نویز مصنوعی [11] و [12]. در ITS هدف این است که محتوای پیام محرمانه از حملهٔ شنود محافظت شود. بااین‌حال، در برخی سناریوها با ملاحظات امنیتی متفاوت، فرستنده و گیرنده می‌خواهند وجود ارتباطات خود را از یک متخاصم، مخفی نگه‌دارند و به‌اصطلاح یک مخابره پنهان[3] برپا کنند [13] و [14]. در ادبیات مخابره پنهان، گره متخاصم (Warden) گره‌ای است که سعی می‌کند تشخیص دهد که آیا در شکاف زمانی فعلی، فرستنده سیگنال اطلاعاتی را برای گیرنده ارسال کرده است یا خیر. توجه شود که وقتی Warden حضور مخابره اطلاعات را تشخیص می‌دهد، می‌تواند یک حملهٔ خصمانه به شبکه انجام دهد.

در سال‌های اخیر، مخابره پنهان و امنیت لایه فیزیکی در سناریوهای مختلف ارتباطی بی‌سیم مانند ارتباطات پهبادها [15]، [16] و نیز شبکه‌های رله مشارکتی [17] و [18] بررسی‌شده است. به‌طور خاص، در مرجع [16]، ارتباطات پنهان در حضور یک پهباد با فرض عدم قطعیت مکان گره‌های زمینی در نظر گرفته شد. همچنین محققین در منابع [13] و [14] ارتباطات پنهان را در یک نمونه اینترنت اشیاء[4] (IoT) بررسی کردند و نشان دادند که وجود تداخل از سایر دستگاه‌ها می‌تواند برای پشتیبانی از مخابره پنهان مفید باشد. بااین‌حال، اکثر کارهای تحقیقاتی پیشین، سخت‌افزارهای به‌کارگرفته شده در گره‌ها را ایدئال فرض کرده‌اند؛ درحالی‌که در عمل، تجهیزات در بخش فرستنده و گیرنده از نقیصه‌هایی از قبیل نویز فاز[5]، عدم تعادل[6] I/Q، غیرخطی بودن تقویت‌کننده، خطاهای کوانتیزه‌کردن، مبدل‌ها، میکسرها، فیلترها و نوسان‌سازها[7] رنج می‌برند [19]. هرکدام از این عیوب، به نحوی به سیگنال پیام آسیب می‌زنند. هرچند نقیصه‌های سخت‌افزاری غیرقابل‌اجتناب هستند ولی شدت نقیصه‌ها به تصمیم‌گیری‌های مهندسین در طراحی سخت‌افزاری مربوط می‌شود. می‌توان برای کاهش اثر مخرب هرکدام از نقیصه‌های سخت‌افزاری از راهکارهای جبران سازی بهره برد؛ ولی حتی بعد از جبران سازی، قدری نقیصه باقی خواهد ماند [19] و [20]. این موضوع در دستگاه‌های مخابراتی با نرخ ارسال بالا مانند LTE-A و 5G که در آن‌ها تجهیزات ارزان‌قیمت بکار گرفته می‌شود [21]، حائز اهمیت است. در مقایسه باکارهای اخیر [22] و [23] که به ترتیب تأثیر عدم تعادل I/Q و نویز فاز را در یک شبکه مخابراتی در حضور یک شنودگر خارجی مطالعه کرده‌اند، کل نقیصه‌های سخت‌افزاری را می‌توان بعد از اعمال جبران‌سازهای مناسب به‌صورت یک نویز برآیند در نظر گرفت [20]، [21]، [24-27]. به‌طور خاص، در مرجع [24] عملکرد مخابرات پنهان برای دستگاه‌های ارتباطی مبتنی بر سطح هوشمند قابل تنظیم[8] (RIS) در حضور یک ناظر و با در نظر گرفتن نقیصه سخت‌افزاری موردبررسی قرار می‌گیرد. در مراجع [25]، [26] و [27] نیز امنیت لایه فیزیکی در شبکه‌های مشارکتی مبتنی بر رله‌های تقویت و ارسال و در حضور نقیصه‌های سخت‌افزاری مورد تحلیل و طراحی قرارگرفته است. توجه شود که در مراجع اخیر [20]، [21]، [24-27] مخابرات پنهان مدنظر نبوده است.

در این کار تحقیقاتی، متفاوت با اکثر کارهای پیشین در حوزهٔ امنیت شبکه‌های بی‌سیم که سخت‌افزارهای فرستنده و گیرنده را ایدئال فرض کرده‌اند، در این مقاله، نقیصه‌های سخت‌افزاری رادیو فرکانسی[9] (RF) در تحلیل و طراحی مخابرات پنهان در نظر گرفته می‌شود. این موضوع در تحلیل‌های امنیت شبکه از اهمیت بالایی برخوردار است؛ زیرا با ایدئال فرض کردن سخت‌افزارها ممکن است تحلیل‌های شبکه این اطمینان را بدهد که امنیت شبکه برقرار است؛ در حالی در عمل به دلیل نقیصه‌ها این مهم رخ ندهد و برای شبکه چالش‌هایی را ایجاد نماید. برای مقابله با این چالش در این مقاله، یک شبکه شامل یک منبع، یک مقصد، یک گره متخاصم (ناظر) و یک اختلال‌گر دوست در حضور نقیصه‌های سخت‌افزاری موردبررسی قرار می‌گیرد. وظیفه

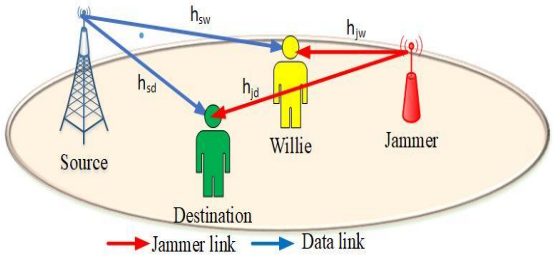
[1] Information Theoretic Secrecy
[2] Wiretap channel
[3] Covert communication
[4] Internet-of-Things

[5] Phase noise
[6] Imbalance
[7] Oscillator
[8] Reconfigurable Intelligent Surface
[9] Radio frequency

اختلال‌گر، فریب دادن ناظر است به‌طوری‌که به‌طور پیوسته سیگنال اختلال ارسال می‌نماید. برای ارزیابی مدل سیستم پیشنهادی با در نظر گرفتن نقیصه‌ها در تمام گره‌های موجود در شبکه، یک مسئله بهینه‌سازی باهدف بیشینه کردن نرخ پنهان پیشنهاد داده می‌شود. در مسئله پیشنهادی، محدودیت حداکثر توان موجود در منبع و اختلال‌گر و الزامات برقراری مخابره پنهان به‌صورت توأمان موردتوجه قرارگرفته‌اند. ازآنجایی‌که مسئله بهینه‌سازی پیشنهادی غیر محدب است برای حل آن از روش‌های Epigraph و DC استفاده نموده و درنهایت یک الگوریتم تکراری برای حل آن پیشنهاد می‌شود.

2- مدل سیستم

همان‌طور که در شکل (1) نشان داده‌شده است، سیستم موردمطالعه ما یک شبکه بدون سیم متشکل از یک منبع، یک مقصد، در حضور یک اختلال‌گر دوست و یک ناظر متخاصم (Willie) است. تمام گره‌های موجود در این مدل سیستم، مجهز به یک آنتن می‌باشند. ناظر موجود در شبکه، یک گره خارجی است که سعی بر کشف این موضوع دارد که آیا فرستنده در اسلات زمانی فعلی برای گیرنده اطلاعاتی ارسال کرده است یا خیر؟ اگر ناظر متوجه ارسال داده توسط منبع شود، می‌تواند حمله خصمانه‌ای را علیه شبکه انجام دهد. برای چنین دستگاهی، استراتژی کمکی مبتنی بر وجود سیگنال اختلال در شبکه پیشنهاد می‌شود که بتواند با پنهان کردن مخابره بین فرستنده و گیرنده به جلوگیری از حمله احتمالی توسط ناظر یاری دهد. در این مدل سیستم، نقیصه سخت‌افزاری را موردتوجه قرار داده و تأثیر آن بر کارایی



شکل (1): مدل سیستم

شبکه موردبررسی قرار می‌گیرد. این مدل سیستم پیشنهادی در شبکه‌هایی از قبیل شبکه‌های نظامی مفید خواهد بود.

به‌منظور ایجاد خطا در آشکارسازی مخابره توسط ناظر، فرستنده در برخی از اسلات‌های زمانی به ارسال داده مبادرت می‌ورزد و در بقیه اسلات‌ها خاموش می‌ماند. برای ارسال داده از روش دسترسی چندگانه تقسیم زمانی[1] استفاده می‌شود و به‌منظور فریب دادن ناظر، چه منبع داده ارسال کند و چه نکند اختلال‌گر به‌طور پیوسته سیگنال اختلال را ارسال خواهد کرد.

این مخابره در قالب T اسلات زمانی که هر اسلات شامل ارسال n سمبل است اجرا خواهد شد. لازم به ذکر است که قبل از راه‌اندازی شبکه، اسلات‌های زمانی و شاخص اسلات‌هایی که منبع در آن به ارسال داده می‌پردازد به گیرنده اطلاع‌رسانی خواهد شد. در شبکه در نظر گرفته‌شده، فرض می‌شود که تمامی گره‌های موجود به‌صورت نیمه دوطرفه عمل می‌کنند. همچنین فرض می‌شود که گره‌ها به‌صورت کامل با یکدیگر هم‌زمان هستند .سیگنال داده در منبع و اختلال در اختلال‌گر در هر اسلات زمانی به ترتیب به‌صورت $\mathbf{x}=\left[x^1,x^2,\ldots,x^n\right]$ و $J=\left[j^1,j^2,\ldots,j^n\right]$ بیان می‌شود.

بر این اساس، سیگنال دریافتی در گره m (مقصد و ناظر) در اسلات زمانی i به‌صورت زیر است.

$$\begin{cases} H_0: y_m[i]=(J[i]+\eta_j)h_{jm}+n_m[i]+\eta_m^{(1)} \\ H_1: y_m[i]=(x[i]+\eta_s)h_{sm}+ \\ \qquad (J[i]+\eta_m)h_{jm}+n_m[i]+\eta_m^{(2)} \end{cases} \quad (1)$$

که $n_m \sim CN\left(0,\sigma_m^2\right)$ نویز دریافتی در گره گیرنده m است و همچنین کانال بین منبع-گره m و اختلال‌گر-گره m به ترتیب به‌صورت $h_{sm} \sim CN(0,1)$ و $h_{jm} \sim CN(0,1)$ تعریف می‌شود. دو حالت H_0 و H_1 مبین ارسال و عدم ارسال داده توسط منبع می‌باشند. η_m نقیصه در گیرنده m است. نتایج تجربی در [2] تأیید می‌کنند که این نویزهای اغتشاشی به‌خوبی با توزیع گوسی مدل می‌شوند و البته این مدل از دیدگاه قضیه حد مرکزی نیز قابل‌درک است. ویژگی کلیدی این مدل این است که واریانس نویز در هر آنتن نسبت مستقیمی با توان سیگنال در آن آنتن دارد [2]. در گیرنده m این نویزهای اغتشاشی یادشده با توجه به قضیه حد مرکزی دارای یک توزیع گوسی به‌صورت $\eta_m^{(1)} \sim CN\left(0,\kappa_m^2 p_j |h_{jm}|^2\right)$ و $\eta_m^{(2)} \sim CN\left(0,\kappa_m^2 p_j |h_{jm}|^2+\kappa_m^2 p |h_{sw}|^2\right)$ است. لازم به ذکر است که نقیصه در گره‌های ارسال‌کننده سیگنال یعنی منبع و اختلال‌گر به ترتیب به‌صورت $\eta_s \sim CN\left(0,\kappa_s^2 p_s\right)$ و $\eta_j \sim CN\left(0,\kappa_j^2 p_j\right)$ تعریف می‌شود. ناظر مبتنی بر توان سیگنال دریافت شده تصمیم می‌گیرد که آیا مخابره‌ای بین گره‌های شبکه صورت گرفته است و یا خیر. با توجه به مطالب

[1] Time-Division Multiple-Access (TDMA)

بیان‌شده توزیع سیگنال دریافتی در ناظر به‌صورت زیر تعریف می‌شود.

$$y_w^i \mid H_0 \sim CN\left(0, p_j \mid h_{jw} \mid^2 + \kappa_j^2 p_j \mid h_{jw} \mid^2 + \kappa_w^2 p_j \mid h_{jw} \mid^2 + \sigma_w^2\right)$$

$$y_w^i \mid H_1 \sim CN\left(0, p \mid h_{sw} \mid^2 + \kappa_s^2 p \mid h_{sw} \mid^2 + p_j \mid h_{jw} \mid^2 + \kappa_j^2 p_j \mid h_{jw} \mid^2 + \kappa_w^2 p_j \mid h_{jw} \mid^2 + \kappa_w^2 p \mid h_{sw} \mid^2 + \sigma_w^2\right) \quad (2)$$

در مخابره پنهان، ناظر یک آستانه تصمیم‌گیری را انتخاب می‌کند و مبتنی بر مقایسهٔ کل توان دریافت شده در اسلات زمانی و آستانه مذکور، تصمیم بر وجود یا عدم وجود مخابره می‌گیرد. به‌عبارت‌دیگر، ناظر مبتنی بر $\frac{\sum_{i=1}^{n} \mid y_w^i \mid^2}{n} \underset{H_0}{\overset{H_1}{\gtrless}} \omega$ تصمیم‌گیری می‌کند. برای سادگی در نوشتار دو پارامتر زیر تعریف می‌شوند:

$$\theta_{jw} \triangleq 1 + \kappa_j^2 + \kappa_w^2$$
$$\mu \triangleq 1 + \kappa_s^2 + \kappa_w^2 \quad (3)$$

با توجه به رابطه (3) رابطه (4) به‌صورت زیر بازنویسی می‌شود:

$$\begin{cases} y_w^i \mid H_0 \sim CN(0, p_j \theta_{jw} \mid h_{jw} \mid^2 + \sigma_w^2) \\ y_w^i \mid H_1 \sim CN(0, p\mu \mid h_{sw} \mid^2 + p_j \theta_{jw} \mid h_{jw} \mid^2 + \sigma_w^2) \end{cases} \quad (4)$$

هنگامی‌که منبع سیگنال داده را ارسال کند ولی ناظر تصمیم بر H_0 بگیرد، از دست دادن آشکارسازی با احتمال P_{MD} به وقوع می‌پیوندد. همچنین اگر منبع ارسال داده خود را متوقف کند ولی ناظر تصمیم بر H_1 بگیرد، هشدار غلط با احتمال P_{FA} اتفاق می‌افتد. بنابراین مخابره در صورتی پنهان خواهد بود که "$for\ any\ \varepsilon \geq 0, P_{MD} + P_{FA} \geq 1 - \varepsilon, \text{as } n \to \infty$" برقرار باشد. برای محاسبه احتمال‌های P_{MD} و P_{FA} و با توجه مقدار آستانه تصمیم‌گیری ناظر یعنی ω روابط زیر قابل‌استخراج است:

$$P_{FA} = P\left(\frac{\sum_{i=1}^{n} \mid y_w^i \mid^2}{n} \geq \omega \mid H_0\right)$$
$$P_{MD} = P\left(\frac{\sum_{i=1}^{n} \mid y_w^i \mid^2}{n} \leq \omega \mid H_1\right) \quad (5)$$

برای محاسبه مقادیر P_{FA} و P_{MD} لازم است توزیع انرژی سیگنال به‌دست‌آمده در رابطه (4) محاسبه شود. در روابط بالا $\frac{\sum_{i=1}^{n} \mid y_w^i \mid^2}{n}$ میانگین انرژی دریافتی در هر ارسال است که دارای توزیع خی[1]-دو با 2n درجه آزادی است.

$$\begin{cases} \frac{\sum_{i=1}^{n} \mid y_w^i \mid^2}{n} \mid H_0 \sim (\sigma_w^2 + \gamma) \frac{\chi_{2n}^2}{n} \\ \frac{\sum_{i=1}^{n} \mid y_w^i \mid^2}{n} \mid H_1 \sim (\sigma_w^2 + \gamma) \frac{\chi_{2n}^2}{n} \end{cases} \quad (6)$$

که با توجه به رابطه (4) γ به‌صورت زیر تعریف می‌شود:

$$\gamma = \begin{cases} H_0 : p_j \theta_{jw} \mid h_{jw} \mid^2 \\ H_1 : p\mu \mid h_{sw} \mid^2 + p_j \theta_{jw} \mid h_{jw} \mid^2 \end{cases} \quad (7)$$

برای ادامه تحلیل‌ها، نیاز به دانستن توزیع متغیر تصادفی γ است که این توزیع به‌صورت زیر قابل‌بیان است:

$$f(\gamma) = \begin{cases} H_0 : \frac{1}{p_j \theta_{jw} \sigma_{jw}} e^{-\frac{\gamma}{p_j \theta_{jw} \sigma_{jw}}} \\ H_1 : \frac{1}{p_j \theta_{jw} \sigma_{jw} - p\mu\sigma_{sw}} \left[e^{-\frac{\gamma}{p_j \theta_{jw} \sigma_{jw}}} - e^{-\frac{\gamma}{p\mu\sigma_{sw}}} \right] \end{cases} \quad (8)$$

بر این اساس مقادیر P_{FA} و P_{MD} را می‌توان به‌صورت زیر بازنویسی نمود.

$$\begin{cases} P_{FA} = P\left((\sigma_w^2 + \gamma) \frac{\chi_{2n}^2}{n} \geq \omega \mid H_0\right) \\ P_{MD} = P\left((\sigma_w^2 + \gamma) \frac{\chi_{2n}^2}{n} \leq \omega \mid H_1\right) \end{cases} \quad (9)$$

اکنون با توجه به قانون قوی اعداد بزرگ[2] (SLLN) رابطه (9) به‌صورت زیر به دست می‌آید:

$$\frac{\chi_{2n}^2}{n} \underset{n \to \infty}{\xrightarrow{SLLN}} 1$$
$$\begin{cases} P_{FA} = P\left((\sigma_w^2 + \gamma) \geq \omega \mid H_0\right) \\ P_{MD} = P\left((\sigma_w^2 + \gamma) \leq \omega \mid H_1\right) \end{cases} \quad (10)$$

حال با توجه به رابطه (10) و توزیع به‌دست‌آمده برای γ می-

[1] Chi-squared
[2] Strong Law of Large Numbers (SLLN)

توان به محاسبه مقادیر احتمال‌های هشدار غلط و از دست دادن آشکارسازی پرداخت.

$$P_{FA}=\left(p_j\theta_{jw}\,|\,h_{jw}\,|^2\geq\omega-\sigma_w^2\,|\,H_0\right)=\int_{\omega-\sigma_w^2}^{\infty}\frac{1}{p_j\theta_{jw}\sigma_{jw}}e^{-\frac{\gamma}{p_j\theta_{jw}\sigma_{jw}}}d\gamma=e^{-\frac{\omega-\sigma_w^2}{p_j\theta_{jw}\sigma_{jw}}} \quad (11)$$

$$\begin{aligned}P_{MD}&=P(p\mu\,|\,h_{sw}\,|^2+p_j\theta_{jw}\,|\,h_{jw}\,|^2\leq\omega-\sigma_w^2\,|\,H_1)\\&=\int_0^{\omega-\sigma_w^2}\frac{1}{p_j\theta_{jw}\sigma_{jw}-p\mu\sigma_{sw}}e^{-\frac{\gamma}{p_j\theta_{jw}\sigma_{jw}}}d\gamma-\\&\int_0^{\omega-\sigma_w^2}\frac{1}{p_j\theta_{jw}\sigma_{jw}-p\mu\sigma_{sw}}e^{-\frac{\gamma}{p\mu\sigma_{sw}}}d\gamma\\&=1+\frac{p\mu\sigma_{sw}}{p_j\theta_{jw}\sigma_{jw}-p\mu\sigma_{sw}}e^{-\frac{\omega-\sigma_w^2}{p\mu\sigma_{sw}}}-\\&\frac{p_j\theta_{jw}\sigma_{jw}}{p_j\theta_{jw}\sigma_{jw}-p\mu\sigma_{sw}}e^{-\frac{\omega-\sigma_w^2}{p_j\theta_{jw}\sigma_{jw}}}\end{aligned} \quad (12)$$

به جهت سادگی در نوشتار، دو پارامتر جدید به‌صورت $\alpha=p_j\theta_{jw}\sigma_{jw}$ و $\beta=p\mu\sigma_{sw}$ تعریف می‌شود. با توجه به روابط به‌دست‌آمده، اکنون می‌توان شرط محرمانگی مخابرات را محاسبه کرد:

$$P_{FA}+P_{MD}=1+\frac{\beta}{\alpha-\beta}e^{-\frac{\omega-\sigma_w^2}{\beta}}-\frac{\alpha}{\alpha-\beta}e^{-\frac{\omega-\sigma_w^2}{\alpha}}+e^{-\frac{\omega-\sigma_w^2}{\alpha}}\geq 1-\varepsilon, \quad (13)$$

که این قید به‌صورت زیر ساده می‌گردد:

$$\frac{\beta}{\alpha-\beta}\left[e^{-\frac{\omega-\sigma_w^2}{\alpha}}-e^{-\frac{\omega-\sigma_w^2}{\beta}}\right]\leq\varepsilon \quad (14)$$

مقدار ω را ناظر انتخاب می‌کند و با توجه به عدم وجود سیگنالینگ بین منبع و ناظر، این مقدار در منبع نامعلوم است. اما از طرف دیگر، منبع و اختلال‌گر باید مقدار توان برای ارسال داده و سیگنال اختلال را محاسبه کنند که این مقدار به آستانه تصمیم‌گیری در ناظر ربط دارد. برای مقابله با این چالش، یک سناریو بدترین حالت موردتوجه قرار خواهد گرفت؛ یعنی حالتی که ناظر توانایی داشته باشد مقدار بهینه این آستانه را محاسبه نمایید، یعنی مقداری که خطای تشخیص شنودگر را به حداقل خود می‌رساند. لازم به ذکر است اگر در این حالت مخابره پنهان وجود داشته باشد به ازای همه مقادیر آستانه نیز یک مخابره پنهان تجربه خواهد شد.

در این مرحله به محاسبه مقدار بهینه ω به‌گونه‌ای که رابطه زیر را کمینه کند پرداخته می‌شود:

$$\min_{\omega}\ \frac{\beta}{\alpha-\beta}\left(e^{-\frac{\omega-\sigma_w^2}{\alpha}}-e^{-\frac{\omega-\sigma_w^2}{\beta}}\right) \quad (15)$$

برای محاسبه مسئله بهینه‌سازی بدون قید (17)، می‌توان از تابع هدف نسبت به متغیر بهینه‌سازی مشتق گرفته و برابر صفر قرارداد و مقدار ω بهینه را محاسبه نمود.

$$\frac{\partial(P_{FA}+P_{MD})}{\partial\omega}=0\Rightarrow\omega_{opt}=\frac{1}{\frac{1}{\alpha}-\frac{1}{\beta}}\ln(\frac{\beta}{\alpha})+\sigma_w^2 \quad (16)$$

اکنون با قرار دادن مقدار ω_{opt} به‌دست‌آمده از رابطه (16)، مقدار کمینه رابطه (13) به‌صورت زیر به دست می‌آید:

$$P_{FA}+P_{MD}\,|_{\omega_{opt}}=\frac{\beta}{\alpha-\beta}\left[e^{-\frac{\beta\ln(\frac{\beta}{\alpha})}{\beta-\alpha}}-e^{-\frac{\alpha\ln(\frac{\beta}{\alpha})}{\beta-\alpha}}\right]\leq\varepsilon \quad (17)$$

پس از انجام ساده‌سازی‌های لازم بر روی رابطه (17)، الزام داشتن یک مخابره پنهان در مدل سیستم پیشنهادشده به‌صورت زیر ساده می‌شود:

$$\frac{\alpha}{\alpha-\beta}\ln(\frac{\beta}{\alpha})\leq\ln(\varepsilon) \quad (18)$$

بعد از محاسبه الزام مخابره پنهان به‌صورت ساده‌شده، در ادامه به محاسبه سیگنال دریافتی در گیرنده نهایی و نرخ قابل‌دستیابی در گیرنده اصلی پرداخته می‌شود. سیگنال دریافتی در گیرنده اصلی به‌صورت زیر است:

$$y_d^i=(x[i]+\eta_s)h_{sd}+(J[i]+\eta_j)h_{jd}+\eta_d[i]+n_d[i] \quad (19)$$

که دارای توزیع به‌صورت زیر است:

$$y_d^i\sim CN(0,\mu_d P\,|\,h_{sd}\,|^2+\lambda p_j\,|\,h_{jd}\,|^2+\sigma_d^2) \quad (20)$$

که $\mu_d\sim 1+\kappa_s^2+\kappa_d^2$ و $\lambda_d\sim 1+\kappa_j^2+\kappa_d^2$.

3- فرمول‌بندی مسئله بهینه‌سازی

با توجه به سیگنال دریافتی در گیرنده اصلی و واریانس توزیع آن، می‌توان سیگنال به نویز گیرنده اصلی را به‌صورت زیر محاسبه نمود:

$$SNR_d=\frac{P\,|\,h_{sd}\,|^2}{(\kappa_d^2+\kappa_s^2)P\,|\,h_{sd}\,|^2+\lambda_d p_j\,|\,h_{jd}\,|^2+\sigma_d^2} \quad (21)$$

بر این اساس نرخ قابل‌دسترسی در گیرنده اصلی به‌صورت زیر

خواهد بود:

$$R=\log(1+\frac{P|h_{sd}|^2}{(\kappa_d^2+\kappa_s^2)P|h_{sd}|^2+\lambda p_j|h_{jd}|^2+\sigma_d^2+\sigma}) \quad (22)$$

در این بخش، به‌منظور تحلیل و ارزیابی کارایی و عملکرد مدل سیستم پیشنهادشده، یک مسئله بهینه‌سازی را باهدف بیشینه کردن نرخ امن و در نظر گرفتن الزامات مخابره پنهان در ناظر، به‌صورت توأمان فرمول‌نویسی می‌شود. مسئله بهینه‌سازی پیشنهادی به‌صورت زیر فرمول‌بندی می‌شود:

$$\max_{P,p_j}\log\left(1+\frac{P|h_{sd}|^2}{(\kappa_d^2+\kappa_s^2)P|h_{sd}|^2+\lambda p_j|h_{jd}|^2+\sigma_d^2}\right) \quad (23)$$
$$s.t: \mathrm{C1}: 0\le P\le P^{\max}$$
$$C2: 0\le p_j\le p_j^{\max}$$
$$C3: \frac{p_j\theta_{jw}\sigma_{jw}}{p_j\theta_{jw}\sigma_{jw}-p\mu\sigma_{sw}}\ln(\frac{p\mu\sigma_{sw}}{p_j\theta_{jw}\sigma_{jw}})\le\ln(\varepsilon)$$

C1 و C2 به ترتیب نشان‌دهنده محدودیت توان ارسالی در منبع و اختلال‌گر بوده و $P^{\max}$ و $p_j^{\max}$ به ترتیب حداکثر توان موجود در گره‌های منبع و اختلال‌گر می‌باشند. همچنین C3 نیز قید الزام مخابره پنهان است. در مسئله بهینه‌سازی (23)**23** قیدهای C1 و C2 خطی هستند اما قید C3 و تابع هدف مسئله غیر محدب می‌باشند. برای حل مسئله باید به روشی قید C3 را به‌صورت محدب و تابع هدف را به‌صورت مقعر بازنویسی کرد. برای محدب نمودن قید C3 با تعریف متغیر کمکی t و استفاده از روش Epigraph مسئله (23) به‌صورت زیر بازنویسی می‌شود:

$$\max_{p,p_j,t}\log\left(1+\frac{P|h_{sd}|^2}{(\kappa_d^2+\kappa_s^2)P|h_{sd}|^2+\lambda p_j|h_{jd}|^2+\sigma_d^2}\right)$$
$$s.t: 0\le P\le P^{\max} \quad (24)$$
$$0\le p_j\le p_j^{\max}$$
$$\left(p_j\theta_{jw}\sigma_{jw}\right)\ln\left(\frac{p\mu\sigma_{sw}}{p_j\theta_{jw}\sigma_{jw}}\right)-t\ln(\varepsilon)\le 0$$
$$p_j\theta_{jw}\sigma_{jw}-p\mu\sigma_{sw}\le t$$

تمامی قیدهای مسئله (24)**24** محدب می‌باشند. در ادامه سعی می‌شود تابع هدف مسئله با استفاده از تقریب DC[1] به یک تابع مقعر تقریب زده شود. با استفاده از قوانین حاکم بر تابع لگاریتم، می‌توان تابع هدف را به‌صورت تفاضل دو تابع لگاریتمی به‌صورت زیر بازنویسی می‌شود:

$$R=\sum(p,p_j)-\Omega(p,p_j) \quad (25)$$

که $\sum(p,p_j)$ و $\Omega(p,p_j)$ به‌صورت زیر تعریف می‌شوند:

$$\sum(p,p_j)=\log\left(P|h_{sd}|^2+\left(\kappa_s^2+\kappa_d^2\right)P|h_{sd}|^2+\lambda P_j|h_{jd}|^2+\sigma_d^2\right) \quad (26)$$
$$\Omega(p,p_j)=\log\left(\left(\kappa_s^2+\kappa_d^2\right)P|h_{sd}|^2+\lambda P_j|h_{jd}|^2+\sigma_d^2\right)$$

با توجه به مقعر بودن تابع لگاریتم هر دو تابع $\sum(p,p_j)$ و $\Omega(p,p_j)$ مقعر می‌باشند. اما قرینه تابع $\Omega(p,p_j)$ یعنی $-\Omega(p,p_j)$ در رابطه R مقعر نیست، بنابراین در ادامه به‌تقریب تابع $\Omega(p,p_j)$ پرداخته می‌شود. برای تقریب این تابع از روش DC استفاده نموده و به‌صورت زیر تقریب زده می‌شود:

$$\tilde{\Omega}(p,p_j)=\Omega(p(k-1),p_j(k-1))+\nabla\Omega(p(k-1),p_j(k-1))\times\left[p(k)-p(k-1),p_j(k)-p_j(k-1)\right] \quad (27)$$

اکنون با جایگذاری تقریب تابع هدف، مسئله بهینه‌سازی به‌صورت یک مسئله محدب بازنویسی می‌شود:

$$\max_{p,p_j,t}\left(\sum(p,p_j)-\tilde{\Omega}(p,p_j)\right)$$
$$s.t: 0\le P\le P^{\max} \quad (28)$$
$$0\le p_j\le p_j^{\max}$$
$$\left(p_j\theta_{jw}\sigma_{jw}\right)\ln\left(\frac{p\mu\sigma_{sw}}{p_j\theta_{jw}\sigma_{jw}}\right)-t\ln(\varepsilon)\le 0$$
$$p_j\theta_{jw}\sigma_{jw}-p\mu\sigma_{sw}\le t$$

الگوریتم 1: الگوریتم تکراری حل مسئله بهینه‌سازی تخصص توان

1. مقداردهی اولیه: k=0 قرار بده (k شماره تکرار است) و به متغیرهای بهینه‌سازی مقدار اولیه بده $p(0)$ و $p_j(0)$
2. $p=p(k)$ و $p_j=p_j(\mathrm{k})$ قرار بده
3. (28) را حل کن و جواب را در $p(k+1)$ و $p_j(\mathrm{k+1})$ قرار بده
4. اگر دو شرط $|p(k+1)-p(k)|\le\tau$ و $|p_j(k+1)-p_j(k)|\le\tau$ برقرار باشند الگوریتم را متوقف کن و نتایج را برگردان در غیر این صورت؛
5. یک واحد به k اضافه کن (k = k + 1) و به مرحله 2 برگرد.

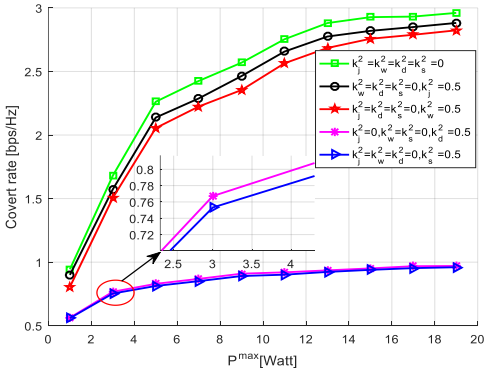
[1] Difference of two concave functions

از جعبه ابزارهای موجود از قبیل CVX برای حل مسئله بهینه‌سازی محدب (28) استفاده می‌شود. علاوه‌براین، از آنجایی‌که از روش DC استفاده‌شده است باید از یک الگوریتم تکراری استفاده نمود، این الگوریتم در الگوریتم 1 آورده شده است. این الگوریتم زمانی که شرط توقف یعنی $\left|p_j(k+1)-p_j(k)\right|\le\tau$ و $\left|p(k+1)-p(k)\right|\le\tau$ برقرار شود متوقف خواهد شد که τ آستانه توقف است.

4-نتایج شبیه‌سازی

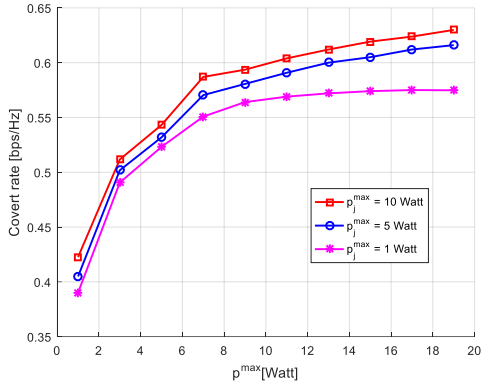
در این بخش به ارائه نتایج شبیه‌سازی مدل سیستم پیشنهادی پرداخته و آن‌ها از حیث نتایج دسته‌بندی می‌شوند. در شبیه‌سازی‌ها محل قرارگیری گره‌ها به‌صورت $L_s=(0,0)$، $L_D=(1,0)$، $L_w=(0,-1)$، $L_j=(0,-2)$ و ضمناً $\sigma_d^2=1$ است.

در شکل (2) تأثیر نقیصه سخت‌افزاری هر یک از گره‌های موجود در شبکه بر نرخ پنهان موردبررسی قرار داده می‌شود. همان‌طور که در این شکل دیده می‌شود وجود نقیصه در هر یک از گره‌های موجود در شبکه موجب کاهش نرخ پنهان می‌شود. ملاحظه می‌شود وجود نقیصه در گیرنده و فرستنده به ترتیب بیشترین تأثیر مخرب را روی نرخ پنهان دارد و این در حالی است که نقیصه در اختلال‌گر کمترین تأثیر را دارد. به‌عنوان‌مثال، وقتی مقدار نقیصه در اختلال‌گر، ناظر، گیرنده و فرستنده برابر 0.5 در نظر گرفته می‌شود، نرخ پنهان نسبت به حالتی که هیچ نقیصه‌ای در هیچ‌یک از گره‌ها وجود ندارد به ترتیب 4.2٪، 8٪، 62.2٪ و 62.8٪ کاهش می‌یابد.



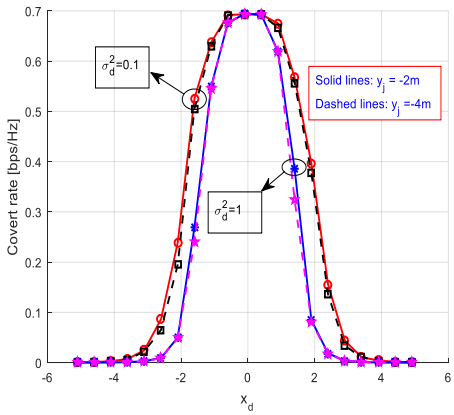
شکل (2): تأثیر نقیصه سخت‌افزاری گره‌ها بر نرخ پنهان، $p_j^{\max}=10w$.

بر این اساس، در چنین شبکه‌هایی طراحی فرستنده و گیرنده با کمترین نقیصه سخت‌افزاری نسبت به گره‌های دیگر یک امر ضروری بوده و در بهبود مخابره پنهان نقش مؤثری خواهد داشت.



شکل (3): تأثیر حداکثر توان موجود در فرستنده و اختلال‌گر، $[\kappa_s^2,\kappa_d^2,\kappa_w^2,\kappa_j^2]=[0.5,0.5,0.5,0.5]$.

شکل (3) تأثیر حداکثر توان موجود در فرستنده و اختلال‌گر را موردبررسی قرار می‌دهد. همان‌طور که در این شکل دیده می‌شود با افزایش حداکثر توان موجود برای اختلال، نرخ پنهان افزایش می‌یابد، علت این امر این است که با افزایش توان اختلال‌گر اگرچه اثر تخریبی آن برگیرنده نیز افزایش می‌یابد ولی در این حالت فرستنده نیز می‌تواند سیگنال اطلاعات خود را با توان بیشتری ارسال نماید و همچنان این سیگنال پنهان بماند؛ زیرا توان سیگنال پوششی یعنی سیگنال اختلال نیز افزایش‌یافته است. علاوه‌براین، لازم به ذکر است تأثیر افزایش حداکثر توان ارسالی موجود در فرستنده بر نرخ پنهان، به توان اختلال‌گر وابسته است. این مهم را می‌توان با تحلیل منحنی $P_j^{\max}=1$ ملاحظه نمود. همان‌طور که ملاحظه می‌شود در این منحنی، نرخ پنهان نسبت به افزایش توان فرستنده به اشباع می‌رسد که علت این امر نیز این است که وقتی سیگنال اختلال با توان پایین ارسال می‌شود فرستنده مجاز نیست توان سیگنال داده را به مقدار زیادی افزایش دهد؛ زیرا در این حالت، الزامات مخابره پنهان برآورده نخواهد شد و ناظر توانایی تشخیص مخابره را خواهد داشت.



شکل (4): تأثیر توان نویز گیرنده و موقعیت اختلال‌گر بر نرخ پنهان، $[\kappa_s^2,\kappa_d^2,\kappa_w^2,\kappa_j^2]=[0.5,0.5,0.5,0.5]$، $p_j^{\max}=10W$ و $P^{\max}=10W$.

شکل (4) نرخ پنهان را برحسب مکان گیرنده اصلی به تصویر می‌کشد. در این تحلیل محل قرارگیری گره‌ها به‌صورت $L_s=(0,0)$، $L_D=(x_d,0)$، $L_w=(0,-1)$ و $L_j=(0,y_j)$ است. همان‌طوری که در این شکل دیده می‌شود، هنگامی‌که اختلال‌گر از ناظر شبکه دور می‌شود اثر تخریبی آن روی ناظر کمتر شده که منجر به کاهش نرخ پنهان می‌شود. از طرفی دیگر، وقتی گیرنده به سمت فرستنده حرکت می‌کند، ضمن برقراری الزام مخابره پنهان، توان دریافتی در گیرنده بیشتر شده و درنتیجه نرخ پنهان افزایش می‌یابد. همچنین در این شکل، اثر نویز در گیرنده نیز موردمطالعه قرار داده‌شده است و مشاهده می‌شود که با افزایش توان نویز از 0.1 به 1 نرخ پنهان تقریباً 64% کاهش می‌یابد.

5- نتیجه‌گیری

این مقاله، به طراحی یک پروتکل مخابره پنهان با اختصاص توان به فرستنده و اختلال‌گر می‌پردازد. با توجه به اینکه تجهیزات مخابراتی از نقصیه سخت‌افزاری رنج می‌برند، می‌توان از این پدیده به‌عنوان یک پارامتر کنترلی در جهت برقراری امنیت بهره گرفت. طبق شبیه‌سازی‌های انجام‌شده، وجود نقیصه در ناظر اثر مثبتی بر بهبود امنیت داشته است، درحالی‌که این امر در گیرنده اصلی تأثیر مخربی بر نرخ پنهان دارد. نتایج شبیه‌سازی نشان داده است که نقیصه سخت‌افزاری فرستنده و گیرنده بیشترین تأثیر را بر نرخ پنهان و نقیصه سخت‌افزاری اختلال‌گر نیز کمترین تأثیر را بر نرخ پنهان دارد به صورتی که، وقتی مقدار نقیصه در اختلال‌گر، ناظر، گیرنده و فرستنده برابر 0.5 در نظر گرفته می‌شود نرخ پنهان نسبت به حالتی که هیچ نقیصه‌ای در هیچ‌یک از گره‌ها وجود ندارد به ترتیب 4.2٪، 8٪، 62.2٪ و 62.8٪ کاهش می‌یابد. با توجه به نتایج حاصله، طراحی فرستنده و گیرنده با کمترین نقیصه سخت‌افزاری نسبت به گره‌های دیگر یک امر ضروری بوده و در بهبود عملکرد مخابره پنهان نقش مؤثری خواهد داشت. برای آینده پیشنهاد می‌شود ایده تولید کلید مخفی [28] در مخابرات پنهان مورداستفاده قرار گیرد. برای توسعه می‌توان تخمین کانال را واقع‌بینانه در نظر گرفت و لذا تأثیر تخمین را در نرخ پنهان ارزیابی کرد.

10- مراجع

[1] C. E. Shannon, “Communication theory of secrecy systems,” Bell. Syst. Techn. J., vol. 28, no. 4, pp. 656–715, Oct. 1949.

[2] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. D. Renzo, “Safeguarding 5G wireless communication networks using physical layer security,” IEEE Commun. Mag., vol. 53, no. 4, pp. 20–27, Apr. 2015.

[3] A. D. Wyner, “The wire-tap channel,” Bell Syst. Techn. J., vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[4] A. Khisti and G. Wornell, “Secure transmission with multiple antennas I: The MISOME wiretap channel,” IEEE Trans. Inf. Theory, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.

[5] A. Khisti and G. W. Wornell, “Secure transmission with multiple antennas—Part II: The MIMOME wiretap channel,” IEEE Trans. Inf. Theory, vol. 56, pp. 5515–5532, Nov. 2010.

[6] T. Lv, H. Gao, and S. Yang, “Secrecy transmit beamforming for heterogeneous networks,” IEEE J. Sel. Areas Commun., vol. 33, no. 6, pp. 1154–1170, Jun. 2015.

[7] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, “Transmit antenna selection for security enhancement in MIMO wiretap channels,” IEEE Trans. Commun., vol. 61, no. 1, pp. 144–154, Jan. 2013.

[8] H. Alves, R. D. Souza, M. Debbah, and M. Bennis, “Performance of transmit antenna selection physical layer security schemes,” IEEE Signal Process. Lett., vol. 19, no. 6, pp. 372–375, Jun. 2012.

[9] H. M. Wang, F. Liu, and M. Yang, “Joint cooperative beamforming, jamming, and power allocation to secure AF relay systems,” IEEE Trans. Veh. Technol., vol. 64, no. 10, pp. 4893–4898, Oct. 2015.

[10] T. Lv, Y. Yin, Y. Lu, S. Yang, E. Liu, and G. Clapworthy, “Physical detection of misbehavior in relay systems with unreliable channel state information,” IEEE J. Sel. Areas Commun., vol. 36, no. 7, pp. 1517–1530, Jul. 2018.

[11] 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 Transactions on Information Forensics and Security, vol. 17, pp. 53-68, 2022.

[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, 2020.

[13] Z. Liu, J. Liu, Y. Zeng, and J. Ma, “Covert wireless communication in IoT network: From AWGN channel to THz band,” IEEE Internet Things J., vol. 7, pp. 3378–3388, 2020.

[14] Z. Liu, J. Liu, Y. Zeng, and J. Ma, “Covert wireless communications in IoT: Hiding information in interference,” IEEE Wireless Commun., vol. 25, pp. 46–52, 2018.

[15] H. Wang, Y. Zhang, X. Zhang, and Z. Li, “Secrecy and covert communications against UAV surveillance via multi-hop networks,” IEEE Trans. Commun., vol. 68, no. 1, pp. 389–401, Jan. 2020.

[16] X. Zhou, S. Yan, J. Hu, J. Sun, J. Li, and F. Shu, “Joint optimization of a UAV’s trajectory and transmit

power for covert communications," IEEE Trans. Signal Process., vol. 67, no. 16, pp. 4276–4290, Aug. 2019.

[17] J. Wang, W. Tang, Q. Zhu, X. Li, H. Rao, and S. Li, "Covert communication with the help of relay and channel uncertainty," IEEE Wireless Commun. Lett., vol. 8, no. 1, pp. 317–320, Feb. 2019.

[18] M. Forouzesh, P. Azmi, A. Kuhestani, and P. L. Yeoh, "Covert communication and secure transmission over untrusted relaying networks in the presence of multiple wardens," IEEE Trans. Commun., vol. 68, no. 6, pp. 3737–3749, Jun. 2020.

[19] C. Studer, M. Wenk, and A. Burg, "MIMO transmission with residual transmit-RF impairments," Smart Antennas (WSA), 2010 International ITG Workshop, pp. 189–196, IEEE, 2010.

[20] V. Shahiri, A. Kuhestani and L. Hanzo, "Short-Packet Amplify-and-Forward Relaying for the Internet-of-Things in the Face of Imperfect Channel Estimation and Hardware Impairments," IEEE Transactions on Green Communications and Networking, vol. 6, no. 1, pp. 20-36, March 2022.

[21] M. Ragheb, A. Kuhestani, M. Kazemi, H. Ahmadi and L. Hanzo, "RIS-Aided Secure Millimeter-Wave Communication Under RF-Chain Impairments," IEEE Transactions on Vehicular Technology, vol. 73, no. 1, pp. 952-963, Jan. 2024.

[22] A. Boulogeorgos, D. Karas, and G. Karagiannidis, "How much does I/Q imbalance affect secrecy capacity?" IEEE Communications Letters, 20(7):1305–1308, 2016.

[23] J. Zhu, R. Schober, and V. Bhargava, "PLS for massive MIMO systems impaired by phase noise," 17th International Workshop in Signal Processing Advances in Wireless Communications (SPAWC), 2016 IEEE, pp. 1–5. 2016.

[24] W. Zhang and L. Yang, "Covert transmission of RIS-aided communication networks in the presence of imperfect CSI and hardware impairments," 2023 IEEE/CIC International Conference on Communications in China, pp. 1-5, 2024.

[25] M. Baratian, H. Zayyani and A. Kuhestani, "PLS with the aid of compressive sensing in the presence of non-ideal relays by removing the effect of HWIs by providing an iterative method," Journal of Electronic & Cyber Defense,vol. 11, no. 4, pp. 75-82, Mar. 2024. (In Persian).https://dor.isc.ac/dor/20.1001.1.23224347.1402.11.4.6.3

[26] V. Shahiri, M. Forouzesh, H. Behroozi, A. Kuhestani and K. -K. Wong, "Deep learning aided secure transmission in wirelessly powered untrusted relaying in the face of hardware impairments," IEEE Open Journal of the Communications Society, vol. 5, pp. 2196-2210, May 2024.

[27] Z. Ezzati, A. Mohammadi, V. Pourahmadi, and A. Kuhestani, "A machine learning multi-hop physical layer authentication with hardware impairments," vol. 30, pp. 1453–1464, 2024.

[28] A. H. Khalili Tirandaz, "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, vol. 10, no. 2, pp. 19-32, Mar. 2022. (In Persian).https://dor.isc.ac/dor/20.1001.1.23224347.1401.10.2.3.9