Electronical & Cyber Defence
Vol. 13, No. 1, Spring 2025, Serial No. 49

Robust Physical Layer Security Using Frequency Diverse Array Directional Modulation

M.Tayeb Masoud , H. Khaleghi Bizaki *
* Professor, Malek Ashtar University of Technology , Tehran, Iran.
Received:2024 /12/17, Revised: 2025/02/13, Accepted: 2025/03/13, Published: 2025/04/21

DOR: https://dor.isc.ac/dor/20.1001.1.23224347.1404.13.1.6.1

ABSTRACT

In parallel with the rapid development of modern wireless communication technologies, the security and reliability of these systems have always been a major challenge in their design. Physical layer security is an effective solution for ensuring security in telecommunications systems, and it has gained significant attention in recent years. In physical layer security based on frequency diverse array directional modulation, the beam of the transmitted signal depends on both angle and distance. The modulation constellation can only be properly received within a small range around the legitimate receiver and is intentionally degraded in other directions. Although this method is effective when accurate information about the location of the legitimate receiver is available, but it suffers from secrecy performance degradation in the presence of positioning estimation errors, which are highly probable in cellular wireless networks. This paper proposes a novel solution to mitigate the impact of location estimation errors to improve the performance of physical layer security by enhancing the secrecy rate of the system. Numerical simulations demonstrate the desirable performance of this method in the robustness of the secrecy rate degradation against positioning estimation errors in the legitimate receiver.

Keywords: Physical Layer Security, Random frequency Diverse Array, Directional Modulation, Position Estimation Error, Secrecy Rate.

❖ Corresponding Author Email: bizaki@yahoo.com

"پدافند الکترونیکی و سایبری"
سال سیزدهم، شماره ۱، بهار۱۴۰۴، ص۸۲-۷۳
شاپا الکترونیکی: ۸۹۷۹-۲۹۸۰ شاپا چاپی: ۴۳۴۷-۲۳۲۲

علمی-پژوهشی

مقاوم‌سازی مدولاسیون جهتی مبتنی بر آرایه چندگانگی فرکانسی در برابر خطای تخمین موقعیت

مهدی طیب مسعود [۱]، حسین خالقی بیزکی [۲]

۱- دانشجوی دکتری، ۲- استاد، دانشگاه صنعتی مالک اشتر، تهران، ایران.

(دریافت: ۱۴۰۳/۰۹/۲۷، بازنگری: ۱۴۰۳/۱۱/۲۵، پذیرش: ۱۴۰۳/۱۲/۲۳، انتشار: ۱۴۰۳/۰۲/۰۱)

DOR: https://dor.isc.ac/dor/20.1001.1.23224347.1404.13.1.6.1

چکیده

همزمان با توسعه روزافزون فناوری ارتباطی بی‌سیم مدرن، امنیت و قابلیت اطمینان این سیستم‌ها همواره یکی از چالش‌های پیشروی طراحی آن بوده است. امنیت لایه فیزیکی یک راهکار کارآمد برای تأمین امنیت انتشار در سیستم‌های مخابراتی است که در سال‌های اخیر توجه بسیاری را به خود جلب کرده است. در امنیت لایه فیزیکی مبتنی بر مدولاسیون جهتی چندگانگی فرکانسی، پرتو سیگنال ارسالی به دو بعد زاویه و فاصله وابسته است به‌گونه‌ای که منظومه مدولاسیون صرفاً در محدوده کوچکی در اطراف گیرنده قانونی به‌درستی قابل دریافت بوده و در سایر جهات به‌عمد تخریب می‌شود. اگرچه کار آیی این روش زمانی که موقعیت گیرنده قانونی به‌درستی تعیین گردد، قابل‌قبول است؛ اما با بروز خطای تخمین موقعیت که امری محتمل در شبکه‌های بی‌سیم سیار است، عملکرد محرمانگی سیستم به‌شدت افت پیدا می‌کند. برای غلبه بر این مشکل، در این مقاله یک راهکار مقاوم‌سازی در برابر خطای تخمین موقعیت ارائه می‌شود به‌گونه‌ای که با بیشینه کردن نرخ محرمانگی ارگادیک سیستم و تخصیص بهینه توان، منجر به بهبود عملکرد امنیت لایه فیزیکی می‌شود. شبیه‌سازی‌های عددی مبین عملکرد مطلوب این روش در مقاوم‌سازی نرخ محرمانگی در برابر خطای تخمین موقعیت گیرنده قانونی است؛ به‌گونه‌ای که نرخ محرمانگی تا یک بیت بر ثانیه بر هرتز در مقایسه با روش غیرمقاوم بهبود می‌یابد.

کلیدواژه‌ها: امنیت لایه فیزیکی، آرایه چندگانگی فرکانسی تصادفی، مدولاسیون جهتی، خطای تخمین موقعیت، نرخ محرمانگی.

۱- مقدمه

در مقایسه با ارتباطات سیمی، فناوری‌های ارتباطی بی‌سیم به دلیل ویژگی‌های مؤثر خود مانند انعطاف‌پذیری، قابلیت توسعه و هزینه پایین، پیشرفت‌های زیادی را با خود به همراه داشته‌اند. بااین‌حال، ماهیت همه‌پخشی ارتباطات بی‌سیم باعث آسیب‌پذیری در برابر آشکارسازی‌های غیرمجاز می‌شود؛ بنابراین، چالش امنیت انتشار بی‌سیم در لایه فیزیکی، توجهات قابل‌تأملی را در سال‌های اخیر به خود جلب کرده است [۱-۴].

مدولاسیون جهتی به‌عنوان یک فناوری جدید در امنیت لایه فیزیکی ارتباطات بی‌سیم، امکان حفظ الگوی سیگنال در جهت ارتباط امن از پیش تعیین‌شده را فراهم می‌کند؛ درحالی‌که منظومه سیگنال ارسالی در سایر جهت‌ها تخریب می‌شود؛ بنابراین، احتمال شنود پایین و احتمال شناسایی پایین را می‌تواند برای انتقال امن بی‌سیم فراهم آورد. در [۵, ۶] بر اساس مدولاسیون مستقیم آنتن در میدان نزدیک، یک ساختار آنالوگ پیشنهاد شده است که امکان جلوگیری از تمایز سیگنال توسط شنودگر را فراهم می‌کند. برای سناریوی میدان دور، یک طرح مدولاسیون مشابه با تنظیم بهینه انحراف فاز هر المان در [۷, ۸] پیشنهاد شده است؛ به‌گونه‌ای که در جهت تعیین‌شده، منظومه سیگنال به‌صورت کامل قابل‌استخراج بوده و در سایر جهت‌ها به‌طور عمدی تخریب شود. بااین‌حال، این طرح‌های ترکیبی نیازمند سوئیچ‌های فرکانس رادیویی سریع و یا تغییردهنده‌های فاز با سرعت سوئیچینگ در نرخ مدولاسیون هستند که محدودیت‌هایی را در تحقق و کاربرد آن‌ها ایجاد می‌کند.

نویسنده مسئول: Bizaki@yahoo.com

در [۹, ۱۰] نویسندگان روش‌های تحلیلی جدیدی بر اساس ترکیب سیگنال تحریک و بردارهای نویز مصنوعی پیشنهاد کرده‌اند که به‌صورت دیجیتال در باند پایه قابل تحقق هستند. به‌طورکلی، باید توجه داشت که مدولاسیون جهتی ترکیبی با نویز مصنوعی، می‌تواند نسبت سیگنال به نویز را در مکان کاربر مجاز تضمین کرده و در سایر نقاط به‌صورت خودخواسته تخریب کند. اما تمامی این روش‌های ذکر شده، بر پایه تغییر شیفت فاز (آرایه فازی) استوار هستند. درنتیجه، هنگامی‌که گیرنده قانونی و شنودگرها در یک جهت یکسان قرار گرفته باشند، امنیت انتقال در لایه فیزیکی به‌صورت کامل تضمین نمی‌شود؛ بنابراین، منطقی است که سایر طرح‌هایی که امکان برقراری ارتباطات بی‌سیم امن در دو بعد فاصله-زاویه را فراهم می‌کنند، موردبررسی قرار گیرند.

[۱۱] به‌عنوان یک روش پیشرو، آرایه چندگانگی فرکانسی[1] (*FDA*) فرصت‌های جدیدی را برای ارتباطات بی‌سیم امن فراهم می‌کند و اخیراً توجه فراوانی را به خود جلب کرده است. اگرچه *FDA* می‌تواند به‌عنوان یک تکنیک ویژه آرایه فازی در نظر گرفته شود، اما تفاوت‌هایی بین آن‌ها وجود دارد. در واقع، تفاوت اساسی بین آرایه فازی و *FDA* در این است که در *FDA*، افزایش‌های کوچکی در فرکانس تحریک المان‌های آرایه وجود دارند [۱۲] درحالی‌که المان‌های آرایه فازی همگی از یک فرکانس کاری استفاده می‌کنند. به همین دلیل، الگوی پرتو آرایه فازی تنها به زاویه وابسته است، درحالی‌که الگوی پرتو *FDA* به دو پارامتر زاویه و فاصله وابسته است [۱۳-۱۵]. به دلیل این خاصیت، *FDA* پتانسیل‌های بالقوه‌ای در کاربردهای راداری [۱۶-۱۸]، حسگری [۱۹] و سیستم‌های ارتباطی بی‌سیم [۲۰] پیدا کرده است. بااین‌حال، برهم‌نهی زاویه و فاصله در الگوی پرتوی *FDA*، ظرفیت آن را در برخی از کاربردهای خاص محدود کرده است.

برای حل این مشکل، چندین رویکرد مبتنی بر افزایش غیرخطی فرکانس آرایه‌های *FDA* برای جداسازی الگوی پرتو فاصله-زاویه پیشنهاد شده است [۲۱-۲۴]. در [۲۱] ، یک طرح افزایش غیرخطی لگاریتمی ارائه‌شده است، اما عملکرد بعد فاصله در آن قابل‌قبول نیست. در [۲۲] افزایش‌های مربعی و مکعبی فرکانس پیشنهاد شده است که در هر دو حالت جداسازی پرتو فرستنده و تعیین موقعیت هدف بهتر عمل می‌کند. علاوه بر این، با اختصاص یک فرکانس اتصال تصادفی به هر آرایه *FDA*، نویسندگان در [۲۳, ۲۵] یک آرایه چندگانگی فرکانسی تصادفی (*RFDA*) پیشنهاد کرده‌اند به‌گونه‌ای که همبستگی زاویه-فاصله را می‌توان در آشکارسازی، به‌طور مؤثر تضعیف کرد.

در تمامی روش‌های فوق فرض شده است که فرستنده اطلاعات کاملی از موقعیت گیرنده قانونی دارد. در یک نگاه کلی، عملکرد محرمانگی مدولاسیون جهتی به میزان قابل‌توجهی به اطلاعات فرستنده از موقعیت گیرنده وابسته است. به‌خصوص در روش‌های با پیچیدگی بیشتر، مانند *FDA* که در آن دریافت صحیح سیگنال ارسالی، به محدوده کوچکی در اطراف گیرنده قانونی خلاصه می‌شود [۲۶]؛ اما در عمل در شبکه‌های بی‌سیم سیار که در آن ممکن است موقعیت گیرنده در هرلحظه تغییر کند، تخمین اطلاعات موقعیتی با خطا همراه خواهد بود. برای افزایش مقاومت در برابر خطای اندازه‌گیری در [۲۷] یک الگوریتم ترکیبی مقاوم چندپرتوی مدولاسیون جهتی بدون در اختیار داشتن اطلاعات کامل از موقعیت شنودگر برای آرایه فازی ارائه شده است. در [۲۸] نیز این راهکار مقاوم برای سناریوی *MU-MIMO* تعمیم‌یافته است. برای بیشینه‌سازی نرخ محرمانگی سیستم‌های مدولاسیون جهتی به کمک نویز مصنوعی، در [۲۹] دو روش بهینه‌سازی مقاوم ارائه شده است: راهکار شکل‌دهی پرتو مبتنی بر توان تکرارشونده و راهکار تخصیص توان مبتنی بر نرخ محرمانگی. علاوه بر این در [۳۰] یک راهکار مدولاسیون جهتی مقاوم و امن برای شبکه‌های رله پیشنهاد شده است.

در پژوهش‌های فوق صرفاً مقاوم‌سازی مدولاسیون جهتی مبتنی بر آرایه فازی که پیچیدگی کمتری دارد، مورد توجه قرار گرفته است. لذا باتوجه‌به اهمیت موضوع خطای تخمین موقعیت گیرنده (شامل زاویه و فاصله از فرستنده) در *FDA* و تأثیر غیرقابل‌چشم‌پوشی آن در عملکرد امنیت لایه فیزیکی مبتنی بر مدولاسیون جهتی آرایه چندگانگی فرکانسی، در این مقاله به بررسی تأثیر این خطا و مقاوم‌سازی سیستم در برابر بروز این خطا می‌پردازیم. هدف این مقاله ارائه یک راهکار مقاوم در برابر این خطای تخمین است که درنتیجه آن عملکرد محرمانگی سیستم بهبود می‌یابد. با توجه به اینکه توزیع خطای تخمین و آمارگان آن برای فرستنده معلوم است، در این مقاله با لحاظ کردن اثر این خطای تخمین بر نرخ محرمانگی ارگادیک، یک راهکار مقاوم برای تخصیص بهینه توان برای بیشینه کردن نرخ محرمانگی ارگادیک ارائه شده است.

۲- مدل سیستم

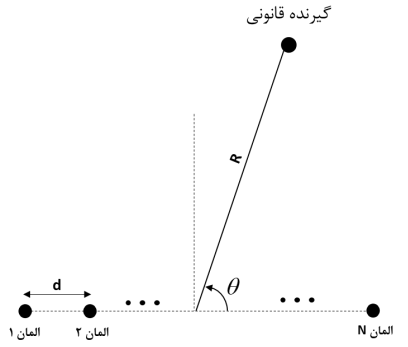
یک آرایه چندگانگی فرکانسی تصادفی، شکل (۱) نشان داده شده است. فرض بر این است که عناصر آرایه به‌صورت خطی و با فاصله یکنواخت از یکدیگر قرارگرفته و مرجع فاز، مرکز آرایه در نظر گرفته می‌شود. مطابق تعریف، در آرایه چندگانگی فرکانسی، فرکانس تحریک هر یک از المان‌های آرایه به میزان کوچکی نسبت به فرکانس حامل، افزایش می‌یابند. فرکانس تخصیص داده شده به عنصر n-ام به‌صورت رابطه زیر است [۲۹]:

$$f_n = f_c + k_n \Delta f, \qquad n = 0,1,...,N-1 \qquad (۱)$$

که در آن f_c فرکانس مرکزی حامل و Δf اندازه شیفت فرکانسی هر المان را نشان می‌دهد. در آرایه چندگانگی فرکانسی

[1] *Frequency Diverse Array*

تصادفی، این شیفت فاز به‌صورت تصادفی انجام می‌شود؛ لذا متغیر k_n یک متغیر تصادفی مستقل با توزیع یکسان *(i.i.d)* است که به‌صورت یک بردار تصادفی $\mathbf{k}=[k_0,k_1,...,k_{N-1}]$ نمایش داده می‌شود. توزیع k_n یک قاعده مشخص برای تخصیص فرکانس حامل به عناصر مختلف آرایه را مشخص می‌کند.

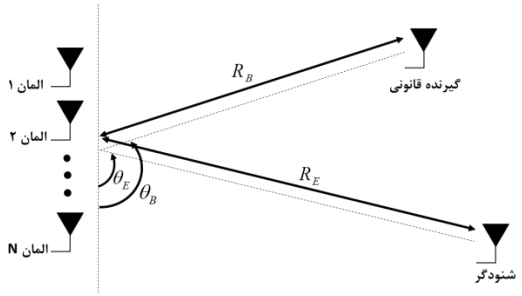


شکل (۱): ساختار آرایه چندگانگی فرکانسی تصادفی

برای یک گیرنده قانونی در موقعیت مشخص (θ,R)، بردار هدایت نرمالیزه[1] شده را می‌توان به‌صورت زیر بیان نمود:

$$\boldsymbol{h}(\theta,R)=\frac{1}{\sqrt{N}}\left[e^{j\Psi_0(\theta,R)},e^{j\Psi_1(\theta,R)},...,e^{j\Psi_{N-1}(\theta,R)}\right]^T \quad (۲)$$

که در آن $\Psi_n(\theta,R)$ اختلاف فاز المان n -ام نسبت به المان مرجع است. ازآنجاکه مدولاسیون جهتی یک فناوری سمت فرستنده است، سیستم نشان داده شده در شکل (۱) به‌صورت یک کانال *MISO* در نظر گرفته می‌شود. مطابق شکل (۲)، در این مدل، فرستنده (آلیس) مجهز به N آنتن بوده و گیرنده قانونی (باب) و شنودگر دارای یک آنتن هستند. فرض می‌شود که موقعیت گیرنده قانونی، (θ_B,R_B)، به‌طور دقیق برای فرستنده معلوم بوده درحالی‌که موقعیت شنودگر، (θ_E,R_E)، برای فرستنده نامعلوم است. همچنین مدل کانال به‌صورت دیدمستقیم و افت فضای آزاد فرض می‌شود.



شکل (۲): مدل *MISO* مدولاسیون جهتی مبتنی بر آرایه چندگانگی فرکانسی تصادفی

به‌منظور افزایش امنیت سیستم در زمانی که شنودگر در موقعیت نزدیک به گیرنده قانونی قرار دارد از نویز مصنوعی استفاده می‌شود. در این صورت سیگنال ارسالی ترکیبی از سیگنال اطلاعات و نویز مصنوعی به‌صورت زیر خواهد بود [۲۹]:

$$s=\sqrt{\alpha P_t}\,\mathbf{v}x+\sqrt{(1-\alpha)P_t}\,\mathbf{w} \quad (۳)$$

که در آن x یک سمبل مختلط انتخابی از منظومه سیگنال، P_t توان فرستنده و α ضریب تخصیص توان بین سیگنال اطلاعات و نویز مصنوعی است. همچنین، $\mathbf{v}$ بردار شکل‌دهی پرتو برای سیگنال اطلاعات و $\mathbf{w}$ برابر با بردار نویز مصنوعی است. ازآنجاکه فرستنده دانشی در مورد موقعیت شنودگر ندارد، به‌منظور بیشینه شدن نسبت سیگنال به نویز و اختلال در گیرنده قانونی، لازم است تا بردار نویز مصنوعی بر بردار کانال گیرنده قانونی متعامد باشد، یعنی [۲۹]:

$$\mathbf{v}=\mathbf{h}(\theta_B,R_B) \quad (۴)$$

که در آن $\mathbf{h}(\theta_B,R_B)$ بردار هدایت آرایه چندگانگی فرکانسی تصادفی در فرستنده به سمت گیرنده قانونی بوده که با جایگزینی (θ,R) با (θ_B,R_B) در رابطه (۲) به دست می‌آید. علاوه بر آن، بردار نویز مصنوعی $\mathbf{w}$ در رابطه (۳)، باید در فضای پوچ بردار $\mathbf{h}(\theta_B,R_B)$ قرار داشته باشد، یعنی $\mathbf{h}^H(\theta_B,R_B)\mathbf{w}=0$، تا از تداخل با گیرنده قانونی اجتناب شود. تحت این شرایط، بردار $\mathbf{w}$ را می‌توان به‌صورت زیر نمایش داد [۳۱]:

$$\begin{aligned}\mathbf{w}&=\frac{\left(\mathbf{I}_N-\mathbf{h}(\theta_B,R_B)\mathbf{h}^H(\theta_B,R_B)\right)\mathbf{z}}{\left\|\left(\mathbf{I}_N-\mathbf{h}(\theta_B,R_B)\mathbf{h}^H(\theta_B,R_B)\right)\mathbf{z}\right\|}\\&=\frac{\left(\mathbf{P}(\theta_B,R_B)\right)\mathbf{z}}{\left\|\mathbf{P}(\theta_B,R_B)\mathbf{z}\right\|}\end{aligned} \quad (۵)$$

که در آن $\mathbf{z}$ یک بردار متشکل از N متغیر تصادفی گوسی مختلط مستقل با توزیع یکسان و متقارن چرخشی با متوسط صفر و واریانس واحد، به‌صورت $\mathbf{z}\sim \mathrm{CN}(0,\mathbf{I}_N)$، است.

با توجه به رابطه (۳)، سیگنال دریافتی در گیرنده قانونی برابر است با:

$$\begin{aligned}y(\theta_B,R_B)&=\mathbf{h}^H(\theta_B,R_B)\mathbf{s}+n_B\\&=\sqrt{\alpha P_t}\,\mathbf{h}^H(\theta_B,R_B)\mathbf{v}x+n_B\\&=\sqrt{\alpha P_t}\,x+n_B\end{aligned} \quad (۶)$$

که در آن n_B نویز گوسی سفید جمع شونده با توزیع $n_B\sim CN\left(0,\sigma_B^2\right)$ است. با توجه به رابطه (۶)، نسبت سیگنال به نویز و اختلال در گیرنده قانونی برابر خواهد بود با:

$$SINR_B=\gamma_B=\frac{\alpha P_t}{\sigma_B^2}=\alpha\mu_B \quad (۷)$$

که در آن $\mu_B=P_t/\sigma_B^2$.

در مقابل، سیگنال دریافتی در شنودگر را می‌توان به‌صورت زیر نمایش داد:

[1] Normalized Steering Vector

$$y(\theta_E,R_E)=\mathbf{h}^H(\theta_E,R_E)\mathbf{s}+n_E$$
$$=\sqrt{\alpha P_t}\mathbf{h}^H(\theta_E,R_E)\mathbf{h}(\theta_B,R_B)x \quad (۸)$$
$$+\sqrt{(1-\alpha)P_t}\mathbf{h}^H(\theta_E,R_E)\mathbf{w}+n_E$$

که در آن n_E نویز گوسی سفید جمع شونده با توزیع $n_E\sim CN\left(0,\sigma_E^2\right)$ بوده و $\mathbf{h}(\theta_E,R_E)$ بردار هدایت آرایه چندگانگی فرکانسی تصادفی فرستنده به شنودگر است که با جایگذاری (θ_E,R_E) بجای (θ,R) در رابطه (۲) حاصل شده است.

مطابق رابطه (۸)، عبارت $\sqrt{P_t}\mathbf{h}^H(\theta_E,R_E)\mathbf{h}(\theta_B,R_B)$، دامنه و فاز سیگنال در شنودگر را تخریب می‌کند. علاوه بر آن، عبارت $\mathbf{h}^H(\theta_E,R_E)\mathbf{w}$ به دلیل عدم تعامد بین $\mathbf{h}^H(\theta_E,R_E)$ و $\mathbf{w}$، صفر نخواهد بود. لذا این عبارت نیز باعث تخریب منظومه سیگنال در شنودگر می‌شود. با توجه به رابطه (۸)، نسبت سیگنال به نویز و اختلال در شنودگر برابر خواهد بود با:

$$SINR_E=\gamma_E=\frac{\alpha P_t\left|\mathbf{h}^H(\theta_E,R_E)\mathbf{h}(\theta_B,R_B)\right|^2}{(1-\alpha)P_t\left|\mathbf{h}^H(\theta_E,R_E)\mathbf{w}\right|^2+\sigma_E^2}$$
$$=\frac{\alpha\mu_B\left|\mathbf{h}^H(\theta_E,R_E)\mathbf{h}(\theta_B,R_B)\right|^2}{(1-\alpha)\mu_B\left|\mathbf{h}^H(\theta_E,R_E)\mathbf{w}\right|^2+\beta} \quad (۹)$$

که در آن $\beta\triangleq\sigma_E^2/\sigma_B^2$.

نرخ محرمانگی را به‌صورت زیر تعریف می‌کنیم [۳۲]:

$$R_S=R_B-R_E \quad (۱۰)$$

که در آن R_B و R_E به ترتیب نرخ‌های مربوط به کانال فرستنده به گیرنده قانونی و فرستنده به شنودگر است. با جایگذاری روابط (۷) و (۹) در رابطه (۱۰) خواهیم داشت:

$$R_S=R_B-R_E$$
$$=\log_2(1+SINR_B)-\log_2(1+SINR_E)$$
$$=\log_2\left(1+\frac{\alpha P_t}{\sigma_B^2}\right)$$
$$-\log_2\left(1+\frac{\alpha P_t\left|\mathbf{h}^H(\theta_E,R_E)\mathbf{h}(\theta_B,R_B)\right|^2}{(1-\alpha)\left|\mathbf{h}^H(\theta_E,R_E)\mathbf{w}\right|^2+\frac{\sigma_E^2}{\sigma_B^2}}\right) \quad (۱۱)$$

۳- مقاوم‌سازی در برابر خطای تخمین موقعیت در روش پیشنهادی

زاویه و فاصله تخمین زده‌شده توسط الگوریتم‌های موقعیت‌یابی، به ترتیب با $\hat{\theta}_B$ و $\hat{R}_B$ نمایش داده می‌شود. به دلیل ماهیت شبکه‌های بی‌سیم سیار، این تخمین در اکثر مواقع با خطا همراه خواهد بود. اگر خطای تخمین متناظر با زاویه و فاصله، به ترتیب با $\Delta\theta_B$ و ΔR_B نمایش داده شود، زاویه و فاصله تخمین زده شده را می‌توان به‌صورت $\hat{\theta}_B=\theta_B+\Delta\theta_B$ و $\hat{R}_B=R_B+\Delta R_B$ نشان داد [۳۳, ۳۴]. بر همین اساس می‌توان نوشت:

$$\mathbf{h}_B(\theta,R)=\hat{\mathbf{h}}_B(\theta,R)+\Delta\mathbf{h}_B(\theta,R)$$
$$\triangleq\hat{\mathbf{h}}_B+\Delta\mathbf{h}_B \quad (۱۲)$$

نرخ ارگادیک که نشان‌دهنده میانگین نرخ قابل‌دستیابی است، یک معیار اساسی پرکاربرد برای ارزیابی عملکرد امنیت لایه فیزیکی است. نرخ محرمانگی ارگادیک به‌صورت زیر تعریف می‌شود.

$$R_{S,E}=E\{R_S\} \quad (۱۳)$$

که در آن $E\{\ \}$ نمایانگر امید ریاضی است.

با توجه به ماهیت تصادفی $\Delta\theta_B$ و ΔR_B، پارامترهای $\hat{\theta}_B$ و $\hat{R}_B$ را می‌توان دو متغیر تصادفی مستقل از یکدیگر در نظر گرفت. فرض می‌شود که $\Delta\theta_B$ و ΔR_B به ترتیب دارای توزیع $\Delta\theta_B\sim CN\left(0,\sigma_{\Delta\theta_B}^2\right)$ و $\Delta R_B\sim CN\left(0,\sigma_{\Delta R_B}^2\right)$ باشند. با توجه به رابطه (۱۱) و استفاده از نامساوی جنسن [۳۵] یعنی $E\{\log_2 x\}\le\log_2 E\{x\}$، می‌توان نوشت:

$$R_{S,E}=\underset{\Delta h_B}{E}\{R_S\}$$
$$=\underset{\Delta h_B}{E}\left\{\log_2\left(1+\frac{\alpha P_t}{\sigma_B^2}\right)-\log_2\left(1+\frac{\alpha P_t\left|\mathbf{h}_E^H\mathbf{h}_B\right|^2}{(1-\alpha)\left|\mathbf{h}_E^H\mathbf{w}\right|^2+\frac{\sigma_E^2}{\sigma_B^2}}\right)\right\} \quad (۱۴)$$
$$\ge\log_2\left(1+\frac{\alpha P_t}{\sigma_B^2}\right)-\log_2\left(1+\frac{\alpha P_t\ \underset{\Delta h_B}{E}\left\{\left|\mathbf{h}_E^H\mathbf{h}_B\right|^2\right\}}{(1-\alpha)\left|\mathbf{h}_E^H\mathbf{w}\right|^2+\frac{\sigma_E^2}{\sigma_B^2}}\right)$$

ذر ادامه، کران پایین رابطه (۱۴)، به عنوان بدترین حالت نرخ محرمانگی، مورد استفاده قرار می‌گیرد.

$$R_{S,E}^{LB}=\log_2\left(1+\frac{\alpha P_t}{\sigma_B^2}\right)-\log_2\left(1+\frac{\alpha P_t\ \underset{\Delta h_B}{E}\left\{\left|\mathbf{h}_E^H\mathbf{h}_B\right|^2\right\}}{(1-\alpha)\left|\mathbf{h}_E^H\mathbf{w}\right|^2+\frac{\sigma_E^2}{\sigma_B^2}}\right) \quad (۱۵)$$

از رابطه (۱۵)، عبارت $\underset{\Delta h_B}{E}\left\{\left|\mathbf{h}_E^H\mathbf{h}_B\right|^2\right\}$ را می‌توان به‌صورت زیر محاسبه کرد:

$$\begin{aligned}\underset{\Delta h_B}{E}\left\{\left|\mathbf{h}_E^H\mathbf{h}_B\right|^2\right\} &= \underset{\Delta h_B}{E}\left\{\left|\mathbf{h}_E^H\left(\hat{\mathbf{h}}_B+\Delta\mathbf{h}_B\right)\right|^2\right\}\\ &= \underset{\Delta h_B}{E}\left\{\mathbf{h}_E^H\left(\hat{\mathbf{h}}_B+\Delta\mathbf{h}_B\right)\left(\hat{\mathbf{h}}_B+\Delta\mathbf{h}_B\right)^H\mathbf{h}_E^H\right\}\\ &= \underset{\Delta h_B}{E}\left\{\mathbf{h}_E^H\hat{\mathbf{h}}_B\hat{\mathbf{h}}_B^H\mathbf{h}_E+\mathbf{h}_E^H\hat{\mathbf{h}}_B\Delta\mathbf{h}_B^H\mathbf{h}_E\right.\\ &\quad\left.+\mathbf{h}_E^H\Delta\mathbf{h}_B\hat{\mathbf{h}}_B^H\mathbf{h}_E+\mathbf{h}_E^H\Delta\mathbf{h}_B\Delta\mathbf{h}_B^H\mathbf{h}_E\right\}\\ &= \mathbf{h}_E^H\hat{\mathbf{h}}_B\hat{\mathbf{h}}_B^H\mathbf{h}_E+\mathbf{h}_E^H\underset{\Delta h_B}{E}\left\{\Delta\mathbf{h}_B\Delta\mathbf{h}_B^H\right\}\mathbf{h}_E\\ &= \mathbf{h}_E^H\hat{\mathbf{h}}_B\hat{\mathbf{h}}_B^H\mathbf{h}_E+\mathbf{h}_E^H R\left(\Delta\mathbf{h}_B\right)\mathbf{h}_E\end{aligned} \quad (۱۶)$$

که در آن ماتریس همبستگی $R\left(\Delta\mathbf{h}_B\right)$ به‌صورت $R\left(\Delta\mathbf{h}_B\right)=\underset{\Delta\mathbf{h}_B}{E}\left\{\Delta\mathbf{h}_B\Delta\mathbf{h}_B^H\right\}=R_{\Delta\mathbf{h}_B}$ تعریف می‌شود به‌طوری‌که با توجه به رابطه (۲) داریم:

$$\begin{aligned}R_{\Delta\mathbf{h}_B}(p,q) &= E\left\{\frac{1}{N}e^{j\frac{2\pi}{\lambda}(p-q)d\cos\Delta\theta+\left(k_p-k_q\right)\Delta f\,\Delta R}\right\}\\ &= \int_{-\Delta R_{\max}}^{\Delta R_{\max}}\int_{-\Delta\theta_{\max}}^{\Delta\theta_{\max}}\frac{1}{N}e^{j\frac{2\pi}{\lambda}(p-q)d\cos\Delta\theta+\left(k_p-k_q\right)\Delta f\,\Delta R}\\ &\quad\times g\left(\Delta\theta\right)f\left(\Delta R\right)d\Delta\theta d\Delta R\end{aligned} \quad (۱۷)$$

که در آن $f\left(\Delta\theta\right)$ و $g\left(\Delta R\right)$ به ترتیب توابع چگالی احتمال $\Delta\theta_B$ و ΔR_B است. با فرض استقلال $\Delta\theta_B$ و ΔR_B از یکدیگر، رابطه (۱۷) را می‌توان به‌صورت دو انتگرال مستقل محاسبه کرد. لذا داریم:

$$\begin{aligned}R_{\Delta\mathbf{h}_B,\theta}(p,q) &= \frac{2}{N\sqrt{2\pi}\sigma_{\Delta\theta}}\int_0^{\Delta\theta_{\max}}e^{j\frac{2\pi}{\lambda}(p-q)d\cos\Delta\theta}e^{-\frac{(\Delta\theta)^2}{2\sigma_{\Delta\theta}^2}}d\Delta\theta\\ &= \frac{2}{N\sqrt{2\pi}\sigma_{\Delta\theta}}\int_0^{\Delta\theta_{\max}}e^{j\frac{2\pi}{\lambda}(p-q)d\left(1-\frac{(\Delta\theta)^2}{2}\right)}e^{-\frac{(\Delta\theta)^2}{2\sigma_{\Delta\theta}^2}}d\Delta\theta\\ &= \frac{2e^{j\frac{2\pi}{\lambda}(p-q)d}}{N\sqrt{2\pi}\sigma_{\Delta\theta}}\int_0^{\Delta\theta_{\max}}e^{\frac{-j\pi(p-q)d(\Delta\theta)^2}{\lambda}}e^{-\frac{(\Delta\theta)^2}{2\sigma_{\Delta\theta}^2}}d\Delta\theta\\ &= \frac{2e^{j\frac{2\pi}{\lambda}(p-q)d}}{N\sqrt{2\pi}\sigma_{\Delta\theta}}\int_0^{\Delta\theta_{\max}}e^{\frac{-j2\pi(p-q)d\sigma_{\Delta\theta}^2(\Delta\theta)^2-\lambda(\Delta\theta)^2}{2\lambda\sigma_{\Delta\theta}^2}}d\Delta\theta\\ &= \frac{2e^{j\frac{2\pi}{\lambda}(p-q)d}}{N\sqrt{2\pi}\sigma_{\Delta\theta}}\int_0^{\Delta\theta_{\max}}e^{\frac{j2\pi(p-q)d\sigma_{\Delta\theta}^2-\lambda}{2\lambda\sigma_{\Delta\theta}^2}(\Delta\theta)^2}d\Delta\theta\end{aligned} \quad (۱۸)$$

همچنین برای بخش دوم رابطه (۱۷) می‌توان نوشت:

$$\begin{aligned}R_{\Delta\mathbf{h}_B,R}(p,q) &= \int_{-\Delta R_{\max}}^{\Delta R_{\max}}e^{\frac{j2\pi\left(k_p-k_q\right)\Delta f\,\Delta R}{\lambda}}f\left(\Delta R\right)d\Delta R\\ &= \frac{2}{\sqrt{2\pi}\sigma_{\Delta R}}\int_0^{\Delta R_{\max}}e^{\frac{j2\pi\left(k_p-k_q\right)\Delta f\,\Delta R}{\lambda}}e^{-\frac{(\Delta R)^2}{2\sigma_{\Delta R}^2}}d\Delta R\end{aligned} \quad (۱۹)$$

با محاسبه عددی انتگرال‌های روابط (۱۸) و (۱۹) مقدار ماتریس همبستگی $R\left(\Delta\mathbf{h}_B\right)$ مشخص خواهد شد. همچنین از رابطه (۱۴) مشاهده می‌شود که اثر خطای تخمین موقعیت به‌صورت کامل در نرخ ارگادیک لحاظ شده است و با توجه به اینکه در محاسبه مقادیر نرخ محرمانگی ارگادیک از آمارگان خطای تخمین موقعیت استفاده شده است، روش پیشنهادی نسبت به این خطا مقاوم است.

۴- تخصیص بهینه توان در روش مقاوم پیشنهادی

با توجه به اینکه اضافه شدن نویز مصنوعی باعث کاهش سهم توان سیگنال پیام و درنتیجه کاهش نسبت سیگنال به نویز در گیرنده قانونی می‌شود، عملکرد محرمانگی کلی سیستم افت می‌یابد؛ لذا تخصیص بهینه توان به‌منظور بیشینه کردن نرخ محرمانگی، یک چالش مهم است که تأثیر قابل‌توجهی بر عملکرد محرمانگی سیستم دارد. مطابق روابط (۱۳) و (۱۵)، نسبت سیگنال به نویز و تداخل، تابعی از α ، $\mathbf{v}$ و $\mathbf{w}$ است یعنی $SINR=f\left(\alpha,\mathbf{v},\mathbf{w}\right)$. در نتیجه مسئله بهینه‌سازی را می‌توان به‌صورت زیر نمایش داد.

$$\begin{aligned}&\alpha^*=\max_{\alpha,\mathbf{v},\mathbf{w}}\ R_{S,E}^{LB}\left(\alpha,\mathbf{v},\mathbf{w}\right)\\ &\text{s.t.}\begin{cases}0\le\alpha\le 1.\\ \mathbf{v}^H\mathbf{v}=1\\ \mathbf{w}^H\mathbf{w}=1\end{cases}\end{aligned} \quad (۲۰)$$

با توجه به فرض مسئله که در آن هدف از بهینه‌سازی یافتن ضریب توان بهینه برای بیشینه کردن نرخ محرمانگی است، به‌منظور بیشینه شدن نسبت سیگنال به نویز در گیرنده، مطابق رابطه (۴)، بردار جهت‌دهی پرتو ثابت و معادل بردار هدایت آرایه فرض شده است. همچنین بردار نویز مصنوعی نیز مطابق رابطه (۵) بر اساس فضای پوچ بردار $\mathbf{h}\left(\theta_B,R_B\right)$ و برای سادگی محاسبات به‌صورت ثابت فرض شده است. لذا مسئله بهینه‌سازی به ضریب تخصیص توان محدود شده و قید آن به‌صورت $0\le\alpha\le 1$ در نظر گرفته شده است؛ یعنی:

$$\begin{aligned}&\alpha^*=\max_{\alpha}\ R_{S,E}^{LB}\left(\alpha\right)\\ &\text{s.t. } 0\le\alpha\le 1.\end{aligned} \quad (۲۱)$$

به دلیل پیچیدگی محاسباتی یافتن پاسخ فرم بسته برای رابطه فوق بسیار مشکل است. لذا مشابه [۳۶, ۳۷] در این مقاله از روش جستجوی جامع[1] برای یافتن نقاط بهینه استفاده شده است. با حل این مسئله بهینه‌سازی، امکان تخصیص توان بهینه در راهکار مقاوم پیشنهادی فراهم خواهد شد.

وقتی‌که $N\to\infty$ میل کند، مقدار $\left|\mathbf{h}^H\left(\theta_E,R_E\right)\mathbf{h}\left(\theta_B,R_B\right)\right|^2$ در رابطه (۱۱) به میانگین خود یعنی $E\left\{\left|\mathbf{h}^H\left(\theta_E,R_E\right)\mathbf{h}\left(\theta_B,R_B\right)\right|^2\right\}$ میل می‌کند. یعنی با

[1] *Exhustive Search*

$N \to \infty$ مقدار کران پایین نرخ محرمانگی به مقدار ارگادیک میل می‌کند. می‌توان نوشت:

$$R_{S,E}^{\infty} \geq \log_2\left(1+\frac{\alpha P_t}{\sigma_B^2}\right) - \log_2\left(1+\frac{\alpha P_t \overbrace{\underset{\Delta h_B}{E}\left\{\left|\mathbf{h}_E^H \mathbf{h}_B\right|^2\right\}}^{0}}{\left(1-\alpha\right)\underbrace{\left|\mathbf{h}_E^H \mathbf{w}\right|^2}_{0}+\frac{\sigma_E^2}{\sigma_B^2}}\right) \quad (۲۲)$$

$$\geq \log_2\left(1+\frac{\alpha P_t}{\sigma_B^2}\right)$$

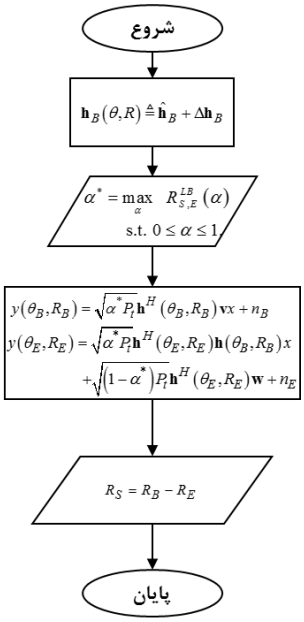
مطابق تعریف، هر چه تعداد المان‌های آرایه آنتن افزایش یابد، قابلیت درهم‌ریزی و تخریب منظومه مدولاسیون در جهات ناخواسته نیز افزایش می‌یابد. درنتیجه با افزایش تعداد المان آرایه آنتن، نرخ محرمانگی افزایش می‌یابد. تا جایی که در تعداد المان بی‌نهایت، پرتو جهت‌دهی شده به سمت گیرنده قانونی به‌صورت نقطه‌ای شده و حضور شنودگر در اطراف گیرنده قانونی تأثیری بر عملکرد محرمانگی سیستم نخواهد داشت.

بر اساس راهکار پیشنهادی، ابتدا در فرستنده، ضریب تخصیص توان بهینه با بیشینه کردن حد پایین نرخ ارگادیک، در حضور خطای تخمین موقعیت گیرنده قانونی، محاسبه شده (رابطه ۲۱) و سپس سیگنال‌های پیام و نویز مصنوعی متناسب با این ضریب ارسال می‌شوند. باتوجه‌به اینکه در محاسبه این ضریب اثر خطای تخمین لحاظ شده (رابطه ۱۵) و بهینه‌سازی بر این اساس انجام گرفته، عملکرد محرمانگی سیستم نسبت به این خطا مقاوم است. سیگنال دریافتی در گیرنده قانونی و شنودگر را می‌توان به‌صورت زیر نمایش داد:

$$y\left(\theta_B, R_B\right) = \sqrt{\alpha^* P_t}\left(\hat{\mathbf{h}}_B + \Delta\mathbf{h}_B\right)^H \mathbf{v}x + n_B \quad (۲۳)$$

$$y\left(\theta_E, R_E\right) = \sqrt{\alpha^* P_t}\mathbf{h}_E^H\left(\hat{\mathbf{h}}_B + \Delta\mathbf{h}_B\right)x + \sqrt{\left(1-\alpha^*\right)P_t}\mathbf{h}_E^H\mathbf{w} + n_E \quad (۲۴)$$

در نهایت با استفاده از رابطه (۱۱) نرخ محرمانگی قابل محاسبه است. در شکل (۳) فرآیند محاسبه نرخ محرمانگی در راهکار پیشنهادی، نمایش داده شده است.



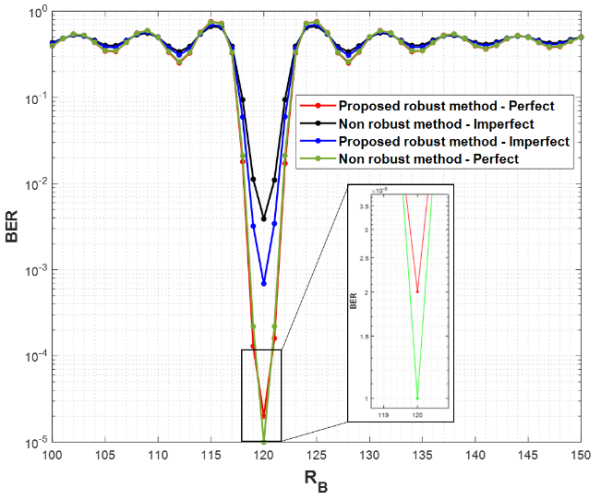
شکل (۳): فرآیند محاسبه نرخ محرمانگی در راهکار مقاوم پیشنهادی

۵- شبیه‌سازی و تحلیل نتایج

به‌منظور بررسی عملکرد راهکار پیشنهادی، شبیه‌سازی عددی در دستور کار قرار گرفته است. فرض شده است که گیرنده قانونی در زاویه ۴۵ درجه و بافاصله ۱۲۰ متری نسبت به فرستنده قرار دارد. فرکانس مرکزی $1GHz$، اختلاف فرکانس المان‌های آرایه برابر $3MHz$، فاصله المان‌ها با یکدیگر نصف طول‌موج و $\beta = \frac{\sigma_E^2}{\sigma_B^2} = 1$ فرض شده است.

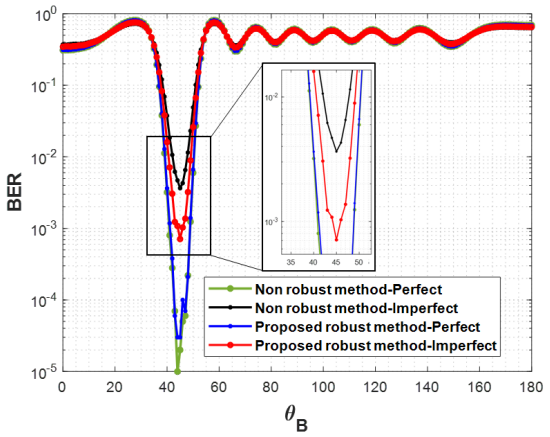
در شکل (۴)، نرخ خطای بیت سیگنال با مدولاسیون $BPSK$ دریافت شده در گیرنده قانونی نسبت به فاصله از فرستنده، نشان داده شده است. فرض شده است که فرستنده مجهز به آرایه‌ای با ۱۶ المان بوده و خطای تخمین فاصله به‌صورت متغیر تصادفی نرمال با $\sigma_R = 1$ و $\mu_R = 0$ در نظر گرفته‌شده است. همچنین، میزان سیگنال به نویز برابر $10dB$قرار داده شده است. مطابق انتظار، سیستم به فاصله از پیش اندازه‌گیری شده حساسیت بالایی دارد. چراکه مدولاسیون جهتی برای موقعیت فعلی گیرنده قانونی، یعنی $(\theta_B, R_B) = (45^0, 120m)$، تنظیم شده است. مطابق شکل (۳) برای سیستم بدون مقاوم‌سازی [۲۹] و در شرایط در اختیار داشتن اطلاعات کامل و دقیق از موقعیت گیرنده، مقدار کمینه نرخ خطا برابر با 1×10^{-5} و در فاصله ۱۲۰ متری از فرستنده حاصل شده است؛ اما مشاهده می‌شود که با رخداد خطای تخمین فاصله به میزان حداکثر $\Delta R = 1$ متر، نرخ خطای گیرنده قانونی به‌شدت افت پیدا کرده و تا 3.64×10^{-3} کاهش می‌یابد. این مهم، اثر قابل‌توجه خطای تخمین موقعیت در افت عملکرد مدولاسیون جهتی مبتنی بر آرایه چندگانگی

فرکانسی را نشان می‌دهد؛ اما با به‌کارگیری روش پیشنهادی برای مقاوم‌سازی در برابر خطای تخمین موقعیت، این افت عملکرد در نرخ خطای بیت، به میزان چشم‌گیری بهبود پیدا کرده و به 7.1×10^{-4} رسیده است. در شرایطی که خطایی در تخمین موقعیت رخ ندهد، به دلیل در نظر گرفتن مشخصات آماری خطا در مقاوم‌سازی، روش پیشنهادی افت کوچکی در نرخ خطای بیت دارد که با توجه به ذات شبکه‌های بی‌سیم که در آن احتمال رخداد خطای تخمین فاصله بسیار بالاست، می‌توان از این افت عملکرد چشم‌پوشی کرد.



شکل (۴): منحنی نرخ خطای بیت به ازای مقادیر مختلف فاصله گیرنده قانونی از فرستنده

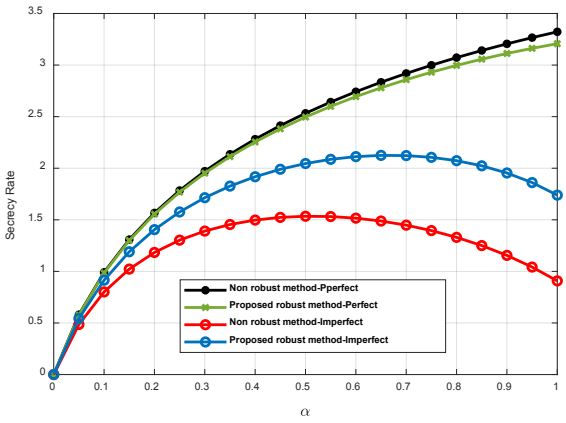
مطابق آنچه برای بُعد فاصله نشان داده شد، خطای تخمین زاویه گیرنده قانونی نسبت به فرستنده نیز تأثیر بالایی در عملکرد مدولاسیون جهتی مبتنی بر آرایه چندگانگی فرکانسی دارد. این مهم در شکل (۵) نشان داده شده است. خطای تخمین فاصله به‌صورت متغیر تصادفی نرمال با $\sigma_\theta=1$ و $\mu_\theta=0$ در نظر گرفته‌شده است. میزان سیگنال به نویز نیز برابر $10dB$ فرض شده است. مجدداً مشاهده می‌شود که میزان کمینه نرخ خطای بیت در زاویه مطلوب ۴۵ درجه و برای شرایط بدون مقاوم‌سازی [۲۹] رخ داده است. با بروز خطای تخمین، نرخ خطای بیت تا 3.9×10^{-3} افت پیدا می‌کند؛ اما با به‌کارگیری روش مقاوم پیشنهادی، در حضور خطای تخمین، عملکرد سیستم بهبود یافته و نرخ خطا تا 6.9×10^{-4} می‌رسد.



شکل (۵): منحنی نرخ خطای بیت به ازای مقادیر مختلف زاویه گیرنده قانونی از فرستنده

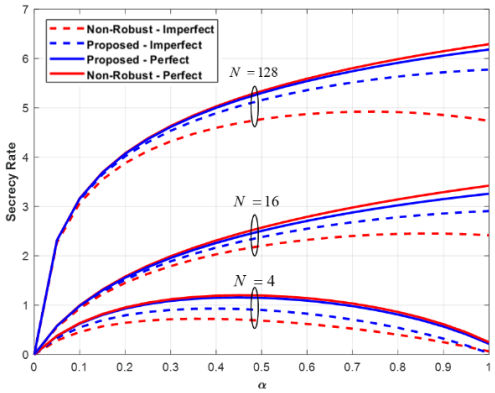
به‌منظور بررسی اثر تخمین موقعیت بر عملکرد امنیت لایه فیزیکی مبتنی بر مدولاسیون جهتی، در این بخش شبیه‌سازی نرخ محرمانگی برای حالت‌های مختلف سیستم، با و بدون مقاوم‌سازی، در دستور کار قرار گرفته است.

شکل (۶)، منحنی‌های نرخ محرمانگی به ازای ضریب تخصیص توان بین سیگنال پیام و نویز مصنوعی، یعنی α را نشان می‌دهد. فرض شده است که شنودگر در موقعیت $(\theta_E,R_E)=(40^\circ,115m)$ قرار دارد. مطابق انتظار، در حالت بدون مقاوم‌سازی و بدون خطای تخمین، منحنی نرخ محرمانگی بیشترین مقدار را در α-های متناظر، نسبت به سایر حالات دارد. در حالت بدون مقاوم‌سازی، در صورت بروز مقدار بیشینه خطای تخمین، $(\Delta\theta_{B,\max},\Delta R_{B,\max})=(1^\circ,1m)$، نسبت سیگنال به نویز در گیرنده قانونی کاهش خواهد یافت. در این حالت ممکن است مدولاسیون جهتی به‌اشتباه برای موقعیتی نزدیک به شنودگر طراحی شود. این دو عامل می‌تواند نرخ محرمانگی را به‌شدت کاهش دهد. این موضوع به‌وضوح در شکل (۶) و در نمودار مربوط به حالت بدون مقاوم‌سازی با حضور خطای تخمین، قابل مشاهده است. مطابق شکل (۶)، در راهکار مقاوم پیشنهادی، نرخ محرمانگی در حضور خطای تخمین موقعیت به نویز مصنوعی به میزان مطلوبی بهبود یافته و مقدار بیشینه آن به ازای ۳۰ درصد از تخصیص توان به نویز مصنوعی ($\alpha=\alpha^*=0.7$)، قابل‌دستیابی است. در این نقطه کاری، مقدار نرخ محرمانگی بیش از یک بیت بر هرتز بر ثانیه نسبت به روش بدون مقاوم‌سازی بهبود یافته است. عملکرد راهکار پیشنهادی در شرایط بدون رخداد خطای تخمین، افت کمی در نرخ محرمانگی را نشان می‌دهد که با توجه به احتمال بالای رخداد خطا در ارتباطات بی‌سیم، قابل صرف‌نظر کردن است.



شکل (۶): منحنی نرخ خطای بیت به ازای مقادیر مختلف زاویه گیرنده قانونی از فرستنده

همان‌گونه که در بخش ۳ بیان شد، هر چه تعداد المان‌های آرایه آنتن افزایش یابد، ضمن افزایش قابلیت تفکیک‌پذیری مدولاسیون جهتی، نرخ محرمانگی افزایش می‌یابد. تا جایی که در تعداد المان بی‌نهایت، پرتو جهت‌دهی شده به سمت گیرنده قانونی، به‌صورت نقطه‌ای شده و حضور شنودگر در اطراف گیرنده قانونی تأثیری بر عملکرد محرمانگی سیستم نخواهد داشت. اما در مقابل حساسیت سیستم به خطای تخمین نیز افزایش خواهد یافت. این موضوع با شبیه‌سازی در شکل (۷) نشان داده شده است. ملاحظه می‌شود که درروش غیر مقاوم، با افزایش تعداد المان‌های آنتن نرخ محرمانگی هم به میزان قابل‌توجهی افزایش می‌یابد؛ اما هر چه تعداد المان‌ها بیشتر باشد، خطای تخمین موقعیت باعث افت بیشتری در عملکرد محرمانگی می‌شود. این رفتار در راهکار پیشنهادی نیز قابل‌مشاهده است، اما میزان افت عملکرد محرمانگی در مقایسه با روش غیر مقاوم به‌مراتب کمتر است.



شکل (۷): منحنی نرخ محرمانگی به ازای مقادیر مختلف ضریب تخصیص توان و تعداد مختلف المان‌های آرایه آنتن

۵- نتیجه‌گیری

در این مقاله یک راهکار جدید جهت مقاوم‌سازی مدولاسیون جهتی مبتنی بر آرایه چندگانگی فرکانسی تصادفی، در برابر خطای تخمین موقعیت گیرنده قانونی ارائه و عملکرد آن در ایجاد محرمانگی در امنیت لایه فیزیکی در حضور خطای تخمین مورد ارزیابی قرار گرفت. راهکار پیشنهادی با لحاظ کردن مشخصات آماری خطای تخمین در نرخ ارگادیک، می‌تواند عملکرد مطلوبی از خود نشان دهد. با شبیه‌سازی‌های عددی نشان داده شد که عملکرد محرمانگی در راهکار پیشنهادی در مقایسه با [۲۹]، برای آرایه با ۱۲۸ المان و $\alpha = 1$، به میزان از یک بیت بر هرتز بر ثانیه بهبود یافته است.

۶- مراجع

[1] Y. Liu, H.-H. Chen, and L. Wang, "Physical Layer Security for Next Generation Wireless Networks: Theories, Technologies, and Challenges," IEEE Communications Surveys & Tutorials, vol. 19, no. 1, pp. 347-376, 2017, doi: 10.1109/COMST.2016. 2598968.

[2] A. K. Yerrapragada, T. Eisman, and B. Kelley, "Physical Layer Security for Beyond 5G: Ultra Secure Low Latency Communications," IEEE Open Journal of the Communications Society, vol. 2, pp. 2232-2242, 2021, doi: 10.1109/OJCOMS.2021.3105185.

[3] B. Li, Z. Fei, C. Zhou, and Y. Zhang, "Physical-Layer Security in Space Information Networks: A Survey," IEEE Internet of Things Journal, vol. 7, no. 1, pp. 33-52, 2020, doi:10.1109/JIOT.2019.2943900.

[4] B. Maryam, Z. Hadi, and A. Kuhestani, "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," (in Fa), Journal of Electronic and Cyber Defense, vol. 11, no. 4, pp. 75-82, 2024. https://dor.isc.ac/dor/20.1001.1.23224347.1402.11.4.6.3

[5] A. Babakhani, D. B. Rutledge, and A. Hajimiri, "Near-field direct antenna modulation," IEEE Microwave Magazine, vol. 10, no. 1, pp. 36-46, 2009, doi: 10.1109/MMM.2008.930674.

[6] A. Babakhani, D. B. Rutledge, and A. Hajimiri, "Transmitter Architectures Based on Near-Field Direct Antenna Modulation," IEEE Journal of Solid-State Circuits, vol. 43, no. 12, pp. 2674-2692, 2008, doi: 10.1109/JSSC.2008.2004864.

[7] M. P. Daly and J. T. Bernhard, "Directional Modulation Technique for Phased Arrays," IEEE Transactions on Antennas and Propagation, vol. 57, no. 9, pp. 2633-2640, 2009, doi: 10.1109/TAP.2009.2027047.

[8] M. P. Daly, E. L. Daly, and J. T. Bernhard, "Demonstration of Directional Modulation Using a Phased Array," IEEE Transactions on Antennas and Propagation,

vol. 58, no. 5, pp. 1545-1550, 2010, doi: 10.1109/TAP.2010.2044357.

[9] Y. Ding and V. F. Fusco, "A Vector Approach for the Analysis and Synthesis of Directional Modulation Transmitters," IEEE Transactions on Antennas and Propagation, vol. 62, no. 1, pp. 361-370, 2014, doi: 10.1109/TAP.2013.2287001.

[10] Y. Ding and V. F. Fusco, "Directional modulation far-field pattern separation synthesis approach," IET Microwaves, Antennas & Propagation, vol. 9, no. 1, pp. 41-48, 2015, doi: https://doi.org/10.1049/iet-map.2014.0331.

[11] W. Q. Wang and H. C. So, "Transmit Subaperturing for Range and Angle Estimation in Frequency Diverse Array Radar," IEEE Transactions on Signal Processing, vol. 62, no. 8, pp. 2000-2011, 2014, doi: 10.1109/TSP.2014.2305638.

[12] P. Antonik, M. C. Wicks, H. D. Griffiths, and C. J. Baker, "Frequency diverse array radars," in 2006 IEEE Conference on Radar, 24-27 April 2006, p. 3 pp., doi: 10.1109/RADAR.2006.1631800.

[13] T. Eker, S. Demir, and A. Hizal, "Exploitation of Linear Frequency Modulated Continuous Waveform (LFMCW) for Frequency Diverse Arrays," IEEE Transactions on Antennas and Propagation, vol. 61, no. 7, pp. 3546-3553, 2013, doi: 10.1109/TAP.2013.2258393.

[14] Y. Wang, W. Q. Wang, and H. Chen, "Linear Frequency Diverse Array Manifold Geometry and Ambiguity Analysis," IEEE Sensors Journal, vol. 15, no. 2, pp. 984-993, 2015, doi: 10.1109/JSEN.2014.2359074.

[15] W. Q. Wang, "Range-Angle Dependent Transmit Beampattern Synthesis for Linear Frequency Diverse Arrays," IEEE Transactions on Antennas and Propagation, vol. 61, no. 8, pp. 4073-4081, 2013, doi: 10.1109/TAP.2013.2260515.

[16] W. Q. Wang, "Subarray-based frequency diverse array radar for target range-angle estimation," IEEE Transactions on Aerospace and Electronic Systems, vol. 50, no. 4, pp. 3057-3067, 2014, doi: 10.1109/TAES.2014.120804.

[17] P. F. Sammartino, C. J. Baker, and H. D. Griffiths, "Frequency Diverse MIMO Techniques for Radar," IEEE Transactions on Aerospace and Electronic Systems, vol. 49, no. 1, pp. 201-222, 2013, doi: 10.1109/TAES.2013.6404099.

[18] H. Shao, J. Li, H. Chen, and W. Q. Wang, "Adaptive Frequency Offset Selection in Frequency Diverse Array Radar," IEEE Antennas and Wireless Propagation Letters, vol. 13, pp. 1405-1408, 2014, doi: 10.1109/LAWP.2014.2340893.

[19] H. Huang and W. Q. Wang, "FDA-OFDM for integrated navigation, sensing, and communication systems," IEEE Aerospace and Electronic Systems Magazine, vol. 33, no. 5-6, pp. 34-42, 2018, doi: 10.1109/MAES.2018.170109.

[20] W.-Q. Wang, "DM using FDA antenna for secure transmission," (in en), IET Microwaves, Antennas & Propagation, vol. 11, no. 3, pp. 336-345, 2016/10/04/ 2016, doi: 10.1049/iet-map.2016.0303.

[21] W. Khan, I. M. Qureshi, and S. Saeed, "Frequency Diverse Array Radar With Logarithmically Increasing Frequency Offset," IEEE Antennas and Wireless Propagation Letters, vol. 14, pp. 499-502, 2015, doi: 10.1109/LAWP.2014.2368977.

[22] K. Gao, W.-Q. Wang, J. Cai, and J. Xiong, "Decoupled frequency diverse array range–angle-dependent beampattern synthesis using non-linearly increasing frequency offsets," IET Microwaves, Antennas & Propagation, vol. 10, no. 8, pp. 880-884, 2016, doi: https://doi.org/10.1049/iet-map.2015.0658.

[23] Y. Liu, H. Ruan, L. Wang, and A. Nehorai, "The Random Frequency Diverse Array: A New Antenna Structure for Uncoupled Direction-Range Indication in Active Sensing," IEEE Journal of Selected Topics in Signal Processing, vol. 11, no. 2, pp. 295-308, 2017, doi: 10.1109/JSTSP.2016.2627183.

[24] H. Khodadadi and S. FALSAFI , "Improvement of Security in Wireless Communication Networks with Directional Modulation and Artificial Noise," (in Fa), Journal of Electronic and Cyber Defense, vol. 10, no. 4, pp. 11-18, 2023. https://dor.isc.ac/dor/20.1001.1.23224347.1401.10.4.2.2

[25] M. Tayyeb Massoud and H. Khaleghi Bizaki, "Optimal Power Allocation for Maximizing Secrecy Rate in Physical Layer Security Using Frequency Diverse Array Directional Modulation and Artificial Noise," (in fa), International Journal of Electrical and Computer Engineering (IJECE), no. 1, pp. 67-75, 2024.

[26] S. Lv, J. Hu, Y. Chen, Z. Xu, and Z. D. Chen, "Establishing Secrecy Region for Directional Modulation Scheme with Random Frequency Diverse Array," in GLOBECOM 2020 - 2020 IEEE Global Communications Conference, 2020, pp. 1-6, doi: 10.1109/GLOBECOM42002.2020.9322647.

[27] F. Shu, X. Wu, J. Li, R. Chen, and B. Vucetic, "Robust Synthesis Scheme for Secure Multi-Beam Directional Modulation in Broadcasting Systems," IEEE Access, vol. 4, pp. 6614-6623, 2016, doi: 10.1109/ACCESS.2016.2614825.

[28] F. Shu, W. Zhu, X. Zhou, J. Li, and J. Lu, "Robust Secure Transmission of Using Main-Lobe-Integration-Based Leakage Beamforming in Directional Modulation MU-MIMO Systems," IEEE Systems Journal, vol. 12, no. 4, pp. 3775-3785, 2018, doi: 10.1109/JSYST.2017.2764142.

[34] H. K. Bizaki and A. Falahati, "Tomlinson–Harashima precoding with imperfect channel side information," The 9th International Conference on Advanced Communication Technology, vol. 2, pp. 987-991, 2007.

[35] H. Khaleghi Bizeki, Wireless Communication Systems, Malek Ashtar University of Technology Publications, First Edition, 2010.

[36] Z. Lu et al. "Optimal power allocation for secure directional modulation networks with a full-duplex UAV user," Science China Information Sciences, vol. 62, no. 8, p. 80304, 2019, doi: 10.1007/s11432-019-9928-5.

[37] F. Shu et al. "Alternating iterative secure structure between beamforming and power allocation for UAV-aided directional modulation networks," Physical Communication, vol. 33, pp. 46-53, 2019, doi: https://doi.org/10.1016/j.phycom.2018.12.003.

[29] S. Wan et al., "Power Allocation Strategy of Maximizing Secrecy Rate for Secure Directional Modulation Networks," IEEE Access, vol. 6, pp. 38794-38801, 2018, doi: 10.1109/ACCESS.2018.2815779.

[30] X. Zhou, J. Li, F. Shu, Q. Wu, Y. Wu, W. Chen, and L. Hanzo, "Secure SWIPT for Directional Modulation-Aided AF Relaying Networks," IEEE Journal on Selected Areas in Communications, vol. 37, no. 2, pp. 253-268, 2019, doi: 10.1109/JSAC.2018.2872372.

[31] J. Hu, F. Shu, and J. Li, "Robust Synthesis Method for Secure Directional Modulation With Imperfect Direction Angle," (in en), IEEE Commun. Lett., vol. 20, no. 6, pp. 1084-1087, 2016, doi: 10.1109/LCOMM.2016.2550022.

[32] A. D. Wyner, "The wire-tap channel," Bell system technical journal, vol. 54, no. 8, pp. 1355-1387, 1975.

[33] H. Khaleghi Bizaki and M. Tayyeb Masoud, "Deep MIMO Detection with Imperfect CSI," Advanced Signal Processing, vol. 5, no. 1, pp. 1-7, 2021.