# بهبود امنیت لایه فیزیکی در سیستم کدکننده زمان-فضا مبتنی بر مدل تعمیم یافته Alamouti

**علیرضا بقائی پوری[1]  محمد ترابی[2]**

۱- دانشجوی دکتری، دانشکده مهندسی برق- دانشگاه شهید بهشتی- تهران- ایران
a_baghaeipouri@sbu.ac.ir

۲- استادیار، دانشکده مهندسی برق- دانشگاه شهید بهشتی - تهران- ایران
m_torabi@sbu.ac.ir

**چکیده: در این مقاله روشی جهت بهبود امنیت لایه فیزیکی در سیستم کدکننده زمان-فضا مبتنی بر مدل تعمیم‌یافته Alamouti ارائه شده است. در روش پیشنهادی با فرض اطلاع داشتن از کانال مربوط به گیرنده مجاز، علاوه بر استفاده از نویز مصنوعی جهت افزایش امنیت، داده‌های ارسالی از هر آنتن به کانال مربوط به گیرنده مجاز وابسته می‌شود. همچنین فرستنده جهت دستیابی به امنیت بالاتر با استفاده از کدکننده فضا-زمان پیشنهادی از بیش از دو آنتن جهت ارسال داده در هر زمان استفاده می-نماید. در هر یک از حالات یک‌مسیره، دومسیره و چندمسیره با نویز مصنوعی روابط ریاضی تئوری مربوط به امنیت لایه فیزیکی ارائه شده‌است. نتایج شبیه‌سازی حالات مختلف بیانگر میزان افزایش امنیت روش پیشنهادی نسبت به روش‌های موجود فعلی است.**

**واژه‌های کلیدی: امنیت لایه فیزیکی، کدهای زمان-فضا، ظرفیت محرمانگی، نویز مصنوعی**

---

**تاریخ ارسال مقاله:** ۱۳۹۷/۲/۲۷
**تاریخ پذیرش مشروط مقاله:** ۱۳۹۷/۹/۱۹
**تاریخ پذیرش مقاله :** ۱۳۹۸/۴/۲

**نام نویسنده‌ی مسئول:** دکتر محمد ترابی
**نشانی نویسنده‌ی مسئول :** ایران – تهران – ولنجک – بلوار دانشجو – دانشگاه شهیدبهشتی – دانشکده‌ی برق

## ۱- مقدمه

با روند رو به رشد استفاده از خدمات بی‌سیم و افزایش چشمگیر حجم و سرعت تبادل اطلاعات، امنیت انتقال داده‌ها بیش از پیش مورد توجه قرار گرفته است چرا که در صورت فاش شدن بخش محدودی از اطلاعات در حال تبادل، احتمال نفوذ و دستیابی کاربران غیرمجاز به سایر اطلاعات مهم وجود خواهد داشت. در گذشته رمزنگاری اطلاعات، به عنوان روشی مطمئن جهت جلوگیری از فاش شدن اطلاعات شناخته می‌شد. دلیل اتکا و اطمینان به روش‌های رمزنگاری قدرت محاسبات نسبتا پایین پردازنده‌های موجود بود و تقریبا احتمال رمزشکنی در مدت زمان قابل قبول غیرممکن به نظر می‌رسید. اما با پیشرفت تکنولوژی و ساخت پردازنده‌های قوی با توان محاسباتی بسیار بالا این زمان کمتر گردید و در کنار آن نیز اشکالات برخی روش‌های رمزنگاری اثبات گردید. بنابراین سیستم‌های رمزنگاری دیگر نمی‌توانند مانند قبل و به تنهایی امنیت انتقال اطلاعات را تضمین کنند. در کنار این دغدغه برخی پژوهشگران با یادآوری ماهیت ذاتی انتقال بی‌سیم اطلاعات و اثرات طبیعی کانال، نویز و سایر پارامترها بر سیگنال ارسالی، مبحث امنیت لایه فیزیکی را به عنوان مکملی برای رمزنگاری مطرح نمودند. از اولین کارها در این زمینه می‌توان به کار واینر [۱] اشاره نمود. پس از آن پژوهشگران در سیستم‌های مختلف و کاربردی روش‌هایی را جهت دستیابی به امنیت در لایه فیزیکی مطرح نمودند و این روند همچنان ادامه دارد.

امروزه سیستم‌های چندورودی، چندخروجی(MIMO) به دلیل توانایی در افزایش نرخ تبادل اطلاعات و افزایش دایورسیتی[1] از جمله سیستم‌های پرکاربرد می‌باشند [۳] , [۲]، لذا مسئله امنیت این سیستم‌ها نیز از جمله مواردی است که همچنان پذیرای پژوهش‌های جدیدی در این زمینه است. از جمله مقالاتی که مدل واینر را برای بیش از یک آنتن در حضور نویز سفید بررسی کرده‌اند می‌توان به [۴] و [۵] اشاره نمود. علاوه بر این جهت دستیابی به دایورسیتی در سیستم‌های MIMO روش‌هایی تحت عنوان کدینگ زمان-فضا[2] معرفی شد که در آن هدف از افزایش تعداد آنتن، افزایش دایورسیتی جهت دریافت اطلاعات با شانس خطای کمتر است که محققانی همچون تارخ، الموتی و همکارانشان در [۶] و [۷] روش‌هایی جهت دست‌یابی به این هدف معرفی کرده‌اند.

از پژوهش‌هایی که در راستای امنیت لایه فیزیکی در سیستم‌هایی که بر اساس کدینگ زمان-فضا طراحی شده‌اند انجام گرفته می‌توان به [۸] اشاره نمود که نویسندگان در این مقاله با افزودن نویز مصنوعی به دنبال افزایش امنیت هستند. در این مقاله روابط تحلیلی به صورت کامل بررسی نشده و به دو آنتن در فرستنده و گیرنده بسنده شده است. همچنین در [۹] نویسندگان سعی کرده‌اند با چرخش تصادفی فاز سمبل‌های ارسالی در مدلی مانند مدل الموتی به امنیت دست پیدا کنند. همچنین در [۱۰] ابتدا گیرنده مجاز سیگنالی را برای فرستنده ارسال می‌نماید و فرستنده با توجه به ضرایب کانالی که با استفاده از سیگنال دریافتی تخمین زده شده فاز ثابتی را به سیگنال ارسالی اعمال می‌کند که شنودگر به دلیل تفاوت کانال قادر به شناسایی آن نخواهد بود. در [۱۱] نویسندگان اثر خطای تخمین کانال را در سیستم MIMO-STBC بررسی کرده‌اند. همچنین در [۱۲] نویسندگان حالتی را بررسی کرده‌اند که چندین کاربر قصد ارتباط با یک کاربر را دارند و همه از مدل الموتی استفاده می‌کنند. در این حالت سعی شده با استفاده از نویز مصنوعی، امنیت را تا حد قابل قبولی بهبود بخشید. علاوه بر این در [۱۳] از یک پیش‌کدگذار و یک وفق‌دهنده جهت کاهش خطا و افزایش امنیت استفاده شده و روابط مربوطه نیز ارائه شده است.

در این مقاله روش جدیدی را جهت بهبود و افزایش امنیت لایه فیزیکی در سیستم کدکننده زمان-فضا مبتنی بر مدل تعمیم یافته الموتی ارائه کرده‌ایم. همچنین روابط تحلیلی برای دو معیار سنجش و اندازه‌گیری میزان محرمانگی لایه فیزیکی، یعنی ظرفیت کانال امن سیستم و احتمال قطع ارتباط محرمانه در سیستم پیشنهادی بدست آورده و ارائه داده‌ایم. از طرفی با افزایش تعداد آنتن و ایجاد وابستگی بین سیگنال ارسالی و کانال گیرنده مجاز و همچنین تولید نویز مصنوعی شانس تخمین اطلاعات توسط شنودگر را بیش از پیش کاهش داده‌ایم.

لازم به ذکر است که، بنا به اطلاع نویسندگان، نتایج و تحلیل‌های ارائه شده در این مقاله کاملاً جدید بوده و تاکنون در مجله دیگری منتشر نشده است.

بخش‌های بعدی مقاله بدین صورت تنظیم شده است. در بخش ۲ روابط اولیه در یک مدل ساده و تک مسیره (یک آنتن در فرستنده و یک آنتن در هر گیرنده) بررسی شده است. در بخش ۳ روابط برای مدل الموتی با دو مسیر (دو آنتن در فرستنده و یک آنتن در هر گیرنده) آورده شده است به صورت کامل‌تری بررسی شده است. در بخش ۴ روش پیشنهادی که بر اساس مدل تعمیم یافته الموتی می باشد که در آن فرستنده از چندین آنتن به همراه نویز مصنوعی استفاده می‌کند ارائه شده و همچنین روابط تحلیلی لازم آورده شده است. در بخش ۵ نتایج عددی و شبیه‌سازی‌های مختلفی جهت بررسی ابعاد روش پیشنهادی ارائه گردیده و در نهایت در بخش ۶ نتیجه‌گیری انجام شده است.

## ۲- مدل تک مسیره

در این بخش، به محاسبه ظرفیت محرمانگی[3] و احتمال قطع ارتباط محرمانه[4] برای مدل ساده‌ای که تنها از یک فرستنده، یک گیرنده مجاز و یک گیرنده غیرمجاز تشکیل شده و هر کدام نیز دارای یک آنتن می‌باشند پرداخته شده است. سپس از روابط بدست آمده در بخش‌های بعدی مقاله استفاده خواهیم کرد.

مطابق شکل (۱)، فرض کنید فرستنده سیگنال $s(t)$ را با توان $E_s$ ارسال کند. سیگنال پس از طی دو مسیر مختلف توسط گیرنده‌ها دریافت می‌شود. با فرض این که دو کانال مستقل از هم باشند و اثر کانال را به صورت محوشوندگی از نوع رایلی بلوکی فرض کنیم، سیگنال دریافتی توسط گیرنده‌ها را می‌توان به صورت (۱) نمایش داد:

$$r_d = h_d s + n_d, \quad r_e = h_e s + n_e, \tag{۱}$$

که در آن $h_d$ و $h_e$ به ترتیب نشان‌دهنده ضرایب کانال از فرستنده به گیرنده مجاز و شنودگر هستند که با فرض کانال رایلی این متغیرهای تصادفی گوسی با میانگین صفر و به ترتیب دارای واریانس $\lambda_d$ و $\lambda_e$ خواهند بود. همچنین، $n_d$ و $n_e$ بیانگر نویز AWGN در هر یک از مسیرها با واریانس $\sigma^2$ است. با توجه به توضیحات داده شده، تابع چگالی احتمال $|h_d|^2$ و $|h_e|^2$ به صورت نمایی به ترتیب با میانگین $\lambda_d$ و $\lambda_e$ خواهد بود. به عبارتی

$$f_{|h_d|^2}(x) = \frac{1}{\lambda_d} e^{-x/\lambda_d}, \quad f_{|h_e|^2}(y) = \frac{1}{\lambda_e} e^{-y/\lambda_e}. \tag{۲}$$

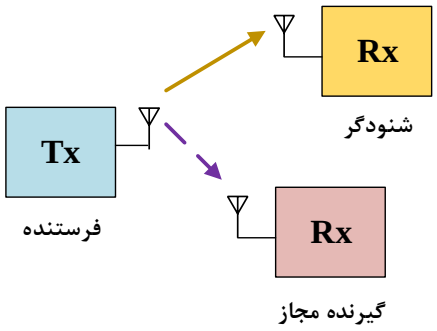
در این صورت ظرفیت کانال گیرنده مجاز و ظرفیت کانال شنودگر به ترتیب به صورت رابطه (۳) محاسبه می‌گردند:

$$C_d = \log_2\left(1+\frac{|h_d|^2 E_s}{\sigma^2}\right), \quad C_e = \log_2\left(1+\frac{|h_e|^2 E_s}{\sigma^2}\right), \tag{۳}$$

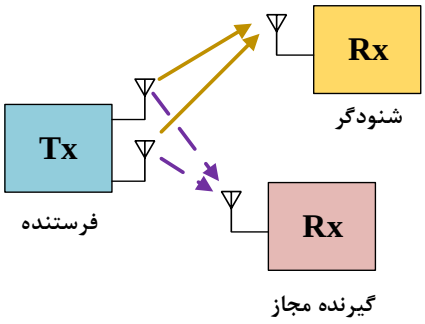
که در آن $C_d$ ظرفیت کانال گیرنده مجاز و $C_e$ ظرفیت کانال شنودگر است. با توجه به [14] ظرفیت محرمانگی به صورت رابطه (۳) تعریف می‌گردد:

$$C_s = [C_d - C_e]^+, \tag{۴}$$

که در آن $C_s$ ظرفیت محرمانگی و $[x]^+ = \max(x,0)$ می‌باشد.




**شکل (۱): مدل تک‌مسیره**




**شکل (۲): مدل دومسیره**

در این صورت ظرفیت محرمانگی سیستم مدنظر به صورت (۵) قابل نمایش است

$$C_s = \left[\log_2\left(1+\frac{|h_d|^2 E_s}{\sigma^2}\right) - \log_2\left(1+\frac{|h_e|^2 E_s}{\sigma^2}\right)\right]^+ \simeq \log_2\left(\frac{|h_t|^2}{|h_e|^2}\right). \tag{۵}$$

علاوه بر این مطابق [۱۵] احتمال قطع رابطه محرمانه به صورت رابطه (۶) تعریف می‌گردد:

$$P_s = P(C_s < R), \tag{۶}$$

که در آن R نشان‌دهنده نرخ محرمانگی مدنظر است.

در این مدل جهت خلاصه‌نویسی از محاسبات لازم جهت بدست آوردن احتمال فوق صرف‌نظر می‌کنیم چرا که در بخش بعد، همین محاسبات برای مدل با پیچیدگی بیشتر، آورده خواهد شد. نتیجه نهایی احتمال فوق در مدل تک مسیره مدنظر به صورت رابطه (۷) می‌باشد

$$P_s = \frac{\lambda_e 2^R}{\lambda_e 2^R + \lambda_d}. \tag{۷}$$

که در آن $\lambda_d$ و $\lambda_e$ میانگین متغیرهای تصادفی $|h_d|^2$ و $|h_e|^2$ می‌باشند که این متغیرها با فرض کانال رایلی دارای توزیع نمایی هستند.

## ۳- مدل دومسیره

در این بخش، ظرفیت محرمانگی و احتمال قطع ارتباط محرمانه را برای مدل Alamouti محاسبه و بررسی خواهیم کرد تا در نهایت از روابط بدست آمده جهت مقایسه عملکرد روش پیشنهادی با روش کنونی استفاده گردد.

در این مدل فرستنده از دو آنتن مستقل جهت ارسال همزمان داده‌ها استفاده می‌نماید. در زمان $t$ فرستنده دو سمبل مختلف $s_0$ و $s_1$ را به ترتیب توسط آنتن اول و دوم ارسال می‌کند و در زمان $t+T$ نیز سمبل‌های $s_1$ و $s_0^*$ را توسط آنتن اول و دوم ارسال می‌نماید. مطابق شکل (۲) سیگنال ارسالی پس از طی دو مسیر مختلف توسط گیرنده مجاز و شنودگر دریافت می‌شود.

فرض کنید $h_{0d}$ و $h_{1d}$ ضرایب مربوط به دو کانال از فرستنده به گیرنده مجاز، همچنین $h_{0e}$ و $h_{1e}$ ضرایب مربوط به شنودگر باشد. در مدل الموتی فرض می‌شود گیرنده قادر است ضرایب کانال را بدون خطا تخمین بزند. در این صورت بر اساس آنچه در [۷] آمده در مدل الموتی سیگنال دریافتی توسط گیرنده مجاز در دو اسلات زمانی با هم ترکیب شده تا $\hat{s}_0$ و $\hat{s}_1$ بدست آید و سپس با استفاده از آشکارساز ML سمبل‌های ارسالی یعنی $s_0$ و $s_1$ آشکارسازی گردد. این ترکیب جهت آشکارسازی سمبل اول و دوم به صورت رابطه (۸) خواهد بود.

$$\begin{aligned}\hat{s}_0 &= h_{0d}^* r(t) + h_{1d} r^*(t+T)\\ &= \left(|h_{0d}|^2 + |h_{1d}|^2\right)s_0 + h_{0d}^* n_0 + h_{1d} n_1^*,\\ \hat{s}_1 &= h_{1d}^* r(t) - h_{0d} r^*(t+T)\\ &= \left(|h_{0d}|^2 + |h_{1d}|^2\right)s_1 + h_{1d}^* n_0 - h_{0d} n_1^*,\end{aligned} \qquad (۸)$$

که در آن $s_0$ و $s_1$ بیانگر سمبل ارسالی اول و دوم است که بایستی بر اساس ماتریس فضا-زمان الموتی کد شده و توسط آنتن‌ها ارسال گردد. علاوه بر این $r(t)$ و $r(t+T)$ سیگنال دریافتی در اسلات زمانی اول و دوم است. همچنین $n_0$ و $n_1$ بیانگر نویز سفید جمع شونده در هریک از مسیرهاست. جهت محاسبه واریانس نویز بهتر است بخش نویز را مطابق رابطه (۹) به صورت ماتریسی بازنویسی کنیم

$$n = h_{0d}^* n_0 + h_{1d} n_1^* = \underbrace{\begin{bmatrix} h_{od}^* & h_{1d}\end{bmatrix}}_{\mathbf{A}}\begin{bmatrix} n_0 \\ n_1^*\end{bmatrix}. \qquad (۹)$$

بنابراین واریانس نویز را میتوان به صورت رابطه (۱۰) محاسبه نمود

$$\sigma^2 = \mathbf{A}\sigma^2\mathbf{I}_2\mathbf{A}^{\mathbf{H}} = \left(|h_{0d}|^2 + |h_{1d}|^2\right)\sigma^2, \qquad (۱۰)$$

که در آن $\mathbf{I}_2$ بیانگر ماتریس واحد ۲×۲ می‌باشد. حال با توجه به توان سیگنال تخمینی و نویز، با استفاده از رابطه ظرفیت کانال، می‌توان ظرفیت کانال گیرنده مجاز و ظرفیت کانال شنودگر را به ترتیب به صورت رابطه (۱۱) محاسبه نمود

$$\begin{aligned}C_d^{tb} &= \log_2\left(1 + \frac{0.5\left(|h_{0d}|^2 + |h_{1d}|^2\right)^2 E_s}{\left(|h_{0d}|^2 + |h_{1d}|^2\right)\sigma^2}\right),\\ C_e^{tb} &= \log_2\left(1 + \frac{0.5\left(|h_{0e}|^2 + |h_{1e}|^2\right)^2 E_s}{\left(|h_{0e}|^2 + |h_{1e}|^2\right)\sigma^2}\right).\end{aligned} \qquad (۱۱)$$

که در آن $C_d^{tb}$ و $C_e^{tb}$ به ترتیب ظرفیت کانال گیرنده مجاز و ظرفیت کانال شنودگر است. همچنین $E_s$ توان سیگنال ارسالی است. ضریب ۰/۵ به این دلیل ایجاد شده که فرستنده از دو آنتن جهت ارسال سیگنال استفاده می‌کند بنابراین با فرض پخش یکنواخت توان، توان هر یک از آنتن‌ها نصف توان ارسالی کل خواهد بود. ضمنا جهت مقایسه عادلانه توان ارسالی کل در این حالت، برابر با توان ارسالی در حالت تک آنتن فرض شده است.

با استفاده از روابط (۴) و (۱۱) ظرفیت محرمانگی را می‌توان به صورت رابطه (۱۲) بدست آورد

$$C_s^{tb} \simeq \left[\log_2\left(\frac{|h_{0d}|^2 + |h_{1d}|^2}{|h_{0e}|^2 + |h_{1e}|^2}\right)\right]^+, \qquad (۱۲)$$

در این صورت در سیستم مدنظر احتمال قطع رابطه محرمانه به صورت رابطه (۱۳) قابل محاسبه خواهد بود

$$P_s^{tb} = P\left(C_s^{tb} < R\right) = P\left(\frac{|h_{0d}|^2 + |h_{1d}|^2}{|h_{0e}|^2 + |h_{1e}|^2} < 2^R\right), \qquad (۱۳)$$

جهت محاسبه احتمال فوق فرض کنید $X^{tb} = |h_{0d}|^2 + |h_{1d}|^2$ ، $Y^{tb} = |h_{0e}|^2 + |h_{1e}|^2$ و $Z^{tb} = X^{tb}/Y^{tb}$. در این صورت رابطه (۱۳) به صورت (۱۴) بازنویسی می‌گردد

$$\begin{aligned}P_s^{tb} &= P(Z^{tb} < 2^R) = F_{Z^{tb}}(2^R)\\ &= \int_0^\infty \int_0^{2^R y} f_{X^{tb}}(x) f_{Y^{tb}}(y)dxdy\\ &= \int_0^\infty F_{X^{tb}}(2^R y) f_{Y^{tb}}(y)dy.\end{aligned} \qquad (۱۴)$$

با این فرض که دو کانال مستقل باشند به سادگی می‌توان نشان داد که تابع چگالی احتمال $X^{tb}$ به صورت (۱۵) خواهد بود:

$$f_{X^{tb}}(x) = \begin{cases} \dfrac{x e^{-x/\lambda_d}}{\lambda_d^2} & \lambda_{0d} = \lambda_{1d} = \lambda_d \\ \dfrac{e^{x/\lambda_{1d}} - e^{x/\lambda_{1d}}}{\lambda_{0d} - \lambda_{1d}} e^{\frac{-x(\lambda_{0d} - \lambda_{1d})}{\lambda_{0d}\lambda_{1d}}} & \lambda_{0d} \neq \lambda_{1d} \end{cases} \qquad (۱۵)$$

که در آن $\lambda_{0d}$ و $\lambda_{1d}$ میانگین متغیرهای تصادفی $|h_{0d}|^2$ و $|h_{1d}|^2$ می‌باشند که این متغیرها با فرض کانال رایلی دارای توزیع نمایی هستند. با توجه به این که از جنبه میانگین بهره کانال، مسیرهای بین آنتن‌های یک فرستنده و یک گیرنده‌ی مشخص مشابه هستند، می‌توان از بخش اول رابطه (۱۵) جهت محاسبه تابع چگالی احتمال استفاده نمود. بنابراین تابع توزیع احتمال $X^{tb}$ به صورت رابطه (۱۶) محاسبه خواهد شد

$$F_{X^{tb}}(x) = \int_0^x \frac{t e^{-t/\lambda_d}}{\lambda_d^2} dt = 1 - \frac{x}{\lambda_d} e^{-x/\lambda_d} - e^{-x/\lambda_d}. \qquad (۱۶)$$

در نهایت با استفاده از روابط (۱۵) و (۱۶)، رابطه (۱۳) به صورت رابطه (۱۷) تکمیل و احتمال قطع ارتباط محرمانه از رابطه (۱۷) قابل محاسبه خواهد بود.

$$P_s^{tb}=\int_0^{\infty}\left(1-\frac{2^R y}{\lambda_d}e^{-\frac{2^R y}{\lambda_d}}-e^{-\frac{2^R y}{\lambda_d}}\right)\frac{ye^{-y/\lambda_e}}{\lambda_e^2}dy$$
$$=-\frac{e^{\frac{-y(\lambda_e 2^R+\lambda_d)}{\lambda_d\lambda_e}}}{\lambda_e}\left[\frac{-\lambda_d^2\lambda_e(3\lambda_e 2^R+\lambda_d)}{(\lambda_e 2^R+\lambda_d)^3}-\frac{2^R y^2}{\lambda_e 2^R+\lambda_d}\right.$$
$$\left.-\frac{\lambda_d y(3\lambda_e 2^R+\lambda_d)}{(\lambda_e 2^R+\lambda_d)^2}+(\lambda_e+\mathrm{y})e^{\frac{2^R y}{\lambda_d}}\right]_0^{\infty}$$
$$=1-\frac{\lambda_d^2(3\lambda_e 2^R+\lambda_d)}{(\lambda_e 2^R+\lambda_d)^3}. \qquad (۱۷)$$

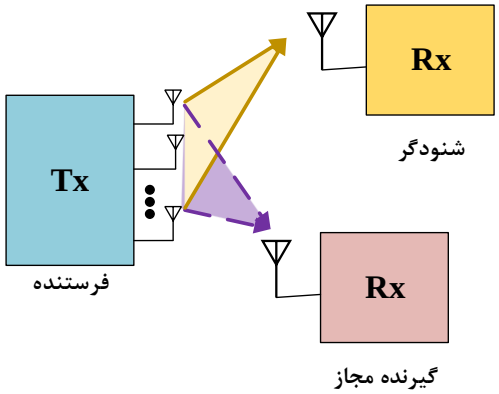
## ۴- مدل چندمسیره با نویز مصنوعی

در این مدل مطابق شکل (۳) فرض می‌شود فرستنده از $N$ آنتن جهت ارسال داده‌ها استفاده می‌کند. مدل کدکننده زمان-فضا به کار رفته در این سیستم در واقع مبتنی بر مدل تعمیم‌یافته الموتی است. همچنین فرستنده با ارسال نویز در زیرفضای صفر[۵] گیرنده مجاز به دنبال کاهش شانس فاش شدن اطلاعات است.در این سیستم سیگنال دریافتی گیرنده مجاز به صورت (۱۸) خواهد بود

$$r_d(t)=\mathbf{h}_d\mathbf{x}_0+n_{d,0}$$
$$r_d(t+T)=\mathbf{h}_d\mathbf{x}_1+n_{d,1} \qquad (۱۸)$$

که در آن $\mathbf{h}_d$ یک بردار $1\times N$ است که عناصر آن ضرایب مربوط به کانال بین هر یک از آنتن‌های فرستنده و گیرنده مجاز است. علاوه بر این $\mathbf{x}_i, i=0,1$ یک بردار $N\times 1$ حاوی سیگنال ارسالی در هر زمان است که از دو بخش تشکیل شده: بخش مربوط به اطلاعات و بخش مربوط به نویز مصنوعی. با استفاده از آن‌چه در [۱۶] ارائه شده است، جهت بیان این بردار نیاز به ماتریسی با ستون‌های متعامد و ابعاد $N\times N$ به نام $\mathbf{W}$ داریم که ستون اول آن را با استفاده از ضرایب کانال بدست آورده‌ایم. به عبارت دیگر $\mathbf{W}=[\mathbf{w}_1 \quad \mathbf{W}_2]$ که در آن $\mathbf{w}_1=\mathbf{h}_d^H/\|\mathbf{h}_d\|$ و $\mathbf{W}_2$ ماتریسی با ابعاد $N\times(N\text{-}1)$ می‌باشد که ستون‌های آن بر بردار $\mathbf{w}_1$ عمود هستند. با توجه به این‌که در مدل الموتی گیرنده داده ارسالی را با استفاده از دو سیگنال متوالی دریافتی با فاصله زمانی $T$ تخمین می‌زند، ما نیز می‌بایست بخش اطلاعات سیگنال را با همین خاصیت تعریف نماییم. از طرفی قصد ما این است که تا حد ممکن شنودگر را در دریافت پیام دچار مشکل نماییم، لذا بخش اطلاعات سیگنال را به ضرایب کانال بین فرستنده و گیرنده مجاز وابسته می‌کنیم و سپس نویز مصنوعی را در زیرفضای صفر گیرنده مجاز اضافه می‌کنیم.

با این توضیحات سیگنال فرستنده در زمان‌های $t$ و $t+T$ را به صورت رابطه (۱۹) تعریف می‌کنیم




**شکل (۳): مدل چندمسیره**

$$\mathbf{x}_0=\mathbf{w}_1(h_{0d}s_0+h_{1d}s_1)+\mathbf{W}_2\mathbf{v},$$
$$\mathbf{x}_1=\mathbf{w}_1(-h_{0d}s_1^*+h_{1d}s_0^*)+\mathbf{W}_2\mathbf{v}. \qquad (۱۹)$$

که در آن $s_i$ نمایان‌گر سمبل اطلاعات و $\mathbf{v}$ برداری $(N\text{-}1)\times 1$ است که عناصر آن متغیرهای تصادفی گوسی مختلط و **i.i.d** با واریانس $\sigma_v^2$ هستند. ضمنا همان طور که مشاهده می‌شود در این مدل نیز در طول دو اسلات زمانی، دو سمبل ارسال می‌شود. بنابراین نرخ کد همچنان برابر با یک باقی می‌ماند. این موضوع صرف نظر از تعداد آنتن‌هاست چرا که با افزایش تعداد آنتن‌ها، مطابق رابطه (۱۹) تعداد سمبل‌های ارسالی تغییر نمی‌کند و تنها طول $\mathbf{w}_1$ و مقادیر آن عوض می‌شود که این به معنی تغییر اندازه سیگنال ارسالی از هر آنتن است. جهت مقایسه عادلانه این روش با حالت قبل بایستی مجموع توان ارسالی آنتن‌ها در این حالت با حالت تک آنتن ($P_s^{\text{single}}$) برابر باشد. چون $\mathbf{W}$ ماتریسی متعامد است می‌توان توان ارسالی کل را به صورت (۲۰) محاسبه نمود

$$E_{total}^{Nbranch}=\left|h_{0d}\hat{s}_0+h_{1d}\hat{s}_1\right|^2E_s^{Nbranch}+(N-1)\sigma_v^2 \qquad (۲۰)$$

در حالی که $E_{total}^{Nbranch}$ توان کل ارسالی در مدل چندمسیره است و مقدار آن باید با حالت تک مسیره یکسان باشد. همچنین $E_s^{Nbranch}$ توان ارسالی مربوط به هر سمبل در حالت چندمسیره است. بر این اساس فرض شده که $s_i=\sqrt{E_s^{Nbranch}}\hat{s}_i$ و $|\hat{s}_i|=1$ می‌باشد. اگر نسبت کسری از توان که به بخش اطلاعات اختصاص داده شده به کل توان را با $\phi$ نمایش دهیم روابط زیر به سادگی قابل دستیابی خواهد بود.

$$\left|h_{0d}\hat{s}_0+h_{1d}\hat{s}_1\right|^2E_s^{Nbranch}=\phi E_{total}^{Nbranch},$$
$$\sigma_v^2=\frac{(1-\phi)E_{total}^{Nbranch}}{N-1}. \qquad (۲۱)$$

در بخش شبیه‌سازی جهت مقایسه عادلانه از این تخصیص توان استفاده خواهد شد.

در گیرنده مجاز با استفاده از رابطه (۱۸) و با توجه به این نکته که تمامی ستون‌های $\mathbf{W}_2$ بر $\mathbf{h}_d$ عمود است، سیگنال دریافتی را می‌توان به صورت (۲۲) بیان نمود

$$\begin{aligned} r_d(t) &= \|\mathbf{h}_d\|(h_{0d}s_0 + h_{1d}s_1) + n_{d,0} \\ r_d(t+T) &= \|\mathbf{h}_d\|(-h_{0d}s_1^* + h_{1d}s_0^*) + n_{d,1}. \end{aligned} \quad (۲۲)$$

چون گیرنده مورد استفاده در مدل پیشنهادی مشابه گیرنده الموتی عمل می‌کند، مطابق آن‌چه در [7] آمده و در رابطه (۸) هم بیان گردید، سیگنال‌های دریافتی در دو اسلات زمانی با هم ترکیب شده تا مطابق (۲۳) تخمینی از سیگنال دریافتی بدست آید

$$\begin{aligned} \tilde{s}_0 &= h_0^* r_d(t) + h_1 r_d^*(t+T) \\ &= \|\mathbf{h}_d\|\left(|h_{0d}|^2 + |h_{1d}|^2\right)s_0 + h_{0d}^* n_{d,0} + h_{1d} n_{d,1}^* \end{aligned} \quad (۲۳)$$

به صورت مشابه خواهیم داشت

$$\begin{aligned} \tilde{s}_1 &= h_1^* r_d(t) - h_0 r_d^*(t+T) \\ &= \|\mathbf{h}_d\|\left(|h_{0d}|^2 + |h_{1d}|^2\right)s_1 - h_{0d} n_{d,1}^* + h_{1d}^* n_{d,0} \end{aligned} \quad (۲۴)$$

همانطور که مشاهده می‌شود در این حالت نویز مصنوعی تأثیری بر سمبل‌های تخمین زده شده ندارد. اما در همین شرایط سیگنال دریافتی شنودگر به صورت (۲۵) خواهد بود

$$\begin{aligned} r_e(t) &= \mathbf{h}_e\mathbf{w}_1(h_{0d}s_0 + h_{1d}s_1) + \mathbf{h}_e\mathbf{W}_2\mathbf{v} + n_{e,0} \\ r_e(t+T) &= \mathbf{h}_e\mathbf{w}_1(-h_{0d}s_1^* + h_{1d}s_0^*) + \mathbf{h}_e\mathbf{W}_2\mathbf{v} + n_{e,1} \end{aligned} \quad (۲۵)$$

چون $\mathbf{W}_2$ و $\mathbf{h}_e$ متعامد نیستند نویز مصنوعی در گیرنده غیرمجاز حذف نمی‌گردد. علاوه بر این $\mathbf{h}_e\mathbf{w}_1 = \left(\mathbf{h}_e\mathbf{h}_d^H\right)/\|\mathbf{h}_d^H\|$. بنابراین در صورتی که گیرنده غیرمجاز از کانال بین فرستنده و گیرنده مجاز آگاه نباشد قادر به بازیابی اطلاعات ارسالی نخواهد بود. در این حالت تخمین سیگنال ارسالی حتی با اعمال ضریبی مشابه آن چه در گیرنده مجاز داشتیم به صورت (۲۶) خواهد بود، که در ادامه به وضوح خواهیم دید که شنودگر را به مشکل خواهد انداخت

$$\begin{aligned} \tilde{s}_0 &= \frac{(\mathbf{w}_1^H\mathbf{h}_e^H)}{|\mathbf{h}_e\mathbf{w}_1|^2}h_{0d}^* r_e(t) + \frac{(\mathbf{w}_1^T\mathbf{h}_e^T)}{|\mathbf{h}_e\mathbf{w}_1|^2}h_{1d} r_e^*(t+T) \\ \tilde{s}_1 &= \frac{(\mathbf{w}_1^H\mathbf{h}_e^H)}{|\mathbf{h}_e\mathbf{w}_1|^2}h_{1d}^* r_e(t) - \frac{(\mathbf{w}_1^T\mathbf{h}_e^T)}{|\mathbf{h}_e\mathbf{w}_1|^2}h_{0d} r_e^*(t+T) \end{aligned} \quad (۲۶)$$

دقت شود که در رابطه بالا ما ضرایب را نرمالیزه کرده‌ایم که البته در نتیجه تخمین هیچ تأثیری ندارد و این کار تنها به جهت ساده‌سازی انجام شده است. با استفاده از روابط (۲۵) و (۲۶) تخمین سمبل‌ها به صورت (۲۷) خواهد شد

$$\begin{aligned} \tilde{s}_0 &= \left(|h_{0d}|^2 + |h_{1d}|^2\right)s_0 + \frac{(\mathbf{w}_1^H\mathbf{h}_e^H)}{|\mathbf{h}_e\mathbf{w}_1|^2}h_{0d}^*(\mathbf{h}_e\mathbf{W}_2\mathbf{v} + n_{e,0}) \\ &+ \frac{(\mathbf{w}_1^T\mathbf{h}_e^T)}{|\mathbf{h}_e\mathbf{w}_1|^2}h_{1d}(\mathbf{h}_e^*\mathbf{W}_2^*\mathbf{v}^* + n_{e,1}^*) \end{aligned} \quad (۲۷)$$

و به طور مشابه رابطه زیر را بدست می آوریم

$$\begin{aligned} \tilde{s}_1 &= \left(|h_{0d}|^2 + |h_{1d}|^2\right)s_1 + \frac{(\mathbf{w}_1^H\mathbf{h}_e^H)}{|\mathbf{h}_e\mathbf{w}_1|^2}h_{1d}^*(\mathbf{h}_e\mathbf{W}_2\mathbf{v} + n_{e,0}) \\ &- \frac{(\mathbf{w}_1^T\mathbf{h}_e^T)}{|\mathbf{h}_e\mathbf{w}_1|^2}h_{0d}(\mathbf{h}_e^*\mathbf{W}_2^*\mathbf{v}^* + n_{e,1}^*). \end{aligned} \quad (۲۸)$$

از رابطه (۲۸) به وضوح می‌توان دریافت که با توجه به عدم حذف نویز مصنوعی و پیچیدگی خاصی که روش پیشنهادی در سیگنال دریافتی شنودگر ایجاد کرده است، شنودگر در تخمین اطلاعات با مشکل روبرو خواهد شد. حال می‌توان ظرفیت کانال گیرنده مجاز و شنودگر را محاسبه نمود. با استفاده از روابط (۲۲) و (۲۵) ظرفیت کانال گیرنده مجاز و ظرفیت کانال گیرنده شنودگر به ترتیب به صورت روابط (۲۹) و (۳۰) خواهد شد

$$C_d^{Nb} = \log_2\left(1 + \frac{\|\mathbf{h}_d\|^2\left(|h_{0d}|^2 + |h_{1d}|^2\right)^2 E_s^{Nbarnch}}{\left(|h_{0d}|^2 + |h_{1d}|^2\right)\sigma_n^2}\right), \quad (۲۹)$$

$$C_e^{Nb} = \log_2\left(1 + \frac{\left(|h_{0d}|^2 + |h_{1d}|^2\right)^2 E_s^{Nbranch}}{|z|^2\left(|h_{0d}|^2 + |h_{1d}|^2\right)\sigma_n^2 + |z|^2\left(|h_{0d}|^2 + |h_{1d}|^2\right)\|\mathbf{h}_e\mathbf{W}_2\|^2\sigma_v^2}\right). \quad (۳۰)$$

در حالی که $|z| = 1/|\mathbf{h}_e\mathbf{w}_1|$ می‌باشد. حال با استفاده از روابط (۲۹) و (۳۰) ظرفیت محرمانگی به صورت زیر محاسبه می‌گردد

$$C_s^{Nb} \simeq \left[\log_2\left(\frac{\|\mathbf{h}_d\|^2|\mathbf{h}_e\mathbf{w}_1|^{-2}\left(|h_{0d}|^2 + |h_{1d}|^2\right)\sigma_n^2}{\left(|h_{0d}|^2 + |h_{1d}|^2\right)\sigma_n^2} + \frac{\|\mathbf{h}_d\|^2|\mathbf{h}_e\mathbf{w}_1|^{-2}\left(|h_{0d}|^2 + |h_{1d}|^2\right)\|\mathbf{h}_e\mathbf{W}_2\|^2\sigma_v^2}{\left(|h_{0d}|^2 + |h_{1d}|^2\right)\sigma_n^2}\right)\right]^+. \quad (۳۱)$$

در بخش شبیه‌سازی در مورد رابطه فوق توضیحات بیشتری ارائه خواهد شد. در نهایت با استفاده از (۳۱) احتمال قطع ارتباط محرمانه نیز به صورت زیر محاسبه می‌گردد

$$\begin{aligned} P_s^{Nb} &= P(C_s^{Nb} < R) \\ &= P\left(\left[\log_2\left(\frac{\|\mathbf{h}_d\|^2|\mathbf{h}_e\mathbf{w}_1|^{-2}\left(|h_{0d}|^2 + |h_{1d}|^2\right)\sigma_n^2}{\left(|h_{0d}|^2 + |h_{1d}|^2\right)\sigma_n^2} + \frac{\|\mathbf{h}_d\|^2|\mathbf{h}_e\mathbf{w}_1|^{-2}\left(|h_{0d}|^2 + |h_{1d}|^2\right)\|\mathbf{h}_e\mathbf{W}_2\|^2\sigma_v^2}{\left(|h_{0d}|^2 + |h_{1d}|^2\right)\sigma_n^2}\right)\right]^+ < R\right) \end{aligned} \quad (۳۲)$$

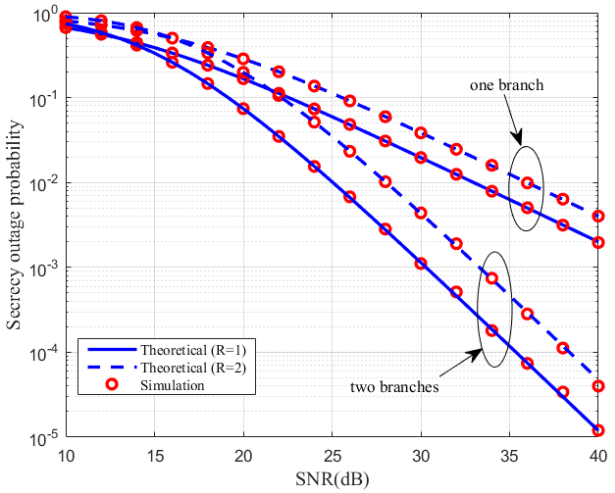
## ۵- نتایج شبیه‌سازی

در این بخش، عملکرد روش پیشنهادی و همچنین عملکرد حالت دو مسیره با داشتن نویز مصنوعی و بدون نویز مصنوعی،با استفاده از نتایج

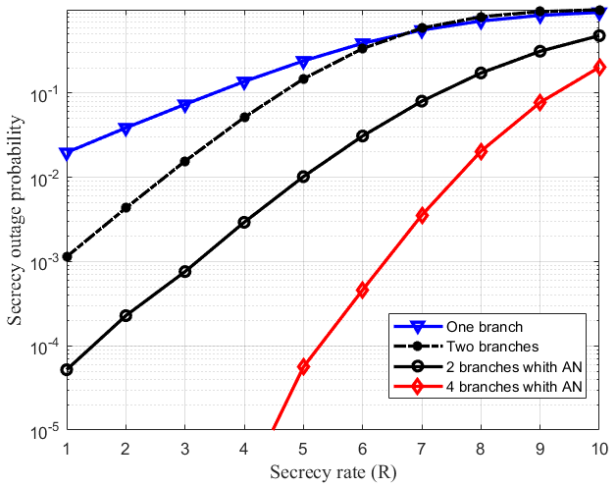
عددی و شبیه سازی‌ها مورد بررسی و مقایسه قرار می‌گیرد. برای تایید درستی تحلیل‌ها و روابط ریاضی بدست آمده، نتایج حاصل از شبیه‌سازی مونت-کارلو نیز آورده می شود.

ابتدا جهت نمایش صحت روابط تحلیلی و نمایش برتری روش الموتی بر ارسال مستقیم داده از نظر امنیت لایه فیزیکی ما مدل تک مسیره را با دومسیره در حالتی که $\lambda_{0e}=\lambda_{1e}=10dB$ و $\lambda_{1d}=\lambda_{0d}$ در شکل (۴) مقایسه کرده‌ایم. عملکرد در دو نرخ $R$=1 و $R$=2 نمایش داده شده است. در SNR های نسبتا بالا برتری روش الموتی بر مدل تک مسیره به وضوح قابل مشاهده است. ضمنا ما در شکل (۴) نتایج شبیه‌سازی و تئوری را در یک نمودار نمایش داده‌ایم تا صحت روابط بدست آمده در بخش‌های قبل نیز نشان دهیم.

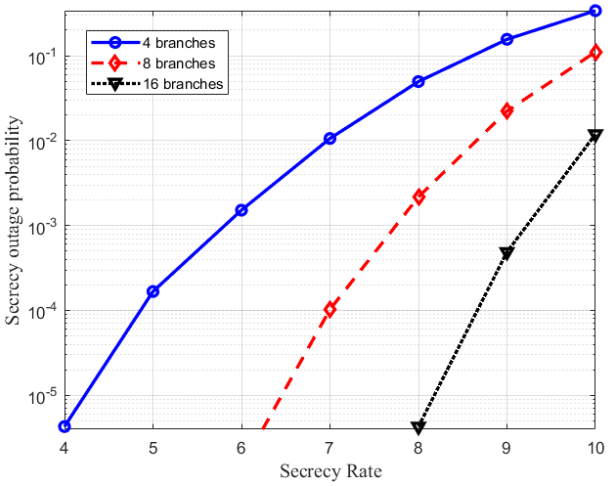
در شکل (۵) احتمال قطع ارتباط محرمانه را به ازای نرخ‌های مختلف شبیه‌سازی و مقایسه کرده‌ایم. مطابق شکل، شبیه‌سازی برای ارسال تک مسیره، دو مسیره، دومسیره با نویز مصنوعی و چهارمسیره با نویز مصنوعی انجام شده است. در این حالت فرض شده که $P_s^{*}=1$ , $\sigma_n^2=1$ . ضمنا در حالت‌هایی که بیش از یک آنتن در اختیار داریم، توان سمبل‌ها به گونه‌ای تنظیم شده که توان ارسالی کل با حالت تک‌مسیره یکسان گردد. همچنین در حالت-هایی که نویز مصنوعی داریم، ضریب تخصیص توان ۰٫۵ فرض شده است یعنی مطابق تعریفی که در بخش قبل انجام شد $\phi=0.5$ درنظر گرفته شده است. از طرفی برای کانال گیرنده مجاز $\lambda_{id}=30dB$ و برای کانال شنودگر $\lambda_{ie}=10dB$ فرض شده است. در این شکل نیز مشاهده می‌شود که مدل چهارآنتنه با نویز مصنوعی نسبت به سایرین از امنیت بالاتری برخوردار است.



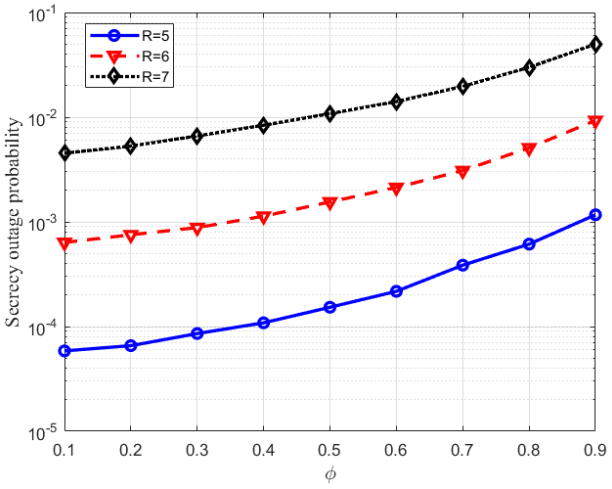

**شکل (۴): احتمال قطع ارتباط محرمانه به ازای SNRهای مختلف برای حالت تک مسیره و دو مسیره**




**شکل (۵): احتمال قطع ارتباط محرمانه به ازای نرخ‌های مختلف برای حالت تک مسیره، دو مسیره، دو مسیره با نویز مصنوعی و چهار مسیره با نویز**




**شکل (۶): احتمال قطع ارتباط محرمانه به ازای نرخ‌های مختلف و تعداد ۴، ۸ و ۱۶ مسیر(آنتن در فرستنده) به همراه نویز مصنوعی**




**شکل (۷): احتمال قطع ارتباط محرمانه به ازای ضرایب تخصیص توان متفاوت در حالت چهار مسیره (۴ آنتن در فرستنده) با نویز مصنوعی**

در شکل (۶) اثر افزایش تعداد آنتن‌ها نمایش داده شده است. در این شبیه‌سازی نیز $\lambda_{id}=30dB$ و $\lambda_{ie}=10dB$ فرض شده است. طبق روابط بدست آمده در رابطه (۳۱) مشاهده شد که احتمال قطع ارتباط محرمانه به نُرم بهره‌های مسیر سیگنال وابسته است. از طرفی با توجه به این که گیرنده مجاز از کانال بهتری برخوردار است، با افزایش تعداد آنتن نُرم بهره‌های مربوط به کانال گیرنده مجاز نسبت به نُرم کانال گیرنده غیرمجاز رشد بیشتری پیدا می‌کند و لذا افزایش تعداد آنتن شرایط را از لحاظ امنیت بهبود می‌بخشد. اگر بخواهیم این برتری را به گونه‌ای دیگر بیان کنیم باید گفت که صرف نظر از نویز مصنوعی، میانگین بهره‌های چند مسیر با تابع چگالی احتمال یکسان از بهره تنها یک مسیر با همان تابع چگالی بهتر خواهد بود و لذا این انتظار را از قبل داشتیم که با مدل پیشنهادی و کدکننده فضا-زمان پیشنهاد شده به ظرفیت امن بیشتری دست پیدا کنیم. البته بهای افزایش تعداد آنتن پیچیدگی بیشتر سیستم خواهد بود که باید آن را نیز در زمان استفاده عملی مدنظر قرار داد.

در شکل (۷) نیز تأثیر ضریب تخصیص بر میزان امنیت را بررسی کرده‌ایم. طبق رابطه (۳۱) این انتظار را از قبل داشتیم که با افزایش انرژی نویز مصنوعی، امنیت بیشتری را شاهد باشیم. البته به این قیمت که با فرض توان ارسالی ثابت، هر چه توان نویز مصنوعی را بیشتر کنیم ناچار به کاهش بیشتر انرژی سیگنال اطلاعات خواهیم بود. واضح است که کاهش انرژی سیگنال اطلاعات، احتمال خطا در تخمین اطلاعات ارسالی در گیرنده مجاز را افزایش می‌دهد و وقتی مجاز به کاهش این ضریب هستیم که از نظر انرژی محدودیت زیادی در فرستنده نداشته باشیم. چرا که در این حالت می‌توان با در نظر گرفتن توان کافی جهت بازیابی کم‌نقص اطلاعات در گیرنده مجاز، توان نویز مصنوعی را تا حد ممکن بالا برد و امکان بازیابی اطلاعات را برای شنودگر تا حد ممکن سخت‌تر کرد.

## ۶- نتیجه‌گیری

در این مقاله، روش جدیدی جهت دستیابی به امنیت بیشتر در سیستم‌های مبتنی بر مدل تعمیم‌یافته Alamouti که از کدینگ زمان-فضا جهت انتقال داده استفاده می‌کنند، معرفی و بررسی شد. در این روش علاوه بر استفاده از نویز مصنوعی، اثرات کانال در سیگنال ارسالی دخیل گردید تا شنودگر که از کانال گیرنده مجاز بی‌اطلاع است در تخمین اطلاعات دچار مشکل گردد. از طرفی با افزایش تعداد آنتن‌ها و تعمیم روابط مربوط به ارسال داده، همچنین ارائه کدکننده فضا-زمان متناسب با سیستم پیشنهادی، نشان دادیم چگونه با افزایش تعداد آنتن‌ها می‌توان به امنیت بالاتری دست یافت. ضمنا روابط تحلیلی در هر بخش ارائه گردید و در نهایت با شبیه‌سازی حالات تک-مسیره، دو مسیره و چندمسیره برتری روش پیشنهادی نسبت به سایر روش‌ها را نشان دادیم. همچنین اثر تغییر برخی پارامترها مانند ضریب تخصیص توان به سیگنال و نویز نیز مورد بررسی قرار گرفت.

## مراجع


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

[۲] جواد زراعتکارمقدم, حمید فرخی، ناصر ندا، "بررسی تأثیر فاصله بین آنتنها در فرستنده و گیرنده بر روی ظرفیت کانال MIMO،" مجله مهندسی برق و الکترونیک ایران، دوره ۱۳، شماره ۲، صفحات ۱۱-۱۸، ۱۳۹۵

[3] بیانی فر مهدی، رضوی زاده سید محمد. "بررسی کارایی توان کانال تداخلی رله چند ورودی-چند خروجی انبوه ."مجله مهندسی برق و الکترونیک ایران، دوره ۱۴، شماره ۲، صفحات ۱۱-۲۲، ۱۳۹۶

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

[5] T. Liu and S. Shamai, “A note on the secrecy capacity of the multiple-antenna wiretap channel,” IEEE Trans. Inf. Theory, vol. 55, no. 6, pp. 2547–2553, 2009.

[6] V. Tarokh, N. Seshadri, and A. R. Calderbank, “Space-time codes for high data rate wireless communication: Performance criterion and code construction,” IEEE Trans. Inf. Theory, vol. 44, no. 2, pp. 744–765, 1998.

[7] S. M. Alamouti, “A simple transmit diversity technique for wireless communications,” IEEE J. Sel. Areas Commun., vol. 16, no. 8, pp. 1451–1458, 1998.

[8] M. Ahmed and L. Bai, “Space Time Block Coding Aided Physical Layer Security in Gaussian MIMO Channels,” 2017 14th Int. Bhurban Conf. Appl. Sci. Technol., pp. 805–808, 2017.

[9] T. Allen, J. Cheng, and N. Al-Dhahir, “Secure space-time block coding without transmitter CSI,” IEEE Wirel. Commun. Lett., vol. 3, no. 6, pp. 573–576, 2014.

[10] X. Li, R. Fan, X. Ma, J. An, and T. Jiang, “Secure Space-Time Communications over Rayleigh Flat Fading Channels,” IEEE Trans. Wirel. Commun., vol. 15, no. 2, pp. 1491–1504, 2016.

[11] S. S. Chauhan, P. Verma, M. Mathur, M. Agarwal, and T. Gupta, “Physical layer security of MIMO STBC over Rayleigh fading channels in the presence of channel estimation error,” Optik (Stuttg)., vol. 127, no. 19, pp. 7625–7630, 2016.

[12] T. Allen, A. Tajer, and N. Al-Dhahir, “Secure Alamouti MAC Transmissions,” IEEE Trans. Wirel. Commun., vol. 16, no. 6, pp. 3674–3687, 2017.

[13] J. M. Hamamreh, E. Guvenkaya, T. Baykas, and H. Arslan, “A practical physical-layer security method for precoded OSTBC-based systems,” IEEE Wirel. Commun. Netw. Conf. WCNC, vol. 2016-Septe, no. Wcnc, 2016.

[14] M. R. Abedi, N. Mokari, H. Saeedi, and H. Yanikomeroglu, “Robust Resource Allocation to Enhance Physical Layer Security in Systems With Full-Duplex Receivers: Active Adversary,” IEEE Trans. Wirel. Commun., vol. 16, no. 2, pp. 885–899, 2017.

[15] C. Liu and R. Malaney, “Location-Based Beamforming and Physical Layer Security in Rician Wiretap Channels,” IEEE Trans. Wirel. Commun., vol. 15, no. 11, pp. 7847–7857, 2016.

[16] R. Negi, “Secret Communication using Artificial Noise,” pp. 1906–1910, 2005.

## زیرنویس‌ها

[1] Diversity
[2] Space Time Block Code (STBC)
[3] Secrecy Capacity
[4] Secrecy Outage Probability
[5] Null