

## فرا سطح اطلاعات آشوبناک برای ارتباط امن مستقیم لایه فیزیکی

### چکیده

امنیت اطلاعات بی سیم با گسترش روزافزون سیستم‌های ارتباطی بی سیم پخش، توجه زیادی را به خود جلب کرده است. استفاده از سیستم‌های آشوبناک برای روش‌های ارتباطی امن، با توجه به مزایای ذاتی آنها از جمله تصادفی بودن بالا و حساسیت به شرایط اولیه، به یک حوزه تحقیقاتی برجسته تبدیل شده است. با این حال، رویکردهای مبتنی بر آشوب موجود معمولاً نیاز دارند که گیرنده‌های مشروع به پارامترهای سیستم آشوبناک به عنوان کلیدهای رمزگشایی دسترسی داشته باشند، که اغلب شامل عملیات پیچیده در سطح دیجیتال است. در این مطالعه، ما یک طرح ارتباطی امن لایه فیزیکی جدید ارائه می‌دهیم که به یک فرا سطح اطلاعات متکی است که ویژگی‌های بازتاب محلی آن به صورت پویا توسط الگوهای آشوبناک تعدیل می‌شود. رویکرد ما یک روش تولید الگوی مختلط "یکباره" را معرفی می‌کند که همزمان امنیت ارتباطات و کارایی انتقال را تضمین می‌کند. مهمتر از همه، طرح پیشنهادی ما الزام سختگیرانه برای عملیات رمزگشایی را حذف می‌کند و گیرنده مشروع را قادر می‌سازد تا مستقیماً به داده‌های اصلی دسترسی پیدا کند در حالی که گیرنده‌های نامشروع سیگنال‌های رمزگذاری شده آشوبناک را دریافت می‌کنند. این رویکرد مزایای قابل توجهی را نشان می‌دهد که شامل امنیت بالا، معماری ساده و سازگاری ذاتی رو به عقب است. استراتژی نوآورانه ما، چشم‌انداز جدیدی را برای پیشرفت سیستم‌های ارتباطی بی سیم امن نسل بعدی فراهم می‌کند.

در چشم‌انداز ارتباطی که به سرعت در حال تحول است، حفظ امنیت اطلاعات به ویژه با پذیرش فراگیر سیستم‌های ارتباطی بی سیم پخش 1، به طور فزاینده‌ای حیاتی شده است.

برای شبکه‌های بی سیم نسل بعدی (G6)، یک روند قابل توجه، پیشرفت محیط‌های رادیویی هوشمند است که به صورت پویا به شرایط متغیر پاسخ می‌دهند و می‌توانند عملکرد شبکه و تجربه کاربر 2 را بهینه کنند. هسته اصلی این الگو، ادغام سطوح هوشمند قابل پیکربندی مجدد 3 است. این پلتفرم‌های متامتریال قابل برنامه‌ریزی 4، که به عنوان متاسطوح اطلاعاتی 5 نیز شناخته می‌شوند، شامل آرایه‌های دو بعدی از عناصر زیر طول موج هستند که سیگنال‌های الکترومغناطیسی را بر اساس الگوهای کدگذاری دیجیتال، مانند هم فاز یا خارج از فاز در حالت دودویی، منعکس می‌کنند. این قابلیت پویا، تنظیمات بلادرنگ برای انتشار سیگنال را امکان‌پذیر می‌کند و منجر به بهبود قدرت سیگنال، کاهش تداخل و افزایش بهره‌وری کلی انرژی می‌شود. با این حال، این پیشرفت همچنین چالش‌های جدیدی را در امنیت لایه فیزیکی ایجاد می‌کند که ناشی از استفاده‌های مخرب بالقوه از این فناوری‌ها 6-9 است. نکته قابل توجه این است که همانطور که در ادامه نشان داده خواهد شد، ادغام فرا سطح اطلاعات می‌تواند یک راه حل جذاب برای ارتباطات امن نیز ارائه دهد، به ویژه هنگامی که در کنار سیستم‌های آشوبناک به کار گرفته شود. آشوب، یک پدیده فراگیر در طبیعت، خود را از طریق حساسیت نمایی در تکامل یک سیستم غیرخطی به شرایط اولیه نشان می‌دهد. این امر منجر به پیش‌بینی ناپذیری الگوریتمی بلندمدت و رفتاری

شبهه به تصادفی بودن می‌شود<sup>10</sup>. به دلیل این ویژگی‌های متمایز، سیستم‌های آشوبناک به کانون توجه در تحقیقات در مورد رمزگذاری اطلاعات و ارتباطات امن تبدیل شده‌اند<sup>11</sup>. افزایش علاقه به این حوزه به دهه 1990 برمی‌گردد، که با کشف اساسی همگام‌سازی آشوب<sup>12</sup> مشخص شد و پایه و اساس روش‌های مختلف ارتباطی امن ریشه در آشوب را بنا نهاد.

سیستم‌های ارتباطی اولیه مبتنی بر آشوب بر تشخیص منسجم<sup>13-15</sup> متکی بودند، که در آن سیستم‌های آشوبناک سیگنال‌های آشوبناک آنالوگ یا دیجیتال را برای انتقال ایمن تولید می‌کردند. در این سیستم‌ها، گیرنده یک کپی هماهنگ از سیگنال آشوبناک ایجاد می‌کرد تا داده‌های منتقل شده را بازیابی کند. یکی از تکنیک‌های قابل توجه، کلیدزنی تغییر آشوب<sup>14</sup> بود که از دو سیستم آشوبناک مستقل در فرستنده استفاده می‌کرد. این روش یک دنباله دیجیتال دودویی را با استفاده از یک سوئیچ تغییر در سیگنال منتقل شده رمزگذاری می‌کرد. در گیرنده، سیگنال دریافتی دودویی را با خودهمزمان را هدایت می‌کرد و نماد انتقال را با تشخیص انسجام بین سیگنال دریافتی و سیگنال خروجی آنها تعیین می‌کرد. رویکرد دیگر، که به عنوان ماسک آشوبناک افزایشی<sup>16</sup> شناخته می‌شود، شامل معرفی یک سیگنال آشوبناک افزایشی به یک سیگنال داده آنالوگ برای ایجاد سیگنال منتقل شده بود. گیرنده سیگنال آشوبناک را از طریق هماهنگ‌سازی آشوب بازسازی کرد و اطلاعات آنالوگ را با کم کردن سیگنال آشوبناک از سیگنال دریافتی استخراج نمود.

در حالی که این روش در ایمن‌سازی در برابر استراق سمع کنندگانی که از پارامترهای سیستم آشوبناک آگاهی ندارند، مؤثر بود، اما به دلیل تغییرات توان در سیگنال ارسالی، خطرات امنیتی بالقوه‌ای داشت. در روشی متفاوت به نام مدولاسیون آشوبناک<sup>17</sup>، سیگنال آنالوگ برای انتقال مستقیماً به یک سیستم آشوبناک تزریق می‌شد و فضای فاز یا پارامترهای آن را تغییر می‌داد تا یک سیگنال آشوبناک حاوی اطلاعات آنالوگ تولید کند. اگرچه این رویکرد عملکرد بهتری در مقایسه با کلیدزنی تغییر آشوبناک و پوشش آشوبناک افزایشی ارائه می‌دهد، اما به شدت به طراحی دقیق کنترل‌کننده گیرنده متکی بود.

برای غلبه بر محدودیت‌های ذکر شده، توجه تحقیقاتی قابل توجهی به سیستم‌های ارتباطی مبتنی بر آشوب که از تشخیص غیرمنسجم استفاده می‌کنند، معطوف شده است. یک پیشرفت کلیدی در این حوزه، معرفی کلیدزنی تغییر آشوبناک دیفرانسیلی<sup>18</sup> است. در این طرح، هر دوره نماد به دو اسلات تقسیم می‌شود که شامل یک سیگنال آشوبناک مرجع و یک سیگنال داده است. این مورد اخیر با ضرب یک دنباله دودویی {1، -1} در یک سیگنال مرجع آشوبناک تأخیری به دست می‌آید. یک سوئیچ تغییر بین سیگنال مرجع و سیگنال داده برای تولید سیگنال انتقال متناوباً عمل می‌کند. در گیرنده، عملیات همبستگی بر روی سیگنال دریافتی و نسخه‌های تأخیری آن انجام می‌شود و به دنبال آن تمایز آستانه برای

به دست آوردن نتیجه رمزگشایی شده انجام می‌شود. این رویکرد به دلیل انتقال همزمان سیگنال مرجع آشوبناک و سیگنال داده، در برابر اعوجاج‌های خطی و غیرخطی در کانال، مقاومت نشان داده است و بر حساسیت مشاهده شده در کلیدزنی تغییر آشوبناک غلبه می‌کند. با توجه به عملکرد برجسته آن، بررسی نسخه‌های مختلف بهبود یافته کلیدزنی تغییر آشوبناک تفاضلی همچنان نقطه کانونی در حوزه تحقیقات ارتباطات مبتنی بر آشوب است. اکثر روش‌های ارتباطی امن مبتنی بر آشوب، رمزگذاری را در سطح سیگنال با استفاده از مدارهای آشوبناک به کار می‌گیرند. با این حال، در سال‌های اخیر، بررسی جدیدی از تکنیک‌های ارتباطی امن مبتنی بر آشوب در حوزه فرکانس رادیویی (RF) انجام شده است که شامل رمزگذاری داده‌های منتقل شده با استفاده از آرایه‌های آنتن است. به طور خاص، یک مطالعه اخیر، مدولاسیون فاز آشوبناک را در یک سیستم آرایه آنتن با مدولاسیون زمانی 19 پیشنهاد کرده است. این رویکرد نوآورانه، توالی‌های آشوبناک را در حوزه RF برای رمزگذاری توالی‌های متن ساده به کار می‌گیرد و به طور مؤثر آسیب‌پذیری‌های امنیتی مرتبط با سیستم‌های آرایه آنتن با مدولاسیون زمانی را برطرف می‌کند. نکته قابل توجه این است که این روش نیاز به مازول‌های مدولاسیون باند پایه را از بین می‌برد و منجر به یک معماری سخت‌افزاری ساده می‌شود.

به طور کلی، روش‌های ارتباطی امن مبتنی بر آشوب موجود، یک الزام مشترک برای گیرنده دارند که پارامترهای سیستم آشوبناک را برای رمزگشایی داشته باشد. این پارامترها به عنوان کلید در نظر گرفته می‌شوند و کانال‌های انتقال امن را ضروری می‌سازند. در نتیجه، این روش‌ها در حوزه رمزنگاری کلاسیک قرار می‌گیرند.

تاکنون، این حوزه شاهد کاوش محدودی در مورد روش‌های ارتباطی امن لایه فیزیکی بوده است که نیاز به کلیدهای مخفی را از بین می‌برد. برای پرداختن به این شکاف، در این مطالعه، یک طرح جدید مبتنی بر فراسطح اطلاعات آشوبناک معرفی می‌کنیم که بدون تکیه بر کلیدهای مخفی، به طور ایمن عمل می‌کند. این رویکرد نوآورانه، با تولید فعال نویز آشفته‌ی متمایز برای شنودکنندگان بر اساس جهت‌گیری‌هایشان، یک لایه‌ی امنیتی منحصر به فرد ایجاد می‌کند و در نتیجه امنیت کلی ارتباط را افزایش می‌دهد. نکته‌ی مهم این است که گیرنده‌ی قانونی می‌تواند مستقیماً داده‌های با کیفیت بالای مورد نظر را بدون انجام هیچ عملیات رمزگشایی دریافت کند. علاوه بر این، طرح پیشنهادی بسیار سازگار است و می‌تواند به عنوان یک مازول انتقال امن مستقل در کنار فرستنده، بدون ایجاد اختلال در تنظیمات موجود فرستنده‌ی اصلی و گیرنده مستقر شود.

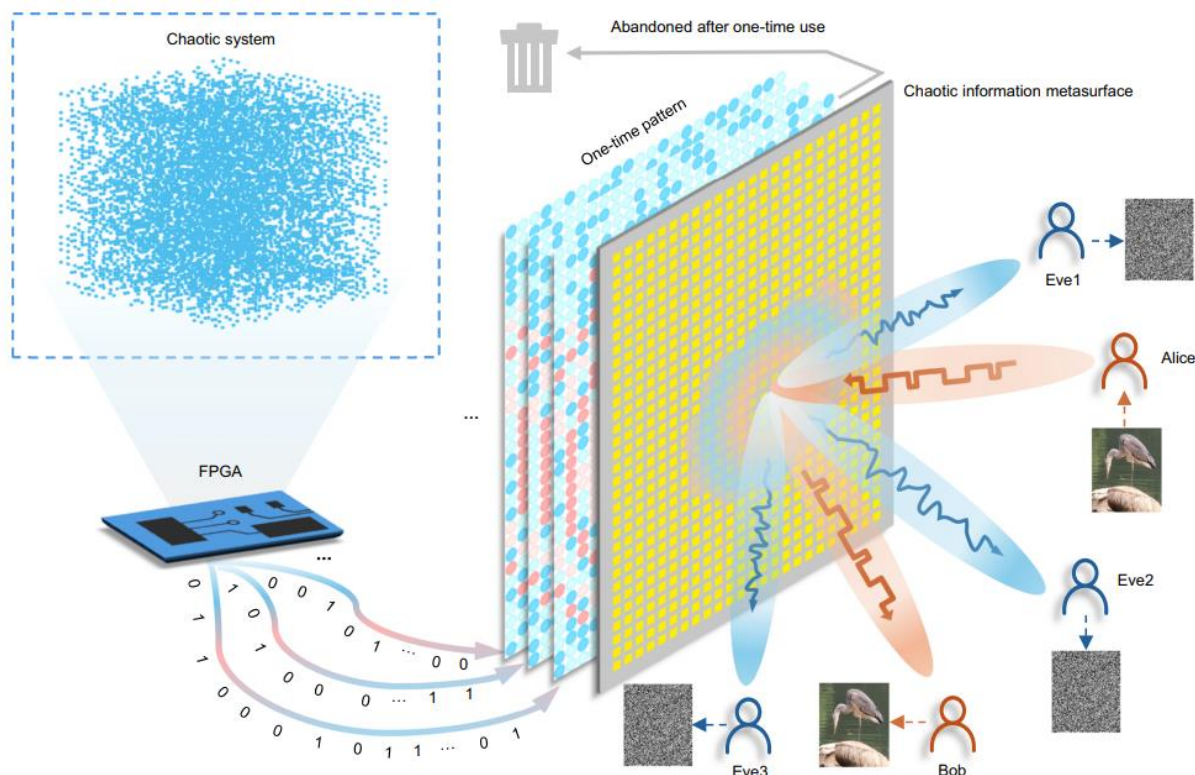
## نتایج

مدل سیستم

همانطور که در شکل 1 نشان داده شده است، ما سناریوی را بررسی می‌کنیم که در آن یک فرستنده قانونی (که به عنوان آلیس شناخته می‌شود) قصد دارد اطلاعات را به صورت بی‌سیم به یک گیرنده قانونی (که به عنوان باب شناخته می‌شود) ارسال کند. در همین حال، یک یا چند استراق سمع کننده بالقوه (که به عنوان ایو برچسب گذاری شده‌اند) وجود دارند که سعی در استراق سمع ارتباط بین آلیس و باب دارند. رویکردهای سنتی انتقال امن لایه فیزیکی، که ریشه در روش‌های حوزه مکانی دارند، از فرستنده‌های چند آنتنه برای تحقق شکل‌دهی پرتو امن استفاده می‌کنند. هدف این استراتژی به حداکثر رساندن انرژی سیگنال دریافتی توسط گیرنده قانونی و در عین حال به حداقل رساندن انرژی دریافتی توسط استراق سمع کنندگان در جهت‌های دیگر است. هدف، تقویت اختلاف بین کانال قانونی (آلیس به باب) و کانال شنود (آلیس به ایو) با افزایش نسبت سیگنال به نویز (SNR) در گیرنده قانونی و سرکوب آن در گیرنده‌های استراق سمع کننده است. با این حال، آسیب‌پذیری‌ها زمانی ایجاد می‌شوند که استراق سمع کنندگان از گیرنده‌های بسیار حساس استفاده می‌کنند یا قدرت نویز ذاتی کانال کم است که به طور بالقوه امنیت انتقال را به خطر می‌اندازد.

طرح انتقال امن لایه فیزیکی پیشنهادی ما از متاسطح اطلاعات برای ایجاد یک کانال ارتباطی بی‌سیم با پراکندگی معکوس استفاده می‌کند. این متاسطح، اطلاعات آشوبناک را به حوزه فضا-زمانی تزریق می‌کند و در عین حال توزیع فضایی انرژی الکترومغناطیسی را تعدیل می‌کند. در این رویکرد، فرستنده سیگنال‌های رمزگذاری نشده را مستقیماً به متاسطح ارسال می‌کند که از الگوهای کدگذاری آشوبناک مختلط بهینه شده برای هدایت کارآمد انرژی به سمت گیرنده مشروع استفاده می‌کند. برای افزایش امنیت، ما یک تکنیک سوئیچینگ "الگوی یک‌باره" را مستقل از دوره نماد باند پایه معرفی می‌کنیم که از نقشه‌های آشوبناک برای تولید الگوهای کدگذاری منحصر به فرد برای هر نماد انتقال در صورت نیاز استفاده می‌کند. این الگوها سیگنال را در استراق سمع کنندگان، که در جهات ناخواسته قرار دارند، از نویز تصادفی غیرقابل تشخیص می‌کنند. نکته مهم این است که سوئیچینگ "الگوی یک‌باره" می‌تواند مقاومت قوی در برابر حملات متن ساده شناخته شده را تضمین کند. برای مکان‌های فرستنده (آلیس) و گیرنده (باب)، متاسطح اطلاعات به دو بخش تقسیم می‌شود: متا (شامل متاتم‌های NmetaA) و متاB (شامل متاتم‌های NmetaB). بخش متا مسئول پیاده‌سازی الگوی کدگذاری متمرکز استاتیک CmetaA است که توزیع فضایی انرژی الکترومغناطیسی را تعدیل می‌کند و SNR بالایی را برای گیرنده مشروع، باب، تضمین می‌کند. در مقابل، متاB از الگوهای کدگذاری آشوبناک پویا CmetaB(t) برای تزریق اطلاعات آشوبناک استفاده می‌کند و رمزگذاری فضایی-زمانی را در لایه فیزیکی فراهم می‌کند. تحت این چارچوب، پاسخ‌های واسطه‌شده توسط متاسطح برای پیوندهای آلیس-متاسطح-باب و آلیس-متاسطح-ایو را می‌توان به ترتیب به صورت  $HA \rightarrow E(t)$  و  $HA \rightarrow B(t)$  بیان کرد (به نمادگذاری در بخش «روش‌ها» مراجعه کنید). نکته قابل توجه این است که وقتی  $NmetaA = 0$  باشد، الگوی کدگذاری متاسطح کاملاً توسط آشوب هدایت می‌شود و تصادفی بودن بالایی را نشان می‌دهد. برعکس، وقتی  $NmetaB = 0$  باشد، الگوی کدگذاری کاملاً متمرکز می‌شود و انرژی سیگنال و SNR باب را به حداکثر می‌رساند. نکته مهم این است که از آنجایی که الگوی کدگذاری متمرکز استاتیک (metaA) اعمال می‌شود و مؤلفه آشوبناک (metaB) تأثیر

حداقلی بر گیرنده قانونی دارد، باب سیگنال را به شکل رمزگذاری نشده آن دریافت می کند. این امر نیاز به تبادل کلید لایه فیزیکی بین آلیس و باب را از بین می برد و فرآیند انتقال امن را ساده کرده و خطر رهگیری کلید را کاهش می دهد. علاوه بر این، آلیس و باب می توانند بدون هیچ گونه تغییری در مدولاسیون خود، به استفاده از تجهیزات فرستنده و گیرنده موجود خود ادامه دهند. و الگوریتم های دمدولاسیون، که سازگاری بی نقص این طرح را با تنظیمات سخت افزاری فعلی برجسته می کند.



انتقال امن اطلاعات از آلیس به باب از طریق متاسطح اطلاعات آشوبناک در دو مرحله کلیدی رخ می دهد. اولاً، آلیس، فرستنده، مدولاسیون باند پایه مرسوم را با استفاده از مدارهای RF استاندارد انجام می دهد. در مرحله بعد، متاسطح اطلاعات، سوئیچینگ الگوی کدگذاری آشوبناک را اعمال می کند، که از رویکرد "الگوی یک باره" پیروی می کند که مدولاسیون فضا-زمانی را القا می کند. هنگامی که آلیس از تکنیک های مدولاسیون باند پایه، مانند کلیدزنی تغییر فاز (PSK)، استفاده می کند، دامنه و فاز سیگنال های دریافت شده در جهات مختلف تحت تأثیر نماد باند پایه منتقل شده و الگوهای کدگذاری متاسطح قرار می گیرند. این الگوهای کدگذاری بهینه شده، حداقل نویز را در محل باب تضمین می کنند، در حالی که پاسخ های دامنه-فاز بسیار تصادفی را در تمام جهات ناخواسته دیگر ایجاد می کنند و به طور مؤثر سیگنال را رمزگذاری کرده و انتقال را ایمن می کنند.

**تولید توالی آشوبناک**

الگوهای کدگذاری در فواصل زمانی گسسته سوئیچ می‌شوند. به طور خاص، برای مجموعه‌ای از لحظات زمانی گسسته  $t_n$  و مجموعه‌ای از مقادیر آشوبناک گسسته  $x_i$ ، الگوهای کدگذاری فراسطحی با استفاده از نگاشت آشوبناک  $f_{chaos}$  و تابع نگاشت الگوی کدگذاری  $g$  تولید می‌شوند.

$$x_{i+1} = f_{chaos}(x_i) \quad (1)$$

$$e_n = x_{768n}, x_{768n-1}, x_{768n-2}, \dots, x_{768n-767} \quad (2)$$

$$C_{metaB}(t_n) = g(x_{f_n}) \quad (3)$$

که در آن  $C_{metaB}(t_1)$ ،  $C_{metaB}(t_2)$ ، ...،  $C_{metaB}(t_n)$  نشان دهنده توالی‌های الگوی کدگذاری آشوبناک هستند. در این مطالعه، ما از نگاشت لجستیک تک‌بعدی رایج استفاده می‌کنیم که به صورت زیر بیان می‌شود:  $x_{i+1} = \mu x_i(1 - x_i)$ ، که در آن  $x_i \in (0, 1)$  و  $\mu \in (0, 4)$  یک پارامتر سیستم است. برای اطمینان از اینکه دنباله  $\{x_i\}$  رفتار آشوبی پایدار نشان می‌دهد، پارامتر  $\mu$  باید در محدوده  $(3.5699456, 4]$  قرار گیرد، به استثنای فواصل ایزوله خاص که به عنوان "جزایر پایداری" شناخته می‌شوند. در سیستم فراسطح آشوبناک ما، هم پارامتر  $\mu$  و هم مقدار اولیه  $x_1$  هر "الگوی یک‌باره" به طور تصادفی در محدوده‌های معتبر انتخاب می‌شوند. پس از آن، این دنباله‌های آشوبناک کوانتیزه می‌شوند تا دنباله‌های دودویی یک‌بعدی تولید شوند که سپس برای تشکیل الگوهای کدگذاری فراسطح دوبعدی 1 بیتی ترکیب می‌شوند. برای دستیابی به این هدف، ما از روش بیت کم‌اهمیت (LSB) برای نگاشت دنباله‌های آشوبناک به ... استفاده می‌کنیم. الگوهای کدگذاری فراسطح دوبعدی. هر گروه  $x_{en}$  شامل ۷۶۸ عنصر است که مربوط به یک الگوی کدگذاری فراسطحی است.  $C_{metaB}(t_n)$ . هر مقدار آشوبناک  $x_i$  در نمادگذاری ممیز شناور به صورت  $x_i = 0.a_1a_2\dots a_k$  نمایش داده می‌شود، که در آن  $a_k$  نشان دهنده کم ارزش‌ترین بیت است. با ارزیابی برابری  $a_k$ ، دنباله آشوبناک به یک دنباله دودویی تبدیل می‌شود که سپس برای تولید یک الگوی کدگذاری دوبعدی برای فراسطح کوانتیزه شده ۱ بیتی استفاده می‌شود.

جزئیات بیشتر دنباله آشوبناک در یادداشت تکمیلی ۱ ارائه شده است.

تکنیک‌های مبتنی بر آشوب مزایای قابل توجهی نسبت به روش‌های تولید اعداد شبه تصادفی مرسوم، به ویژه از نظر غیرقابل پیش‌بینی بودن و حساسیت به شرایط اولیه، ارائه می‌دهند.

به عنوان مثال، الگوریتم Mersenne Twister 21-23، که معمولاً در برنامه‌های نرم‌افزاری برای تولید اعداد شبه تصادفی استفاده می‌شود، می‌تواند به سرعت توالی‌های بسیار طولانی تولید کند. با این حال، این الگوریتم خطرات امنیتی را در سناریوهایی مانند ارتباطات رمزگذاری شده ایجاد می‌کند. همانطور که استراق سمع‌کنندگان می‌توانند با تحلیل معکوس بخش‌هایی با طول مشخص، توالی‌های آینده را پیش‌بینی کنند [21]. اگر چنین روش‌های تولید اعداد شبه تصادفی در سیستم

پیشنهادی استفاده شوند، یک استراق سمع کننده می تواند به طور بالقوه بخش هایی از کدگذاری فراسطح را از طریق تخمین کانال بازسازی کند و متعاقباً حالت های کدگذاری آینده را پیش بینی کند و در نتیجه امنیت سیستم را به خطر بیندازد. برای کاهش این آسیب پذیری های امنیتی، نداشت آشوبناک یک رویکرد امیدوارکننده برای تولید اعداد شبه تصادفی با کیفیت بالا در ارتباطات امن ارائه می دهد. ویژگی های کلیدی آن - حساسیت به مقادیر اولیه، غیرقابل پیش بینی بودن و غیرخطی بودن - توانایی آن را در حفاظت از اطلاعات افزایش می دهد.

## الگوریتم تولید الگوی مختلط

همانطور که قبلاً بحث شد، الگوهای کدگذاری متاسطح تولید شده از طریق نگاشت و کوانتیزاسیون آشوبناک، درجه بالایی از تصادفی بودن را نشان می دهند. با این حال، هنگامی که  $N_{metaA} = 0$  باشد، که نشان می دهد الگوی کدگذاری متاسطح کاملاً آشوبناک است، عملکرد لینک ارتباط بی سیم backscatter بدتر می شود و منجر به انتقال ناکارآمد به سمت گیرنده مشروع، باب، می شود. برعکس، هنگامی که  $N_{metaB} = 0$  باشد، الگوی کدگذاری متاسطح کاملاً متمرکز می شود و کیفیت انتقال بالا را در محل باب تضمین می کند، اما فاقد تصادفی بودن لازم برای جلوگیری از استراق سمع است.

بنابراین، یافتن تعادل بهینه بین اثربخشی انتقال و امنیت از طریق تخصیص و توزیع مناسب الگوهای کدگذاری آشوبناک بسیار مهم است. برای پرداختن به این چالش، ما یک الگوریتم تولید الگوی کدگذاری مختلط مبتنی بر وزن پیشنهاد می کنیم. در مرحله اول، برای موقعیت های فرستنده و گیرنده مشروع داده شده، الگوی کدگذاری متمرکز استاتیک  $C_{metaA}$  با استفاده از الگوریتم اصلاح شده 24،25 Gerchberg-Saxton (GS) تولید می شود. در مرحله بعد، وزن نرمال شده هر متا-اتم را محاسبه می کنیم تا سهم آن را در پاسخ الکترومغناطیسی در موقعیت باب کمی کنیم. به طور خاص، برای یک متا-اتم عمومی  $n$  ام، وزن نرمال شده  $W_n$  به صورت زیر تعریف می شود:

$$W_n = \frac{Re(H_{A \rightarrow M \rightarrow B})Re(H_{A \rightarrow n \rightarrow B}) + Im(H_{A \rightarrow M \rightarrow B})Im(H_{A \rightarrow n \rightarrow B})}{\max_{i=1,2,\dots,N} ([Re(H_{A \rightarrow M \rightarrow B})Re(H_{A \rightarrow i \rightarrow B}) + Im(H_{A \rightarrow M \rightarrow B})Im(H_{A \rightarrow i \rightarrow B})])} \quad (4)$$

که در آن  $N$  نشان دهنده تعداد کل متا-اتم ها است، و

$$H_{A \rightarrow M \rightarrow B} = \sum_{n \in metaA \& metaB} \underbrace{h_{A \rightarrow n \rightarrow B} \exp(j \angle_n^A)}_{H_{A \rightarrow n \rightarrow B}} \quad (5)$$

در اینجا،  $H_{A \rightarrow M \rightarrow B}$  و  $H_{A \rightarrow n \rightarrow B}$  به ترتیب نشان دهنده پاسخ های واسطه شده توسط متاسطح کل آرایه متاسطح و متا-اتم  $n$  ام هستند، زمانی که فقط الگوی کدگذاری متمرکز استاتیک  $C_{metaA}$  اعمال می شود. در الگوریتم تولید الگوی

مختلط ما، ابتدا وزن نرمال شده برای هر متا-اتم را محاسبه می‌کنیم. در مرحله بعد، برای متا-اتم  $m$ ، کدگذاری مربوط به الگوی فوکوس در صورتی حفظ می‌شود که وزن نرمال شده  $W_n$  از یک آستانه از پیش تعیین شده  $\tau$  تجاوز نکند، در غیر این صورت با یک الگوی آشوبناک جایگزین می‌شود. این فرآیند منجر به ایجاد الگوهای کدگذاری مختلط می‌شود، همانطور که در شکل a2 و b نشان داده شده است. جزئیات بیشتر در مورد الگوریتم تولید الگوی مختلط در یادداشت تکمیلی 2 ارائه شده است. در مرحله بعد، مقادیر  $N_{metaA}$  و  $N_{metaB}$  باید متعادل شوند. برای دستیابی به این هدف، ضریب اختلاط  $\alpha = N_{metaA} = \delta N_{metaA} + N_{metaB}$  را معرفی می‌کنیم. برای ارزیابی اولیه تأثیر ضریب اختلاط  $\alpha$  بر خواص میدان پراکندگی، یک سیستم مختصات استوانه‌ای  $\phi$ ،  $\theta$ ،  $r$  را در نظر می‌گیریم که در مبدا متاسطح متمرکز شده است، همانطور که در شکل c2 نشان داده شده است. آنتن منبع در (1.15 متر، 0 درجه، 0 متر) قرار دارد، در حالی که موقعیت تمرکز هدف در (3 متر، 0 درجه، -0.34 متر) است. با استفاده از معادلات 11 و 12 از بخش "روش‌ها"، توزیع دامنه نرمال شده میدان پراکندگی را بر روی نیمکره‌ای که شامل موقعیت تمرکز هدف است و در مبدا متمرکز شده است، محاسبه می‌کنیم. این نتایج، که مربوط به ضرایب اختلاط مختلف است، همانطور که در شکل d2 نشان داده شده است، نشان می‌دهد که الگوهای کدگذاری مختلط، که با ضرایب اختلاط مناسب تولید می‌شوند، می‌توانند انرژی الکترومغناطیسی را به طور مؤثر بر روی ناحیه هدف متمرکز کنند، حتی در حالی که بخشی از متاتم‌ها برای تزریق اطلاعات آشفته استفاده می‌شوند. در سراسر مقاله، ما انحراف معیار نرمال شده دامنه نویز نسبت به سیگنال ارسالی را به صورت  $\sigma$  تعریف می‌کنیم.

شکل e2 نتایج عددی را بر حسب نمودارهای صورت فلکی سیگنال در زوایای آزمون مختلف ارائه می‌دهد، که در آن ضریب اختلاط  $\alpha$  روی 0.469،  $\sigma$  روی  $2 \times 10^{-3}$  تنظیم شده است و آنتن منبع یک سیگنال مدوله شده PSK8 با فرکانس حامل 2.47 گیگاهرتز ارسال می‌کند. نتایج نشان می‌دهد که با یک ضریب اختلاط مناسب انتخاب شده، متاسطح اطلاعات آشوبناک می‌تواند سیگنال‌ها را در مناطق غیر هدف رمزگذاری کند و در عین حال کیفیت سیگنال را در منطقه هدف حفظ کند، زیرا متاتم‌ها در بخش دینامیکی طبق نگاشت آشوبناک تغییر می‌کنند.

نتایج شبیه‌سازی بیشتر در یادداشت‌های تکمیلی 3 و 4 ارائه شده است.

در ادامه، ما تجزیه و تحلیل دقیق‌تری را در سطح سیستم ارتباطی با در نظر گرفتن پارامترهای مختلفی مانند ضرایب اختلاط، دامنه نویز و موقعیت آنتن انجام می‌دهیم. این ارزیابی ما را قادر می‌سازد تا ضریب اختلاط بهینه را در شرایط مختلف شناسایی کنیم.

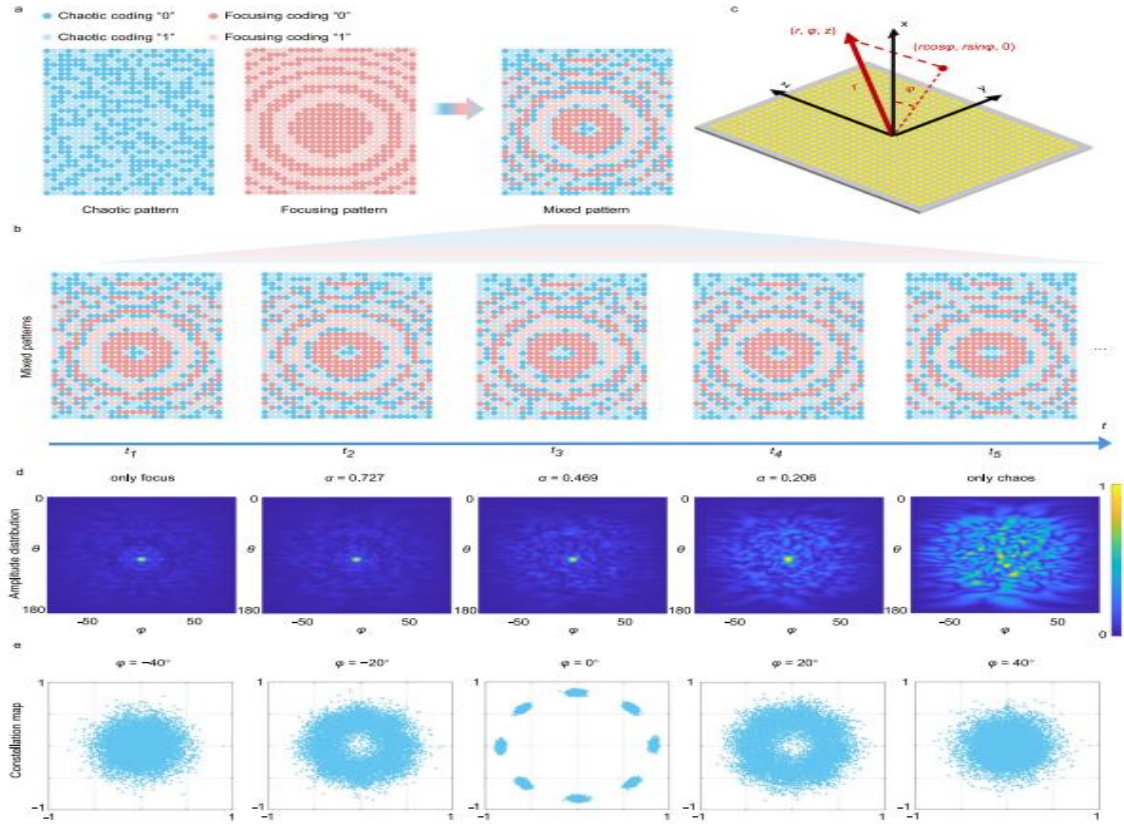
نتایج شبیه‌سازی



با پیروی از اصول ذکر شده، ما شبیه‌سازی‌های عددی را بر اساس MATLAB انجام می‌دهیم، همانطور که در شکل 3 نشان داده شده است. به طور خاص، ما عملکرد متاسطح اطلاعات آشوبناک پیشنهادی را که در 2.47 گیگاهرتز کار می‌کند، در یک کانال تک ورودی-تک خروجی (SISO) ارزیابی کردیم. در شبیه‌سازی‌ها، آنتن فرستنده به طور مداوم یک سیگنال مدوله شده PSK8 متشکل از 104 نمونه را به گیرنده قانونی ارسال می‌کند، در حالی که متاسطح اطلاعات آشوبناک  $24 \times 32$  با الگوهای کدگذاری آشوبناک برای مدوله کردن ویژگی‌های کانال بارگذاری می‌شود.

با توجه به اینکه آنتن‌هایی که در آزمایش‌های بعدی استفاده کردیم، شدت تابش تقریباً یکنواختی را در محدوده 0 تا 180 درجه نشان می‌دهند، الگوهای تابش فرستنده و گیرنده روی مقادیر ثابت تنظیم می‌شوند. در شکل‌های  $a3$  و  $b3$ ، فرستنده در (1.15 متر، 0 درجه، 0 متر) قرار دارد و گیرنده قانونی در (3 متر، 0 درجه، -0.34 متر) قرار دارد. در شکل‌های  $c3$  و  $d3$ ، فرستنده در (0.75 متر، 0 درجه، -0.57 متر) قرار دارد و گیرنده قانونی در (3 متر، 0 درجه، 0 متر) قرار دارد. برای ارزیابی مستقیم تأثیر فراسطح اطلاعات آشوبناک بر ویژگی‌های کانال مدولاسیون، نرخ خطای بیت (BER) را بررسی می‌کنیم و فرض می‌کنیم که گیرنده می‌تواند به طور ایده‌آل تداخل ناشی از نویز کانال افزایشی را هنگام تعیین ناحیه‌ی تصمیم‌گیری با استفاده از سیگنال مرجع فیلتر کند. برای ارزیابی تأثیر فراسطح اطلاعات آشوبناک بر عملکرد ارتباطی در مکان‌های مختلف گیرنده، آنتن‌های گیرنده در (3 متر،  $\phi$ ، -0.34 متر) در شکل  $a3$  و (3 متر،  $\phi$ ، 0 متر) در شکل  $c3$  قرار گرفته‌اند، و زاویه آزیموت  $\phi$  از -90 درجه تا 90 درجه با افزایش 1 درجه نمونه‌برداری شده است. در اینجا، انحراف معیار نرمال‌شده دامنه نویز  $\sigma$  روی  $2 \times 103$  تنظیم شده است. این شبیه‌سازی رابطه بین BER و زاویه آزیموت  $\phi$  را برای آستانه‌های مختلف  $\tau$  و عوامل اختلاط  $\alpha$  اعمال شده بر فراسطح اطلاعات آشوبناک بررسی می‌کند. برای مقایسه، ما همچنین نتایج شبیه‌سازی را برای مواردی ارائه می‌دهیم که فراسطح فقط از الگوی کدگذاری متمرکز در هر زیرنمودار استفاده می‌کند. نتایج نشان می‌دهد که فراسطح اطلاعات آشوبناک، هنگامی که با ضریب اختلاط مناسب  $\alpha$  پیکربندی شود، به طور مؤثر کیفیت ارتباط را برای کاربران غیرمجاز در سایر مکان‌های مکانی کاهش می‌دهد، در حالی که کیفیت ارتباط رضایت‌بخش را برای گیرنده‌های مشروع حفظ می‌کند. انتخاب  $\alpha$  بسیار مهم است: ضریب اختلاط بزرگتر، کیفیت ارتباط را برای گیرنده مشروع افزایش می‌دهد، اما اثر تداخل را بر گیرنده‌های غیرمجاز کاهش می‌دهد و بر بده بستان فوق‌الذکر تأکید می‌کند. آستانه  $\tau$  و ضریب اختلاط مربوطه  $\alpha$  از طریق جاروب پارامتر انتخاب می‌شوند.

به طور خاص، سیستم اطلاعات آشوبناک، آستانه‌های کاندید را در فواصل یکنواخت نمونه‌برداری می‌کند و بالاترین آستانه‌ای را انتخاب می‌کند که BER گیرنده مشروع را زیر حداکثر حد قابل تحمل نگه می‌دارد. این فرآیند مقادیر نهایی  $\tau$  و  $\alpha$  را به دست می‌دهد. جزئیات بیشتر در یادداشت تکمیلی 2 ارائه شده است.

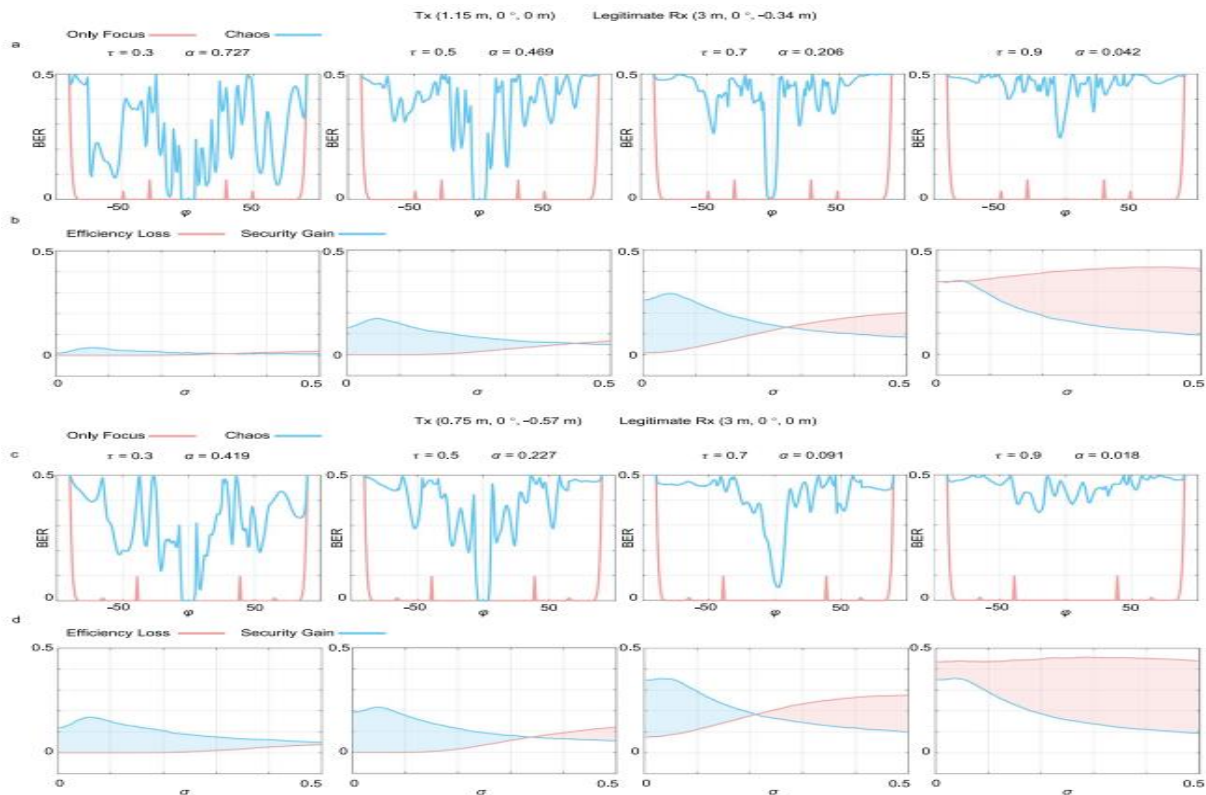


شکل ۲ | تولید الگوهای کدگذاری مختلط. (الف) تولید یک الگوی مختلط با ترکیب یک الگوی آشوبناک با یک الگوی کانونی. (ب) الگوهای کدگذاری مختلط در گام‌های زمانی مختلف. (ج) سیستم مختصات استوانه‌ای استفاده شده. (د) توزیع دامنه نرمال شده میدان‌های پراکندگی برای مقادیر مختلف فاکتورهای اختلاط.  $\theta$  و  $\phi$  به ترتیب نشان‌دهنده زاویه قطبی و زاویه آزیموتال نقاط روی نیمکره مشاهده هستند. (ه) نتایج عددی نمودارهای صورت فلکی سیگنال‌های دریافتی در زوایای آزیموت مختلف، برای یک فاکتور اختلاط  $\alpha = 0.469$  فرکانس عملیاتی ۲.۴۷ گیگاهرتز است و انحراف معیار نرمال شده دامنه نویز  $\sigma$  روی  $2 \times 10^{-3}$  تنظیم شده است.

علاوه بر این، دامنه نویز بر پاسخ کلی کانال تأثیر می‌گذارد و انتخاب ضریب اختلاط را نیز به سطح نویز وابسته می‌کند. برای ارزیابی تأثیر عوامل اختلاط مختلف تحت انحراف معیار نرمال شده متغیر دامنه نویز  $\sigma$ ، فرآیند شبیه‌سازی که قبلاً شرح داده شده است را اعمال می‌کنیم. برای تعیین کمیت مناسب تأثیر فراسطح اطلاعات آشوبناک بر کارایی و امنیت سیستم‌های ارتباطی، دو معیار کلیدی را معرفی می‌کنیم: کاهش کارایی  $L_e$  و افزایش امنیت  $G_s$  که به صورت زیر تعریف می‌شوند:

$$L_e = BER_{chaos}(\varphi_{legitimate\ receiver}) - BER_{only\ focus}(\varphi_{legitimate\ receiver}) \quad (6)$$

$$G_s = \min_{\varphi_1}(BER_{chaos}(\varphi_1)) - \min_{\varphi_2}(BER_{only\ focus}(\varphi_2)) \quad (7)$$



شکل 3 | نتایج شبیه‌سازی انتقال امن لایه فیزیکی بر اساس فراسطح اطلاعات آشوبناک. الف) BER برای گیرنده‌ها در موقعیت‌های مختلف، زمانی که فرستنده و گیرنده قانونی به ترتیب در (1.15 متر، 0 درجه، 0 متر) و (3 متر، 0 درجه، 3)

-0.34 متر) قرار دارند. ب) تلفات کارایی و افزایش امنیت مربوطه به عنوان تابعی از  $\sigma$ ، انحراف معیار نرمال شده دامنه نویز، زمانی که فرستنده در (1.15 متر، 0 درجه، 0 متر) قرار دارد و گیرنده قانونی در (3 متر، 0 درجه، -0.34 متر) قرار دارد. ج) د) همانطور که در پنل‌های (الف) و (ب) به ترتیب نشان داده شده است، اما برای فرستنده و گیرنده قانونی که به ترتیب در (0.75 متر، 0 درجه، -0.57 متر) و (3 متر، 0 درجه، 0 متر) قرار دارند.

$$\left| \varphi_1 - \varphi_{\text{legitimate user}} \right| > 10^\circ, \quad \left| \varphi_2 - \varphi_{\text{legitimate user}} \right| > 10^\circ \quad (8)$$

در اینجا،  $\delta\varphi_{\text{chaos}}$  و  $\delta\varphi_{\text{only focus}}$  BER به ترتیب نشان‌دهنده BER در زاویه  $\phi$  هستند، زمانی که سطح متا با الگوی کدگذاری ترکیبی و الگوی کدگذاری متمرکز بارگذاری می‌شود.  $\phi_{\text{legitimate user}}$  به زاویه آزمون که گیرنده مشروع در آن قرار دارد اشاره دارد. تلفات کارایی Le تأثیر الگوی کدگذاری ترکیبی را بر راندمان ارتباط برای گیرنده مشروع اندازه‌گیری می‌کند. بهره امنیتی Gs توانایی الگوی کدگذاری ترکیبی را در کاهش ارتباط برای استراق سمع‌کنندگانی که فراتر از یک انحراف زاویه‌ای خاص از موقعیت گیرنده مشروع قرار دارند، کمی می‌کند. تلفات کارایی و بهره امنیتی شبیه‌سازی شده

برای  $\sigma$  های مختلف به ترتیب در شکل‌های b3 و d3 برای سناریوهای شکل a3 و c3 نشان داده شده است. به طور کلی، با افزایش انحراف معیار نرمال دامنه نویز  $\sigma$ ، GS ابتدا افزایش و سپس کاهش می‌یابد، در حالی که Le به طور کلی یک روند صعودی تدریجی را نشان می‌دهد. یک استثنا در نمودار چهارم شکل b3،  $d$  ( $\tau = 0.9$ ) رخ می‌دهد که در آن تنها تعداد محدودی از الگوهای کدگذاری متمرکز استاتیک توسط الگوریتم GS تولید می‌شوند. در نتیجه، BER برای گیرنده‌های قانونی از 0.3 فراتر می‌رود و ارتباط قابل اعتماد را حتی در سطوح نویز پایین‌تر تقریباً غیرممکن می‌کند.

## نتایج تجربی

برای اعتبارسنجی یافته‌های نظری و عددی خود، آزمایش‌های تجربی را در یک محیط داخلی واقعی با استفاده از دستگاه متاسطح اطلاعات آشوبناک و یک رادیوی تعریف‌شده توسط نرم‌افزار (Ettus)

(USRP X310) برای انتقال و دریافت سیگنال انجام می‌دهیم. همانطور که در شکل a4 نشان داده شده است، متاسطح اطلاعات آشوبناک با یک متاسطح قابل برنامه‌ریزی 1 بیتی  $32 \times 24$  عنصری که در حدود 2.47 گیگاهرتز کار می‌کند، پیاده‌سازی شده است. متا-اتم  $54 \times 54$  میلی‌متر مربع اندازه دارد و از دو لایه زیرلایه تشکیل شده است، همانطور که در شکل b264 نشان داده شده است. لایه بالایی از F4B

(با گذردهی نسبی 2.55 و تانژانت تلفات 0.0019) ساخته شده است، در حالی که لایه پایینی FR4 (با گذردهی نسبی 4.4 و تانژانت تلفات 0.03) است. هر متا-اتم توسط یک دیود SMP1345-079LF مثبت-ذاتی-منفی (PIN) کنترل می‌شود که می‌تواند بین حالت‌های «روشن» و «خاموش» تغییر حالت دهد. حداقل فاصله سوئیچینگ برای هر دیود PIN تقریباً 2.5 میکروثانیه است. همانطور که در شکل c264 نشان داده شده است، هر متا-اتم یک تغییر فاز محلی در موج الکترومغناطیسی منعکس شده در فرکانس کاری ایجاد می‌کند، با اختلاف فاز تقریباً 180 درجه بین حالت‌های «روشن» و «خاموش»، در حالی که دامنه‌های تقریباً یکسانی را حفظ می‌کند. در نتیجه، این پلتفرم قابل برنامه‌ریزی را می‌توان به عنوان یک متا-سطح تغییر فاز 1 بیتی ایده‌آل تقریب زد. این پلتفرم توسط یک کامپیوتر میزبان از طریق یک آرایه گیت قابل برنامه‌ریزی میدانی (FPGA) کنترل می‌شود که ارسال فرمان را با استفاده از یک سیگنال ساعت 50 مگاهرتز هماهنگ می‌کند و الگوهای کدگذاری را از کامپیوتر میزبان با استفاده از پروتکل TCP/IP بارگذاری می‌کند. نتایج آزمایش تحت پیکربندی‌های مختلف در شکل‌های d-g4 ارائه شده است تا عملکرد متاسطح اطلاعات آشوبناک را در جنبه‌های مختلف تأیید کند. در این آزمایش‌ها، فرستنده یک سیگنال مدوله شده با PSK8 ارسال می‌کند که توسط متاسطح اطلاعات آشوبناک مدوله شده و توسط آنتن‌های مستقر در مکان‌های مختلف دریافت می‌شود. ابتدا، همانطور که در شکل‌های d4 و e نشان داده شده است، اطلاعات وضعیت کانال (CSI) و نمودارهای صورت فلکی کاربر قانونی و استراق سمع‌کننده‌ها را هنگامی که متاسطح با الگوهای آشوبناک مختلط و فقط الگوهای متمرکز بارگذاری شده است، به ترتیب مقایسه می‌کنیم. به طور خاص، در شکل d4، فرستنده و کاربر قانونی به ترتیب در (1.15 متر، 0 درجه، 0 متر) و (3 متر، 0 درجه، -0.34 متر) قرار دارند. ضریب اختلاط  $\alpha$  متاسطح اطلاعات آشوبناک روی 0.469 تنظیم شده است. در شکل e4، فرستنده و کاربر قانونی

به ترتیب در (0.75 متر، 0 درجه، -0.57 متر) و (3 متر، 0 درجه، 0 متر) قرار دارند و ضریب اختلاط  $\alpha$  روی 0.227 تنظیم شده است. در همین حال، دو شنودگر در انحرافات آزمون 20 درجه و 40 درجه نسبت به کاربر قانونی برای هر دو شکل d4 و e قرار دارند. اندازه‌گیری‌های CSI نشان می‌دهد که وقتی از کدگذاری قانونی استفاده می‌شود، سیستم می‌تواند قدرت سیگنال کاربر قانونی را به طور قابل توجهی افزایش دهد در حالی که قدرت سیگنال شنودگر را کاهش می‌دهد. با این حال، از آنجایی که الگوی کدگذاری کنترلی متاسطح ایستا است، فاز شنودگر CSI نسبتاً پایدار باقی می‌ماند. در این حالت، نمودار صورت فلکی شنودگر هنوز در محدوده تحمل نویز دمودولاسیون PSK8 قرار دارد. در مقابل، هنگامی که از الگوی آشوبی مختلط استفاده می‌شود، متاسطح با الگوهای آشوبی پویا کار می‌کند و باعث ایجاد CSI متغیر مکانی-زمانی می‌شود که مسئول رمزگذاری انتخابی کانال شنودگر است. در نتیجه، فاز CSI شنودگر با گذشت زمان به سرعت تغییر می‌کند، اما فاز CSI کاربر مشروع نسبتاً پایدار می‌ماند. بنابراین، کاربر مشروع می‌تواند نمودارهای صورت فلکی PSK8 قابل تشخیص را دریافت کند، اما شنودگر در انجام آن شکست می‌خورد. نتایج فوق تفاوت‌ها و مزایای متاسطح اطلاعات آشوبی ما را در مقایسه با استفاده از الگوهای کدگذاری قانونی نشان می‌دهد. برای کمی‌سازی بیشتر عملکرد متاسطح اطلاعات آشوبی، نتایج انتقال اطلاعات برای گیرنده‌ها در موقعیت‌های مختلف هنگام استفاده از الگوهای آشوبی مختلط در شکل‌های f4 و g4 ارائه شده است. در اینجا، نتیجه انتقال اطلاعات با عملیات XOR را مشخص می‌کنیم که در صورت متفاوت بودن بیت دریافت از بیت ارسال، 1 و در غیر این صورت 0 می‌شود. در شکل f4، فرستنده و گیرنده‌ها به ترتیب در (1.15 متر، 0 درجه، 0 متر) و (3 متر،  $\phi$ ، -0.34 متر) قرار گرفته‌اند، و زاویه آزمون  $\phi$  گیرنده قانونی روی 0 درجه تنظیم شده است، که با پیکربندی استفاده شده در شبیه‌سازی‌های عددی سازگار است. ضریب اختلاط  $\alpha$  فراسطح اطلاعات آشوبناک روی 0.469 تنظیم شده است. در شکل g4، فرستنده و گیرنده‌ها به ترتیب در (0.75 متر، 0 درجه، -0.57 متر) و (3 متر،  $\phi$ ، 0 متر) قرار گرفته‌اند و ضریب اختلاط  $\alpha$  روی 0.227 تنظیم شده است. علاوه بر این، اندازه‌گیری‌های BER مربوطه در جدول 1 ارائه شده است. قبل از پایان این بخش، بحث مختصری در مورد نرخ انتقال اوج سیستم ارائه می‌دهیم. نرخ انتقال اوج به حداقل فاصله سوئیچینگ متاسطح محدود می‌شود تا از قابلیت‌های رمزگذاری سیستم پیشنهادی به طور کامل استفاده شود. به طور خاص، دوره نماد سیستم باید طولانی‌تر از حداقل فاصله سوئیچینگ متاسطح باشد تا اطمینان حاصل شود که متاسطح می‌تواند تداخل کانال متفاوتی را برای هر نماد از طریق سوئیچینگ الگو فراهم کند. حداقل فاصله سوئیچینگ متاسطح 2.5 میکروثانیه است و سیستم از مدولاسیون PSK8 استفاده می‌کند. بنابراین، نرخ انتقال نماد اوج  $1 \times \text{نماد } 2:5 = 4 \times 105$  نماد هرتز است و نرخ انتقال بیت اوج مربوطه  $3 \times 4 \times 105$  نماد هرتز  $= 1:2 \times 106$  بیت هرتز است.

## بحث

متاسطح اطلاعات آشوبناک پیشنهادی، یک طرح ارتباطی امن لایه فیزیکی جدید را معرفی می‌کند که بدون کلیدهای مخفی عمل می‌کند. فرستنده از یک آنتن جهت‌دار که به سمت متاسطح هدف‌گیری شده است، استفاده می‌کند و نشأت

اطلاعات را از طریق مسیر مستقیم بین فرستنده و گیرنده به حداقل می‌رساند. هنگامی که استراق سمع‌کنندگان، با استفاده از آنتن‌های معمولی یا متاسطح‌های اطلاعات 7، در یک طرف متاسطح آشوبناک و فرستنده قرار می‌گیرند، توانایی آنها در رهگیری سیگنال‌ها به طور قابل توجهی مختل می‌شود و امنیت را تضمین می‌کند. با این حال، اگر استراق سمع‌کننده بین فرستنده و متاسطح اطلاعات آشوبناک باشد، ممکن است مقداری نشت اطلاعات رخ دهد. برای کاهش این، فرستنده باید نزدیک به متاسطح قرار گیرد و ناحیه قابل رهگیری سیگنال مستقیم را کاهش دهد. در مواردی که این ناحیه به اندازه کافی کوچک باشد، می‌توان آن را ایزوله یا تحت نظارت قرار داد تا از دسترسی استراق سمع‌کنندگان به آن جلوگیری شود. به طور خلاصه، طرح ما با اطمینان از اینکه استراق سمع‌کنندگان نویز آشوبناک را دریافت می‌کنند در حالی که گیرنده مشروع به طور مستقیم و بدون رمزگشایی به داده‌های اصلی دسترسی پیدا می‌کند، امنیت را افزایش می‌دهد. این سیستم با تنظیمات موجود بسیار سازگار است و اعتبارسنجی تجربی با یک فراسطح که در حدود 2.47 گیگاهرتز کار می‌کند، اثربخشی آن را تأیید می‌کند. این راه‌حل نوآورانه، مسیری امیدوارکننده برای پیشبرد ارتباطات بی‌سیم امن در شبکه‌های نسل بعدی ارائه می‌دهد.

## روش‌ها

### مدل سیگنال فراسطح اطلاعات آشوبناک

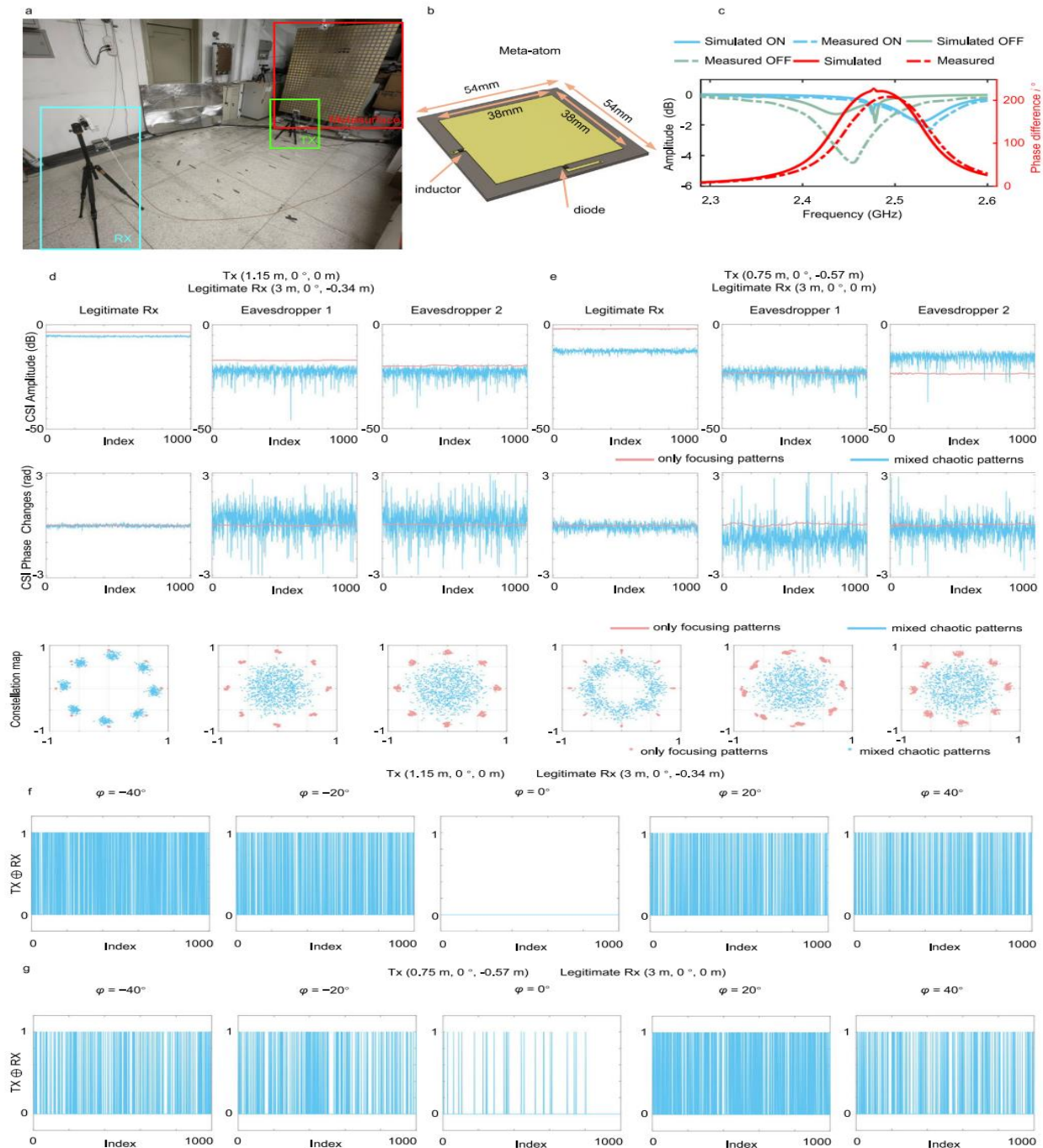
در یک مدل کانال معمولی با نویز افزایشی، سیگنال‌های دریافت شده توسط گیرنده قانونی، باب، و شنودگر، ایو، را می‌توان به صورت زیر بیان کرد7:

$$y(\mathbf{r}_B; t) = \sqrt{P_A} x_A(t) H_{A \rightarrow B} + \sqrt{P_A} x_A(t) h_{A \rightarrow B} + \epsilon_B \quad (9)$$

$$y(\mathbf{r}_E; t) = \sqrt{P_A} x_A(t) H_{A \rightarrow E} + \sqrt{P_A} x_A(t) h_{A \rightarrow E} + \epsilon_E \quad (10)$$

$$H_{A \rightarrow B}(t) = \sum_{n \in \text{meta}A} \underbrace{\frac{\sqrt{G_A(\mathbf{r}_n) G_n(\mathbf{r}_B, \mathbf{r}_A) G_B(\mathbf{r}_n) \Delta}}{(4\pi)^2 |\mathbf{r}_A - \mathbf{r}_n| |\mathbf{r}_B - \mathbf{r}_n|} \exp(jk(|\mathbf{r}_A - \mathbf{r}_n| + |\mathbf{r}_B - \mathbf{r}_n|)) \exp(j \varnothing_n^A)}_{h_{A \rightarrow n \rightarrow B}} + \sum_{n \in \text{meta}B} \underbrace{\frac{\sqrt{G_A(\mathbf{r}_n) G_n(\mathbf{r}_B, \mathbf{r}_A) G_B(\mathbf{r}_n) \Delta}}{(4\pi)^2 |\mathbf{r}_A - \mathbf{r}_n| |\mathbf{r}_B - \mathbf{r}_n|} \exp(jk(|\mathbf{r}_A - \mathbf{r}_n| + |\mathbf{r}_B - \mathbf{r}_n|)) \exp(j \varnothing_n^B(t))}_{h_{A \rightarrow n \rightarrow B}} \quad (11)$$





شکل ۴ | اعتبارسنجی تجربی انتقال امن لایه فیزیکی مبتنی بر متاسطح اطلاعات آشوبناک. الف) نمونه اولیه متاسطح و چیدمان آزمایشی. ب) هندسه متاسطح. ج) پاسخ بازتاب متاسطح. د) نتایج اندازه‌گیری شده نمودارهای CSI و صورت فلکی که مواردی را که در آنها الگوهای مختلط آشوبناک و فقط متمرکز استفاده می‌شوند، مقایسه می‌کنند. فرستنده در (۱.۱۵ متر، ۰ درجه، ۰ متر، ۰ درجه، -۰.۳۴ متر) قرار دارد، استراق سمع کننده ۱ و استراق سمع کننده ۲ به ترتیب در (۳ متر، ۰ درجه، ۰ درجه، ۰ درجه، -۰.۳۴ متر) قرار دارند. ه) همانند پنل‌های (د)، اما فرستنده در موقعیت (۰.۷۵ متر، ۰ درجه، -۰.۵۷ متر) قرار دارد، گیرنده قانونی در موقعیت (۳ متر، ۰ درجه، ۰ متر، ۰ درجه، ۰ متر) قرار دارد، استراق سمع کننده ۱ و استراق سمع کننده ۲ به ترتیب در

موقعیت‌های (3 متر، 20 درجه، 0 متر) و (3 متر، 40 درجه، 0 متر) قرار دارند. ف عملیات XOR جریان بی‌تی ارسال و دریافت در موقعیت‌های مختلف برای الگوهای آشوبناک مختلط، برای فرستنده در موقعیت (1.15 متر، 0 درجه، 0 متر) و گیرنده قانونی در موقعیت (3 متر، 0 درجه، 0 متر) قرار دارد. ز همانند پنل‌های (و)، اما فرستنده در موقعیت (0.75 متر، 0 درجه، -0.57 متر) قرار دارد و گیرنده قانونی در موقعیت (3 متر، 0 درجه، 0 متر) قرار دارد.

**Table 1 | Measured BER performance when employing mixed chaotic patterns and only focusing patterns, where the transmitter sends bitstreams containing  $3 \times 10^3$  samples and the receivers are located at azimuthal deviations of  $0^\circ$ ,  $\pm 20^\circ$  and  $\pm 40^\circ$ , respectively, relative to the legitimate user**

Experimental Settings			Measured BER in Different Positions (%)				
Tx	Legitimate Rx		$\varphi = -40^\circ$	$\varphi = -20^\circ$	$\varphi = 0^\circ$	$\varphi = 20^\circ$	$\varphi = 40^\circ$
(1.15 m, $0^\circ$ , 0 m)	(3 m, $0^\circ$ , -0.34 m)	Only focusing patterns	0	0	0	0	0
		Mixed chaotic patterns	46.9	26.9	0	22.7	22.4
(0.75 m, $0^\circ$ , -0.57 m)	(3 m, $0^\circ$ , 0 m)	Only focusing patterns	0	0	0	0	0
		Mixed chaotic patterns	17.8	17.1	2.8	35.7	17.8

$$H_{A \rightarrow E}(t) = \sum_{n \in \text{metaA}} h_{A \rightarrow n \rightarrow E} \exp(j \varnothing_n^A) + \sum_{n \in \text{metaB}} h_{A \rightarrow n \rightarrow E} \exp(j \varnothing_n^B(t)) \quad (12)$$

$$\varnothing_n^A = f(C_{\text{metaA}}, n), \varnothing_n^B(t) = f(C_{\text{metaB}}(t), n) \quad (13)$$

$$h_{A \rightarrow B} = \frac{\exp(jk|\mathbf{r}_A - \mathbf{r}_B|)}{4\pi|\mathbf{r}_A - \mathbf{r}_B|} \sqrt{G_A(\mathbf{r}_B)G_B(\mathbf{r}_A)} \quad (14)$$

$$h_{A \rightarrow E} = \frac{\exp(jk|\mathbf{r}_A - \mathbf{r}_E|)}{4\pi|\mathbf{r}_A - \mathbf{r}_E|} \sqrt{G_A(\mathbf{r}_E)G_E(\mathbf{r}_A)} \quad (15)$$

که در آن  $PA$  و  $x_A(t)$  به ترتیب نشان دهنده توان تابشی و داده‌های منتقل شده آلیس هستند؛  $HA \rightarrow B$  و  $HA \rightarrow E$  به ترتیب نشان دهنده پاسخ‌های واسطه متاسطحی پیوندهای آلیس-متاسطح-باب و آلیس-متاسطح-ایو هستند، در حالی که  $HA \rightarrow B$  و  $HA \rightarrow E$  به ترتیب به پاسخ‌های پیوندهای آلیس-باب و آلیس-ایو بدون متاسطح اشاره دارند. این مجموعه‌ها روی تمام متاتم‌های تشکیل دهنده متاسطح اعمال می‌شوند. علاوه بر این،  $r_A$ ،  $r_B$ ،  $r_E$ ،  $r_n$  به ترتیب موقعیت‌های آلیس، باب، ایو و  $n$ امین متاتم هستند.  $An+$  پاسخ فاز  $n$ امین متاتم از متاسطح قابل برنامه‌ریزی ۱ بی‌تی بارگذاری شده با الگوی کدگذاری متمرکز استاتیک  $C_{\text{metaA}}$  است، و  $Bn\delta t_p+$  پاسخ فاز  $n$ امین متاتم از متاسطح قابل برنامه‌ریزی ۱ بی‌تی بارگذاری شده با الگوی کدگذاری آشوبناک پویا  $C_{\text{metaB}}(t)$  است. به طور خاص، هنگامی که بیت الگوی کدگذاری بارگذاری شده ( $C_{\text{metaA}}$  یا  $C_{\text{metaB}}\delta t_p$ ) 0 یا 1 باشد، پاسخ فاز مربوطه به ترتیب 0 یا 180 درجه است. علاوه بر این، مساحت متاتم است؛  $GA$ ،  $GB$ ،  $GE$ ،  $Gn$  به ترتیب الگوهای تابش توان آنتن‌های آلیس، باب، ایو و  $n$ امین متاتم هستند؛  $\varepsilon_B$  و  $\varepsilon_E$  به ترتیب نشان دهنده نویز افزایشی در باب و ایو هستند. دامنه آنها از توزیع گاوسی و فاز آنها از توزیع یکنواخت پیروی می‌کند؛  $z$  نشان دهنده واحد موهومی و  $k$  عدد موج فضای آزاد است. نکته قابل توجه این است که فرض وجود یک آنتن جهت‌دار در فرستنده، امکان صرف نظر کردن از مؤلفه‌های موج مستقیم را فراهم می‌کند. علاوه بر این، داده‌ها و کدهایی که از یافته‌های کار ما پشتیبانی می‌کنند، به ترتیب در Source Data و Supplementary Software ارائه شده‌اند.