طرح کاهش توام PAPR و رمزنگاری لایه فیزیکی مبتنی بر کدهای قطبی و دنباله آشوبی در سیستم OFDM

چکیده

امنیت و کدگذاری کانال از جمله مسائل مهم در سیستم‌های مخابراتی هستند. نسل پنجم شبکه‌های مخابراتی موبایل، نیازمند تکنولوژی‌های بالاتر برای کدگذاری[1] و رمزنگاری[2] هستند. در سال‌های اخیر، کدهای قطبی به عنوان یکی از شیوه‌های کدگذاری مفید و موثر، توجه زیادی را به خود جلب کرده‌اند. همچنین نسبت حداکثر توان به متوسط توان (PAPR) یکی از مشکلات موجود در سیستم‌های دسترسی چندگانه با استفاده تقسیم‌بندی متعامد فرکانس[3] است که بر روی عملکرد سیستم‌های OFDM به طور موثر، اثر می‌گذارد. در این مقاله، یک رویکرد برای کاهش توام PAPR و رمزنگاری لایه فیزیکی پیشنهاد شده است که تلاش می کند تا مسئله PAPR را حل کرده و به طور همزمان به سطح بالایی از امنیت در سیستم انتقال دست یابد. در این رویکرد از تکنولوژی تولید کلید در کانال‌های مخابراتی برای دستیابی به یک مقدار اولیه برای دنباله‌های آشوبی، بهره می‌بریم. سپس از دنباله‌های آشوبی برای رمزنگاری اطلاعات و کاهش همزمان PAPR استفاده می شود. همچنین از بهترین بیت‌های اطلاعاتی کدهای قطبی برای نگهداری شماره سریال[4] کدهای آشوبی استفاده می‌شود. نتایج شبیه‌سازی و آنالیزهای تئوری نشان می‌دهد که طرح پیشنهادی علاوه بر اینکه در لایه فیزیکی به یک امنیت بالا می‌رسد، همچنین باعث می‌شود که بدون افزایش دوره عکس العمل[5] و پیچیدگی[6]، نسبت PAPR در سیستم OFDM کاهش می‌یابد.

[1] coding
[2] encryption
[3] orthogonal frequency-division multiplexing (OFDM)
[4] Serial number
[5] latency
[6] complexity

واژگان کلیدی: کدهای قطبی، دسترسی چندگانه با استفاده از تقسیم‌بندی متعامد فرکانس (OFDM)، نسبت دامنه توان به حداکثر توان (PAPR)، بیت‌های اطلاعاتی، دنباله آشوبی[۷]

I) مقدمه

با توجه به رشد سریع تکنولوژی مخابرات بیسیم، نسل پنجم (5G) به یکی از کانون‌های تحقیقاتی[۸]در مخابرات بیسیم تبدیل شده است.5G نیازهای تجاری متنوعی از کار، زندگی و سرگرمی را برآورده می کند علاوه بر این ، 5G برای تأمین نیازهای متنوع تجاری در همه چیز مانند صنایع، مراقبت های پزشکی و حمل و نقل و تمام حوزه‌های صنعت نفوذ خواهد کرد. تکنولوژی‌های اصلی مخابرات موبایل نسل پنج، به طور عمده در تکنولوژی انتقال بسیار کارآمد بیسیم و تکنولوژی شبکه بیسم با تراکم بالا، گنجانده شده است [۱]. تکنولوژی کدگذاری کانال با عملکرد و بهره‌وری بالا، یکی از زمینه‌های تحقیقاتی مهم در نسل پنج است. در سال ۱۹۴۸، شانون تئوری ریاضیاتی مخابرات را پیشنهاد داد [۲]. در سال ۱۹۶۲ گالاگر[۹] کدهای بررسی توازن[۱۰]با تراکم پایین (LDPC) را پیشنهاد داد [۳]. سی برور[۱۱]و همکاران، کدهای انقلابی توربو[۱۲]را پیشنهاد دادند. با این حال، نه کدهای توربو و نه کدهای LDPC از لحاظ تئوری نتوانستند ثابت کنند که به حد شانون در ظرفیت برسند. پروفسور آریکان[۱۳]ابتدا کدهای قطبی را پیشنهاد داد و به دقت ثابت کرد که کدهای قطبی می‌توانند در کانال‌های بدون حافظه[۱۴]و گسسته باینری، به ظرفیت کانال برسد. در سال ۲۰۱۶ رویکرد کدهای قطبی به عنوان راه حل نهایی برای عرصه باند وسیع موبایل (eMBB) از کانال نترل نسل پنج بود و توانست با موفقیت به پروتکل چارچوب مخابراتی پایه نسل پنج وارد شود [۶]. در سال ۲۰۱۸ نسخه ای از سیستم نسل۵ که استاندارد 3GPP را برآورده می‌کند و از کدهای قطبی پشتیبانی می‌کند، به طور رسمی منتشر شد.

---

[7] chaotic sequences
[8] Research hotspot
[9] Gallager
[10] Parity check
[11] C. Berrou
[12] revolutionary Turbo codes
[13] Arikan
[14] memoryless

مخابرات بیسیم در مقایسه با مخابرات با سیم دارای ویژگی‌های پخش[15]، تحرک[16] و بازبودننیت [17] است و این ویژگی‌ها باعث می‌شود که قابلیت رهگیری[18] و مورد استراق سمع قرار گرفتن[19] در مخابرات بیسیم افزایش یابد و در نتیجه مسائل امنیتی در مخابرات بیسیم به طور فزاینده‌ای برجسته می‌شود [۷]. با این حال باید فرض شود که انتقال لایه فیزیکی در تکنولوژی‌های مخابراتی ایمن سنتی، عاری از خطا است. الگوریتم‌های رمزنگاری در لایه‌های بالاتر پیچیدگی محاسباتی زیادی دارد. تکنولوژی‌های ارتباطی امن سنتی، یک مکانیزم امنیتی مبتنی بر ویژگی‌های کانال لایه فیزیکی طراحی نکرده‌اند. امنیت لایه فیزیکی بیسیم (PLS) [8] باعث استفاده کامل از ویژگی‌های کانال‌ها در لایه فیزیکی بیسیم می‌شود و هر دو طرف قانونی ارتباط می‌توانند اطلاعات اصلی را بازیابی کنند، در حالی که افراد استراق سمع کننده نمی‌توانند اطلاعات محرمانه را به دست آورند. در حالت کلی، PLS (امنیت لایه فیزیکی) شامل کدگذاری امنیتی [۹]-[۱۱]، تداخل همکارانه[20] [۱۲] و[۱۳] .و تولید کلید [۱۴]-[۱۶] می‌باشد. کدهای قطبی به خاطر ساختار رمزنگاری تو در تو[21]، ساختارهای ویژه و عملکردی عالی دارند که این ساختارهای تو در تو می توانند برنده شدن تصادفی را در کدگذاری PLS تحقق بخشند. بنابراین بسیاری از محققان کدهای قطبی را در مدل کانال شنود[22] به کار برده‌اند [۱۹] و [۱۹]-[۲۱] که این امر باعث توسعه‌ی بیشتر در تئوری کدگذاری PLS می‌شود. علاوه بر این، رمزنگاری آشوبی یکی از مهمترین راه‌های پیاده‌سازی PLS است.نگاشت استدلالی[23] به عنوان یکی از نگاشت‌های آشوبی تک بعدی، از تکامل مدل جمعیت حشرات[24] مشتق می‌شود[۲۲] که می‌تواند برای رمزنگاری داده‌ها، دنباله‌های شبه تصادفی تولید کند. با این حال، اکثر مقالات موجود، کاربرد رمزنگاری آشوبی در کدگذاری کانال و مدولاسیون را به طور کامل در نظر نمی‌گیرند.

---

1 broadcasting
1 mobility
1 1 openness
1 intercepted
1 eavesdropped
2 Cooperative interference
2 2 Nested codeword structure
2 Wiretapping channel
2 Logistic mapping
2 evolution of the insect population model
5
6
7 7
8
9
0
1 1
2
3
4

OFDM یک تکنیک اصلی انتقال چندکاربره است که بخاطر عملکرده فوق العاده‌ی آن، کاربردهای گسترده‌ای در مخابرات بیسیم دارد. با این حال،PAPR یکی از مشکلات اصلی سیستم‌های OFDM است [۲۳].PAPRبالا به این معنی است که تقویت کننده خطی توان، در ناحیه تقویت غیرخطی کار خواهد کرد که این امر بر روی عملکرد سیستم OFDM تاثیر می‌گذارد. برای کاهش PAPR در سیستم‌های OFDM، تکنیک‌هایی نظیر SLM [۲۴] و [۲۵] ، دنباله انتقال جزئی (PTS) [۲۶] و [۲۷] ، برش[۲۵][۲۸] و [۲۹] و کدگذاری [۳۰] و [۳۱] پیشنهاد شده است که از بین این پیشنهادات، تکنیک SLM از دنباله فاز تصادفی برای تولید چندین دنباله جایگزین استفاده می‌کند، سپس دنباله‌ای که دارای کمترین PAPRاست ارسال می‌شود که این مسئله در کاهش PAPR موثر است. با این حال به وجود مولد دنباله فاز تصادفی و حافظه، نیاز پیدا خواهیم کرد.

برای رفع مشلکلات فوق، ما یک رویکرد توام مبتنی بر کدگذاری کانال، رمزنگاری و کاهش PAPR را در نظر می‌گیریم. اهداف اصلی این مقاله به قرار زیر است:

- ما از ویژگی‌های کانال‌های بیسیم بین دو طرف قانئنی ارتباط، برای طراحی کلید به عنوان مقدار اولیه برای دنباله‌های آشوبی استفاده می‌کنیم. دنباله‌های آشوبی برای رمزنگاری بیت‌های اطلاعاتی به کار می‌روند تا کاربر قانونی بتواند اطلاعات را به درستی رمزگشایی کند، در حالی که کسی که قصد استراق سمع دارد، نمیتواند اطلاعات را به طور موثر به دست آورد.
- ما در این رویکرد از ایده‌ی تکنیک SLM اقتباس می‌کنیم اما در فرآیند کدگذاری از تکنیک کاهش PAPR استفاده می‌کنیم که این تکنیک با تکنیک SLM تفاوت دارد. از سیگنال با کمترین PAPR برای ارسال در سیستم-های مخابراتی استفاده می‌شود که باعث تضمین امنیت و کاهش همزمان PAPR می‌شود.
- از دنباله‌های آشوبی مورد استفاده در رمزنگاری به عنوان مولد دنباله تصادفی برای کاهش PAPR در سیستم‌های OFDMاستفاده می‌شود که در مقایسه با SLM ، از دنباله‌های تصادفی اضافی استفاده نمی‌کند و باعث ساده سازی کل سیستم انتقال می‌شود.

---

[2] clipping [5]

- با بهره‌گیری از ویژگی‌های قطبش کانال، بهترین بیت‌های اطلاعاتی کدهای قطبی را انتخاب می‌کنیم تا بیت‌های شاخص از دنباله‌های آشوبی را انتقال دهیم. با چنین ترتیبی می‌توان به عملکرد بهتری از BER در طرح پیشنهادی دست یافت. به علاوه، به خاطر تاخیر اندک و پیچیدگی کم در فرآیند کدگذاری کدهای قطبی، طرح پیشنهادی بر روی پیچیدگی محاسباتی و تاخیر[۲۶]سیستم تاثیر نمی‌گذارد.

دقت شود که این مقاله، یک تحقیق بیشتردرباره مقاله قبلی ما است که در IEEE Access منتشر شده بود که در آن از الگوریتم رمزنگاری آشوبی مبتنی بر ویژگی‌های کانال بیسیم، گزارش شده بود. تفاوت‌های بین این مقاله و مقاله قبلی به این شرح است: مورد اول اینکه ما برای درک رمزنگاری، به جای استفاده از بیت‌های ثابت[۲۷]بر دنباله آشوبی تمرکز می‌کنیم.دوم این اینکه ایده‌ی SLM را به کار برده و رویکرد طرح را پیشنهاد می‌دهیم که می‌تواند برای کاهش PAPRو بهبود امنیت در سیستم OFDM استفاده شود.

ساختارادامه مقاله به این صورت است: در قسمت II مطالب مقدماتی در مورد طرح خود را به طور خلاصه معرفی می‌کنیم. در بخش III مدل سیستم و طرح پیشنهادی را معرفی خواهیم کرد. در بخش IV یک الگوریتم رمزنگاری آشوبی با بازخورو تاخیریافته مبتنی بر خصوصیات کانال بیسیم ارائه می‌شود. نتایج شبیه‌سازی و آنالیزهای امنیت در بخش Vمورد بحث قرار می‌گیرند و در بخش VI به نتیجه گیری پرداخته می‌شود.

II) مقدمات

برای درک بهتر خوانندگان از این طرح، ویژگی قطبش کانال تحلیل می‌شود. همچنین تکنولوژی تولید کلید و دنباله آشوبی مورد استفاده برای رمزنگاری، شرح داده شده است. در انتها طرح کلی را که از ایده‌ی SLM اقتباس شده است، معرفی خواهد شد.

A) انتخاب بیت‌های اطلاعاتی کدهای قطبی

کدهای قطبی به عنوان نوعی از روش کدگذاری کانال خطی مبتنی بر قطبش کانال هستند. قطبش شامل دو فرآیند است: ترکیب کانال‌ها و تقسیم کانال‌ها. وقتی که تعداد کانال‌های بازترکیب شده به بینهایت برسد، قطبش رخ خواهد

---

[2] latency
[2] Frozen bits
[6]
[7]

داد. ظرفیت کانال در کانال‌های بخشی[۲۸] به عدد یک می‌رسد (که این کانال‌ها کانال‌های خوب هستند) و ظرفیت کانال برای سایر کانال‌ها به عدد صفر می‌رسد (که این کانال‌ها کانال‌های بد هستند). در فرستنده، بیت‌های اطلاعاتی بر روی کانال‌های خوب قرار داده می‌شوند و زمانی که طول کد (N) به سمت بینهایت میل می‌کند، به حد ظرفیت شانون خواهیم رسید.

ظرفیت کانال‌های متقارن مربوط به کانال‌های بیتی در شکل ۱ نشان داده شده است که در آن طول کد برابر ۸ است و احتمال مخدوش شدگی[۲۹] برابر ۰,۵ است ($\varepsilon = 0.5$)

شکل ۲ موقعیت قطبش کانال برای ($N = 1024$) است. می‌توان فهمید که ظرفیت اغلب کانال‌های بیت برابر با صفر یا یک است و فقط تعداد محدودی از کانال‌ها دارای ظرفیت در محدوده بین صفر و یک هستند. کدهای قطبی از کانال‌های بیتی با ظرفیت بالا برای انتقال اطلاعات منبع استفاده می‌کنند.

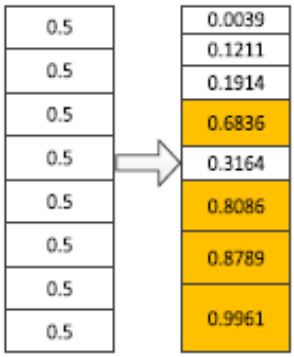

FIGURE 1. Bit channel capacities distribution when N = 8.

[2] Part channel [8]
[2] Erasure probability [9]

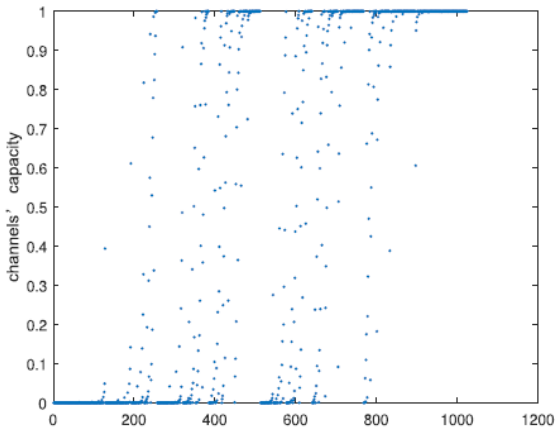

FIGURE 2. The phenomenon of channel polarization when N = 1024.

B) تولید کلید مبتنی بر ویژگی‌های کانال بیسیم

بخاطر برخی از ویژگی‌های کانال‌های بیسیم از جمله تقابل زمانی کوتاه،[۳۰]قابلیت متغیر با زمان بودن و یگانگی زمان-فضا میتوان کلید را به عنوان یک منبع تصادفی طبیعی، ایجاد کرد. ایده اصلی تولید کلید بر مبنای خصوصیات کانال بیسیم این است که هر دو طرف مجاز(قانونی) در مخابره، کانال بیسیم را آشکارسازی و تعیین کمیت می‌کنند و سپس از طریق مذاکره اطلاعات[۳۱]و افزایش امنیت و سایر تکنیک‌ها می‌توانند در یک زمان همدوس[۳۲]به یک کلید مشابه دست یابند.فرآیند تولید کلید در شکل ۳ رسم شده است که میتوان آن را به صورت زیر، شرح داد:

۱) آشکارسازی کانال‌ها: در زمان همدوسی، هر دو طرف مجاز در ارتباط، به طور متناوب سیگنال‌های آشکارسازی را ارسال می‌کنند و مقادیر مشاهده شده ویژگی کانال بیسیم را به دست می‌آورند. ویژگی‌های اصلی کانال‌های بیسیم برای استخراج کلیدها، ویژگی تاخیر نسبی چند مسیره[۳۳][۳۳] و اطلاعات حالت کانال[۳۴](CSI) است. CSI شامل پاسخ فرکانسی کانال [۳۴] و پاسخ ضربه کانال (شامل دامنه و فاز) است.

---

[30] Short time reciprocity
[31] Information negotiation
[32] Coherent time
[33] multipath relative delay
[34] channel state information

۲) مقدارسنجی[۳۵]ویژگی‌های کانال: هر دو طرف مجاز در ارتباط، از یک رویکرد مشابه برای مقدارسنجی استفاده می‌کنند و مقادیر مشاهده شده ویژگی‌های کانال را به کلیدهای اولیه تعیین می‌کنند. طرح‌های بسیاری برای مقدارسنجی وجود دارد از جمله رویکرد مقدارسنجی چندبیتی [۳۵]، رویکرد مقدارسنجی دو آستانه‌ای [۳۶] و رویکرد مقدارسنجی مبتنی بر خطای کمی‌سازی تعاملی.

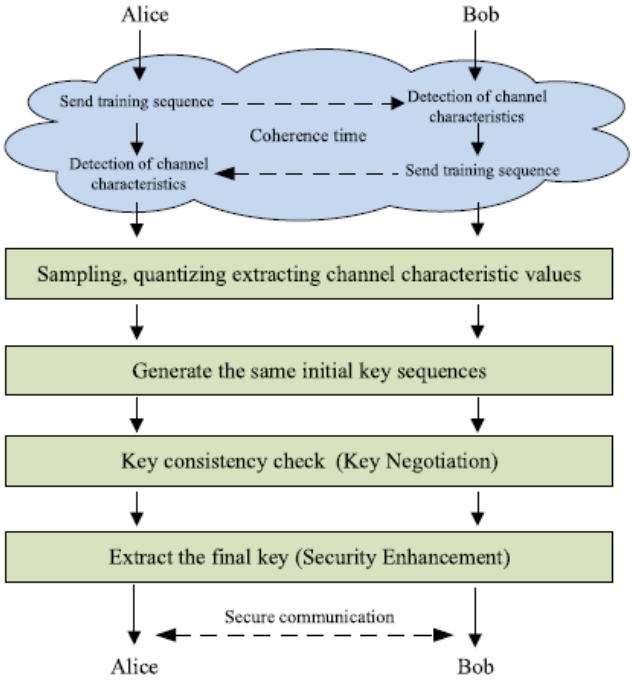

FIGURE 3. Key generation flow chart.

۳) مذاکره اطلاعات: با توجه به عواملی همچون تداخل نویز کانال، خطای آشکارسازی و عوامل دیگر، ممکن است در کلیدهای اولیه، اطلاعات متناقض وجود داشته باشد. بنابراین هر دو طرف مجاز در ارتباط برای تعامل اطلاعات از یک کانال مشترک استفاده می‌کنند تا بتوانند کلیدهای سازگار به دست آورند. تعامل اطلاعات می‌تواند شامل بررسی توازن[۳۶]برای یک دنباله متوالی از کلیدها و غیره باشد. مرجع [۳۸] دستورالعمل‌های طراحی عملی در سیستم‌های تولید کلید امن را ارائه می‌دهد. کار انجام شده در [۳۹] به بررسی و اندازه‌گیری رابطه بن همبستگی متقابل ناشی از نویز و اندازه‌گیری‌های غیرهمزمان می‌پردازد. بنابراین هر دو طرف مجاز در ارتباط می‌توانند با استفاده از مذاکره

3 quantificatioin 5
3 Parity check 6

اطلاعات، اثر ناقص بودن حالت اطلاعات کانال را حذف کنند. شیوه‌های موجود برای مذاکره اطلاعات عبارتند از: روش متوالی‌سازی[۴۰][7]، روش جستجوی دودویی [۴۱]و برخی شیوه‌های کدهای تصحیح کننده خطا [۴۳] و [۴۴].

۴) افزایش امنیت: در فرآیند آشکارسازی کانال و مذاکره اطلاعات، ممکن است که گیرنده غیرقانونی، برخی از اطلاعات موجود در خصوص کلید را استراق سمع کند که این امر یک تهدید بالقوه برای امنیت کلید_ها است. بنابراین طرفین مجاز در ارتباط از ابزارهایی استفاده می‌کنند تا بتوانند برخی از اطلاعاتی به دست آمده توسط استراق سمع کننده را، حذف کنند. در حال حاضر توابع درهم سازی [۴۵][8] و [۴۶] و استخراج کننده‌ها[۴۶][9]، روش‌های اصلی افزایش امنیت هستند.

C) تولید سلسله مراتب

تولید دنباله‌های آشوبی: سیستم آشوبی بخاطر ویژگی هایش از جمله حساسیت به مقدار اولیه و برگشت ناپذیری،[۴۰] به عنوان یک مولد منبع شبه تصادفی در نظر گرفته می‌شود. دنباله‌های آشوبی گسستهبا استفاده از سیستم‌های نگاشت آشوب گسسته، تولید می‌شوند. سپس با استفاده از روش‌های کمّی سازی مناسب، به دنباله‌های دوتایی آشوبی دیجیتال، کمّی سازی می‌شوند.

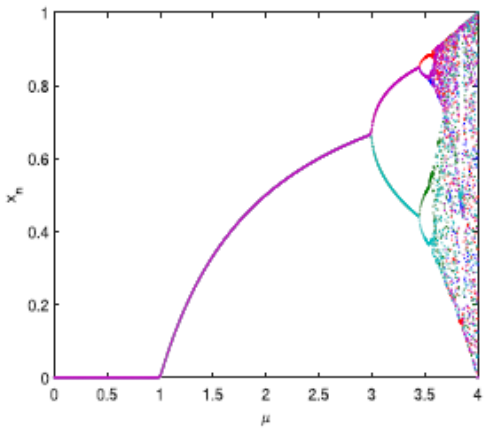

FIGURE 4. Bifurcation diagram of logistic map.

---

[3] cascade
[3] Hash function
[3] extractor
[4] irreversibility
[7]
[8]
[9]
[0]

سیستم آشوبی گسسته معمولی، یک نگاشت لجستیک است که در این طرح مورد استفاده قرار می‌گیرد. معادله نگاشت را می‌توان به صورت زیر در نظر گرفت:

$$x_{n+1} = \mu x_n (1 - x_n) \qquad (1)$$

که $x_n \in (0,1), n = 1,2, \ldots$ و $\mu \in (0,4]$ پارامتر سیستماتیک است. اگر مقدار اولیه که x_1 و پارامتر μ تنظیم شوند، آنگاه یک دنباله آشوبی معین یعنی $\{x_n\}_{n=1}^{\infty}$ بر اساس معادله (۱) به دست می‌آید.

نمودار شکاف گاه[1](دوشاخگی) نگاشت لجستیک بر حسب تغییرات پارامترها در شکل ۴ نشان داده شده است که به وضوح انتقال نگاشت لجستیک را از دوره دو برابر شدن دوشاخگی به آشوب را به تصویر می‌کشد. از روی نمودار میتوان مشاهده کرد که نگاشت لجستیک به ازای مقادیر مختلف برای μ، ویژگی‌های مختلفی را نشان می‌دهد.

ما از حوزه فرکانس مربوط به کانال‌های بیسیم برای استخراج اطلاعات فاز به عنوان یک مقدار اولیه برای دنباله آشوبی استفاده می‌کنیم. برای اطمینان از عمل متقابل کانال‌ها در سیستم‌های مخابراتی بیسیم، فرض می‌شود که آشکارسازی هر کانال بین دو طرف قانونی ارتباط(مخابره) در طول زمان همدوسی کانال قرار دارد. علاوه بر این، تمامی سیگنال‌های استفاده شده در این الگوریتم، سیگنال‌های فرکانسی هستند.

D) نسبت حداکثر توان به مقدار متوسط توان در سیستم‌های OFDM و تکنیک SLM: خروجی سیستم-های مدولاسیون چند حاملی، بر خلاف سیستم‌های تک حاملی، جمع آثار تعداد زیادی از حامل‌ها است. اگر فازهای این زیر حامل‌ها، یکسان و منطبق[2]باشند، توان لحظه‌ای بسیار بیشتر از متوسط توان خواهد بود و این امر باعث افزایش PAPR می‌شود. تقویت کننده توان در محدوده خطی دینامیکی وسیعی عمل خواهد کرد. در غیر اینصورت، هنگامی که پیک سیگنال فراتر از محدوده خطی تقویت کننده توان باشد، باعث ایجاد اعوجاج سینال خواهد شد که این امر همچنین منجر به ایجاد اختلال در بین زیرحامل‌ها و تشعشعات خارج از باند می‌شود تا تداخل تقابل را ایجاد نماید. یکی از راه حل‌ها این است که از یک تقویت کننده توان با محدوده کاری خطی بسیار بزرگ بهره ببرد. با این

---

1 bifurcation 4

2 coincident 4

حال، محدوده کاری خطی بزرگ، منجر به کاهش عملکرد تقویت کننده شده و به تسهیلات فرستنده، پیچیدگی اضافه می‌کند.

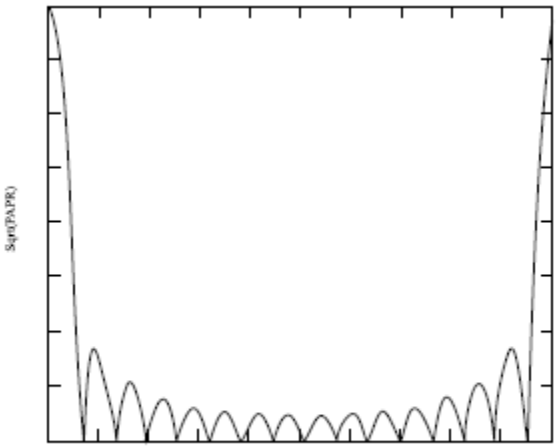

FIGURE 5. The problem of PAPR in OFDM system.

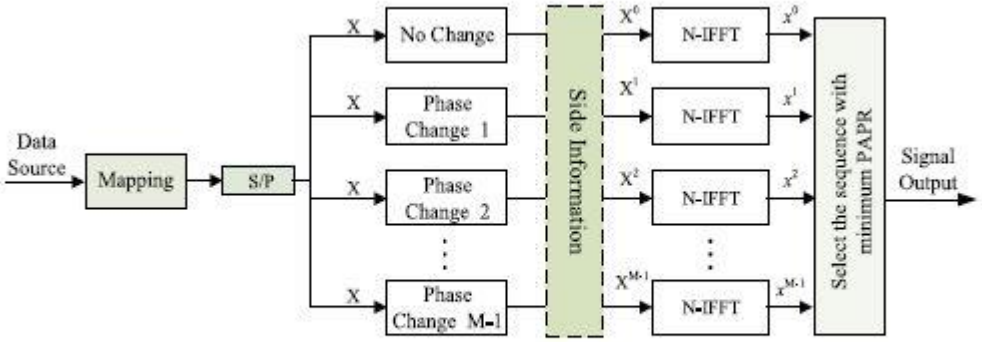

FIGURE 6. SLM structure diagram.

۱) نسبت PAPR در سیستم‌های OFDM

سمبل OFDM در مقایسه با سیستم‌های تک حاملی، از روی هم قرار گرفتن زیرحامل‌های مدوله شده مستقل، ایجاد می‌شود که ممکن است پیک بزرگتری برای توان سیگنال ایجاد کرده و PAPRبزرگتری را ایجاد می‌کند. تعریف PAPRبه صورت معادله (۲) و (۳) است:

$$\mathrm{PAPR}(dB) = 10\log_{10}\frac{\max\{|x_n|^2\}}{E\{|x_n|^2\}} \qquad (2)$$

$$x_n = \frac{1}{\sqrt{N}}\sum_{k=0}^{1} X_k W_N^{nk} \qquad (3)$$

که x_n سیگنال خروجی بعد از عمل IFFT (معکوس تبدیل فوریه سریع) و $w_N = e^{-j\,2\pi/N}$ است.

برای سیستم OFDM با تعداد N زیرحامل، زمانی که همه‌ی زیر کانال‌ها یکسان باشند، پیک توان سیگنال N برابر مقدار متوسط توان است. به عنوان مثال در شکل ۵، مقدار N برابر با ۱۶ قرار داده شده و نشان می‌دهد که PAPR در سیستم‌های OFDM بزرگ است. در این حالت، همه زیرحامل‌ها توسط سمبل‌هایی با فاز اولیه یکسان، مدوله شده‌اند. در این شکل می‌بینیم که پیک توان ۱۶ برابر مقدار متوسط توان است. برای موج حامل مدوله نشده، ضریب PAPR برابر صفر است. بنابراین در سیستم‌های OFDM ، مقدار PAPRبزرگ است.

توابع چگالی تجمعی مکمل (CCDFS)های PAPR برای اندازه‌گیری کاهش عملکرد PAPR ایجاد شده‌اند. تابع CCDF به صورت معادله ۴ به دست می‌آید:

$$\frac{1}{R}\sum_{k=1}^{R} m_k \qquad (4)$$

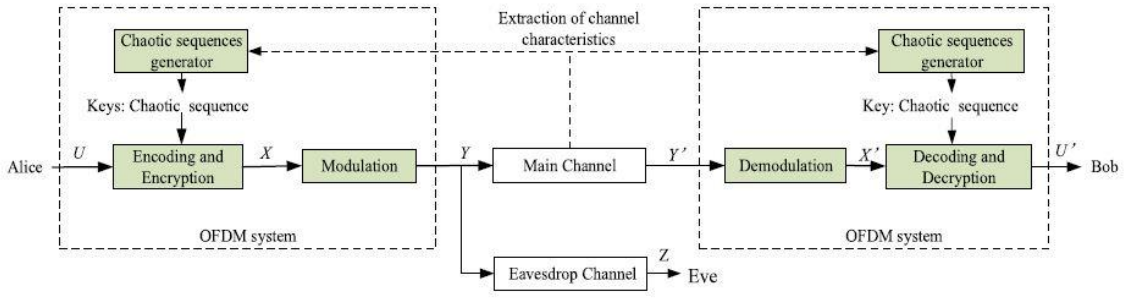

FIGURE 7. Block diagram of the communication system mode.

که در آن

$$m_k = \begin{cases} 1, & when\ PAPR > PAPR_0 \\ 0, & other \end{cases}$$

۲)ایده SLM

ایده اصلی SLM این است که در یک دنباله‌ی Mتایی با فازهای متفاوت، دنباله‌ی با کمترین PAPR انتخاب و ارسال شود. در شکل ۶ مدل سیستم با استفاده از تکنیک SLM رسم شده است.

دنباله‌های دودویی مربوط به منبع داده، با استفاده از رمزنگاری قطبی به نقاط منظومه[۴۳]نگاشت می‌شوند که نقاط منظومه توسط X نشان داده می‌شود و این نقاط با استفاده از معادله ۵ توصیف می‌شوند.

$$X = [X_0, X_1, \ldots, X_{N-1}] \qquad (5)$$

توسط مولد فاز تصادفی، (M-1) دنباله با فاز تصادفی ایجاد می‌کنیم. μ امین بردار دنباله با فاز تصادفی، با استفاده از معادله ۶ توصیف می‌شود:

$$P(\mu) = (P_0^{\mu}, P_1^{\mu}, \ldots, P_{N-1}^{\mu}) \qquad (6)$$

که $\mu = 1,2, \ldots, M-1$ و $P_i^{\mu} = \exp\left(j\,\varphi_i^{(\mu)}\right)$. $i = 0,1, \ldots, N-1$ همچنین $\varphi_i^{(\mu)}$ دارای توزیع یکنواخت در بازه $[0,2\pi)$ است.

دنباله داده ورودی برای دسترسی به M دنباله با مقادیر PAPR متفاوت، (M-1) دنباله‌های فاز تصادفی را به ترتیب ضرب می‌کند. بنابراین μامین دنباله بعد از عمل ضرب، به صورت معادله ۷ نوشته می‌شود که عملگر $<\bullet>$ نشان‌دهنده ضرب نقطه به نقطه است.

$$\begin{aligned} X(\mu) &= (X_0^{(\mu)}, X_1^{(\mu)}, \ldots, X_{N-1}^{(\mu)}) = < X \bullet P(\mu) > \\ &= (X_0 P_0^{\mu}, X_1 P_1^{\mu}, \ldots, X_{N-1} P_{N-1}^{\mu}) \end{aligned} \qquad (7)$$

سپس بر روی M دنباله خروجی متفاوت، عمل IFFT انجام می‌شود. برای μامین دنباله می‌توان نشان داد که :

$$x_{\mu} = \mathrm{IFFT}[X(\mu)], \quad (n = 0, \ldots, N-1) \qquad (8)$$

---

4 constellation 3

از بین این M دنباله، دنباله با کمترین PAPR ارسال می‌شود. اطلاعات جانبی‌ای که مشخص‌کننده این است که کمترین PAPR مربوط به چه دنباله‌ای است نیز به دنباله اضافه می‌شود. قابل ذکر است که آشکارسازی صحیح این اطلاعات برای بازسازی سمبل OFDM بسیار اهمیت دارد.بنابراین باید شرایط خوبی از کانال را برای انتقال این اطلاعات جانبی، فراهم کرد.

III) مدل سیستم و رویکرد طراحی:

بلوک دیاگرام مدل سیستم به کار رفته در این مقاله، در شکل ۷ رسم شده است.

در سیستم‌های OFDM، فرستنده (آلیس) یک پیغام را برای گیرنده مجاز (باب) ارسال می‌کند و این ارسال در حالی است که فرد استراق سمع کننده می‌خواهد به پیغام ارسالی دسترسی داشته باشد. آلیس و باب کلید را از طریق کانال اصلی بیرون می‌کشند. به دلیل منحصر به فرد بودن زمان-فضای کانال‌های بیسیم،استراق سمع کننده هیچ اطلاعاتی از کلید ندارد. هنگامی که آلیس یک پیغام را برای باب ارسال می‌کند، پیغام متنی ساده با استفاده از ماژول‌های رمزنگاری و کدگذاری، کدگذاری و رمزنگاری شده و به متن رمزنگاری شده‌ی X تبدیل می‌شود. سپس X مدوله شده و به شکل موج Y تبدیل می‌شود. هنگامی که باب Y' را دریافت می‌کند،ابتدا بر اساس ماژول دمدولاسیون، X' به دست آمده و سپس بر اساس ماژول رمزگشا و کدگشا به U' دسترسی پیدا می‌کند. از آنجا که اطلاعات به دست آمده توسط استراق سمع کننده (Eve) یک کد رمز شده‌ی Z است، فرآیند رمزگشایی بسیار دشوار می‌شود. علاوه بر این،کاهش PAPR به طور همزمان با فرآیند رمزگشایی در سیستم OFDM استفاده شده است که جزییات آن در ادامه به تصویر کشیده شده است.

بلوک دیاگرام فرستنده در شکل ۷ نمایش داده شده است که دارای گام‌های زیر است:

- گام یک: کلید بر اساس ویژگی‌های کانال توسط مولد کلید تولید می‌شود که این عمل در شکل ۳ نشان داده شده است. سپس مقدار اولیه کلید پس از کوانتیزاسیون[4]به مولد دنباله آشوبی ارسال می‌شود تا دنباله‌های آشوبی را ایجاد کند. سپس با توجه به طول کد، دنباله‌های آشوبی به

[4] quantization [4]

$V = 2^{\nu}$ $(\nu = 0,1,2, \dots)$ قسمت تقسیم می‌شوند که ν شماره سریال است. به عنوان مثال همانطور که در شکل ۹ نشان داده شده است، اگر $\nu = 2$ یعنی $V = 4$ و دنباله‌های آشوبی بااستفاده از اعداد 00 و 01 و 10 و 11 اندیس گذاری می‌شوند، شاخص شماره سریال[۴۵]و اطلاعاتی که می‌خواهیم ارسال کنیم ،بر روی بیت‌های اطلاعاتی کدهای قطبی قرار داده می‌شوند.

گام دوم: همانگونه که در شکل ۱۰ نشان داده شده است، موقعیت بیت‌های کدهای قطبی به غیر از موقعیت شاخص شماره سریال را با استفاده از کدهای آشوبی رمز می‌کنیم (موقعیت بیت‌های کد قطبی رمز می‌شوند ولی موقعیت شاخص شماره سریال رمز نمی‌شود). دنباله‌های آشوبی با استفاده از شاخص شماره سریال انتخاب می‌شوند. به عنوان مثال هنگامی که طول کد ۱۲۸ بیت و نرخ کد برای کدهای قطبی برابر با .۲۵ باشد، دو تا از بیت‌های اطلاعاتی برای ذخیره و نگه داری شاخص شماره سریال استفاده می‌شوند و ۳۰ بیت دیگر برای دنباله آشوبی رمزشده توسط الگوریتم XOR هستند.

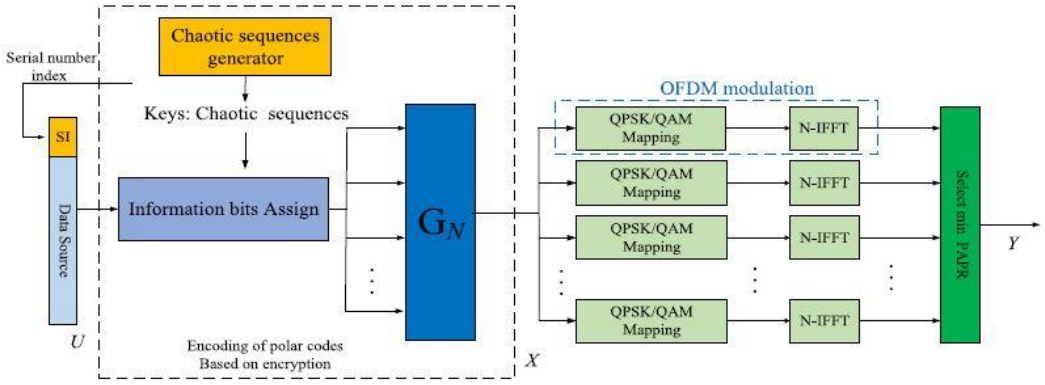

FIGURE 8. The block diagram of the sender.

[4] Serial number index [5]

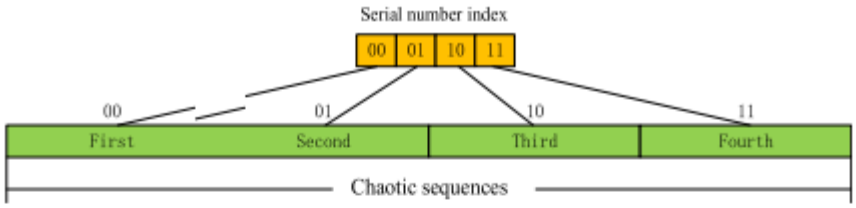

FIGURE 9. The sne snumber indices of chaotic sequences.

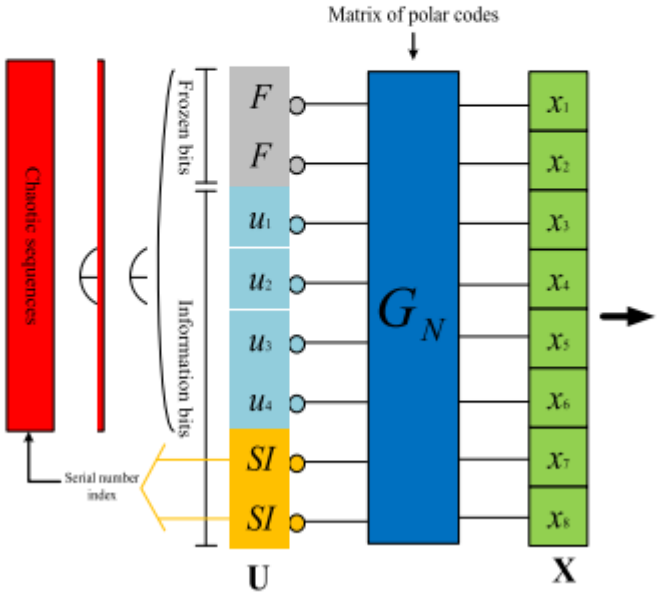

FIGURE 10. The process of encryption and encoding.

- گام سوم: فرستنده (آلیس) دنباله اطلاعات رمزنگاری شده U را با استفاده از کدهای قطبی، رمز می‌کند که توسط معادله ۹ توصیف می‌شود.

$$X = UG_N(A) + U_{A^c}G_N(A^c) \qquad (9)$$

که N طول کد و $G_N(A)$ یک زیرماتریس از G_N است.

- گام چهارم: سیگنال کد شده به سیستم OFDM داده می‌شود و PAPR مربوط به دنباله‌های آشوبی متفاوت، محاسبه می‌گردند. سپس سیگنال با کمترین PAPR برای ارسال انتخاب می‌شود.

از گام‌های بالا می‌توان مشاهده کرد که فرآیند رمزنگاری با کاهش PAPR ترکیب شده است که این کار باعث می‌شود در مقایسه با تکنیک SLM، مولد دنباله فاز تصادفی حذف می‌شود. علاوه بر این، با توجه به عملکرد متفاوت کانال‌های

قطبی، ما کانال با بیشترین ظرفیت را برای انتقال شاخص شماره سریال انتخاب می‌کنیم که این کار باعث افزایش عملکرد سیستم می‌شود. لازم به ذکر است که رمزگذاری قزبی در طرح پیشنهادی برای استفاده در نسخه V دنباله، مورد نیاز است. با این حال، فرآیند رمزگذاری کدهای قطبی توسط ماتریس بسیار ساده G_N ارائه شده است که این بدان معنی است که کدگذاری V بر روی پیچیدگی سیستم، تاثیری ندارد.

بلوک دیاگرام گیرنده در شکل ۱۱ نشان داده شده است که دارای گام‌های زیر است:

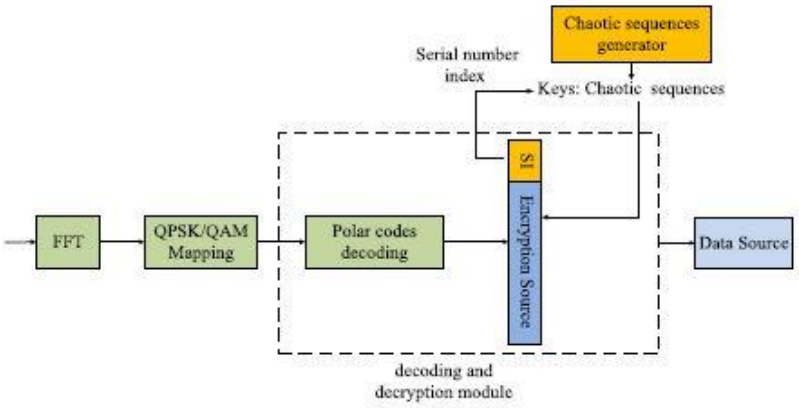

FIGURE 11. The block diagram of the receiver.

- گام اول: سیگنال دریافتی دمدوله می‌شود. دقت شود که سیگنال دریافتی سیگنالی است که دارای کمترین PAPR بوده است. بنابراین ما باید عمل دمدولاسیون را فقط بر اساس ندولاسیون مربوطه انجام دهیم.
- گام دوم: از کدگشای SC برای کدگشایی استفاده می‌کنیم. عبارت تصمیم‌گیری برای رمزگشایی به صورت معادله ۱۰ است:

$$\hat{u}_i = \begin{cases} u_i, & i \in A^c \\ h_i(y_1^N, \hat{u}_1^{i-1}), & i \in A \end{cases} \qquad (10)$$

که A مجموعه بیت‌های اطلاعاتی و A^c مجموعه بیت‌های ثابت است. $h_i(y_1^N, \hat{u}_1^{i-1})$ به صورت زیر است:

$$h_i(y_1^N, \hat{u}_1^{i-1}) \triangleq \begin{cases} 0, & L_N^i(y_1^N, \hat{u}_1^{i-1}) \geq 1 \\ 1, & otherwise \end{cases} \qquad (11)$$

برای محاسبه احتمال انتقال هر کانال بیت، از آشکارساز SC استفاده می‌شود. سپس اطلاعات نسبت درست نمایی[۴۶] در هر کانال بیت به صورت تکراری محاسبه می‌شود تا یک تصمیم برای هر کدام از اطلاعات انتقالی، اتخاذ شود. اطلاعات نسبت درست نمایی به صورت معادله ۱۲ توصیف می‌گردد:

$$L_N^i(y_1^N, \hat{u}_1^{i-1}) = \log \frac{W_N^i(y_1^N, \hat{u}_1^{i-1}|0)}{W_N^i(y_1^N, \hat{u}_1^{i-1}|1)} \qquad (12)$$

گام سوم: گیرنده به دلیل تولید کلید،می‌تواند کلید اولیه را دریافت نماید. کلید اولیه به یک مولد دنباله آشوبی مشابه ارسال می‌شود تا همان دنباله آشوبی را ایجاد کند. بعد از رمزگشایی، گیرنده می‌تواند شاخص شماره سریال را پیدا کند که این شاخص بر روی بهترین بیت‌های اطلاعات کد قطبی قرار داده می‌شود. سپس بخش دنباله آشوبی مربوطه را با استفاده از شاخص شماره سریال جستجو می‌کند. همانگونه که در شکل ۹ نشان داده شده است، اگر گیرنده شاخص 00 را به عنوان بهترین بیت‌های اطلاعاتی دریافت نماید، اولین توالی آشوبی که متناظر با شماره سریال 00 است را در نظر می‌گیرد. در نهایت دنباله‌های دریافتی با استفاده از الگوریتم XOR و توسط دنباله آشوبی، رمزگشایی می‌شود. سپس دنباله اطلاعات رمزگشایی شده، به دست می‌آید.

در گیرنده فرآیندهای دمدولاسیون و رمزگشایی به روش‌های معمول انجام می‌شود. در ابتدا گیرنده اطلاعات جانبی را به طور مستقیم از بهترین بیت‌های اطلاعاتی پس از کد گشایی قطبی، به دست می‌آورد (چون بهترین بیت‌های اطلاعاتی توسط فرستنده رمز نشده اند). پی می‌توان با استفاده از اطلاعات جانبی، بخش‌های دنباله آشوبی که توسط فرستنده استفاده شده است رل تعیین کرده و در نهایت، گیرنده از بخش‌های دنباله آشوبی برای رمزگشایی بیت‌های اطلاعاتی استفاده می‌کند. بر این اساس، هیچگونه پیچیدگی اضافی در دریافت وجود ندارد.

---

4 Likelihood ratio 6

IV)نتایج شبیه سازی:

در این قسمت بر روی عملکرد کاهش PAPR رویکرد پیشنهادی در مقایسه با تکنیک SLM و عملکرد BER تحت کانال‌های مختلف می‌پردازیم.

در شکل ۱۲، بهبود کاهش PAPR مربوط به رویکرد polar-SLM پیشنهادی با رویکرد SLM سنتی به ازای طول کدهای متفاوت، با یکدیگر مقایسه شده است. تعداد دنباله‌های آشوبی یعنی V برابر با ۴ است. مشاهده می‌شود که رویکرد پیشنهادی به ازای $N = 128$ و ۲۵۶ و ۵۱۲ از نظر کاهش PAPR دارای عملکردی مشابه با رویکرد SLM است. بنابراین ثابت شد که رویکرد polar-SLM مانند SLM سنتی، در سیستم‌های OFDM مقدار PAPR را به ازای طول کدهای متفاوت، به طور موثر کاهش می‌دهد.

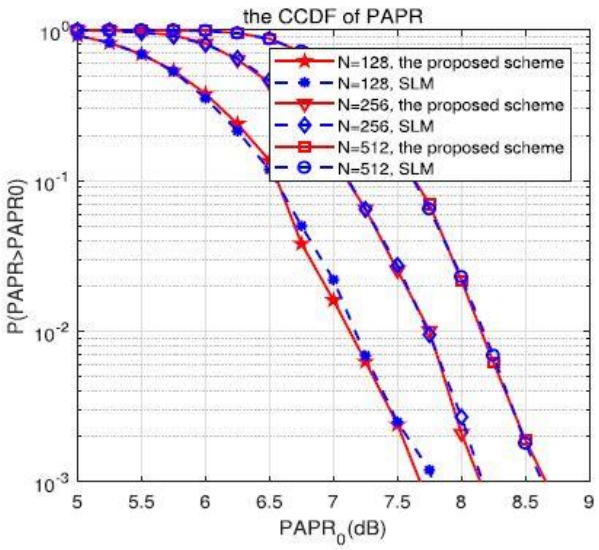

FIGURE 12. The PAPR comparison of SLM and polar-SLM methods with different code lengths.

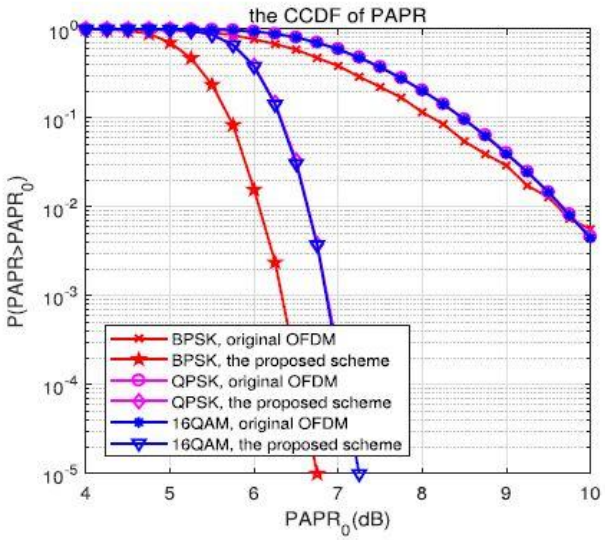

FIGURE 13. The influence of different modulation methods on proposed scheme and original scheme.

در شکل ۱۳،رویکرد polar-SLM پیشنهادی با مدولاسیون‌های BPSK,QPSK و 16QAM به کار رفته شده است. در حالی که تعداد بخش‌های دنباله آشوبی (V) برابر با ۸ و طول کد (N) برابر با ۱۲۸ است.

می‌توان مشاهده کرد که عملکرد کاهش PAPR با افزایش V، به تدریج بهبود می‌یابد. زیرا به ازای مقادیر PAPR مختلف، می‌توان بخش‌های بیشتری از دنباله آشوبی را اننتخاب کرد. بنابراین فرستنده برای تنظیم عملکرد کاهش PAPR، می‌تواند شاخص شماره سریال را متناسب با پیژگی‌های تقویت کننده انتخاب نماید.

در شکل ۱۵ و ۱۶ مقایسه عملکرد BER بین طرح پیشنهادی و سیستم OFDM ای که از تکنیک‌های SLM و کدهای قطبی استفاده می‌نماید، ارایه شده است. ما از مدولاسیون‌های BPSK و QPSK بر روی کانال‌های AWGN استفاده کرده ایم. توجه شود که در طرح پیشنهادی، فرآیند کدگذاری و کاهش PAPR ترکیب می‌شوند که در آن بهترین کانال‌های کدهای قطبی برای اطلاعات جانبی انتخاب می‌شوند. در حالی که در رویکرد OFDM معمولی، فرآیندهای رمزگذاری قطبی و فرآیند SLM از یکدیگر مجزا هستند. طول کدها به ترتیب به صورت $N = 64$ و $N = 128$ و اندیس شماره سریال $\nu = 4$ هستند. می‌توان مشاهده کرد که طرح پیشنهادی به ازای طول کدهای مختلف و مدولاسیون‌های مختلف، عملکرد BER بهتری را به دست می‌آورد.

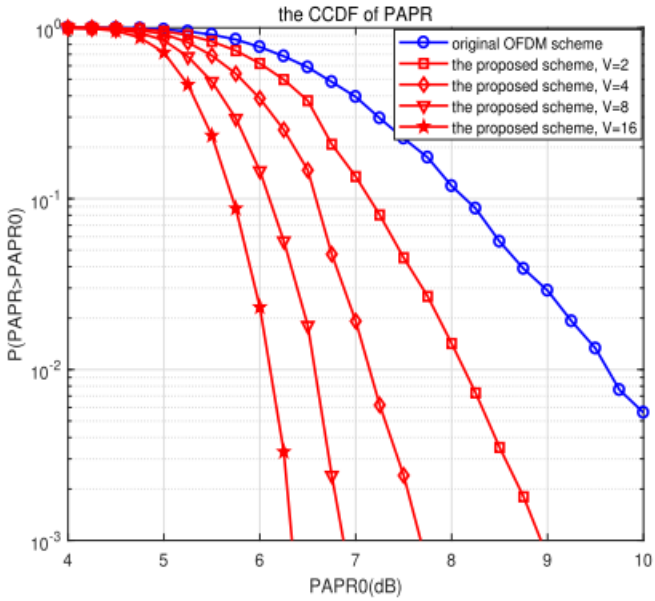

FIGURE 14. PAPR of proposed scheme with different indices lengths.

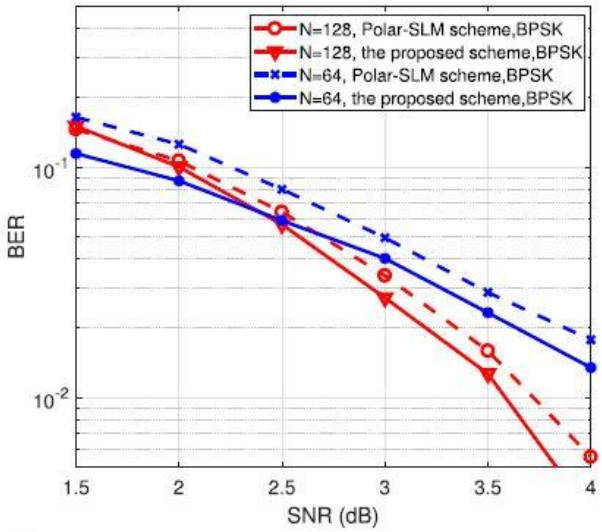

FIGURE 15. BER performances comparisons of the proposed scheme and polar coding-SLM at code lengths $N = 64$ and $N = 128$, BPSK over AWGN channel.

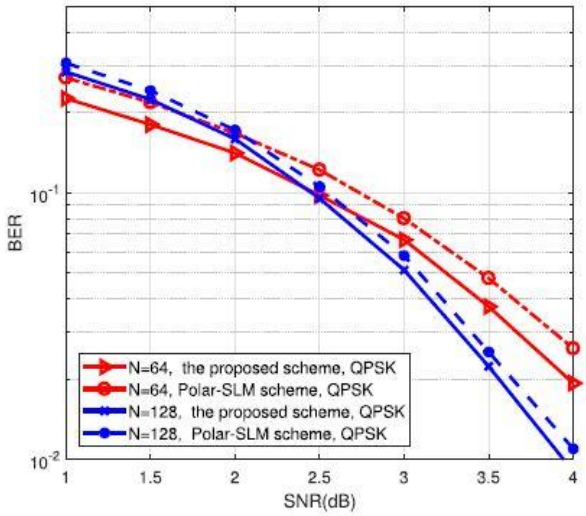

FIGURE 16. BER performances comparisons of the proposed scheme and polar coding-SLM at code lengths $N = 64$ and $N = 128$, QPSK over AWGN channel.

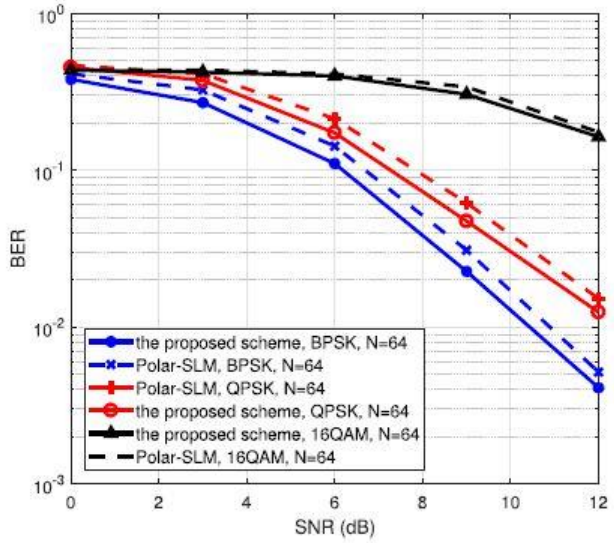

FIGURE 17. BER performances comparisons of the proposed scheme and polar coding-SLM at code lengths $N = 64$, BPSK, QPSK and 16QAM over Rayleigh fading channel.

برای تایید بیشتر در خصوص امکان پذیری طرح پیشنهادی، ما شبیه سازی BER را برای کانال فرکانس انتخابی با محوشدگی رایلی اجرا می‌کنیم که این کانال دارای ۱۰ انشعاب[۷]آلست. باید دقت کرد که شبیه‌سازی BER در حالت کانال ایده آل انجام شده است. در شکل‌های ۱۶ و ۱۷ مقایسه عملکرد BER بین طرح پیشنهادی و کدگذاری

[4] tap [7]

SLM و کدگذاری قطبی به ازای مدولاسیون‌های مختلف بر روی کانال رایلی ارایه شده است. مدولاسیون‌های BPSK و QPSK و 16QAM بر روی کانال رایلی و طول کد $N = 64$ و $N = 128$ انجام شده است. به طور مشابه در رویکرد پیشنهادی فرآیندهای کاهش PAPR و کدگذاری قطبی با یکدیگر ترکیب شده اند و مقدار ν برابر با ۴ است. می‌توان مشاهده کرد که رویکرد پیشنهادی بر روی کانال رایلی و به ازای مدولاسیون‌های مختلف دارای عملکرد BER بهتری است.

رویکرد پیشنهادی در مقایسه با رویکرد polar-SLM عملکرد بهتری بر روی کانال‌های رایلی یا کانال‌های AWGNدارد. می‌توان توضیح داد که کانال‌های ترکیبی با ظرفیت کانال بزرگ، برای انتقال اطلاعات جانبی قابلیت اعتماد بیشتری دارند.

برای بررسی میزان حساسیت به مقادیر اولیه کلید،از زبان سطح بالای c++ و کتابخانه محاسباتی با دقت چندگانه (GNU) استفاده کرده ایم. نتایج بررسی ها در جدول ۱ نشان داده شده است. می‌بینیم که زمانی که مقدار اولیه به صورت تصادفی بین (۱و۰) باشد، میزان اختلاف برابر با $۱۰^{-۱۰}$ است و ضریب اختلاف برای دنباله تصادفی حدود ٪۵۰ است. در دنباله‌های آشوبی تا حدی تفاوت وجود دارد و استراق سمع کننده نمی‌تواند اطلاعات متن رمزی را کشف کند. یعنی الگوریتم دارای دقت کلید بالا و حساسیت کلید قوی است.

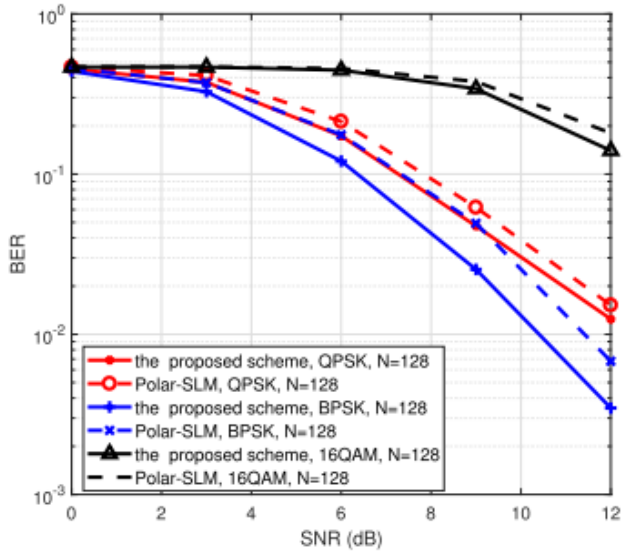

FIGURE 18. BER performances comparisons of the proposed scheme and polar coding-SLM at code lengths $N = 128$, BPSK, QPSK and 16QAM over Rayleigh fading channel.

TABLE 1. Sensitivity detection results of chaotic sequence key.

Key difference accuracy	Chaos sequence differences
10^{-10}	50.38%
10^{-20}	50.17%
10^{-30}	50.03%
10^{-40}	49.97%
10^{-50}	49.87%

V) نتیجه‌گیری:

در این مقاله، کاهش PAPR در سیستم OFDM با رمزنگاری مبتنی بر مشخصه کدگذاری کدهای قطبی، ترکیب شده است. بر اساس ویژگی‌هایی که کانال‌های بیسیم دارند، برای رمزنگاری از دنباله‌های آشوبی استفاده شد. با الهام از ایده‌ی SLM، دنباله‌های آشوبی برای کاهش PAPR به کار رفت و مدل سیستم نیز ساده شد. همچنین اطلاعات جانبی مربوط به شاخص شماره سریال توسط کانالی که دارای بیشترین ظرفیت و کدگذاری قطبی بود، انتقال داده شد که این امر باعث بهبود عملکرد BER شد. بنابراین طرح پیشنهادی می‌تواند PAPR را به طور موثر از سیستم OFDM کاهش داده و رمزنگاری را در فرآیند کدگذاری محقق کند که امنیت و قابلیت اطمینان سیستم را افزایش می‌دهد.

REFERENCES

[1] C. J. Zhang, J. Ma, G. Y. Li, Y. Kishiyama, S. Parkvall, G. Liu, and Y. H. Kim, "Key technology for 5G new radio," *IEEE Commun. Mag.*, vol. 56, no. 3, pp. 10–11, Mar. 2018.

[2] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.*, vol. 27, no. 3, pp. 379–423, Jul. 1948.

[3] R. G. Gallager, "Low-density parity-check codes," *IRE Trans. Inf. Theory*, vol. 8, no. 1, pp. 21–28, Jan. 1962.

[4] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding: Turbo-codes. 1," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2002, pp. 1064–1070.

[5] E. Arikan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3051–3073, Jul. 2008.

[6] *NR and NG-RAN Overall Description—Rel. 15*, document TS 38.212, 3GPP, 2018.

[7] K. Ren, H. Su, and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communications," *IEEE Wireless Commun.*, vol. 18, no. 4, pp. 6–12, Aug. 2011.

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

[9] R. Hooshmand and M. R. Aref, "Polar code-based secure channel coding scheme with small key size," *IET Commun.*, vol. 11, no. 15, pp. 2357–2361, 2017.

[10] C. Li, G. Xuan, C. W. Tan, and R. W. Yeung, "Fundamental limits on a class of secure asymmetric multilevel diversity coding systems," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 737–747, Apr. 2018.

[11] Y. Huang, W. Li, and J. Lei, "Concatenated physical layer encryption scheme based on rateless codes," *IET Commun.*, vol. 12, no. 12, pp. 1491–1497, 2018.

[12] K. Pham and K. Lee, "Non-cooperative interference alignment for multicell multiuser MIMO uplink channels," *IET Commun.*, vol. 11, no. 5, pp. 648–654, 2017.

[13] H. Zeng, X. Qin, Y. Xu, S. Yi, Y. T. Hou, and W. Lou, "Cooperative interference neutralization in multi-hop wireless networks," *IEEE Trans. Commun.*, vol. 66, no. 2, pp. 889–903, 2018.

[14] Y. Peng, P. Wang, W. Xiang, and Y. Li, "Secret key generation based on estimated channel state information for TDD-OFDM systems over fading channels," *IEEE Trans. Wireless Commun.*, vol. 16, no. 8, pp. 5176–5186, Aug. 2017.

[15] B. Chen, C. Zhu, W. Li, J. Wei, V. C. M. Leung, and L. T. Yang, "Original symbol phase rotated secure transmission against powerful massive MIMO eavesdropper," *IEEE Access*, vol. 4, pp. 3016–3025, 2016.

[16] J. Zhang, R. Woods, T. Q. Duong, A. Marshall, Y. Ding, Y. Huang, and Q. Xu, "Experimental study on key generation for physical layer security in wireless communications," *IEEE Access*, vol. 4, pp. 4464–4477, 2016.

[17] M. Andersson, V. Rathi, R. Thobaben, J. Kliewer, and M. Skoglund, "Nested polar codes for wiretap and relay channels," *IEEE Commun. Lett.*, vol. 14, no. 8, pp. 752–754, Aug. 2010.

[18] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. 2011.

[19] W. Hao, L. Yin, and H. Qin, "Secrecy transmission scheme based on 2-D polar coding over block fading wiretap channels," *IEEE Commun. Lett.*, vol. 22, no. 5, pp. 882–885, May 2018.

[20] R. Hooshmand and M. R. Aref, "Efficient polar code-based physical layer encryption scheme," *IEEE Wireless Commun. Lett.*, vol. 6, no. 6, pp. 710–713, Dec. 2017.

[21] M. A. M. Sayed, R. Liu, and C. Zhang, "A novel scrambler design for enhancing secrecy transmission based on polar code," *IEEE Commun. Lett.*, vol. 21, no. 8, pp. 1679–1682, Aug. 2017.

[22] R. M. May, "Simple mathematical models with very complicated dynamics," *Nature*, vol. 261, pp. 459–467, Jun. 1976.

[26] M. Singh and S. K. Patra, "Partial transmit sequence optimization using improved harmony search algorithm for PAPR reduction in OFDM," *ETRI J.*, vol. 39, no. 6, pp. 782–793, 2017.

[27] M. Yoshida, H. Nashimoto, and T. Miyajima, "PTS-based PAPR reduction by iterative p-norm minimization without side information in OFDM systems," *IEICE Trans. Commun.*, vol. E101, no. 3, pp. 856–864, 2018.

[28] J. Hou, X. Zhao, F. Gong, H. Fei, and J. Ge, "PAPR and PICR reduction of OFDM signals with clipping noise-based tone injection scheme," *IEEE Trans. Veh. Technol.*, vol. 66, no. 1, pp. 222–232, Jan. 2017.

[29] Y. Lin, K. Song, and M. S. Yun, "Iterative clipping noise recovery of OFDM signals based on compressed sensing," *IEEE Trans. Broadcast.*, vol. 63, no. 4, pp. 706–713, Dec. 2017.

[30] M. R. Motazedi and R. Dianat, "Reduction of PAPR in coded OFDM using fast Reed–Solomon codes over prime Galois fields," *Int. J. Electron.*, vol. 104, no. 2, pp. 328–342, 2016.

[31] C.-Y. Hsu and H.-C. Liao, "Generalised precoding method for PAPR reduction with low complexity in OFDM systems," *IET Commun.*, vol. 12, no. 7, pp. 796–808, 2018.

[32] X. Lu, J. Lei, W. Li, K. Lai, and Z. Pan, "Physical layer encryption algorithm based on polar codes and chaotic sequences," *IEEE Access*, vol. 7, pp. 4380–4390, 2019.

[33] J. Zhang, R. Woods, A. Marshall, and T. Q. Duong, "Verification of key generation from individual OFDM Subcarrier's channel response," in *Proc. GLOBECOM Workshops*, Dec. 2016, pp. 1–6.

[34] N. Patwari, J. Croft, S. Jana, and S. K. Kasera, "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements," *IEEE Trans. Mobile Comput.*, vol. 9, no. 1, pp. 17–30, Jan. 2009.

[35] S. T. Ali, V. Sivaraman, and D. Ostry, "Secret key generation rate vs. reconciliation cost using wireless channel characteristics in body area networks," in *Proc. IEEE/IFIP Int. Conf. Embedded Ubiquitous Comput.*, Hong Kong, Dec. 2010, pp. 644–650.

[36] C. Chen and M. A. Jensen, "Secret key establishment using temporally and spatially correlated wireless channel coefficients," *IEEE Trans. Mobile Comput.*, vol. 10, no. 2, pp. 205–215, Feb. 2010.

[37] X. Zhu, F. Xu, E. Novak, C. C. Tan, Q. Li, and G. Chen, "Using wireless link dynamics to extract a secret key in vehicular scenarios," *IEEE Trans. Mobile Comput.*, vol. 16, no. 7, pp. 2065–2078, Jul. 2017.

[38] J. Zhang, B. He, T. Q. Duong, and R. Woods, "On the key generation from correlated wireless channels," *IEEE Commun. Lett.*, vol. 21, no. 4, pp. 961–964, Apr. 2017.

[39] J. Zhang, R. Woods, T. Q. Duong, A. Marshall, and Y. Ding, "Experimental study on channel reciprocity in wireless key generation," in *Proc. IEEE Int. Workshop Signal Process. Adv. Wireless Commun.*, Jul. 2016, pp. 1–5.

[40] Y. Wei, K. Zeng, and P. Mohapatra, "Adaptive wireless channel probing for shared key generation based on PID controller," Dept. IEEE Educ. Activities, Tech. Rep., Sep. 2013.

[41] Y. Wei, K. Zeng, and P. Mohapatra, "Adaptive wireless channel probing for shared key generation based PID controller," Dept. IEEE Educ. Activities, Tech. Rep., Sep. 2013.

[42] H. Liu, J. Yang, Y. Wang, and Y. Chen, "Collaborative secret key extraction leveraging received signal strength in mobile wireless networks," in *Proc. IEEE INFOCOM*, Orlando, FL, USA, Mar. 2013, pp. 927–935.

[43] H. Liu, J. Yang, Y. Wang, Y. Chen, and C. E. Koksal, "Group secret key generation via received signal strength: Protocols, achievable rates, and implementation," *IEEE Trans. Mobile Comput.*, vol. 13, no. 12, pp. 2820–2835, Dec. 2014.

[44] D. Chen, N. Cheng, N. Zhang, K. Zhang, Z. Qin, and X. Shen, "Multi-message authentication over noisy channel with polar codes," in *Proc. IEEE Int. Conf. Mobile Ad Hoc Sensor Syst.*, Orlando, FL, USA, Oct. 2017, pp. 46–54.

[45] D. Chen, N. Zhang, R. Lu, X. Fang, K. Zhang, Z. Qin, and X. Shen, "An LDPC code based physical layer message authentication scheme with prefect security," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 748–761, Apr. 2018.

[23] G. Wunder, R. F. H. Fischer, H. Boche, S. Litsyn, and J.-S. No, "The PAPR problem in OFDM transmission: New directions for a long-lasting problem," *IEEE Signal. Process. Mag.*, vol. 30, no. 6, pp. 130–144, Nov. 2013.

[24] S.-H. Wang, K.-C. Lee, and C.-P. Li, "A low-complexity architecture for PAPR reduction in OFDM systems with near-optimal performance," *IEEE Trans. Veh. Technol.*, vol. 65, no. 1, pp. 169–179, Jan. 2016.

[25] D. J. G. Mestdagh, J. L. G. Monsalve, and J.-M. Brossier, "GreenOFDM: A new selected mapping method for OFDM PAPR reduction," *Electron. Lett.*, vol. 54, no. 7, pp. 449–450, 2018.

[46] Q. Wang, H. Su, K. Ren, and K. Kim, "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks," in *Proc. IEEE INFOCOM*, Orlando, FL, USA, Apr. 2011, pp. 1422–1430.

[47] A. Alamdar-Yazdi and F. R. Kschischang, "A simplified successive-cancellation decoder for polar codes," *IEEE Commun. Lett.*, vol. 15, no. 12, pp. 1378–1380, Dec. 2011.