رمزکننده و رمز گشای نوین کدهای LT جهت بهبود خطا در کانال محو شونده باینری

سید مسعود میررضایی[۱]

۱- استادیار- دانشکده مهندسی برق- دانشگاه صنعتی شاهرود- شاهرود - ایران

sm.mirrezaei@shahroodut.ac.ir

چکیده: کدهای Luby Transform (LT) اولین کلاس از کدهای محو شونده می باشد که آنرا کدهای محو شونده فراگیر می نامند. ویژگی های چنین کدهایی به درستی در زمان استفاده از فایلهای داده ای با حجم زیاد مشخص می شوند، اما در زمان استفاده از آنها برای پیام های با طول کم، عملکرد خوبی از خود نشان نمی دهند. در این مقاله، یک رمزکننده و رمز گشای جدید، مشخصا یک رمزکننده LT کارآمد با استفاده از توزیع مقاوم سالیتان (RSD) به عنوان یک روش تولید جدید درجه راست و توزیع جدید درجه چپ که در کانال محو شونده باینری (BEC) تست شده است ارائه می شود. توزیع درجه سمت چپ یک کد LT به عنوان یک توزیع پواسون جهت محافظت کلی در نظر گرفته شده است. شکل دهی جدید درجه چپ گره ها، کارایی بهتری از کدهای LT را ایجاد می نماید که با طرحهای با قابلیت بالا در سایر مقالات مقایسه شده است.

در بسته های اطلاعاتی به طول $k = 256$ و نرخ خطای بیتی 10^{-8}، نرخ کدگذاری تحقق یافته این مدل ۰/۵۸ می باشد که ۲۵٪ بیشتر از طرح توسعه یافته BP آقای جمشیدی و همکارانش می باشد. نتایج تجربی نشان می دهد که این کدک جدید منجر به پیشرفت در کلیه ویژگی های سیستم می شود. به این ترتیب، این کار گامی در جهت طراحی و ساخت کدهای بهینه تر برای کانال BEC برداشته است.

واژه‌های کلیدی: رمز گذاری کانال، کدهای فواره ای، کدهای Luby Transform (LT)، سمبولهای افزونه، کانال باینری محو شونده .

نوع مقاله: پژوهشی

DOI: 10.52547/jiaeee.20.3.107

تاریخ ارسال مقاله: ۱۴۰۰/۰۲/۲۵

تاریخ پذیرش مشروط مقاله: ۱۴۰۱/۰۳/۰۸

تاریخ پذیرش مقاله: ۱۴۰۱/۰۷/۲۴

نام نویسنده‌ی مسئول: دکتر سید مسعود میررضایی

نشانی نویسنده‌ی مسئول: ایران – شاهرود – بلوار دانشگاه – دانشگاه صنعتی شاهرود – دانشکده‌ی مهندسی برق

۱- مقدمه

در سال ۱۹۹۸، آقای بیرز و همکارانش کد فواره ای دیجیتال[۱] را به عنوان یک مدل تصحیح خطای احتمالی کلی توسعه داده اند. بدون نرخ بودن، یکی از برجسته ترین و مهمترین خصوصیات کد های فواره ای دیجیتال می باشد [۱, ۲]. یکی از کاربردهای کدهای بدون نرخ در سیستم های ارتباطی صوتی در زیر آب می باشد [۳]. کاربرد دیگر این کدها کاهش میزان خطا در کانال ارتباطی برای ارسال بسته های ویدیویی و کدگذاری آنهاست [۴]. بسته های کدگذاری شده مانند یک چشمه، بطور مداوم تحویل داده می شوند و هر گیرنده می تواند پس از دریافت تعداد کافی از بسته ها، داده های منبع را بازیابی کند. کدهای LT [۵]، کدهای Raptor [۶] و کدهای برخط [۷] به عنوان نمونه ای از کدهای فواره ای دسته بندی می شوند. برخلاف دو مورد دیگر، روش کدگذاری کدهای LT ساده تر و با هزینه بسیار کمتر می باشد و همچنین دامنه وسیع تری از کاربردها را به دنبال دارد.

توزیع درجه، نقش مهمی در کارآیی کدگذاری و کدگشایی کدهای LT دارد، بنابراین توزیع درستی برای کاربردهای ارتباطی پیچیده مبتنی بر کد فواره ای دیجیتال فوق الذکر لازم می باشد. با توجه به موارد فوق، پنج دسته توزیع درجه وجود دارد: ۱- توزیع ایده آل سالیتان (ISD)[۲]: ۲- توزیع مقاوم سالیتان (RSD)[۳]؛ ۳- توزیع همه در یک بار(all-at-once)؛ ۴- توزیع دوتایی؛ ۵- توزیع نمایی دوتایی. کارهای زیادی به جهت بهبود بهره وری در کد LT با بهینه سازی توزیع درجه انجام شده است، و برخی خروجی های مفیدی نیز حاصل شده است.

بر خلاف کارهای گذشته، که در آنها کانال بی سیم بصورت محو شوندگی بلوکی در نظر گرفته شده است، یعنی ضریب محو شوندگی در طول ارسال یک بلوک داده تغییرنمی کند، در [۸, ۹] تغییرات آرام زمانی را که کانال در طول ارسال یک بلوک تجربه می کند در نظر گرفته شده است و به طراحی کدینگ وفقی برای چنین سیستمی پرداخته شده است. الگوریتم ارایه شده بر اساس کدگشایی توام می باشد و هدف آن رسیدن به احتمال خطایی پایین تر از سطح آستانه مجاز، با انتخاب یک کدینگ وفقی است که کمترین انرژی مصرفی را دارد. البته در مقاله مذکور جهت استخراج درجه بیت های کدگذاری شده از توزیع RSD به عنوان یک توزیع بهینه استفاده می شود.

یکی دیگر از کاربردهای کدگذاری کانال تلفیق آن با رمزنگاری می باشد که در دهه های اخیر بدان نگاه شده است. مقاله [۱۰] روش جدیدی از تلفیق کدگذاری و رمزنگاری را برای افزایش امنیت ارایه داده است که مبتنی بر کدگذاری قطبی می باشد و در آن علاوه بر پیچیدگی زیاد و عدم همبستگی بین بیتهای ارسالی از حداقل کلید رمز در آن استفاده شده است. نتایج این الگوریتم نشان دهنده آن است که در سیستم تلفیقی علاوه برعدم دانایی دشمن از کلیدهای الگوریتم های رمز، خرابی کانال و قطبی شدگی کانال به کمک رمزگذار آمده و حداکثر میزان ابهام و گیجی مورد نظر شانون را برای دشمن فراهم می کند.

کدگذاری کانال جهت ارسال و دریافت داده ها در سامانه های دورسنجی روشی برای پردازش داده های در حال ارسال از مبدا به مقصد می باشد که نویسندگان در مقاله [۱۱] به بررسی و ارزیابی کدهای مختلف کانال در این حوزه پرداخته اند و با بیان راه حل جدید از جمله ترکیب کدهای مختلف به نتایج معقولی دست پیدا کرده اند.

آقای ین و همکارانش اندازه موج دار بهبود یافته[۴] با RSD تصحیح شده را در نظر گرفته اند [۱۲]، که اندازه موج دار به گونه ای کنترل می شود که اندازه آن به اندازه طول داده یعنی k در رمزگشای BP نزدیک می باشد. در این روش، نرخ کدگشایی موفقیت آمیز بیشتر از توزیع RSD سنتی می باشد. LT-W توسط آقای لو و همکارانش به عنوان یک الگوریتم کدگشایی دیگر پیشنهاد شد [۱۳]. در این مقاله برای گسترش بیشتر قابلیت کدگشایی کدک، روش Wiedemann به فرآیند کدگشایی LT اعمال شده است. نویسندگان نشان داده اند که این روش از عملکرد فرایند اصلی کدگشایی LT پشتیبانی می کند و سربار بسته را کاهش می دهد. علاوه بر این، روش RSD مبتنی بر حافظه[۵](MBRSD) توسط آقای هیاجنه و همکارانش مورد بررسی قرار گرفت [۱۴]. برای MBRSD، بیت کدگذاری شده با درجه یک، بیت پیامی را انتخاب می کند که درجه آن حداکثر مقدار در طول عملکرد کدگذاری را داشته باشد. در این روش، اثرات نامطلوب فرآیند کدگشایی کاهش می یابد. علاوه بر این، در مقایسه با یک کد LT سنتی، هنگامی که MBRSD با مدل اندازه موج دار کاهش یافته[۶] متعلق به آقای سونرنسون ترکیب می شود [۱۵]، خطا را تا حدی کاهش می دهد.

در مقاله [۱۶]، نویسندگان نشان می دهند که ساختارهای زائد در نمودار تنر، راندمان کدگشایی کدهای LT را تغییر می دهد. آنها برخی از تجزیه و تحلیل ها را در مورد این فرم های اضافی انجام می دهند و برای بازیابی بیت های کدگذاری شده از کدهای LT، الگوریتم افزونه کاهشی (Low Redundancy -LR) را پیشنهاد می دهند. هنگامی که الگوریتم LR استفاده می شود، نتایج شبیه سازی نشان می دهد که در میان کدهای LT مورد بررسی، از لحاظ احتمال کدگشایی موفق و میانگین ضریب سربار بهبود چشمگیری یافته است.

از آنجا که درک مدل توزیع درجه برای کاربردهای ارتباطی مشارکتی مبتنی بر کد فواره ای دیجیتال ضروری است؛ آقای لو و همکارانش، برای بهینه سازی توزیع درجه از کدهای LT کوچک، روش مبتنی بر بهینه سازی دسته جوجه ها یا Swarm Chicken (ECSO) را پیشنهاد داده اند [۱۷]. نتایج شبیه سازی و مقایسه نشان می دهد که راه حل پیشنهادی کارایی بسیار بهتری نسبت به دو نفر دیگر به دست آورده است.

روش کدگشایی OFBP[۷](انتشار باور بر خط) برای کدهای LT در [۱۸] ارائه شده است. این روش فرآیند کدگشایی را به محض دریافت

هر بیت کدگذاری شده آغاز می کند. نتایج شبیه سازی مزیت روش پیشنهادی را برای کدهای LT بررسی کرده است. علاوه بر این، زمان کدگشایی واقعی الگوریتم پیشنهادی بسیار کوتاه تر از الگوریتم BP سنتی است.

نویسندگان مقاله [۱۹]، احتمال انتقال اندازه موج دار را بین دو مرحله مجاور کدگذار BP در کدهای LT مورد بررسی قرار داده اند و به صورت فرمولی بیان کرده اند. نتایج حاصل از بررسی، تابع جمعی احتمال (PMF)[۸] را برای اندازه موج دار در هر مرحله از کدگشایی نشان می دهد. در ضمن جهت ارزیابی سیستم تابع احتمال شرطی بدست آمده در اندازه قبلی موج دار واقع در مرحله قبلی و تعداد بیتهای منبعی که بازیابی می شوند اندازه گیری می شوند.

آقای اوکپوتس و همکارانش، توزیع پواسون کوتاه شده (TPD)[۹] را برای تولید بیت های کدگذاری شده در یک کد فواره ای منظم پیشنهاد داده اند [۲۰]. سیستم های ذخیره سازی توزیع شده خطاپذیر، شکل جدید و مورد پذیرش برای کاربردهای خاص می باشد.

ادامه این مقاله به شرح زیر ارائه می گردد:

بخش ۲ به معرفی مختصری از کدهای LT می پردازد و مروری بر روش BP کدهای LT در کانالهای محو شونده باینری (BEC)[۱۰] ارائه می شود. در بخش ۳، رمزکننده و رمز گشای جدید LT پیشنهاد می گردد که شامل کدگذار جدید و طراحی کدگشای متعلق به آن می باشد. در بخش ۴ نتایج عددی حاصل از شبیه سازی ارائه می شود. نهایتا در بخش ۵ مقاله نتیجه گیری ارائه می گردد.

۲- مدل سیستم

اولین دسته از کدهای عملیاتی فواره ای دیجیتالی، کدهای LT می باشند که دارای پیچیدگی های کم، مقیاس پذیری بالا و قابلیت اطمینان برای انتقال داده از طریق کانال های محو شونده می باشند. علاوه بر این، کدهای LT نیز از اصلی ترین کدهای فواره ای کاربردی دیگر، مانند کدهای LT منظم [۱۹]، کدهای Raptor [۶]، کدهای فواره ای توزیع شده [۲۲] و ... هستند. فرض می شود بسته های داده دارای k بیت اطلاعاتی باشند. کدهای LT می توانند به صورت $\Omega(x), k, n$ نشان داده شوند که در آن k تعداد بیتهای اطلاعاتی، n تعداد بیتهای کد شده و $\Omega(x) = \sum_{i=1}^{k} \Omega_d x^d$ توزیع درجه گره های خروجی می باشد که در آن Ω_d احتمال اینکه بیت کد شده دارای درجه d باشد است. در جدول (۱) کلمات اختصار بیشتری به همراه تعاریف آنها نشان داده شده است.

جدول (۱): مفاهیم واختصارات بکار رفته

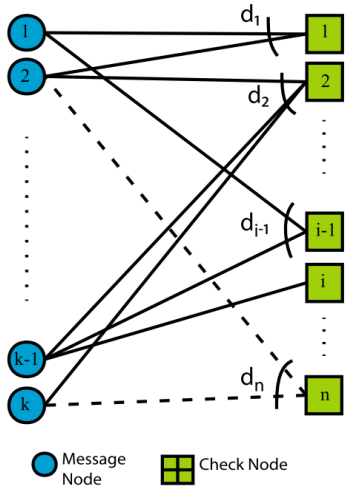
NOMENCLATURE			
توزیع مقاوم سالیتون (RSD)	Ω(x)	تعداد بیتهای ورودی	k
احتمال محو کنندگی کانال	α	ضریب سربار	ε
درجه سمبل کد شده c_i	$d(c_i)$	تعداد بیتهای کد شده	N
مجموعه بیتهای داده ای برای تولید سمبل c_i	$\mathbf{rs}(c_i)$	نرخ کد	R = k/n

۲-۱- کدگذاری کدهای LT

کدهای LT، کدهای فواره ای هستند که با توزیع درجه تعیین می شوند و بیت های کدگذاری شده را با استفاده از دو مرحله زیر تولید می کنند:

- به صورت تصادفی درجه d از میان توزیع درجه $\Omega_1, \Omega_2, \dots, \Omega_k$ انتخاب می شود که در آن Ω_i احتمال اینکه i انتخاب شود می باشد.
- به صورت تصادفی و یکنواخت d بیت متفاوت اطلاعاتی انتخاب می شود و بیت x_n که حاصل XOR آنهاست، تولید می شوند.

خروجی این روش بیت کدگذاری شده برای ارسال به کانال است. شکل (۱) نمونه ای از کدگذار LT را نشان می دهد. همانطور که در این شکل نشان داده شده است، با استفاده از توزیع درجه خاص، گره های چک (بیتهای کدگذاری شده) از گره های پیام ساخته می شوند. مقدار d مربوط به بیت کدگذاری شده، درجه آن نامیده می شود و توزیع نمونه برداری آن را، توزیع درجه می نامند.



شکل(۱): ساختار رمز گذار LT

بسیاری از پارامترهای سیستم به انتخاب نوع توزیع درجه وابستگی دارند. این پارامترها شامل نرخ متوسط تحقق یافته، امکان شروع موفقیت آمیز و ادامه روند کدگشایی، میزان خطا، میزان هزینه کدگذاری و کدگشایی می باشند. از این رو، طرح توزیع درجه بسیار مهم است و در آثار بسیاری مانند [۲۵،۲۴،۲۳،۶،۵] مورد مطالعه قرار گرفته است. از این رو یکی از نوآوریهای این مقاله ارائه توزیع درجه جدیدی می باشد که کمک به بهینه کردن پارامترهای مهم ذکر شده در بالا می باشد.

۲-۲- رمزگشایی کدهای LT

به طور خاص، در کانال محو شونده، فرآیند کدگشایی می تواند الگوریتم ساده شده sum-product باشد [۲۶]. با استفاده از الگوریتم ساده شده که در زیر می توان مراحل آن را خلاصه کرد، پیامهایی که منتقل می شوند کاملاً مشخص یا ناشناخته هستند نشان داده می شود [۲۶]:

۱- اولین تلاش برای پیدا کردن بیت کد شده از درجه اول (d_n) می باشد که فقط به یک بیت اطلاعاتی (m_k) متصل می باشد. (اگر بیت رمز شده از درجه ۱ وجود نداشته باشد عملیات کدگشایی متوقف خواهد شد و امکان ادامه کدگشایی وجود ندارد)

- مقدار $m_k=d_n$ قرار داده می شود.
- بیت m_k را با تمامی بیتهای کدشده $d_{n'}$ که به m_k متصل می باشند جمع می کنیم:

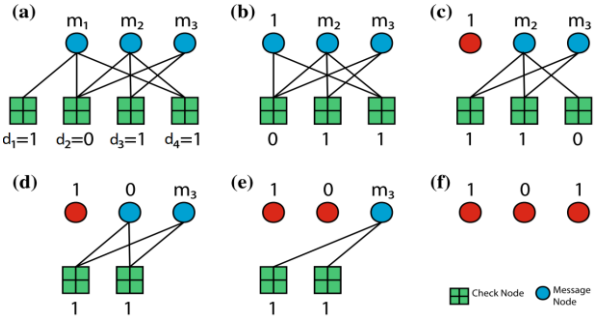
$$d_{n'} := d_{n'} + m_k \quad \text{برای تمامی } n' \text{ ها که } G_{n'k} = 1$$

- تمامی یالهایی که به m_k متصل می باشند حذف می شود.

۲- گام اول تا زمانی که همه m_k ها بازیابی شوند ادامه داده می شود.

این روش به عنوان یک مثال در شکل ۲ نشان داده شده است. حلقه های قرمز و آبی به عنوان بیت های پیام نشان داده شده اند، در حالی که مربع های دارای تقاطع برای بیت های کدگذاری شده نشان داده می شوند. بیت های کدگذاری شده را با XOR کردن بیت های پیام انتخاب شده تولید می شوند. چهار بیت کدگذاری شده و سه بیت پیام وجود دارد که مقادیر $(d_1, d_2, d_3, d_4)= 1011$ می باشند.

در ابتدای آغاز فرآیند کدگشایی، تنها بیت کدگذاری شده درجه ۱ انتخاب می شود (شکل ۲-a). این مقدار در m_1 کپی شده است (شکل ۲-b)، بیت کدگذاری شده را حذف کرده و سپس مقدار جدید m_1 به d_2 و d_4 اضافه می شود (شکل ۲-c). گره m_1 از نمودار جدا می شود. در تکرار بعدی (شکل ۲-c)، d_4 گره درجه یک است که فقط به بیت پیام۲ متصل شده است. اکنون m_2 را برابر با d_4 در نظر می گیریم (شکل ۲-d)، و سپس این مقدار را به d_2 و d_3 اضافه می کنیم (شکل ۲-e). سرانجام، مشاهده می شود که d_2 و d_3 (با مقدار یکسان) به m_3 متصل شده و می توانند برای بازیابی m_3 استفاده شوند (شکل ۲-f).



شکل (۲): یک رمزگشای BP ساده برای کد LT در کانال محو شونده [۲۴]

با توجه به مباحث گفته شده در بالا و مثال بیان شده، ممکن است تحت دو وضعیت مختلف تلاش جهت کدگشایی با شکست مواجه شود. وضعیت اول: اگر بیت پیامی وجود داشته باشد که به هیچ بیت کدگذاری شده وصل نشده باشد، کدگشایی با شکست همراه خواهد بود. در وضعیت دوم، اگر گره ای از درجه یک وجود نداشته باشد، کدگشایی قطعا شکست خواهد خورد. هر دو وضعیت نمونه ای از مجموعه های متوقف شونده (Stopping Sets) می باشند.

با این وجود، کدگشایی همراه با موفقیت بستگی به توزیع درجات دارد. توزیع درجه باید به گونه ای انتخاب شود که فرآیند کدگشایی در حال پیشروی باشد و همیشه یک گره با درجه یک وجود داشته باشد و هیچ بیت پیامی بدون ارتباط با بیت های کدگذاری شده وجود نداشته باشد.

۳- طراحی کدکننده و کدگشای نوین

برای داشتن یک کدک (کدکننده و کدگشا) LT که به خوبی طراحی شده و اطمینان حاصل شود که روند کدگشایی می تواند شروع و ادامه یابد، باید بسیاری از بیت های کدگذاری شده با درجه پایین وجود داشته باشد. علاوه بر این، چند بیت کدگذاری شده، باید اتصالات زیادی داشته باشند(درجه بالا) تا اطمینان حاصل شود که همه بیت های ورودی در عمل کدگذاری شرکت می کنند. پس برای طراحی توزیع مناسب درجه راست (RDD)[11] باید دو موضوع را در نظر گرفت:

۱. برخی از بیت های خروجی باید درجه بالایی داشته باشند تا از محافظت مناسب و اتصال نمودار فراگیر اطمینان حاصل شود.

۲. برخی از بیت های خروجی باید درجه کمی برای شروع روند کدگشایی و همچنین تا حصول موفقیت داشته باشند و همچنان پیچیدگی کدگذاری و کدگشایی را در مقدار کم نگه دارند.

یکی از افرادی که بر روی توزیع درجه، بسیار زیاد کار کرده است، آقای لوبی می باشد که به اصطلاح به آن، توزیع ایده آل سالیتان ISD [۲۷] گویند و به شرح زیر می باشد:

$$\rho(d) = \begin{cases} \frac{1}{k}, & d = 1 \\ \frac{1}{d(d-1)}, & d = 2,3,\dots,k \end{cases} \quad (۱)$$

برای تأکید بیشتر، اولین توزیع درجه بهینه برای کدهای LT، ISD می باشد. برای اینکه ISD قابل تصور باشد، آقای لوبی، RSD را به منظور کنترل بهتر تعداد مورد انتظار بیت های خروجی از درجه یک معرفی کرده است. برای این منظور ، تابع $\tau(d)$ به شرح زیر است:

$$\tau(d) = \begin{cases} \frac{S}{kd}, & d = 1,2,\dots,\left(\frac{k}{S}\right)-1 \\ \frac{S}{k}\log\left(\frac{S}{\delta}\right), & d = k/S \\ 0, & d > k/S \end{cases} \quad (۲)$$

که در آن $S = c.\ln\left(\frac{k}{\delta}\right).\sqrt{k}$. سپس ISD در رابطه (۱) به رابطه (۲) اضافه می شود و برای بدست آوردن RSD ، نرمالیزه می شود. $\Omega(d)$ به شکل زیر بدست می آید:

$$\Omega(d) = \frac{\rho(d) + \tau(d)}{\beta} \qquad (۳)$$

که در آن $\beta = \sum_d \rho(d) + \tau(d)$ می باشد. با حداکثر احتمال خطای δ، تعداد بیت های کدگذاری شده در گیرنده برای بازیابی کلیه بیت های منبع (k) برابر با $n = (1+\varepsilon)k$ می باشد.

ژاوو و همکارانش دو نوع ساختار افزونگی را در کد LT توصیف می کنند [۱۶]. آنها همچنین روش کدگذاری را با عنوان روش کم افزونه (LR) که در سازماندهی بیت های کدگذاری شده مورد استفاده قرار می گیرند، پیشنهاد داده اند. رویکرد پیشنهادی با هدف کاهش افزونگی کدهای LT و اصلاح بهره وری کدگشایی در همان پیچیدگی انجام شده است.

در مقاله [۱۴]، نویسندگان طرح کد جدید LT را برای کانال BEC ارائه می دهند. طرح با کلمه مخفف MBDRSD[۱۲] با ایجاد فرم توزیع درجه چپ (LDD)[۱۳]، کلیه پارامترهای بهره وری سیستم را اصلاح می کند.

در مقاله [۲۸] آقای جمشیدی و همکارانش، از کدگشایی به روش BP توسعه یافته پس از عدم موفقیت کدگشایی BP سنتی سخن به میان می آورند و نشان می دهند که این روش کدگشایی برای بسته بیتهای منبع با طول کم بسیار مفید می باشند. پیچیدگی محاسباتی آن به همان اندازه روش BP سنتی می باشد و می تواند احتمال کدگشایی موفقیت آمیز در سربار ثابت را افزایش دهد. به عبارت دیگر، BP توسعه یافته پیشنهادی آنها می تواند با یک پیام کوتاه باعث کاهش سربار در اجرای آنها شود.

در کلیه آثار قبلی که در بالا به آن اشاره شد، کدگشاها نمی توانند عدم وجود بیت کدگذاری درجه یک در هر مرحله را تحمل کنند و با شکست مواجه خواهند شد. یکی از نوآوریهایی این مقاله پرداختن به این موضوع می باشد و روشی ارایه می شود که حتی در صورت عدم وجود بیت های کدگذاری شده از درجه یک، کدگشایی متوقف نمی شود. در قسمت بعد ابتدا روش کلی BP سنتی توضیح داده خواهد شد و در قسمتهای بعد، نوآوریهای مقاله به تفصیل بیان خواهد شد.

۳-۱- الگوریتم کدگشای BP

کدگشایی BP یک الگوریتم محبوب برای اکثر کدهای تنک می باشد و روش آن در شکل (۳) توضیح داده شده است.

BP Decoding:

1. Find one encoded packet with degree 1.
2. Put the value of the encoded packet as the value of its neighbor. Call it released encoding packet. The set of the source packets that must be recovered but not processed yet by the algorithm is called ripple set.
3. Pick a packet from the ripple set.
4. xor this packet with those unreleased encoding packets that have this packet in their neighbors.
5. Reduce the degree of xor ed encoding packet by one.
6. Back to step 1.

شکل (۳): مراحل متعلق به الگوریتم رمزگشای BP سنتی [۲۹]

روش فوق تا زمانی که همه بیت های منبع مشخص شوند تکرار می شود و یا اینکه هیچ بیت کدگذاری شده با درجه یک وجود نداشته باشد. اگر مجموعه موج دار قبل از بازیابی تمام بیت های منبع خالی شود، روش کدگشایی متوقف می شود و گیرنده در انتظار دریافت بیت های کدگذاری شده جدید با درجه یک می ماند. علاوه بر مباحث گفته شده، کدگشایی BP کمترین پیچیدگی محاسباتی را در بین الگوریتم های کدگشایی دیگر دارد، که به عنوان یکی از دلایل محبوبیت این الگوریتم به حساب می آید.

۳-۲- طرح جدید کدگذار

در ساختار کد LT معمولی، کدگذار بطور یکنواخت، بیت های پیام را به عنوان نمونه انتخاب می کند. در ارائه طرح جدید، انتخاب غیر یکنواخت گره ها به نفع انتخاب گره های پیام با درجه بالا برای افزایش تعداد بیت های کدگذاری شده با درجه پایین پیشنهاد می شود. برای این منظور، درجه لحظه ای هر گره پیام در هر زمان معین از روش کدگذاری در نظر گرفته می شود. الگوریتم پیشنهادی برای شکل دادن LDD با RSD به عنوان کد LT پیشنهادی بیان می شود. در الگوریتم ۱ روش پیشنهادی توضیح داده شده است (شکل (۴) را مشاهده نمایید).

Algorithm 1:

1- Generate a degree *d* from the right-hand side distribution, similar to RSD.
2- If *d* = 1, choose the data symbol with the highest instantaneous degree without a replacement.
3- If *d* ≠ 1, choose 2**d* uniformly distributed data symbols.
4- Using the message degree stack/list, we sort and choose the *d* lowest-degree nodes to form the encoded bit.
5- Perform an XOR of the chosen *d* data symbols to generate and transmit the code symbol C_n.
6- Repeat steps 1–5 until an acknowledgement signal is received.

شکل (۴): الگوریتم کدگذار جدید برای کد LT

۳-۳- طرح جدید کدگشا

اگر یک کدگذار LT در یک مجموعه متوقف شونده (SS) گیر کند، BP معمولی متوقف می شود و قادر به ادامه نخواهد بود. در چنین مواردی، باید روشی برای رهایی کدگذار از مجموعه متوقف کننده ارائه شود. روش جدید ارائه شده از این واقعیت نشات می گیرد که یک

کدگذار BP یک روش انتقال پیام در بطنش وجود دارد. پیچیدگی محاسباتی آن به همان اندازه کدگشای BP سنتی می باشد ولی می تواند احتمال کدگشایی موفقیت آمیز با سربار یکسان را افزایش دهد. این طرح جدید ابتدا با کدگشایی سنتی BP آغاز به کار می کند و در صورتی که در مجموعه متوقف کننده افتاد طرح ارائه شده جدید شروع به کار خواهد کرد.

همانطور که قبلاً ذکر شد، عدم یافتن بیت کد شده با درجه یک در کدگشایی در هر مرحله از فرآیند کدگشایی، منجر به شکست کدگشایی می شود. در کدگذار LT، بیت های کدگذاری شده با XOR کردن بیت های اطلاعاتی که به طور تصادفی انتخاب شده اند تولید می شوند. اگر یک بیت کدگذاری شده با درجه یک پیدا شود، بیت اطلاعاتی که به گره با درجه یک متصل می باشد مستقیماً کدگشایی می شود. در ادامه، بیت اطلاعات تعریف شده به بیت های کدگذاری شده دیگری اضافه می شوند که شامل بیت های اطلاعاتی در شکل گیری XOR آنها هستند. با این روش درجه بیت های کدگذاری شده کاهش می یابد. این را می توان به صورت ریاضی به شرح زیر توضیح داد: اگر

$$c_i = m_l \ \ and \ c_k = m_l \oplus m_p \oplus \ldots,$$

که c_k به صورت $c_k = c_i \oplus c_k$ کاهش می یابد.

برای بیت های کدگذاری شده که دارای درجه بیش از یک هستند، این عمل دارای محبوبیت می باشد. اگر c_i یک بیت کدگذاری شده باشد در آن $\deg(c_i) > 1$. آنگاه مجموعه اجرا را می توان بدین شکل $\mathrm{rs}(c_i) = \{m_l, m_s, \ldots\}$ تعریف کرد. این مجموعه شامل بیت های داده ای می باشد که هنگام تولید c_i مورد استفاده قرار می گیرد. اگر $\mathrm{rs}(c_i) \subset \mathrm{rs}(c_j)$، آنگاه c_j می تواند به $c_j = c_i \oplus c_j$, کاهش یابد، در این صورت درجه c_j ، به شکل $\deg(c_j) = \deg(c_j) - \deg(c_i)$ خواهد شد. این فرمول زمانی استفاده می شود که کدگشا نتواند بیت کدگذاری شده با درجه یک را پیدا کند، و بنابراین درجه گره را برای رسیدن به درجه یک می توان به درجه پایین تر کاهش داد. بعد از آن، می توان روش سنتی BP را برای کدگشایی اجرا کرد. این روش تا زمانی که رویکرد فوق قابل اجرا باشد ادامه خواهد یافت، در غیر این صورت کدگشا وارد مرحله بعدی الگوریتم می شود. دلیل آن هم این می باشد که هیچکدام از مجموعه های اجرا دیگر زیر مجموعه ای نخواهند داشت و این مرحله از کار متوقف می شود. مرحله بعدی بیت های کدگذاری شده با درجه دو را جستجو می کند. در این مرحله، رمزگشا سعی می کند درجه خود را تا درجه یک کاهش دهد. پس از آن، از الگوریتم رمزگشای سنتی BP برای کدگشایی بیت های کدگذاری شده باقیمانده استفاده می کند. این روند تا زمانی که تمام بیت های کدگذاری شده بازیابی نشده باشند ادامه می یابد. روش ذکر شده به صورت کامل در الگوریتم ۲ شرح داده شده است (شکل (۵) را ملاحظه کنید).

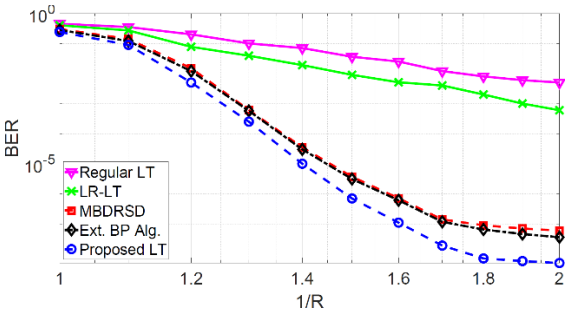
Algorithm 2:

d: The degree of check nodes
G : The generator matrix with dimensions $k \times n$
m: Selected information bits
c: Encoded bits
r_i : i^{th} row of G^T
$d(r_i)$: The number of 1s in row r_i,
for $i = 1 \rightarrow n$ do
A: Check the row contains a single 1 in G^T. (It is equal a degree one encoded bit).
If there is degree one set $G_{ij} = 0$, j = 1, … , k, that is, set the corresponding column elements to 0, and remove the row containing a single 1 from G^T.
If there is no degree one encoded bit, then calculate $d(r_i \oplus r_j)$, for j = i+1, i+2, … , n.
If $d(r_i \oplus r_j) = 1$,
Update G matrix
goto A.
end for
If L encoded bits are not recovered *then* choose a bit randomly with degree 2 among the remaining encoded bits.
Remove its neighbors from those encoded bits which also have these two encoded bits as the neighbor. To do so, xor their values with these encoded bits and decrease their degree 2 units.
Continue this process until finding a degree 1 encoded bit and go back to the traditional BP decoding algorithm.

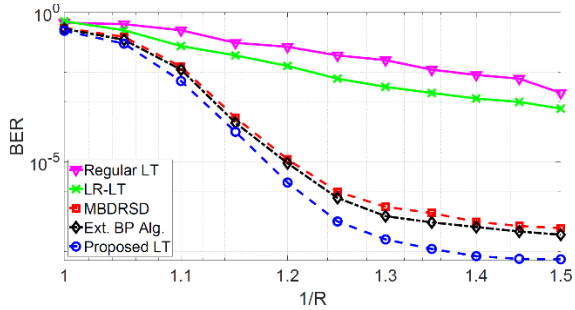
شکل (۵): الگوریتم کدگشای فرض شده برای کدهای LT

۴- نتایج شبیه سازی

برای بررسی اثربخشی کدک LT پیشنهادی از طریق شبیه سازی، ۱۰۰۰۰۰ بلوک پیام از طریق کانال BEC با استفاده از توزیع RSD ارسال شده است. نتایج BER[۱۴] با استفاده از روش مونت کارلو با میانگین گیری از همه نتایج بدست آمده است. در این بخش، مقایسه بین طرح پیشنهادی و الگوریتم معمولی LT، Low Redundancy (LR) در [۱۶] ، الگوریتم MBDRSD که ترکیبی از MBRSD [۱۴] و DRSD [۱۵] است، و همچنین طرح جدید آقای جمشیدی و همکارانش [۲۸] نشان داده شده است. از توزیع RSD با پارامترهای c = 0.02 و δ = 0.1 استفاده می شود. برای این منظور، تعداد بیت های کدگذاری شده اضافه شده به هر تلاش متوالی کدگشایی BP برابر با (k / 10) می باشد. علاوه بر این، نرخ کدگذاری به معنای نرخ کدگذاری انتقال یافته می باشد، یعنی بیت های محو شده در این نرخ در نظر گرفته می شوند. تعداد بیت های پیام، k، در یک بلوک پیام ۲۵۶ و ۱۰۲۴ بیت می باشد. این بسته ها توسط کدگذار از کانال در شرایط مختلف ارسال می شوند و سپس توسط ۵ نوع رمزگشا، بسته ها بازیابی می شوند. پارامترهای مهمی مانند BER و احتمال کدگشایی موفقیت آمیز برحسب نرخ کدگذاری، ضریب سربار و احتمال محو شدگی کانال مورد بررسی قرار گرفته است و نتایج در زیر مورد تجزیه و تحلیل قرار خواهند گرفت.



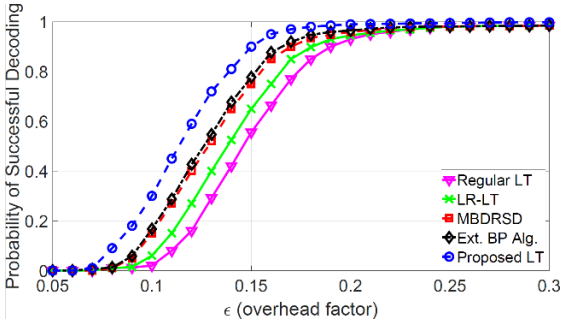
شکل (۶): BER بر حسب عکس نرخ کدگذاری برای طرح های مختلف در k = 256 بر روی کانال BEC با احتمال محو شونده α = 0.02.



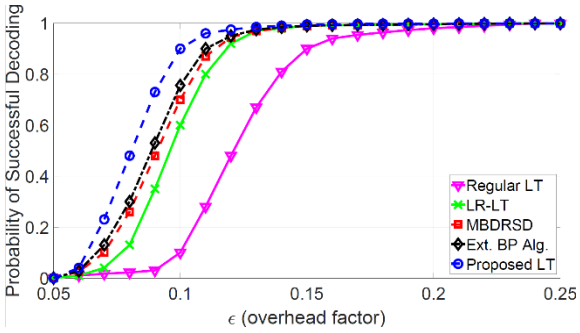
شکل (۷): BER بر حسب عکس نرخ کدگذاری برای طرح های مختلف در k = 1024 بر روی کانال BEC با احتمال محو شونده α = 0.02.

شکل (۶) و شکل (۷) نمودار BER را بر حسب معکوس نرخ کدگذاری متغیر (1/R) برای طرحهای مختلف نشان می دهد. منحنی در شکلهای ذکر شده به ترتیب برای k = 256 و ۱۰۲۴ بدست آمده است. نمودار تغییرات BER برای همه الگوریتم های ذکر شده ترسیم شده است. نتایج نشان می دهد که الگوریتم پیشنهادی نسبت به سایر موارد بهتر عمل کرده است.

با توجه به اشکال و نمودار های فوق، دلیل این پیشرفت قطعاً دو پدیده است که همزمان اتفاق می افتند. اول، در طراحی کدگذار به گونه ای که درجه گره های سمت راست به درستی تعیین می شوند، و دوم، در طرف دیگر کانال (رمز گشا)، پس از قطعی شدن عدم وجود گره با درجه یک، کدگشا تلاش می کند درجه ای پایین تر را با استفاده از درجه های موجود که برای کدگشایی ساخته شده است پیدا کند و باعث موفقیت بیشتر برای کدگشا شود.

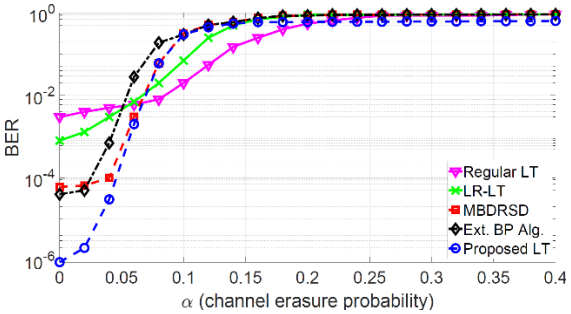


شکل (۸): احتمال کدگشایی موفق در طرح های مختلف بر حسب ضریب سربار در k = 256 با α = 0.2 .



شکل (۹): احتمال کدگشایی موفق در طرح های مختلف بر حسب ضریب سربار در k = 1024 با α = 0.2

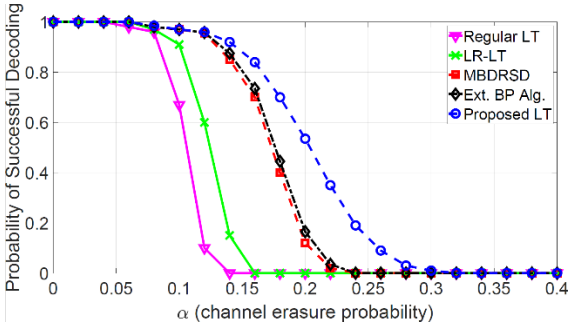
بهبود عملکرد مشابهی را می توان از منحنی احتمال کدگشایی موفقیت آمیز در شکل (۸) و شکل (۹) مشاهده کرد. در این موارد، از نظر ε ، همچنین مشاهده می شود که روش پیشنهادی به پیشرفت مورد انتظار دست پیدا می کند.



شکل (۱۰): BER بر حسب احتمال محو کنندگی کانال برای طرح های مختلف در k = 256 بر روی BEC با ε = 0.5.

شکل (۱۰)، BER را در برابر احتمال محو شدگی کانال (α) برای پنج کدگذار نشان می دهد. در این حالت مقدار پارامترها روی k = 256 و ε = 0.5 تنظیم می شوند. این منحنی نشان می دهد که الگوریتم پیشنهادی در این مقاله نسبت به کدک های دیگر برای پارامتر α با مقادیر بیش از 0.2 میزان BER کمتری دارد.

در شکل (۱۱)، منحنی های احتمال کدگشایی موفقیت آمیز بر حسب احتمال محو کنندگی کانال (α) برای پنج کدگذار می باشد. نشان می دهد که روش ارائه شده در این مقاله می تواند تقریباً همان رفتار کدگشایی را در منطقه آبشاری حفظ کند و همانطور که انتظار می رود، کاهش قابل توجهی از خطا را داشته باشد.



شکل (۱۱): احتمال کدگشایی موفق بر حسب احتمال محو کنندگی کانال برای طرح های مختلف در k = 256 برروی BEC با ε = 0.15

۵- نتیجه‌گیری

در این مقاله، یک کدگذار و همچنین کدگشای جدید برای کد LT درون کانال BEC طراحی شده است. از آنجا که کد LT از طریق توزیع درجه خاص تولید می شود و نتایج خوب روش کدگذاری جدید در ساختار شکل گیری درجه های سمت چپ به فرم جدید نشان از معرفی خانواده ای جدید از کد LT می باشد. طرح پیشنهادی با شکل دادن به توزیع درجه سمت چپ یا معادل آن در نمای موج، کلیه موارد مربوط به عملکرد سیستم را بهبود می بخشد. نتایج عددی حاصل از شبیه سازی صحت روش ارائه شده را بررسی می کند. به عبارت دیگر، نتایج شبیه سازی مونت کارلو نشان می دهد که چگونه کدگشایی، با موفقیت از مجموعه های متوقف کننده جهت پیشبرد هدف کدگشایی، خارج می شود. پیشرفت های نسبی زیادی در میزان نرخ خطا و احتمال کدگشایی موفقیت آمیز با کدگذار جدید در چندین موقعیت حاصل می شود. برای مثال، احتمال کدگشایی موفقیت آمیز بیش از ۸۳٪ بهبود می یابد، در حالی که $k = 256$ با $\alpha = 0.2$ و ضریب سربار برابر با 0.15 می باشد.

مراجع

[1] Byers, J. W., Michael L., Michael M., and Ashutosh R. "A digital fountain approach to reliable distribution of bulk data" ACM SIGCOMM Computer Communication Review Vol. 28, No. 4, 1998.

[2] Zhao, Y., Zhang Y., Francis CM L., Yu H., and Zhu Z. "Improved online fountain codes" IET Communications Vol.12, No. 18, 2018.

[3] Bahrami, N., Nor Hisham Haji K., Azli Y., TENGKU M. N. I., and TENGKU F. B. "Effect of Underwater Ambient Noise on Quadraphase Phase-shift Keying Acoustic Sensor Network Links in Extremely Low Frequency Band" International Journal of Engineering Vol. 30, No. 7, 2017.

[4] Khademi, M. "Adaptive Spectral Separation Two Layer Coding with Error Concealment for Cell Loss Resilience" International Journal of Engineering Vol. 13, No. 2, 2000.

[5] Luby, M. "LT codes" In The 43rd Annual IEEE Symposium on Foundations of Computer Science, 2002. Proceedings., pp. 271-280. IEEE, 2002.

[6] Shokrollahi, A. "Raptor codes" IEEE/ACM Transactions on Networking (TON) Vol. 14, No. SI, 2006.

[7] James S., Hayajneh K. F., and Yousefi S. "Robust quaternary fountain codes in AWGN interference" IET Communications Vol. 12, No. 20, 2018.

[۸] نادری، سمیرا و زارعی، زهرا و حقیقت، جواد و اسلامی، محسن"یک روش کدینگ وفقی با استفاده از اطلاعات حالت کانال منبع-رله و کدهای همینگ، برای مصالحه بین توان و احتمال خطا در شبکه های حسگر بی سیم" فصلنامه صنایع الکترونیک، دوره: ۹، شماره: ۴ ، ۱۳۹۷

[۹] نادری گوارشکی، یونس و خانی، حسن و رحیمی نژاد، احسان،"بررسی میزان بهبود کارایی ناشی از کدگذاری کانال در سیستم مخابراتی فراپهن باند در حضور تداخل میان سمبلی و نویز ناشی از چندی سازی تک بیتی "،سیزدهمین سمپوزیوم بین المللی پیشرفت های علوم و تکنولوژی:سرزمین پایدار، پژوهش های نوین در مهندسی برق و پزشکی،داورزن ،۱۳۹۷

[۱۰] کنارکوهی، محمد و توکلی، حسن. "ارائه روشی نوین برای تلفیق کدگذاری کانال و رمزنگاری مبتنی بر کدگذاری قطبی." پدافند الکترونیکی و سایبری ، دوره: ۴، شماره:۱ ، ۱۳۹۵.

[۱۱] سازدار، امیرمهدی، نجاتی جهرمی، منصور و احمدلو ، افشین. "بررسی و مقایسه و انواع روش‌های کد کذاری کانال در طراحی سامانه های دورسنجی فضایی بر اساس استاندارد CCSDS." علوم و فنون نظامی دوره: ۹, شماره ۲۶، ۱۳۹۳.

[12] Kuo-Kuang, Liao Y., Chen C., and Chang H. "Modified robust soliton distribution (MRSD) with improved ripple size for LT codes" IEEE Communications Letters Vol.17, No. 5, 2013.

[13] Lu, H., Feng L., Jianfei C., and Chuan H. F. "LT-W: Improving LT decoding with Wiedemann solver" IEEE Transactions on Information Theory Vol. 59, No. 12, 2013.

[14] Hayajneh K.F., Yousefi S., and Valipour M., "Improved Finite- Length Luby-Transform Codes in the Binary Erasure Channel" J. IET Commun., Vol. 9, No. 8, 2015.

[15] Sorensen J.H., Popovski P., and Ostergaard J., "Design and Analysis of LT Codes with Decreasing Ripple Size" IEEE Trans. Commun., Vol. 60, No. 11, 2012.

[16] Jiguang H., Hussain I., Li Y., Juntti M., and Matsumoto T. "Distributed LT codes with improved error floor performance" IEEE Access Vol. 7 pp. 8102-8110, 2019.

[17] Luo, P., Hui F., Weiguang S., Xiaoli Q., Yuhao Z., and Xueqing Z. "An ECSO-based approach for optimizing degree distribution of short-length LT codes" EURASIP Journal on Wireless Communications and Networking, Vol 76, No. 1, 2019.

[18] Suo, L., Gengxin Z., Dongmin B., Jing L., Haiping C., and Zijun L. "On the Fly Belief Propagation Decoding Algorithm for LT Codes" In International Conference in Communications, Signal Processing, and Systems, pp. 1793-1800. Springer, Singapore, 2017.

[19] Khonsari, H., Okpotse T., Valipour M., Yousefi S. "Analysis of ripple size evolution in the LT process" IET Communications Vol. 12, No. 14, 2018.

[20] Okpotse, T., and Shahram Y. "Systematic Fountain Codes for Massive Storage Using the Truncated Poisson Distribution" IEEE Transactions on Communications Vol. 67, No. 2, 2018.

[21] Yuan, X., and Li P. "On systematic LT codes" IEEE Communications letters Vol. 12, No. 9, 2008.

[22] Puducheri, S., Jorg K., and Thomas E. F. "Distributed LT codes" In 2006 IEEE International Symposium on Information Theory, pp. 987-991. IEEE, 2006.

[23] Han, Wei, Shengkai Xu, Daqing Huang, and Cheng Xu. "Analysis and Design of Rateless Two-way Relay Networks Based on a Multiply-and-Forward Scheme" Applied Sciences Vol. 10, No. 7, 2020.

[24] Hayajneh K. F., and Yousefi S. "Overlapped LT codes over the binary erasure channel: analysis and design" IET Communications Vol, 13, No. 16, 2019.

[25] Peng L., Fan H., Shi W., Qi X., Zhao Y., and Zhou X."An ECSO-based approach for optimizing degree distribution of short-length LT codes" EURASIP Journal

on Wireless Communications and Networking, No. 1, 2019.
[26] MacKay, D. J. "Fountain codes" IEE Proceedings-Communications Vol. 152, No. 6, 2005.
[27] Mirrezaei S.M., Faez K., Yousefi S. "Towards fountain codes. part ii: Belief propagation decoding" Wireless personal communications Vol. 77. No. 2, 2014.
[28] Jamshidi, A., and Moloudi S. "Extended Belief Propagation Decoding of Luby Transform Codes for the Small Number of Encoded Packets" Iranian Journal of Science and Technology, Transactions of Electrical Engineering Vol. 41, No. 4, 2017.
[29] Yedidia, J. S., William T. F., and Yair W. "Understanding belief propagation and its generalizations." Exploring artificial intelligence in the new millennium Vol. 8, 2003.

زیرنویس‌ها

[1] Digital Fountain Codes
[2] Ideal Soliton Distribution
[3] Robust Soliton Distribution
[4] improved ripple size
[5] Memory-Based RSD
[6] reduced ripple size scheme
[7] On the Fly Belief Propagation
[8] Probability Mass Function
[9] Truncated Poisson Distribution
[10] Binary Erasure Channel
[11] Right Degree Distribution
[12] Memory-Based Decreasing Ripple Size Distribution
[13] Left Degree Distribution
[14] Bit Error Rate