

تخمین ماتریس بررسی توازن کد کانولوشنال با نرخ k/n

در محیط نویزی مبتنی بر تبدیل والش- هادامارد

محمد خاکسار و حسین خالقی بیزکی

گذشت زمان و ناشی از پیشرفت و تکامل در دانش مخابرات است. همچنین به دلیل ایجاد سادگی در استفاده کاربران، لازم است سیستم‌های مخابراتی تولیدشده با استانداردهای متنوع در مناطق جغرافیایی گوناگون و همچنین مقاطع زمانی مختلف سازگار باشند. بنابراین رادیوها باید بتوانند به صورت هوشمند و نرم‌افزاری خود را با شرایط اقتضایی و استانداردهای شبکه‌ای که در آن به کار گرفته می‌شوند، تطبیق دهند. این تطبیق می‌تواند با کمک فرستنده و با دریافت اطلاعات اولیه از آن یا به صورت کور تنها با مشاهده و تحلیل سیگنال دریافتی صورت پذیرد. از این رو در برخی موارد لازم است تا یک رادیوی هوشمند، پارامترهای ارسال لایه فیزیکی شبکه، مانند نرخ ارسال، مدولاسیون، و از جمله کد تصحیح خطای کانال را به صورت کور تخمین بزند.

از جمله کدهای پرستفاده در سیستم‌های مخابراتی، کد کانولوشنال^۱ است. پژوهش‌های بسیاری در زمینه تخمین کور پارامترهای کدهای کانولوشنال انجام شده است: ابتدا Rice پیشنهادی را برای شناسایی کدگذار کانولوشنال در حالت خاص نرخ $1/n$ ، در سال ۱۹۹۵ مطرح کرد [۱]. این روش تنها برای حالت رشته دریافتی بدون نویز عمل کرده و برای شرایط نویزی کاربرد ندارد. در سال ۱۹۹۷، Filiol این روش را برای کد کانولوشنال با نرخ k/n توسعه داد [۲]. در ادامه، Baribier و همکاران در سال ۲۰۰۶ روشی جبری را برای تخمین پایه‌های کد دوگان کدهای خطی و کانولوشنال پیشنهاد کردند [۳]. Cote و همکاران در [۴] از روش پیشنهادی در [۵] که برای شناسایی و بازیابی کدهای باینری خطی پیشنهاد شده بود برای شناسایی کد کانولوشنال در شرایط نویزی بهره بردند. Wang و همکاران در [۶] روشی را بر مبنای الگوریتم اقلیدسی^۲ توسعه دادند و برای حالت کد کانولوشنال با نرخ $1/2$ به کار گرفتند. Dingel و همکاران روشی احتمالاتی بر مبنای بیشینه کردن امید^۳ را در [۷] برای شناسایی کد کانولوشنال با نرخ $1/n$ توسعه دادند که در آن نیاز به دانستن طول کلمات کد بوده و علاوه بر این، دارای پیچیدگی محاسباتی زیادی نیز می‌باشد. در [۸] Marizan و همکاران از ویژگی‌های جبری کد کانولوشنال بهره بردند و روشی مبتنی بر مرتبه^۴ برای شناسایی کد کانولوشنال با نرخ کلی k/n در حالت نویز پایین، یعنی کانال BSC با $P_e < 0.1$ پیشنهاد دادند، اما قلی‌زاده و همکاران در [۹] نشان دادند که رابطه تجربی پیشنهادشده در [۸] در حالت کلی برقرار نبوده و تنها برای نرخ کد $(n-1)/n$ صحیح است. آنها به صورت تحلیلی الگوریتمی جامع برای تخمین پارامترهای کد کانولوشنال پیشنهاد دادند.

در کاربردهای عملی، رشته‌بیت دریافتی ممکن است حاوی تعداد بیت خطای زیادی باشد و نرخ خطای آن حتی به 10^{-2} و بسیار بالاتر از آن

چکیده: یکی از چالش‌های رادیوهای هوشمند برای تطبیق خود با استانداردهای شبکه، تخمین کور پارامترهای ارسال و دریافت لایه فیزیکی است. این پارامترها می‌توانند شامل نرخ ارسال، مدولاسیون و شیوه کدگذاری اطلاعات برای مقابله با خطای کانال باشند. از این رو تخمین کد کانال، شامل پارامترهای کد، ماتریس بررسی توازن و ماتریس مولد، یکی از مسایل مطرح در زمینه رادیوهای نرم‌افزاری است. عموماً تخمین کد با استفاده از روش‌های جبری مانند روش اقلیدسی و روش‌های مبتنی بر محاسبه مرتبه بر روی رشته‌بیت دریافتی انجام می‌گیرد. اشکال عمده این روش‌ها، کارایی ضعیف آنها در محیط‌های نویزی است. یک روش برای حل مسأله تخمین کد، استفاده از روش‌های مبتنی بر تبدیل، مانند تبدیل والش- هادامارد می‌باشد. در این مقاله، الگوریتم جدیدی بر مبنای تبدیل والش- هادامارد برای بازسازی ماتریس بررسی توازن کد کانولوشنال با نرخ دلخواه k/n در شرایط نویزی بالا، یعنی کانال BSC با $P_e > 0.1$ ارائه می‌شود که دارای کارایی به مراتب بهتری نسبت به روش‌های قبلی است. در این الگوریتم، با بهره‌جستن از ویژگی‌های جبری کد کانولوشنال، یک دستگاه معادلات با $n-k$ معادله مستقل برای تخمین سطرهای ماتریس بررسی توازن، ایجاد شده و سپس با استفاده از تبدیل والش- هادامارد، معادلات به دست آمده حل می‌شوند. نتایج شبیه‌سازی از عملکرد مناسب روش پیشنهادی در شرایط نویزی بالا حکایت دارد.

کلیدواژه: رادیوی نرم‌افزاری، کد کانولوشنال، تخمین ماتریس بررسی توازن، تبدیل والش- هادامارد.

۱- مقدمه

سیستم‌های مخابرات دیجیتال با هدف افزایش نرخ داده و در عین حال افزایش قابلیت اطمینان و کیفیت سرویس، همواره تحت توسعه و بهینه‌سازی هستند. هر فرستنده و گیرنده مخابراتی از بلوک‌های مختلفی تشکیل شده است. یکی از بلوک‌های اساسی در هر سیستم مخابراتی دیجیتال، بلوک‌های کدگذار و کدبردار است که با هدف جبران خطای بیت ناشی از اثرات کانال و در نتیجه افزایش قابلیت اطمینان سیستم‌های مخابراتی مورد استفاده قرار می‌گیرد.

با وجود این که بیش از نیم‌قرن از ابداع کدهای تصحیح خطا می‌گذرد، کماکان این کدها با هدف بهبود توأم بازدهی بیت و افزایش قابلیت‌های تصحیح خطا در حال تحقیق و توسعه هستند. بنابراین یکی از واقعیت‌های موجود در سیستم‌های مخابراتی، تعدد استانداردها در سیستم‌های مختلف و تغییر جزئیات بلوک‌های سیستم‌های مخابراتی، از جمله بلوک کدگذار، با

این مقاله در تاریخ ۱۸ اردیبهشت ۱۳۹۷ دریافت و در تاریخ ۱۱ دی ماه ۱۳۹۷ بازنگری شد.

محمد خاکسار، مجتمع دانشگاهی برق و الکترونیک، دانشگاه صنعتی مالک اشتر، تهران، ایران، (email: z.m.khaksar@gmail.com).

حسین خالقی بیزکی (نویسنده مسئول)، مجتمع دانشگاهی برق و الکترونیک، دانشگاه صنعتی مالک اشتر، تهران، ایران، (email: bizaki@gmail.com).

1. Convolutional Code
2. Euclidean Algorithm
3. Expectation Maximization
4. Rank

به طوری که K را طول مؤثر کد^۳ گویند. اگر دنباله ورودی با $m(D)$ و دنباله خروجی با $c(D)$ نشان داده شود، فرایند کدگذاری را می‌توان به صورت زیر توصیف کرد

$$c(D) = m(D).G(D) \quad (۳)$$

در عمل کدگذاری‌هایی که استفاده می‌شوند بهینه^۴ هستند. یک کدگذار بهینه است اگر دارای بیشینه ممکن فاصله آزاد میان همه کدهای پارامترهای یکسان باشد. دلیل استفاده زیاد از این کدها این است که به ازای شرایط یکسان، قابلیت تصحیح خطای این کدها بسیار بیشتر است. به همین منظور در این مقاله فرض بر این است که در فرستنده از کدهای بهینه استفاده شده باشد.

۲-۲ کد دوگان کدهای کانولوشنال

فرض کنید C^\perp فضای دوگان کد C باشد. ماتریس مولد کد دوگان کد کانولوشنال که ماتریس بررسی توازن نیز نامیده می‌شود، می‌تواند برای توصیف کد کانولوشنال به کار رود. این ماتریس چندجمله‌ای با ابعاد $(n-k) \times n$ به شکل زیر قابل بیان است [۸]

$$H(D) = \begin{bmatrix} h_{1,1}(D) & \dots & h_{1,k}(D) & | & h_1(D) & \dots & \cdot \\ \vdots & \ddots & \vdots & | & \vdots & \ddots & \vdots \\ h_{n-k,1}(D) & \dots & h_{n-k,k}(D) & | & \cdot & \dots & h_n(D) \end{bmatrix}_{(n-k) \times n} \quad (۴)$$

و در قضیه زیر نیز صدق می‌کند:

قضیه ۱: فرض کنید $G(D)$ ماتریس مولد کد C باشد. ماتریس چندجمله‌ای $H(D)$ یک ماتریس بررسی توازن کد C است هر گاه [۱۲]

$$G(D).H^T(D) = 0 \quad (۵)$$

نتیجه فرعی ۱: فرض کنید $H(D)$ یک ماتریس بررسی توازن کد C باشد. دنباله خروجی $c(D)$ ، یک دنباله کلمه کد C است اگر و تنها اگر

$$c(D)_{1 \times n} . H^T(D)_{n \times (n-k)} = 0_{1 \times (n-k)} \quad (۶)$$

بر اساس ویژگی‌های کد دوگان و کدگذارهای کانولوشنال، حافظه کد دوگان که با μ^\perp نشان داده می‌شود به صورت زیر تعریف می‌شود [۱۳]

$$\mu^\perp = \sum_{i=1}^k \mu_i \quad (۷)$$

که در آن μ_i حافظه‌های تعریف شده در (۲) هستند.

ماتریس $H(D)^T$ دارای $n-k$ سطر است و بنابراین (۶) از $n-k$ معادله با حاصل \cdot تشکیل شده است. برای به دست آوردن $G(D)$ یا ماتریس معادل آن یعنی $H(D)$ ، تلاش می‌شود $n-k$ معادله بالا به طور مستقل از یکدیگر حل شوند.

اگر $H_i(D)$ برابر با i امین سطر ماتریس $H(D)$ باشد طبق (۶) داریم

$$c(D)_{1 \times n} . H_i^T(D)_{n \times 1} = 0_{1 \times 1}, \quad i = 1 : n-k \quad (۸)$$

$$H_i(D) = [h_{i,1}(D) \quad h_{i,2}(D) \quad \dots \quad h_{i,n}(D)]$$

که در آن $h_{i,j}(D)$ ها چندجمله‌ای‌هایی با درجه حداکثر μ^\perp به صورت زیر است

برسد که در این حالت، روش‌های رایج اشاره شده در قبل، مانند روش‌های اقلیدسی و روش‌های مبتنی بر مرتبه، کارایی ندارند. در [۱۰] Liu و همکاران روشی بر مبنای تبدیل والش- هادامارد^۱ برای شناسایی کد کانولوشنال با نرخ $1/n$ در شرایط نویز بالا، یعنی کانال BSC با $P_e > 0.05$ پیشنهاد دادند. در ادامه [۱۰]، Wang و همکاران در [۱۱] روشی بر مبنای تبدیل والش- هادامارد دوبخشی برای شناسایی کد کانولوشنال با نرخ $(n-1)/n$ در شرایط نویز بالا، یعنی کانال BSC با $P_e > 0.07$ ارائه دادند که نسبت به [۱۰] پیچیدگی محاسباتی و حافظه مورد نیاز آن بسیار کمتر است. نقصان دو مقاله اخیر در این است که مسئله تخمین کد را تنها برای حالت خاص با نرخ $1/n$ و $(n-1)/n$ حل نموده و راه حلی برای نرخ کلی k/n ارائه نکردند.

بر این اساس، مقاله حاضر، الگوریتمی جدید جهت تخمین کور ماتریس بررسی توازن^۲ برای حالت کلی نرخ k/n ، با فرض دریافت رشته‌بیت نویزی با نرخ خطای بالا، یعنی کانال BSC با $P_e > 0.07$ ارائه می‌دهد. این روش که بر مبنای تبدیل والش- هادامارد است، از ویژگی‌های جبری کد کانولوشنال بهره می‌برد.

ساختار مقاله حاضر بدین گونه می‌باشد که در بخش ۲، در ابتدا مفاهیم کدهای کانولوشنال و کد دوگان آنها و مقدمات مسئله ارائه شده و در ادامه، ویژگی‌های ماتریس بررسی توازن کد کانولوشنال بررسی می‌شود. در بخش ۳ پس از بیان ایده اصلی مقاله و روش استفاده از تبدیل والش- هادامارد در تخمین کد دوگان، الگوریتم تخمین کد دوگان برای کد کانولوشنال با نرخ دلخواه k/n تشریح می‌شود. در ادامه و در بخش ۴، عملکرد الگوریتم پیشنهادی مورد ارزیابی و بررسی قرار می‌گیرد. در خاتمه در بخش ۵ جمع‌بندی مختصری از دستاوردهای مقاله ارائه می‌شود.

۲- کدهای کانولوشنال و تبدیل والش- هادامارد

۱-۲ تعاریف اولیه و مدل ریاضی

حافظه یکی از مهم‌ترین مشخصه‌های کدگذارهای کانولوشنال است. بر خلاف کدگذارهای بلوکی، خروجی یک کدگذار کانولوشنال در هر لحظه به ورودی در لحظات قبلی بستگی دارد. به همین دلیل معمولاً کدگذارهای کانولوشنال را با ماتریس‌های چندجمله‌ای مولد نمایش می‌دهند. فرض کنید C یک کد کانولوشنال (n, k, μ) باشد، به صورتی که n تعداد خروجی‌ها، k تعداد ورودی‌ها و μ مرتبه حافظه کدگذار است. ماتریس مولد چندجمله‌ای کد C یعنی $G(D)$ ، با مرتبه k به صورت زیر تعریف می‌شود

$$G(D) = \begin{bmatrix} g_{1,1}(D) & \dots & g_{1,n}(D) \\ \vdots & \ddots & \vdots \\ g_{k,1}(D) & \dots & g_{k,n}(D) \end{bmatrix}_{k \times n} \quad (۱)$$

حافظه i امین ورودی یعنی μ_i و مرتبه حافظه کد کانولوشنال به صورت زیر تعریف می‌شوند [۱۲]

$$\mu_i = \max_{j=1, \dots, n} \deg(g_{i,j}), \quad \forall i = 1, \dots, k \quad (۲)$$

$$\mu = \max_{i=1, \dots, k} \mu_i = K - 1$$

3. Constraint Length

4. Optimal

1. Walsh-Hadamard Transform

2. Parity-Check Matrix

Archive of SID

$$y(D) = c(D) + e(D) \tag{۱۲}$$

که در آن $c(D)$ که برداری با درایه‌های چندجمله‌ای در حوزه تبدیل است، دنباله گذشته خروجی (۳) می‌باشد. معادله (۱۱) برای حالت رشته‌بیت دریافتی نویزی به صورت (۱۳) قابل بیان است. در حالت نویزی، عبارت $Y_{(N+1) \times (\mu^+ + 1)n} \cdot h_{i,(\mu^+ + 1)n \times 1}$ دقیقاً برابر \cdot نیست و در عمل سعی می‌شود با زیادکردن سطرهای ماتریس Y یا همان تعداد معادله‌ها به وسیله افزایش طول مشاهده رشته‌بیت دریافتی، y ، اثر نویز را کاهش داد تا احتمال خطا در تشخیص بردارهای h_i کاهش یابد.

چالشی که در اینجا وجود دارد این است که ماتریس ضرایب همه $n-k$ (۱۳)، یعنی Y یکسان است (به ازای تمامی $i = 1 : n-k$ یک Y داریم).

برای حل این مشکل باید به روشی بتوان به ضرایب متفاوت برای این دستگاه‌های معادلات رسید. برای این منظور باید به طریقی (۱۳) را به صورت زیر تبدیل نمود

$$Y_s \cdot h_s \approx \cdot, s = 1 : n-k \tag{۱۴}$$

نحوه انجام این کار با استفاده از دانسته‌های قبلی در مورد بردار h_i در بخش ۲-۳ و روش حل این دستگاه‌ها (یافتن h_i ها) در بخش ۳ توضیح داده خواهد شد.

۳-۲ ویژگی‌های ماتریس بررسی توازن کد کانولوشنال

به منظور بهره‌بردن از ویژگی‌های جبری کد کانولوشنال در حل مستقل $n-k$ (۱۳)، باید ماتریس بررسی توازن به صورت عمیق‌تری مورد

$$h_{i,j}(D) = h_{i,j}(\cdot) + h_{i,j}(1) \cdot D + h_{i,j}(\tau) \cdot D^\tau + \dots + h_{i,j}(\mu^+) \cdot D^{\mu^+} \tag{۹}$$

$$j = 1 : n$$

$$i = 1 : n-k$$

ذکر این نکته لازم است که تمامی روابط بیان شده در بالا و فرمت داده‌های آنها در حوزه تبدیل (حوزه D) بیان شده‌اند اما در گیرنده، دنباله گذشته دریافتی به صورت یک دنباله زمانی است. از آنجا که این داده، حجم زیادی دارد و برای تغییر فرمت آن به حوزه تبدیل نیاز به پردازش دارند، به منظور کاهش پیچیدگی پیاده‌سازی بهتر است روابط مورد نیاز برای تخمین پایه‌های کد دوگان را به حوزه زمان بیان کنیم.

اگر c_m یک برش دلخواه از دنباله رشته‌بیت گذشته (بدون نویز) در حوزه زمان با طول $(N + \mu^+ + 1)n$ در نظر گرفته شود، (۸) می‌تواند به صورت زیر بازنویسی گردد [۱۱]

$$\sum_{j=1}^n \sum_{l=0}^{\mu^+} c_{n(l+t)+j-1} \cdot h_{i,j}(\mu^+ - l) = \cdot \tag{۱۰}$$

$$t = 0 : N, i = 1 : n-k$$

که می‌توان آن را به صورت ضرب ماتریسی (۱۱) نیز بیان نمود. با توجه به این که هدف مقاله حاضر تخمین ماتریس کد دوگان بر اساس رشته‌بیت دریافتی نویزی است، برای مدل کردن خطای تولیدشده در سیستم انتقال، کانال BSC با احتمال خطای P_e در نظر گرفته شده و الگوی خطا با $e(D)$ و دنباله دریافتی نویزی با $y(D)$ نشان داده می‌شود به گونه‌ای که

$$\begin{bmatrix} c_1 & c_2 & \dots & c_{n-1} & c_n & \dots & c_{\mu^+ n} & \dots & c_{(\mu^+ + 1)n-1} \\ c_n & c_{n+1} & \dots & c_{2n-1} & c_{2n} & \dots & c_{(\mu^+ + 1)n} & \dots & c_{(\mu^+ + 2)n-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ c_{Nn} & c_{Nn+1} & \dots & c_{(N+1)n-1} & c_{(N+1)n} & \dots & c_{(N+\mu^+)n} & \dots & c_{(N+\mu^+ + 1)n-1} \end{bmatrix}_{(N+1) \times (\mu^+ + 1)n} \cdot \begin{bmatrix} h_{i,1}(\mu^+) \\ h_{i,2}(\mu^+) \\ \vdots \\ h_{i,n}(\mu^+) \\ h_{i,1}(\mu^+ - 1) \\ \vdots \\ h_{i,n}(\mu^+ - 1) \\ \vdots \\ h_{i,1}(\cdot) \\ \vdots \\ h_{i,n}(\cdot) \end{bmatrix}_{(\mu^+ + 1)n \times 1} = \tag{۱۱}$$

$$C_{(N+1) \times (\mu^+ + 1)n} \cdot h_{i,(\mu^+ + 1)n \times 1} \approx \cdot, i = 1 : n-k$$

$$\begin{bmatrix} y_1 & y_2 & \dots & y_{n-1} & y_n & \dots & y_{\mu^+ n} & \dots & y_{(\mu^+ + 1)n-1} \\ y_n & y_{n+1} & \dots & y_{2n-1} & y_{2n} & \dots & y_{(\mu^+ + 1)n} & \dots & y_{(\mu^+ + 2)n-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ y_{Nn} & y_{Nn+1} & \dots & y_{(N+1)n-1} & y_{(N+1)n} & \dots & y_{(N+\mu^+)n} & \dots & y_{(N+\mu^+ + 1)n-1} \end{bmatrix}_{(N+1) \times (\mu^+ + 1)n} \cdot \begin{bmatrix} h_{i,1}(\mu^+) \\ h_{i,2}(\mu^+) \\ \vdots \\ h_{i,n}(\mu^+) \\ h_{i,1}(\mu^+ - 1) \\ \vdots \\ h_{i,n}(\mu^+ - 1) \\ \vdots \\ h_{i,1}(\cdot) \\ \vdots \\ h_{i,n}(\cdot) \end{bmatrix}_{(\mu^+ + 1)n \times 1} = \tag{۱۳}$$

$$Y_{(N+1) \times (\mu^+ + 1)n} \cdot h_{i,(\mu^+ + 1)n \times 1} \approx \cdot, i = 1 : n-k$$

Archive of SID

$$[c_1(D) \dots c_k(D) \ c_{k+s}(D)]. \begin{bmatrix} h_{s,1}(D) \\ \vdots \\ h_{s,k}(D) \\ h(D) \end{bmatrix} = \sum_{i=1}^k c_i(D)h_{s,i}(D) + c_{k+s}(D)h(D) = 0, \quad (21)$$

$$\forall s = 1, \dots, n-k$$

بنابراین $(n-k)$ بردار (18) که بردارهای بررسی توازن نامیده می‌شوند، اگر بدون عناصر همیشه صفر آنها در نظر گرفته شوند، به صورت زیر قابل بیان هستند

$$h_s = (H_{\mu^+}^{(s)} \ H_{\mu^+-1}^{(s)} \ \dots \ H_1^{(s)}) \quad (22)$$

به طوری که $H_l^{(s)}$ ، یک بردار سطری با اندازه $(k+1)$ است که به صورت زیر تعریف می‌شود

$$H_l^{(s)} = (h_{s,1}(l) \ \dots \ h_{s,k}(l) \ h(l)) \quad (23)$$

اندازه بردارهای بررسی توازن (22) با S نشان داده می‌شود

$$S = (k+1) \cdot (\mu^+ + 1) \quad (24)$$

۳- روش پیشنهادی

به منظور تخمین ماتریس کدگذار با نرخ دلخواه k/n ، به تخمین ماتریس کدگذار کد دوگان متناظر آن یعنی $H(D)$ ، با $n-k$ سطر نیاز است. الگوریتم پیشنهادی، روشی را برای بازسازی تعداد $n-k$ بردار h_j (18) از رسته‌بیت دریافتی و در نتیجه به دست آوردن $H(D)$ و در پی آن ماتریس کدگذار $G(D)$ ارائه می‌دهد. با توجه به این که تمرکز الگوریتم پیشنهادی بر روی تخمین ماتریس مولد کد است، فرض بر این است که n ، k و μ^+ با روش‌های دیگر، مثلاً $[8]$ تخمین زده شده باشند. همچنین همان طور که از ماتریس C (11) مشخص است، به منظور حصول نتیجه صفر در حاصل ضرب ماتریسی این رابطه، مکان ابتدای برش دلخواه مشاهده داده در حوزه زمان باید مضربی از n باشد. این هم‌زمان‌سازی با تخمین پارامترهای کد انجام می‌شود. هم‌زمان‌سازی اشاره شده نیز به همراه تخمین پارامتر در این پژوهش، انجام شده فرض می‌شود.

همان طور که در انتهای بخش ۲-۲ اشاره شد چالشی که برای تخمین تعداد $n-k$ بردار h_j در (13) وجود داشت این بود که دستگاه معادلات برای همه h_j ها یکسان بود. به عبارت دیگر، ماتریس ضرایب همه $n-k$ (13) ، یعنی Y ، یکسان بود.

برای حل این چالش و به دست آوردن $n-k$ دستگاه معادله مختلف، از نکته‌ای که در انتهای بخش ۲-۳ در رابطه با عناصر همیشه صفر ماتریس بررسی توازن بیان شد، به عنوان دانسته قبلی در مورد h_j ها استفاده می‌شود: بردارهای h_j (13) دارای عناصر همیشه صفر هستند و به عبارت دیگر با حذف این عناصر از بردار h_j و تبدیل آن به بردار h_s و در پی آن حذف ستون‌های متناظر با این صفرها در ماتریس Y و تبدیل

$$H_l = \left[\begin{array}{ccc|ccc} h_{1,1}(l) & \dots & h_{1,k}(l) & | & h_1(l) & \dots & \cdot \\ \vdots & \dots & \vdots & | & \vdots & \ddots & \vdots \\ h_{i,1}(l) & \dots & h_{i,k}(l) & | & \cdot & h_i(l) & \cdot \\ \vdots & \dots & \vdots & | & \vdots & \ddots & \vdots \\ h_{n-k,1}(l) & \dots & h_{n-k,k}(l) & | & \cdot & \dots & h_l(l) \end{array} \right] \quad (17)$$

بررسی قرار گیرد. برای این منظور، نمایش باینری ماتریس بررسی توازن در (4) را به صورت زیر در نظر بگیرید $[8]$

$$H = \begin{bmatrix} H_{\mu^+} & \dots & H_1 & H_1 & \cdot & \cdot & \dots \\ \cdot & H_{\mu^+} & \dots & H_1 & H_1 & \cdot & \dots \\ \cdot & \cdot & H_{\mu^+} & \dots & H_1 & H_1 & \cdot \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots \end{bmatrix} = \begin{bmatrix} [& \mathcal{H} &] & \cdot & \cdot & \dots \\ \cdot & [& \mathcal{H} &] & \cdot & \dots \\ \cdot & \cdot & [& \mathcal{H} &] & \dots \\ \vdots & \vdots & \vdots & \ddots & \ddots & \ddots \end{bmatrix} \quad (15)$$

که در آن

$$[\quad \mathcal{H} \quad] = [H_{\mu^+} \ H_{\mu^+-1} \ \dots \ H_1 \ H_1] \quad (16)$$

به صورتی که $H_l, \forall l = 0, \dots, \mu^+$ ماتریس‌هایی با اندازه $(n-k) \times k$ به صورت (17) هستند. ماتریس بررسی توازن (15) ، در اصل از نسخه‌های شیف‌یافته $(n-k)$ بردار سطری تشکیل شده است. این بردارهای سطری را با طول $n \cdot (\mu^+ + 1)$ به صورت $h_i, \forall i = 1, \dots, n-k$ نشان داده و به صورت زیر تعریف می‌کنیم

$$h_i = (H_{\mu^+}^{(i)} \ H_{\mu^+-1}^{(i)} \ \dots \ H_1^{(i)} \ H_1^{(i)}) \quad (18)$$

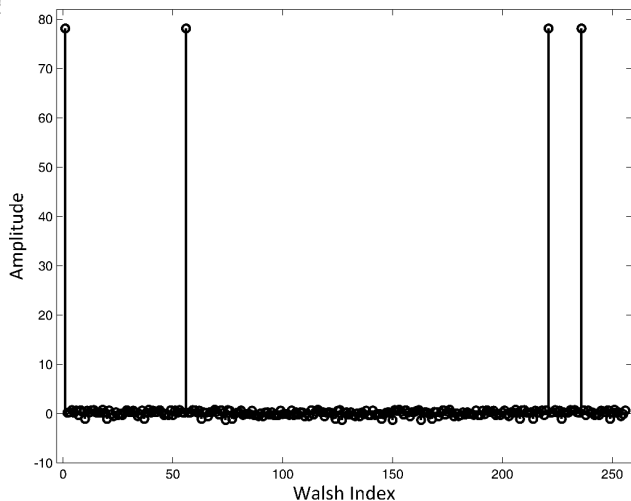
به طوری که $H_l^{(i)}$ سطر i ام ماتریس H_l ، یک بردار سطری با طول n به صورت زیر است

$$H_l^{(i)} = (h_{i,1}(l) \ \dots \ h_{i,k}(l) \ \cdot_{j-1} \ h_i(l) \ \cdot_{n-k-i}) \quad (19)$$

که در آن \cdot_p برداری تمام صفر با اندازه p است. همان طور که مشاهده می‌شود در (19) دو دسته بردار صفر وجود دارد و بنابراین در بردار h_i (18) به تعداد $2 \times (\mu^+ + 1)$ دسته بردار صفر در مکان‌های زیر قرار دارند

- دسته اول و دوم: از $k+1$ تا $k+s-1$ ، و از $k+s+1$ تا n .
- دسته دوم و سوم: از $k+n+1$ تا $k+n+s-1$ ، و $k+n+s+1$ تا $2n$.
- ...
- دسته $2\mu^+ + 1$ ام و $2(\mu^+ + 1)$ ام: از $k + \mu^+ n + 1$ تا $k + \mu^+ n + s - 1$ و از $k + \mu^+ n + s + 1$ تا $(\mu^+ + 1)n$.

به طوری که $s = 1: n-k$. لازم به ذکر است که h_i های (18) ، همان h_i های (13) می‌باشند. در حالت کدگذار کانولوشنال با نرخ k/n ، هر h_i از $(\mu^+ + 1) \cdot (n-k)$ درایه صفر تشکیل شده است. در این حالت با حذف درایه‌های همیشه صفر، (6) به $(n-k)$ معادله به صورت (21) تجزیه می‌شود



شکل ۲: طیف والش بردار V برای کد (۲.۱.۲) به ازای مقدار غیر صحیح μ^+ .

صحت پارامترهای تخمین زده شده یعنی k ، n و μ^+ را می‌توان از تعداد پیک‌های طیف والش بردار v دریافت. بر اساس طیف والش به دست آمده در (۳۰) سه حالت وجود دارد [۱۱]: اگر n و k مفروض صحیح نباشد، در طیف والش پیکی مشاهده نخواهد شد. اگر n و k صحیح باشند و μ^+ مفروض هم به درستی در نظر گرفته شده باشند، در کنار پیکی که در صفر وجود دارد تنها یک پیک دیگر در طیف والش وجود خواهد داشت (شکل ۱). تبدیل مکان این پیک به مقدار باینری، بردار h_s را در دستگاه (۲۵) نتیجه خواهد داد. اگر n و k مفروض صحیح باشند و μ^+ صحیح نباشند، همان طور که در شکل ۲ نشان داده شده است، چندین جواب برای دستگاه معادلات و در نتیجه چندین پیک خواهیم داشت که تعداد این پیک‌ها با پارامترهای کد دارای رابطه است [۱۰] و [۱۱].

۲-۳ الگوریتم پیشنهادی

با توجه به مباحث مطرح شده در بخش قبلی، الگوریتم پیشنهادی برای تخمین ماتریس بررسی توازن کد به شرح زیر قابل بیان است:
ورودی‌ها: n ، k ، μ^+ ، پارامتر هم‌زمانی و برش دلخواهی از رشته‌بیت دریافتی

خروجی‌ها: $h_j, \forall j = 1, \dots, n-k$

قدم اول: تشکیل ماتریس Y با توجه به رشته‌بیت دریافتی بر اساس (۱۳).

قدم دوم: $s = 1$

قدم سوم: تبدیل ماتریس ضرایب Y به Y_s بر اساس توضیحات بخش ۳.

قدم چهارم: محاسبه بردار v و طیف والش آن با توجه به (۲۸) و (۳۰).
 قدم پنجم: یافتن مکان پیک $H(v)$ و تبدیل آن به بردار باینری h_s .
 قدم ششم: جایگذاری صفرهای حذف شده، تبدیل h_s به h_j مطابق (۱۸) و (۱۹).

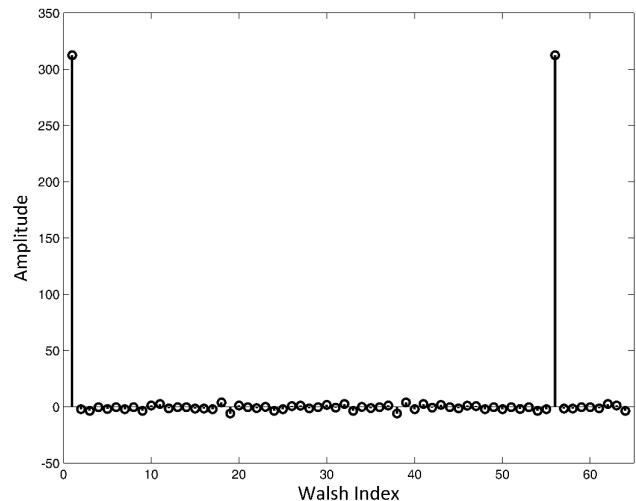
قدم هفتم: به مقدار s ، یک واحد اضافه شود.

قدم هشتم: اگر $s < n-k$ ، برو به قدم سوم و در غیر این صورت برو به قدم بعد.

قدم نهم: چاپ h_1 تا h_{n-k} در خروجی.

قدم دهم: پایان.

این الگوریتم به صورت روندنا در شکل ۳ ارائه شده است. از آنجا که الگوریتم پیشنهادی، $n-k$ بار تکرار الگوریتم [۹] (از حیث محاسبه



شکل ۱: طیف والش بردار V برای کد (۲.۱.۲) به ازای مقادیر صحیح n و μ^+ .

آن به ماتریس Y_s ، نتیجه حاصل ضرب تغییر نخواهد کرد. به عبارت دیگر، دو دستگاه (۱۳) و (۱۴) یکسان خواهند بود. با حذف این صفرها، تعداد سطرهای بردار h_s و ماتریس Y_s برابر با S (رابطه (۲۴)) خواهد شد. در این صورت (۱۳) به رابطه زیر تبدیل می‌گردد

$$Y_s h_s \approx 0, \quad s = 1 : n-k \quad (25)$$

که همان (۱۴) در بخش ۲-۲ است که هدف‌گذاری شده بود به آن دست پیدا کنیم. در اینجا هدف، حل معادله فوق است. یکی از روش‌های حل معادله فوق استفاده از تبدیل والش - هادامارد می‌باشد که در ادامه بیان می‌شود.

۳-۱ تبدیل والش - هادامارد

یکی از کاربردهای تبدیل والش - هادامارد، حل معادلات خطی در میدان باینری F_2 است. در این قسمت از این تبدیل برای حل دستگاه (۲۵) استفاده می‌شود [۱۱].

i امین سطر ماتریس Y_s در (۲۵) را به صورت بردار Y_{s_i} با ابعاد S در نظر گرفته و به عدد دهدهی v_i به صورت رابطه زیر تبدیل کنید

$$v_i = [Y_{s_i}(1), Y_{s_i}(2), \dots, Y_{s_i}(S)] \cdot [2^0, 2^1, \dots, 2^{S-1}]^T \quad (26)$$

بردار جدید v_i با طول 2^S به صورت زیر ساخته می‌شود

$$v_i = [\underbrace{0, \dots, 0}_{v_i}, 1, 0, \dots, 0] \quad (27)$$

ماتریس Y_s همانند ماتریس Y دارای $N+1$ سطر است و v به صورت رابطه زیر برای همه سطرهای ماتریس محاسبه می‌شود

$$v = \sum_{i=1}^{N+1} v_i \quad (28)$$

تعریف ماتریس هادامارد را به صورت زیر در نظر بگیرید

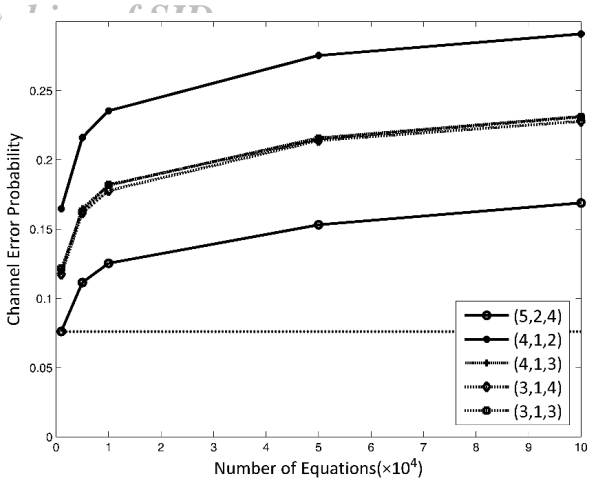
$$H_h^m = \begin{bmatrix} H_h^{m-1} & H_h^{m-1} \\ H_h^{m-1} & -H_h^{m-1} \end{bmatrix} \quad (29)$$

که در آن داریم $H_h^1 = [1]$.

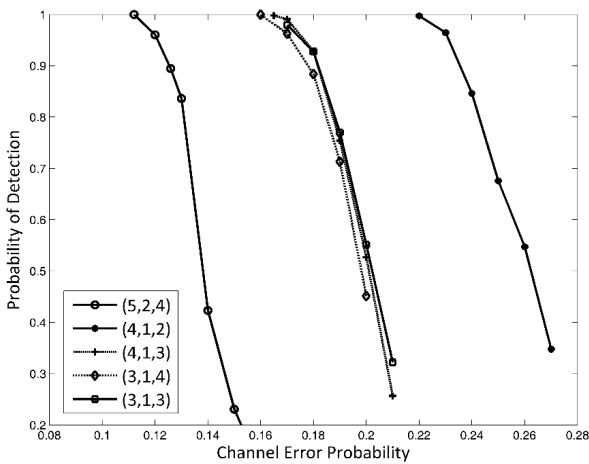
تبدیل والش - هادامارد بردار v به صورت زیر قابل بیان است [۱۴]

$$H(v) = v \cdot H_h^{(\mu^+ + 1)n+1} \quad (30)$$

به طوری که $H(v)$ طیف والش بردار v نامیده می‌شود.



شکل ۴: عملکرد الگوریتم در مقادیر مختلف از بلوک مشاهدات (N)، تعداد سطریهای ماتریس Y (۱۳).

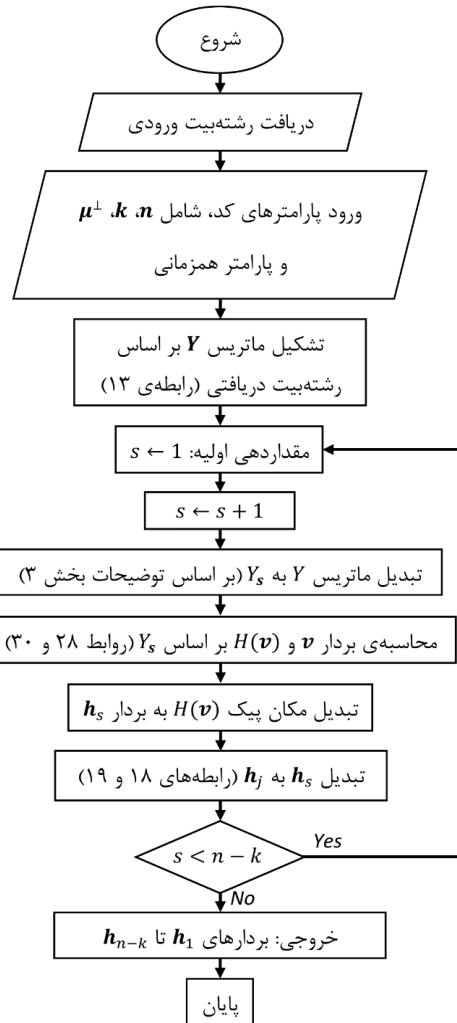


شکل ۵: عملکرد الگوریتم پیشنهادی در نرخ خطاهای مختلف.

به منظور ارزیابی اثر طول بلوک مشاهده رشته‌بیت دریافتی بر کارایی الگوریتم پیشنهادی، در شکل ۴ نرخ خطایی از کانال که می‌توان در آن ماتریس بررسی توازن را با احتمال ۹۰٪ شناسایی کرد بر حسب طول بلوک مشاهده رسم شده است. محور افقی در این شکل بر حسب تعداد سطریهای ماتریس Y (۱۳)، یا همان تعداد معادله‌ها که معیاری از طول بلوک رشته‌بیت مشاهده شده است می‌باشد.

همان‌طور که مشاهده می‌شود عملکرد الگوریتم پیشنهادی با افزایش طول بلوک مشاهده از رشته‌بیت دریافتی بهبود می‌یابد و نرخ خطای کانال که در آن، عملکرد الگوریتم حتی با طول کوتاه بلوک مشاهده، قابل قبول است حدود ۷٪ می‌باشد که در شکل با خط افقی نقطه‌چین نشان داده شده است. اگرچه با افزایش طول بلوک مشاهده تا تعداد ۱۰۰۰۰ معادله (تعداد سطریهای ماتریس Y (۱۳))، عملکرد الگوریتم با سرعت زیادی بهبود می‌یابد و پس از آن، سرعت بهبود عملکرد، کاهش یافته و تقریباً ثابت می‌ماند. بنابراین طول مشاهدات به اندازه ۱۰۰۰۰ معادله، یک مقدار قابل قبول خواهد بود.

در شکل ۵ احتمال شناسایی صحیح کد دوگان برای طول مشاهده معادل با ۱۰۰۰۰ معادله نشان داده شده است. از این شکل مشاهده می‌شود که الگوریتم پیشنهادی، حتی برای نرخ خطاهای بالا دارای کارایی حدود ۱۰۰٪ می‌باشد و این برتری الگوریتم پیشنهادی نسبت به مقالات مشابه است. برای بررسی دقیق‌تر این موضوع، شبیه‌سازی بعد را در نظر بگیرید.



شکل ۳: روندنمای الگوریتم پیشنهادی تخمین کد کانولوشنال.

پیچیدگی محاسباتی) با تفاوت در ابعاد ماتریس (۱۳) است، با استفاده از [۱۰]، پیچیدگی محاسباتی الگوریتم پیشنهادی از مرتبه $O(S \times 2^S)$ و حافظه مورد نیاز نیز برابر با 2^{2S} است که در آن S ، متغیر تعریف شده در (۲۴) است.

بحث: الگوریتم پیشنهادی در حالت خاص نرخ $(n-1)/n$ برابر با الگوریتم ارائه شده در [۱۱] می‌باشد. به عبارت دیگر، الگوریتم ارائه شده در [۱۱] یک حالت خاص از الگوریتم پیشنهادی در این مقاله می‌باشد. ماتریس بررسی توازن در الگوریتم پیشنهادی برای حالت خاص $(n-1)/n$ ، تنها یک سطر خواهد داشت و اندیس i در بردار h_i (۱۸) تنها مقدار ۱ را اختیار خواهد کرد. در این بردار، درایه‌های همیشه صفر وجود ندارد و در این حالت تنها یک دستگاه معادلات باینری (۱۳) برای تخمین h نیاز است. در این حالت، S (۲۴)، برابر با L در [۱۱] خواهد بود و پیچیدگی محاسباتی الگوریتم پیشنهادی و الگوریتم [۱۱] یکسان و برابر با $O(L \times 2^L)$ و حافظه مورد نیاز نیز یکسان و برابر با 2^{2L} خواهند بود.

۴- شبیه‌سازی الگوریتم و بررسی کارایی

به منظور بررسی کارایی الگوریتم پیشنهادی در نرخ خطاهای بالا، رشته‌بیت‌هایی با کدهای کانولوشنال مختلف با نرخ‌های ۱/۳، ۱/۴ و ۲/۵ تولید شده و از کانال BSC با احتمال خطاهای از ۰/۰۸ تا ۰/۲۷ عبور داده شده‌اند.

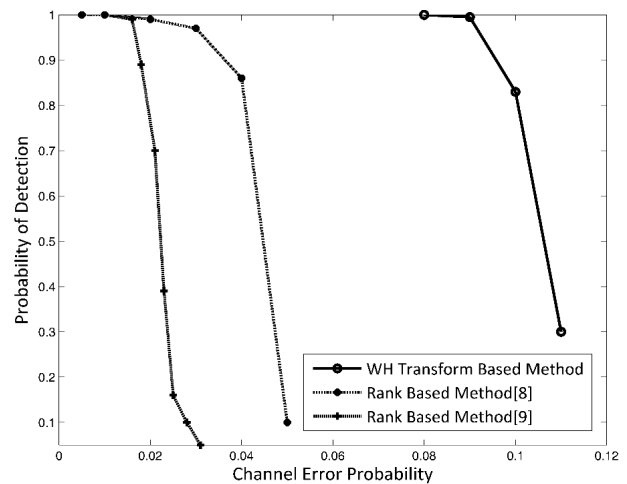
- [3] J. Barbier, G. Sicot, and S. Houcke, "Algebraic approach for the reconstruction of linear and convolutional error correcting codes," *International Journal of Applied Mathematics and Computer Science*, vol. 2, no. 3, pp. 113-118, Nov. 2006.
- [4] M. Cote and N. Sendrier, "Reconstruction of convolutional codes from noisy observation," in *Proc. IEEE Int. Symp. on Information Theory, ISIT'09*, pp. 546-550, Seoul, South Korea, 28 June-3 Jul. 2009.
- [5] A. Valembois, "Detection and recognition of a binary linear code," *Discrete Applied Mathematics*, vol. 111, no. 1-2, pp. 199-218, Jul. 2001.
- [6] F. Wang, Z. Huang, and Y. Zhou, "A method for blind recognition of convolution code based on euclidean algorithm," in *Proc. Int. Conf. on Wireless Communications, Networking, and Mobile Computing, WiCom'07*, pp. 1414-1417, Shanghai, China, 21-25 Sept. 2007.
- [7] J. Dingel and J. Hagenauer, "Parameter estimation of a convolutional encoder from noisy observations," in *Proc. IEEE Int. Symp. on Information Theory, ISIT'07*, pp. 1776-1780, Nice, France, 24-29 Jun. 2007.
- [8] M. Marazin, R. Gautier, and G. Burel, "Blind recovery of k/n rate convolutional encoders in a noisy environment," *EURASIP J. on Wireless Communications and Networking*, vol. 2011, no. 168, Article, 9 pp., Nov. 2011.
- [9] A. Gholizadeh Soteh and H. Khaleghi Bizaki, "On the analytical solution of rank problem in the convolutional code identification context," *IEEE Communications Letters*, vol. 20, no. 3, pp. 442-445, Jan. 2016.
- [10] J. Liu, X. J. Wang, and X. Y. Zhou, "Blind recognition of convolutional coding based on Walsh-Hadamard transform," *J. of Electronics and Information Technology*, vol. 32, no. 4, pp. 884-888, Apr. 2010.
- [11] F. Wang, H. Xie, and Z. Huang, "Blind reconstruction of convolutional code based on segmented Walsh-Hadamard transform," *J. of Systems Engineering and Electronics*, vol. 25, no. 5, pp. 748-754, Nov. 2014.

[۱۲] ح. خالقی بیزکی، نظریه کدگذاری کانال، انتشارات دانشگاه صنعتی مالک اشتر، چاپ دوم، فروردین ۱۳۹۴.

- [13] G. Forney, "Structural analysis of convolutional codes via dual codes," *IEEE Trans. on Information Theory*, vol. 19, no. 4, pp. 512-518, Jul. 1973.
- [14] T. Beer, "Walsh Transforms," *American J. of Physics*, vol. 49, no. 5, pp. 466-472, May 1981.

محمد خاکسار در سال ۱۳۸۷ موفق به دریافت مدال برنز المپیاد کشوری فیزیک شد. پس از آن تحصیلات خود در مقطع کارشناسی در رشته مهندسی برق گرایش مخابرات را در سال ۱۳۹۴ از دانشگاه علم و صنعت ایران به پایان رساند و در سال ۱۳۹۷ مدرک کارشناسی ارشد خود را در رشته مهندسی مخابرات گرایش سیستم از دانشگاه صنعتی مالک اشتر دریافت نمود. او مدیریت موفق یک پروژه پیچیده صنعتی پیاده سازی پلتفرم اینترنت اشیا را در کارنامه خود دارد و از سال ۹۶ تاکنون مدیر ارشد فناوری در یک شرکت دانش بنیان فعال در حوزه اینترنت اشیا می باشد. زمینه های تحقیقاتی مورد علاقه اش، شبکه های مشارکتی، شبکه های حسگر بی سیم، اینترنت اشیا، شبکه های مخابراتی توان پایین، الگوریتم های با پیچیدگی محاسباتی پایین و پیاده سازی سخت افزاری الگوریتم های مخابراتی است.

حسین خالقی بیزکی مدرک دکتری خود را در رشته مهندسی برق گرایش مخابرات سیستم در سال ۱۳۸۶ از دانشگاه علم و صنعت ایران دریافت نمود. نام برده دانشیار مخابرات دانشگاه صنعتی مالک اشتر و مولف سه کتاب و بیش از ۴۰ مقاله ژورنال و کنفرانسی می باشد. علاقمندی های تحقیقاتی ایشان شامل تئوری اطلاعات و کدینگ، مخابرات سیار، سیستم های مخابراتی MIMO به ویژه نسل چهارم و پنجم مخابرات سیار و دیگر زمینه های مرتبط با پردازش سیگنال ها و سیستم های مخابراتی دیجیتال می باشد.



شکل ۶: مقایسه عملکرد الگوریتم پیشنهادی با [۸] و [۹] برای کد $C(2,1,7)$.

برای مقایسه در شکل ۶ کارایی الگوریتم پیشنهادی با الگوریتم های پیشنهاد شده در [۸] و [۹] که به حل مسئله مشابه در شرایط نویزی با روشی مبتنی بر مرتبه پرداخته اند، برای کد $C(2,1,7)$ مقایسه شده است. برای الگوریتم پیشنهادی، شبیه سازی مونت کارلوی ۱۰۰۰۰ تایی برای چندین احتمال خطای متفاوت کانال BSC انجام شده است. مطابق شکل ۶ الگوریتم پیشنهادی در نرخ های خطای واقعی در اکثر کاربردهای عملی، $P_e < 0.1$ ، عملکرد قابل توجهی نسبت به روش های پیشین از خود به نمایش می گذارد.

۵- نتیجه گیری

در این مقاله روشی برای تخمین ماتریس بررسی توازن کد کانولوشنال با نرخ دلخواه k/n با استفاده از رشته بیت دریافتی نویزی به کمک تبدیل والش - هادامارد توسعه داده شد. برخلاف [۸] در این پژوهش به جای استفاده از روش مبتنی بر مرتبه، از روش مبتنی بر تبدیل استفاده شده که دارای کارایی به مراتب بیشتری در برابر نویز می باشد. استفاده از ویژگی های جبری کد دوگان در ساده سازی مسئله و تبدیل آن به حل $n-k$ دستگاه معادله که به روش غیر تکراری مبتنی بر تبدیل حل می شوند، ایده اصلی این مقاله می باشد. در پایان عملکرد الگوریتم برای نرخ های خطای کانال در شرایط عملی، بررسی شد و عملکرد قابل توجه الگوریتم در تخمین صحیح کد دوگان در مقایسه با روش های پیشین در [۸] و [۹] مشاهده شد. الگوریتم پیشنهادی می تواند ماتریس بررسی توازن را در نرخ خطای کانال حداقل ۱۰٪ به ازای طول مشاهده کافی و معقول (۱۰۰۰۰ معادله) به درستی شناسایی کند.

مراجع

- [1] B. Rice, "Determining the parameters of a rate $1/n$ convolutional encoder over $GF(q)$," in *Proc. 3rd Int. Conf. on Finite Fields and Applications*, 4 pp., Glasgow, USA, Jul. 1995.
- [2] E. Filiol, "Reconstruction of convolutional encoders over $GF(q)$," in *Proc. 6th IMA Int. Conf. on Cryptography and Coding*, pp. 101-109, Cirencester, UK, 17-19 Dec. 1997.