

## ارائه الگوریتم شناسایی کور پارامترهای جایگردان بلوکی در سامانه‌های مخابرات ماهواره‌ای

مرتضی حاجی محمدی<sup>۱</sup>، علی ناصری<sup>۲\*</sup>

۱- دانشجوی کارشناسی ارشد ۲- دانشیار دانشگاه جامع امام حسین (ع)

(دریافت: ۹۲/۱۰/۲۳، پذیرش: ۹۴/۰۴/۰۹)

### چکیده

جایگردان<sup>۱</sup> روشی است که برای غلبه بر خطای انفجاری در سامانه‌های شامل تصحیح خطا، به طور گسترده‌ای استفاده می‌شود. در یک محیط غیر تعاملی مثل شنود سیگنال ماهواره که گیرنده از ساختار فرستنده اطلاع چندانی ندارد، نیاز است جایگردان شناسایی شود که در غیر این صورت از شناسایی باقی اجزاء و تکمیل فرایند شنود باز خواهیم ماند. در سامانه‌های ماهواره‌ای استفاده از یک بلوک کدگذاری ترکیبی شامل کد ریدسالامون و یک جایگردان به همراه کد کانولوشنال بسیار متداول است. در این مقاله با فرض اینکه کد کانولوشنال شناسایی شده است، الگوریتمی برای تشخیص جایگردان ارائه شده است. در این الگوریتم با دانش بر وجود کد ریدسالامون، شناسایی دوره جایگردان صورت گرفته، درجه میدان غیرباینری محاسبه و هم‌زمانی بین سیگنال فرستنده و گیرنده شنود انجام می‌گیرد و در نهایت با بررسی عامل‌های مختلف دوره جایگردان، عاملی که طول کد ریدسالامون را ارضاء کند، عمق جایگردان خواهد بود. در الگوریتم پیشنهادی در مقایسه با روش‌های موجود اولاً پیچیدگی محاسباتی به  $O(n^2)$  کاهش یافته است و ثانیاً در مجموع دقت شناسایی و هم‌زمانی نیز افزایش یافته است و علاوه بر این، بر اساس شبیه‌سازهای انجام شده، به‌منظور شناسایی عمق جایگردان از پارامتر  $\text{var}(\varphi_0(k))$  و به‌منظور هم‌زمانسازی از پارامتر  $\emptyset$  بهره گرفته شده است.

**کلید واژه‌ها:** شناسایی کور، عمق جایگردان، دوره جایگردان، روش حذفی گوس جردن از طریق محورگیری.

## An Algorithm for Blind Identification of Block Interleaving Parameters in Communication System via Satellite

M. Hajimohammadi, A. Naseri\*

Imam Hussein University

(Received: 13/01/2014; Accepted: 30/06/2015)

### Abstract

Interleaving is a widely used technique to overcome the burst error in systems featuring error correction. In a non-cooperative environment such as satellite signal in which receiver is not aware of the structure of transmitter, interleaver should be identified, otherwise it would be impossible to identify the residual components and completing the hearing process. In satellite systems, it is a common practice to use a combinatory coding block, including reed-solomon codes and an interleaver with convolutional codes. This research presumes that convolutional code is identified and an algorithm is suggested for recognition of interleaver. In this algorithm, based on the presence of reed-solomon code, interleaving period is identified, non-binary field degree is calculated, and a factor meeting the length of reed-solomon code would be the interleaver depth. Comparing with other available methods, in our suggested algorithm, computational complexity are reduced to  $O(n^2)$  and simultaneity and accuracy of identification is higher. Additionally, Based on the simulations performed, the  $\text{var}(\varphi_0(k))$  in order to identify the depth of Interleaver and  $\emptyset$  have been used in order to synchronization.

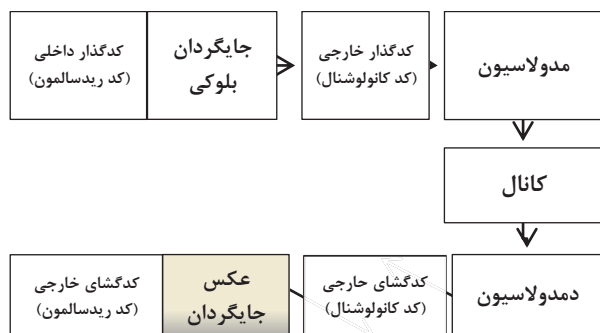
**Keywords:** Blind Identification, Interleaving Depth, Interleaving Period, GJETP.

\*Corresponding Author E-mail: anaseri@ihu.ac.ir

<sup>1</sup> Interleaving

## ۱. مقدمه

انواع این کدها می‌توان به کدهای بلوکی رشته‌ای سری و موازی نام برد. به عنوان مثال، یک کد رشته‌ای سری متداول که در سامانه‌های مخابراتی ماهواره‌ای مبتنی بر استاندارد<sup>۵</sup> CCSDS استفاده می‌شود، از ترکیب کد ریدسالامون به عنوان کد خارجی، کد کانولوشنال به عنوان کد داخلی و یک جایگردان مابین آن‌ها استفاده شده است. البته ممکن است که در بعضی سامانه‌ها از کد داخلی صرف نظر شود اما ترکیب کد ریدسالامون و یک جایگردان به طور گسترده‌ای مورد استفاده قرار می‌گیرد. دو نوع مختلف جایگردانی که به طور معمول استفاده می‌شود، جایگردان بلوکی<sup>۶</sup> و جایگردان کانولوشنال<sup>۷</sup> نام دارند که استفاده از جایگردان بلوکی به همراه یک کد بلوکی به طور گسترده در سامانه‌های شامل بلوک جایگردان استفاده می‌شود [۴] و [۵]. در یک محیط تعاملی<sup>۸</sup> گیرنده به طور کامل از ساختار فرستنده آگاه است بنابراین به راحتی می‌تواند عمل عکس جایگردانی را انجام دهد.

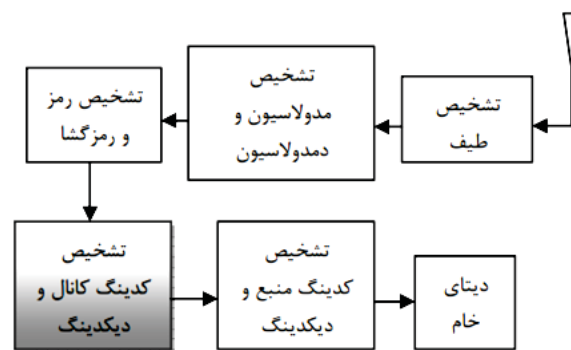


شکل ۲. دیاگرام یک سامانه مخابراتی دیجیتال شامل جایگردان [۲]

حال یک محیط غیرتعاملی (مانند کاربردهای نظامی و مراقبت طیف) را در نظر بگیرید که در آن گیرنده از ساختار فرستنده آگاهی چندانی ندارد. بنابراین، در چنین سامانه‌ای برای شناسایی یک سیگنال ناشناخته، شناسایی کور<sup>۹</sup> پارامترهای جایگردان نیاز است. مطالعات بسیاری در زمینه شناسایی کور پارامترهای کدگذاری و جایگردان صورت گرفته است.

مقالاتی نیز در زمینه شناسایی کور جایگردان نیز ارائه شده‌اند [۱۱-۶]. برای نخستین بار بولر و گوتیه الگوریتمی بر مبنای جبر خطی برای تخمین کور دوره جایگردان، نرخ کد و نحوه هم‌زمان‌سازی داده شوند شده در محیط بدون نویز به کمک محاسبه مرتبه نرمالیزه شده ماتریس تحلیل ارائه نموده‌اند [۶]. سیکات و هوک الگوریتمی برای محاسبه پارامترهای جایگردان در محیط نویزی ارائه داده‌اند که در آن بر اساس روش حذفی گوس- جردن از طریق

سامانه‌های شنود مخابراتی بخش اساسی از جنگ الکترونیک به حساب می‌آیند. این سامانه‌ها وظیفه شناسایی، دمدولاسیون و کدبرگردان سیگنال مخابراتی دریافتی را بر عهده دارند. بلوک دیاگرام شکل (۱) یک سامانه شنود را نشان می‌دهد [۱] در این مقاله به جایگردان<sup>۱</sup> که یکی از بخش‌های اصلی سامانه‌های شامل تصحیح خطا در بلوک تشخیص کدگذاری کانال و کدبرگردان در یک سامانه شنود مخابراتی است، می‌پردازد.



شکل ۱. بلوک دیاگرام سامانه‌های شنود مخابراتی [۱]

بسیاری از کدهای شناخته شده که استفاده از آن‌ها برای افزایش قابلیت اعتماد در انتقال اطلاعات توصیه شده است، زمانی کارایی دارند که خطاهای ناشی از کانال از نظر آماری مستقل باشند. این مطلب در مورد کانال گوسی سفیدجمع‌شونده<sup>۲</sup> مصداق دارد. در عین حال کانال‌هایی مثل کانال محوشدگی<sup>۳</sup> و چندمسیری<sup>۴</sup> وجود دارند که مشخصه خطای آن‌ها انفجاری است. چنین خطاهایی که به صورت رشته‌ای رخ می‌دهند توسط کدهای معمول تصحیح نمی‌شوند. یک روش کارآمد برای مقابله با خطاهای انفجاری، جایگردانی داده‌های کدشده است [۲]. بنابراین در بسیاری از کاربردهای مخابراتی جایگردان به منظور تصحیح خطا به کدگذاری افزوده شده، بدین صورت که بعد از کدکننده کانال یک جایگردان قرار می‌گیرد. جایگردان، سمبل‌های کانال را به منظور اینکه سمبل‌هایی از یک کلمه کد با طولی کمی بیش از طول معمول خطای انفجاری جدا شوند، پخش می‌کند. بنابراین، جایگردان به طور مؤثری باعث می‌شود که کانال برای دی‌کدکننده شبیه یک کانال با خطای تصادفی ظاهر شود. شکل (۲) دیاگرام یک سامانه مخابراتی دیجیتال که از جایگردان استفاده می‌کند را نشان می‌دهد.

روش دیگری، به جایگردان برای تولید کدهای ترکیبی (کدهای چند مرحله‌ای) نیاز دارد. کدهای ترکیبی با طول بزرگ می‌تواند به سادگی در چند مرحله دی‌کد شوند و عملکرد را به طور قابل ملاحظه‌ای در مقایسه با کدهای یک مرحله‌ای بهبود بخشند [۳]. از

<sup>5</sup> Consultative Committee for Space Data Systems

<sup>6</sup> Block Interleaving

<sup>7</sup> Convolutional Interleaving

<sup>8</sup> Cooperative Context

<sup>9</sup> Blind Recognition

<sup>1</sup> Interleaver

<sup>2</sup> AWGN

<sup>3</sup> Fading

<sup>4</sup> Multipath

$$S = b_c \cdot n_c \quad (۴)$$

که در آن،  $n_c$  طول کلمه کد و  $b_c$  عمق جایگردان نامیده می‌شود [۶].

**مدل ریاضی مسئله:** کلید شناسایی تخمین کور پارامترهای جایگردان این است که بلوک جایگردان حتماً بعد از بلوک کدگذاری قرار می‌گیرد [۲]. بنابراین ابتدا مدل بلوک کدگذاری را تشریح می‌شود، بنابراین از یک ماتریس مولد  $G_c$  با مرتبه کامل<sup>۳</sup> برای کد کردن اطلاعات  $\tilde{x}$  به طول  $k_c$  سمبل به خروجی کد شده  $\tilde{y}$  به طول  $n_c$  سمبل استفاده می‌شود که  $k_c < n_c$  می‌باشد:

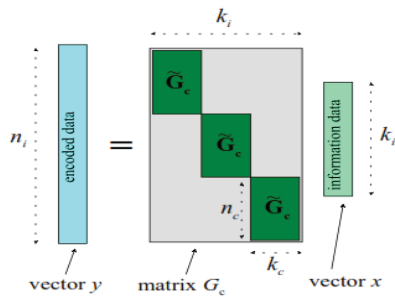
$$\tilde{y} = \tilde{G}_c \cdot \tilde{x} \quad (۵)$$

نسبت طول داده اطلاعات به طول داده کدشده، نرخ کد نامیده می‌شود.

$$r = \frac{k_c}{n_c} \quad (۶)$$

همان‌طور که در قسمت قبل گفته شد، هر  $b_c$  کلمه کد به طول  $n_c$  سمبل به بلوک جایگردان وارد می‌شود، بنابراین جایگشت مشابه‌ای روی طول‌های  $S$  سمبلی از سیگنال شنود اعمال شده است. اثر عمل جایگردان به روی کدگذاری مشابه آن است که از کدی به طول  $n_c$  (بنابراین می‌توان  $k_i = b_c \cdot k_c, n_i = b_c \cdot n_c$ ) استفاده شده است. بنابراین می‌توان مدل کدگذاری را برای هر  $b_c$  سمبل داده اطلاعات به صورت شکل (۳) نشان داد. بنابراین داریم:

$$y = G_c \cdot x \quad (۷)$$



شکل ۳. ساختار ماتریس مولد کد [۶]

حال می‌توان معادله (۷) را برای جایگردانی جریان سمبل‌های کدشده به ترتیب  $y$  را به سمبل‌های جایگردان شده به ترتیب  $Z$  به طول مشابه  $S$  سمبل را به کار گرفت. بنابراین داریم:

$$z = G_i \cdot x \quad (۸)$$

که مطابق شکل (۴)،  $G_i = P \cdot G_c$  خواهد بود که با توجه به ویژگی‌های ماتریس  $P$  و  $G_c$  خود نیز یک ماتریس با مرتبه کامل است [۶]. توجه کنید که در این مقاله  $\tilde{G}_c$  ماتریس مولد کد ریدسالاامون است.

محورگیری (GJETP)<sup>۱</sup> پایین مثلثی کردن ماتریس تحلیل انجام می‌گیرد، سپس وزن همینگ ستون‌های ماتریس پایین مثلثی شده به عنوان معیاری برای شناسایی دوره جایگردان قرار می‌گیرد [۷]. این روش در مقاله‌ای دیگر برای یک داده غیر باینری به روش حذف گوس-جردن در میدان متناهی از طریق محورگیری (FFGE)<sup>۲</sup> تعمیم داده شده است و با محاسبه واریانس وزن صفر در ستون‌های ماتریس تحلیل نیز قدرت تخمین دوره جایگردان بهبود یافته است [۸]. در ادامه، دیگران نیز مطالعاتی پیرامون انواع مختلف جایگردان شامل کانولوشنال [۹]، حلزونی [۱۰] نیز انجام داده‌اند.

در این مقاله با فرض اینکه از کدگذاری ترکیبی شامل کد ریدسالاامون و جایگردان استفاده شده است، شناسایی جایگردان و هم‌زمانی‌سازی جریان داده مورد نظر است. بنابراین بخش‌های مختلف مقاله به صورت زیر تنظیم شده است. ابتدا در بخش ۲ به تعاریف و مبانی ریاضی مسئله پرداخته شده است. در بخش ۳ الگوریتم پیشنهادی مبتنی بر ترکیبی از دو روش شناسایی کور جایگردان پیشنهاد شده است. در بخش ۴ شبیه‌سازی و ارائه ارزیابی و در بخش ۵ نتیجه‌گیری ارائه شده است.

## ۲. تعاریف و مبانی ریاضی

در این بخش از مقاله ابتدا مختصری به مبانی ریاضی مربوط به جایگردان و الگوریتم‌های شناسایی کور و مفاهیم اولیه پرداخته می‌شود.

**جایگردان:** یک جایگردان سامان‌های با خروجی و ورودی منحصر به فرد است که دنباله‌ای از نمادها و سمبل‌ها یک الفبای ثابت  $\mathcal{A}$  را از بلوک کدگذاری دریافت کرده و دنباله خروجی را می‌سازد که دنباله خروجی نیز با همان الفبای مشابه، به جز ترتیب در باقی موارد به دنباله ورودی شبیه است. اگر  $y_i \in \mathcal{A}$ ،  $i$  امین ورودی و  $z_i \in \mathcal{A}$ ، نیز  $i$  امین خروجی بلوک جایگردان باشد، رابطه جایگشتی از عناصر  $y_i$  را نشان می‌دهد که در خروجی جایگردان ظاهر می‌شود که برای آن می‌توان نوشت:

$$z_i = y_{\pi(i)} \quad , \quad \exists I_{\pi}: i \xrightarrow{S} \pi(i) \quad (۱)$$

$$z = Py \quad (۲)$$

$y$  خروجی بلوک کدگذاری نیز می‌باشد و معادله (۷)، شکل ماتریسی عمل جایگردان را نشان می‌دهد که در آن  $P$  ماتریس جایگردان است.

$S$  نشان دهنده دوره جایگردان است که نشان می‌دهد جایگشت  $I_{\pi}$  برای هر  $S$  سمبل ورودی  $y_i$  یکسان خواهد بود [۴].

$$I_{\pi}(i + S) = I_{\pi}(i) \quad (۳)$$

برای سادگی ساختار گیرنده، همواره دوره جایگردان مضربی از طول کد می‌باشد و می‌توان نوشت:

<sup>۳</sup> Full Rank

<sup>۱</sup> Gauss-Jordan Elimination Through Pivoting

<sup>۲</sup> Finite Field Gauss Elimination

$$H(n_a, d) = \tilde{H}(n_a, d) + E \quad (11)$$

که در آن،  $\tilde{H}(n_a, d)$  ماتریس تحلیل بدون خطا و  $E$  شامل همه خطاهای انتقال است [۱۱].

اگر فرض کنید که  $H(S, d)$  ماتریس تحلیل به طول صحیح برابر با دوره جایگردان تشکیل شده است و هم‌زمانی صورت گرفته باشد، در یک کانال بدون نویز تعدادی از ستون‌های این ماتریس وابسته خطی به ستون‌های باقیمانده است. اما در چنین کانالی ناشی از نویز می‌تواند وابستگی ستون‌های ماتریس  $H(S, d)$  از بین برود.

**مرتبه یک ماتریس:** مرتبه یک ماتریس به ابعاد  $n_a \times k_a$  با تابع rank محاسبه می‌شود که نشان دهنده حداقل تعداد سطرها و ستون‌های مستقل خطی یک ماتریس می‌باشد، بنابراین می‌توان نوشت [۶]:

$$\text{rank}(Z) \leq \min(k_a, n_a) \quad (12)$$

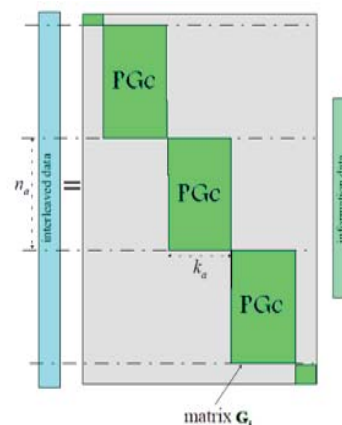
مرتبه نرمالیزه شده یک ماتریس نیز با  $\rho$  نیز نشان داده می‌شود، بنابراین می‌توان نوشت:

$$\rho = \frac{\text{rank}(Z)}{n_a} \quad (13)$$

از مرتبه ماتریس نیز برای بررسی وابستگی خطی جریانی از داده شنود به منظور یافتن وجود با عدم وجود کدگذاری استفاده می‌شود.

**شناسایی بر اساس مرتبه نرمالیزه شده ماتریس تحلیل:** بدین منظور ابتدا داده دریافتی به بردارهای تحلیل  $1 \times n_a$  تقسیم می‌شود که  $n_a$  تخمین اولیه از طول دوره جایگردان است. بردارهای تحلیل به صورت ستونی در کنار هم چیده شده و ماتریس تحلیل  $Z$  را تشکیل می‌دهند. جریان داده شنود شده به ازای طول‌های مختلف بردار تحلیل ( $n_a$ های مختلف) در ماتریس تحلیل چیده شده و مقدار  $\rho$  به ازای مقادیر مختلف  $n_a$  محاسبه می‌شود. همانطوری که در شکل (۶) نشان داده شده است، در صورتی که  $n_a$  ضریب صحیحی از دوره جایگردان باشد ( $n_a = S$ )، بیت‌های افزونگی<sup>۳</sup> چندین ستون از ماتریس تحلیل را به خود اختصاص داده و به تعداد این ستون‌ها که وابسته خطی از سایر ستون‌های ماتریس تحلیل هستند، مرتبه ماتریس کاهش می‌یابد و  $\rho < 1$  است. در غیر این صورت ( $n_a \neq S$ )، مرتبه ماتریس تحلیل، کامل و مقدار  $\rho = 1$  است.

فرض کنید  $d$  سمبل اول داده جایگردان شده به طول دوره  $S$  از دست رفته باشد، در این حالت اگر پس از یافتن مقدار دوره جایگردان،  $(n_a - \hat{d})$  سمبل اول داده شنود را در نظر بگیرید و مقدار مرتبه ماتریس تحلیل (ستون‌های ماتریس تحلیل برابر مقدار ثابت  $S$  در نظر گرفته شود) را بر حسب مقادیر مختلف  $\hat{d}$  محاسبه نمایید، کمترین مقدار  $\rho$  زمانی به دست می‌آید که  $\hat{d} = d$  باشد. بدین ترتیب هم‌زمانی جریان داده شنود و ماتریس تحلیل امکان‌پذیر می‌شود [۶].



شکل ۴. ساختار ماتریس کدگذاری و جایگردان [۶]

**کد ریدسالامون:** کد ریدسالامون یک کد (BCH) غیرباینری با  $s=1$  است یعنی ریشه‌های چندجمله‌ای مولد، متعلق به همان میدانی است که سمبل‌های کد از آن میدان انتخاب می‌شوند. در این کد چون  $s=1$  است، داریم:  $\alpha^i(x) = x - \alpha^i$ ، در نتیجه:

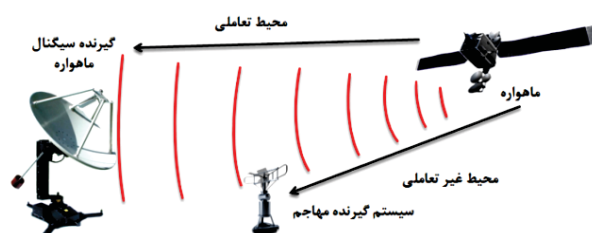
$$g(x) = (x - \alpha)(x - \alpha^2) \dots (x - \alpha^{2^t}) \quad (9)$$

همچنین برای کد ریدسالامون می‌توان نوشت:

$$d_{\min} = 2t + 1 = n - k + 1. \quad (10)$$

به کد RS که به طریق اشاره شده ساخته می‌شود کد RS اولی  $(n, n-2t, 2t+1)$  گویند که  $n = q - 1 = 2^m - 1$  است [۲].

**مدل کانال:** در قسمت قبل بردار  $z$  را به عنوان جریان داده‌ای که کدگذاری و جایگردان بر روی آن صورت گرفته است معرفی شد. حال محیط غیر تعاملی شکل (۵) را در نظر بگیرید.



شکل ۵. محیط تعاملی و غیر تعاملی در فرایند شنود یک ماهواره

در چنین سامانه‌ای عدم هم‌زمانی جریان داده شنود را با سامانه گیرنده مهاجم با پارامتر  $\hat{d}$  نشان می‌دهند، در واقع مقدار  $n_a - \hat{d}$  بیت از دست رفته است. بنابراین اگر ماتریس تحلیل را با طول دوره تخمین  $n_a$  در نظر بگیرید؛ در واقع بلوک‌های  $n_a$  تایی از بردار شنود  $Z$ ، ستون‌های ماتریس تحلیل هستند که با نماد  $H(n_a, \hat{d})$  نشان داده می‌شوند.

$H(n_a, \hat{d})$  که نشان دهنده ماتریس تحلیل در یک کانال باینری متقارن (BSC)<sup>۱</sup> با نرخ خطای بیت<sup>۲</sup> (BER) و احتمال خطای  $P_e$  است، می‌تواند به صورت زیر نشان داده شود:

<sup>۲</sup> Bit Error Rate

<sup>۳</sup> Parity Bit

<sup>۱</sup> Binary Semmetric Channel

این الگوریتم برای میدان‌های غیرباینری به روش (FFGE)<sup>۱</sup> تعمیم یافته است و از میانگین و واریانس  $\varphi_0(k)$  جهت تخمین دوره جایگردان استفاده شده است که  $\varphi_0(k)$  نشان دهنده نرخ صفر در  $k$ -امین ستون ماتریس تحلیل است [۸].

**ارزیابی روش‌های موجود:** از تحلیل دقیق روش‌های موجود و تئوری جایگردان دریافت می‌شود که اولاً جایگردان بر خلاف سایر بلاک‌های بلوک کدگذاری مثل بلوک کدگذار که باعث ایجاد افزونگی در جریان داده می‌شود یا بلوک تصادفی‌ساز<sup>۲</sup> که باعث تغییر بایاس جریان داده می‌شود، ماهیت داده را تغییر نمی‌دهد و تنها به روی اندیس جریان داده تغییر ایجاد می‌کند، بنابراین برای شناسایی آن ناگزیر از استفاده از ویژگی‌های سایر بلوک‌های کدگذاری مثل بلاک کدگذار هستیم و با تحلیل بر روی انواع مختلف کدگذارها می‌توان در روند شناسایی جایگردان بهبود ایجاد نمود. بنابراین در این مقاله، با تمرکز بر روی استاندارد CCSDS مربوط به سامانه‌های مخابرات ماهواره‌ای، به شناسایی جایگردان در این نوع سامانه‌ها که در لایه کدگذاری آن یک کد ریدسalamون به همراه جایگردان استفاده شده است، پرداخته شده است.

ثانیاً، عموماً سه پارامتر  $\varphi(k)$ ، و میانگین و واریانس  $\varphi(k)$  برای شناسایی کور جایگردان مورد استفاده قرار گرفته است.

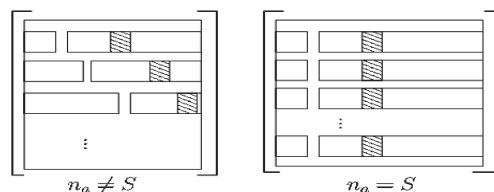
عملکرد این پارامترها برای شناسایی کور جایگردان و هم‌زمان‌سازی متفاوت است که در تحقیقات پیشین به این مسئله پرداخته نشده است. اگر چه واریانس در مقابل  $\varphi(k)$  عملکرد بهتری برای شناسایی دوره در میزان ثابتی از جریان شنود دارد [۸]. اما هم‌زمان‌سازی جریان داده با این پارامتر نتیجه بخش نیست. بنابراین در این مقاله با در نظر گرفتن دو مطلب ذکر شده، الگوریتم پیشنهادی ارائه خواهد شد.

### ۳. ارائه الگوریتم پیشنهادی

الگوریتم پیشنهادی ما با در نظر گرفتن وجود جایگردان و کد ریدسalamون در سه بخش ارائه شده است. در بخش اول الگوریتم پیشنهادی دوره جایگردان شناسایی می‌شود (شکل ۷- بخش اول). در بخش دوم هم‌زمانی جریان داده با سامانه شناسایی کور جایگردان پیشنهادی انجام می‌گیرد (شکل ۷- بخش دوم). در نهایت، در بخش سوم الگوریتم پیشنهادی عمق جایگردان شناسایی می‌شود (شکل ۷- بخش سوم).

الف- تشریح الگوریتم شناسایی جایگردان پیشنهادی (بخش اول): در این قسمت به تشریح فرایند الگوریتم پیشنهادی به منظور شناسایی دوره جایگردان پرداخته می‌شود. از آنجایی که دوره جایگردان همیشه مضرب صحیحی از طول کد می‌باشد و سامانه شنود پیشنهادی برای یک سامانه مخابراتی مبتنی بر استاندارد

این الگوریتم برای حالتی که داده دریافتی نویزی باشد و نرخ کد بزرگ باشد (یعنی  $r$  نزدیک به ۱ باشد)، دیگر کارایی ندارد.



شکل ۶. ساختار ماتریس تحلیل Z در دو حالت مختلف [۱۱]

**روش حذف چرخشی گوس جردن از طریق محورگیری:** روش حذف چرخشی گوس جردن از طریق محورگیری، روشی است که در آن یک سری عملیات سطری و ستونی مقدماتی بر روی ماتریس انجام می‌گیرد که حاصل آن یک ماتریس پایین مثلثی است. با این ویژگی که ستون‌های وابسته ماتریس تمام صفر خواهند بود و برای آن می‌توان نوشت:

$$L(n_a, d) = A_1 \cdot H(n_a, d) \cdot A_2 \quad (14)$$

که در آن، برای پایین مثلثی کردن ماتریس تحلیل H از دو ماتریس  $A_1$  و  $A_2$  استفاده شده است، به طوری که ماتریس  $A_1$  نشان‌دهنده تغییرات سطری مقدماتی و ماتریس  $A_2$  نشان دهنده تغییرات ستونی مقدماتی و ضرب‌ها و جمع‌هایی است که در حوزه گالو بر روی ماتریس تحلیل انجام گرفته است و  $L(n_a, d)$  ماتریس پایین مثلثی شده با ویژگی‌های ذکر شده می‌باشد.

**شناسایی بر اساس روش GJETP:** مدل کانال BSC را در نظر بگیرید، در چنین حالتی مرتبه ماتریس معیار مناسبی برای سنجش وابستگی خطی نیست. در این حالت روش (GJETP) جهت حل این مشکل ارائه شده است.

اگر جریان داده شنود برابر MS سمبل باشد، ابتدا (GJETP) برای پایین مثلثی کردن ماتریس تحلیل شامل سمبل‌های خطا دار استفاده می‌شود. سپس مقدار نرمالیزه شده  $\varphi(k)$  به عنوان یک معیار سنجش برای هر یک از ستون‌های ماتریس تحلیل محاسبه شده و مورد استفاده قرار می‌گیرد.

$$\varphi(k) = \frac{B_k}{m_B} \quad (15)$$

در این رابطه،  $B_k$  برابر تعداد یک‌های ستون  $k$ ام ماتریس تحلیل پس از اعمال الگوریتم (GJETP) و  $m_B$  برابر میانگین تعداد یک‌های قرار گرفته در هر یک از ستون‌های ماتریس تحلیل قبل از اعمال (GJETP) است. در صورتی که  $n_a$  در نظر گرفته شده، برابر با طول دوره جایگردان باشد، مقدار عبارت  $\varphi(k)$  برای تعدادی از ستون‌های ماتریس تحلیل کمتر از یک حد آستانه  $\beta$  می‌باشد. به عبارت دیگر عناصر ستون‌هایی که ترکیب خطی از ستون‌های دیگر می‌باشند برابر حداقل وزن خواهند بود. به این ترتیب طول دوره جایگردان در کانال نویزی قابل محاسبه خواهد بود و هم‌زمانی انجام می‌گیرد [۷].

<sup>1</sup> Finite Field Gauss Elimination with Pivoting

<sup>2</sup> Scrambler



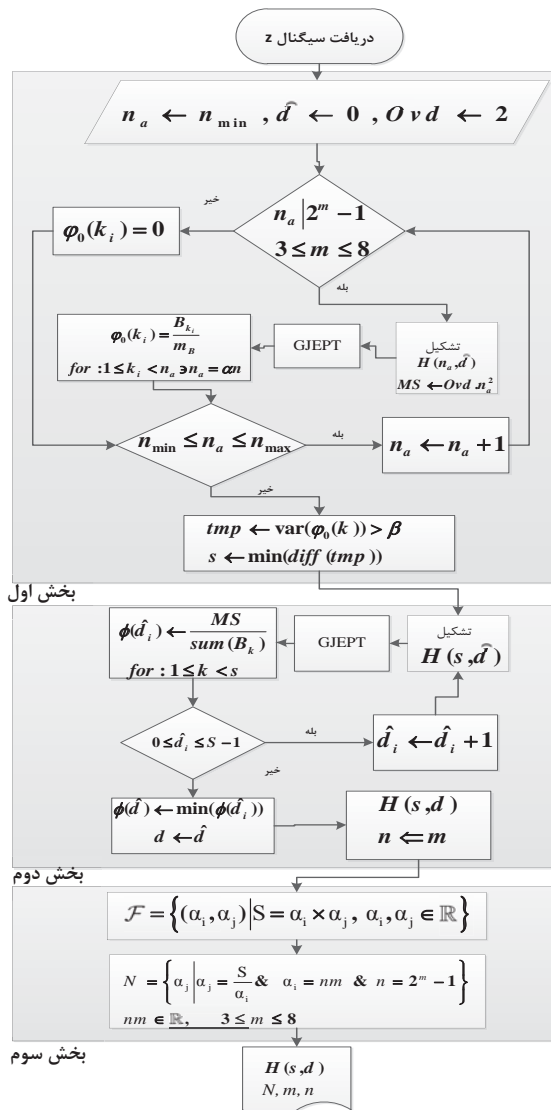
تعریف می‌شود که رفتار مناسبی برای هم‌زمان‌سازی در احتمال خطاهای مختلف نشان می‌دهد و داریم:

$$\phi(\hat{d}_i) = \frac{MS}{\text{sum}(B_k)}, \quad 0 \leq \hat{d}_i \leq S-1 \quad (19)$$

در اندیسی که مقدار  $\phi(\hat{d}_i)$  بیشینه می‌شود، مقدار بیتی که می‌بایست به منظور هم‌زمانی حذف شود را به‌دست آمده است.

$$d = \text{arg max}_{\hat{d}_i} (\phi(\hat{d}_i)) \quad (20)$$

با محاسبه  $d$  بخش دوم الگوریتم پیشنهادی نیز انجام گرفته است، بنابراین  $H(s, d)$  محاسبه شده است.



شکل ۷. الگوریتم شناسایی کور دوره جایگردان و هم‌زمانی

ج- تشریح الگوریتم شناسایی جایگردان پیشنهادی (بخش سوم): حال می‌بایست عمق جایگردان محاسبه شود. از آنجا که می‌دانیم بلوک جایگردان در سامانه مورد نظر همراه کد ریدسلاامون استفاده شده است. بنابراین با داشتن طول جایگردان به بررسی عامل‌های مختلف طول جایگردان می‌پردازیم. اگر مجموعه  $\mathcal{F}$  مجموعه همه زوج مرتب‌هایی، به صورت زیر باشد:

$$\mathcal{F} = \{(\alpha_i, \alpha_j) | S = \alpha_i \times \alpha_j, \alpha_i, \alpha_j \in \mathbb{R}\} \quad (21)$$

CCSDS در سامانه‌های مخابراتی ماهواره‌ای است که به طور متداول از کد ریدسلاامون به همراه جایگردان استفاده می‌کند، دوره جایگردان مقادیر محدودی از ضرایب کد ریدسلاامون به طول  $n$  می‌باشد. بنابراین باید  $|n| \leq k$  یعنی باید دوره جایگردان طول کد را بشمارد. از طرفی حداقل طول کد برای یک کد ریدسلاامون برای  $m=3$  برابر هفت می‌باشد که با فرض در نظر گرفتن حداقل میزان عمق جایگردان برابر ۲،  $n_{min} = 14$  خواهد بود. همچنین به طور معمول طول مورد استفاده برای این سامانه‌ها حداکثر  $255 (m=8)$  می‌باشد، بنابراین می‌توان نوشت:

$$n_a | 2^m - 1, \quad 3 \leq m \leq 8 \quad \& \quad n_{min} = 14 \quad (16)$$

در هر مرحله از اجرای الگوریتم مقدار  $MS$  بیت از جریان داده انتخاب و ماتریس تحلیل تشکیل می‌شود. این مقدار حداقل میزان داده مورد نیاز برای اجرای الگوریتم حذف گوسی است و داریم:

$$MS = Ovd \times n_a^2 \quad (17)$$

$H(n_a, \hat{d})$  معیاری برای افزایش بیت‌هایی که در فرایند تشکیل  $H(n_a, \hat{d})$  مورد استفاده قرار می‌گیرد، است. این افزایش ابعاد ماتریس می‌تواند با استفاده از روش حرکت بر روی بلاک‌های مختلفی از جریان داده<sup>۱</sup> موجب بهبود الگوریتم شناسایی گردد که البته نیازمند افزایش مدت زمان شنود داده است.

پس از اجرای الگوریتم GJEPT نرخ رخداد صفر برای هر ستون از ماتریس  $H(n_a, \hat{d})$  به صورت زیر محاسبه می‌شود:

$$\phi_0(k) = \frac{B_k}{n_a m_B} \quad (18)$$

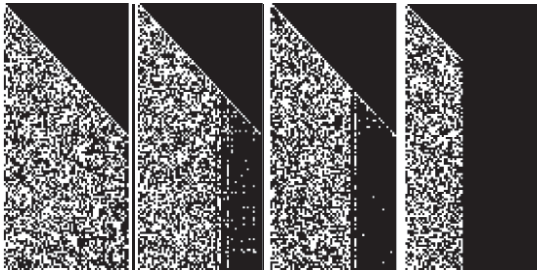
که در آن،  $B_k$  تعداد صفرها،  $m_B$  مقدار میانگین ستون  $k$  ام در ماتریس تحلیل و  $n_a$  تعداد ستون‌های ماتریس تحلیل است. اضافه شدن پارامتر  $n_a$  در فرمول پیشنهادی در مقایسه با فرمول (۱۵) به دلیل تفاوت در مقدار داده‌ای است که در هر مرحله از اجرای برنامه، برای اجرای الگوریتم GJEPT خوانده می‌شود.

در ادامه واریانس بردار  $\phi_0$  اندازه‌گیری می‌شود. به ازای فاصله اندیسی از  $n_a$  که مقدار  $\text{var}(\phi_0(k)) > \beta$  باشد، دوره جایگردان محاسبه می‌شود. که مقدار  $\beta$  معیاری برای شناسایی درست دوره جایگردان است که در ادامه نموداری برای تشخیص مقدار  $\beta$  در احتمال خطاهای مختلف به صورت تجربی محاسبه شده است.

ب- تشریح الگوریتم شناسایی جایگردان پیشنهادی (بخش دوم): در این قسمت از اجرای برنامه دوره جایگردان شناسایی شده است و ماتریس تحلیل به صورت  $H(S, \hat{d})$  داریم. حال می‌خواهیم هم‌زمانی را برای ماتریس تحلیل فوق با اندازه‌گیری مقدار  $\hat{d}$  انجام دهیم. از بررسی پارامترهای معرفی شده در بخش قبل دریافت می‌شود که مقدار واریانس به هیچ وجه نمی‌تواند معیار مناسبی برای هم‌زمان‌سازی باشد. در این قسمت پارامتر دیگری را به صورت زیر

<sup>۱</sup> Sliding Window

به ترتیب از سمت راست به چپ برای مقادیر ۰ و ۰/۰۵ و ۰/۱ و ۰/۲ ترسیم شده است. در حالت بدون خطا تعداد ستون‌های تمام سیاه برابر تعداد افزونگی می‌باشد و با افزایش خطا تعداد ستون‌های وابسته خطی کاهش می‌یابد.



شکل ۸. ساختار ماتریس تحلیل به طول ۶۳ پس از اجرای GJETP

برای شبیه‌سازی بعدی، پارامترهای جدول (۲) در نظر گرفته شده است.

جدول ۲. شرایط در نظر گرفته شده برای شبیه‌سازی

ب	الف	شکل
۰/۰۰۶	۰/۰۰۱	نرخ خطا (BER)
۱۵	۱۵	طول کد (n)
۷	۷	طول پیام (k)
۳	۳	عمق جایگردان
۱۸۰	۱۸۰	دوره جایگردان در میدان باینری
RS	RS	نوع کد

در شکل‌های (۹) و (۱۰) فرایند شناسایی کور دوره جایگردان به کمک الگوریتم پیشنهادی در شکل (۷) بر اساس پارامترهای واریانس  $var(\varphi_0(k))$  و میانگین  $\xi(n_a)$  و  $\xi$  که در فرمول (۱۹) معرفی شده، انجام شده است. در این نمودار محور x، تغییرات  $n_a$  را نشان می‌دهد. محور y، پارامتر مورد استفاده برای شناسایی را نشان می‌دهد که به ترتیب از سمت راست به چپ  $var(\varphi_0(k))$ ،  $\xi(n_a)$  و  $\xi$  هستند و محور z نشان دهنده مقدار نرمالیزه شده پارامتر به بیشترین مقدار به دست آمده برای آن پارامتر است.

همان‌طور که در شکل (۱۰) مشاهده می‌شود، پارامتر  $var(\varphi_0(k))$  معیار مناسب‌تری برای شناسایی دوره جایگردان است. در این شکل فاصله دو پیک متوالی مقدار ۱۸۰، به درستی محاسبه شده است. توجه داشته باشید که دوره جایگردان در این شبیه‌سازی در میدان باینری برابر حاصلضرب عمق جایگردان، طول کد و میدان کد است. بنابراین دوره جایگردان برابر  $۳ \times ۱۵ \times ۴ = ۱۸۰$  است.

به همین دلیل در الگوریتم پیشنهادی ما (شکل ۷)، پارامتر  $var(\varphi_0(k))$  برای شناسایی دوره جایگردان استفاده شده است.

اگر یکی از عامل‌ها، برابر یکی از طول کدهای ممکن برای کد ریدسalamون باشد، از تقسیم اندازه دوره جایگردان بر طول کد در میدان باینری، عمق جایگردان محاسبه می‌شود.

$$N = \left\{ \alpha_j \mid \alpha_j = \frac{S}{\alpha_i} \ \& \ \alpha_i = nm \ \& \ n = 2^m - 1 \right\} \quad (22)$$

$$nm \in \mathbb{R}, \quad 3 \leq m \leq 8$$

جدول (۱) زیر طول‌های ممکن برای یک کد ریدسalamون در میدان باینری و غیر باینری را نشان می‌دهد.

حال با داشتن طول کد و عمق جایگردان با بررسی وابستگی‌های موجود در ماتریس تحلیل  $H(s, d)$  نیز می‌توان نوع جایگردان را هم مشخص نمود. به عنوان مثال در شکل (۸) که برای ماتریس  $H(s, d)$  برای کد ریدسalamون به طول دوره جایگردان برابر ۶۳ در میدان باینری رسم شده است. اولاً برای محاسبه عمق، عامل‌های ۶۳ را به صورت  $(7 \times 9)$ ،  $(3 \times 21)$  و  $(1 \times 63)$  می‌یابیم. مشاهده می‌شود که از میان عامل‌های بالا تنها ۲۱ می‌تواند برابر با طول کد ریدسalamون در میدان باینری باشد. بنابراین عمق جایگردان برابر ۳ می‌باشد. ثانیاً از آنجا که ستون‌های با صفر غالب در ماتریس تحلیل  $H(s, d)$  نشان دهنده ستون‌های وابسته است. بنابراین چیدمان قرار گرفتن این وابستگی‌ها در طول جایگردان می‌تواند مبنایی بر شناسایی نوع جایگردان مورد استفاده باشد.

جدول ۱. طول کدهای ممکن برای کد ریدسalamون در میدان باینری

طول کد در میدان باینری (mn)	طول کد در میدان غیر باینری (n)	درجه میدان غیر باینری $GF(2^m)$
۲۱	۷	m=3
۶۰	۱۵	m=4
۱۵۵	۳۱	m=5
۳۷۸	۶۳	m=6
۸۸۹	۱۲۷	m=7
۲۰۴۰	۲۵۵	m=8

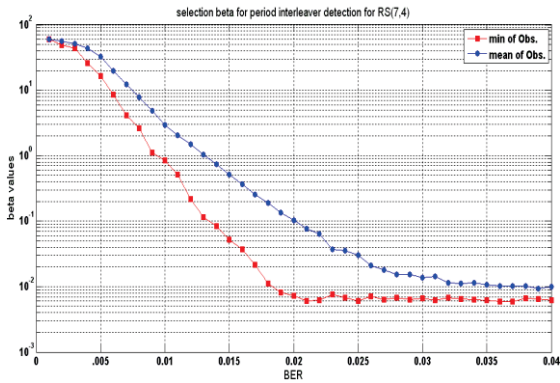
#### ۴. شبیه‌سازی و ارزیابی الگوریتم پیشنهادی

در این قسمت نتایج شبیه‌سازی‌ها و ارزیابی نتایج ارائه می‌شود. شبیه‌سازی‌ها به کمک نرم‌افزار متلب انجام شده است.

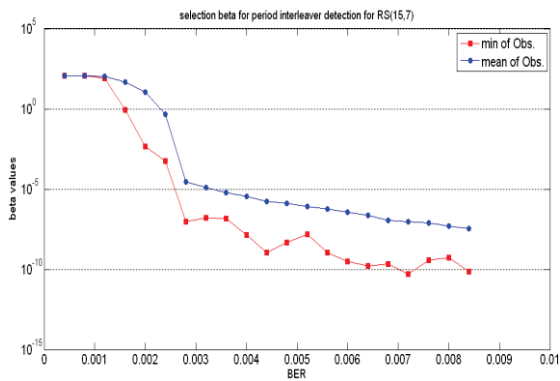
در اولین شبیه‌سازی ساختار ماتریس تحلیل پس از اجرای الگوریتم GJETP برای یک کد RS(7,3) با عمق جایگردان ۳ به ازای احتمال خطاهای مختلف در یک کانال BSC نشان داده شده است. بدین منظور از دستور imtool در نرم‌افزار متلب استفاده شده است.

در شکل (۸)، نقاط سیاه نشان دهنده مقدار صفر و نقاط سفید نشان دهنده مقدار یک در ماتریس تحلیل است. بنابراین از آنجا که پس از اجرای عملیات GJETP در ماتریس پایین مثلثی حاصل، ستون‌های وابسته خطی برابر صفر می‌شود. ستون‌های با صفر غالب نشان دهنده محل قرار گرفتن ستون‌های وابسته خطی است. چهار ماتریس نشان داده شده در شکل (۸) به ازای احتمال خطای مختلف

مشاهده می‌شود که برای RS(7,3) تا BER ۰/۰۱۱ و برای RS(15,7) تا BER ۰/۰۰۹ احتمال شناسایی با دقت بسیار خوبی وجود دارد.

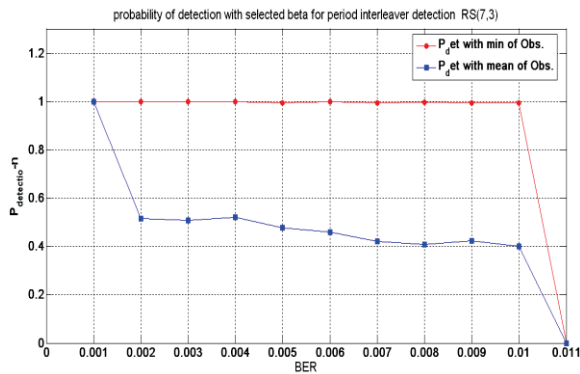


شکل ۱۱. مقدار  $\beta$  بر حسب BER برای محاسبه دوره جایگردان برای RS(7,3)

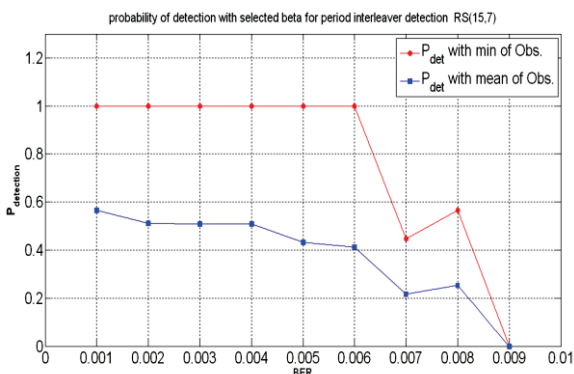


شکل ۱۲. مقدار  $\beta$  بر حسب BER جهت محاسبه دوره جایگردان برای

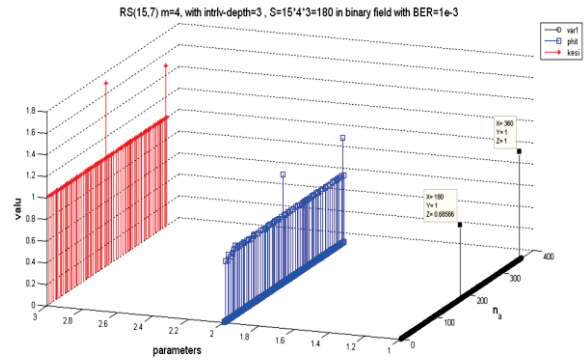
RS(15,7)



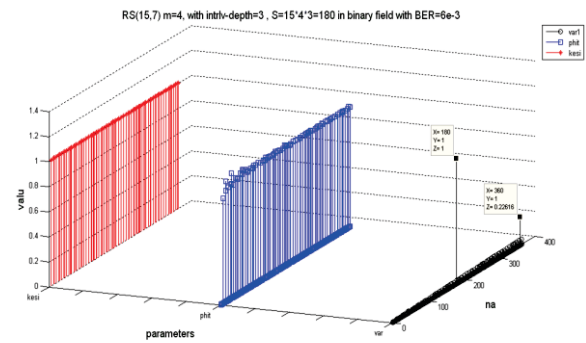
شکل ۱۳. نمودار احتمال شناسایی دوره جایگردان با در نظر گرفتن  $\beta$



شکل ۱۴. نمودار احتمال شناسایی دوره جایگردان با در نظر گرفتن  $\beta$



شکل ۹. مقایسه پارامترهای  $var(\varphi_0(k))$  و  $\xi(n_a)$  و  $\phi$  در  $BER=1e-3$



شکل ۱۰. مقایسه پارامترهای  $var(\varphi_0(k))$  و  $\xi(n_a)$  و  $\phi$  در  $BER=6e-3$

در این مثال اگر بخواهید عمق جایگردان را محاسبه کنید، پس از محاسبه طول دوره جایگردان از شکل (۱۰) برابر با ۱۸۰ عامل‌های آن را به صورت زیر محاسبه می‌شود.

$$(1,180), (2,90), (3,60), (4,45), (5,36), (6,30), (9,20), (10,18), (12,15)$$

از میان این عامل‌ها تنها ۶۰ برای  $m=4$  می‌تواند، طول یک کد ریدسalamon در میدان باینری باشد.

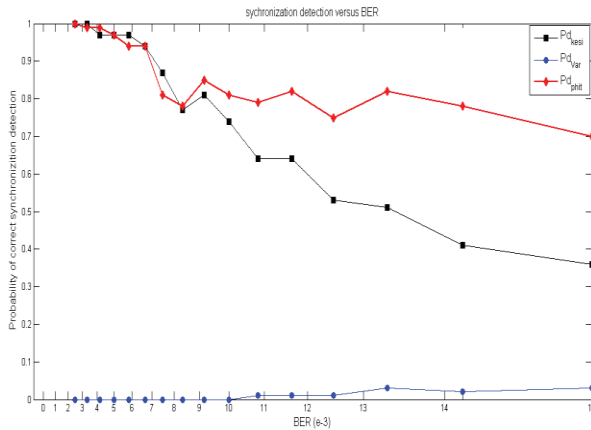
$$m \times (2^m - 1) = 4 \times 15 = \text{ریدسalamon کد طول}$$

بنابراین عمق جایگردان و درجه میدان غیرباینری برای کد ریدسalamon محاسبه شده است.

برای به‌دست آوردن مقدار  $\beta$  به صورت تجربی نتایج حاصل از شبیه‌سازی برای مقدار حداقل و میانگین  $var(\varphi_0(k))$  در نقاط برابر با دوره جایگردان برای  $m=3, m=4, m=5$  و با تعداد تکرار به ترتیب برابر ۱۰۰۰ و ۵۰۰ بار محاسبه شده است و بر حسب مقادیر مختلف BER در شکل (۱۱ و ۱۲) نشان داده شده است. در این نمودار محور عمودی مقدار  $\beta$  و محور افقی مقدار BER را نشان می‌دهد. خطی که با مثلث نشانه‌گذاری شده، میانگین مشاهدات و خطی که با دایره نشانه‌گذاری شده، حداقل مشاهدات را نشان می‌دهد. حال مقدار  $\beta$  ای که از دو نمودار اخیر به‌دست آمده است، مبنای شناسایی دوره جایگردان می‌شود.

در شکل های (۱۳) و (۱۴) محور عمودی احتمال شناسایی دوره جایگردان و محور افقی نشان دهنده BER است. نمودار با نماد دایره احتمال شناسایی را بر اساس حداقل مشاهدات و نمودار با نماد مربع احتمال شناسایی بر اساس میانگین مشاهدات را نشان می‌دهد.





شکل ۱۶. مقایسه پارامترهای  $var(\varphi_0(k))$  و  $\xi(n_a)$  و  $\emptyset$  در همزمان-سازی

در نهایت با بررسی پیچیدگی محاسباتی الگوریتم در می‌یابیم که پیچیدگی اجرای GJETP در الگوریتم پیشنهادی در مقایسه با روش ارائه شده در مرجع [۱۲] از  $O(n^3)$  به  $O(n^2)$  کاهش یافته است.

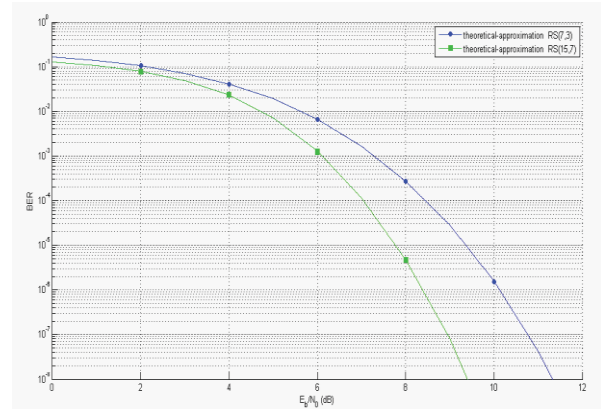
## ۵. نتیجه‌گیری

در این مقاله الگوریتمی با پیچیدگی محاسباتی کم برای شناسایی کور پارامترهای جایگردان شامل دوره جایگردان، همزمان‌سازی و عمق جایگردان در یک سامانه مخابرات ماهواره‌ای که از ترکیب جایگردان و کد ریدسلاسون استفاده می‌کند، ارائه شده است. در الگوریتم پیشنهادی بر اساس شبیه‌سازهای انجام شده، به‌منظور شناسایی عمق جایگردان از پارامتر  $var(\varphi_0(k))$  و به‌منظور همزمان‌سازی از پارامتر  $\emptyset$  بهره گرفته شده است. علاوه بر این، با این الگوریتم می‌توان طول کد ریدسلاسون و  $m$  را محاسبه کرد که برای شناسایی کامل کد ریدسلاسون در ادامه کار می‌تواند مفید باشد. این سامانه با SNR های در حدود ۷ دسیبل قادر است به طور خودکار و با در نظر گرفتن مقدار آستانه محاسبه شده دوره جایگردان را محاسبه نماید و هم زمانی را با موفقیت انجام دهد. البته اگر شناسایی بلادرنگ مورد نظر نباشد با تحلیل نمودارهای ارائه شده و انجام مرحله‌ای الگوریتم ارائه شده قادر خواهید بود که با SNR های کمتر نیز موفق به شناسایی جایگردان و هم زمانی شوید.

## ۶. مراجع

- [1] Naseri, A.; Maymanat, M. "Proposed Algorithm for Channel Coding Detection in Communication Surveillance Systems"; J. Passive Defence Sci & Tech. 2011, 2, 101-110.
- [2] Proakis, J. G.; Salehi M. "Digital Communications"; Mc Graw Hill Eds, 5th Ed, 475-481, 2008.
- [3] Ramsey, L. "Realization of Optimum Interleaver"; IEEE Transactions on Information Theory 1970, IT-16.
- [4] Heegard, C.; Wicker, S. B. "Turbo Coding"; Kluwer Academic Publisher, 1st Ed., 1999.
- [5] Andrews, K.; Heegard, C. "A Theory of Interleavers"; Technical Report 97-1634, Computer Science Department, Cornell University, June 1997.

شکل (۱۵) به کمک bertool در نرم‌افزار متلب ترسیم شده است که مقدار SNR به BER را برای سامان‌های با مدولاسیون OQPSK با کد ریدسلاسون مفروض در نمودارهای قبل نشان می‌دهد که می‌تواند مدلی مناسب برای سامانه مخابرات ماهواره‌ای مورد نظر باشد. با توجه به نتایج به‌دست آمده روش مذکور برای SNR های در حدود ۶dB مناسب است.



شکل ۱۵. نمودار SNR به BER برای سامانه مخابراتی مورد نظر

در این قسمت از شبیه‌سازی، پارامترهای مختلف معرفی شده برای همزمان‌سازی بر اساس پارامترهای جدول (۳) انجام گرفته است.

## جدول ۳. شرایط در نظر گرفته شده برای شبیه‌سازی

الف	شکل
[۰ :.۱۵]	نرخ خطا (BER)
۷	طول کد (n)
۳	طول پیام (k)
۳	عمق جایگردان
۶۳	دوره جایگردان در میدان باینری
۱۰۰	تعداد تکرار در هر احتمال خطا
RS	نوع کد
۲	تعداد بیت از دست رفته

نتایج حاصل از شبیه‌سازی در شکل (۱۶) نشان داده شده است. در این نمودار محور عمودی احتمال شناسایی درست تعداد بیت از دست رفته و محور افقی، محوری لگاریتمی است که مقدار BER را نشان می‌دهد. نمودار با نماد لوزی معرف شناسایی بر اساس پارامتر  $\emptyset$  که در رابطه (۱۷) معرفی شده است، نمودار با نماد مربع معرف شناسایی بر اساس پارامتر  $\xi(n_a)$  و نمودار با نماد دایره معرف شناسایی بر اساس پارامتر  $var(\varphi_0(k))$  است. نمودار نشان می‌دهد:

بر خلاف شناسایی دوره جایگردان پارامتر واریانس، پارامتر مناسبی جهت همزمان‌سازی نیست. برای BER کمتر از  $0/009$  پارامترهای  $\xi(n_a)$  و  $\emptyset$  وضعیت مشابه‌ای دارند ولی برای BER بیشتر از  $0/009$  پارامتر  $\emptyset$  برای همزمان‌سازی مناسب‌تر است. بنابراین در قسمت دوم شکل (۷) این پارامتر به منظور همزمان‌سازی پیشنهاد شده است.

- [10] Jeong, J.; Yoon, D.; Lee, J. "Blind Reconstruction of a Helical Scan Interleaver"; IEEE 978-1-4577-0031-6, ICICS 2011.
- [11] Sicot, H.; Houcke S. "Blind Detection of Interleaver Parameters"; ICASSP, IEEE 0-7803-8874-7, pp: III:829-832, 2005
- [12] Galoppo, N., Govindaraju, N. K., Henson, M., Manocha, D. "Efficient Algorithms for Solving Dense Linear Systems on Graphics Hardware"; In Proc. of the 2005 ACM/IEEE Conf. on Supercomputing (p. 3). IEEE Computer Society, Nov, 2005.
- [6] Burel, G.; Roland, G. L. "Blind Estimation of Encoder and Interleaver Characteristics in a Non Cooperative Context"; In Second IASTED Int. Conf. on Communications, Internet and Information Tech.; 275-280; Scotlande, 2003.
- [7] Sicot, G.; Houcke, S. "Blind Detection of Interleaver Parameters"; IEEE International Conference on Acoustics, Speech and Signal Processing, 2005, 3, 829-832.
- [8] Lu, L.; Kwok, H. L.; Yong, L. G. "Blind Detection of Interleaver Parameters for Non-Binary Code Data Stream"; IEEE ICC 2009.
- [9] Jia, Y. Q.; Li, P. L.; Lu, G. "Blind Estimation of Convolutional Interleaver Parameters"; Wireless Communications, Networking and Mobile Computing (WiCOM), 8th Int. Conf. on IEEE, 2012.