تخمین پارامترهای کد RS در شرایط نویزی

احمد قلی‌زاده سوته[1]، حسین خالقی بیزکی[2]، حمیدرضا فاطمی مفرد[3]

[1]دانشجوی دکترای مخابرات سیستم، دانشگاه صنعتی مالک اشتر، تهران.

[2]دانشیار مجتمع دانشگاهی برق و الکترونیک، دانشگاه صنعتی مالک اشتر، تهران، bizaki@gmail.com

[3]استادیار مجتمع دانشگاهی برق و الکترونیک، دانشگاه صنعتی مالک اشتر، تهران.

چکیده

این مقاله به مسئله تخمین پارامترهای کد RS در شرایط نویزی می‌پردازد. این مسئله درکاربردهای نظامی و همچنین طراحی گیرنده‌های رادیو-شناختی مطرح می‌شود. علیرغم کاربرد وسیع کدهای RS، تا کنون تنها چند روش معدود برای تخمین آن پیشنهاد شده است. اغلب این روش‌ها از پیچیدگی بالایی برخوردار بوده و تنها در نرخ‌های خطای پایین کارایی دارند. در این مقاله یک روش کاملا جدید، موثر و با پیچیدگی پایین برای تخمین کد RS پیشنهاد می‌شود. در این روش ابتدا طول کد و چندجمله‌ای اولیه و سپس طول پیام تعیین می‌شود. تعیین این پارامترها بر مبنای تشخیص کدهای یک مجموعه خاص انجام می‌شود. ویژگی اصلی این مجموعه، حضور کلمات کد ارسالی در تمام کدهای متعلق به آن است. در این مقاله آزمایشی برای تشخیص کدهای این مجموعه پیشنهاد می‌شود. در این آزمایش، بیت‌های بررسی توازن مجددا توسط بیت-های پیام دریافتی محاسبه شده و با بیت‌های بررسی توازن دریافتی مقایسه می‌شوند. اگر اختلاف این بیت‌ها از مقدار حد آستانه کمتر باشد، حضور کد RS در مجموعه تایید می‌شود. در این مقاله دو حد آستانه مناسب برای این آزمایش پیشنهاد می‌شود. حد آستانه اول بر مبنای قاعده تصمیم‌گیری حداقل-بیشینه طراحی شده و به احتمال خطای کانال وابسته است. ولی حد آستانه دوم کاملا تجربی بوده و مستقل از خطای کانال است. نتایج شبیه‌سازی کارایی بالای این روش را تایید می‌کنند. به عنوان مثال این روش می‌تواند پارامترهای کد RS با طول ۶۳ را تا نرخ خطای 4×10^{-3} به طور کامل تخمین بزند.

کلیدواژه

کد RS، روش جبری، بیت‌های بررسی توازن، سیستم رادیوشناختی، آزمایش حد آستانه، چندجمله‌ای اولیه.

مقدمه

در سیستم‌های مخابراتی پیشرفته از کدهای تصحیح خطا برای مقابله با خطای کانال استفاده می‌شود. برای این منظور فرستنده چند بیت معنادار را با استفاده از یک کدگذار کانال به اطلاعات ارسالی اضافه می‌کند. گیرنده نیز با استفاده از یک کدگشای کانال مناسب از این بیت‌ها برای تشخیص و تصحیح خطای کانال بهره می‌برد. پارامترهای کدگذار برای طراحی چنین کدگشایی باید از قبل معلوم باشند. با این حال گیرنده در بسیاری از کاربردهای عملی از قبیل سیستم‌های نظامی و غیراشتراکی[1] این اطلاعات را در اختیار ندارد. در این حالت اصطلاحا گفته می‌شود که گیرنده، کور است؛ زیرا پارامترهای فرستنده باید تخمین زده شوند. یکی از کاربردهای مهم این گیرنده در سیستم‌های رادیو-شناختی[2] است. یک سیستم رادیو-شناختی می‌تواند خود را بر اساس پارامترهای تخمینی تنظیم کند. یکی از کاربردهای جذاب این سیستم در زمینه استراق سمع[3] است که در آن یک کاربر غیرمجاز قصد دارد تا اطلاعات مبادله شده بین دو سیستم مخابراتی را شنود کند.

مسئله تخمین کدگذار کانال تا کنون در بسیاری از مقالات مورد بررسی قرار گرفته است. برای مثال در [۴-۱]یک روش مبتنی بر مرتبه برای تخمین پارامترهای کدهای بلوکی پیشنهاد شده است. در این روش رشته دریافتی به صورت سطری در ماتریس‌هایی با ابعاد مختلف قرار گرفته و سپس از فضای تهی و مرتبه این ماتریس‌ها برای تخمین پارامترهای کد استفاده می‌شود. با وجود پیچیدگی زیاد، کارایی این روش تنها در کدهایی با طول پایین مناسب است. مراجع [۸-۵]نیز از همین روش برای تخمین کدهای کانولوشنال[4] و توربو[5] بهره برده‌اند. روش مبتنی بر نسبت شبیه‌نمایی لگاریتمی[6] یکی دیگر از روش‌هایی است که در تخمین کدهای کانال پیشنهاد شده

[1] Non-Cooperative Communication

[2] Cognitive Radio

[3] Eavesdropping

[4] Convolutional Code

[5] Turbo

[6] Log-Likelihood Ratio

تاریخ دریافت : ۱۳۹۴/۰۹/۰۱ تاریخ پذیرش : ۱۳۹۵/۰۹/۲۲

است [۱۲-۹]. محققین در [۱۳-۱۶]نیز از ریشه‌ها و عامل‌های[۷] کلمات کد دریافتی برای تخمین چندجمله‌ای مولد کدهای چرخشی[۸] باینری بهره برده‌اند.

در این مقاله سعی بر آن است تا به مسئله تخمین پارامترهای کد RS[۹] در شرایط نویزی پرداخته شود. کد RS یکی از مهمترین کدهای چرخشی غیرباینری است. قابلیت تصحیح خطای بالا به همراه پیاده‌سازی آسان، این کد را به یکی از پرکاربردترین کدهای کانال مبدل کرده است. برای نمونه این کدها به طور وسیع در سیستم‌های مخابراتی و ذخیره‌سازی استفاده می‌شوند. با این حال تحقیقات بسیار کمی در زمینه تخمین پارامترهای آن انجام شده است. در [۱۹-۱۷]یک روش مبتنی بر تبدیل فوریه برای تخمین پارامترهای کد RS پیشنهاد شده است. تخمین در این روش بر مبنای صفرهای طیف کلمات کد دریافتی انجام می‌شود. یکی از معایب اصلی این روش پیچیدگی زیاد آن در تخمین کدهایی با طول بالا است. محققین در [۲۰، ۲۱]از الگوریتم اقلیدسی[۱۰] برای تخمین کد RS بهره برده‌اند. تخمین در این روش بر مبنای بزرگترین عامل مشترک کلمات کد دریافتی انجام می‌شود. عملکرد این روش تنها در نرخ‌های خطای بسیار پایین مناسب است. در [۲۲، ۲۳]یک روش مبتنی بر تبدیل ماتریس برای تخمین چندجمله‌ای مولد کد RS پیشنهاد شده است. برای عملکرد صحیح این روش باید طول پیام و طول کد از قبل مشخص باشند. محققین در [۲۴]نیز از روشی مشابه با روش مبتنی بر مرتبه که در [۴-۱]پیشنهاد شد، برای تخمین طول و چندجمله‌ای اولیه کد RS استفاده کرده‌اند. با وجود پیچیدگی بالا، این روش تنها در نرخ‌های خطای بسیار پایین کارایی دارد.

در این مقاله یک روش کاملا جدید، موثر و با پیچیدگی پایین برای تخمین کد RS در شرایط نویزی پیشنهاد می‌شود. تخمین پارامترها در این روش مبتنی بر مجموعه‌ای از کدهای مرتبط با کد RS فرستنده است. این مجموعه شامل کدهایی است که می‌توانند مولد کلمات کد ارسالی باشند. به عبارت دیگر، کلمات کد ارسالی در تمام کدهای این مجموعه قرار دارند. در این مقاله آزمایشی برای تشخیص اعضای این مجموعه پیشنهاد می‌شود. در این آزمایش بیت‌های بررسی توازن[۱۱] مجددا توسط بیت‌های پیام ارسالی تولید می‌شوند. معیار تصمیم‌گیری در این آزمایش تعداد اختلاف بین بیت‌های بررسی توازن تولید شده و بیت‌های بررسی توازن دریافتی است. اگر تعداد اختلاف‌ها از مقدار حد آستانه کمتر باشد، کد موردنظر به عنوان یک کد مجموعه اعلام می‌شود. در این مقاله دو مقدار حد آستانه مناسب برای این آزمایش پیشنهاد می‌شود. یکی از این مقادیر بر مبنای قاعده تصمیم‌گیری حداقل-بیشینه[۱۲] طراحی شده و برای حالتی مناسب است که احتمال خطای کانال معلوم باشد. حد آستانه دیگر نیز کاملا تجربی بوده و با فرض عدم آگاهی از احتمال خطای کانال انتخاب شده است. نتایج شبیه‌سازی نشان می‌دهند که عملکرد روش پیشنهادی قطع نظر از نوع حد آستانه در شرایط نویزی بسیار مناسب است. به عنوان مثال این روش می‌تواند پارامترهای کد RS با طول ۶۳ را تا نرخ خطای 4×10^{-3} به طور کامل تخمین بزند. پیچیدگی محاسباتی این الگوریتم از درجه $O(n^3)$ است که برای مسائل عملی بسیار مناسب می‌باشد.

این مقاله در ادامه به صورت زیر تنظیم شده است. در بخش ۲ کد RS به طور مختصر معرفی می‌شود. بخش ۳ به بیان مدل مسئله تخمین کد RS می‌پردازد. در بخش ۴ مبنای ریاضی روش پیشنهادی تشریح می‌شود. سپس بخش ۵ به تشریح مراحل تخمین پارامترهای کد RS در این روش می‌پردازد. در بخش ۶ چند مثال شبیه‌سازی به منظور ارزیابی عملکرد الگوریتم پیشنهادی ارائه می‌شود. بخش ۷ نیز نتایج این مقاله را به طور مختصر جمع‌بندی کرده و برخی از مسائل حل نشده در زمینه تخمین کد RS را مطرح می‌کند. نهایتا در پیوست مقاله دو حد آستانه برای آزمایش کدهای RS پیشنهاد می‌شود.

توصیف ریاضی کد RS

کدهای RS در زمره کدهای چرخشی غیرباینری قرار می‌گیرند. فرض کنید که کد $RS(n,k)$ در میدان باینری توسعه یافته[۱۳] $GF(2^m)$ تعریف شده باشد. طول کلمات این کد برابر $n=2^m-1$ سمبل بوده و قابلیت تصحیح خطای آن نیز برابر با $t=(n-k)/2$ سمبل است. چندجمله‌ای مولد این کد به صورت زیر تعریف می‌شود [۲۵]:

$$g(x)=(x-\alpha)(x-\alpha^2)\ldots(x-\alpha^{2t}) \qquad (۱)$$

پارامتر α مولفه اولیه[۱۴] میدان $GF(2^m)$ را نشان می‌دهد. چندجمله‌ای اولیه این میدان نیز برابر با $p(x)$ است.

فرض کنید که $u_s(x)$ چندجمله‌ای پیام متناظر با سمبل‌های ورودی کدگذار RS باشد. در این صورت عملیات کدگذاری می‌تواند به صورت زیر نوشته شود:

$$c_s(x)=u_s(x).g(x) \qquad (۲)$$

که در آن $c_s(x)$ چندجمله‌ای کد متناظر با سمبل‌های خروجی کدگذار RS است (زیرنویس s نماد سمبل است). به

---

۷ Factors
۸ Cyclic Codes
۹ Reed-Solomon
۱۰ Euclidean Algorithm
۱۱
۱۲ Minimax Decision Rule
۱۳ Extended Binary Fields
۱۴

این نکته توجه داشته باشید که ضرایب چندجمله‌ای‌های $u_s(x)$، $c_s(x)$ و $g(x)$ تماما مولفه‌هایی از میدان $GF(2^m)$ هستند.

عملیات کدگذاری و کدگشایی در کدهای غیربایتری بر روی سمبل‌ها (یعنی تعداد مشخصی از بیت‌ها) انجام می‌شوند. به عنوان مثال کد $RS(n,k)$ هر km بیت پیام را به کلمه کدی با طول nm بیت می‌نگارد. عملیات کدگذاری در سه مرحله انجام می‌شود:

۱. تبدیل هر m بیت متوالی پیام به یک سمبل در میدان بایتری توسعه یافته $GF(2^m)$

۲. کدگذاری k سمبل پیام به n سمبل کد مطابق با رابطه (۲)

۳. تبدیل هر سمبل در کلمه کد به بردار m-بیتی متناظر

فرض کنید $g(x)=g_0+g_1x+\cdots+g_{n-k}x^{n-k}$ چندجمله‌ای مولد کد RS باشد. در این صورت رابطه (۲) می‌تواند در قالب ماتریسی زیر بازنویسی شود:

$$C_s = U_s \cdot \mathbf{G} \qquad (۳)$$

که در آن U_s و C_s به ترتیب بردارهای متناظر با سمبل‌های پیام و سمبل‌های کد بوده و ماتریس مولد $\mathbf{G}$ نیز به صورت زیر تعریف می‌شود:

$$\mathbf{G}=\begin{bmatrix} g_0 & g_1 & \cdots & g_{n-k} & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{n-k} & 0 & \cdots & 0 \\ 0 & 0 & g_0 & g_1 & \cdots & g_{n-k} & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \ddots & \cdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & g_0 & g_1 & \cdots & g_{n-k} \end{bmatrix} \qquad (۴)$$

در اغلب سیستم‌های مخابراتی عملی از کدگذارهای سیستماتیک استفاده می‌شود. در این کدگذار بیت‌های پیام بدون تغییر در انتهای کلمه کد قرار می‌گیرد. فرض کنید $U=[u_0 \;\; u_1 \;\; \cdots \;\; u_{km-1}]$ و $C=[c_0 \;\; c_1 \;\; \cdots \;\; c_{nm-1}]$ به ترتیب بردارهای بایتری متناظر با بردارهای غیربایتری U_s و C_s باشند. برای تبدیل یک بردار غیربایتری به بردار بایتری باید تمام سمبل‌های آن به بردارهای m-بیتی متناظر تبدیل شوند. توجه داشته باشید که طول بردارهای U_s، C_s، U و C به ترتیب برابر با k، n، km و nm است. در یک کدگذار سیستماتیک، کلمه کد بایتری C می‌تواند به صورت زیر نوشته شود:

$$C=[\underbrace{v_0 \;\; v_1 \;\; \cdots \;\; v_{(n-k)m-1}}_{\text{Parity-check bits}} \;\; \underbrace{u_0 \;\; u_1 \;\; \cdots \;\; u_{km-1}}_{\text{Message bits}}] \qquad (۵)$$

که در آن $V=[v_0 \;\; v_1 \;\; \cdots \;\; v_{(n-k)m-1}]$ بردار بررسی توازن بایتری نامیده می‌شود. فرض کنید $v_s(x)$ چندجمله‌ای غیربایتری متناظر با بردار بایتری V باشد. آنگاه رابطه زیر برقرار است [۲۵]:

$$v_s(x)=u_s(x).x^{n-k} \bmod g(x) \qquad (۶)$$

که در آن mod نشان دهنده عملگر باقیمانده است.

مدل سیستم

کد RS یکی از پرکاربردترین کدهای کانال است. مسئله تخمین این کد در بسیاری از سیستم‌های غیراشتراکی و نظامی مطرح می‌شود. مدل این مسئله به صورت کاملا شماتیک در شکل ۱ ترسیم شده است.

در این مسئله فرض می‌شود که فرستنده از یک کدگذار سیستماتیک RS برای مقابله با خطای کانال استفاده می‌کند. این کدگذار L رشته پیام $U^{(i)}, i=1,2,\ldots,L$ را به کلمات کد $C^{(i)}, i=1,2,\ldots,L$ می‌نگارد. فرستنده نیز رشته بایتری زیر را پس از مدوله کردن به سمت کانال انتقال ارسال می‌کند:

$$X=[C^{(1)} \;\; C^{(2)} \;\; \cdots \;\; C^{(L)}] \qquad (۷)$$

این بردار بایتری از طریق یک کانال نویزی به تخمین‌گر کدگذار RS در گیرنده کور وارد می‌شود. منظور از کانال مجموعه تمام بلوک‌هایی هستند که بین کدگذار فرستنده و کدگشای گیرنده قرار می‌گیرند، مانند مدولاتور، کانال انتقال فیزیکی، دمدولاتور (کور) و غیره. در این مسئله یک کانال بایتری متقارن[۱۵] با احتمال خطای ε در نظر گرفته می‌شود. در این حالت رشته دریافتی می‌تواند به صورت زیر نوشته شود:

$$Y=X+E \qquad (۸)$$

که در آن E بردار خطای کانال است. هر کدام از بیت‌های این بردار با احتمال ε برابر با یک و با احتمال $1-\varepsilon$ برابر با صفر هستند. کدگشای کور باید تمام پارامترهای کدگذار RS را بر مبنای رشته Y استخراج کند. این پارامترها عبارتند از:

۱. طول کد؛ یعنی $n=2^m-1$

۲. طول پیام؛ یعنی $k=n-2t$

۳. چندجمله‌ای اولیه میدان $GF(2^m)$؛ یعنی $p(x)$

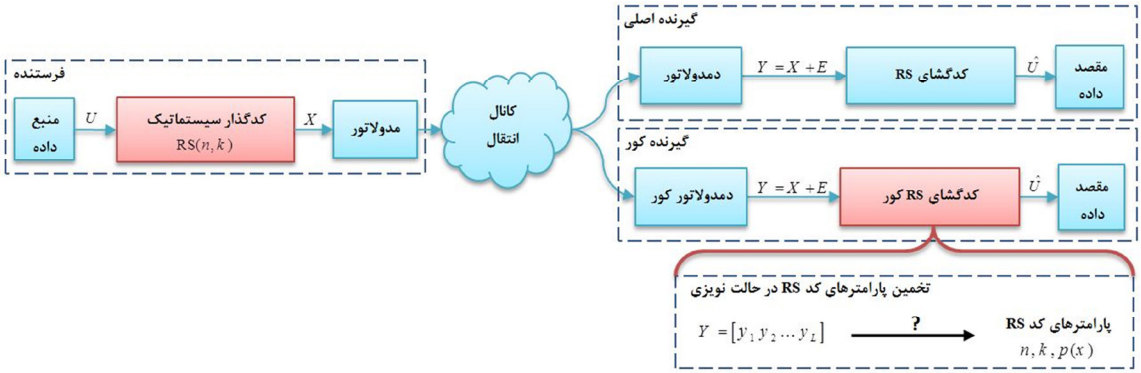
این سه پارامتر، کد RS را به طور کامل توصیف می‌کنند. به عبارت دیگر به ازای هر سه-تایی $(n,k,p(x))$ تنها و تنها یک کد RS بایتری وجود دارد. ما در ادامه این کد را مختصرا به صورت $RS(n,k,p)$ نشان می‌دهیم. پارامتر p معادل هشت-هشتی[۱۶] چندجمله‌ای $p(x)$ است. برای محاسبه p ابتدا ضرایب چندجمله‌ای $p(x)=p_0+p_1x+\ldots+p_mx^m$ به صورت بایتری $(p_m \; p_{m-1}\ldots p_1 \; p_0)_2$ نوشته شده و سپس هر سه بیت متوالی به مبنای ۸ تبدیل می‌شوند. در ضمن اگر تعداد بیت‌ها مضربی از ۳ نباشد، چند بیت صفر از سمت چپ به عدد بایتری اضافه می‌شود. به عنوان مثال معادل هشت-هشتی چندجمله‌ای $1+x^3+x^5$ برابر با $(101001)_2=(51)_8$ است.

در بخش‌های پیش رو یک روش جبری کاملا جدید و موثر برای تخمین پارامترهای کد $RS(n,k,p)$ پیشنهاد می‌شود.

---

۱۵ Binary Symmetric Channel

۱۶



شکل ۱. ترسیم مسئله تخمین پارامترهای کد RS

مبنای ریاضی روش پیشنهادی

مبنای کار روشی که در این مقاله پیشنهاد می‌شود، مجموعه‌ای است که به صورت زیر تعریف می‌شود:

تعریف ۱: مجموعه S متناظر با کد $\mathrm{RS}(n,k,p)$ شامل تمام کدهای $\mathrm{RS}(n,k',p)$ با طول پیام $k' \geq k$ است.

مثال ۱: مجموعه S برای کد $\mathrm{RS}(31,25,45)$ شامل کدهای زیر است:

$$\mathrm{S}=\{\mathrm{RS}(31,25,45),\mathrm{RS}(31,27,45),\mathrm{RS}(31,29,45)\}$$

قضیه زیر رابطه بین کدهای مجموعه S را بیان می‌کند:

قضیه ۱: فرض کنید که کلمه کد C متعلق به کد $\mathrm{RS}(n,k,p)$ باشد. آنگاه C متعلق به تمام کدهای دیگر مجموعه S نیز است.

اثبات: فرض کنید که $k' \geq k$ باشد. همچنین فرض کنید که $g(x)$ و $g'(x)$ به ترتیب چندجمله‌ای‌های مولد کدهای $\mathrm{RS}(n,k,p)$ و $\mathrm{RS}(n,k',p)$ بوده و t و t' نیز به ترتیب قابلیت تصحیح خطای آن‌ها باشند. آنگاه با توجه به رابطه (۱) خواهیم داشت:

$$g(x)=g'(x)\times(x-\alpha^{2t'+1})(x-\alpha^{2t'+2})\ldots(x-\alpha^{2t}) \qquad (۹)$$

حال فرض کنید که C متعلق به کد $\mathrm{RS}(n,k,p)$ بوده و $c_s(x)$ نیز چندجمله‌ای متناظر با آن باشد. آنگاه با توجه به روابط (۲) و (۹) می‌توان نوشت:

$$\begin{aligned} c_s(x) &= u_s(x).g(x) \\ &= c_s(x).g'(x)\times(x-\alpha^{2t+1})\ldots(x-\alpha^{2t'}) \\ &\overset{\Delta}{=} u'_s(x).g'(x) \end{aligned} \qquad (۱۰)$$

رابطه فوق نشان می‌دهد که $c_s(x)$ مضربی از چندجمله‌ای $g'(x)$ است. لذا کلمه کد $c_s(x)$ متعلق به کد $\mathrm{RS}(n,k',p)$ نیز است. □

در این بخش آزمایشی برای تشخیص کدهای مجموعه S از روی رشته دریافتی پیشنهاد می‌شود. ما این آزمایش را آزمایش حد آستانه می‌نامیم. این آزمایش بر مبنای رشته ورودی تشخیص می‌دهد که آیا کد فرضی $\mathrm{RS}(\hat{n},\hat{k},\hat{p})$ متعلق به مجموعه S است و یا خیر؟ به منظور توضیح بهتر این آزمایش، در زیربخش‌های بعدی ابتدا حالت بدون نویز و سپس حالت نویزی بررسی می‌شود.

آزمایش حد آستانه در شرایط غیرنویزی

فرستنده‌ای را در نظر بگیرید که از کد سیستماتیک $\mathrm{RS}(n,k,p)$ برای کدگذاری L بردار پیام $U^{(i)},i=1,2,\ldots,L$ استفاده می‌کند. هر کدام از این بردارها متشکل از km بیت پیام هستند. فرض کنید که $C^{(i)}$ کلمه کد nm-بیتی متناظر با بردار پیام $U^{(i)}$ باشد. همچنین مطابق با روابط (۷) و (۸) فرض کنید که X و Y به ترتیب بردارهای Lmn-بیتی ارسالی و دریافتی باشند.

با توجه به قضیه ۱، کلمه کد $C^{(i)}$ متعلق تمام کدهای مجموعه S است. لذا برای هر کدام از کدهای این مجموعه می‌توان آن را همانند رابطه (۵) به دو قسمت پیام و بررسی توازن تفکیک کرد. این تفکیک برای کد $\mathrm{RS}(n,k',p)\in\mathrm{S}$ به صورت زیر است:

$$C^{(i)}=\left[V_{k'}^{(i)}\quad U_{k'}^{(i)}\right] \qquad (۱۱)$$

که $U_{k'}^{(i)}$ و $V_{k'}^{(i)}$ در آن بردارهای $k'm$-بیتی پیام و $(n-k')m$-بیتی بررسی توازن متناظر با کد $\mathrm{RS}(n,k',p)$ هستند. توجه کنید که اگر $k'=k$ باشد، $U_{k'}^{(i)}=U^{(i)}$ و $V_{k'}^{(i)}=V^{(i)}$ خواهد بود.

فرض کنید که می‌خواهیم حضور کد فرضی $\mathrm{RS}(\hat{n},\hat{k},\hat{p})$ را در مجموعه S توسط آزمایش حد آستانه بررسی کنیم. مراحل این آزمایش پیشنهادی به صورت زیر است:

مرحله ۱: تفکیک بردار Y به بردارهای $\hat{n}\hat{m}$-بیتی $Y^{(i)},i=1,2,\ldots,\hat{L}$؛ برابر با $\hat{L}=\left\lfloor\frac{Lnm}{\hat{n}\hat{m}}\right\rfloor$ است.

مرحله ۲: تفکیک $(\hat{n}-\hat{k})\hat{m}$ بیت اول $Y^{(i)}$ به عنوان بردار $V^{(i)}$ و $\hat{k}\hat{m}$ بیت آخر $Y^{(i)}$ به عنوان بردار $\hat{U}^{(i)}$.

مرحلـه ۳: کدگـذاری $\hat{U}^{(i)}$ توسـط کـد $\mathrm{RS}(\hat{n},\hat{k},\hat{p})$ بـرای محاسبه کلمه کد $\hat{C}^{(i)}$.

مرحله ۴: تفکیک $(\hat{n}-\hat{k})\hat{m}$ بیت اول $\hat{C}^{(i)}$ به عنـوان بـردار $\tilde{V}^{(i)}$.

مرحله ۵: محاسبه تعداد اختلاف‌های بین تمام بردارهای $\hat{V}^{(i)}$ و $\tilde{V}^{(i)}$؛ یعنی:

$$d=\sum_{i=1}^{\hat{L}}\mathrm{wt}\left(\hat{V}^{(i)}+\tilde{V}^{(i)}\right) \qquad (۱۲)$$

عملگر $\mathrm{wt}(.)$ وزن همینگ بردار موردنظر را محاسبه می‌کند.

مرحله ۶: تعیین نتیجه آزمایش بر مبنای مقدار d.

در ادامه نشان خواهیم داد که مقدار d در حالت غیرنویزی تنها زمانی برابـر بـا صـفر اسـت کـه کـد $\mathrm{RS}(\hat{n},\hat{k},\hat{p})$ متعلـق بـه مجموعه S باشد. این یک معیار بسیار مناسب برای تشـخیص کدهای مجموعه S در حالت غیرنویزی است.

در حالت غیرنویزی، بردار دریافتی برابر با بـردار ارسـالی اسـت؛ یعنی $Y=X$. لذا اگر شـرط $\hat{n}=n$ برقـرار باشـد، بردارهـای $Y^{(i)}$ که در مرحله ۱ محاسبه می‌شوند، برابـر بـا کلمـات کـد $C^{(i)}$ خواهند بود. توجه داشته باشید کـه عـدم برقـراری ایـن شرط، ساختار بردارهای $Y^{(i)}$ را به طور کامل از بین می‌برد. به عنوان مثال این بردارها دیگـر از خاصـیت چرخشـی برخـوردار نیستند. لذا اگر $\hat{n}\neq n$ باشـد، بردارهـای $Y^{(i)}$ مـی‌تواننـد بـه صورت بردارهای باینری کاملا تصـادفی در نظـر گرفتـه شـوند. لازم به ذکر است که تمام کدهای مجموعـه S دارای طـول n هستند.

فرض کنید که k' طول پیام متناظر با یکی از کدهای مجموعه S باشد؛ یعنی $k'\geq k$. در این صـورت اگـر شـروط $\hat{n}=n$ و $\hat{k}=k'$ به طور همزمان برقرار باشند، بردارهـای $\hat{U}^{(i)}$ و $\hat{V}^{(i)}$ که در مرحله ۲ محاسبه می‌شوند، همانند رابطه (۱۱) به ترتیب برابـر بـا بـردار پیـام و بـردار بررسـی تـوازن متنـاظر بـا کـد $\mathrm{RS}(n,k',p)\in \mathrm{S}$ خواهنـــد بـــود؛ یعنـــی $\hat{U}^{(i)}=U_{k'}^{(i)}$ و $\hat{V}^{(i)}=V_{k'}^{(i)}$.

همانگونه که پیش از این نیز اشاره شد، پارامترهـای سـه-گانـه (n,k,p) به طور کامل یک کد RS را توصیف مـی‌کننـد. لـذا اگر شرط $\hat{p}=p$ نیز علاوه بر دو شرط فوق برقرار باشد، مـی-تـوان گفـت کـه کـد مـورد آزمـایش در حقیقـت همـان کـد $\mathrm{RS}(n,k',p)$ است. در این حالت اگـر بـردار پیـام حاصـل در مرحله ۲ (یعنی $\hat{U}^{(i)}=U_{k'}^{(i)}$) مجددا توسط کد $\mathrm{RS}(n,k',p)$ کدگذاری شود (مطابق بـا مرحلـه ۳)، دقیقـا کلمـه کـد $C^{(i)}$ حاصل می‌شود؛ یعنی $\hat{C}^{(i)}=C^{(i)}$. در نتیجه بردارهای بررسی توازن $\tilde{V}^{(i)}$ که در مرحله ۴ محاسبه می‌شـوند، برابـر بـا بـردار بررسی توازن ارسالی خواهند بـود؛ یعنـی $\tilde{V}^{(i)}=\hat{V}^{(i)}=V_{k'}^{(i)}$. در این حالت مقدار d بر طبق رابطه (۱۲) برابر با صفر است.

توجه داشته باشید کـه رابطـه $\tilde{V}^{(i)}=\hat{V}^{(i)}$ (معـادل بـا رابطـه $d=0$) تنها به ازای کدهای مجموعه S برقرار است. به عنوان مثال، عدم برقراری شرط $\hat{n}=n$ خاصیت چرخشـی بردارهـای $\hat{C}^{(i)}$ را از بین می‌برد. عدم برقراری شـرط $\hat{k}\geq k$ نیـز تنـاظر بین بردارهای $\hat{U}^{(i)}$ و $\hat{V}^{(i)}$ را از بین می‌برد؛ یعنی این بردارها دیگر بردارهای پیام و بررسی توازن متناظر با یک کلمه کد RS نیستند. عدم برقراری شرط $\hat{p}=p$ نیز موجب تشخیص اشتباه کد RS در مرحله ۳ می‌شود. این امر نیـز باعـث مـی‌شـود کـه بردارهای $\hat{V}^{(i)}=V_{k'}^{(i)}$ و $\tilde{V}^{(i)}$ با هم برابر نشوند.

عدم برقراری هر کدام از سه شرط مذکور رابطه بـین بردارهـای $\hat{V}^{(i)}$ و $\tilde{V}^{(i)}$ را به طور کامل از بین می‌برد. در این حالت می-توان بردارهای $\hat{V}^{(i)}$ و $\tilde{V}^{(i)}$ را نسبت به هم کـاملا مسـتقل و تصادفی در نظر گرفت. لذا احتمال تغایر هر کـدام از بیـت‌هـای آن‌ها برابر با ۰٫۵ است. به عبارت دیگر، هـر کـدام از بیـت‌هـای بردار $\hat{V}^{(i)}+\tilde{V}^{(i)}$ مستقلا با احتمال ۰٫۵ برابر با یک و با همین احتمال برابر با صفر هستند. با توجه به این که تعداد کل بیـت-های بررسی توازن برابر با $N\overset{\Delta}{=}\hat{L}(\hat{n}-\hat{k})\hat{m}$ است، ایـن بیـت‌هـا می‌توانند دقیقا با $\binom{N}{z}$ حالت مختلف در z بیت متفاوت باشند (یعنی $d=z$). در نتیجه توزیع احتمال متغیر d برای کدهایی که در مجموعه S قرار ندارند، به صورت زیر است [۲۶]:

$$\Pr(d=z)=\binom{N}{z}0.5^{z}(1-0.5)^{N-z}=\binom{N}{z}.\frac{1}{2^{z}} \qquad (۱۳)$$

این رابطه نشان دهنده توزیع دوجملـه‌ای[۱۷] $\mathrm{B}(N,0.5)$ اسـت. تابع احتمال متناظر با توزیع دوجمله‌ای $\mathrm{B}(N,\varepsilon)$ بـه صـورت زیر تعریف می‌شود [۲۶]:

$$f_Z(z)=\binom{N}{z}\varepsilon^{z}(1-\varepsilon)^{N-z} \qquad (۱۴)$$

میانگین و واریانس این توزیع بـه ترتیـب برابـر بـا $\mu=N\varepsilon$ و $\sigma^2=N\varepsilon(1-\varepsilon)$ هستند.

به طور خلاصه، قاعده تصمیم‌گیـری در مرحلـه ۶ بـرای حالـت غیرنویزی می‌تواند به این صورت بیان شود: اگـر $d=0$ باشـد، کد $\mathrm{RS}(\hat{n},\hat{k},\hat{p})$ متعلق به مجموعـه S بـوده و در غیـر ایـن صورت خارج از مجموعه S است. البتـه ایـن قاعـده در حالـت نویزی کارایی ندارد، زیرا نویز باعث تغییر در مقدار d مـی‌شـود. در زیربخش بعدی به بررسی تاثیر نویز بر آزمایش حـد آسـتانه پرداخته می‌شود.

آزمایش حد آستانه در شرایط نویزی

در این بخش تاثیر نویز بر روی مقدار d بررسی مـی‌شـود. ابتـدا کدهای خارج از مجموعه S را در نظر بگیرید. همانگونه که در

۱۷

زیربخش قبل دیدید، بردارهای $\hat{V}^{(i)}$ و $\tilde{V}^{(i)}$ در این کدها کاملا مستقل و تصادفی هستند. همین امر موجب می‌شود که متغیر d دارای تصادفی‌ترین توزیع احتمال ممکن باشد؛ یعنی توزیع $\mathrm{B}(N,0.5)$. لذا وجود نویز تاثیری بر روی این توزیع ندارد؛ زیرا وجود خطای کانال قطعا خاصیت تصادفی را بیشتر می‌کند. در ادامه تاثیر نویز بر روی کدهای مجموعه S بررسی می‌شود.

یک کانال باینری متقارن را با احتمال خطای ε در نظر بگیرید. رشته‌ای که از طریق این کانال دریافت می‌شود، نسخه‌ای تغییر یافته از رشته ارسالی است؛ یعنی $Y=X+E$. فرض کنید که $E_V^{(i)}$ و $E_U^{(i)}$ به ترتیب بردارهای خطای موجود در بردارهای $V_{k'}^{(i)}$ و $U_{k'}^{(i)}$ باشند؛ یعنی $\hat{V}^{(i)}=V_{k'}^{(i)}+E_V^{(i)}$ و $\hat{U}^{(i)}=U_{k'}^{(i)}+E_U^{(i)}$. با این فرض ممکن است یکی از دو حالت زیر رخ دهد:

حالت ۱: فرض کنید که $E_U^{(i)}$ یک بردار تمام-صفر باشد. بردار $\hat{U}^{(i)}$ در این حالت بدون خطا است؛ یعنی $\hat{U}^{(i)}=U_{k'}^{(i)}$. لذا همانند حالت غیرنویزی، رابطه $\tilde{V}^{(i)}=V_{k'}^{(i)}$ برقرار است. در نتیجه خواهیم داشت:

$$\hat{V}^{(i)}+\tilde{V}^{(i)}=V_{k'}^{(i)}+V_{k'}^{(i)}+E_V^{(i)}=E_V^{(i)} \qquad (۱۵)$$

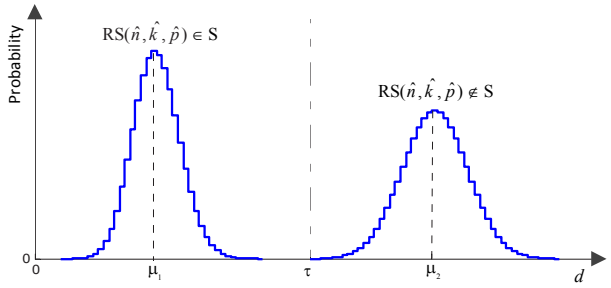
با توجه به این رابطه، هر کدام از بیت‌های بردار $\hat{V}^{(i)}+\tilde{V}^{(i)}$ مستقلا با احتمال ε برابر با یک و با احتمال $(1-\varepsilon)$ برابر با صفر هستند. در نتیجه متغیر d در این حالت دارای توزیع $\mathrm{B}(N,\varepsilon)$ است.

حالت ۲: فرض کنید که $E_U^{(i)}$ یک بردار تمام-صفر نباشد. بردار $\hat{U}^{(i)}$ در این حالت برابر با بردار پیام ارسالی نیست؛ یعنی $\hat{U}^{(i)}\neq U_{k'}^{(i)}$. توجه داشته باشید که تغییر حتی یک بیت پیام می‌تواند به یک کلمه کد کاملا متفاوت منجر شود. لذا بردار $\hat{C}^{(i)}$ که در مرحله ۳ حاصل می‌شود، با کلمه کد $C^{(i)}$ کاملا متفاوت است. این امر رابطه بین بردارهای $\hat{V}^{(i)}$ و $\tilde{V}^{(i)}$ را به طور کامل از بین می‌برد. در نتیجه متغیر d در این حالت دارای توزیع $\mathrm{B}(N,0.5)$ است.

بردار $E_U^{(i)}$ متشکل از $(\hat{n}-\hat{k})\hat{m}$ بیت مستقل بوده و هرکدام از آن‌ها با احتمال ε برابر با یک هستند. در نتیجه احتمال رخداد حالت ۱ (یعنی صفر بودن تمام بیت‌ها) برابر با $\lambda\overset{\Delta}{=}(1-\varepsilon)^{(\hat{n}-\hat{k})\hat{m}}$ است. احتمال رخداد حالت ۲ نیز برابر با $1-\lambda$ است. با توجه به این مطلب، توزیع احتمال متغیر d در حالت نویزی می‌تواند به صورت زیر نوشته شود:

$$d\sim\begin{cases}\lambda\mathrm{B}(N,\varepsilon)+(1-\lambda)\mathrm{B}(N,0.5) & ;\ \mathrm{RS}(\hat{n},\hat{k},\hat{p})\in\mathrm{S}\\ \mathrm{B}(N,0.5) & ;\ \mathrm{RS}(\hat{n},\hat{k},\hat{p})\notin\mathrm{S}\end{cases} \qquad (۱۶)$$

این توزیع‌ها به صورت شماتیک در شکل ۲ رسم شده‌اند. میانگین این توزیع‌ها به ترتیب برابر با $\mu_1=\lambda N\varepsilon+(1-\lambda)N/2$ و $\mu_2=N/2$ است. همچنین به راحتی می‌توان نشان داد که واریانس آن‌ها به ترتیب برابر $\sigma_1^2=\lambda N\varepsilon(1-\varepsilon)+(1-\lambda)N/4+\lambda(1-\lambda)(N/2-N\varepsilon)^2$ و $\sigma_2^2=N/4$ است. همانگونه که در شکل ۲ نیز می‌بینید، از تفاوت بین توزیع‌های احتمال می‌توان برای تشخیص کدهای مجموعه S بهره برد. برای انجام این کار باید یک حد آستانه مناسب بین مقادیر μ_1 و μ_2 انتخاب شود (در پیوست مقاله دو مقدار مناسب برای حد آستانه پیشنهاد شده است). این مقدار در شکل ۲ با متغیر τ مشخص شده است. مقدار d برای تصمیم‌گیری در مرحله ۶ باید با مقدار τ مقایسه شود. اگر مقدار d کوچکتر از τ باشد، کد مورد آزمایش به عنوان یک کد مجموعه S اعلام می‌شود.



شکل ۲: توزیع احتمال متغیر d در شرایط نویزی

روش پیشنهادی

روشی که در این بخش برای تخمین پارامترهای کد RS پیشنهاد می‌شود، بر مبنای خواص مجموعه S استوار است. این خواص عبارتند از:

خاصیت ۱: تمام کدهای مجموعه S دارای طول کد n و چندجمله‌ای مولد p هستند.

خاصیت ۲: تمام کدهای $\mathrm{RS}(n,k',p)$ با طول پیام بزرگتر و یا مساوی k در مجموعه S قرار دارند.

با توجه به این خواص، تخمین پارامترهای کد RS می‌تواند در دو مرحله کاملا مجزا انجام شود. این مراحل در زیربخش‌های پیشرو تشریح شده‌اند.

تخمین پارامترهای n و p

با توجه به خاصیت اول مجموعه S، تخمین پارامترهای n و p می‌تواند با یافتن حداقل یکی از اعضای این مجموعه انجام شود. از طرفی بر طبق خاصیت ۲، کد $\mathrm{RS}(n,n-2,p)$ همواره یکی از اعضای مجموعه S است. لذا برای تخمین پارامتر n و p تنها کافیست که تمام کدهای RS با نرخ $\frac{n-2}{n}$ مورد آزمایش حد آستانه قرار گیرند. مقادیر n و p برابر با پارامترهای اولین کدی هستند که حضور آن در مجموعه S توسط آزمایش حد آستانه تایید شود.

تخمین پارامترهای k

با توجه به خاصیت دوم مجموعه S، کمترین طول پیام در این مجموعه متعلق به کد RS اصلی است؛ یعنی کد $RS(n,k,p)$. لذا ساده‌ترین روش برای تخمین پارامتر k این است که کدهای $RS(n,\hat{k},p)$ را به ترتیب معکوس (بر حسب طول پیام) مورد آزمایش قرار دهیم. با توجه به خاصیت ۲، کد $RS(n,k,p)$ آخرین کدی است که حضور آن در مجموعه S توسط آزمایش حد آستانه تایید می‌شود. در نتیجه طول پیام آخرین کد تایید شده برابر با پارامتر k است.

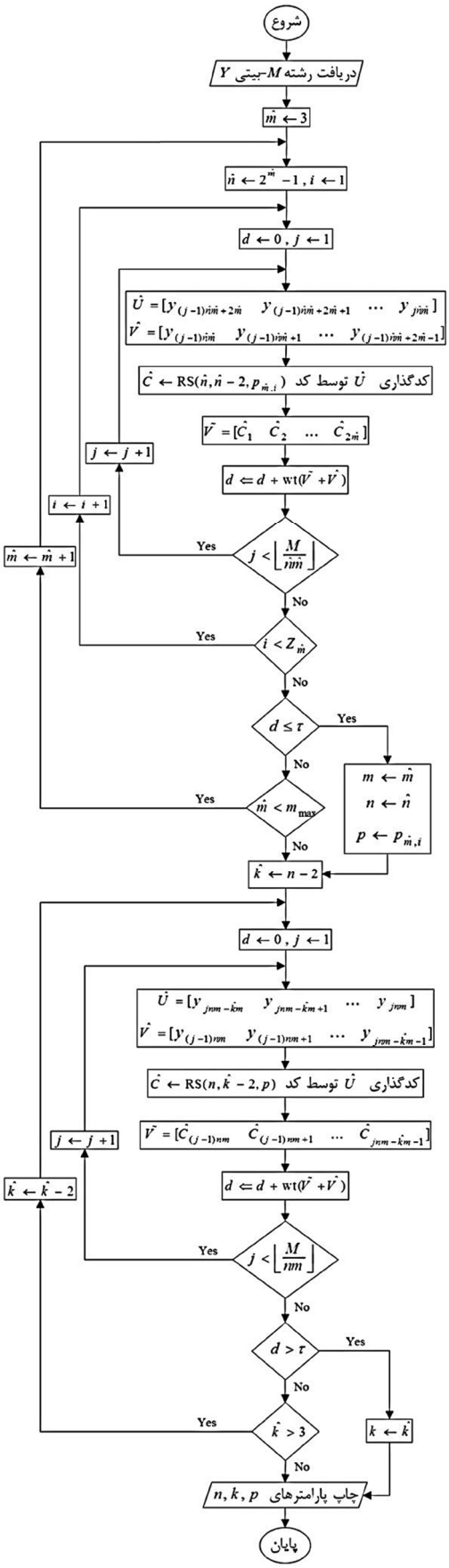
پیچیدگی محاسباتی الگوریتم

الگوریتم پیشنهادی به صورت فلوچارت در شکل ۳ ارائه شده است. پارامتر $m_{\max}$ در این فلوچارت بزرگترین مقدار را برای جستجوی پارامتر m نشان می‌دهد. با توجه به این که طول کدهای RS در کاربردهای عملی از مقدار ۲۵۵ تجاوز نمی‌کند، ما مقدار ۸ را برای $m_{\max}$ پیشنهاد می‌دهیم. پارامتر $Z_{\hat{m}}$ در این فلوچارت برابر با تعداد تمام چندجمله‌ای‌های اولیه با درجه $\hat{m}$ است. پارامتر $p_{\hat{m},i}$ نیز یکی از این چندجمله‌ای‌های اولیه را نشان می‌دهد که با اندیس i شماره‌گذاری شده است.

بیشترین محاسبات در الگوریتم پیشنهادی برای کدگذاری بیت‌های پیام انجام می‌شود. برای تخمین پارامترهای n و p تنها کدهای نرخ $\frac{n-2}{n}$ آزمایش می‌شوند که تعداد آن‌ها برای مقدار $\hat{m}$ برابر با $Z_{\hat{m}}$ است. برای تخمین پارامتر k نیز دقیقا $\frac{n-k}{2}$ کد دیگر مورد آزمایش قرار می‌گیرند. کدگذاری یک بردار پیام توسط کد $RS(\hat{n},\hat{k},\hat{p})$ با پیچیدگی محاسباتی از درجه $O(\hat{n}^2\hat{m}^2)$ قابل انجام است. لذا با توجه به این که تعداد کل بردارهای پیام دریافتی برابر با $\left\lfloor \frac{Lnm}{\hat{n}\hat{m}} \right\rfloor$ است، پیچیدگی محاسباتی الگوریتم پیشنهادی می‌تواند به صورت رابطه تقریبی زیر نوشته شود:

$$C = \sum_{\hat{m}=3}^{m}\left(Z_{\hat{m}} \left\lfloor \frac{Lmn}{\hat{n}\hat{m}} \right\rfloor (\hat{n}\hat{m})^2 \right) + \frac{(n-k)}{2} L(nm)^2 \approx O(n^3) \qquad (۱۷)$$

این رابطه نشان می‌دهد که الگوریتم پیشنهادی از پیچیدگی نسبتا پایینی برخوردار بوده و در نتیجه برای کاربردهای زمان-واقعی[۱۸] بسیار مناسب می‌سازد. توجه داشته باشید که رابطه فوق در حقیقت بیشترین مقدار پیچیدگی ممکن را برای این الگوریتم نشان می‌دهد؛ زیرا کدگذارهای RS در عمل می‌توانند با پیچیدگی بسیار کمتر از $O(\hat{n}^2\hat{m}^2)$ پیاده‌سازی شوند که استفاده از آن‌ها منجر به کاهش پیچیدگی محاسباتی الگوریتم پیشنهادی می‌شود.



نتایج شبیه‌سازی

در این بخش چند مثال شبیه‌سازی به منظور بررسی عملکرد الگوریتم پیشنهادی ارائه می‌شود. برای این منظور، الگوریتم پیشنهادی بر روی چند کد RS با پارامترهای مختلف اعمال شده است. معیار ارزیابی عملکرد، احتمال تشخیص صحیح پارامترهای کد RS به ازای نرخ‌های مختلف خطای کانال است. در تمام شبیه‌سازی‌ها از $L=100$ کلمه کد استفاده شده است. به ازای هر کدام از مقادیر ε، مراحل زیر مستقلا ۳۰۰ بار اجرا شده‌اند:

۱. تولید یک رشته پیام تصادفی باینری با طول $L_k = L \times km$

۲. کدگذاری رشته پیام توسط کدگذار سیستماتیک $\mathrm{RS}(n,k,p)$ و تولید رشته کدی با طول $L_n = L \times nm$

۳. عبور کلمات کد از یک کانال باینری متقارن با احتمال خطای ε

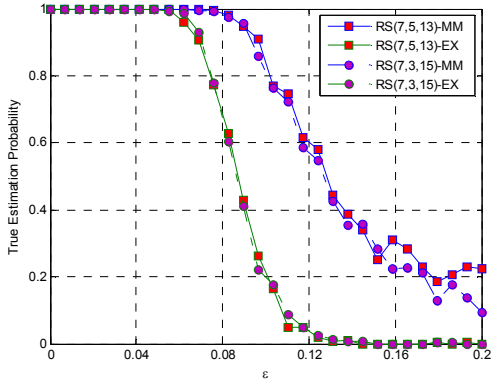
۴. تخمین پارامترهای کد RS از روی رشته نویزی با استفاده از الگوریتم پیشنهادی

۵. مقایسه پارامترهای تخمینی با مقادیر واقعی

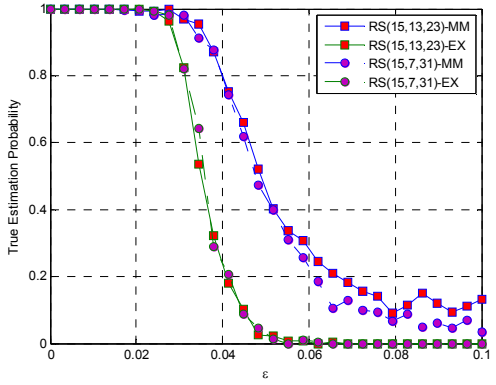
مراحل فوق مستقلا برای هر کدام از مقادیر حدود آستانه اجرا شده‌اند. نتایج شبیه‌سازی در شکل‌های ۴ تا ۷ رسم شده‌اند. منحنی‌های مرتبط با حدود آستانه حداقل-بیشینه و تجربی در این شکل‌ها به ترتیب با نمادهای MM و EX مشخص شده‌اند. قطع نظر از نوع حد آستانه، نتایج شبیه‌سازی از عملکرد بالای الگوریتم پیشنهادی حکایت دارند.

همانگونه که در شکل‌های ۴ تا ۷ نیز می‌توان دید، عملکرد الگوریتم پیشنهادی با حد آستانه حداقل-بیشینه همواره بهتر از عملکرد آن با حد آستانه تجربی است. علت این امر نیز واضح است؛ حد آستانه حداقل-بیشینه با فرض آگاهی از مقدار نرخ خطای کانال طراحی شده و لذا نسبت به حد آستانه تجربی بهینه‌تر است. البته انتخاب مناسب حد آستانه تجربی موجب شده تا افت عملکرد آن نسبت به حد آستانه حداقل-بیشینه زیاد نباشد. البته باید به این نکته توجه داشت که در بسیاری از مسائل عملی احتمال خطای کانال مجهول بوده و در این کاربردها تنها می‌توان از حد آستانه تجربی استفاده کرد.

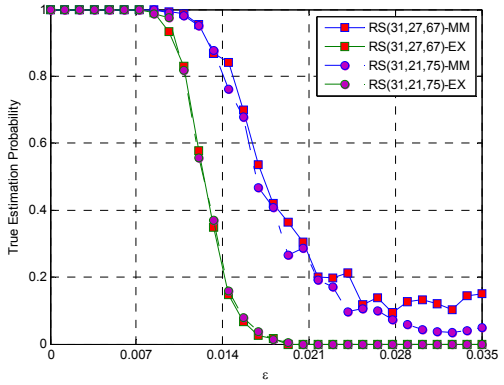
با توجه به نتایج شبیه‌سازی، عملکرد الگوریتم پیشنهادی نسبت به پارامترهای k و p تقریبا ثابت است. به عنوان مثال به احتمال تخمین صحیح کدهای $\mathrm{RS}(7,5,13)$ و $\mathrm{RS}(7,3,15)$ در شکل ۴ توجه کنید. با وجود پارامترهای k و p متفاوت در این کدها، الگوریتم پیشنهادی (بر مبنای حد آستانه حداقل-بیشینه) موفق به تخمین کامل (یعنی تخمین با احتمال یک)



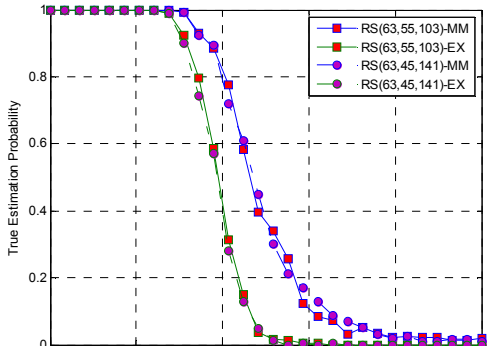
شکل ۴: احتمال تخمین صحیح پارامترهای کد RS با طول $n=7$



شکل ۵: احتمال تخمین صحیح پارامترهای کد RS با طول $n=15$



شکل ۶: احتمال تخمین صحیح پارامترهای کد RS با طول $n=31$



نکته دیگری که از نتایج شبیه‌سازی می‌توان دریافت این است که احتمال تخمین صحیح پارامترهای کد متناسب با افزایش طول کلمات کد کاهش می‌یابد. به عنوان مثال احتمال تخمین کامل پارامترهای کد (با فرض حد آستانه حداقل-بیشینه) در طول‌های $n = 7,15,31,63$ به ترتیب در نرخ‌های خطای $\varepsilon = 0.045,0.011,0.037,0.008$ قابل حصول است (هر کدام از این نرخ‌های خطا تقریبا نصف نرخ خطای قبلی است). به این نکته توجه داشته باشید که افزایش طول کد، احتمال نویزی بودن کلمات کد دریافتی را افزایش می‌دهد. این امر باعث نزدیکی بیشتر توزیع‌های احتمال متغیر d در شکل ۲ شده و در نتیجه احتمال تشخیص صحیح کدهای مجموعه S کاهش می‌یابد.

نتیجه‌گیری

در این مقاله الگوریتمی کاملا جدید و موثر برای تخمین پارامترهای کد RS در شرایط نویزی پیشنهاد شد. تشخیص پارامترها در این روش بر مبنای مجموعه‌ای خاص از کدهای RS انجام می‌پذیرد. ویژگی اصلی این مجموعه، حضور کلمات کد دریافتی در تمام کدهای متعلق به آن است. به موجب خواص این مجموعه، پارامترهای کد می‌توانند در دو مرحله کاملا مجزا تعیین شوند. این امر موجب می‌شود که الگوریتم پیشنهادی از پیچیدگی نسبتا پایینی برخوردار باشد. در این مقاله یک آزمایش مبتنی بر حد آستانه برای تشخیص کدهای این مجموعه پیشنهاد شد. در این آزمایش، بیت‌های بررسی توازن مجددا توسط بیت‌های پیام دریافتی تولید شده و از تعداد اختلاف آن‌ها با بیت‌های توازن دریافتی برای تصمیم‌گیری در مورد کد استفاده می‌شود. برای این منظور دو مقدار حد آستانه مناسب با فرض معلوم یا مجهول بودن نرخ خطای کانال پیشنهاد شد. نتایج شبیه‌سازی نشان می‌دهند که عملکرد الگوریتم پیشنهادی (قطع نظر از نوع حد آستانه) در شرایط نویزی بسیار مناسب است. به عنوان مثال این روش می‌تواند کدهای RS با طول ۳۱ و ۶۳ را به ترتیب تا نرخ‌های خطای 8×10^{-3} و 4×10^{-3} به طور کامل تخمین بزند. پیچیدگی الگوریتم پیشنهادی از درجه $O(n^3)$ است که این امر آن را برای کاربردهای زمان-واقعی بسیار مناسب ساخته است.

همانگونه که می‌دانید، کد RS در زمره کدهای چرخشی غیرباینری قرار دارد. لذا تعمیم روش پیشنهادی به کدهای چرخشی دیگر می‌تواند موضوع تحقیق دیگری در این زمینه باشد. همچنین نحوه عملکرد این روش در حالت تصمیم‌گیری نرم[۱۹] می‌تواند در کاری مجزا مورد بررسی قرار گیرد.

پیوست

در این پیوست دو حد آستانه مناسب برای آزمایش کدهای RS پیشنهاد می‌شود. حد آستانه اول برای زمانی مناسب است که نرخ خطای کانال معلوم باشد. در حالی که حد آستانه دوم بر مبنای عدم آگاهی از نرخ خطای کانال طراحی شده است.

قبل از پیشنهاد این مقادیر باید اشاره شود که افزایش تعداد کلمات کد دریافتی به طور کلی (قطع نظر از نوع حد آستانه) موجب بهبود در تشخیص کدهای مجموعه S می‌شود. این موضوع را می‌توان با توجه به شکل ۲ توضیح داد. مطابق با این شکل، فشردگی بیشتر منحنی‌های احتمال باعث تفکیک بهتر آن‌ها و در نتیجه بروز خطای کمتر در تشخیص می‌شود.

به راحتی می‌توان نشان داد که افزایش تعداد کلمات کد دریافتی موجب فشردگی نسبی این منحنی‌ها می‌شود. برای این منظور، متغیر نرمالیزه شده $r \overset{\Delta}{=} d/n$ را در نظر بگیرید. میانگین r برای منحنی‌های احتمال به ترتیب برابر با $\mu_1' = \mu_1/N = \lambda\varepsilon + (1-\lambda)/2$ و $\mu_2' = \mu_1/N = 1/2$ است. واریانس متغیر r نیز برای این توزیع‌ها به ترتیب برابر $\sigma_1'^2 = \sigma_1^2/N^2 = \lambda\varepsilon(1-\varepsilon)/N + (1-\lambda)/4N + \lambda(1-\lambda)(1/2-\varepsilon)^2$ و $\sigma_2'^2 = \sigma_2^2/N^2 = 1/4N$ است. با توجه به این روابط، افزایش N موجب کاهش واریانس r در هر دو توزیع می‌شود. این در حالی است که میانگین r به مقدار N وابسته نیست. این امر در حقیقت به معنای فشردگی نسبی منحنی‌های احتمال است.

پیشنهاد حد آستانه با فرض آگاهی از احتمال خطا

فرض کنید که P_{FA} احتمال تشخیص اشتباه یک کد خارج از مجموعه S باشد. ناحیه متناظر با این احتمال قسمتی از مساحت زیر منحنی دوم است که در سمت راست مقدار τ قرار دارد (شکل ۲ را ببینید). این احتمال با توجه به رابطه (۱۱) می‌تواند به صورت زیر نوشته شود:

$$P_{FA} = \left(\frac{1}{2}\right)^N \sum_{z=0}^{\tau} \binom{N}{z} \qquad (۱۸)$$

همچنین فرض کنید P_M احتمال عدم تشخیص صحیح یک کد مجموعه S باشد. ناحیه متناظر با این احتمال نیز قسمتی از مساحت زیر منحنی اول است که در سمت چپ حد آستانه قرار دارد. لذا مقدار آن برابر با رابطه زیر است:

$$P_M = \sum_{z=\tau+1}^{N} \binom{N}{z} \varepsilon^z (1-\varepsilon)^{N-z} \qquad (۱۹)$$

با توجه به این دو تعریف، احتمال خطای کلی می‌تواند به صورت زیر نوشته شود [۲۷]:

$$P_e = \pi P_M + (1-\pi) P_{FA} \qquad (۲۰)$$

که در آن π نسبت کدهایی است که متعلق به مجموعه S هستند. برای محاسبه حد آستانه بهینه باید احتمال خطای

[۱۹]

فوق بر حسب مقدار τ کمینه گردد. البته مقدار π باید برای حل این مسأله معلوم باشد. ولی این شرط در مسأله تشخیص کدهای مجموعه S برقرار نیست؛ زیرا تعداد کدهای این مجموعه را نمی‌توان پیش از تخمین آن تعیین کرد. البته این یک مشکل کاملا شایع در مسائل تصمیم‌گیری بهینه است که غالبا توسط قاعده تصمیم‌گیری حداقل-بیشینه حل می‌شود [۲۷]. این قاعده ساده و موثر در مسائلی استفاده می‌شود که توزیع‌های احتمال پیشین معلوم نیستند. این قاعده در واقع بیشترین احتمال خطای ممکن را حداقل می‌کند. برای یافتن حد آستانه بر مبنای قاعده تصمیم‌گیری حداقل-بیشینه باید معادله زیر بر حسب پارامتر τ حل شود [۲۷]:

$$P_M = P_{FA} \qquad (۲۱)$$

حل تحلیلی این معادله با توجه به پیچیدگی روابط (۱۸) و (۱۹) ممکن نیست. ولی برای ساده‌سازی آن می‌توان از تقریب زیر استفاده کرد [۲۶]:

$$\mathrm{B}(x,p) \approx \mathrm{N}\,(xp, xp(1-p)) \qquad (۲۲)$$

که در آن $\mathrm{N}\,(xp, xp(1-p))$ نشان دهنده یک توزیع نرمال با میانگین xp و واریانس $xp(1-p)$ است. با توجه به این تقریب، رابطه (۲۱) می‌تواند با اندکی محاسبات ساده به صورت زیر نوشته شود:

$$Q\left(\frac{\tau-\mu_2}{\sigma_2}\right) \approx Q\left(\frac{\mu_1-\tau}{\sigma_1}\right) \qquad (۲۳)$$

که در آن تابع $Q(x)$ به صورت زیر تعریف می‌شود:

$$Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^{\infty} e^{-\frac{x^2}{2}} dx \qquad (۲۴)$$

نهایتا با حل معادله (۲۳) رابطه زیر حاصل می‌شود:

$$\tau \approx \frac{\mu_1\sigma_2 + \mu_2\sigma_1}{\sigma_1+\sigma_2} \qquad (۲۵)$$

توجه داشته باشید که این رابطه به مقدار ε وابسته است.

پیشنهاد حد آستانه با فرض عدم آگاهی از احتمال خطا

با توجه به رابطه (۱۶)، توزیع اول متغیر d به نرخ خطای کانال وابسته است. یعنی این توزیع با تغییر مقدار ε جابجا می‌شود. ولی توزیع دوم مستقل از نرخ خطای کانال است. در نتیجه بهترین انتخاب برای حد آستانه مقداری نزدیک به مرکز توزیع دوم است. بر مبنای یک قاعده معروف، احتمال پیشامد $|d-\mu_2| > 4\sigma_2$ را می‌توان با تقریب بسیار خوبی برابر با صفر در نظر گرفت. در نتیجه ما مقدار تجربی زیر را برای حد آستانه پیشنهاد می‌دهیم:

$$\tau = \mu_2 - 4\sigma_2 \qquad (۲۶)$$

توجه داشته باشید که این رابطه مستقل از مقدار ε است.

مراجع

[1] A. Valembois, "Detection and recognition of a binary linear code," Discrete Applied Mathematics, vol. 111, no. 1, pp. 199-218, July 2001.

[2] M. Cluzeau, "Block code reconstruction using iterative decoding techniques" IEEE International Symposium on Information Theory (ISIT), Seattle, WA, pp. 2269-2273, July 2006.

[3] M. Cluzeau and M. Finiasz, "Recovering a code's length and synchronization from a noisy intercepted bitstream," IEEE International Symposium on Information Theory (ISIT), Seoul, pp. 2737-2741, June 2009.

[4] L. Lu, K. Li and Y.Guan, "Blind detection of interleaver parameters for non-binary coded data streams," IEEE International Conference on Communications (ICC), Dresden, pp. 1-4, June 2009.

[5] M. Marazin, R. Gautier and G. Burel, "Blind recovery of k/n rate convolutional encoders in a noisy environment," EURASIP Journal on Wireless Communications and Networking, vol. 2011, no. 168, pp. 1-9, Nov. 2011.

[6] M. Marazin, R. Gautier and G. Burel, "Algebraic method for blind recovery of punctured convolutional encoders from an erroneous bitstream," IET Signal Processing, vol. 6, no. 2, pp. 122-131, Apr. 2012.

[7] Z. Jing, H. Zhiping, S. Shaojing and Z. Yimeng, "Blind identification of convolutional codes in soft-decision situations," International Journal of Modern Communication Technologies Research (IJMCTR), vol. 2, no. 4, May 2014.

[8] W. Chen and G. Wu, "Blind Recognition of (n-1)/n Rate Punctured Convolutional Encoders in a Noisy Environment," Journal of Communications, vol. 10, no. 4, Jan. 2015.

[9] Y.G. Debessu, W. Hsiao-Chun, J. Hong and S.Y. Chang, "Blind encoder parameter estimation for turbo codes," IEEE Global Communications Conference (GLOBECOM), Anaheim, CA, pp. 4233-4237, Dec. 2012.

[10] R. Moosavi and E.G. Larsson, "Fast blind recognition of channel codes," IEEE Transaction on Communications, vol. 62, no. 5, pp.1393-1405, May 2014.

[11] Y.G. Debessu, W. Hsiao-Chun and J. Hong, "Novel blind encoder parameter estimation

Letters, vol. 16, no. 12, pp. 1917-1920, Dec. 2012.

[12] J. Dingel and J. Hagenauer, "Parameter estimation of a convolutional encoder from noisy observations," IEEE International Symposium on Information Theory (ISIT), Nice, pp. 1776-1780, June 2007.

[13] J. Wang, Y. Yue and J. Yao, "A method of blind recognition of cyclic code generator polynomial," International Conference on Wireless Communications Networking and Mobile Computing (WiCOM), Chengdu, pp. 1-4, Sept. 2010.

[14] J. Wang, Y. Yue and J. Yao, "Statistical recognition method of binary BCH code," Communications and Network, vol. 3, no. 1, pp. 17-22, Feb. 2011.

[15] J. Zhou, Z. Huang, C. Liu, S. Su and Y. Zhang, "Information-dispersion-entropy-based blind recognition of binary BCH codes in soft decision situations," Entropy, vol. 15, no. 5, pp. 1705-1725, May 2013.

[16] Z. Jing, H. Zhiping, S. Shaojing and Y. Shaowu, "Blind recognition of binary cyclic codes," EURASIP Journal on Wireless Communications and Networking, vol. 2013, no. 1, Aug. 2013.

[17] L. Jian, X. Nuo and Z. Xiyuan, "Blind recognition method of RS coding," Journal of University of Electronic Science and Technology of China, vol. 38, no. 3, pp. 363-367, Mar. 2009.

[18] L. Xizai, S. Shaojing and H. Zhiping, "A fast blind recognition method of RS coding," Journal of National University of Defense Technology, vol. 33, no. 4, pp. 123-127, Apr. 2011.

[19] L. Ouxin, G. Lu and L. Hongshu, "Blind reconstruction of RS code," Asian Journal of Applied Sciences, vol. 8, no. 1, pp. 37-45, Jan. 2015.

[20] Q. Lin, H. Shiqi, W. Lei and W. Yong, "A fast blind recognition method of RS codes," Journal of Circuits and Systems, vol. 16, no. 2, pp. 71-76, Feb. 2011.

[21] Q. Lin, H. Shiqi and L. Jinshan, "Recognition method of RS codes based on Euclidean algorithm in galois field," Journal of Detection and Control, vol. 33, no. 2, pp. 63-67, Feb. 2011.

[22] L. Yujun and Y. Yuping, "Studies on the features of rs codes over finite fields," Journal of Information Engineering University, vol. 8, no. 1, pp. 64-67, Jan. 2007.

[23] W. Niancheng and Y. Xiaojing, "Blind recognition of RS code based on code roots statistic," Journal of Communication Countermeasures, vol. 4, no. 1, pp. 18-21, Apr. 2010.

[24] W. Niancheng, Y. Xiaojing and B. Yu, "A new recognition method of RS codes," Journal of Electronic Warfare Technology, vol. 2, no. 1, pp. 36-40, Feb. 2011.

[25] S. Lin and D.J. Costello, Error control coding: fundamentals and applications, second edition, Prentice Hall: Englewood Cliffs, NJ, 2004.

[26] A. Papoulis, Probability, random variables, and stochastic processes, New York: McGraw Hill, 1965.

[27] M. Barkat, Signal detection and estimation, second edition, Norwood, MA: Artech House Inc, 2005.