بسم الله الرحمن الرحیم

دانشگاه جامع امام حسین (ع)
دانشکده و پژوهشکده جنگ الکترونیک و دفاع سایبری

امام خامنه‌ای (مدظله‌العالی):

دفاع الکترونیک برای ما خیلی مهم است؛ روی مسائل الکترونیک کار کنید.

۱۳۸۸/۱۱/۳۰

مجله علمی- پژوهشی

پدافند الکترونیکی و سایبری

ویژه نامه کنفرانس بین المللی ترکیبیات، رمزنگاری و محاسبات، سال ۱۳۹۵، شاپا: ۴۳۴۷-۲۳۲۲

صاحب امتیاز: دانشگاه جامع امام حسین (علیه السلام)

مدیر مسئول: دکتر علیرضا صادقی

سردبیر: دکتر عبدالرسول میرقدری

مدیر اجرایی: سعید زردار

- دارای رتبه علمی- پژوهشی بر اساس نامه شماره ۳/۸۵۵۹۵ مورخ ۹۲/۶/۱۲ از وزارت علوم، تحقیقات و فناوری
- دارای پروانه انتشار به شمارهٔ ۹۱/۲۷۷۶۲ مورخ ۹۱/۹/۲۰ از وزارت فرهنگ و ارشاد اسلامی
- چاپخانه: خیابان لاله‌زار نو، بن‌بست فاخته، پلاک ۵، چاپ هدف
- کارشناس: مهندس عزیزاله طبرزدی
- صفحه‌آرا: مهندس مهربان اسماعیل زاده
- ویراستار ادبی: سعید زردار
- قیمت: ۱۰۰،۰۰۰ ریال

این مجله در پایگاه‌های زیر نمایه می‌شود:

پایگاه استنادی علوم جهان اسلام ((ISC) www.isc.gov.ir)
مرکز اطلاعات و مدارک علمی ایران (www.irandoc.ac.ir)
بانک اطلاعات نشریات علمی کشور (www.magiran.com)
پایگاه علمی جهاد دانشگاهی (www.SID.ir)
پایگاه مجلات تخصصی نور (www.noormags.ir)

این مجله به‌صورت فصلنامه توسط دانشکده و پژوهشکده جنگ الکترونیک و دفاع سایبری منتشر می‌گردد.

نشانی: تهران، بزرگراه شهید بابایی، دانشگاه جامع امام حسین (ع)، موقعیت امام صادق (ع)، ساختمان باقرالعلوم (ع)، دایره نشریات،
دفتر مجله پدافند الکترونیکی و سایبری صندوق پستی: ۱۸۷-۱۶۵۳۵ تلفن: ۷۳۸۲۹۲۰۰ نمابر: ۷۳۸۲۹۱۳۹

http://ecdj.ihu.ac.ir **Email: ecdjournal@ihu.ac.ir**

از نگارندگان گرامی تقاضا می‌شود مقاله خود را مطابق راهنمای تدوین مقالات مجله ((پدافند الکترونیکی و سایبری)) تهیه و ارسال نمایند:

الف) نحوه ارسال:

۱. ابتدا به پایگاه مجله "www.ecdj.ihu.ac.ir" مراجعه و ثبت‌نام نموده و پس از دریافت کد کاربری و رمز عبور، اقدام به بارگذاری مقاله خود نمایند.

۲. مقاله ارسال شده، نباید در هیچ مجله داخلی و یا خارجی چاپ شده باشد و در حین داوری توسط این مجله، نباید برای مجله دیگری ارسال شود.

۳. ارائه آدرس رایانامه و شماره تلفن همراه تمام نویسندگان و معرفی ۵ داور متخصص پیشنهادی در هنگام بارگذاری مقاله الزامی است.

ب) نحوه نگارش:

۱.مقاله مطابق با قالب مجله از نظر نوع، فونت، سایز قلم، درج شکل‌ها و ... باید به زبان فارسی و با استفاده از نرم‌افزار Word حداقل در ۸ و حداکثر در ۱۵صفحه به‌صورت دو ستونی با عرض هر ستون ۷٫۵cm و حاشیه‌ها از هر طرف ۲٫۵cm تهیه شود.

۲. صفحه نخست مقاله باید شامل عنوان مقاله، نام نویسنده‌ها، چکیده و واژه‌های کلیدی در دو بخش فارسی و لاتین، به‌صورت تک ستونی باشد.

۳. متن اصلی مقاله باید حداقل شامل بخش‌های مقدمه، متن اصلی، نتیجه‌گیری و مراجع باشد.

۴. شماره مرجع مورد استفاده به ترتیب و در کنار متن مربوطه داخل کروشه آورده شود (مثال [۲]).

۵. اشکال و نمودارها باید کیفیت مطلوب داشته باشد. اندازه قلم و شکل‌ها باید به گونه‌ای انتخاب شود که در چاپ سیاه و سفید مجله، خوانا و مشخص باشد.

۶. عنوان جدول‌ها در بالای آن‌ها و نام شکل‌ها در زیر آن‌ها به‌صورت وسط‌چین شماره‌گذاری شود.

۸. مرتبه علمی یا عنوان شغل نویسندگان مقاله و محل انجام تحقیق همچنین کلمات و عبارات لاتین(غیر از اختصارات) باید در پاورقی آورده شوند.

ج) نام، اندازه قلم و محتوی مقاله مطابق جدول انتخاب شوند:

صفحه اول مقاله		نام قلم	اندازه قلم
عنوان مقاله (حداکثر۱۵ کلمه، وسط‌چین)	بخش فارسی	B Titr	۱۴
نام نویسنده‌ها (نویسنده مسئول با ستاره مشخص شود)		B Lotus Bold	۱۲
محل انجام تحقیق، مرتبه علمی یا عنوان شغلی		B Lotus	۱۰
چکیده (حداکثر ۱۰ خط، تک ستونی)		B Nazanin	۱۱
واژه‌های کلیدی (حداکثر۶ کلمه)		B Nazanin Bold	۱۱
عنوان مقاله (حداکثر۱۵ کلمه، وسط‌چین)	بخش لاتین	Times New Roman Bold	۱۴
نام نویسنده‌ها (نویسنده مسئول با ستاره مشخص شود)		Times New Roman Bold	۱۰
محل انجام تحقیق		Times New Roman	۹
چکیده (تک ستونی)		Times New Roman Italic	۱۰
واژه‌های کلیدی (حداکثر۶ کلمه)		Times New Roman	۱۰
رایانامه نویسنده مسئول (به صورت پاورقی)		Times New Roman	۸
متن مقاله		**نام قلم**	**اندازه قلم**
متن مقاله دو ستونی (Single Space)		B Nazanin	۱۱
کلمه‌های انگلیسی داخل متن		Times New Roman	۹
عنوان بخش‌ها (مثال: ۳.)		B Nazanin Bold	۱۳
عنوان زیر بخش‌ها (مثال: ۱،۳.)		B Nazanin Bold	۱۲
شماره جدول‌ها و شکل‌ها (وسط چین)		B Nazanin Bold	۱۰
توضیحات جدول‌ها و شکل‌ها		B Nazanin	۱۰

د) مراجع در پایان مقاله و در بخش مراجع به صورت زیر و با فونت Times New Roman-8 **ارائه شوند:**

۱. مراجع فارسی به لاتین ترجمه شده و در انتهای مرجع، اصطلاح (in Persian) ذکر گردد.

۲. مقاله‌های چاپ‌شده در مجلات:

[1] G. Hsin Lai, Ch. Chen, B. Chiang Jeng, and W. Chao, "Ant-based IP traceback," Expert Systems with Applications vol. 34 pp. 3071-3080, 2008.

۳. مقاله‌های ارائه‌شده در کنفرانس‌ها:

[1] H. Zeidanloo and J. M. Zadeh,"A Taxonomy of Botnet Detection Techniques", 3rd IEEE Conference paper , 2010.

۴. کتاب‌ها:

[1] J. Padhye, V. Firoiu, and D. Towsley, "A stochastic model of TCP Reno congestion avoidance and control," Univ. of Massachusetts, Amherst, MA, CMPSCI Tech. Rep. 99-02, 1999.

۵. گزارش‌های ثبت اختراع (پتنت):

[1] R. E. Sorace, V. S. Reinhardt, and S. A. Vaughn, "High-speed digital-to-RF converter," U.S. Patent 5 668 842, Sept. 16, 1997.

۶. پایان‌نامه‌ها:

[1] R. T. Enander, "Lead Particulate and Methylene Chloride Risks in Automotive Refinishing" Ph.D. Thesis, Tufts Univ ,Medford, MA, 2001.

۷. پایگاه‌های اینترنتی:

[1] OWASP, "Risk Rating Methodology" http://www.owasp.org, 2009.

فهرست مقالات ..... صفحه

محورهای فعالیت مجله

دانشکده و پژوهشکده جنگ الکترونیک و دفاع سایبری دانشگاه جامع امام حسین(ع) به‌منظور نشر

دانش تخصصی و کمک به رشد، توسعه و تعمیق سطح دانش در محورهای زیر، اقدام به انتشار

مجله علمی- پژوهشی «پدافند الکترونیکی و سایبری» به‌صورت فصلنامه نموده است.

۱- ترکیبیات (گراف- کد- طرح های ترکیبیاتی-درخت ها- مربع های لاتین- مشبکه ها)

۲- رمزنگاری (مبانی ریاضی رمزنگاری - طراحی و تحلیل انواع رمزهای متقارن و نامتقارن - تحلیل سامانه‌های رمز - نهان‌نگاری - نهان‌کاوی - توابع چکیده ساز - پروتکل‌های رمز نگاری - امنیت - مدیریت کلید)

۳- محاسبات (محاسبات عددی - محاسبات ابری - محاسبات کوانتومی - محاسبات تصادفی - محاسبات فازی - محاسبات الگوریتمی - پیچیدگی محاسبات)

۴- امنیت اطلاعات، پنهان‌نگاری، پروتکل‌ها و استانداردها

۵- ردیابی، مکان‌یابی، آشکارسازی و شنود سیگنال

۶- مدل‌سازی و شبیه‌سازی

۷- پردازش سیگنال حوزه‌های مرتبط

کلیه اساتید، پژوهشگران و دانشجویان می‌توانند مقالات خود را که در هیچ مجله‌ای چاپ نشده باشد، با فرمت مشخص شده به نشانی http://ecdj.ihu.ac.ir در پایگاه مجله بارگذاری نمایند.

مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"
ویژه‌نامه کنفرانس بین‌المللی ترکیبیات، رمزنگاری و محاسبات، ص ۴ -۱

ساختن توابع *APN* جدید

مهدی علائیان[1*]، سید محمدکاظم حسینی‌پور[2]

۱- استاد، دانشگاه علم و صنعت ایران، ۲- مدرس دانشگاه علم و صنعت ایران

(دریافت: ۹۵/۰۷/۰۵، پذیرش: ۹۶/۰۳/۰۱)

چکیده

تابع F از $\mathbb{F}_{2^n}$ به خودش که n یک عدد صحیح مثبت است تقریباً ناخطی تام (APN) نامیده می‌شود، هرگاه برای هر $a \neq 0$ و هر b از $\mathbb{F}_{2^n}$ معادله $F(x+a)+F(x)=b$ حداکثر دو جواب در $\mathbb{F}_{2^n}$ داشته باشد. در این مقاله یک تابع APN جدید روی $\mathbb{F}_{2^n}$ که n یک عدد صحیح زوج است را معرفی می‌کنیم.

واژه‌های کلیدی: تقریباً خم، تقریباً ناخطی تام، یکنواختی تفاضل، جعبه‌های جانشینی

۱- مقدمه

در این مقاله n را همواره یک عدد صحیح مثبت در نظر می‌گیریم.

فرض کنیم $F:\mathbb{F}_2^n \to \mathbb{F}_2^n$. در این صورت F را می‌توان به‌طور یکتا به‌صورت:

$$F(x_1,x_2,\dots,x_n)=\sum_{i=1}^{n} c(u)\prod_{i=1}^{n} x_i^{u_i},$$

نمایش داد که در آن $c(u)\in\mathbb{F}_2^n$. این نمایش را فرم نرمال جبری F گویند. درجه جبری F که آن‌را با $d^0(F)$ نشان می‌دهیم عبارت است از درجه فرم نرمال جبری آن، یعنی:

$$d^0(F)=\sum_{x\in\mathbb{F}_2^n} u=(u_1,u_2,\dots u_n)\in\mathbb{F}_2^n, c(u)\neq 0\}.$$

تابع $F:\mathbb{F}_2^n \to \mathbb{F}_2^n$ را خطی[1]، آفین[2] یا کوادراتیک[3] گویند هرگاه به ترتیب دارای درجه جبری یک، حداکثر یک و حداکثر دو باشد. توجه داشته باشید که میدان $\mathbb{F}_{2^n}$ به عنوان فضای برداری با $\mathbb{F}_2^n$ یک‌ریخت است. لذا هر تابع از $\mathbb{F}_2^n$ به خودش را می‌توان به‌عنوان تابعی از $\mathbb{F}_{2^n}$ به $\mathbb{F}_{2^n}$ درنظر گرفت. هر تابع مانند F از $\mathbb{F}_{2^n}$ به خودش یک نمایش یکتا به‌صورت یک چندجمله‌ای[4] از درجه حداکثر 2^n-1 روی $\mathbb{F}_{2^n}$ مانند

$$F(x)=\sum_{i=1}^{2^n-1} c_i x^i,\ \ c_i\in\mathbb{F}_{2^n} \qquad (۱)$$

دارد. برای هر $0\le k\le n$ تعداد ضرایب ناصفر $k_s\in\{0,1\}$ در بسط دودویی $k=\sum_{i=1}^{n-1} k_s 2^s$ را -2 وزن k نامیده و آن‌را با $w_2(k)$ نشان می‌دهیم. درجه جبری F برابر است با بیشینه -2 وزن توان‌های i از چندجمله‌ای $F(x)$ به‌طوری‌که $c_i\neq 0$، یعنی $d^0(F)=max_{0\le i\le n-1, c_i\neq 0} w_2(i)$ [۱۱]. بنابراین، اگر F خطی باشد، آن‌گاه نمایش آن به فرم (۱) عبارت است از $F(x)=\sum_{i=1}^{n-1} c_i x^{2^i}$ و اگر آفین باشد نمایشی به‌صورت $F(x)=c+\sum_{i=1}^{n-1} c_i x^{2^i}$ دارد و درصورتی‌که کوادراتیک باشد می‌توان آن‌را به‌صورت:

$$F(x)=\ c+\sum_{i=1}^{n-1} c_i x^{2^i}+\sum_{0\le j<k<n} d_{kj} x^{2^k+2^j},$$

نوشت.

برای تابع $F:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$ مجموعه جواب‌های معادله:

$$F(x+a)+F(x)=b \qquad (۲)$$

در $\mathbb{F}_{2^n}$ را که $a,b\in\mathbb{F}_{2^n}$ با $\delta_F(a,b)$ نشان می‌دهیم، یعنی:

$$\delta_F(a,b)=\{x\in\mathbb{F}_{2^n}: F(x+a)+F(x)=b\}.$$

تابع $F:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$ را δ_F-یکنواخت تفاضلی گوییم هرگاه:

$$\delta_F=\max_{a\in\mathbb{F}_{2^n}^*, b\in\mathbb{F}_{2^n}} |\delta_F(a,b)|,$$

و اگر $\delta_F=2$، آن‌گاه F تقریباً ناخطی تام یا APN نامیده می‌شود. توجه داشته باشید که $\delta_F\ge 2$ زیرا a و 0 هر دو جواب‌های معادله *(2)* به ازای $b=F(0)+F(a)$ در $\mathbb{F}_{2^n}$ اند. به‌علاوه، δ_F همواره زوج است زیرا اگر x جواب معادله (۲) باشد،

* رایانامه نویسنده مسئول: alaeiyan@iust.ac.ir

1- Linear
2- Affine
3- Quadratic

آن‌گاه $x+a$ نیز جوابی از این معادله است.

برهان: برای اعداد صحیح و مثبت δ تابع F از $\mathbb{F}_{2^n}$ به خودش به‌طور تفاضلی δ-یکنواخت نامیده می‌شود هرگاه برای هر $a \neq 0$ و b از $\mathbb{F}_{2^n}$ معادله $F(x+a)=F(x)=b$ حداکثر δ جواب در $\mathbb{F}_{2^n}$ داشته باشد. توابع روی $\mathbb{F}_{2^n}$ که به‌عنوان $s-box$ در رمزهای بلوکی استفاده می‌شوند باید دارای یک‌نواختی تفاضلی پایینی باشند تا در برابر حملات تفاضلی امنیت بیش‌تری داشته باشند [۱]. از این جهت توابع 2-یکنواخت تفاضلی بهینه‌اند زیرا برای هر تابع روی $\mathbb{F}_{2^n}$ داریم: $\delta \geq 2$.

برای هر تابع $F: \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ قرار می‌دهیم:

$$\lambda_F(a+b) = \sum(-1)^{tr(bF(x)+ax)}, a, b \in \mathbb{F}_{2^n},$$

که $tr(x) = x + x^2 + \cdots + x^{2^{n-1}}$ تابع اثر از $\mathbb{F}_{2^n}$ به $\mathbb{F}_2$ است. مجموعه $\{\lambda_F(a,b) | a, b \in \mathbb{F}_{2^n}, b \neq 0\}$ طیف والش F نامیده می شود.

اگر طیف والش F مساوی $\left\{0, \pm 2^{\frac{n+1}{2}}\right\}$ باشد، آن‌گاه تابع تقریباً خم[1] (AB) نامیده می‌شود. بنابراین، توابع AB فقط برای n های فرد موجودند. این توابع بیشترین امنیت را در برابر حملات خطی دارند [۱۰] . هر تابع AB، APN نیز هست [۹] و برای nهای فرد هر تابع کوادراتیک APN است اگر و تنها اگر AB باشد [۸] . یک بررسی جامع از توابع APN و AB را می توان در [۷] یافت. اخیراً چند خانواده از توابع APN کوادراتیک ساخته شده است [۲-۵]. در [۶] یک روش برای ساختن توابع APN کوادراتیک با استفاده از یک تابع APN شناخته‌شده در قالب قضیه زیر ارائه شده است:

قضیه ۱-۱- فرض کنیم F یک تابع APN کوادراتیک از $\mathbb{F}_{2^n}$ به خودش و f یک تابع بولی کوادراتیک روی $\mathbb{F}_{2^n}$ باشد. همچنین فرض کنیم:

$$\varphi_F(x,a) = F(x+a) + F(x) + F(o) + F(a),$$
$$\varphi_f(x,a) = f(x+a) + f(x) + f(o) + f(a).$$

در این صورت، اگر برای هر $a \neq 0$ از $\mathbb{F}_{2^n}$ تابع بولی خطی l_a که در شرایط زیر صدق می‌کند

$$l_a(\varphi_F(x,a)) = \varphi_f(x,a). \qquad (1)$$

(۲) اگر برای $x \in \mathbb{F}_{2^n}$ داشته باشیم $\varphi_F(x,a) = 1$، آن‌گاه $l_a(1) = 0$، آن‌گاه $F(x)+f(x)$ تابعی APN است.

در بخش دوم این مقاله با استفاده از این قضیه و تابع APN کوادراتیک $F(x) = x^3$ یک تابع APN روی $\mathbb{F}_{2^n}$ که n عددی زوج است را می‌سازیم و در بخش سوم نتیجه‌گیری مختصری ارائه می‌گردد.

۲- ساختن توابع APN کوادراتیک جدید

گزاره ۲-۱- اگر $F: F_{2^n} \to F_{2^n}$ یک تابع کوادراتیک باشد و $a \in F_{2^n}^*$، آن‌گاه برای هر $b \in F_{2^n}$ داریم:

$$|\delta_F(a,b)| = |\delta_F(a, F(a)+F(0))|.$$

برهان: چون F کوادراتیک است، پس دارای نمایشی به صورت:

$$F(x) = c + \sum_{i=0}^{2^n-1} c_i x^{2^i} + \sum_{0 \leq i<k<n} d_{kj} x^{2^k+2^j},$$

است. تابع $G: \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ را با ضابطه:

$$G(x) = \sum_{0 \leq j<k<n} d_{jk}(x^{2^k}a^{2^j} + x^{2^j}a^{2^k}),$$

تعریف می کنیم. اگر $\mathbb{F}_{2^n}$ را به‌عنوان فضای برداری روی $\mathbb{F}_2$ در نظر بگیریم، آن‌گاه G یک تبدیل خطی است زیرا برای هر $x, y \in \mathbb{F}_{2^n}$،

$$G(x+y) = \sum_{0 \leq j<k<n} d_{jk}((x+y)^{2^j}a^{2^k} + (x+y)^{2^k}a^{2^j}),$$

$$= \sum_{0 \leq i<j<n} d_{jk}(x^{2^j}a^{2^k} + y^{2^j}a^{2^k} + x^{2^k}a^{2^j} + y^{2^k}a^{2^j}),$$

$$= \sum_{0 \leq j<k<n} d_{jk}(x^{2^j}a^{2^k} + x^{2^k}a^{2^j}) + \sum_{0 \leq j<k<n} d_{jk}(y^{2^j}a^{2^k} + y^{2^k}a^{2^j}),$$

$$= G(x) + G(y),$$

و $G(0) = 0$. حال فرض کنیم برای $a \in \mathbb{F}_{2^n}^*$ و $b \in \mathbb{F}_{2^n}$، x جوابی از معادله $F(x+a) = F(x) = b$ باشد. چون:

$$F(x+a) = c + \sum_{i=0}^{n-1}(x+a)^{2^i} + \sum_{0 \leq j<k<n} d_{jk}(x+a)^{2^j+2^k},$$
$$= c + \sum_{i=0}^{n-1} x^{2^i} + \sum_{i=0}^{n-1} a^{2^i} + \sum_{0 \leq j<k<n} d_{jk}[(x^{2^j} + a^{2^j})(x^{2^k} + a^{2^k})],$$
$$= c + \sum_{i=0}^{n-1} x^{2^i} + \sum_{i=0}^{n-1} a^{2^i} + \sum_{0 \leq j<k<n} d_{jk}x^{2^j+2^k} + \sum_{0 \leq j<k<n} d_{jk}a^{2^j+2^k} + \sum_{0 \leq j<k<n} d_{jk}(x^{2^j}a^{2^k} + x^{2^k}a^{2^j}),$$

$$= F(x) + F(0) + F(a) + G(x).$$

پس داریم:

$$G(x) + F(0) + F(a) = b$$

و در نتیجه:

$$G(x) = F(0) + F(a) + b.$$

بنابراین:

1- almost bent

$$\delta_F(a,b) = G^{-1}(F(0)+F(a)+b). \quad (۳)$$

از این‌رو:

$$\delta_F(a,F(0)+F(a)) = G^{-1}(0) = kerG.$$

از طرفی داریم:

$$|Ker\ G| = |G^{-1}(F(0)+F(a)+b)|.$$

لذا بنابر رابطه (۳):

$$|\delta_F(a,b)| = |\delta_F(a,F(0)+F(a))|.$$

نتیجه ۲-۲: فرض کنیم $F:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$ تابعی کوادراتیک باشد. در این صورت، F تابعی APN است هرگاه برای هر $a\in\mathbb{F}_{2^n}$ معادله $F(x)+F(x+a)=F(0)+F(a)$ دو جواب در $\mathbb{F}_{2^n}$ داشته باشد.

فرض کنیم F تابعی کوادراتیک و APN از $\mathbb{F}_{2^n}$ به خودش باشد و $a\in\mathbb{F}_{2^n}^*$. هم‌چنین فرض کنیم:
$L=\{\varphi_F(x,a)|x\in\mathbb{F}_{2^n}\}.$

چون F کوادراتیک است دارای نمایشی به صورت:

$$F(x)=c+\sum_{i=0}^{2^n-1}c_ix^{2^i}+\sum_{0\le i<k<n}d_{kj}x^{2^k+2^j},$$

است که $c,a_i,d_{jk}\in\mathbb{F}_{2^n}$. تابع $G:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$ را با ضابطه:

$$G(x)=\sum_{0\le j<k<n}d_{jk}(x^{2^k}a^{2^j}+x^{2^j}a^{2^k}),$$

تعریف می‌کنیم. همان‌طورکه در برهان گزاره ۲-۱ مشاهده کردید G خطی است و برای هر $x\in\mathbb{F}_{2^n}$ داریم:

$$F(x+a)=F(x)+F(0)+F(a)+G(x).$$

پس برای هر $x,y\in\mathbb{F}_{2^n}$:

$$\varphi_F(x+y,a)=F(x+y+a)+F(x+y)+F(a)+F(0),$$

$$=(F(x+y)+F(0)+F(a)+G(x+y))+F(x+y)+F(a)+F(0),$$

$$=G(x+y),$$

$$=G(x)+G(y).$$

از طرفی داریم:

$$\varphi_F(x,a)+\varphi_F(y,a)=F(x+a)+F(x)+F(a)+F(0)+F(y+a)+F(y)+F(a)+F(0),$$

$$=F(x+a)+F(x)+F(y+a)+F(y),$$

$$=(F(x)+F(0)+F(a)+G(x))+F(x)+(F(y)+F(0)+F(a)+G(y))+F(y),$$

$$=G(x)+G(y).$$

از این‌رو:

$$\varphi_F(x+y,a)=\varphi_F(x,a)+\varphi_F(y,a). \quad (۴)$$

لذا L زیرفضای $\mathbb{F}_{2^n}$ است. چون f نیز کوادراتیک است، داریم:

$$\varphi_f(x+y,a)=\varphi_f(x,a)+\varphi_f(y,a).$$

اینک تابع $l_a:L\to\mathbb{F}_{2^n}$ را با ضابطه:

$$l_a(\varphi_F(x,a))=\varphi_f(x,a)$$

تعریف می‌کنیم. این تابع خوش تعریف است زیرا اگر برای $x,y\in\mathbb{F}_{2^n}$ داشته باشیم $\varphi_F(x,a)=\varphi_F(y,a)$، آن‌گاه $\varphi_F(x,a)+\varphi_F(y,a)=0$ و در نتیجه بنابر رابطه (۴)، $\varphi_F(x+y,a)=0$. اما چون F تابعی APN است، از این تساوی نتیجه می‌شود که $x+y=0$ یا $x+y=a$. اگر $x+y=0$، آن‌گاه $x=y$ و در نتیجه $\varphi_f(x,a)=\varphi_f(y,a)$ و اگر $x+y=a$، آن‌گاه $y=x+a$ و لذا:

$$\varphi_f(y,a)=\varphi_f(x+a,a)=f(x+a+a)+f(x+a)+f(a)+f(0),$$

$$=f(x)+f(x+a)+f(a)+f(0),$$

$$=\varphi_f(x,a).$$

پس داریم $l_a(\varphi_F(x,a))=l_a(\varphi_F(y,a))$. لذا l_a خوش تعریف است. بعلاوه برای هر $x,y\in\mathbb{F}_{2^n}$:

$$l_a(\varphi_F(x,a)+\varphi_F(y,a))=l_a(\varphi_F(x+y,a)),$$

$$=\varphi_f(x+y,a),$$

$$=\varphi_f(x,a)+\varphi_f(y,a),$$

$$=l_a(\varphi_F(x,a))+l_a(\varphi_F(y,a)).$$

پس خطی است. علاوه بر این، l_a را می‌توان به یک تابع خطی از $\mathbb{F}_{2^n}$ به $\mathbb{F}_2$ توسعه داد. لذا همواره تابع $l_a:\mathbb{F}_{2^n}\to\mathbb{F}_2$ موجود است که شرط (۲) قضیه ۱-۱ را بر آورده می‌کند.

قضیه ۲-۳- فرض کنیم n یک عدد صحیح مثبت و زوج باشد. دراین صورت تابع $f(x)=tr(x^9+x^3)$ روی $\mathbb{F}_{2^n}$، APN است.

برهان: فرض کنیم $F(x)=x^3$ و $f(x)=tr(x^9+x^3)$. در این

صورت، F یک تابع APN کوتدراتیک و f یک تابع بولی کوتدراتیک خطی است و داریم $\varphi_F(x,a)=a^2x+ax^2$ و $\varphi_f(x,a)=tr(a^8x+ax^8+ax^2+a^2x)$. برای هر عضو ناصفر a از $\mathbb{F}_{2^n}$ تابع بولی خطی l_a را به صورت زیر در نظر می‌گیرم:

$$l_a(y)=tr(a^6y+a^3y^2+a^{-3}y^4+y)$$

از این‌رو:

$$l_a(\varphi_F(x,a))=tr(a^6(a^2x+ax^2)+a^3(a^4x^2+a^2x^4)+a^{-3}(a^8x^4+a^4x^8)+a^2x+ax^2$$
$$=tr(a^8x+ax^8+a^2x+ax^2)$$
$$=\varphi_f(x,a).$$

اینک فرض کنیم وجود داشته باشد $x\in\mathbb{F}_{2^n}$ به‌طوری‌که $\varphi_F(x,a)=1$. در این صورت:

$$l_a(1)=tr(a^6+a^3+a^{-3}+1)=tr(a^{-3}+1)$$
$$=tr(a^{-3})+tr(1).$$

چون n زوج است، $tr(1)=0$. از این‌رو:

$$l_a(1)=tr(a^{-3})$$
$$=tr(\frac{a^2x+ax^2}{a^{-3}})$$
$$=tr\left(\left(\frac{x}{a}\right)+\left(\frac{x}{a}\right)^2\right)=0.$$

لذا به موجب قضیه ۱-۱، $x^3+tr(x^9+x^3)$ تابعی APN است.

۳- نتیجه‌گیری

توابع APN بیشترین امنیت را در برابر حملات تفاضلی دارا هستند. چندین روش برای ساختن توابع APN ارائه شده است. یکی از این روش‌ها در قالب قضیه ۱-۱ در بخش اول این مقاله معرفی شد. در این مقاله با استفاده از این روش تابع APN کوادراتیک $x^3+tr(x^9+x^3)$ روی $\mathbb{F}_{2^n}$ که n عددی صحیح و زوج است ساخته شد.

۴- مراجع

[1] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," J. Cryptology, vol. 4, no. 1, pp. 3-72, 1991.

[2] C. Bracken, E. Byrne, N. Markin, and G. McGuire, "New families of quadratic almost perfect nonlinear trinomials and multinomials," Finite Fields Appl., vol. 14, pp. 703–714, 2008.

[3] C. Bracken, E. Byrne, N. Markin, and G. McGuire, "A few more quadratic APN functions," preprint, 2008.Available at http:// www.arxiv.org/abs/0804.4799.

[4] L. Budaghyan and C. Carlet, "Classes of quadratic APN trinomials and hexanomials and related structures," IEEE Trans. Inform. Theory, vol. 54, no. 5, pp. 2354–2357, 2008.

[5] L. Budaghyan, C. Carlet, and G. Leander, "Two classes of quadratic APN binomials inequivalent to power functions," IEEE Trans. Inform. Theory, vol. 54, no. 9, pp. 4218–4229, 2008.

[6] L. Budaghyan, C. Carlet, and G. Leander, "Constructing new APN functions from known ones," Finite Fields and Their Applications, vol. 15, issue 2, pp. 150-159, 2009.

[7] C. Carlet, "Vectorial boolean functions for cryptography," chapter of the monography Boolean Methods and Models, Y. Crama, P. Hammer (Eds.), Cambridge Univ. Press, in press.

[8] C. Carlet, P. Charpin, and V. Zinoviev, "Codes, bent functions and permutations suitable for DES-like cryptosystems," Des. Codes Cryptogr., vol. 15, no. 2, pp. 125–156, 1998.

[9] F. Chabaud and S. Vaudenay, "Links between differential and linear cryptanalysis," in: Advances in Cryptology EUROCRYPT'94, in: Lecture Notes in Comput. Sci., vol. 950, Springer-Verlag, New York, pp. 356–365, 1995.

[10] M. Matsui, "Linear cryptanalysis method for DES cipher," in: Advances in Cryptology EUROCRYPT'93, in: Lecture Notes in Comput. Sci., Springer-Verlag, pp. 386–397, 1994.

مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"
ویژه‌نامه کنفرانس بین‌المللی ترکیبیات، رمزنگاری و محاسبات، ص ۱۱ -۵

کران‌های جدیدی بر روی نسبت اطلاعات ضرب دکارتی کلاس‌هایی از گراف‌ها

عباس چراغی[۱*]، محمد غلامی[۲]

۱- استادیار، گروه ریاضی، دانشکده ریاضی و کامپیوتر خوانسار ۲- دانشیار، دانشکده علوم ریاضی، دانشگاه شهرکرد، پژوهشگاه دانش‌های بنیادین
(دریافت: ۹۵/۰۷/۰۵، پذیرش: ۹۶/۰۳/۰۷)

چکیده

در این مقاله، کران پایینی برای نسبت اطلاعات حاصل‌ضرب دکارتی یک درخت دلخواه با قطر حداقل ۳ و دور C_m برای هر $m \geq 3$ خواهیم یافت. علاوه براین، بهترین نسبت اطلاعات طرح تسهیم راز کامل برپایه گراف C_6^d را تعیین می‌کنیم که در آن، C_6^d گراف حاصل از ضرب دکارتی دور به طول ۶ با گراف d- مکعب است. به طور دقیق‌تر، نشان داده می‌شود که برای هر $d \geq 1$، نسبت اطلاعات C_6^d دقیقاً برابر با $\frac{d(d+3)+3}{2(d+1)}$ است.

واژه‌های کلیدی: طرح تسهیم راز، نسبت اطلاعات، حاصل‌ضرب دکارتی

۱- مقدمه

طرح تسهیم راز، روشی برای توزیع اطلاعات در میان مجموعه‌ای از سهام‌داران است، به‌طوری‌که تنها مجموعه‌های مجاز قادر به کشف راز باشند. راه‌کار اصلی تسهیم راز این است که داده محرمانه (راز) به بخش‌هایی تقسیم شود، به‌گونه‌ای که با زیرگروه‌های خاصی از این بخش‌ها، بتوان راز را بازیابی‌کرد. اگر علاوه بر این، مجموعه‌های غیرمجاز دارای هیچ اطلاعات اضافی در مورد راز نباشند، یعنی سهم‌های آنان به طور آماری از راز مستقل باشد، در این صورت طرح (تسهیم راز) کامل نامیده می‌شود. توصیف مجموعه‌های مجاز در میان تمامی زیرمجموعه‌های ممکن از سهام‌داران یک ساختار دسترسی نامیده می‌شود. Shamir [۱] و Blakley [۲] در ابتدا مساله طرح تسهیم راز را مطرح کرده و طرح‌های تسهیم رازی را ارائه دادند که هر زیرمجموعه A از سهام‌داران با اندازه $|A| \geq k$ قادر به بازسازی راز هستند و هر زیرمجموعه A از سهام‌داران با اندازه $|A| < k$ هیچ اطلاعاتی درباره راز به‌دست نیاورند. این طرح‌ها، (n,k)- طرح‌های آستانه‌ای نامیده می‌شوند، مقدار k آستانه طرح نامیده می‌شود و n تعداد سهام‌داران می‌باشد. سوال اصلی در مورد کارآیی این روش به این صورت است: به ازای هر بیت از راز، چه تعداد بیت از اطلاعات سهام‌داران می‌بایست به خاطر سپرده شود؟

نسبت اطلاعات این طرح، نسبت مابین بیش‌ترین اندازه از سهم‌ها و اندازه مقدار راز است، در حالی‌که نسبت یک ساختار دسترسی، کم‌ترین نسبت اطلاعات طرح‌هایی است که بر روی این ساختار دسترسی شناخته شده‌اند.

یکی از مسائل نظری و عملی در این مقوله، تعیین یا یافتن کران‌های قابل قبول برای نسبت اطلاعات ساختار دسترسی‌های متفاوت است که توسط تعدادی از پژوهشگران، توجه قابل قبولی را به خود منعطف ساخته است.

ارتباط عملی این موضوع برپایه مشاهدات زیر است. در ابتدا، توجه داریم که امنیت هر دستگاهی با افزایش مقدار اطلاعاتی که می‌بایست مخفی نگه داشته شود (یعنی سهم سهام‌داران)، تمایل به کاهش دارد. ثانیاً، اگر سهم‌هایی که به سهام‌داران داده می‌شود، خیلی بزرگ باشد، آن‌گاه حافظه مورد نیاز برای سهام‌داران خیلی بزرگ خواهد شد و در همان لحظه، الگوریتم‌های توزیع سهام ناکارآمد خواهند شد. بنابراین، مهم است بهترین نسبت اطلاعات ساختارهای دسترسی را داشته باشیم. در راستای این هدف، یافتن کران‌های بالایی و پایینی روی نسبت اطلاعات ارزشمند خواهد بود.

حالت خاص، زمانی است که یک ساختار دسترسی توسط یک گراف تعریف شود که در آن مجموعه راس‌ها، همان مجموعه سهام‌داران و یال‌ها، مجموعه‌های مجاز کمینه هستند. در این مقاله، ما ساختارهای دسترسی بر پایه گراف‌ها را مورد مطالعه

* رایانامه نویسنده مسئول: a.cheraghi@khn.ui.ac.ir

قرار خواهیم داد و طرح تسهیم راز برای ساختار دسترسی بر پایه یک گراف را طرح تسهیم راز آن گراف می‌نامیم. در طرح‌های تسهیم راز، مساله یافتن کران روی اندازه سهم‌هایی که به سهام‌داران داده می‌شود یا به طور هم ارز نسبت اطلاعات، یکی از مسائل اساسی در این باره بوده و توجه زیادی را توسط محققین به خود جلب ساخته است.

نسبت اطلاعات برای اغلب گراف‌ها با حداکثر ۶ راس در مراجع [۳-۸] مطرح شده است. درخت‌ها، دارای نسبت اطلاعات $2-\frac{1}{k}$ هستند که در آن، k یک مقدار صحیح است [۹]. هم‌چنین، برای هر d، دسته‌ای از گراف‌های نامتناهی با بیشترین درجه d ساخته شده که نسبت دقیق اطلاعات آنها $\frac{d+1}{2}$ است [۱۰]. برای نمونه، گراف‌های کامل دارای نسبت اطلاعات ۱ هستند، مسیرهای با ۴ راس یا بیش‌تر، همانند دورهای با طول حداقل ۵، دارای نسبت اطلاعات $\frac{3}{2}$ هستند. در مرجع [۱۱]، Csirmazنسبت اطلاعات گراف‌های d-مکعبی را یافته و ثابت کرده است که نسبت اطلاعات این گراف‌ها برابر با $d/2$ می‌باشد.

Brickell و Stinson [۵ و۱۲] چندین کران بالایی و پایینی برای نسبت اطلاعات ساختار دسترسی‌های مبتنی بر گراف‌ها یافته‌اند. Stinson [۱۲] نشان داد که نسبت اطلاعات یک گراف با بیش‌ترین درجه d حداکثر برابر با $\frac{d+1}{2}$ است. Brickell و Davenport [۴] نشان دادند که یک گراف دارای نسبت اطلاعات ۱ است اگر و تنها اگر گراف، دوبخشی کامل باشد. علاوه براین، Blundo در مرجع [۳] یک شکاف در مقادیر نسبت اطلاعات گراف‌ها را نشان داد؛ به طور دقیق‌تر، آن‌ها بر روی این مطلب که توسط Brickell و Davenport [۴] به‌دست آمده بود، تاکید کرده و نشان دادند که اگر گراف G یک گراف کامل دوبخشی نباشد، آن‌گاه هر طرح تسهیم راز برای آن گراف، دارای نسبت اطلاعات حداقل $\frac{3}{2}$ است.

در مرجع [۱۳] طرح‌های بهینه بررسی شده اند و در مرجع [۱۴]، نویسندگان یک $(3,3)$-طرح تسهیم راز آستانه‌ای شبه کوانتومی را طراحی نموده‌اند که فارغ از مولد کوانتومی، راز را با سه قسمت کلاسیک به اشتراک می‌گذارد، به طوری که qubitها در یک پایه کلاسیک اندازه‌گیری شده و ارسال آن‌ها بدون اختلال صورت می‌پذیرد.

طرح‌های تسهیم راز مطرح‌شده در این مقاله همگی کامل هستند. یعنی زیرمجموعه‌های مجاز می‌توانند راز را به‌دست آورند، درحالی‌که زیرمجموعه‌های غیر مجاز با استفاده از سهم‌هایشان نمی‌توانند هیچ‌گونه اطلاعاتی از راز به‌دست آورند.

۲- برخی تعاریف اولیه

فرض کنید Σ یک طرح تسهیم راز با مجموعه P از n سهام‌دار باشد. واسطه $p_0 \notin P$ و $Q = P \cup \{p_0\}$ را در نظر بگیرید. در یک طرح، سهم p_0 را راز درنظر می‌گیریم. s_i را سهم سهام‌دار $i \in Q$ فرض کنید. با توجه به همه $(n+1)$-تایی‌های ممکن $(s_{p_0}, s_1, s_2, ..., s_n)$ از سهم‌ها، نگاشت $\pi_i : E \to E_i$ را برای یک مجموعه مشخص E چنان تعریف می‌کنیم که برای هر $e \in E$ اعضاء $(\pi_i(e))_{i \in Q}$ سهم‌های یک راز باشند. ما فقط نگاشت‌های پوشا را در نظر می‌گیریم، بنابراین، برای هر سهام‌دار $i \in Q$ مجموعه E_i همان مجموعه همه سهم‌های ممکن سهام‌دار i-ام می‌باشد. اگر یک توزیع احتمال در E را درنظر بگیریم، آن‌گاه هر یک از نگاشت‌ها یک توزیع احتمال در E_i القاء می‌کند. بنابراین، می‌توان $H(E_i)$ را به‌عنوان Shannon entropy هر یک از متغیرهای تصادفی در نظر گرفت.

برای هر زیرمجموعه $A = \{i_1, ..., i_r\} \subset Q$، آنتروپی مشترک $H(E_{i_1}, ..., E_{i_r})$ را به صورت $H(A)$ می‌نویسیم و قرارداد مشابهی را برای آنتروپی شرطی قرار می‌دهیم. به‌طور مثال، داریم:

$$H(E_j \mid A) = H(E_j \mid E_{i_1}, ..., E_{i_r})$$

مجموعه Γ را ساختار دسترسی Σ درنظر بگیرید. از آن‌جا که نگاشت‌های π_i طرح تقسیم راز کامل Σ را تعریف می‌کنند، لذا $H(E_{p_0}) > 0$. درضمن اگر $A \in \Gamma$، داریم $H(E_{p_0} \mid A) = 0$. این تساوی بیانگر آن است که تمامی اطلاعات راز توسط یک مجموعه مجاز، مشخص می‌گردد. درحالی‌که اگر $A \notin \Gamma$ داریم:

$$H(E_{p_0} \mid A) = H(E_{p_0})$$

این تساوی بیانگر آن است که یک مجموعه غیرمجاز قادر به برملاکردن حتی یک بیت از اطلاعات راز نمی‌باشد.

به منظور اندازه‌گیری طول سهام هر طرح، از آنتروپی سهام آن طرح استفاده می‌شود. *نرخ* اطلاعات طرح تسهیم راز Σ به صورت $\rho(\Sigma) = \frac{H(E_0)}{\max_{i \in P} H(E_i)}$ تعریف می‌شود. مقدار $R(\Sigma) = 1/\rho(\Sigma)$ را نسبت *اطلاعات* طرح Σ گویند. هر دو مقدار ρ و R را به عنوان ضریب تاثیر یک طرح به کار می‌برند. این پارامترها را

می‌توان برای ارزیابی بهترین راندمان طرح‌های یک ساختار دسترسی مشخص استفاده نمود. نرخ اطلاعات *بهینه* $\rho(\Gamma)$ برای یک ساختار دسترسی Γ را انرخ‌های $\rho(\Sigma)$ روی تمامی طرح‌های Σ تعریف‌شده برای ساختار دسترسی Γ گویند. نسبت اطلاعات بهینه ساختار دسترسی Γ نیز به صورت $R(\Gamma)=1/\rho(\Gamma)$ تعریف می‌شود. در ادامه نسبت اطلاعات برخی ساختارهای دسترسی مبتنی بر ضرب دکارتی چندین گراف محاسبه و یا بر روی آن کران‌هایی معرفی می‌گردد.

۳- نسبت اطلاعات دسته‌ای از گراف‌ها

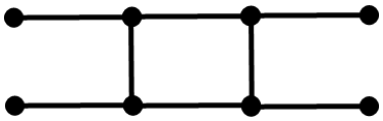
در ادامه به برخی قضایا و نتایج کاربردی در این مقاله می‌پردازیم.

زیرگراف H از گراف G که تنها با حذف زیرمجموعه‌ای از رئوس گراف G به‌دست می‌آید را زیر گراف القایی G گویند.

قضیه ۳-۱- [۱۵] اگر G یک گراف و H زیرگراف القایی آن باشد آن‌گاه:

$$R(H)\le R(G).$$

قضیه ۳-۲- [۱۵] فرض کنید G گراف نردبانی شکل (۱) باشد. آن‌گاه $R(G)=2$.



شکل (۱): گراف نردبانی

در نظریه گراف، حاصل ضرب دکارتی $G\square H$ از گراف‌های G و H گرافی است که مجموعه راس‌های $G\square H$ حاصل‌ضرب دکارتی $V(G)\times V(H)$ بوده و هر دو راس (u,u') و (v,v') مجاور هستند اگر و تنها اگر $u=v$ و u' در H با v' مجاور باشد یا $u'=v'$ و u در G با v مجاور باشد. حاصل‌ضرب دکارتی دارای خاصیت جابه‌جایی است، یعنی گراف‌های $G\square H$ و $H\square G$ به طور طبیعی یک‌ریخت هستند. این عملگر دارای خاصیت شرکت‌پذیری است، یعنی گراف‌های $F\square(G\square H)$ و $(F\square G)\square H$ به طور طبیعی یک‌ریخت هستند.

فرض کنید که T_n یک درخت n راسی باشد. حاصل ضرب دکارتی درخت T_n با یک دور به طول m را با نماد $T_{n,m}$ نمایش می‌دهیم، در واقع $T_{n,m}=T_n\square C_m$.

بیش‌ترین فاصله موجود بین رئوس گراف را قطر گراف گویند.

قضیه ۳-۳- اگر T_n درخت n راسی با قطر حداقل ۳ باشد و $m\ge 4$. آن‌گاه $R(T_{n,m})\ge 2$.

اثبات: برای آن‌که نشان دهیم $R(T_{n,m})\ge 2$ کافی است نشان دهیم $T_{n,m}$ شامل یک زیر گراف القایی یک‌ریخت با گراف شکل (۱) است.

از آن‌جایی که قطر درخت T_n حداقل ۳ است، لذا T_n حداقل شامل یک مسیر القایی به فرم $P: a_1-a_2-a_3-a_4$ می‌باشد. به علاوه فرض کنید دور C_m به فرم $C_m: b_1-b_2-\cdots-b_m-b_1$ باشد. حال بر طبق شکل (۲) برخی رئوس $T_{n,m}$ را به صورت زیر نام‌گذاری می‌نماییم:

$$A=(a_2,b_1)\ ,\ B=(a_2,b_2),$$
$$C=(a_3,b_2)\ ,\ D=(a_4,b_2),$$

$$a=(a_1,b_3)\ ,\ b=(a_2,b_3),$$
$$c=(a_3,b_3)\ ,\ d=(a_3,b_4).$$

اگر $X:=\{A,B,C,D,a,b,c,d\}\subseteq V(T_{n.m})$ آن‌گاه به وضوح زیرگراف القایی $T_{n,m}[X]$ یک‌ریخت با گراف شکل (۱) است، لذا داریم:

$$2=R(T_{n,m}[X])\le R(T_{n,m}).$$

۴- نتایج اصلی

حال، فرض کنید گراف C_n دور به طول n و K_n گراف کامل با n راس باشد. تعریف کنید: $C_n^d=C_n\square K_2\square K_2\square\cdots\square K_2$ جایی که تعداد کپی‌های K_2 در این حاصل‌ضرب برابر با d است. به آسانی می‌توان بررسی کرد که برای هر $n\ge 2$ و $d\ge 0$، گراف C_n^d یک گراف $(d+2)$-منظم راس‌ترایا با $n\times 2^d$ راس است و برای n زوج، گراف C_n^d نیز یک گراف دوبخشی است. هدف اصلی این مقاله، قضیه زیر است که مقدار دقیق نسبت اطلاعات C_6^d را تعیین می‌کند و با $R(C_6^d)$ نمایش داده می‌شود.

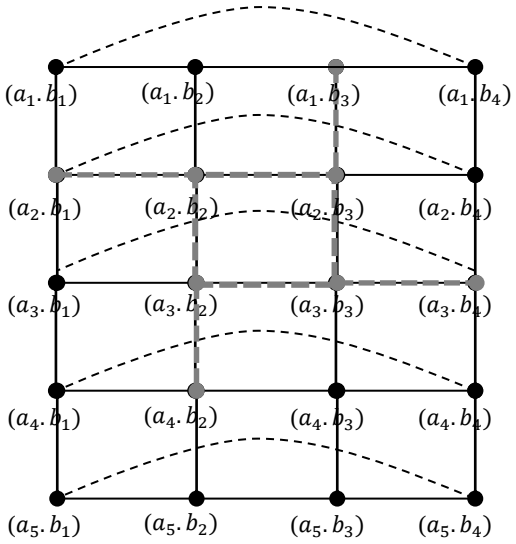
قضیه ۴-۴- برای عدد صحیح نامنفی d، نسبت اطلاعات C_6^d برابر با $\frac{d(d+3)+3}{2(d+1)}$ است.

برای اثبات قضیه فوق نیاز به بیان مطالب زیر است:

یک طرح تسهیم راز کامل S برای گراف G، خانواده‌ای از متغیرهای تصادفی ξ_v برای هر $v\in V(G)$ و متغیر تصادفی ξ برای راز در نظر گرفته می‌شود. بنابراین، اگر uv یالی از G باشد، آن‌گاه ξ_u و ξ_v به همراه یک‌دیگر قادر به تعیین متغیر تصادفی ξ خواهند بود. علاوه بر این، اگر A مجموعه مستقلی

از رئوس باشد، آن‌گاه ξ و مجموعه $\{\xi_v : v \in A\}$ به طور آماری مستقل هستند.

اندازه متغیر تصادفی ξ توسط آنتروپی اندازه‌گیری می‌شود (که محتوای اطلاعاتی نامیده می‌شود) و آن را با نماد $H(\xi)$ نمایش می‌دهند، این روش توسط Blundo در سال ۱۹۹۵ مطرح گردید. نسبت اطلاعات هر راس $v \in V(G)$ برابر با $\frac{H(\xi_v)}{H(\xi)}$ است. این تساوی بیان می‌کند که برای هر بیت راز، چه میزان بیت اطلاعات توسط v به خاطر سپرده می‌شود.



شکل (۲): ضرب دکارتی مسیر با دور

نسبت اطلاعات میانگین و نسبت اطلاعات در بدترین حالت S به ترتیب همان نسبت اطلاعات میانگین در بین تمامی سهام‌داران و بیش‌ترین نسبت اطلاعات در بین آن‌ها است. فرض کنید S یک طرح تسهیم راز کامل روی گراف G باشد، به طوری‌که متغیرهای تصادفی ξ_v برای هر $v \in V(G)$ و متغیر تصادفی ξ برای راز درنظر گرفته می‌شوند. برای هر زیرمجموعه A از رئوس تعریف می‌کنیم:

$$f(A) := \frac{H(\xi_v : v \in A)}{H(\xi)}$$

واضح است که نسبت اطلاعات میانگین S همان میانگین اعضای مجموعه‌ی $\{f(v) : v \in V\}$ می‌باشد. در بدترین حالت، نسبت اطلاعات برابر با بیش‌ترین مقدار در این مجموعه است. با استفاده از خواص استاندارد توابع آنتروپی **[۴]** داریم:

الف) خاصیت مثبت‌بودن: $f(\varnothing) = 0$ و در حالت کلی $f(A) \geq 0$

ب) خاصیت یک‌نوایی: اگر $A \subseteq B \subseteq V(G)$ آنگاه $f(A) \leq f(B)$

ج) خاصیت زیرمدولی:

$$f(A) + f(b) \geq f(A \cap B) + f(A \cup B)$$

یک نتیجه معروف در نظریه اطلاع آن است که اگر ξ و ς دو متغیر تصادفی باشند، متغیر تصادفی ς، مقدار ξ را تعیین می‌کند اگر و تنها اگر $H(\varsigma\xi) = H(\xi)$.

هم‌چنین ξ و ς به طور آماری مستقل هستند اگر:

$$H(\varsigma\xi) = H(\varsigma) + H(\xi).$$

با توجه به این مطلب و تعریف طرح تسهیم راز کامل، خواص زیر را نیز خواهیم داشت:

د) یکنوایی قوی: اگر $A \subseteq B$ همچنین A یک مجموعه مستقل و مجموعه B وابسته باشد، آن‌گاه:

$$f(A) + 1 \leq f(B)$$

ه) زیرمدولی قوی: اگر هیچ‌یک از مجموعه‌های A و B مستقل نباشند، اما $A \cap B$ مستقل باشد، آن‌گاه:

$$f(A) + f(B) \geq 1 + f(A \cap B) + f(A \cup B)$$

- **کران پایین نسبت اطلاعات**

روش‌های معروف آنتروپی که در سال ۱۹۷۹ نشان داده شد، به صورت زیر بیان می‌گردد. به سادگی دیده می‌شود برای هر تابع حقیقی f که در خواص (الف) تا (ه) صدق کرده و مقدار متوسط آن روی مجموعه رئوس G حداقل برابر با r باشد، آن‌گاه، نسبت اطلاعات گراف G حداقل برابر با r خواهد بود **[۳]**.

اثبات قضیه ۴-۴- برای اثبات کران پایین $\frac{d(d+3)+3}{2(d+1)}$ بر روی نسبت اطلاعات C_6^d کافی است نشان دهیم برای هر تابع f با مقدار حقیقی که در خواص (الف) تا (ه) صدق کند، داریم:

$$\sum_{v \in V(C_6^d)} f(v) \geq 3 \times 2^d (d + 2 + \frac{1}{d+1}).$$

این همان نامساوی است که می‌بایست ثابت شود. برای این منظور، مجموعه رئوس گراف C_6^d را به دو قسمت مستقل مجزای A_d و B_d با اندازه یکسان تقسیم می‌کنیم. لذا، داریم:

$$|A_d| = |B_d| = 3 \times 2^d.$$

رئوس A_d فقط همسایه‌هایی در B_d و رئوس در B_d فقط همسایه‌هایی در A_d دارند. گراف $C_6^{d+1} = C_6^d \square K_2$ شامل دو نسخه

مجزا از C_6^d است که مابین رئوس آن‌ها نظیر به نظیر یک تطابق کامل وجود دارد. فرض کنید رئوس هر دونسخه C_6^d به روش فوق به‌ترتیب به‌صورت $A_d \cup B_d$ و $A'_d \cup B'_d$ تقسیم شده باشند، به‌طوری‌که تطابق‌های کامل بین A_d و B'_d و هم‌چنین بین B_d و A'_d باشند. بنابراین، تقسیم رئوس گراف C_6^{d+1} به صورت زیرمجموعه‌های از هم جدای مستقل $A_{d+1} = A_d \cup A'_d$ و $A'_d \cup B'_d$ انجام می‌گردد. با استفاده از این تجزیه، می‌توان از استقرا روی d برای اثبات کران پایین $R(C_6^d)$ استفاده کرد. در مراحل استقرا از نمادگذاری زیر استفاده خواهیم کرد که در آن منظور از bA اجتماع مجموعه A با مجموعه تک‌عضوی b می‌باشد.

$$[[A,B]] = \sum_{b\in B} f(bA) - \sum_{a\in A} f(A-\{a\}).$$

در زمان استفاده از این نام‌گذاری فرض می‌کنیم که مجموعه‌های A و B دارای اندازه‌های یکسان هستند. اکنون، می‌توانیم ثابت کنیم که کران پایین $R(C_6^d)$ برابر با $\frac{d(d+3)+3}{2(d+1)}$ است.

لم ۴-۵- برای هر $d \geq 1$ داریم:

$$R(C_6^d) \geq \frac{d(d+3)+3}{2(d+1)}.$$

اثبات: برای اثبات لم فوق به بیان ادعای زیر نیازمندیم.

ادعا: برای گراف C_6^d با افراز رئوس آن به مجموعه‌های مستقل $A_d \cup B_d$ داریم:

$$\sum_{v\in C_6^d} f(v) \geq [[A_d, B_d]] + 3\times 2^d (d+1+\frac{1}{d+1}) \qquad (۱)$$

اثبات ادعا: برای اثبات ادعا از استقرا روی d استفاده می‌کنیم**.** فرض کنیم نامساوی فوق به ازای $d=1$ برقرار باشد. اکنون با فرض این‌که نامساوی برای هر دو نسخه C_6^d با مجموعه رئوس v_d و v'_d در گراف C_6^{d+1} با مجموعه رئوس V_{d+1}، برقرار باشد، با تقسیم‌بندی رئوس این گراف به فرم $A_{d+1} = A_d \cup A'_d$ و $B_{d+1} = B_d \cup B'_d$ ثابت می‌کنیم حکم برای C_6^{d+1} نیز برقرار است. اکنون بر اساس فرض استقرا بیان شده داریم:

$$\sum_{v\in V_{d+1}} f(v) = \sum_{v\in V_d} f(v) + \sum_{v\in V'_d} f(v) = [[A_d, B_d]] +$$
$$[[A'_d, B'_d]] + 3\times 2^{d+1}(d+1+\frac{1}{d+1}) \qquad (۲)$$

می‌توان نشان داد:

$$[[A_d, B_d]] + [[A'_d, B'_d]] \geq$$
$$[[A_d A'_d, B_d B'_d]] + 6\times 2^d$$

با ترکیب این نامساوی با معادله (۲) داریم:

$$\sum_{v\in C_6^{d+1}} f(v) \geq [[A_d A'_d, B_d B'_d]] +$$
$$3\times 2^{d+1}(d+1+\frac{1}{d+1}) + 6\times 2^d.$$

اما به سادگی می‌توان دید:

$$3\times 2^{d+1}(d+1+\frac{1}{d+1}) + 6\times 2^d \geq$$
$$3\times 2^{d+1}(d+2+\frac{1}{d+2}),$$

بنابراین:

$$\sum_{v\in C_6^{d+1}} f(v) \geq [[A_d A'_d, B_d B'_d]] +$$
$$3\times 2^{d+1}(d+2+\frac{1}{d+2}),$$

و لذا حکم برای $d+1$ برقرار بوده و ادعا ثابت می‌شود.

اکنون به ادامه اثبات قضیه ۴-۴ می‌پردازیم:

فرض کنید $d \geq 1$ و $V(C_6^d) = A_d \cup B_d$ افراز مجزای رئوس به مجموعه‌های مستقل راسی باشد. از آن‌جایی که در هر یک از بخش‌های مستقل مجزای A_d و B_d دقیقاً 3×2^d راس وجود دارد؛ لذا می‌توانیم بین رئوس این دو دسته یک تطابق کامل درنظر بگیریم. اگر (a,b) یکی از یال‌های این تطابق باشد، با توجه به خاصیت یک‌نوایی قوی داریم:

$$f(bA_d) - f(A_d - \{a\}) \geq 1,$$

که در آن منظور از bA_d اجتماع مجموعه A_d با مجموعه تک‌عضوی b می‌باشد. نامساوی فوق برقرار است چرا که $A_d - \{a\}$ یک مجموعه مستقل راسی است، درحالی‌که bA_d چنین نیست. با درنظرگرفتن رابطه فوق برای هر یک از زوج جملات حاصل از مجموع‌های زیر داریم:

$$[[A_d, B_d]] = \sum_{b\in B_d} f(bA_d) - \sum_{a\in A_d} f(A_d - \{a\}) \geq 3\times 2^d.$$

بنابراین:

$$\sum_{v\in C_6^d} f(v) \geq 3\times 2^d (d+1+\frac{1}{d+1}) + 3\times 2^d =$$
$$3\times 2^d (d+2+\frac{1}{d+1})$$

از آن‌جایی‌که 6×2^d راس در C_6^d وجود دارد، پس حداقل یک راس $v \in C_6^d$ وجود دارد به طوری که:

$$f(v) \geq \frac{3\times 2^d (d+2+\frac{1}{d+1})}{6\times 2^d}$$

و این اثبات را تمام می‌کند، زیرا:

$$R(G) \geq \frac{d(d+3)+3}{2(d+1)}.$$

- **کران بالای نسبت اطلاعات**

برای اثبات کران بالا از روش تجزیه [۱۲] استفاده خواهیم کرد. در این مقاله روشی برای طرح‌های تسهیم راز در حالت کلی ارائه شده است که به آن ساختار λ -تجزیه گویند. این روش، یک ساختار بازگشتی برای تولید یک طرح تسهیم راز با استفاده از طرح‌های تسهیم راز کوچک‌تر به عنوان بلوک‌هایی از طرح اصلی است. این روش در ساختار دسترسی یک گراف، بر پایه یافتن یک پوشش از آن گراف است به‌طوری‌که هر یال از این گراف می‌بایست در حداقل λ تا از زیرگراف‌های این پوشش قرار گیرد. قضیه زیر نحوه استفاده از چنین پوششی را برای معرفی یک کران بر روی ساختار دسترسی گرافی بیان می‌کند.

قضیه۴-۶- [۱۲] فرض کنید G_i خانواده‌ای از زیرگراف‌های G باشد به‌طوری‌که هر یال از گراف G متعلق به حداقل λ تا از G_i-ها باشد. به ازای راس $v \in V(G)$ تعریف کنید:

اگر $v \notin V(G_i)$ تعریف می‌کنیم $r_i(v)=0$ و در غیر این صورت $r_i(v)=R(G_i)$. آن‌گاه:

$$R(G) = sup_{v\in G} \frac{\sum_i r_i(v)}{\lambda}$$

حال، قضیه فوق را برای یافتن کران بالایی مطلوب برای $R(C_6^d)$ به کار می بریم.

لم ۴-۷- به ازای مقدار صحیح نامنفی d داریم:

$$R(C_6^d) \leq \frac{d(d+3)+3}{2(d+1)}$$

اثبات: در این‌جا پوششی از C_6^d توسط دورهای به طول ۴ و ۶ ارائه می‌دهیم و این پوشش‌ها را به اختصار ۲-رخ نامیده می‌شود، به‌طوری‌که هر یال دقیقاً $d+1$ بار و هر راس دقیقاً $\frac{d^2+3d+1}{2}$ بار توسط ۲-رخ‌ها پوشیده می‌شوند که در نتیجه لم ۴-۷ به عنوان نتیجه‌ای از قضیه ۴-۶ اثبات می‌شود.

به وضوح، C_6^d یک گراف $(d+2)$- منظم است که دارای 6×2^d راس می‌باشد. توجه دارید که هر زوج از یال‌های شامل راس v تشکیل یک ۲-رخ می‌دهند. بنابراین، هر راس دقیقاً روی $\binom{d+2}{2}-1$ تا ۲-رخ قرار می گیرد. حال، به سادگی می‌توان بررسی کرد که تمامی ۲-رخ‌ها یک پوشش برای C_6^d تشکیل می‌دهند به‌طوری‌که هر یال از C_6^d مشمول در حداقل $d+1$ از این ۲-رخ‌ها است. بنابراین، ۲-رخ‌ها تشکیل یک $(d+1)$- پوشش از C_6^d می‌دهند. با توجه به مطالب فوق داریم:

$$R(G) \leq \frac{\binom{d+2}{2}-1+\frac{3}{2}}{d+1} = \frac{d(d+3)+3}{2(d+1)}$$

حال، قضیه اصلی از لم **۴-۵** و لم **۴-۷** نتیجه شده و به صورت زیر می‌باشد:

قضیه ۴-۸- برای مقدار صحیح نامنفی d، داریم:

$$R(C_6^d) = \frac{d(d+3)+3}{2(d+1)}.$$

قضیه فوق در واقع مبین یک مقدار دقیق برای نسبت اطلاعات یک رده نامتناهی از گراف‌ها می‌باشد.

۵- نتیجه‌گیری

در این مقاله، نسبت اطلاعات ساختارهای دسترسی گرافی طرح‌های تسهیم راز مورد مطالعه قرار گرفت. به این منظور کران پایینی برای نسبت اطلاعات حاصل ضرب دکارتی یک درخت دلخواه با قطر حداقل ۳ و دور C_m برای هر $m \geq 3$ یافتیم. برای یافتن این کران پایین از نسبت اطلاعات یک زیرگراف القایی معروف و شناخته‌شده در این گراف استفاده شد. علاوه براین، بهترین نسبت اطلاعات، طرح تسهیم راز کامل بر پایه گراف C_6^d را تعین کردیم که در آن، C_6^d گراف حاصل از ضرب دکارتی دور به طول ۶ با گراف d- مکعب است. به طور دقیق‌تر، برای هر $d \geq 1$، ثابت کردیم که $R(C_6^d) = \frac{d(d+3)+3}{2(d+1)}$. جهت ارائه کران بالای نسبت اطلاعات C_6^d، از پوشش این گراف توسط زیرگراف‌هایی با نسبت اطلاعات معین به روش تجزیه Stinson استفاده شد. در بیش‌تر مقالاتی که تاکنون به این موضوع پرداخته‌اند کران‌های غیردقیق و به صورت بازه‌ای ارائه شده است، درحالی‌که در این مقاله نتیجه اصلی به صورت یک کران دقیق معرفی گردیده است.

خواننده علاقمند می‌تواند نسبت اطلاعات دقیق گراف‌های بسیاری که هنوز تعیین نگردیده است را مورد مطالعه قرار دهد.

۶- مراجع

[1] A. Shamir, "How to share a secret," Comm. ACM, 22,vol. 11, pp. 612-613, 1979.

[2] G. R. Blakley, "Safe guarding cryptographic keys," in AFIPS Conference Proceedings, New York, United States of America, pp. 313-317, June 4-7, 1979.

[3] C. Blundo, A. De Santis, D. R. Stinson, and U. Vaccaro, “Graph decomposition and secret sharing schemes,” Journal of Cryptology, vol. 8, pp. 39-64, 1995.

[4] E. F. Brickell and D. M. Davenport, “On the classification of ideal secret sharing schemes,” Journal of Cryptology, vol. 4, pp. 123-134, 1991.

[5] E. F. Brickell and D. R. Stinson, “Some improved bounds on the information rate of perfect secret sharing schemes,” Journal of Cryptology, vol. 5, pp. 153-166, 1992.

[6] M. Dijk, “On the information rate of perfect secret sharing schemes”, Designs Codes and Cryptography, vol. 6, pp. 143-160, 1995.

[7] W. A. Jackson and K. M. Martin, “Perfect secret sharing schemes on five participants,” Designs Codes and Cryptography, vol. 9, pp. 267-286, 1996.

[8] C. Padro, “Lecture notes in secret sharing,” Available at http://eprint.iacr.org/2012/674, 2012.

[9] L. Csirmaz and G. Tardos, “Optimal information rate of secret sharing schemes on trees”, IEEE Trans. Inf. Theory, vol. 59, pp. 2527-2530, 2013.

[10] L. Csirmaz and P. Ligeti, “On an infinite family of graphs with information ratio 2−1/k”, Computing, vol. 85, pp. 127-136, 2009.

[11] L. Csirmaz, “Secret sharing on the d-dimensional cube,” Designs Codes and Cryptography, vol. 74, pp. 719-729, 2015.

[12] D. R. Stinson, “Decomposition construction for secret sharing schemes,” IEEE Trans. Inf. Theory, vol 40, pp. 118-125, 1994.

[13] W. Wang, Z. Li, and Y. Song, “The optimal information rate of perfect secret sharing schemes,” In 2011 International Conference on Business Management and Electronic Information (BMEI), Guangzhou, China, May 13-15, pp. 207-212, 2011.

[14] Z. Karimifard, S. Mashhadi, and D. Ebrahimi Bagha, “Semiquantum Secret Sharing Using Three Particles Without Entanglement,” Journal Of Electronical & Cyber Defence, vol. 4, no. 3, 2016.

[15] L. Csirmaz, “Secret sharing on infinite graphs,” Tetra Mountains Mathematical Publication, vol. 41, pp.1-18, 2008.

مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"
ویژه‌نامه کنفرانس بین‌المللی ترکیبیات، رمزنگاری و محاسبات، ص ۱۶-۱۳

حمله تفاضلی– خطی جدید به الگوریتم‌های رمز قالبی

مسعود هادیان دهکردی[1*]، رقیه تقی‌زاده[2]

۱- استاد، دانشکده ریاضی، دانشگاه علم و صنعت ایران، ۲- دانشجوی دکتری دانشگاه علم و صنعت ایران

(دریافت: ۹۵/۰۷/۰۵، پذیرش: ۹۶/۰۳/۰۶)

چکیده

تحلیل تفاضلی و خطی دو ابزار اصلی برای بررسی امنیت الگوریتم‌های رمز قالبی است. در این مقاله، یک حمله جدید از نوع متن اصلی انتخاب‌شده به الگوریتم‌های رمز قالبی که ترکیبی از دو حمله تفاضلی و خطی است معرفی می‌شود. در این حمله از مشخصه‌های تفاضلی که در بخشی از الگوریتم رمز با احتمال ۱ ایجاد می‌شود و تقریب‌های خطی که همبستگی آنها دقیقا برابر با صفر است، استفاده می‌شود

واژه‌های کلیدی: رمز قالبی، تحلیل تفاضلی، تقریب خطی

۱- مقدمه[1]

تحلیل تفاضلی یک حمله از نوع متن اصلی انتخاب شده است که برای تحلیل الگوریتم‌های رمز قالبی معرفی شد. این حمله اولین بار در سال ۱۹۹۰ توسط بیهام و شامیر در [۱] معرفی شد. حمله خطی نیز توسط Matsui در سال ۱۹۹۳ در [۲] معرفی شد. این حمله از نوع متن اصلی- معلوم است که از تقریب‌های خطی به عنوان تمایزگر استفاده می‌کند.

حملات تفاضلی و خطی دو ابزار مهم در تحلیل و بررسی امنیت الگوریتم‌های رمز قالبی هستند. به کمک تحلیل تفاضلی و خطی حملات موثری به الگوریتم رمز قالبی DES نسبت به جستجوی جامع در کشف کلید مخفی و شکست الگوریتم رمز ارائه شد [۴-۳]. در حال حاضر نیز از این دو روش به عنوان ابزار اساسی در تحلیل الگوریتم‌های رمز قالبی مورد استفاده قرار می‌گیرد

تحلیل تفاضلی- خطی از ترکیب دو حمله تفاضلی و خطی ایجاد می‌شود. این حمله اولین بار توسط Langford در سال ۱۹۹۵ در [۵] معرفی و بر روی ۸ دور الگوریتم رمز قالبی DES اعمال شد. در این حمله از مشخصه‌های تفاضلی که در دورهایی از الگوریتم رمز با احتمال ۱ رخ می‌دهند استفاده می‌کند. اگر در ادامه این دورها، دورهایی باشند که تقریب خطی مناسب را ایجاد کنند، در این حالت امید داریم برای هر جفت متن اصلی انتخاب‌شده برای کلید درست این تقریب خطی با احتمالی برقرار باشد. این حمله در سال ۲۰۰۲ در مقاله [۶] توسط Biham و Dunkelman بهبود داده شد. در حمله معرفی‌شده مشخصه تفاضلی با احتمال کم‌تر از ۱ برقرار است. در این مقاله ما حمله جدیدی از نوع متن اصلی انتخاب‌شده را معرفی می‌کنیم که ترکیبی از حمله تفاضلی و خطی است و در آن از مشخصه‌های که با احتمال ۱ برای دورهایی از رمز برقرار است و تقریب‌های خطی خاصی که با احتمال ½ رخ می‌دهند استفاده می‌شود. . تحلیل خطی- صفر هم‌بستگی یک روش جدید حمله می‌باشد که یک نوع حمله تمایزی است و در برخی موارد منجر به یافتن کلید رمز در الگوریتم‌های رمز قالبی نیز خواهد شد. این حمله توسط Bogdanov در [۸-۷] معرفی شد.

مابقی این مقاله به این صورت سازمان‌دهی می‌شود که در بخش دوم تعاریف و مقدمات مورد نیاز آورده شده است. بخش سوم به معرفی مختصری از حمله تفاضلی و خطی اختصاص یافته است. در بخش چهارم حمله جدید تفاضلی-خطی معرفی می‌شود و در نهایت در بخش پنجم نتیجه‌گیری خواهیم کرد.

۲- تعاریف و مقدمات

فرض کنید V_n نشان‌دهنده فضای برداری باینری n - بعدی باشد. ضرب داخلی دو بردار $a = (a_1, a_2, \dots, a_n) \in V_n$ و $b = (b_1, b_2, \dots, b_n) \in V_n$ که با $a.b$ نمایش داده می‌شود به صورت زیر تعریف می‌شود:

$$a.b = a_1b_1 \oplus a_2b_2 \oplus \dots \oplus a_nb_n \qquad (1)$$

* رایانامه نویسنده مسئول: mhadian@iust.ac.ir

تابع $f: V_n \to V_1$ یک تابع بولی نامیده می‌شود.

تابع $f: V_n \to V_m$ که $f = (f_1, f_2, \dots, f_m)$ و در آن f_iها تابع بولی‌اند یک تابع بولی برداری از بعد m نامیده می‌شود.

یک تابع بولی برداری از بعد m را می‌توان توسط یک ماتریس باینری $m \times n$ مانند U نمایش داد. فرض کنید سطرهای ماتریس U با u_1، u_2،...و u_m نمایش داده شود لذا هر u_i، یک بردار باینری n- بعدی است.

فرض کنید $Y \in V_n$ یک بردار تصادفی و $p_\eta = Pr(\boldsymbol{Y} = \eta)$ در این صورت بردار $p = (p_0, \dots, p_{2^m-1})$ توزیع احتمال آن می‌باشد.

فرض کنید $f: Vn \to Vm$ یک تابع بولی برداری و $\boldsymbol{X}$ یک متغیر تصادفی در V_n باشد که توزیع آن یک‌نواخت باشد. اگر $\boldsymbol{Y} = f(\boldsymbol{X})$ آن‌گاه $\boldsymbol{Y}$ یک متغیر تصادفی در V_m با توزیع احتمال $p(f) = (p_0(f), \dots, p_{2^m-1}(f))$ می‌باشد، جایی‌که $Pr(f(\boldsymbol{X}) = \eta) = p_\eta(f), \eta \in Vm.$ این توزع احتمال، توزیع احتمال f نامیده می‌شود و با $p(f)$ نمایش داده می‌شود.

دو تابع بولی f و g را از لحاظ آماری مستقل گویند هرگاه متغیرهای تصادفی متناظر با آن‌ها از لحاظ آماری مستقل باشند.

هم‌بستگی میان یک متغیر تصادفی $\boldsymbol{X}$ و مقدار ۰ به صورت $Pr(\boldsymbol{X} = 0) - Pr(\boldsymbol{X} = 1)$ تعریف می‌شود. هم‌بستگی یک تابع بولی $g: V_n \to V_1$ با تابع ۰ که به طور خلاصه هم‌بستگی g نامیده می‌شود به صورت زیر تعریف می‌شود:

$$c(g) = 2\,Pr\,(g(\boldsymbol{X}) = 0) - 1 \qquad (۲)$$

لم: فرض کنید $f: Z_2^n \to Z_2^m$. یک تابع بولی با تابع احتمال p باشد در این صورت به ازای هر $\eta \in Z_2^m$ رابطه زیر برقرار است.

$$p_\eta = 2^{-m} \sum_{a \in F_2^m} (-1)^{a.\eta} c(a.f) \qquad (۳)$$

اثبات: اثبات این لم در مقاله [۱۳] آمده است.

۳- تحلیل تفاضلی و خطی

در این بخش برخی تعاریف و نمادگذاری‌هایی که در حمله تفاضلی و خطی مورد نیاز است آورده شده است.

۳-۱- تحلیل تفاضلی

در تحلیل تفاضلی بررسی می‌کند که یک تفاضل خاص در یک زوج متن اصلی ورودی از یک الگوریتم رمز مانند E با یک کلید ثابت، چه تاثیری در تفاضل خروجی متن رمز شده متناظر با آن می‌گذارد.

تعریف: اگر α و β دو قالب n - بیتی باشند احتمال تفاضل (α, β) برای الگوریتم رمز E که با $\Delta\alpha \to \Delta\beta$ نمایش داده می‌شود به صورت زیر محاسبه می‌شود:

$$Pr_E(\Delta\alpha \to \Delta\beta) = Pr\{E(P) \oplus E(P \oplus \alpha) = \beta\} \qquad (۴)$$

برای یک تابع تصادفی انتظار داریم که مقدار احتمال برای هر تفاضل ورودی α و تفاضل خروجی β برابر با 2^{-n} باشد. بنابراین، اگر مقدار $Pr_E(\Delta\alpha \to \Delta\beta)$ بزرگتر از 2^{-n} باشد می‌توان از تفاضل (α, β) و با در اختیار داشتن مقدار کافی جفت متن اصلی انتخاب‌شده (که هر زوج متن اصلی داری تفاضل α باشد) به‌عنوان یک تمایزگر برای تمیز الگوریتم رمز E از یک جای‌گشت تصادفی، استفاده کرد.

۳-۲- تحلیل خطی

در تحلیل خطی از هم‌بستگی میان یک تابع خطی از قالب ورودی الگوریتم و تابع خطی از قالب خروجی، استفاده می‌کند. بیش‌ترین تابع خطی که مورد استفاده قرار می‌گیرد از ضرب داخلی یک بردار خاص (که به آن ماسک ورودی گفته می‌شود) در قالب ورودی یا ضرب داخلی یک بردار خاص (که به آن ماسک خروجی گفته می‌شود) در قالب خروجی یک الگوریتم رمز ایجاد می‌شوند.

تعریف: اگر α و β دو قالب n - بیتی باشند احتمال یک تقریب خطی با ماسک ورودی α و ماسک خروجی β برای الگوریتم رمز E که گاهی با $\Gamma\alpha \to \Gamma\beta$ نیز نمایش داده می‌شود به صورت زیر تعریف می‌شود:

$$Pr_E(\Gamma\alpha \to \Gamma\beta) = Pr\{P \odot \alpha \oplus E(P) \odot \beta = 0\} \qquad (۵)$$

هم‌بستگی یک تقریب خطی $\Gamma\alpha \to \Gamma\beta$ که با ϵ نمایش داده می‌شود به صورت زیر تعریف می‌شود:

$$\epsilon = 2Pr_E(\Gamma\alpha \to \Gamma\beta) - \frac{1}{2} \qquad (۶)$$

برای یک تابع که به صورت تصادفی انتخاب شده باشد احتمال هر تقریب خطی با ماسک ورودی α و ماسک خروجی β برابر با $\frac{1}{2}$ است. بنابراین دارای هم‌بستگی ۰ است. حال اگر یک تقریب خطی با احتمال مخالف $\frac{1}{2}$ در یک الگوریتم رمز پیدا شود با در اختیار داشتن تعداد کافی زوج متن اصلی- متن رمزشده می‌توان از آن تقریب خطی به عنوان یک تمایزگر برای تمیزدادن الگوریتم رمز از یک جای‌گشت تصادفی، استفاده کرد.

۳-۲- تقریب خطی- صفر هم‌بستگی

فرض کنید E یک رمز قالبی n- بیتی باشد. یک تقریب خطی با

ماسک ورودی α و ماسک خروجی β که برای آن $P(\alpha,\beta)=Pr_E(\Gamma\alpha\to\Gamma\beta)=\frac{1}{2}$، باشد را تقریب خطی با هم‌بستگی صفر نامند. در تحلیل خطی- صفر هم‌بستگی از این نوع تقریب‌های خطی استفاده می‌شود.

۴- معرفی حمله تفاضلی- خطی جدید

در این بخش ابتدا مقدماتی از حمله تفاضلی- خطی ارائه می‌شود سپس حمله جدید را معرفی می‌کنیم.

۴-۱- حمله تفاضلی- خطی

فرض کنید الگوریتم رمز E ترکیبی از دو بخش E_0 و E_1 است، به عبارتی $E=E_0\circ E_1$. اگر $\Delta\alpha\to\Delta\beta$ یک مشخصه تفاضلی با احتمال ۱ برای E_0 باشد و $\Gamma\gamma\to\Gamma\delta$ یک تقریب خطی با اریبی ε برای E_1 باشد به قسمی که $\Delta\beta.\Gamma\gamma=0$ در این صورت تمایزگر تفاضلی- خطی زوج $(\Delta\alpha\to\Delta\beta,\Gamma\gamma\to\Gamma\delta)$ تعریف می‌شود. فرض کنید p و p^* نشان‌دهنده دو زوج متن اصلی باشد که $p\oplus p^*=\Delta\alpha$ در این صورت چون $E_0(p)\oplus E_0(p^*)=\Delta\beta$ لذا با احتمال ۱ رابطه $E_0(p).\Gamma\gamma=E_0(p^*).\Gamma\gamma$ برقرار است. تمایزگر تفاضلی- خطی برابر بررسی برقراری رابطه:

$$\delta.\mathrm{E(p)}\oplus\Gamma\delta.E(p^*)=0 \qquad (۷)$$

یا برقراری رابطه:

$$\Gamma\delta.\mathrm{E(p)}=\Gamma\delta.E(p^*) \qquad (۸)$$

تعریف می‌شود.

احتمال برقراری تمایزگر به‌دست‌آمده با فرض شرایطی که در [۵] آمده است، به صورت زیر می‌باشد:

$$\begin{aligned}&p_r(\delta.\mathrm{E(p)}\oplus\delta.E(p^*)=0)\\&=\left(\frac{1}{2}+\varepsilon\right)\left(\frac{1}{2}+\varepsilon\right)+\left(\frac{1}{2}-\varepsilon\right)\left(\frac{1}{2}-\varepsilon\right)\\&=\frac{1}{2}+2\varepsilon^2 \qquad (۹)\end{aligned}$$

برای یک جای‌گشت تصادفی احتمال برقراری هر تمایزگر تفاضلی- خطی برابر با $\frac{1}{2}$ است بنابراین اگر اریبی رابطه فوق به اندازه کافی بزرگ باشد می‌توان از رابطه فوق به عنوان یک تمایزگر استفاده کرد.

۴-۲- تمایزگر تفاضلی- خطی جدید

برای معرفی تمایزگر تفاضلی- خطی جدید از مشخطه‌های تفاضلی با احتمال ۱ و تقریب‌های خطی با هم‌بستگی صفر استفاده می‌شود.

فرض کنید الگوریتم رمز E ترکیبی از دو بخش E_0 و E_1 است، یعنی $E=E_0\circ E_1$. اگر $\Delta\alpha\to\Delta\beta$ یک مشخصه تفاضلی با احتمال ۱ برای E_0 باشد و $\Gamma\gamma\to\Gamma\delta$ یک تقریب خطی با احتمال $\frac{1}{2}$ یا هم‌بستگی صفر، برای E_1 باشد به قسمی که $\Delta\beta.\Gamma\gamma=0$ در این صورت تمایزگر تفاضلی- خطی زوج $(\Delta\alpha\to\Delta\beta,\Gamma\gamma\to\Gamma\delta)$. تعریف می‌شود. فرض کنید p و p^* نشان‌دهنده دو زوج متن اصلی باشد که $p\oplus p^*=\Delta\alpha$ در این صورت چون $E_0(p)\oplus E_0(p^*)=\Delta\beta$ لذا با احتمال ۱ رابطه $E_0(p).\Gamma\gamma=E_0(p^*).\Gamma\gamma$ برقرار است. تمایزگر تفاضلی- خطی برابر با برقراری $\delta.\mathrm{E(p)}\oplus\Gamma\delta.E(p^*)=0$ یا برقراری رابطه $\Gamma\delta.\mathrm{E(p)}=\Gamma\delta.E(p^*)$ تعریف می‌شود.

احتمال برقراری تمایزگر به‌دست‌آمده با فرض شرایطی که در [۵] آمده است، به صورت زیر می‌باشد:

$$p_r(\delta.\mathrm{E(p)}\oplus\delta.E(p^*)=0)=\frac{1}{2} \qquad (۱۰)$$

بنابراین برای الگوریتم رمز E رابطه (۱۰) با هم‌بستگی، وجود دارد. حال می‌توان از تقریب‌های خطی چندگانه استفاده کرد. فرض کنید $a\in F_2^n$ نشان‌دهنده متن اصلی و $b\in F_2^n$ نشان‌دهنده داده‌ای در فرآیند رمزنگاری باشد. حال اگر m رابطه خطی $z_i=<u_i,a>+<w_i,b>$ در یک الگوریتم رمز با احتمال $\frac{1}{2}$ وجود داشته باشد، می‌توان به‌جای درنظرگرفتن هر بیت و محاسبه توزیع احتمال آن به صورت مستقل، توزیع و m-تایی $z=(z_1,\dots,z_m)$. را به دست آود. از طرفی رابطه میان توزیع احتمال z و مقدار هم‌بستگی c_γ برای هر $\gamma\in F_2^m$ به صورت زیر می‌باشد:

$$\Pr[z]=\sum_{\gamma\in F_2^m}(-1)^{<\gamma,z>}c_\gamma \qquad (۱۱)$$

حال اگر هم‌بستگی میان تمامی تقریب‌های خطی برابر با صفر باشد، به عبارتی برای هر $\gamma\neq 0$ مقدار $c_\gamma=0$ باشد با جای‌گذاری این مقادیر در رابطه (۱۱) و محاسبه مقدار احتمال به این نتیجه خواهیم رسید که متغیر تصادفی z در F_2^m دارای توزیع یکنواخت است.

برای حمله فرض کنید N زوج متن اصلی مجزای (p,p^*) برای یک رمز قالبی$(=E_1\circ E_0)$ E n- بیتی که در آن مشخصه تفاضلی $\Delta\alpha\to\Delta\beta$ با احتمال ۱ برای E_0 و m تقریب خطی $\Gamma\gamma\to\Gamma\delta$ با احتمال $\frac{1}{2}$ یا هم‌بستگی ۰ برای E_1 رخ می‌دهد و علاوه بر این $\Delta\beta.\Gamma\gamma=0$ را در اختیار داشته باشیم. اگر برای $i=1,\dots,m$ مقدار $z_i=\Gamma\delta_i.E(p)\oplus\Gamma\delta_i.E(p^*)$ باشد آن‌گاه طبق رابطه (۱۱) متغیر تصادفی $z=(z_1,\dots,z_m)$ دارای توزیع یک‌نواخت در F_2^m است. بنابراین می‌توان رفتار غیرتصادفی N

داده را از داده‌های تصادفی تمیز داد. فرض کنید $V[z]$ نشان‌دهنده تعداد دفعاتی باشد که z مشاهده می‌شود. در ابتدا برای هر $z \in F_2^m$، $V[z]=0$ مقداردهی اولیه می‌شوند سپس برای هر جفت (p,p^*) مقدار z به کمک تقریب‌های خطی به‌دست‌آمده، محاسبه و به شمارنده آن یکی اضافه می‌شود. اکنون آماره T که در [۱۰] آمده است را محاسبه می‌کنیم

$$T=\sum_{i=0}^{2^m-1}\frac{(V[z]-N2^{-m})^2}{N2^{-m}(1-2^{-m})} \qquad (۱۲)$$

اگر N به اندازه کافی بزرگ انتخاب شده باشد آماره T برای داده‌های تصادفی و داده‌هایی که از رمز آمده‌اند دارای دو توزیع متفاوت به شرح زیر است:

۱- آماره T برای کلید صحیح دارای توزیع کای- دو (خی- دو) با میانگین و واریانس زیر است:

$$\mu_0=2^m\times\frac{2^n-N}{2^n-1} \quad \sigma_0^2=2\times 2^m\times\frac{2^n-N}{2^n-1} \qquad (۱۳)$$

۲- آماره T برای کلید نادرست دارای توزیع خی- دو با میانگین و واریانس زیر است:

$$\mu_1=2^m \quad \sigma_1^2=2\times 2^m \qquad (۱۴)$$

فرض کنید α_0 و α_1 نشان‌دهنده خطای نوع اول و دوم باشند در این صورت مقدار آستانه تصمیم به صورت زیر محاسبه می‌شود:

$$\tau=\mu_0+\sigma_0\times z_{1-\alpha_0}=\mu_1+\sigma_1\times z_{1-\alpha_1} \qquad (۱۵)$$

بنابراین مقدار داده مورد نیاز برای تمیزدادن الگوریتم رمز از یک جای‌گشت تصادفی برابر با مقدار زیر است:

$$N=\frac{2^n(z_{1-\alpha_0}+z_{1-\alpha_1})}{\sqrt{l/2}-z_{1-\alpha_1}} \qquad (۱۴)$$

که در آن، برای $0<p<1$، $z_p=\phi^{-1}(p)$ و تابع ϕ، تابع توزیع تجمعی توزیع نرمال است. احتمال موفقیت حمله برابر، $P_s=1-\alpha_0$ می‌باشد.

۵- نتیجه‌گیری

در این مقاله یک حمله جدید از خانواده حملات تفاضلی- خطی معرفی شد که در آن از تقریب‌های خطی که دارای هم‌بستگی دقیقاً صفر بودند استفاده شد. لازم به ذکر است که در این حمله از تقریب‌های خطی که هم‌بستگی آن‌ها صفر است و در حمله تفاضلی- خطی نادیده گرفته می‌شدند، استفاده شده است. از نتایج به‌دست‌آمده می‌توان الگوریتم‌های رمز قالبی که شرایط فوق را داشته باشند مورد تحلیل و بررسی قرار داد.

۶- مراجع

[1] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," In: A. Menezes, S. A. Vanstone, (eds.) CRYPTO 1990, LNCS, vol. 537, pp. 2-21, Springer, Heidelberg, 1990.

[2] M. Matsui and A. Yamagishi, "A new method for known plaintext attack of FEAL cipher," In: R. A. Rueppel, (ed.) EUROCRYPT 1992, LNCS, vol. 658, pp. 81-91, Springer, Heidelberg, 1993.

[3] E. Biham and A. Shamir, "Differential cryptanalysis of the full 16-round DES," In: E. F. Brickell, (ed.) CRYPTO 1992. LNCS, vol. 740, pp. 487-496, Springer, Heidelberg, 1993.

[4] M. Matsui, "Linear cryptanalysis method for DES cipher," In: T. Helleseth, (ed.) EUROCRYPT 1993, LNCS, vol. 765, pp. 386-397, Springer, Heidelberg, 1994.

[5] S. K. Langford and M. E. Hellman, "Differential-linear cryptanalysis. In: Y. Desmedt, (ed.) CRYPTO 1994, LNCS, vol. 839, pp. 17-25, Springer, Heidelberg, 1994.

[6] E. Biham, O. Dunkelman, and N. Keller, "Enhancing differential-linear cryptanalysis," In: Y. Zheng, (ed.) ASIACRYPT 2002, LNCS, vol. 2501, pp. 254-266, Springer, Heidelberg, 2002.

[7] A. Bogdanov and V. Rijmen, "Linear Hulls with Correlation Zero and Linear Cryptanalysis of Block Ciphers," Designs, Codes and Cryptography, Springer-Verlag, to appear, 2012. Preprint available as Cryptology ePrint Archive: Report 2011/123, http://eprint.iacr.org/2011/123.

[8] A. Bogdanov and M. Wang, "Zero Correlation Linear Cryptanalysis with Reduced Data Complexity," FSE'12, LNCS, Anne Canteaut (ed.), Springer-Verlag, to appear, 2012.

[9] A. Bogdanov, G. Leander, K. Nyberg, and M. Wang, "Integral and Multidimensional Linear Distinguishers with Correlation Zero," In: X. Wang, K. Sako, (eds.) ASIACRYPT 2012, LNCS, vol. 7658, pp. 244–261, Springer, 2012.

[10] A. Bogdanov, G. Leander, K. Nyberg, and M. Wang, "Integral and Multidimensional Linear Distinguishers with Correlation Zero," IACR ePrint Archive report, 2012.

[11] H. Soleimany and K. Nyberg, "Zero-correlation linear cryptanalysis of reduced-round LBlock," Designs, Codes and Cryptography, vol. 73, no. 2, pp. 683-698, 2014.

[12] E. Biham, "On Matsui's linear cryptanalysis," In Proc. The Workshop on the Theory and Application of Cryptographic Techniques, pp. 341-355, May 1994.

مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"
ویژه‌نامه کنفرانس بین‌المللی ترکیبیات، رمزنگاری و محاسبات، ص ۲۰ -۱۷

نکاتی در رابطه با کدهای تام گراف‌های فاصله متوازن

حسن خرازی[1*]، مهدی علائیان[2]، حسین شبانی[3]

۱- استادیار، دانشگاه امام حسین (ع) ۲- استاد، دانشگاه علم و صنعت ایران ۳- دکتری ریاضی، دانشگاه کاشان

(دریافت: ۹۵/۰۷/۰۵، پذیرش: ۹۶/۰۳/۰۷)

چکیده

در این مقاله به بررسی وجود کدهای تام در برخی از خانواده‌های گراف‌های فاصله متوازن می‌پردازیم. هم‌چنین برخی نتایج در رابطه با وجود کدهای تام در حاصل‌ضرب دورها و توان‌های این نوع گراف نیز آورده شده است.

واژه‌های کلیدی: گراف‌های فاصله متوازن، کد تام، توان گراف

۱- مقدمه

کدهای تام در گراف به عنوان تعمیمی از کدهای تام در نظریه کد معرفی گردید و شرایط لازم برای وجود این نوع کدها در برخی از خانواده‌های گراف‌ها مورد بررسی قرار گرفت [۱]. این مفهوم مورد توجه محققین در این زمینه قرار گرفت و به بررسی و تعیین وجود آن در گراف‌ها پرداختند [۲]. مسأله تعیین وجود کد تام در یک گراف، یک مسأله NP- سخت است [۳]. بنابراین، برای گراف داده‌شده G تعیین وجود یک کد تام در آن، از مسائل مورد علاقه محققین است و لذا در این زمینه سوالات زیر مطرح است: برای گراف داده‌شده G، آیا این گراف شامل یک کد تام است؟ اگر G شامل یک کد تام باشد آن‌گاه این کد به چه صورتی است؟

منظور از یک گراف در این مقاله یک گراف ساده که فاقد یال‌های چندگانه و طوقه می‌باشد. فرض کنید G یک گراف با مجموعه رأس‌های $V(G)$ و مجموعه یال‌های $E(G)$ است. اگر u و v دو رأس گراف G باشند آن‌گاه یک مسیر بین آن‌ها دنباله‌ای از رأس‌ها و یال‌هاست که هیچ رأس و یالی در آن تکرار نشده است. گراف هم‌بند، گرافی است که بین هر دو رأس آن یک مسیر وجود داشته باشد. طول یک مسیر برابر با تعداد یال‌های آن است. طول یک کوتاه‌ترین مسیر بین رأس u و v را فاصله بین آن‌ها نامیده و با $d_G(u,v)$ و یا به‌صورت $d(u,v)$ نشان داده می‌شود. قطر گراف G که با $diam(G)$ نشان داده می‌شود برابر با بیش‌ترین فاصله ممکن بین همه رأس‌های گراف است.

فرض کنیم $v \in V(G)$ و r یک عدد صحیح مثبت است. در این صورت، یک گوی به مرکز v و شعاع r عبارت است از زیرمجموعه‌ای از رأس‌ها به صورت

$$B(v,r) = \{x \in V(G) : d(v,x) \leq r\}.$$

تعریف: فرض کنید G یک گراف است. در این صورت هر زیرمجموعه مانند C از $V(G)$ را یک کد و هریک از عناصر آن را یک کدواژه می‌نامیم. کد C را یک کد t- تام گوییم هرگاه همه گوی‌ها به شعاع t و مرکز کدواژه‌ها تشکیل یک افراز برای $V(G)$ بدهند. در حالت خاص $t = 1$، کد 1-تام را کد تام می‌نامند.

اگر C یک کد t- تام باشد آن‌گاه گوی‌های $B(v,t)$ که $v \in C$، مجزا هستند و تمام رئوس گراف را می‌پوشانند. فرض بر این است که گراف هم‌بند است، زیرا در غیر این صورت، هر مولفه گراف باید شامل کد t- تام باشد. در حالتی که C یک کد تام است داریم:

- برای هر دو رأس u و v از C، $d(u,v) \geq 3$،
- هر رأس که در C قرار ندارد حداکثر با یک کدواژه مجاور است.

در ادامه به معرفی گراف فاصله متوازن می‌پردازیم. گراف‌های فاصله متوازن ابتدا توسط هاندا (Handa) [۴] در سال ۱۹۹۹ در رابطه با مکعب‌های جزئی مورد بررسی قرار گرفت و سپس این مفهوم در سال ۲۰۰۸ در [۵] به صورت رسمی معرفی و در چارچوب حاصل‌ضرب‌های گوناگون گراف مطالعه گردید.

* رایانامه نویسنده مسئول: hkharazi@ihu.ac.ir

فرض کنید G یک گراف و ab یال دلخواهی از آن است. در این صورت مجموعه همه رئوسی که به a نسبت به b نزدیک‌تر هستند را با W_{ab}^G نشان می‌دهند. به عبارت دیگر:

$$W_{ab}^G = \{u \in V(G): d(u,a) < d(u,b)\}.$$

به طریق مشابه مجموعه W_{ba}^G تعریف می‌شود. هم‌چنین مجموعه ${}_aW_b^G$ به صورت مجموعه رئوسی است که فاصله آن‌ها از دو رأس a و b به یک اندازه است. به بیان دیگر:

$${}_aW_b^G = \{u \in V(G): d(u,a) < d(u,b)\}.$$

برای یال ab سه مجموعه W_{ab}^G، W_{ba}^G و ${}_aW_b^G$ یک افراز رأسی برای G ارائه می‌دهند.

تعریف: گراف G را فاصله متوازن گویند هرگاه برای هر یال ab از آن $|W_{ab}^G| = |W_{ba}^G|$.

در این مقاله وجود کدهای t- تام در برخی گراف‌های فاصله متوازن بررسی خواهند گردید.

۲- کدهای تام در گراف‌های فاصله متوازن

در این بخش به بررسی وجود کدهای تام در برخی گراف‌های فاصله متوازن خواهیم پرداخت. با استفاده از اعمال روی گراف‌ها، می‌توان گراف‌های فاصله متوازن جدیدی ساخت [۶]. پژوهشگران بسیاری در رابطه با وجود کدهای تام در حاصل‌ضرب گرافها مطالعه نموده‌اند [۷-۹]. یکی از این حاصل‌ضرب‌ها، ضرب دکارتی دو گراف G و H ($G \times H$) است که مجموعه رئوس و یال‌های آن برابر است با:

$$V(G \times H) = V(G) \times V(H),$$
$$E(G \times H) = \{(a,b)(c,d): [ac \in E(G) \& b = d] \vee [a = c \,\&\, bd \in E(H)]\}.$$

فرض کنید G و H دو گراف هم‌بند هستند. در این صورت $G \times H$ یک گراف فاصله متوازن است اگر و تنها اگر هر دو گراف G و H فاصله متوازن باشند [۵].

گراف دور C_n با n رأس، فاصله متوازن بوده و لذا حاصل‌ضرب دکارتی تعدادی از دورها نیز فاصله متوازن هستند و در قضیه زیر وجود کدهای تام در این نوع از گراف‌ها را بیان می‌کند.

قضیه ۱ [۱۰، قضیه ۶-۲]: فرض کنید G دورهای C_{n_1}، ...، C_{n_r} برای $r > 1$ است. در این صورت G دارای یک کد t- تام است اگر هر n_i مضربی از $t^r + (t+1)^r$ باشد. به علاوه، یک کد t- تام از G توسط r رأس تعیین می‌گردد.

گراف ابر- مکعب n- بعدی Q_n شامل 2^n رأس به صورت دنباله‌ای از n- تایی‌های دودویی است که دو رأس باهم مجاور هستند هرگاه تنها در یک مولفه اختلاف داشته باشند. این گراف فاصله متوازن بوده و دارای کد ۱- تام است اگر و تنها اگر $n+1$ توانی از ۲ باشد. در حالت کلی، قضیه زیر را می‌توان به راحتی نتیجه گرفت.

قضیه ۲: یک شرط لازم برای وجود یک کد t- تام در Q_n آن است که $\binom{n}{r+1}/\binom{2r+1}{r}$ یک مقدار صحیح باشد.

اثبات. با استفاده از [۱۱] به راحتی حکم به دست می‌آید.

قضیه ۳ [۸، نتیجه ۸]: فرض کنید G یک گراف دوبخشی و k یک عدد صحیح مثبت است. در این صورت حاصل‌ضرب دکارتی 2^k کپی از G با ابرمکعب Q_{2^k-1} دارای کد تام است.

فرض کنید Γ یک گروه متناهی و S زیرمجموعه‌ای از اعضای آن است به‌طوری‌که شامل همانی نیست، $S = S^{-1}$ و Γ را تولید می‌کند. در این صورت، گراف کیلی $Cay(\Gamma, S)$ یک گراف $|S|$- منتظم با مجموعه رئوس $V = \Gamma$ و مجموعه یال‌های $E = \{ab : a^{-1}b \in S\}$.

لم ۴: گراف کیلی $Cay(G,S)$ یک گراف فاصله متوازن است.

اثبات: گراف کیلی یک گراف رأس انتقالی است و لذا فاصله متوازن خواهد بود.

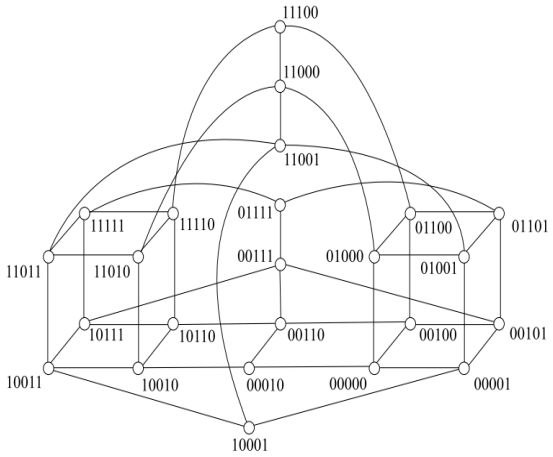
قضیه ۵ [۸، لم ۹]: گراف کیلی $G = Cay(\Gamma, S)$ را در نظر بگیرید که Γ یک گروه آبلی است. در این صورت G دارای کد تام است.

فرض کنید q یک عدد صحیح مثبت است و گراف کیلی $K_{2^q,2^q} \times Q_{2^q-1}$ را در نظر بگیرید که در آن $K_{2^q,2^q}$ گراف دوبخشی کامل است. بنابر مطالب اخیر، نتیجه زیر به‌دست می‌آید:

نتیجه ۶ [۸، نتیجه ۱۱]: برای هر دو عدد صحیح مثبت q و n، گراف $K_{2^q,2^q}^{2^n} \times Q_{2^{q+n}-1}$ دارای کد تام است.

گراف‌های فاصله متوازن شامل بسیاری از خانواده‌های معروف گراف‌ها مانند گراف‌های رأس انتقالی، شبه‌متقارن، پترسن تعمیم یافته و ... می‌باشند. بسیاری از این گراف‌ها، گراف‌هایی منتظم هستند. هم‌چنین گراف‌های نامنتظمی با خاصیت فاصله متوازن بودن وجود دارد. یکی از گراف‌های مشهور فاصله متوازن گرف معرفی شده توسط هاندا شکل (۱) است که آن را به عنوان یک گراف فاصله متوازن نامنتظم معرفی کرد. این گراف یک مکعب

جزئی بوده و قابل نشاندن در ابرمکعب Q_5 است [به مرجع ۴رجوع شود].



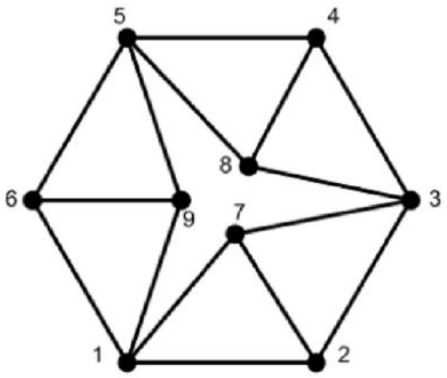
شکل (۱): گراف هاندا

گراف هاندا دارای کد تام نمی‌باشد که در قضیه زیر به آن اشاره شده است.

قضیه ۷: گراف هاندا شامل کد ۱- تام نیست.

اثبات: بررسی عدم وجود کد تام در گراف هاندا ساده است و به‌راحتی با توجه به شکل گراف به‌دست می‌آید.

در میان گراف‌های با تعداد حداکثر ۱۰ رأس، گراف شکل (۲) تنها گراف فاصله متوازن نامنتظم و غیردوبخشی است [۶].



شکل (۲): گراف G_1

فرض کنید k یک عدد صحیح نامنفی است. در این صورت برای $n = 6k + 3$، گراف دور C_{4k+2} با رئوس برچسب‌دار ۱، ۲، ...، $4k + 2$ را در نظر بگیرید و به آن رأس‌هایی با برچسب $4k + 3$، $4k + 4$، ...، $6k + 3$ به گونه‌ای اضافه کنید که رأس $4k + 3$ مجاور رئوس ۱، ۲ و ۳، رأس $4k + 4$ مجاور رئوس ۴، ۵ و ۶، ... و در نهایت رأس $6k + 3$ مجاور رئوس $4k + 1$، $4k + 2$ و ۱ باشد. گراف به‌دست‌آمده از روش فوق را گراف G_k نامیده می‌شود که گرافی نامنتظم است. گراف G_k فاصله متوازن است. دلیل این مطلب آن است که در این گراف هر یال فقط به یکی از سه شکل زیر است:

- یال‌ها از نوع $e = \{i, i + 1\}$، $i = 1,2, \dots ,4k + 2$؛
- یال‌ها از نوع $e = \{2i, 4k + i + 2\}$، $i = 1,2, \dots ,4k + 1$؛
- یال‌ها از نوع $e = \{2i \pm 1, 4k + i + 2\}$، $i = 1,2, \dots ,4k + 1$؛

و در هر یک از حالات فوق مشاهده می‌کنیم که $|W_{ab}| = |W_{ba}| = 3k + 1$.

قضیه ۸: گراف G_k دارای کد تام است اگر و تنها اگر $k = 3t + 1$ که در آن t یک عدد صحیح نامنفی است.

اثبات: مجموعه رئوس G_k را به سه دسته تقسیم می‌کنیم:

- دسته اول V_1: رئوسی که با $4k + 3$، ... $6k + 3$ نام‌گذاری شده اند.
- دسته دومV_2: رئوس درجه ۴ روی دور C_{4k+2} که با دو رأس از رئوس دسته V_1 مجاور هستند.
- دسته سومV_3: رئوس درجه ۳ روی دور C_{4k+2} که با یک رأس از رئوس دسته V_1 مجاور هستند.

حال فرض کنید $C \subset C(G_k)$ یک کد تام و $c_1 \in C$. بدون کاستن از کلیت مسأله، فرض می‌کنید $c_1 \in V_2$. در این صورت لزوماً رأس بعدی $c_2 \in C$ در فاصله ۳ از c_1 قرار دارد و لذا $c_2 \in V_1$ یا $c_2 \in V_3$. فرض کنید $c_2 \in V_3$ و این مطلب در وجود کد تام تأثیری ندارد. به همین ترتیب لزوماً $c_3 \in V_2$ و ... . بنابراین، کد C را می‌توان به صورت c_1، c_2، ...، c_r در نظر گرفت که r یک عدد صحیح مثبت است و تمام c_iها روی دور C_{4k+2} قرار دارند که در آن، $d(c_r, c_1) = 3$. این مطلب ایجاب می‌کند که C_{4k+2} باید دوری به طول $3s$ باشد که s عددی صحیح و مثبت است و در نتیجه $4k + 2 = 3s$. این امر تنها زمانی برقرار است که $k = 3t + 1$ که t یک عدد صحیح نامنفی است.

در ادامه خاصیت فاصله متوازن‌بودن توان یک گراف فاصله متوازن بررسی خواهد گردید. سپس با استفاده از آن وجود کدهای تام در توان‌های گراف‌هایی که فاصله متوازن هستند، بررسی خواهد شد.

توان k-ام گراف G را با G^k نشان‌داده و عبارتی است از گرافی با مجموعه رئوس $V(G^k) = V(G)$ و دو رأس در آن با هم مجاور هستند اگر و تنها اگر فاصله آن‌ها در G حداکثر k باشد.

اگر حداقل مقدار k برابر با قطر گراف باشد آن‌گاه توان k-ام گراف برابر با گراف کامل است. هم‌چنین برای یک رأس مانند x از گراف هم‌بند G و یک عدد صحیح و نامنفی k، مجموعه تمام رئوس به فاصله k را با نماد $N_k(x)$ نشان داده می‌شود. به عبارت دیگر:

$$N_k(x) = \{y \in V(G) : d(x,y) = k\}.$$

قضیه ۹: فرض کنید G یک گراف و k یک عدد صحیح مثبت است. در این صورت اگر گراف G فاصله متوازن باشد آن‌گاه توان k- ام آن G^k نیز فاصله متوازن است.

اثبات: فرض کنید xy یالی از گراف G^k است. در این صورت اگر xy یالی از گراف G باشد آن‌گاه مجموعه رئوس $N_k(x) \cup N_{2k}(x) \cup \ldots$ در $W_{xy}^{G^k}$ قرار دارد و بقیه مجموعه‌های $N_i(x)$ که در آن $i \neq lk$، در ${}_xW_y^{G^k}$ قرار دارند. به طریق مشابه، حکم برای هر یال در G^k برقرار است.

قضیه ۱۰ [۱۱، گزاره ۲]: فرض کنید C_n گراف دور با n رأس است. در این صورت C_n^2 دارای کد تام است اگر و تنها اگر n مضربی از ۵ باشد. به‌علاوه، چنین کدی دارای $\frac{n^2}{5}$ کدواژه است.

مکمل گراف G گراف $\bar{G}$ است که $V(\bar{G}) = V(G)$ و دو رأس در $\bar{G}$ مجاورند اگر و تنها اگر در G مجاور نباشند. در حالتی که گراف G و گراف $\bar{G}$ یک‌ریخت باشند، گراف را خودمکمل گویند. برای مثال گراف مسیر P_4 و دور C_5 چنین هستند. مجموعه $\{(v,v): v \in V(G)\}$ یک کد تام در $G \times \bar{G}$ است و لذا برای هر دو گراف G و H، گراف $G \times (H \times (\overline{G \times H}))$ دارای کد تام است. بنابراین، برای هر گراف G، نامتناهی گراف مانند H وجود دارد که $G \times H$ دارای کد تام است [۱۱].

قضیه ۱۱ [۱۱، گزاره ۳]: اگر G یک گراف خودمکمل با n رأس باشد، آن‌گاه G^2 شامل کدتام از اندازه n است.

۴- نتیجه‌گیری

کدهای تام به جهت آن‌که از نظر تصحیح خطا مناسب هستند، مورد توجه پژوهشگران در این حوزه می‌باشد. بدین منظور ما به معرفی دسته خاصی از این کدها به نام کدهای فاصله متوازن می‌پردازیم. فرض کنید C یک کد و $d(x,y)$ بیان‌گر فاصله بین کدواژه‌های x و y است. در این صورت گوییم x و y مجاورند اگر فاصله بین آن‌ها کمترین مقدار را داشته باشد. قرار دهید:

$$N_x(xy) = \{c \in C : d(c,x) < d(c,y)\},$$
$$N_y(xy) = \{c \in C : d(c,y) < d(c,x)\},$$
$$N_0(xy) = \{c \in C : d(c,x) = d(c,y)\}.$$

سه مجموعه فوق تشکیل یک افراز برای کد C می‌دهند. کد C را "کد فاصله متوازن" گوییم اگر و تنها اگر برای هر دو کد مجاور x و y داشته باشیم $N_x(xy) = N_y(xy)$. برای مثال فرض کنید C کد تام حاصل از گراف C_n برای $n = 3k$ است. در این صورت C فاصله متوازن خواهد بود.

۵- مراجع

[1] N. Biggs, "Perfect Codes in Graphs," J. Combin. Theory, Ser. B, vol. 15, pp. 289–296, 1973.

[2] F. J. MacWilliams and N. J. A. Sloane, "The Theory of Error-Correcting Codes," North-Holland, 8th impression, 1993.

[3] I. Dvorakova-Rulicova, "Perfect Codes in Regular Graphs," Comment. Math. Univ. Carolinae, vol. 29, pp. 79–83, 1988.

[4] K. Handa, "Bipartite Graphs with Balanced (a, b)-partitions," Ars Combin., vol. 51, pp. 113–119, 1999.

[5] J. Jerebic, S. Klavˇzar, and D. F. Rall, "Distance-Balanced Graphs," Ann. Combin. vol. 12, pp. 71-79, 2008.

[6] A. Ilić, S. Klavžar, and M. Milanović, "On Distance-Balanced Graphs," European Journal of Combinatorics, vol. 31, no. 3, pp. 733-737, 2010.

[7] S. Klavzar, S. Spacapan, and J. Zerovnik, "An Almost Complete Description of Perfect Codes in Direct Product of Cycles," Adv. in Appl. Math., vol. 37, no. 1, pp. 2-18, 2006.

[8] M. Mollard, "On Perfect Codes in Cartesian Product of Graphs," European Journal of Combinatorics, vol. 32, no. 3, pp. 398-403, 2010.

[9] J. Zerovnik, "Perfect Codes in Direct Products of Cycles, a Complete Characterization," Adv. in Appl. Math., vol. 41, no. 2, pp. 197-205, 2008.

[10] S. Spacapan, "Perfect Codes in Direct Products of Cycles," Electronic Notes in Discrete Mathematics, vol. 22, pp. 201-205, 2005.

[11] J. Kratochvil, "1-Perfect Codes over Self-Complementary Graphs," Comment. Math. Univ. Carolinae, vol. 26, pp. 589–595, 1985.

[12] J. H. VanLint, "Coding theory (Lecture Notes in Mathematics)," 1973.

مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"
ویژه‌نامه کنفرانس بین‌المللی ترکیبیات، رمزنگاری و محاسبات، ص ۲۹-۲۱

مبهم‌سازی کد با استفاده از تفسیر انتزاعی

محمدهادی علائیان[1*]، سعید پارسا[2]

۱- کارشناس ارشد، دانشگاه علم و صنعت ایران ۲- دانشیار، دانشگاه علم و صنعت ایران

(دریافت: ۹۵/۰۷/۰۵، پذیرش: ۹۶/۰۳/۰۷)

چکیده

هدف تبدیل امضاء کدها به قسمی که تحلیل توسط تفسیر انتزاعی امکان‌پذیر نباشد. تفسیر انتزاعی با خلاصه‌سازی کد، مفهوم کدها را استخراج می‌نماید. از این طریق، علی‌رغم تغییرات اعمال‌شده جهت تغییر شکل ظاهری و نهایتاً امضاء کد بدخواه، مفهوم استخراج و در قالب امضاء کد شناسایی می‌شود. که این ناکارامدی روش های مبهم سازی قبلی را نشان می‌دهد. در این مقاله، روشی برای مبهم‌سازی با تغییر شکل ظاهری کد اسمبلی مستخرج‌شده از کدهای اجرایی، ارایه شده که امکان تفسیر انتزاعی مجدد کد مبهم‌سازی‌شده را از میان بر می‌دارد. روش مبهم‌سازی پیشنهادی این مقاله مبتنی بر تفسیر انتزاعی است. تفسیر انتزاعی به‌طوری انجام خواهد شد که نتوان کد را مجدداً مورد تفسیر انتزاعی قرار داد. ارزیابی‌ها نشان داده که بعد از مبهم‌سازی بدافزارهای شناخته‌شده آنتی‌ویروس‌ها، براساس امضاء، قادر به تشخیص بدافزار مبهم‌سازی‌شده نیستند که نشان‌دهنده اهمیت مبهم‌ساز ارائه شده است.

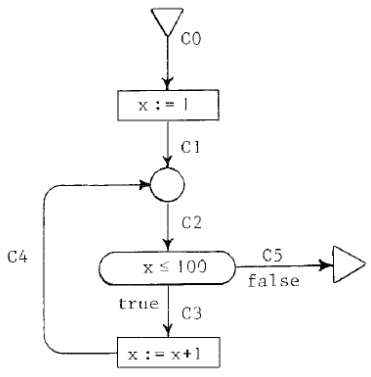
واژه‌های کلیدی: مبهم‌سازی کد، زبان اسمبلی، تحلیل ایستای بازه، تفسیر انتزاعی

۱- مقدمه

مبهم‌سازی یکی از حوزه‌های حفاظت از نرم‌افزار است ولی از طرف دیگر می‌توان با استفاده از این روش‌ها بدافزار جدیدی را با استفاده از نمونه بدافزار قبلی تولید کرد به طوری که بتوان از بدافزارها در برابر تحلیل حفاظت کرد. یک مبهم‌ساز سعی دارد کد را با تغییر حجم کد و افزایش میزان پیچیدگی در برنامه، کد برنامه به طوری پیچیده شود تا مهندسین معکوس نتوانند به‌راحتی کد را مورد بررسی قرار دهند. اولین بار مبهم‌سازی در مرجع [۱] تعریف شده است. فرض کنید $\mathbb{t}:\mathbb{P}\to\mathbb{P}$ یک انتقال‌دهنده برنامه باشد که کد منبع p را به کد انتقال‌یافته p' تبدیل می‌کند، اگر $\mathbb{t}$ یک انتقال‌دهنده کد، قوی باشد و p و p' یک رفتار را از خود نشان دهند؛ یعنی اگر p درجایی از کد به خطا منجر شد، p' نیز در همان‌جا به خطا منجر شود، در این صورت، $\mathbb{t}$ یک انتقال‌دهنده مبهم‌ساز است. منظور از قوی‌بودن، میزان پیچیدگی برنامه است که واحدهای آن می‌توان تعداد حلقه‌ها تودرتو و تعداد اشاره‌گرها در برنامه باشد. علاوه بر قوی‌بودن، شناسایی نشدن روش مبهم‌سازی، سربار (سربار زمانی و چه سربار حافظه) وارده به برنامه مبهم شده و رفع ابهام خودکار، ازجمله معیارهای روش‌های مبهم‌سازی هستند. در حالت کلی، بسته به نوع، روش‌های مبهم‌سازی به چهار دسته تقسیم‌بندی می‌شوند.

۱- مبهم‌سازی ساختاری: در این روش‌ها سعی می‌شود اطلاعات اضافی که به مهندسین معکوس در فهم بهتر و بیش‌تر برنامه کمک می‌کند مانند جملات توصیفی، نام توابع و متغیرها را حذف و یا تغییر دهند.

۲- مبهم‌سازی داده‌ای: هدف تغییر در ساختار داده‌ای برنامه است. با ترکیب و یا جداکردن آرایه‌ها، رمزگذاری بر روی متغیرها ازجمله کارهایی است که در این بخش انجام می‌شود.



شکل (۱): گراف جریان کنترلی به عنوان یک مثال ساده.

* رایانامه نویسنده مسئول: hadi_alaeiyan@comp.iust.ac.ir

۳- مبهم‌سازی کد: این روش سعی دارد تا با تغییردادن گراف جریان کنترلی و جابه‌جایی دستورات خوانایی و روند اجرایی کد را غیرقابل فهم کنند. ازجمله این روش‌ها نانومیتس[1]، ماشین مجازی و موازی‌سازی دستورات هستند.

۴- گزاره‌های مبهم: در این روش با اضافه‌کردن مسیرهای مختلف در کد اجرایی که هرگز این مسیرها در برنامه اجرای نمی‌شوند، سعی به گمراه‌سازی مهندسین معکوس می‌کنند. عموماً این مسیرها را با تولید شرط در برنامه به وجود می‌آورند و در مسیری از شرط، روند اصلی اجرایی برنامه و در دیگری، مسیر گمراه‌کننده قرار می‌گیرد. در اکثر موارد این دسته را زیردسته از مبهم‌سازی کد در نظر می گیرند.

تفسیر انتزاعی یکی از حوزه‌های مهم در تحلیل کد می‌باشد. از آن در حوزه‌های مختلف مانند شناسایی بدافزار، تست نرم‌افزار و موازی‌سازی، بهینه‌سازی کد و امنیت [۲] استفاده می‌گردد. تفسیر انتزاعی یک نظریه عمومی درباره تقریب معنای یک برنامه سیستمی برپایه توابع یک‌نواخت روی مجموعه مرتب جزئی، مخصوصاً مشبکه‌ها است [۳]. با استفاده از این روش می‌توان معنای برنامه را تقریب زد [۴] و معنای انتزاعی برنامه را به دست آورد. یکی از ویژگی‌های عالی این روش، قابلیت تحلیل بر روی همه مسیرهای برنامه است و مشکل انفجار مسیر[2] را ندارد. چون، تحلیل را به صورت ایستا انجام می‌دهد و قسمت‌های دارای حلقه را تقریب می‌زند. به عنوان نمونه این امر در شکل (۱) نشان داده شد.

اکثر روش‌های مبهم‌سازی، بدون اطلاع از درون برنامه، قادر به مبهم‌سازی خوبی برای یک برنامه نخواهند بود. به‌عنوان نمونه، برای استفاده از فن گزاره‌های مبهم در کد، در شرایط معمولی، در هرچند خط کد، یکی از شرایط $7y^2 + 1 \neq x^2$ یا از $3|x^3 - x$ و یا از $14|(3 * 7^{4x+1} + 5 * 4^{2x+1} - 5)$ استفاده می‌کنند و به دلیل همانندبودن این گزاره‌ها سریعاً قادر به تشخیص هستند و بعد از تشخیص، قابل بازگرداندن خواهند بود. لذا با استفاده از تولید خودکار شرط‌هایی که متناسب بامعنای برنامه هستند مانند x>10، ولی با تعداد بالا، چهار فایده خواهد داشت. اول، این شرط‌ها قادرند تا صحت برنامه را چک کنند (زیرا تشخیص داده‌شده که در این مسیر همواره x>10 است). دوم، متناسب با معنای برنامه هستند زیرا تشخیص داده شده که این متغیر در این قسمت از کد نقش کلیدی بازی می‌کند. پس، قابل تشخیص نیستند زیرا در بین دستوراتی مشابه پدیدار نخواهد بود. سوم، سربار زیادی ندارند و چهارم، قادر به تولید مسیر با تعداد بالا هستند که امکان پیچیده‌سازی بیش‌تری را می‌دهند. درنتیجه، همه این موارد موجب می‌شود تا از تفسیر انتزاعی در مبهم‌سازی استفاده شود تا یک مبهم‌سازی قوی‌تری ایجاد شود.

از تفسیر انتزاعی در مبهم‌سازی داده‌ای [۵]، گزاره‌های مبهم [۶] و مبهم‌سازی با استفاده از معنای برنامه [۷] نیز استفاده می‌شود. در مبهم‌سازی داده‌ای با تعریف دو تابع مبهم‌ساز و رفع مبهم‌ساز، سعی می‌شود تا متغیرهای خاصی را مبهم‌سازی کنند. با استفاده از روش گزاره‌های مبهم سعی می‌شود تا با استفاده از معنای کد، شرط تولید کنند و مسیرهای گمراه‌کننده جهت گمراه‌کردن مهندسین معکوس تولید کنند. بر اساس معنای برنامه، با استفاده از روش‌های بهینه‌سازی مانند انتشار ثابت سعی به پاک‌کردن قسمت‌هایی از الگوریتم و کد را دارند تا الگوریتم اصلی در برابر مهندسین معکوس از بین برود.

تحلیل ایستای بازه یک روش تفسیر انتزاعی است که با استفاده از آن می‌توان در هر خط از کد، مقدار بازه‌ای هر متغیر را به‌دست آورد [۸]. برای نمونه، اگر گراف جریان کنترلی شکل (۱) را در نظر داشته باشید، یال‌های این گراف جریان کنترلی که نگهدارنده اطلاعات محیط بلاک اولیه قبلی خود هستند و آن‌ها را با Ci نشان داده شده‌اند، i تعداد بلاک‌های اولیه در گراف جریان کنترلی است. هر محیط شامل اطلاعاتی از حالت برنامه را در خود نگهداری می‌کند. این اطلاعات از هر بلاک به بلاک بعدی انتقال داده می‌شود و اگر به الگوریتم ارائه‌شده در مرجع [۸] توجه کنید، برای مثال ارائه‌شده محیط‌های زیر را خواهید داشت. به عنوان مثال، C2 می‌گوید که اگر مسیر اجرایی برنامه را پیش برویم در یالی که C2 نام‌گذاری شده است مقدار x می‌تواند در بازه [1,100] باشد.

C0 = [,]; C1 = [1, 1]; C2 = [1, 101]; C3 = [1,100];

C4 = [2, 101]; C5 = [101, 101];

الگوریتم به این صورت است که محیط‌ها را از حالت‌های قبلی می‌گیرد، به ازای متغیرهای موجود در محیط‌های قبلی اجتماع می‌گیرد. محاسبات بلاک را اعمال می کند تا مقدار تقریبی حاصل گردد تا در اختیار بلاک بعدی قرار گیرد.

ایده اصلی برای انجام مبهم‌سازی اعمال تحلیل و شناسایی مقدار بازه‌ای متغیرهای مورد استفاده در شرایط تأثیرگذار کد را با توجه به مفهوم برنامه می‌توان دانست. برای این منظور، بر اساس بازه متغیرها شرایطی را می‌توان ایجاد نمود که در زمان

1- Nanomites
2- Path explosion

اجرا هیچ‌گاه برقرار نمی‌شوند. آن‌گاه تحت این‌گونه شرایط می‌توان هرگونه کدی را به برنامه اضافه نمود و اطمینان داشت که هرگز اجرا نمی‌گردد. نکته قابل توجه این است که بعد از یک‌بار مبهم‌سازی، دیگر کد با استفاده از تفسیر انتزاعی قابل‌بررسی و تحلیل ایستا نخواهد بود. هدف ما از مبهم‌سازی، مقابله با تحلیل ایستای کد اجرایی است. با استفاده از اطلاعات حاصل از تفسیر انتزاعی بازه بر روی زبان اسمبلی[1] می‌توان وضعیت ثبات حالت را دانست. در گراف جریان کنترلی برنامه، در انتهای هر بلاک اولیه، دستورالعمل‌های پرش بر اساس مقدار بیت‌ها در ثبات حالت درج می‌شود. با افزایش مسیرهای اجرایی متعدد و به‌خصوص ایجاد حلقه‌های اجرانشدنی در داخل کد، ردیابی بلاک‌های اولیه در کد برنامه‌ها بسیار مشکل می‌شود. پرش‌ها و کد زاید طوری به کد برنامه‌ها افزوده می‌شود که نتوان با استفاده از تفسیر انتزاعی آن‌ها را تشخیص داد. برای این منظور دنباله‌ای از پرش‌هایی که در آن‌ها مسیر نادرست که همواره مسیر نقیض پرش بعدی است، می‌تواند یک مبهم‌ساز داده‌ای و گزاره‌های مبهم، ایده‌آل و قوی بر روی زبان اسمبلی به‌دست آید تا از تحلیل ایستای بازه، شناسایی‌شدن و رفع ابهام خودکار جلوگیری کند.

در ادامه، در فصل دوم روش پیشنهادی توضیح داده خواهد شد و در فصل سوم به بررسی و ارزیابی روش پیشنهادی پرداخته خواهد شد و در فصل آخر نتیجه‌گیری مطرح خواهد شد.

۲- روش پیشنهادی

برای انجام مبهم‌سازی داده‌ای و گزاره‌های مبهم با استفاده از تفسیر انتزاعی برای کدهای اجرایی، نیاز است تا متناسب با معماری ارائه شده در شکل (۲) که در ادامه توضیح داده می‌شود، عمل نمود. در ادامه، متناسب با معماری، درباره تحلیل‌گر ایستای بازه بحث خواهد شد. هم‌چنین، روش پیشنهادی ارائه خواهد شد که در آن نیاز است تا طریقه تولید شرط‌ها و تولید مسیرهای گمراه‌کننده توضیح داده شود.

۲-۱- معماری مبهم‌سازی

در شکل (۲) معماری مطرح برای مبهم‌سازی کد نشان داده شده است. برای ایجاد یک مبهم‌سازی بر روی زبان اجرایی، نیاز است تا در ابتدا کد اجرایی به کد اسمبلی تبدیل شود. البته در تبدیل کد اجرایی به کد اسمبلی مشکلات زیادی از جمله وجود پرش‌های غیرمستقیم، اعمال تحلیل را دشوار می‌سازد ولی تا حد قابل قبولی، قابل حل است. حال گراف جریان کنترلی برنامه، از روی کد اسمبلی حاصل می‌شود [۱۰-۹]. از روی زبان اسمبلی، گراف جریان کنترلی استخراج می‌شود و تحلیل ایستای بازه بر روی گراف جریان کنترلی حاصله اعمال می‌گردد. تا محیط حالت‌های برنامه تقریب زده شوند. در نتیجه با استفاده از اطلاعاتی که در محیط وجود دارد، شرط‌ها و مسیرها تولید می‌شود و در نهایت کد به زبان ماشین جهت اجرا تبدیل می‌شود.

برای تبدیل کد اجرایی به کد اسمبلی از ابزارهای مختلفی مانند beengineer و یا dumpbin می‌توان استفاده کرد. هم‌چنین، برای تولید گراف جریان کنترلی می‌توان متناسب با مرجع [۱۱] عمل نمود. به‌علاوه، برای تحلیل ایستای بازه می‌توان از مرجع [۸] استفاده نمود. در این راستا، یک ابزار تحلیلگر ایستای بازه پیاده‌سازی شده است تا بتوان مبهم‌سازی جهت مقابله با تفسیر انتزاعی داشت. در ادامه، درباره روند انجام مبهم‌سازی توضیحاتی داده خواهد شد.

۲-۲- روش مبهم‌سازی

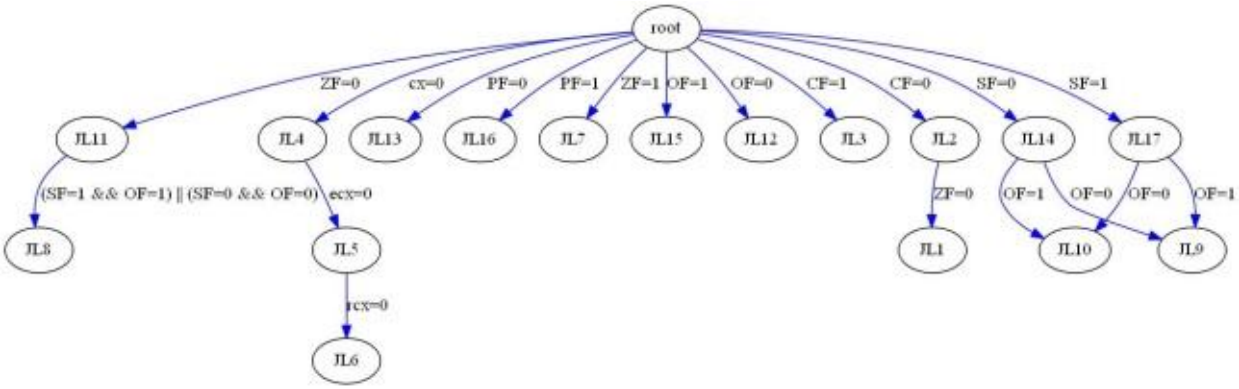
تحلیل ایستای بازه، اطلاعات زیادی از سطح کد در اختیار روش مبهم‌ساز قرار می‌دهد. از این اطلاعات می‌توان در تولید شرط استفاده نمود تا مسیرهای گمراه‌کننده در برنامه افزایش یابند. در هر قسمت از برنامه مقدار ثبات eax یک مقدار بازه‌ای [l, h] دارد و گاه مقدار h با مقدار l می‌تواند یکسان باشد که توسط تحلیل‌گر ایستای بازه استخراج می‌گردد. بازه‌های استخراج‌شده می‌تواند شرط‌های مختلفی از جمله "jge eax, l" را تولید کرد. برای گمراه‌کردن کاربران بدخواه و هم‌چنین تحلیل‌گر ایستا، بلاک اولیه‌ای باید تولید شود که نقیض معنایی شرط را تولید کند. یعنی بلاک اولیه‌ای تولید شود که eax در آن مقداری کم‌تر از l را به خود بگیرد و آن را ورودی به بلاک شرط تولیدشده، قرار دهید. در این صورت، تحلیل‌گر ایستای بازه مقدار 'l را به‌جای l در محیط مربوط به پرش تقریب خواهد زد که انتزاع بیش‌تر و صحت کم‌تری را خواهد داشت. در این صورت تمامیت نیز از بین خواهد رفت. اکنون دو مسیر ورودی به شرط و دو مسیر خروجی به شرط وجود دارد. مسیرهای ورودی، یکی مسیر اصلی و دیگری مسیر نقیض معنایی است. اگر مسیر اصلی را در نظر بگیرید، همواره eax در بازه [l, h] است، پس پرش همواره در مسیر درست صورت می‌پذیرد. مسیر نادرست شرط برای گمراه‌سازی کاربران بدخواه و هم‌چنین تحلیل‌گر ایستای بازه است. با اتصال آن به بلاک اولیه نقیض معنایی شرطی دیگر که به همین صورت ایجاد شده است، متصل خواهد شد. این عمل باعث می‌شود تا جای‌جای کد به هم وابستگی پیدا کنند و پیچیدگی برنامه بیش‌تر شود. این عمل چندین بار تکرار می‌شود تا شرط نهایی، خروجی از نقیض معنایی شرط دیگری شود.

1- Assembly

شکل (۲): معماری مبهم‌سازی کد اجرایی

۲-۳- تولید شرط از روی محیط

از روی محیط‌هایی که تحلیل‌گر ایستای بازه در اختیار قرار می‌دهد، پرش‌های شرطی به صورت خودکار استخراج خواهد شد. اگر دستورات پرشی را از مرجع [۱۲] مورد بررسی قرار دهید، جدول (۱) به دست خواهد آمد. این جدول بیان می‌کند که برای هر نوع پرش چه نوع محیطی در حالت‌های برنامه مورد نیاز است. بعد از تحلیل این جدول، اطلاعات موجود در شکل (۳) به دست خواهد آمد. این شکل بیان می‌کند اگر یک حالت داشته باشید که در محیط آن متغیرهای OF = 1 و SF=1 باشند، می‌توان برای اضافه‌کردن پرش در گراف جریان کنترلی از نوع‌های پرش موجود در ۱۵، ۱۷ و ۹ استفاده کرد.



شکل (۳): چارت وضعیت محیط یک حالت و نوع شرطی که می‌تواند به کار برود.

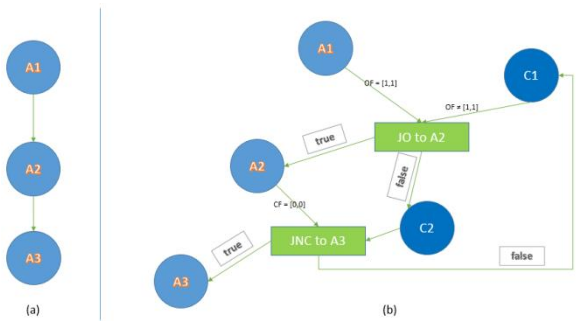
حال با استفاده از شکل (۳) بر روی هر محیطی می‌توان متناسب با مقدارهایی که دارد، پرش‌های شرطی تولید کرد. در ابتدا به صورت تصادفی از روی گراف جریان کنترلی یک محیط انتخاب می‌شود. در مرحله بعد، متناسب با شکل (۳)، لیستی از پرش‌های ممکن انتخاب می‌شود. از لیست پرش‌هایی که می‌توانند در محیط قرار بگیرند یکی به صورت تصادفی انتخاب می‌شود و به عنوان شرط بین دو بلاک اولیه مرتبط با محیط قرار می‌گیرد.

۲-۴- تولید مسیرهای گمراه‌کننده

در سمت راست شکل (۴) یک دنباله متناهی از دستورات را دارید که به صورت متوالی A1→A2→A3 در برنامه اصلی اجرا خواهند شد. فرض کنید با انجام تحلیل ایستای بازه مشاهده می‌شود که بعد از دستور A1 پرچم OF برابر بازه [1,1] و بعد از دستور A2 پرچم CF برابر بازه [0,0] است. در این صورت با توجه به شکل (۳) می‌توان نتیجه گرفت JO می‌تواند یکی از پرش‌های شرطی که همواره از مسیر درست بین A1→A2 عبور می‌کند، باشد. هم‌چنین، در مسیر A2→A3 نیز می‌تواند JNC را قرار داد. ملاحظه می‌شود که مسیر اصلی برنامه تغییر نکرده است چون، A1 به JO تغییر مسیر داده است، مقدار AF همواره برابر ۱ است پس می‌توان نتیجه گرفت که JO همواره به A2 می‌رود. همین‌طور برای پرش JNC نیز می‌توان اعمال کرد. برای این‌که تحلیل‌گر ایستای بازه، تقریب بالاتری داشته باشد. بلاک اولیه‌ای با نام C1 تولید می‌شود که در آن نقیض معنایی OF = 1 یعنی OF ≠ 1 را تولید کند تا تحلیل‌گر، نتیجه تحلیل را برای ورودی به پرش JO، مقدار OF را [0,1] به دست آورد. پس در تحلیل با اعمال تغییرات در همه مسیرها، تحلیلگر ایستای بازه یک تقریب بالاتر و یا نادرستی را نسبت به نتیجه اصلی خواهید داشت و در نتیجه، مجبور به تحلیل در هر دو مسیر شرط خواهد شد و از آن‌جایی که همواره مجبور به تولید حلقه خواهد شد و از آن‌جایی که تحلیل‌گر ایستا خواستار تقریب حلقه است، سپس، از صحت اولیه کاسته خواهد شد.

جدول (۱): شرط‌های لازم جهت پرش

نوع پرش	SF	PF	OF	SF=OF	RCX	ECX	CX	ZF	CF	
JA, JNBE								۰	۰	۱
JAE, JNC, JNB									۰	۲
JB, JNAE, JC, JBE, JNA									۱	۳
JCXZ							۰			۴
JECXZ, JCXZ						۰	۰			۵
JRCXZ, JECXZ, JCXZ					۰	۰	۰			۶
JBE, JNA, JE, JZ								۱		۷
JG, JNL				true				۰		۸
JGE, JNL				true						۹
JL, JNGE, JLE, JNG				false						۱۰
JNE, JNZ								۰		۱۱
JNO			۰							۱۲
JNP, JPO		۰								۱۳
JNS	۰									۱۴
JO			۱							۱۵
JP, JPE		۱								۱۶
JS	۱									۱۷



شکل (۴): نمونه‌ای از مبهم‌سازی

تولید نقیض شرط حائز اهمیت است. از طرفی نباید همواره یک دستور خاص ایجاد کرد. زیرا این عمل کمک به شناسایی زودتر روش می‌گردد. بهترین عمل استفاده از انتخاب‌های تصادفی است. زیرا از خود هیچ الگویی نشان نمی‌دهند. برای تولید نقیض معنایی به صورت تصادفی یک مجموعه از دستورات به صورت متوالی تولید می‌گردد. این دستورات توسط تحلیل‌گر ایستا، تحلیل می‌شوند و هر کدام که نقیض معنایی را تولید کرد می‌تواند مورد استفاده قرار گیرد.

۳- ارزیابی روش پیشنهادی

برای ارزیابی روش مبهم‌سازی ارائه‌شده، ابتدا تحلیل صحت و درستی روش مبهم‌سازی مورد بررسی قرار خواهد گرفت. در ادامه، تابع انتقال‌دهنده از لحاظ توانمندی، برگشت‌پذیری و هزینه اجرایی، ارزیابی می‌شود. در نهایت، با چندی از روش‌های دیگر مبهم‌سازی مقایسه خواهد شد.

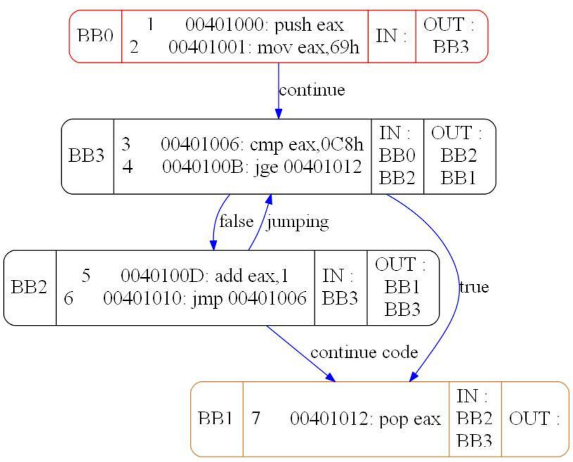
۳-۱- تحلیل صحت و درستی مبهم‌ساز

در مرجع [۶] نشان داده‌شده که چطور می‌توان با قراردادن مسیرهای گمراه‌کننده، بازهم ساختار اصلی برنامه را حفظ کرد. در نتیجه در این قسمت از لحاظ رسمی نشان داده خواهد شد که شرط‌هایی که در برنامه مبهم شده اضافه شده‌اند در مفهوم برنامه و روند اجرایی برنامه هیچ تغییری ایجاد نمی‌کنند.

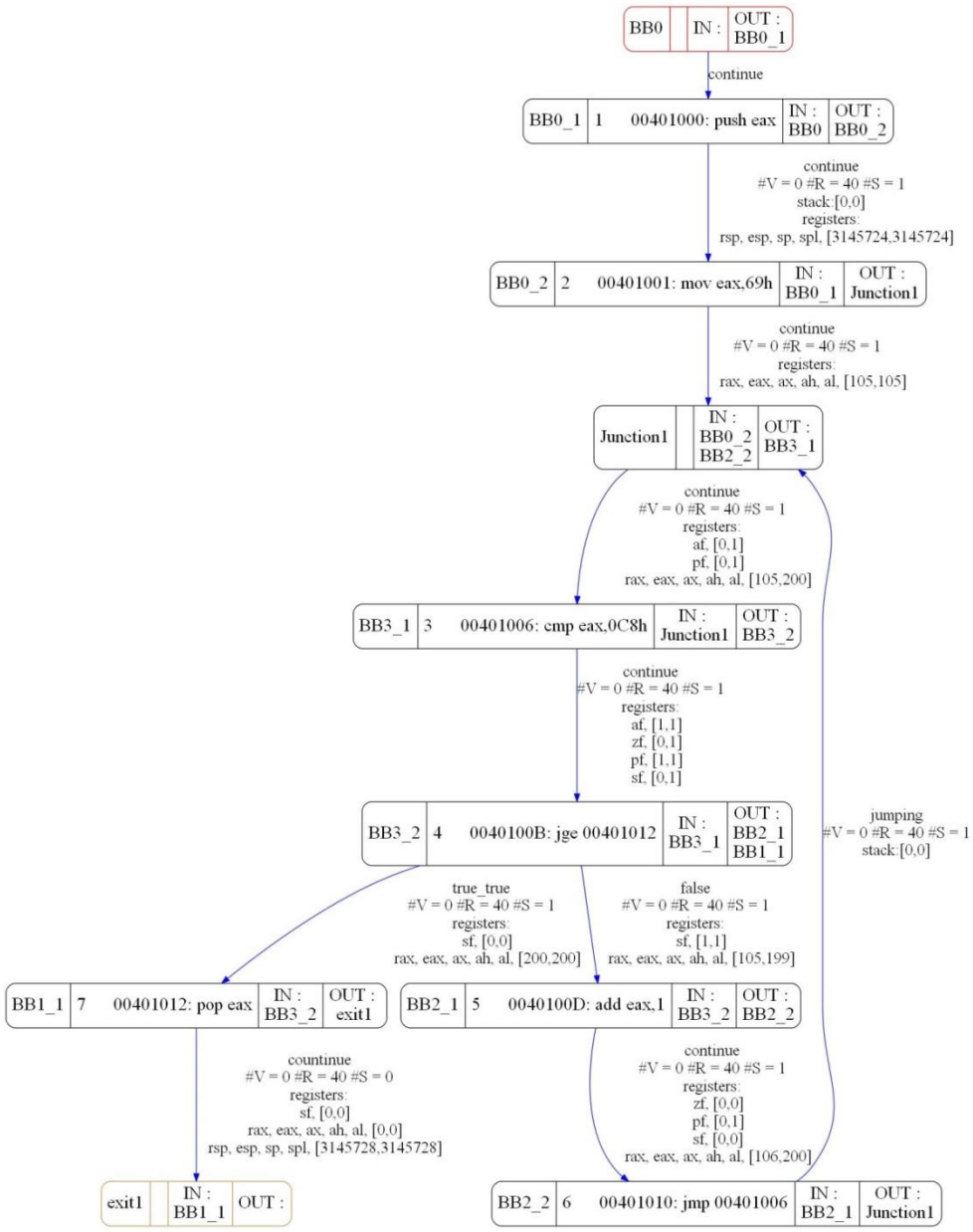
دنباله دستورات $\sigma = \langle \rho_0, C_0 \rangle ^\frown \langle \rho_1, C_1 \rangle ^\frown \langle \rho_2, C_2 \rangle ^\frown \langle \rho_3, C_3 \rangle ^\frown \langle \rho_4, C_4 \rangle$ را در نظر داشته باشید. که در آن، $\langle \rho_i, C_i \rangle$ یک حالت را نشان می دهد که C_i دستور مربطه و ρ_i محیط مربوط به این دستور می باشد. تابع انتقال‌دهنده، t^{ob}، بر روی مجموعه حالت‌های σ با داشتن $\ldots, \langle \rho_i, L_i: A_i \to L_{i+1} \rangle, \langle \rho_{i+1}, L_{i+1}: A_{i+1} \to L_{i+2} \rangle, \ldots, \langle \rho_j, L_j: A_j \to L_{j+1} \rangle,$ که j و i هیچ رابطه‌ای نسبت به هم ندارند، به صورت $t^{op}[\sigma, S^{op}[\![P]\!]] = \{ \langle \rho_i, L_i: A_i \to \tilde{L}_i \rangle, \langle \tilde{\rho}_i, \overline{L}_i: \overline{A}_i \to \tilde{L}_i \rangle, \langle \rho_i, \tilde{L}_i: P^T = tt \to L_{i+1} \rangle, \langle \rho_i, \tilde{L}_i: P^T = ff \to L_j \rangle \}$ عمل می‌کند و به حالت‌ها اضافه می‌کند. که در آن، $\tilde{\rho}_i$ نقیض معنایی ρ_i است که توسط دستورالعمل موجود در $\overline{A}_i$ تولید خواهد شد. مشاهده می‌شود با تکرار این روند، تغییری در روند اجرایی برنامه داده نخواهد شد و درستی تابع مبهم‌ساز t^{ob} نشان داده شده است.

۳-۲- ارزیابی تابع انتقال‌دهنده

برای به‌دست‌آوردن میزان ارزیابی توانمندی از معیارهای بسیاری استفاده می‌شود که در این‌جا از روش Cyclomatic complexity استفاده شده است. این روش میزان تو در تو بودن حلقه‌ها و وابستگی بین بلاک‌های اولیه را نشان می‌دهد. اگر به قطعه کد موجود در گراف جریان کنترلی ارائه‌شده در شکل (۵) توجه کنید، در ادامه شکل (۶) خروجی تحلیل‌گر ایستای بازه را نشان می‌دهد.



شکل (۵): گراف جریان کنترلی از نمونه کد جهت ارزیابی روش



شکل (۶): خروجی تحلیل ایستای بازه از گراف جریان گنترلی شکل (۵)

در هر خط، مقدار بازه‌ای متغیری که تغییر می‌کنند، نشان داده شده است. در نتیجه، گراف جریان کنترلی مبهم‌سازی‌شده نیز در شکل (۷) در سطح مبهم‌سازی ۱ ارائه شده است. منظور از سطح مبهم‌سازی تعداد دفعاتی است که مبهم‌سازی بر روی کد اعمال می‌شود. میزان پیچیدگی این قطعه کد را با سطح‌های مختلف مبهم‌سازی در جدول (۲) نشان داده شده است. پیچیدگی این قطعه کد قبل از مبهم‌سازی برابر دو بوده و با اعمال روش مبهم‌سازی همان‌طورکه در جدول نیز مشاهده می‌شود، با افزایش میزان سطح مبهم‌سازی پیچیدگی برنامه به شدت بالا خواهد رفت و با افزایش میزان پیچیدگی قدرت تحلیل برنامه پایین خواهد آمد و برنامه قابل تحلیل توسط کابران بدخواه نخواهد بود. همچنین، میزان شباهت کد با کد اصلی نیز با روش Cosine Similarity محاسبه شده است، با افزایش سطح مبهم-سازی این میزان شباهت کد با کد اصلی کم شده تا جایی که در سطح ۱۵، میزان شباهت کد مبهم شده با کد اصلی ٪۳۱/۶ می‌باشد که به نسبت یک مبهم‌سازی قوی ارائه شده است.

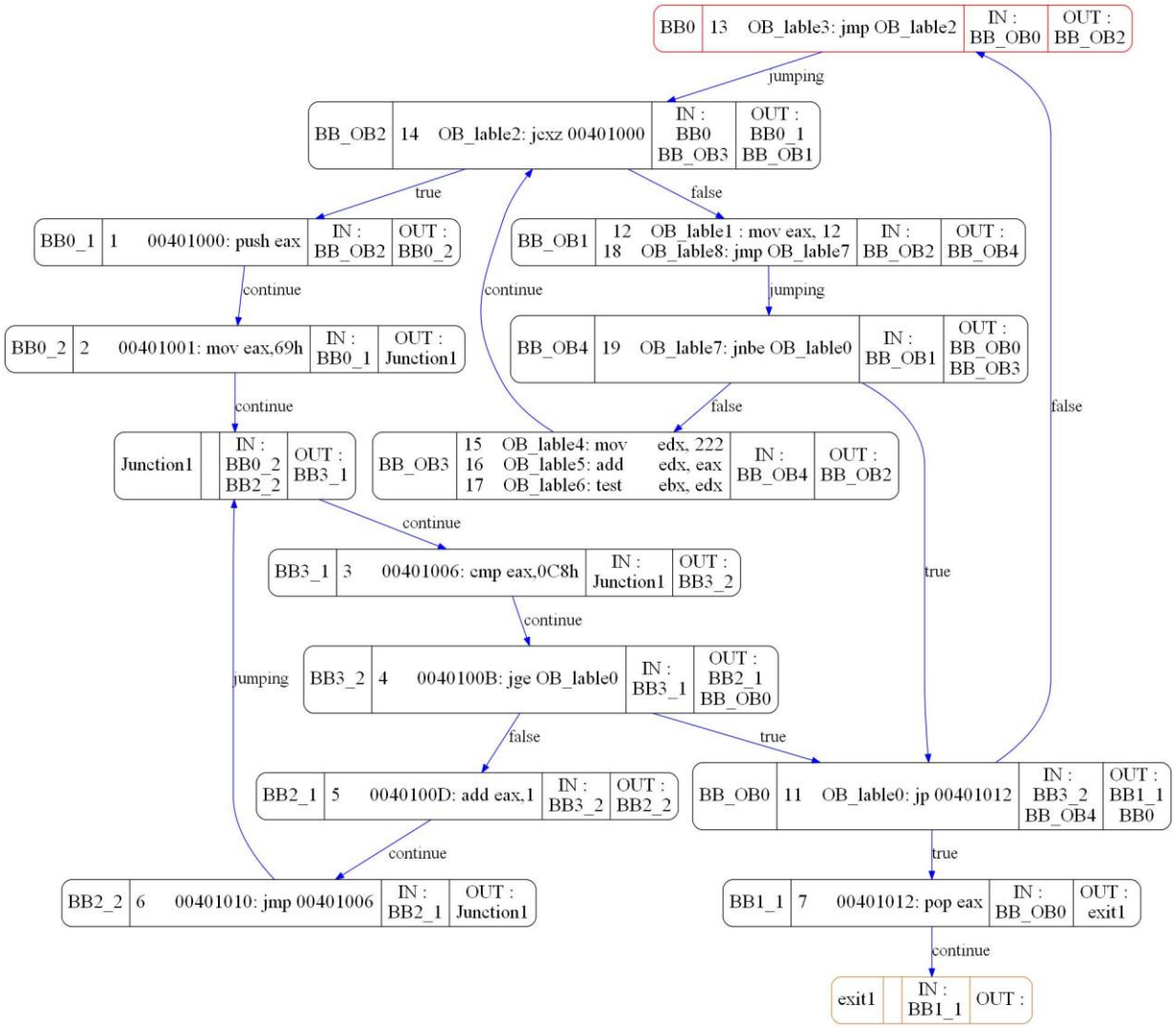
حجم کد، به میزان خطی که دارد، در سطوح مختلف مبهم‌سازی ارائه شده است که با افزایش سطح، حجم کد نیز افزایش یافته است. این درحالی است که در ابتدا کد ۷ خط بیش‌تر نداشته و ۷ خط کد در سطح ۱۵ به ۳۱۹ خط کد تبدیل شده است.

جدول (۲): جدول مقایسه میزان پیچیدگی و شباهت کد مبهم‌شده با کد اصلی از مثال شکل (۵)

سطح مبهم‌سازی	۱	۵	۱۰	۱۵
Cyclomatic complexity قبل از مبهم‌سازی	۲	۲	۲	۲
Cyclomatic complexity بعد از مبهم‌سازی	۵	۲۶	۳۷	۶۰
Cosine Similarity	۰/۷۳۳	۰/۳۴۷	۰/۳۳۰	۰/۳۱۶
Levenshtein Distance similarity	۷	۵۴	۶۰	۶۶
حجم کد به میزان خط	۱۶	۱۵۶	۱۹۶	۳۱۹

۳-۲-۱- ارزیابی برگشت‌پذیری

اگر به گراف جریان کنترلی ارائه شده در شکل (۷) توجه کنید، نمی‌توانید به راحتی بگویید که این کد چه کاری را انجام می‌دهد. در برنامه اصلی یک حلقه جهت افزایش مقدار eax وجود داشته، در حالی که در حال حاضر این عمل با پنج حلقه اجرا نشان داده شده است که در زمان اجرا وارد چهار حلقه دیگر هرگز نخواهد شد. برای برگرداندن این گراف جریان کنترلی به گراف جریان کنترلی اصلی نیاز است که پرش‌هایی که به برنامه اضافه شده‌اند را از برنامه حذف کنند.



شکل (۷): گراف جریان کنترلی مبهم‌شده گراف جریان کنترلی شکل (۵) در سطح ۱

به طور معمول، این عمل به چندین روش قابل انجام است، روش ایستا و پویا. در روش ایستا، یا از تحلیل‌گر ایستا استفاده می‌شود که همان‌طور که در شکل (۸) ملاحظه می‌شود نرم‌افزار IDA pro در تحلیل به دلیل وجود نقض معنایی در برنامه دچار مشکل شده و نقطه شروع دیگری را در برنامه پیدا کرده است. در نتیجه، باید خود کاربر بدخواه کار تحلیل را به‌صورت دستی انجام دهد. از آن‌جایی‌که روش، با ایجاد بلاک‌های مخالف مسیرهای شرطی مانند BB-OB1 و BB-OB3 که به‌ترتیب برای گمراه‌کردن

بلاک‌های اولیه BB-OB4 و BB-OB2 از شکل (۷) می‌باشند را تولید می‌کند، میزان دقت را برای انجام تحلیل ایستا پایین می‌آورد و کاربر نمی‌تواند به‌صورت خودکار مسیر اصلی را از مسیر فرعی تشخیص دهد و در نتیجه گراف جریان کنترلی اصلی برنامه مخفی می‌ماند. پس، این صبر و زمان بیش‌تری را برای تحلیل می‌خواهد و این نیز هدف مبهم‌سازی است.

شکل (۸): قسمتی از کد دیس اسمبل‌شده توسط ابزار IDA pro که مشاهده می‌شود که در تحلیل دچار خطا شده است.

در تحلیل پویا، کاربر با انجام عمل دیباگ[1]، پس از چندین بار طی‌کردن مسیرها می‌تواند متوجه شود که بعضی از شرط‌ها همواره به یک مسیر منتهی می‌شوند. با این عمل، با شک باز هم به‌صورت دستی با شناسایی تک‌تک شرط‌ها، می‌توانند آن‌ها را حذف کند. در نتیجه، به هدف خود که شناسایی نشدن و غیرقابل بازگشت بون به‌صورت خودکار، بوده، دست پیدا کرده‌ایم و هزینه و زمان را برای تحلیل‌گر بالا برده‌ایم.

۳-۳- مقایسه روش‌های مبهم‌سازی

در جدول (۳) معیارهای مبهم‌سازی کد با چندی از ابزارهای مبهم‌سازی معروف نشان داده‌شده است. به همه این روش‌ها مثال ارائه‌شده در شکل (۵) داده شده است. همان‌طورکه ملاحظه می‌شود، در سطح ۱۵ از مبهم‌سازی ارائه‌شده، میزان پیچیدگی‌ای که به برنامه ایجاد کرده است، ۶۰ می‌باشد که از همه روش‌های ارائه‌شده بیش‌تر است. هم‌چنین، میزان تشابه در کد نیز به‌خوبی نشان داده شده است. نکته دیگری که اهمیت بیش‌تری دارد میزان حجم کد است که هرچه کم‌تر باشد برتری دارد. اطلاعات نشان داده شده بیان می‌کند که متناسب با ابزارهای موجود روش ارائه‌شده یک مبهم‌سازی بهتر و بهینه‌تری را ارائه می‌کند.

جدول (۳): مقایسه روش پیشنهادی با ابزارهای مبهم‌سازی معروف

نام مبهم‌ساز	Agile .net	Babel Obfuscator	Crypto Obfuscator	روش ارائه‌شده
Cyclomatic complexity بعد از مبهم‌سازی	۳۰	۱۷	۲۳	۶۰
Cosine Similarity	۰/۴۶	۰/۳۰	۰/۴۲	۰/۳۱
حجم کد برحسب خط	۴۷۷۸	۱۲۶۵	۵۰۱۳	۳۱۹

۴-۳- مبهم‌سازی بر روی بدافزارها

جهت ارزیابی روش، چهار بدافزار مورد مبهم‌سازی قرار گرفتند که در جدول (۴) تعداد ضدبدافزارهایی که آن‌ها را قبل و بعد از مبهم‌سازی شناسایی کردند، نشان داده شده است. این بدافزارها با استفاده از سایت virustotal با ۵۵ نرم‌افزار ضدبدافزار استفاده شده است. همان‌طورکه نشان داده شد، می‌توان با استفاده از مبهم‌سازی بدافزارها، دوباره آن‌ها را مورد استفاده قرار داد.

جدول (۴): بدافزارهای شناسایی‌شده توسط نرم‌افزارهای ضدبدافزار و شناسایی نشدن آن‌ها بعد از مبهم‌سازی

نام بدافزار	تعداد تشخیص قبل از مبهم‌سازی	تعداد تشخیص بعد از مبهم‌سازی
Backdoor.Win32.Wabot.a	۴۹	۱
Net-Worm.Win32.Allaple.b	۵۲	۰
Email-Worm.Win32.Klez.k	۴۹	۰
HEUR:Trojan.Win32.Generic	۴۵	۱

۴- نتیجه‌گیری

با استفاده از اطلاعات به‌دست‌آمده از تحلیل ایستای بازه، در جاهای مختلف کد اسمبلی، به‌صورت تصادفی، شرط‌های پرشی اعمال می‌شود که بتوان با استفاده از آن، کد مد نظر را مبهم‌سازی کرد. هم‌چنین، با تولید نقیض‌های معنایی دقت تحلیل‌گر ایستای بازه را کاهش داد. در نهایت بررسی شد که این روش چقدر قدرت مقاومت در برابر کاربران بدخواه را دارد. هم‌چنین، بررسی شده در سطوح مختلف مبهم‌سازی به چه میزان کد قادر به مبهم‌سازی قوی‌تر و غیرقابل بازگشت به‌صورت خودکار است و نشان داده شده که چگونه کد برنامه دیگر قابل تحلیل توسط تحلیل‌گر ایستای بازه نیست. هم‌چنین، ابزارهای هوشمندی مانند IDA pro نیز قادر به تحلیل این کد نبوده و در تحلیل دچار مشکل می‌شوند.

1- Debug

۵- مراجع

[1] C. Collberg, C. Thomborson, and D. Low, "A taxonomy of obfuscating transformations," Technical Report 148, Dept. of Computer Science, The Univ. of Auckland, 1997.

[2] P. Cousot and R. Cousot, "Abstract interpretation: past, present and future," in Proceedings of the Joint Meeting of the Twenty, 2014.

[3] M. D. Preda, "Code Obfuscation and Malware Detection by Abstract Interpretation," Verona: Universit`a di Verona, 2005.

[4] P. Cousot and R. Cousot, "Systematic design of program transformation frameworks by abstract interpretation," in Proceedings of the 20th Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL '02), 2002.

[5] Y. Zeng and F. Liu, "Abstract Interpretation-based Formal Description of Data Obfuscation," in International Convference on Electonic & Mechanical Engineering and Information Technology, 2011.

[6] M. D. Preda and R. Giacobazzi, "Control code obfuscation by abstract interpretation," in Software Engineering and Formal Methods, SEFM, 2005.

[7] M. D. Preda and R. Giacobazzi, "Semantic-Based Code Obfuscation by Abstract Interpretation," Springer Berlin Heidelberg, 3580 (0302-9743), pp. 1325-1336, 2005.

[8] P. Cousot and R. Cousot, "Abstract interpretation: A unified lattice model for static analysis of programs by construction or approximation of fixpoints," in Proceedings of the 4th ACM Symp. On Principles of Programming Languages (POPL '77), New York. 1977.

[9] N. Hatwar and S. Nimbhorkar, "Disassembly Technique for Software by Teaching and Learning Algorithm," International journal of advenced research in computer engeenring and Technology, vol. 5, no. 4, 2016.

[10] B. Schwarz, S. Debray, and G. Andrews, "Disassembly of executable code revisited," in Ninth Working Conference on Reverse Engineering, 2002.

[11] K. D. Cooper, T. J. Harvey, and T. Waterm, "Building a Control-flow Graph from Scheduled Assembly Code," 2000.

[12] Intel, "Intel® 64 and IA-32 Architectures Software Developer's Manual," 2013.

مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"
ویژه‌نامه کنفرانس بین‌المللی ترکیبیات، رمزنگاری و محاسبات، ص ۳۸ -۳۱

مدل‌سازی و حل مسئله‌ی بازی امنیتی چندهدفی با استفاده از مسئله دوسطحی چندهدفی و کاربرد آن در امنیت مترو

حمید بیگدلی[1*]، حسن حسن‌پور[2]

۱- دانشجوی دکتری، ۲- استادیار، دانشگاه بیرجند

(دریافت: ۹۵/۰۷/۰۵، پذیرش: ۹۶/۰۳/۰۷)

چکیده

در این مقاله بازی‌های امنیتی چندهدفی بین یک مدافع و چند نوع مهاجم مورد مطالعه قرار گرفته است. هدف این مقاله انتخاب راهبرد بهینه مدافع با منابع امنیتی محدود در مقابل حملات احتمالی چند نوع مهاجم به اهداف مورد نظر است. بازی امنیتی چندهدفی مذکور به صورت یک مسئله دوسطحی چندهدفی فرموله شده است. سپس با استفاده از شرایط بهینگی کان- تاکر مسئله به یک مسئله چندهدفی یک سطحی تبدیل می‌شود و روش برنامه‌ریزی آرمانی برای حل آن پیشنهاد می‌گردد. در نهایت، کاربردی از این نوع بازی‌ها در ایجاد امنیت در ایستگاه‌های مترو ارائه می‌گردد.

واژه‌های کلیدی: نظریه بازی، بازی امنیتی، برنامه‌ریزی آرمانی، بهینه‌سازی دوسطحی چندهدفی

۱- مقدمه

در اکتبر سال ۱۹۶۲ اتحاد جماهیر شوروی با استقرار موشک‌های هسته‌ای در کوبا، امنیت آمریکا را تهدید کرد و آمریکایی‌ها خواستار لغو این عملیات شدند. آمریکایی‌ها گزینه‌های مختلفی را مورد بررسی قرار دادند. یکی از آن‌ها پیشنهاد نابودی موشک‌ها توسط حمله هوایی بود. اتخاذ این تصمیم ممکن بود منجر به حمله هسته‌ای شوروی علیه آمریکا شود. گزینه دیگر پیشنهاد محاصره دریایی بود که از استقرار موشک‌های بیش‌تر جلوگیری شود و حمله هوایی هم صورت بگیرد. به مدت چند روز دو کشور در حال بررسی گزینه‌های خود بودند. رئیس‌جمهور آمریکا محاصره دریایی را انتخاب کرد و در همان وقت برای حمله هوایی علیه کوبا آماده شد. پس از چند روز مذاکره، اتحاد جماهیر شوروی موشک‌هایش را برچید. این مسأله نمونه‌ای از اتفاقاتی است که در زندگی روزمره به دفعات با آن مواجه می‌شویم. چگونه وقتی از تصمیم طرف مقابل آگاهی نداریم، بهترین تصمیم را اتخاذ کنیم؟ نظریه بازی شاخه‌ای از تحقیق در عملیات است که رفتار ریاضی حاکم بر یک موقعیت راهبردی را مورد بررسی قرار می‌دهد. پس از انتشار کتاب نظریه بازی و رفتار اقتصادی توسط وان نیومن و مورگنسترن[1] [۱]، نظریه بازی به سرعت رشد یافت و کاربردهای وسیعی در علوم مختلف پیدا کرد. سرهنگ الیور هایوود[2] [۲] در مقاله خود اهمیت نظریه بازی را در تصمیم‌گیری فرماندهی نشان داد. او نبردهای مختلفی از جنگ جهانی دوم را از دید نظریه بازی بررسی کرد و نتیجه گرفت که تصمیم دکترین نظامی مشابه با جواب به دست آمده از نظریه بازی است. ارزیابی سرهنگ هایوود انجمن تحقیق در عملیات را تشویق کرد تا روش‌های نظریه بازی را بیش‌تر مورد بررسی قرار دهند و در تصمیم‌گیری‌های نظامی از این نظریه استفاده کنند. در دهه اخیر، نظریه بازی به طور گسترده در مسائل نظامی و امنیتی مورد استفاده قرار گرفته است [۳]. سناریوهای دزد و پلیس [۴]، امنیت شبکه‌های رایانه‌ای [۵]، نظام دفاع موشکی ضدبالستیک [۶] و تروریسم [۷] ازجمله این کاربردها هستند. اخیراً اقدامات کاربردی در این زمینه در کشور آمریکا و در شهرهای لس‌آنجلس و نیویورک صورت گرفته است [۳]. نظریه بازی به دو نوع بازی مهم طبقه‌بندی می‌شود: بازی‌های همکارانه و بازی‌های غیرهمکارانه [۸]. نویسندگان در کارهای قبلی [۱۱-۹] بازی‌های ماتریسی و دوماتریسی را در محیط فازی مورد بررسی قرار دادند و یک موقعیت در جنگ جهانی دوم را به صورت یک بازی ماتریسی با عایدی‌های فازی مدل‌سازی کرده و نشان دادند که راهبردهای به دست آمده از روش پیشنهادی با

* رایانامه نویسنده مسئول: h.bigdeli@birjand.ac.ir

1- Von Neumann and Morgenstern

2- Oliver Haywood

تصمیم دکترین آمریکا مطابقت دارد. هم‌چنین بازی مذاکرات هسته‌ای بین دو کشور را به صورت یک بازی دوماتریسی چندهدفی مدل‌سازی کرده و یک روش برای محاسبه نقاط تعادل کارای ضعیف آن ارائه دادند. در بسیاری از مسائل حوزه دفاع تصمیم‌گیری و انتخاب راهبرد از اهمیت ویژه‌ای برخوردار است. در این‌گونه مسائل، تصمیم‌گیری منطقی موجب افزایش کارایی نظام خواهد شد. در بسیاری از این مسائل، مدافع دارای منابع امنیتی محدود است و سعی دارد از حملات چندین مهاجم به اهداف جلوگیری کند. نظریه بازی روشی منطقی برای تخصیص منابع امنیتی به اهداف مورد نظر دشمن فراهم می‌کند. در این مقاله، بازی‌های امنیتی چندهدفی مورد بررسی قرار می‌گیرد. این نوع از بازی‌ها بین یک مدافع و چند نوع مهاجم انجام می‌گیرد. در این نوع از بازی‌ها به دنبال یافتن یک راهبرد بهینه برای مدافع هستیم. هدف از این تحقیق، ارائه یک روش برای محاسبه راهبرد بهینه مدافع است در شرایطی که منابع امنیتی مدافع برای حفاظت از اهداف محدود است و مدافع با چندین نوع مهاجم روبرو می‌شود. این نوع از بازی‌ها ممکن است در بسیاری از موقعیت‌های موجود در حوزه دفاع به کار گرفته شود. در این مقاله کاربردی از آن در ایجاد امنیت در ایستگاه‌های مترو بیان می‌شود. این بازی می‌تواند در مسائل امنیتی دیگری هم‌چون امنیت سایبری، امنیت مرزهای کشور و ... مورد استفاده قرار گیرد. بازی‌های امنیتی چندهدفی توسط گروه تحقیقاتی تامب[1] و همکارانش [۱۲] معرفی شد. این گروه در کار تحقیقاتی خود این نوع از بازی‌ها را معرفی کرده و کاربردهایی از آن را در دنیای واقعی نشان دادند. آن‌ها چندین هدف را برای تصمیم‌گیرنده اول در نظر گرفتند و لذا مسئله را به صورت مسئله بهینه‌سازی چندهدفی بیان کردند. در مقاله مذکور، مدل چندهدفی به دست آمده با فرض داشتن بهترین هدف برای تصمیم گیرنده دوم بیان شده است و هیچ روشی برای یافتن این هدف و در نتیجه محاسبه نقاط تعادل بازی ارائه نشده است و تنها به روش‌های حل مسئله چندهدفی پرداخته شده است. در این مقاله مسئله بازی امنیتی چندهدفی به صورت یک مسئله بهینه‌سازی چندهدفی دوسطحی مدل‌سازی می‌شود که تصمیم گیرنده اول در سطح بالا قرار داشته و با یک مسئله چندهدفی روبرو می‌شود و تصمیم‌گیرنده دوم در سطح پائین با یک مسئله تک هدفی روبرو خواهد شد. با نوشتن شرایط بهینگی در سطح دوم به دنبال محاسبه راهبرد کارا برای تصمیم‌گیرنده اول هستیم. این راهبرد نشان می‌دهد که مدافع با منابع امنیتی محدود خود چگونه حملات مهاجمان را به حداقل برساند. ادامه مقاله به صورت زیر سازمان‌دهی شده است. در بخش ۲ مفاهیم پایه‌ای از بازی‌های امنیتی و مسائل بهینه‌سازی دوسطحی و چندهدفی مطرح می‌شود. بخش ۳ به بازی‌های امنیتی چندهدفی می‌پردازد و یک روش برای یافتن راهبردهای رضایت‌بخش این مسائل ارائه می‌شود. در بخش ۴ کاربردی از این نوع بازی‌ها در ایجاد امنیت در ایستگاه‌های مترو مورد بررسی قرار می‌گیرد.

1- Tambe

۲- مفاهیم مقدماتی

در این بخش، مقدماتی از برنامه‌ریزی دوسطحی، بازی‌های امنیتی[2] و بهینه‌سازی چندهدفی بیان می‌شود.

بازی‌های استاکلبرگ[3] که بازی‌های رهبر- پیرو نیز نامیده می‌شوند اولین بار در سال ۱۹۵۲ میلادی توسط استاکلبرگ و براساس برخی از پدیده‌های انحصاری‌سازی در اقتصاد ارائه شد. در بازی‌های استاکلبرگ یک بازیکن به عنوان رهبر (پیشرو)[4] و بقیه به‌عنوان دنباله‌رو (پیرو)[5] عمل می‌کنند. بنابراین مسئله در این حالت در واقع یافتن راهبرد بهینه برای رهبر است با این فرض که پیروان مطابق با راهی منطقی براساس راهبرد رهبر، تابع هدف خود را بهینه می‌کنند. رهبر باید بداند که دنباله‌رو اعمال او را مشاهده می‌کند. یک دنباله‌رو نباید به هیچ وجه یک پیش‌رو غیراستاکلبرگ را لحاظ کند و پیش‌رو باید این را بداند. اگر پیش‌رو حرکتی داشته باشد، در این صورت نمی‌تواند آن‌را پس بگیرد و این به معنای تعهد به یک عمل است. بهتر است این بازی‌ها را با یک مثال امنیتی [۳] شرح دهیم. در یک حوزه امنیتی یک مدافع همواره باید از یک مجموعه از اهداف با توجه به منابع امنیتی محدود محافظت کند، درحالی‌که یک مهاجم قادر است از راهبردهای مدافع آگاهی یابد و بعد از تصمیمی هوشمندانه حمله کند. درصورتی‌که مدافع را در نقش پیش‌رو و مهاجم را در نقش دنباله‌رو فرض کنیم، این دقیقاً با بازی استاکلبرگ مطابقت دارد.

یک فرودگاه ساده با دو پایانه را در نظر بگیرید. فرض کنید تنها یک واحد پلیس امنیتی در این فرودگاه مستقر باشد و یک نوع دشمن داشته باشند. فرض می‌کنیم که پایانه ۱ مهم‌تر از پایانه ۲ باشد. ماتریس بازی به صورت زیر نمایش داده می‌شود:

جدول (۱): ماتریس عایدی

	پایانه ۱	پایانه ۲
پایانه۱	(۵و-۳)	(-۱و۱)
پایانه۲	(-۵و۵)	(۲و-۱)

2- Security games
3- Stuckelborg
4- Leader
5- Follower

اقداماتی که پلیس می‌تواند اتخاذ کند در سطرها و اقدامات دشمن در ستون‌های ماتریس نمایش داده شده است، یعنی پلیس می‌تواند یکی از دو پایانه را برای محافظت انتخاب کند و دشمن نیز یکی از دو پایانه را برای حمله در نظر خواهد گرفت. عایدی‌های حاصل از انتخاب جفت راهبردها در ماتریس بازی نمایش داده شده است و می‌توان نتیجه انتخاب جفت راهبردها را با هم مقایسه کرد. مولفه‌های اول و دوم به ترتیب نشان‌دهنده عایدی مدافع و مهاجم هستند. مولفه اول شاخصی کمی مربوط به قدرت پلیس در اقدام و مولفه دوم شاخصی کمی در قدرت دشمن در حمله است. به عنوان مثال، اگر دشمن پایانه ۱ را برای حمله انتخاب کند، با توجه به این‌که پلیس در پایانه ۱ حضور دارد لذا دشمن شکست سختی خواهد دید. این موقعیت با عایدی ۵ برای پلیس و ۳- برای دشمن نشان داده شده است که این مقادیر با توجه به سناریو و توسط افراد خبره در این زمینه تعیین می‌شود. توجه داشته باشید که عایدی‌ها توسط کارشناسان حوزه امنیت تعیین می‌شود که ممکن است نشان‌دهنده سود یا هزینه و ... باشند. برای به دست آوردن این داده‌ها می‌توان پرسش‌نامه‌ای را با توجه به مسئله مورد نظر تهیه کرد و با پاسخ‌دادن آن‌ها توسط متخصصین حوزه، نتیجه انتخاب راهبردها را کمی‌سازی کرد. با توجه به فرض مهم‌تربودن پایانه ۱ نسبت به ۲، اگر پلیس از پایانه ۱ محافظت کند، دشمن با این تصمیم پلیس به پایانه ۲ حمله می‌کند که یک شکست برای پلیس خواهد بود. حالت‌های دیگر را می‌توان از ماتریس بازی مورد بررسی قرار داده و نتیجه انتخاب راهبردها را بررسی کرد. حال فرض کنید اقدامات پلیس به صورت تصادفی باشد برای مثال پلیس در ۶۰٪ روزها در پایانه ۱ و در ۴۰٪ روزها در پایانه ۲ حضور داشته باشد. واضح است که در این صورت پلیس نتیجه بهتری خواهد گرفت. زیرا یک دشمن با رفتار هوشمندانه خواهد دانست که پلیس ۶۰٪ روزها در پایانه ۱ و ۴۰٪ روزها در پایانه ۲ حضور دارد ولی نمی‌تواند تشخیص دهد که فردا در کدام پایانه حضور دارند. در این نوع بازی راهبردهای پلیس به صورت تصادفی انتخاب می‌شود که آن‌ها را راهبردهای آمیخته پلیس می‌نامند و دشمن در مقابل این راهبرد با یک اقدام –یک حمله- واکنش خواهد داد. سوال کلیدی در این‌جا این است که آیا تقسیم ۶۰٪-۴۰٪ راه‌کار بهینه برای تقسیم منابع امنیتی مناسب است یا این تقسیم باید به صورت دیگری باشد؟

یکی از روش‌های حل این نوع از مسائل بازی، مدل‌سازی مسئله به صورت یک مسئله برنامه‌ریزی دوسطحی [۱۳] است. در مسائل برنامه‌ریزی دوسطحی ابتدا رهبر تصمیم خود را مشخص می‌کند و سپس پیرو با آگاهی از تصمیم رهبر تابع هدفش را بهینه می‌سازد. با توجه به این قاعده رهبر نیز تصمیم خود را طوری اتخاذ می‌کند که انتظار پاسخ معقول پیرو در مقابل تصمیمش را دارد. جواب به دست آمده به صورت روند فوق را جواب تعادل استاکلبرگ می‌نامند. یک مسئله برنامه‌ریزی دوسطحی برای محاسبه تعادل استاکلبرگ به صورت زیر نوشته می‌شود:

$$\underset{x}{maximize}\ z_1(x,y)=c_1x+d_1y$$

که y جواب مسئله زیر است

$$\begin{aligned}\underset{y}{maximize}\ & z_2(x,y)=c_2x+d_2y \\ & Ax+By\le b \\ & x\ge 0, y\ge 0\end{aligned} \qquad (1)$$

که در آن، به ازای $i=1,2$ ، c_i یک بردار سطری n_1 بعدی، d_i یک بردار سطری n_2 بعدی، ماتریس‌های ضرایب A و B به ترتیب ماتریس‌هایی $m\times n_1$ و $m\times n_2$ و b یک بردار ستونی m بعدی است. در مسئله برنامه‌ریزی دو سطحی (۱)، $z_1(x,y)$ و $z_2(x,y)$ به ترتیب نمایش‌دهنده توابع هدف رهبر و پیرو هستند و y,x به ترتیب نشان‌دهنده متغیرهای تصمیم رهبر و پیرو می‌باشند. فرض می‌شود که هر تصمیم گیرنده از تابع هدف و محدودیت‌های حریف آگاهی دارد. ابتدا رهبر تصمیم‌گیری می‌کند و سپس پیرو با آگاهی از تصمیم رهبر، تصمیم خود را اتخاذ می‌کند. یعنی پس از انتخاب راهبرد x توسط رهبر، پیرو مسئله برنامه‌ریزی خطی زیر را حل می‌کند:

$$\begin{aligned}\underset{y}{maximize}\ & z_2(x,y)=c_2x+d_2y \\ & By\le b-Ax \\ & y\ge 0\end{aligned} \qquad (2)$$

با حل این مسئله، جواب بهینه $y(x)$ به‌عنوان پاسخ منطقی پیرو به دست می‌آید. رهبر با این فرض که پیرو پاسخ منطقی $y(x)$ را خواهد داد تابع هدف $z_1(x,y(x))$ خود را بیشینه می‌کند. در این صورت، جواب به دست آمده را جواب استاکلبرگ گویند. برای حل این مسئله در روش کان- تاکر [۱۳] مسئله رهبر با محدودیت‌های شامل شرایط بهینگی کان- تاکر مسئله پیرو (۲) حل می‌شود. شرایط کان- تاکر برای مسئله (۲) به صورت زیر می‌باشد:

$$\begin{aligned} & uB-v=-d_2 \\ & u(Ax+By-b)-vy=0 \\ & Ax+By\le b \\ & y\ge 0, u^T\ge 0, v^T\ge 0\end{aligned} \qquad (3)$$

که در آن، u یک بردار سطری m بعدی و v یک بردار سطری n_2 بعدی است.

اکنون مسئله پیرو (۲) با شرایط (۳) جایگزین گردیده و مسئله برنامه‌ریزی دوسطحی (۱) به صورت معادل زیر که یک مسئله برنامه‌ریزی ریاضی یک سطحی است فرمول‌بندی می‌شود:

$$\begin{aligned} &maximize\ z_1(x,y) = c_1 x + d_1 y \\ &s.t. \quad uB - v = -d_2 && (۴) \\ &\quad u(Ax + By - b) - vy = 0 && (۵) \\ &\quad Ax + By \le b && (۶) \\ &\quad x \ge 0, y \ge 0, u^T \ge 0, v^T \ge 0 && (۷) \end{aligned}$$

از محدودیت‌های (۴) و (۵) می‌توان v را حذف کرد و محدودیت تساوی (۵) را به صورت زیر نوشت که شرایط کمبود مکمل نام دارند.

$$u(b - Ax - By) + (uB + d_2)y = 0 \qquad (۸)$$

فرض کنید A_i و B_i به ترتیب بردارهای سطری iام ماتریس A و B و B^j و d_{2j} به ترتیب بردار ستونی j ام ماتریس B و عنصر j ام بردار d_2 باشند. رابطه (۹) به صورت زیر نوشته می‌شود:

$$\sum_{i=1}^{m} u_i (b_i - A_i x - B_i y) + \sum_{j=1}^{n} y_j (uB^{2j} + d_{2j}) = 0 \qquad (۹)$$

که با توجه به قیود (۳) و (۴) با معادلات زیر معادل است:

$$\begin{aligned} &u_i (b_i - A_i x - B_i y) = 0 \qquad i = 1, \ldots, m \\ &y_j (uB^{2j} + d_{2j}) = 0 \qquad j = 1, \ldots, n_2 \end{aligned}$$

لذا شرط $u_i = 0$ یا $b_i - A_i x - B_i y = 0$ برای $i = 1, \ldots, m$ و شرط $uB^j + d_{2j} = 0$ یا $y_j = 0$ برای $j = 1, \ldots, n_2$ باید به‌طور هم‌زمان برقرار باشند. با معرفی بردارهای $w_1 = (w_{11}, \ldots, w_{1m})$ و $w_2 = (w_{21}, \ldots, w_{2n_2})$، با مولفه‌های صفر یا یک، این شرایط به صورت زیر بیان می‌شود:

$$\begin{aligned} &0 \le u \le M w_1 \\ &0 \le b - Ax - By \le M(e - w_1^T) \\ &0 \le uB + d_2 \le M w_2 && (۱۰) \\ &0 \le y \le M(e - w_2^T) \end{aligned}$$

که در آن، e یک بردار m بعدی با مولفه‌های یک و M یک مقدار ثابت بزرگ است. بنابراین مسئله برنامه‌ریزی ریاضی (۴) با مسئله برنامه‌ریزی صفر- یک آمیخته زیر معادل است.

$$\begin{aligned} &maximize\ z_1(x,y) = c_1 x + d_1 y \\ &s.t. \quad 0 \le u^T \le M w_1^T \\ &\quad 0 \le b - Ax - By \le M(e - w_1^T) && (۱۱) \\ &\quad 0 \le (uB + d_2)^T \le M w_2^T \\ &\quad 0 \le y \le M(e - w_2^T) \\ &\quad x \ge 0 \end{aligned}$$

اکنون توضیح مختصری در مورد بهینه‌سازی چندهدفی ارائه می‌دهیم. در حالت کلی یک مسئله بهینه‌سازی چندهدفی به صورت زیر بیان می‌شود:

$$\begin{aligned} &\max\ f(x) = (f_1(x), \ldots, f_k(x)) \\ &\text{s.t.}\ \ x \in X \end{aligned}$$

اگر بخواهیم مفهوم بهینگی جواب مسئله برنامه‌ریزی تک‌هدفی را برای این مسئله نیز به کار بریم تعریف زیر را خواهیم داشت.

تعریف۲-۱- اگر به ازای هر $x \in X$ و $i = 1, \ldots, k$، نقطه $x^* \in X$ را جواب بهینه کامل مسئله فوق می‌نامند.

با توجه به این‌که چنین جوابی همواره وجود ندارد، به ویژه زمانی‌که اهداف در تقابل یک‌دیگر باشند، مفهوم کارایی به صورت زیر تعریف می‌شود.

تعریف۲-۲- نقطه $x^* \in X$ را جواب کارای مسئله چندهدفی فوق گویند هرگاه نقطه دیگری مانند $x \in X$ موجود نباشد به طوری که به ازای هر $i = 1, \ldots, k$، $f_i(x^*) \le f_i(x)$ و برای حداقل یک j، $f_j(x^*) \ne f_j(x)$.

۳- بازی امنیتی چندهدفی

بازی امنیتی چندهدفی یک بازی چندنفره بین یک مدافع و n نوع مهاجم است. مدافع سعی دارد با استفاده از m منبع یکسان امنیتی از اهداف $T = \{1, 2, \ldots, p\}$ محافظت کند که m منبع به صورت پیوسته بین اهداف قابل توزیع است. راهبرد مدافع را می‌توان به صورت یک بردار پوشش $c = (c_1, \ldots, c_p)$ نشان داد که در آن به ازای $k = 1, \ldots, p$ c_k مقدار پوشش داده شده از هدف k است و احتمال موفقیت مدافع را در جلوگیری از هر حمله‌ای به هدف k نشان می‌دهد. در این مسئله فرض می‌شود که هزینه پوشش هر هدف با منابع در

دسترس، یکسان است. تقسیم این منابع به صورت محض برای مدافع مناسب نخواهد بود زیرا در این حالت ممکن است برخی اهداف را پوشش ندهد و مهاجمان از این نقطه ضعف برای حمله به این اهداف استفاده کنند. بنابراین، مدافع راهبردهای آمیخته را در نظر می‌گیرد که در آن منابع به مجموعه بزرگ‌تری از اهداف تخصیص می‌یابند. این در حالی است که مهاجمان قادرند این راهبردهای آمیخته را مشاهده کنند. فضای راهبرد مدافع به صورت زیر نمایش داده می‌شود:

$$C=\left\{c=(c_1,\ldots,c_p)\,|\,0\le c_k\le 1,\ \sum_{k=1}^{p}c_k\le m\right\} \qquad (۱۲)$$

راهبرد آمیخته برای مهاجم نوع i با بردار $a_i=(a_i^1,a_i^2,\ldots,a_i^p)$ نمایش داده می‌شود که در آن a_i^k احتمال حمله مهاجم نوع i به هدف k است. لذا فضای راهبرد مهاجم نوع i به صورت زیر نمایش داده می‌شود:

$$A=\left\{a_i=\left(a_i^1,a_i^2,\ldots,a_i^p\right)\,|\,a_i^k\ge 0,\ \sum_{k=1}^{p}a_i^k=1\right\} \qquad (۱۳)$$

فرض کنید $U_i^{c,d}(k)$ نشان‌دهنده مطلوبیت مدافع باشد زمانی‌که k توسط مهاجم نوع i انتخاب شده باشد و از طرف مدافع پوشش داده شده باشد. اگر k پوشش داده نشده باشد جریمه مدافع با $U_i^{u,d}(k)$ نمایش داده می‌شود. مطلوبیت مهاجم به طور مشابه با $U_i^{c,a}(k)$ و $U_i^{u,a}(k)$ نمایش داده می‌شود. در حقیقت در این مدل بازی برای هر هدف k، چهار عایدی وجود دارد که دو عایدی برای مدافع در دو حالت پوشش و عدم پوشش هدف، و دو عایدی برای مهاجم نوع i در این دو حالت می‌باشد.

برای یک نمایه راهبرد $\langle c,a_i\rangle$ در بازی بین مدافع و مهاجم نوع i، مطلوبیت‌های مورد انتظار برای دو بازیکن به ترتیب به صورت زیر می‌باشد:

$$U_i^d(c,a_i)=\sum_{k=1}^{p}a_i^kU_i^d(c_k,k), \qquad (۱۴)$$

$$U_i^a(c,a_i)=\sum_{k=1}^{p}a_i^kU_i^a(c_k,k), \qquad (۱۵)$$

که در آن،

$$U_i^d(c_k,k)=c_kU_i^{c,d}(k)+(1-c_k)U_i^{u,d}(k) \qquad (۱۶)$$

$$U_i^a(c_k,k)=c_kU_i^{c,a}(k)+(1-c_k)U_i^{u,a}(k) \qquad (۱۷)$$

به ترتیب عایدی دریافت‌شده مدافع و مهاجم نوع i هستند، درصورتی‌که به هدف k حمله شده باشد و به مقدار c_k پوشش داده شده باشد.

در این بازی ابتدا مدافع تصمیم خود را اتخاذ می‌کند. وی در تصمیم‌گیری خود n نوع مهاجم را لحاظ کرده و به دنبال بیشینه‌سازی مطلوبیت‌هایش در برابر انواع مهاجمان است. او می‌خواهد منابع خود را به گونه‌ای تخصیص دهد که بتواند حتی‌الامکان اهداف را در مقابل انواع مهاجمان پوشش دهد. مهاجم نوع i از این تصمیم مدافع آگاهی دارد و پاسخی منطقی به این تصمیم خواهد داد. یعنی پس از مشاهده تصمیم مدافع بهترین هدف را برای حمله انتخاب می‌کند. بنابراین بازی امنیتی مذکور را می‌توان با مسئله برنامه‌ریزی دو سطحی زیر فرمول‌بندی کرد.

$$\begin{aligned}
&\max_{c}\ \left(U_1^d(c,a_1),\ldots,U_n^d(c,a_n)\right)\\
&s.t.\ \ \sum_{k=1}^{p}c_k\le m\\
&\quad 0\le c_k\le 1,\ k=1,\ldots,p\\
&\quad \max_{a_i}\ U_i^a(c,a_i) \qquad (۱۸)\\
&\quad s.t.\ \sum_{k=1}^{p}a_i^k=1\\
&\quad\quad a_i^k\ge 0,\ k=1,\ldots,p
\end{aligned}$$

با ثابت نگه‌داشتن سیاست بهینه c مدافع، مسئله بهینه‌سازی مهاجم نوع i که یک پاسخ بهینه در مقابل تصمیم c خواهد داد به صورت زیر بیان می‌شود:

$$\begin{aligned}
&\max\ \ U_i^a(c,a_i)\\
&s.t\ \ \ \sum_{k=1}^{p}a_i^k=1 \qquad (۱۹)\\
&\quad\ a_i^k\ge 0\ \ k=1,\ldots,p
\end{aligned}$$

بنابراین برای راهبرد c مدافع، پاسخ بهینه a_i مهاجم نوع i در شرایط بهینگی زیر صدق می‌کند:

$$\begin{aligned}
&v^i\ge(c_kU_i^{c,a}(k)+(1-c_k)U_i^{u,a}(k)),\ k\in T\\
&a_i^k\,(v^i-(c_kU_i^{c,a}(k)+(1-c_k)U_i^{u,a}(k)))=0,\ k\in T\\
&\sum_{k=1}^{p}a_i^k=1 \qquad (۲۰)\\
&a_i^k\ge 0,\ k\in T
\end{aligned}$$

بنابراین، با درنظر گرفتن n مهاجم، برای مدافع مسئله بهینه‌سازی چندهدفی زیر را خواهیم داشت:

$$\max\ (U_1^d(c,a_1),\ldots,U_n^d(c,a_n))$$

$$s.t.\ \sum_{k=1}^{p} c_k \le m$$

$$v^i - (c_{t_k} U_i^{c,a}(k) + (1-c_k)U_i^{u,a}(k)) \ge 0$$

$$, k \in T, i = 1,\ldots,n$$

$$0 \le a_i^k \le M\delta_i^k \quad , k \in T, i = 1,\ldots,n$$

$$0 \le v^i - (c_k U_i^{c,a}(k) + (1-c_k)U_i^{u,a}(k)) \le$$

$$(e-\delta_i^{t_k})M \quad k \in T, i = 1,\ldots,n \qquad (۲۱)$$

$$\sum_{k=1}^{p} a_i^k = 1 \quad i = 1,\ldots,n$$

$$v^i \in \mathbb{R}, \delta_i^k \in \{0,1\} \quad i = 1,\ldots,n, k = 1,\ldots,p$$

$$a_i^k \ge 0 \quad k = 1,\ldots,p$$

$$0 \le c_k \le 1 \quad k = 1,\ldots,p$$

که در آن، M یک مقدار ثابت بزرگ است.

برای حل مسئله بهینه‌سازی چندهدفی (۲۱) روش‌های مختلفی ارائه شده است [۱۴]. ما روش برنامه‌ریزی آرمانی را برای حل این مسائل پیشنهاد می‌کنیم. در این روش، ابتدا از تصمیم‌گیرنده خواسته می‌شود تا آرمان خود را برای هر هدف ($\hat{g}_i, i = 1,\ldots,n$) ارائه کند. درصورتی‌که تصمیم‌گیرنده نتواند این‌کار را انجام دهد n مسئله تک‌هدفی را حل کرده و از مقادیر بهینه به‌دست‌آمده در معرفی آرمان‌های مدافع برای اهداف کمک می‌گیریم. پس از ارائه آرمان‌ها، مسئله‌ای به صورت زیر خواهیم داشت که یک مسئله بهینه‌سازی تک‌هدفی صفر- یک آمیخته است و با روش شاخه و کران [۱۵] قابل حل است.

$$\min \sum_{i=1}^{n} w_i \left(d_i^+ + d_i^-\right)$$

$$s.t \quad \sum_{k=1}^{p} c_k \le m$$

$$0 \le a_i^k \le M\delta_i^k \quad k \in T, i = 1,\ldots,n$$

$$0 \le v^i - (c_k U_i^{c,a}(k) + (1-c_k)U_i^{u,a}(k)) \le$$

$$\left(e-\delta_i^{t_k}\right)M \quad k \in T, i = 1,\ldots,n \qquad (۲۲)$$

$$\sum_{k=1}^{p} a_i^k = 1 \quad i = 1,\ldots,n$$

$$v^i \in \mathbb{R}, \delta_i^k \in \{0,1\} \quad i = 1,\ldots,n, k \in T$$

$$U_i^d(c,a_i) + d_i^+ - d_i^- = \hat{g}_i \quad i = 1,\ldots,n$$

$$0 \le c_k \le 1 \quad k = 1,\ldots,p$$

$$d_i^+, d_i^- \ge 0 \quad i = 1,\ldots,n$$

که در آن، d_i^+ و d_i^- به ترتیب متغیرهای انحرافی بیش‌تر از آرمان و کم‌تر از آرمان می‌باشند. به عبارت دیگر:

$$d_i^+ = \begin{cases} U_i^d - \hat{g}_i & U_i^d \ge \hat{g}_i \\ 0 & U_i^d \le \hat{g}_i \end{cases}$$

و

$$d_i^- = \begin{cases} \hat{g}_i - U_i^d & \hat{g}_i \ge U_i^d \\ 0 & \hat{g}_i \le U_i^d \end{cases}$$

وزن w_i نشان‌دهنده اهمیت تابع هدف ام ($i = 1,\ldots,n$) است. جواب به دست آمده از این مسئله یک جواب رضایت بخش برای مدافع می‌باشد.

۴- کاربرد بازی امنیتی چندهدفی در امنیت مترو

حوزه‌های امنیتی مختلفی در جهان واقعی وجود دارد که در زمان تصمیم‌گیری در مورد یک سیاست امنیتی، چندین هدف را مدنظر قرار می‌دهند. در این بخش می‌خواهیم یک کاربرد از بازی‌های امنیتی چندهدفی را برای تصمیم‌گیری در زمینه حفاظت از ایستگاه‌های مترو ارائه دهیم.

مترو شامل چندین ایستگاه است و روزانه هزاران مسافر را جابه‌جا می‌کند. در کل، در مترو سه نوع مهاجم با اهداف مشخص می‌تواند شناسایی شود. مسافران بی بلیط، مجرمان و تروریست‌ها. تعداد قابل ملاحظه‌ای از اقدامات امنیتی ممکن است در مترو وجود داشته باشد مانند استفاده از دوربین‌ها، گشت‌ها و بازرسی‌های تصادفی. بنابراین، بهتر است به نحوه تخصیص نیروهای امنیتی محدود برای حفاظت از ایستگاه‌های مترو بپردازیم تا بیش‌ترین امنیت در مترو برقرار شود. سه نوع مهاجم متفاوت در این مسئله مشاهده می‌شود که ترجیحات مختلفی دارند و ممکن است پاسخ‌های متفاوتی داشته باشند. به عنوان مثال، مسافران بی‌بلیط معمولاً ایستگاه‌های شلوغ را انتخاب می‌کنند و بیش‌تر مجرمان ایستگاه‌های خلوت را برای رسیدن به هدف‌شان برمی‌گزینند. تروریست‌ها ممکن است برای رسیدن به اهداف سیاسی خود به ایستگاه‌هایی ضربه بزنند که از لحاظ اقتصادی و فرهنگی اهمیت داشته باشند. هم‌چنین، مسئولین امنیتی (مدافع) ممکن است راهبردهای متفاوتی برای جلوگیری از هر نوع مهاجم داشته باشند. ورود مسافران بی‌بلیط هزینه‌ای را برای مترو به دنبال دارد. مدافع با استقرار سیاست‌های امنیتی در برابر مسافران بی‌بلیط از هزینه از دست رفته جلوگیری خواهد کرد. میزان صدمه به اموال و جرائم خشونت‌آمیز توسط مجرمان نیز هزینه بالایی برای مترو خواهد داشت و باعث ایمنی پائین و

درنتیجه کاهش مسافران خواهد شد. تجاوز، سرقت، قتل و ... از جمله این جرائم است. تهدیدات تروریست‌ها ما را بر آن می‌دارد تا سیاست امنیتی خاصی برای مقابله در این خصوص اتخاذ کنیم چراکه در بیش‌تر حملات تروریستی در کشورهای مختلف، تروریست‌ها مترو را یکی از اهداف خود قرار داده‌اند. علی‌رغم احتمال نسبتاً کم‌حمله تروریستی، اقدامات امنیتی طراحی‌شده در این زمینه با توجه به تعداد قابل توجه افراد در معرض خطر همواره باید یک اولویت باشد. مسئولین امنیتی نیاز است تا تمام تهدیدات اعمال‌شده توسط انواع مهاجمان را به منظور ارائه راهبرد امنیتی موثر در نظر بگیرند. بنابراین، دفاع در مقابل هر نوع مهاجم می‌تواند به عنوان یک هدف برای مدافع در نظر گرفته شود، درحالی‌که این اهداف کاملاً متضاد نیستند. به عنوان مثال، اقدام در مقابل مسافران بی‌بلیط ممکن است از وقوع جرم نیز بکاهد. البته با تمرکز زیاد بر روی یک مهاجم ممکن است مهاجم دیگر نادیده گرفته شود. بنابراین، نیاز است تا مسئولین امنیتی منابع امنیتی محدود خود را در این ایستگاه‌ها طوری تخصیص دهند که امنیت مترو بالاتر رود. با توجه به مطالب بخش قبل، برای مقابله با سه نوع مهاجم با یک مسئله بهینه‌سازی چندهدفی روبرو خواهیم شد که روش‌های متفاوتی برای حل این نوع مسئله وجود دارد و روش حل را می‌توان با توجه به همکاری‌های نظام امنیتی انتخاب کرد. با حل این مسئله، راهبردهای آمیخته‌ای را می‌یابیم که راهبردهای کارای امنیتی مدافع نامیده می‌شوند؛ به این معنی که راهبرد دیگری را نمی‌توان یافت که تمامی اهداف به خوبی آن‌ها عمل کرده و حداقل یک هدف بهتر از آن‌ها باشند. البته با استفاده از روش برنامه‌ریزی آرمانی به یک جواب رضایت بخش برای مدافع دست می‌یابیم. اکنون فرض کنید بازی امنیتی مذکور بین مسئولین امنیتی (مدافع) و سه نوع مهاجم (مسافران بی‌بلیط، مجرمان و تروریست‌ها) با درنظرگرفتن دو ایستگاه مترو و یک منبع امنیتی به صورت جداول (۴-۲) نمایش داده شود:

جدول (۲): نمایش بازی بین مدافع و مهاجم نوع۱

	ایستگاه ۱		ایستگاه ۲	
	پوشش داده شده	پوشش داده نشده	پوشش داده شده	پوشش داده نشده
مدافع	۵	-۲	۱۰	۳
مهاجم نوع ۱	-۱	۴	-۱	۱۰

جدول (۳): نمایش بازی بین مدافع و مهاجم نوع ۲

	ایستگاه ۱		ایستگاه ۲	
	پوشش داده شده	پوشش داده نشده	پوشش داده شده	پوشش داده نشده
مدافع	۱	۰	۲	-۲
مهاجم نوع ۲	-۱	۱	۰	۵

جدول (۴): نمایش بازی بین مدافع و مهاجم نوع ۳

	ایستگاه ۱		ایستگاه ۲	
	پوشش داده شده	پوشش داده نشده	پوشش داده شده	پوشش داده نشده
مدافع	۲	-۱	۳	-۲
مهاجم نوع ۳	-۲	۱	-۳	۴

مسئله بهینه‌سازی چندهدفی (۲۱) به صورت زیر نوشته می‌شود:

$$
\begin{aligned}
&maximize\ \{a_1^1(5c_1-2(1-c_1))+a_1^2(10c_2+3(1-c_2)),\\
&a_2^1(c_1+0(1-c_1))+a_2^2(2c_2-2(1-c_2)),\\
&a_3^1(2c_1-(1-c_{t_1}))+a_3^2(3c_2-2(1-c_2))\ \}\\
&s.t \quad c_1+c_2\le 1\\
&0\le v^1-\left(-c_1+4(1-c_1)\right)\le\left(1-\delta_1^1\right)M\\
&0\le v^1-\left(-c_2+10(1-c_2)\right)\le\left(1-\delta_1^2\right)M\\
&0\le v^2-\left(-c_1+(1-c_1)\right)\le\left(1-\delta_2^1\right)M\\
&0\le v^2-\left(-3c_2+4(1-c_2)\right)\le\left(1-\delta_2^2\right)M\\
&0\le v^3-\left(-2c_1+(1-c_1)\right)\le\left(1-\delta_3^1\right)M\\
&0\le v^3-\left(-3c_2+4(1-c_2)\right)\le\left(1-\delta_3^2\right)M \qquad (22)\\
&a_1^1+a_1^2=1\\
&a_2^1+a_2^2=1\\
&a_3^1+a_3^2=1\\
&a_i^k\ge 0, i=1,2,3,\ k=1,2\\
&0\le a_1^1\le M\,\delta_1^1\\
&0\le a_2^1\le M\,\delta_1^2\\
&0\le a_3^1\le M\,\delta_2^1\\
&0\le a_1^2\le M\,\delta_2^2\\
&0\le a_2^2\le M\,\delta_3^1\\
&0\le a_3^2\le M\,\delta_3^2\\
&\delta_i^k\in\{0,1\}, i=1,2,3, k=1,2\\
&0\le c_1\le 1\\
&0\le c_2\le 1
\end{aligned}
$$

مسئله برنامه‌ریزی آرمانی برای محاسبه راهبرد رضایت بخش مدافع به صورت زیر می‌باشد:

$$
\begin{aligned}
&\textit{minimize}\ \ \tfrac{1}{3}\left(d_1^+ + d_1^-\right) + \tfrac{1}{3}\left(d_2^+ + d_2^-\right) + \tfrac{1}{3}\left(d_3^+ + d_3^-\right)\\
&s.t \quad c_1 + c_2 \leqq 1\\
&\quad 0 \leq v^1 - \left(-c_1 + 4\left(1-c_1\right)\right) \leq \left(1-\delta_1^1\right)M\\
&\quad 0 \leq v^1 - \left(-c_2 + 10\left(1-c_2\right)\right) \leq \left(1-\delta_1^2\right)M\\
&\quad 0 \leq v^2 - \left(-c_1 + \left(1-c_1\right)\right) \leq \left(1-\delta_2^1\right)M\\
&\quad 0 \leq v^2 - \left(-3c_2 + 4\left(1-c_2\right)\right) \leq \left(1-\delta_2^2\right)M\\
&\quad 0 \leq v^3 - \left(-2c_1 + \left(1-c_1\right)\right) \leq \left(1-\delta_3^1\right)M\\
&\quad 0 \leq v^3 - \left(-3c_2 + 4\left(1-c_2\right)\right) \leq \left(1-\delta_3^2\right)M\\
&\quad a_1^1 + a_1^2 = 1 \qquad (۲۳)\\
&\quad a_2^1 + a_2^2 = 1\\
&\quad a_3^1 + a_3^2 = 1\\
&\quad a_1^1\left(5c_1 - 2\left(1-c_1\right)\right) + a_1^2\left(10c_2 + 3\left(1-c_2\right)\right) + d_1^+ - d_1^- = 7.8\\
&\quad a_2^1\left(c_1 + 0\left(1-c_1\right)\right) + a_2^2\left(2c_2 - 2\left(1-c_2\right)\right) + d_2^+ - d_2^- = 0.44\\
&\quad a_3^1\left(2c_1 - \left(1-c_1\right)\right) + a_3^2\left(2c_2 - 2\left(1-c_2\right)\right) + d_3^+ - d_3^- = 0.86\\
&\quad a_i^k \geq 0, i = 1,2,3, k = 1,2\\
&\quad \delta_i^k \in \{0,1\}, i = 1,2,3, k = 1,2\\
&\quad 0 \leq a_1^1 \leq M\,\delta_1^1\\
&\quad 0 \leq a_2^1 \leq M\,\delta_1^2\\
&\quad 0 \leq a_3^1 \leq M\,\delta_2^1\\
&\quad 0 \leq a_1^2 \leq M\,\delta_2^2\\
&\quad 0 \leq a_2^2 \leq M\,\delta_3^1\\
&\quad 0 \leq a_3^2 \leq M\,\delta_3^2\\
&\quad 0 \leq c_1 \leq 1\\
&\quad 0 \leq c_2 \leq 1
\end{aligned}
$$

با حل این مسئله با استفاده از نرم‌افزار لینگو[1] به دست می‌آوریم:

$c_1 = 0.43,$

$c_2 = 0.57,$

$a_1^1 = 0,$

$a_1^2 = 1,$

$a_2^1 = 0,$

$a_2^2 = 1,$

$a_3^1 = 0,$

$a_3^2 = 1$

این به این معنی است که مدافع برای حفاظت از دو ایستگاه با یک منبع امنیتی باید حضور منبع امنیتی را به صورت تصادفی با ۴۳٪ در ایستگاه ۱ و ۵۷٪ در ایستگاه ۲ برنامه‌ریزی کند.

۵- نتیجه گیری

در این مقاله، مسئله بازی امنیتی چندهدفی مورد بررسی قرار گرفت. برای حل این مسئله، یک روش برنامه‌ریزی دو سطحی چندهدفی که منجر به یک مسئله بهینه‌سازی چندهدفی می‌شود، پیشنهاد شد. برای بیان اعتبار و کاربرد روش یک مثال عملی برای بررسی امنیت مترو ارائه گردید. در دنیای واقعی ممکن است توابع عایدی بازیکنان به صورت قطعی بیان نشود یا آرمان‌های بازیکنان مبهم باشند. در این صورت می‌توان از نظریه مجموعه‌های فازی برای رفع مشکل استفاده کرد که در پژوهش‌های آینده به بحث در این زمینه خواهیم پرداخت. بازی‌های امنیتی به صورت عملی در کشورهای مختلف در حال اجراست و پیشنهاد می‌شود که از این بازی‌ها در تحلیل مسائل امنیتی کشورمان استفاده شود.

۶- مراجع

[1] J. V. Neumann and O. Morgenstern, "Theory of Games and Economic Behavior," Wiley, New York, 1944.

[2] O. G. Haywood, "Military Decision and Game Theory," Wiley, Journal of the Operations Research Society of America, vol. 2, no. 4, pp. 365-385, 1989.

[3] M. Tambe, "Security and game theory, algorithms, deployed systems, lessons learned," Cambridge university press, 2012.

[4] N. Gatti, "Game Theoretical Insights in Strategic Patrolling: Model and Algorithm in Normal-Form," in ECAI-08, pp. 403–407, 2008.

[5] K. Lye and J. M. Wing, "Game Strategies in Network Security," International Journal of Information Security, vol. 4, no. 1–2, pp. 71–86, 2005.

[6] G. Brown, M. Carlyle, J. Kline, and K. Wood, "A Two-Sided Optimization for Theater Ballistic Missile Defense," in Operations Research, vol. 53, pp. 263–275, 2005.

[7] T. Sandler and D. G. A. M, "Terrorism and Game Theory," Simulation and Gaming, vol. 34, no. 3, pp. 319–337, 2003.

[8] G. Owen, "Game Theory," Academic Press, San Diego, Third Edition, 1995.

[9] H. Bigdeli, H. hassanpour, and J. Tayyebi, "The optimistic and pessimistic solutions of single and multiobjective matrix games with fuzzy payoffs and analysis of some of military problems," Defence Sci. & Tech., Accepted, (In Persian).

[10] H. Bigdeli and H. Hassanpour, "A satisfactory strategy of multiobjective two person matrix games with fuzzy payoffs," Iranian Journal of Fuzzy Systems, vol. 13, pp. 17-33, 2016.

[11] H. Bigdeli, H. Hassanpour, and J. Tayyebi, "Constrained Bimatrix Games with Fuzzy Goals and its Application in Nuclear Negotiations," Submitted paper.

[12] M. Brown, B. An, C. Kiekintveld, F. Ordóñez, and M. Tambe, "An extended study on multi-objective security games" Auton Agent Multi-Agent Syst., vol. 28, pp. 31–71, 2014.

[13] M. Sakawa and I. Nishizaki, "Cooperative and Noncooperative Multi-Level Programming," Springer, New York and London, 2009.

[14] M. Sakawa, "Fuzzy sets and interactive multiobjective optimization," Plenum press, New York and London, 1993.

[15] M. S. Bazaraa and J. J. Jarvis, "Linear Programming and Network Flows," John Wiley & Sons, Inc., NewYork , 1977.

1- Lingo

مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"
ویژه‌نامه کنفرانس بین‌المللی ترکیبیات، رمزنگاری و محاسبات، ص ۴۳ -۳۹

نهان‌نگاری تصویر مبتنی بر SVDچندگانه در حوزه موجک با استفاده از PSO

جواد وحیدی*

استادیار، دانشگاه علم و صنعت ایران

(دریافت: ۹۵/۰۷/۰۵، پذیرش: ۹۶/۰۳/۰۶)

چکیده

هرروزه بر تعداد کسانی که از محصولات رقمی(Digital)، اعم از اصوات، تصاویر و ویدئوهای رقمی، در زندگی روزمره خود استفاده می‌کنند، افزوده می‌شود. از طرف دیگر قابلیت کپی‌برداری از این محصولات، به‌راحتی و بدون افت کیفیت باعث شده است تا همواره طراحی سامانه‌ای که بتواند از این محصولات و حقوق صاحبان آن‌ها حفاظت کند، یکی از نیازهای جدی این عرصه است. امروزه نهان‌نگاری داده در محصولات رقمی، به‌عنوان یک راه‌حل برای پیاده‌سازی و اثبات حق مالکیت، احراز اصالت محتوی و کنترل تعداد نسخه‌های چاپ‌شده از یک اثر را محقق ساخته است. نهان‌نگاری دیجیتالی یعنی قرار دادن یک سیگنال نامحسوس در بین داده‌های رسانه پوششی، به‌طوری‌که هیچ تغییری در داده‌های اصلی نداشته باشد ولی در صورت نیاز بتوان آن را استخراج کرده و به‌عنوان ادعا برای مالکیت اثر دیجیتالی استفاده نمود. در این مقاله، یک روش ترکیبی جدید برای نهان‌نگاری تصاویر ارائه گردید که جهت استخراج تصویر یا متن نهان‌شده پس از حملات عمدی یا غیرعمدی، از الگوریتم توده ذرات (PSO) جهت پیدا کردن مقدار بهینه Scaling factor استفاده‌شده است.

واژه‌های کلیدی: نهان‌نگاری تصاویر رقمی، حوزه تبدیل، تجزیه مقدار منفرد، الگوریتم توده ذرات

۱- مقدمه

نهان‌نگاری برای پنهان کردن یا اضافه کردن داده یا فایلی در فایل دیگر، به‌طوری‌که فقط افراد آگاه با ابزار لازم بتوانند به آن دست یابند و هم‌چنین یکی از راه‌های حفاظت از داده‌های چندرسانه‌ای در برابر نشرهای غیرقانونی و توزیع غیرقانونی آن‌ها است. تفاوت اصلی نهان‌نگاری با پنهان‌نگاری در این است که در نهان‌نگاری هدف اصلی حفظ محصول دیجیتال است درحالی‌که در پنهان‌نگاری، هدف اصلی، پیام پنهان‌شده است.در این روش یک سیگنال ثانویه یا الگو به تصویر، ویدئو و یا داده‌های صوتی جاسازی می‌شود که قابل‌کشف نیست و به‌صورت یک عضو جدایی‌ناپذیر به‌خوبی با داده‌های رقمی اصلی منطبق است و در مقابل هر نوع پردازش سیگنال چندرسانه‌ای [۱-۲] بدون هیچ مشکلی باقی می‌ماند. این اطلاعات ثانویه تعبیه‌شده، علامت نهان‌نگاری رقمی است. علامت نهان‌نگاری رقمی به‌طورکلی، یک کد شناسایی مرئی یا نامرئی است که ممکن است برخی اطلاعات مربوط به گیرنده قانونی و یا نویسنده داده‌های اصلی و قوانین حق نشر به شکل داده‌های متنی و یا تصویری در آن ذخیره‌شده باشد. این علامت نهان‌نگاری رقمی را می‌توان شناسایی و یا استخراج نمود و بعداً به‌عنوان یک ادعا در مورد مالکیت حقیقی داده‌ها از آن استفاده کرد. فقدان یک علامت نهان‌نگاری در تصویری که قبلاً نهان‌نگاری شده بود به این معنی است که محتوای داده رقمی دچار تغییر شده است. نهان‌نگاری رقمی که تحت عملیات انتقال/تبدیل دست‌نخورده باقی می‌مانند، ما را در حفاظت از حقوق مالکیت اثر رقمی کمک می‌کنند. در ادامه این فصل در بخش دوم روش‌های نهان‌نگاری و در ادامه، روش پیشنهادی نهان نگاری در حوزه موجک در بخش سوم شرح داده می‌شود. در انتها در بخش چهارم با نتیجه گیری از پیاده‌سازی‌ها و نتیجه گیری نهایی در بخش پنجم، این مقاله را به پایان می‌رسانیم.

۲- روش‌های نهان‌نگاری

روش‌های نهان‌نگاری می‌توانند به دو زیر دسته تقسیم‌بندی شوند:

۱- روش‌های حوزه مکان ۲- روش‌های حوزه فرکانس

در روش‌های حوزه مکان برای گنجاندن شی رقمی موردنظر، مقادیر پیکسل‌ها به‌طور مستقیم دست‌کاری می‌شود. این روش پیچیدگی کم‌تری دارند، شکننده‌ترند و مقاوم نیستند، اما در روش‌های حوزه فرکانس ابتدا تصاویر به یکی از حوزه‌های فرکانسی انتقال‌یافته و سپس پنهان‌نگاری با دست‌کاری مقادیر در حوزه فرکانس انجام می‌گیرد و درنهایت تصویر به حوزه مکان

*رایانامه نویسنده مسئول: jvahidi@iust.ac.ir

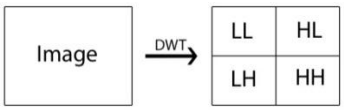
بازگردانده می‌شود. در مقایسه با روش‌های حوزه مکان ثابت‌شده است که روش‌های حوزه فرکانس در دست یافتن به الگوریتم‌های نهان‌نگاری رقمی ازلحاظ غیرقابل مشاهده بودن و نیازمندی‌های استحکام بهتر است. انتقال‌های حوزه فرکانس که عموماً در الگوریتم‌های پنهان‌نگاری تصاویر رقمی مورداستفاده قرار می‌گیرد شامل انتقال‌های زیر است:

دامنه تبدیل کسینوسی گسسته (Discrete cosine transform[1])، دامنه تبدیل فوریه گسسته (Discrete Fourier Transform[2])، دامنه تبدیل موجک گسسته (Discrete wavelet transform[3])، دامنه تبدیل سریع هادامارد (Fast Hadamard Transform[4])، تجزیه مقدار منفرد (Singular Value Decomposition[5]) و غیره.

به‌طورکلی، این مطلب مورد تأیید است که روش‌های حوزه فرکانس، قوی‌تر از روش‌های دامنه فضایی عمل می‌کنند [۳].

۲-۱- تبدیل موجک گسسته (DWT)

استفاده از DWT در فشرده‌سازی و کدینگ سیگنال‌های تصویری هرروز بیش‌تر می‌گردد. دلایل مثبت این روش می‌تواند مصالحه مطلوب کیفیت، امنیت و مقاومت باشد. نکته بااهمیت در این روش وجود خاصیت چندتبدیلی در این حوزه است که می‌توان با بهره‌گیری مناسب این روش پیام را به شیوه مطلوبی در تصویر پخش و جای‌گذاری کرد. تبدیل موجک از تجزیه تصویر در حوزه فرکانسی– فاصله‌ای تشکیل شده است. کم‌ترین باند فرکانسی در کوچک‌ترین فاکتور تجزیه‌ای را با LL نام‌گذاری می‌کنند. HL یعنی بیش‌ترین باند فرکانسی افقی و کم‌ترین باند فرکانسی عمودی است. LH نیز کوچک‌ترین سایز تجزیه در کم‌ترین فرکانس افقی و بیش‌ترین فرکانس عمودی قرار دارد [۴-۵].



شکل (۱): تبدیل موجک گسسته

۳- روش پیشنهادی نهان نگاری در حوزه موجک

در این تحقیق، یک روش نهان‌نگاری غیرقابل مشاهده و مبتنی بر روش SVD چندگانه در حوزه موجک که از الگوریتم PSO جهت افزایش استحکام استفاده‌شده است، پیشنهاد می‌گردد. در الگوریتم پیشنهادی، تصویر میزبان I و تصویر نهان‌نگاری W و تصویر نهان‌نگاری‌شده Iw نامیده شده است و محدودیتی در اندازه تصویر میزبان و نهان شده وجود ندارد زیرا در هنگام قراردادن تصویر نهان‌نگاری داخل تصویر میزبان، تصویر نهان‌نگاری تغییر اندازه داده و هم‌اندازه با زیرباند LL تصویر میزبان می‌گردد هم‌چنین در این روش تصویر نهان‌نگاری و تصویر میزبان می‌تواند رنگی (RGB) باشد [۶-۷].

۳-۱- الگوریتم جاسازی‌کردن تصویر نهان‌نگاری

الگوریتم جاسازی‌کردن تصویر نهان‌نگاری در تصویر میزبان به شرح زیر می‌باشد:

۱- تصویر میزبان I را به سه ماتریس IR , IG , IB تقسیم کن.

۲- در ماتریس i=R,G,B ; Ii ، DWT را اجرا کن و آن را به بلوک‌های i=R,G,B ; Ii_LL , Ii_LH , Ii_HL , Ii_HH تقسیم کن.

۳- در بلوک i=R,G,B ; Ii_LL ، SVD را اجرا کن. [Ii_LL_u, Ii_LL_s ,Ii_LL_v]=svd(Ii_LL) ; i=R,G,B

۴- ابعاد تصویر نهان‌نگاری W را به ابعاد بلوک LL از تصویر میزبان تغییر بده.

۵- تصویر نهان‌نگاری W را به سه ماتریس WR , WG , WB تبدیل کن.

۶- تصویر نهان‌نگاری را در مقیاس فاکتور T=۰/۰۵ ضرب کرده، آن‌گاه با مقادیر منفرد (S) مجموعه LL از تصویر میزبان را جمع کنید: Ii_LL_s2=Ii_LL_s+T*Wi ; i=R,G,B

۷- در ماتریس i=R,G,B ; Ii_LL_s2 ، SVD را اجرا کن.

۸- [Ii_LL_s2_u,Ii_LL_s2_s,Ii_LL_s2_v]= svd(Ii_LL) ; i=R,G,B

۹- معکوس SVD را بشکل زیر اجرا کن.

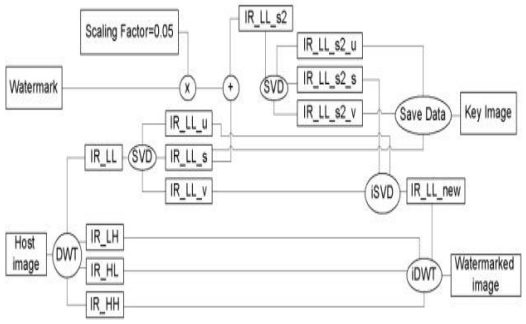
i. Ii_LL_new=Ii_LL_u* Ii_LL_s2_s* Ii_LL_vT

۱۰- معکوس DWT را برای ۴ ماتریس

ii. Ii_LL_new, Ii_LH, Ii_HL, Ii_HH; i=R,G,B اجرا کن و Ii ; i=R,G,B را به دست بیاور.

۱۱- سه ماتریس IR , IG , IB را ادغام و تصویر نهان‌نگاری‌شده Iw را ایجاد کن.

۱۲- سه ماتریس Ii_LL_s2_u , Ii_LL_s , Ii_LL_s2_v (کلید جهت بازیابی تصویر واترمارک) را ذخیره نمایید.



شکل (۲): الگوریتم جاسازی واترمارک در تصویر میزبان.

1- DCT
2- DFT
3- DWT
4- FHT
5- SVD

۳-۲- الگوریتم استخراج واترمارک

الگوریتم استخراج تصویر نهان‌نگاریازتصویر بهشرح زیر می‌باشد:

۱- تصویر واترمارک‌شده I^W را به سه ماتریس I^W_R , I^W_G , I^W_B تقسیم کن.

۲- در ماتریس I^W_i ; i=R,G,B ، DWT را اجرا و آن‌را به بلوک‌های $I^W_i\_HH$; $I^W_i\_HL$, $I^W_i\_LH$, $I^W_i\_LL\_new$ i=R,G,B تقسیم کن.

۳- در بلوک $I_i\_LL\_new$; i=R,G,B ، SVD را اجرا کن.

$[I^W_i\_LL\_u, I^W_i\_LL\_s2\_s , I^W_i\_LL\_v]=svd(I^W_i\_LL\_new)$; i=R,G,B

۴- ماتریس‌های $I_i\_LL\_s2\_v$, $I_i\_LL\_s$, $I_i\_LL\_s2\_u$ که در الگوریتم جاسازی واترمارک ذخیره کرده بودیم را فراخوانی نمایید.

۵- معکوس SVD را به شکل زیر اجرا کن:

$I_i\_LL = I_i\_LL\_u * I_i\_LL\_s * I_i\_LL\_v^T$

۶- معکوس DWT را برای ۴ ماتریس $I_i\_LL, I_i\_LH, I_i\_HL,$ I_i_HH; i=R,G,B اجرا کن و I_i ; i=R,G,B را به دست بیاور.

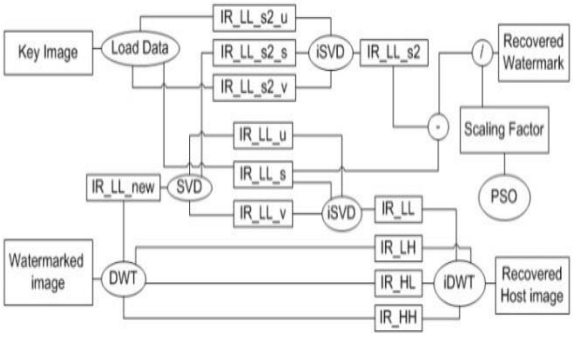
۷- سه ماتریس I_R, I_G, I_B را ادغام کن تا تصویر میزبان استخراج‌شده ایجاد گردد.

۸- معکوس SVD را به‌شکل زیر اجرا کن:

$I_i\_LL\_s2 = I_i\_LL\_s2\_u * I_i\_LL\_s2\_s * I_i\_LL\_s2\_v^T$

۹- ماتریس $I_i\_LL\_s2$ را از $I_i\_LL\_s$ کم کرده سپس بر مقیاس فاکتور T (که بهینه‌ترین مقدار آن از طریق الگوریتم PSO به‌دست می‌آید) تقسیم می‌کنیم: $W_i = (I_i\_LL\_s2 - I_i\_LL\_s)/T$; i=R,G,B

۱۰- سه ماتریس W_R , W_G , W_B را ادغام کن تا تصویر واترمارک استخراج‌شده ایجاد گردد.



شکل (۳): الگوریتم استخراج واترمارک از تصویر میزبان.

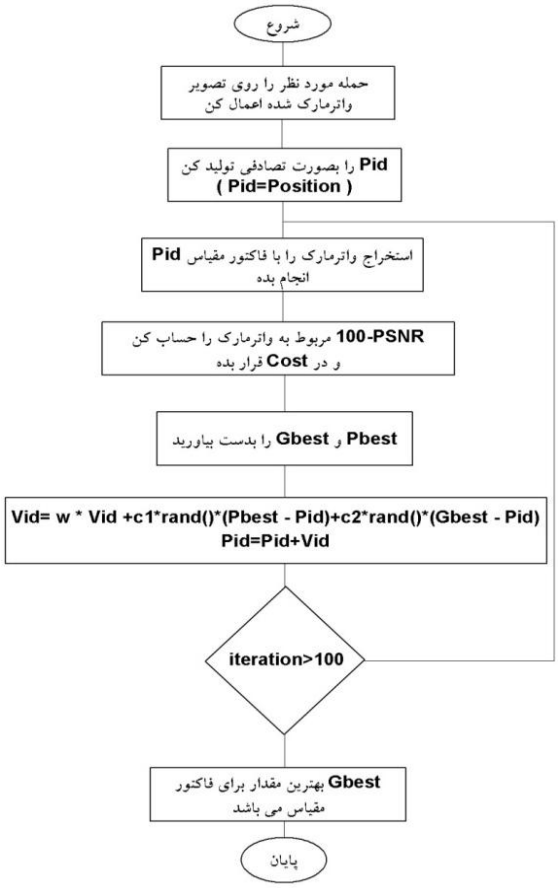
فلوچارت الگوریتم پیشنهادی به همراه الگوریتم PSO جهت استخراج‌کردن واترمارک بر روی تصویر مورد حمله قرار گرفته به‌صورت شکل (۳) می‌باشد.

برای بررسی کیفیت تصاویر نهان‌نگاری پس از فرآیند نهان‌نگاری و اعمال حملات بر روی آن‌ها، روش‌های متعددی وجود دارد. یکی از روش‌های رایج اندازه‌گیری، PSNR یا اوج نسبت وزن سیگنال به نویز و MSE میانگین مربع خطاها می‌باشند که در آن کیفیت بصری تصویر نهان‌نگاری استخراج‌شده W^* و تصویر نهان‌نگاری اصلی مورد بررسی قرار می‌گیرند.

محاسبه PSNR با استفاده از رابطه زیر انجام می‌شود:

$$MSE(W,W') = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}(W(i,j) - W'(i,j))^2 \quad (۱)$$

$$PSNR(W,W') = 10log_{10}\frac{255^2}{MSE(W,W')} \quad (۲)$$



شکل (۴): فلوچارت الگوریتم پرندگان در الگوریتم پیشنهادی.

برای تصاویر با عمق ۸ بیت، مقدار معمول برای PSNR عددی بین ۳۰db و ۵۰db در واحد Decibel می‌باشد. که این مقدار هرچه بیش‌تر باشد بهتر است. برای تصاویر با عمق ۱۶ بیت این مقدار بین ۶۰db تا ۸۰db می‌باشد. درصورتی‌که تصویر واترمارک و تصویر واترمارک استخراج‌شده دقیقاً شبیه به هم باشند (اصلاً نویز وجود نداشته باشد) مقدار MSE برابر صفر خواهد بود پس مقدار PSNRتعریف نشده است. (تقسیم بر صفر) [۸]

۴- نتایج پیاده‌سازی

برای آزمایش طرح نهان‌نگاری مبتنی بر SVD چندگانه پیشنهاد شده، از یک تصویر رنگی RGB شکل (۵. ب) با اندازه ۵۱۲×۵۱۲ پیکسل به عنوان تصویر میزبان I و یک تصویر رنگی RGB شکل (۵. الف) با اندازه ۶۴×۶۴ پیکسل به عنوان تصویر نهان‌نگاری W استفاده شده است. شکل (۵. ج) تصویر نهان‌نگاری‌شده می‌باشد.

(الف) (ب) (ج)

شکل (۵): الف) تصویر نهان. **ب)** تصویر میزبان. **ج)** تصویر نهان‌نگاری شده.

نتایج حاصل از حملات رایج بر روی تصویر نهان‌نگاری‌شده، در جدول (۱) آمده است. الگوریتم [۷] بر روی تصاویر سیاه و سفید می‌باشد. هم‌چنین تصویر استخراج‌شده نیز سیاه و سفید می‌باشد و مقدار PSNR به دست آمده هم بر اساس تصاویر سیاه و سفید می‌باشد ولی روش پیشنهادی ما، بر روی تصاویر رنگی کار می‌کند به این دلیل در جدول زیر در قسمت مربوط به روش پیشنهادی، هم PSNR مربوط به تصاویر رنگی و هم PSNR مربوط به تصاویر سیاه و سفید را قرار داده‌ایم. تا مقایسه به صورت شفاف‌تر صورت گیرد.

جدول (۱):مقایسه روش پیشنهادی و الگوریتم [۷].

ردیف	نوع حمله	روش پیشنهادی			الگوریتم [7]	
		PSNR رنگی	PSNR سیاه‌وسفید	واترمارک	PSNR	واترمارک
1	بدون حمله	33.4592	38.8796		36.3886	
2	JPEG compression	29.7184	38.0371		9.8275	
3	Salt & pepper	23.4389	32.5043		9.2226	
4	Rotation 25°	26.1144	35.8886		3.9984	
5	Rotation 270°	33.4469	38.2667		9.9417	
6	Gaussian	22.1228	32.0910		8.0315	
7	Croping	25.9530	34.8465		2.9464	

در ادامه با توجه به جداول بالا مقایسه‌ای را بین روش پیشنهادی و الگوریتم[۷] ارائه می دهیم.

نخست به شباهت‌های بین این دو روش می‌پردازیم. ابتدا باید در نظر داشته باشید که روش پیشنهاد شده ما و روش [۷] هر دو از طرح‌های نهان‌نگاری مبتنی بر مقادیر منفرد هستند. دوم این‌که هر دو روش نهان‌نگاری برای امنیت طرح نهان‌نگاری، به‌جای استفاده از دنباله اعداد تصادفی در علامت نهان‌نگاری از تصویر با متن معنادار استفاده می‌کنند که این مسئله بر عملکرد روش نهان‌نگاری می‌افزاید و از مشکل تشخیص مثبت- کاذب جلوگیری می‌کند. مطلب بعدی این‌که در هر دو روش، از طرح نهان‌نگاری برگشت ناپذیر استفاده می‌شود و نکته آخر این‌که هر دو روش از طرح نهان‌نگاری به منظور احراز حق مالکیت استفاده می‌شود.

اکنون به تفاوت‌های این دو طرح نهان‌نگاری می‌پردازیم. الگوریتم [۷] از یک روش نهان‌نگاری مبتنی بر SVD خالص استفاده می‌کند. در روش آن‌ها، تصویر میزبان و تصویر نهان‌نگاری باید به‌صورت GrayScale (سیاه و سفید) باشد و این مسئله محدودیتی در این روش است زیرا تصاویر رنگی RGB را پشتیبانی نمی‌کند ولی در روش پیشنهادشده ما، این مشکل برطرف شده است و تصاویر رنگی را پشتیبانی می‌کند. همان طور که در قسمت‌های قبل توضیح داده شد در روش نهان‌نگاری ما تصویر میزبان و تصویر نهان‌نگاری از نوع رنگی RGB هستند و هم‌چنین تصویر نهان‌نگاری ایجادشده نیز یک تصویر رنگی RGB می‌باشد.

در روش [۷] در برابر حملات رایج مقاومت خوبی ندارد. همان طور که در جداول فوق مشاهده کردید این روش نهان‌نگاری در برابر رایج‌ترین حملات ضعیف عمل می‌کند و تصویر نهان‌نگاری استخراج‌شده از آن بدون کیفیت بصری می‌باشد اما روش نهان‌نگاری پیشنهادشده ما در برابر رایج‌ترین حملات مقاومت خوبی از خود نشان داده است نتایج حاصل از آزمایشات در جداول فوق مبین این مسئله می‌باشد.

همچنین، روش پیشنهادشده درصورتی‌که هیچ حمله‌ای بر روی آن انجام نشود تصویر نهان‌نگاری را به خوبی بازیابی می‌کند ولی الگوریتم [۷] در حالتی‌که هیچ حمله‌ای بر روی آن صورت نگیرد تصویر نهان‌نگاری را با کیفیت پایین بازیابی می‌کند.

۵-نتیجه گیری

الگوریتم [۷] از یک روش نهان‌نگاری مبتنی بر SVD خالص استفاده می‌کند. در روش آن‌ها، تصویر میزبان و تصویر نهان‌نگاری باید به‌صورت GrayScale (سیاه و سفید) باشد اما در روش پیشنهادشده ما، این مشکل برطرف شده است و تصاویر رنگی را

پشتیبانی می‌شود. با توجه به آزمایشات انجام‌شده مشاهده کردیم که روش پیشنهادشده درصورتی‌که هیچ حمله‌ای بر روی آن انجام نشود تصویر نهان‌نگاری را به خوبی بازیابی می‌کند ولی الگوریتم [۷] در حالتی‌که هیچ حمله‌ای بر روی آن صورت نگیرد تصویر نهان‌نگاری را با کیفیت پایین بازیابی می‌کند. نتایج آزمایش ها نشان دهنده مزیت روش پیشنهادی نسبت به روش مشابه است.

۶- مراجع

[1] N. Mahmoodabadi, V. VahidAbdolmaleki,and M. Mekdad, "Watermarking Confidential Information By Substitutions Permutations Least Significant Bit," The Fifth National Conference Of Command And Control, 1392.(In Persian)

[2] A. Ghafoor and M. Imran, "A Non-blind Color Image Watermarking Scheme Resistent Against Geometric Attacks," Radioengineering, vol. 21, no. 4, 2012.

[3] A. A. Mohammad, A. Alhaj, and S. Shaltaf, "An improved SVD-based watermarking scheme for protecting rightful ownership," Elsevier, Signal Processing, vol. 88, pp. 2158- 2180, 2008.

[4] A. Agarwal, N. bora, and N. Arora, "Goodput Enhanced Digital Image Watermarking Scheme Based on DWT and SVD," IJAIEM, vol. 2, Issue 9, 2013.

[5] A. K. Gupta and M. S. Raval, "A robust and secure watermarking scheme basedon singular values replacement," Sadhana, vol. 37, Part 4, pp. 425-440, 2012.

[6] H. Biao-Bing and T. Shao-Xian, "A contrast sensitive visible watermarking scheme," IEEE Multimedia, vol.13, no. 2, pp. 60-67, 2006.

[7] S. Shanmugaprabha and N. Malmurugan, "A New Robust Image Watermarking Scheme Based on DWT with SVD," IJASCSE, vol. 3, Issue 4, 2014.

[8] HTTP://en.wikipedia.org/wiki/Peak_signal-to-noise_ratio

مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"
ویژه‌نامه کنفرانس بین‌المللی ترکیبیات، رمزنگاری و محاسبات، ص ۴۷ -۴۵

روش جدید تولید ماتریس کلید و وارون آن برای الگوریتم رمز هیل

سعید محمدیان سمنانی*

استادیار دانشگاه سمنان

(دریافت: ۹۵/۰۷/۰۵، پذیرش: ۹۶/۰۳/۰۶)

چکیده

الگوریتم رمز هیل کاربرد جبر خطی در رمزنگاری است که علمی در کد و دی‌کدکردن پیام‌های متنی است، این رمزنگاری مستلزم استفاده از یک ماتریس$n\times n$ غیرمنفرد با عناصر صحیح است که آن را ماتریس کلید می‌نامیم. این‌گونه ماتریس ها خواصی دارند که در این مقاله قصد داریم تا روش جدیدی برای معرفی آن‌ها و وارون آن‌ها پرداخته و سپس به کمک آن‌ها عبارتی را کدگذاری و سپس آن را دی‌کد نمائیم.

واژه‌های کلیدی: ماتریس کلید، کدگذاری، دی‌کد، رمز هیل

۱- مقدمه

در دنیای امروز حفاظت اطلاعات مبحثی است که از اهمیت بسیار بالایی برخوردار است که این اهمیت شاید در روزگاران پیشین به این نبوده است. علم کدگذاری و رمزگشایی یکی از علوم بسیار مهم و استراتژیک یک به خصوص در صنعت تلفن‌های همراه، ارتباطات، بازرگانی، الکترونیک و ارسال ایمیل‌های خصوصی است.یکی از روش‌های کدگذاری‌کردن اطلاعات استفاده از روش رمز هیل[1] است [۳-۲].

رمز هیل روشی برای ارسال یک پیام متنی به متنی جدید است که قابل فهمبرای هیچ کس دیگری نیست مگر آن‌که شخص با قاعده رمزگشایی آن آشنا باشد. در واقع Hill-K-Cipher به قرار زیر عمل می‌کند. ابتدا به کاراکترهای موجود در ادبیات زبانی که با آن روش Hill-cipher به کار می‌رود اعدادی نسبت داده می‌شود.مثلاً اگر k کاراکتر در ادبیات این زبان استفاده شود به هرکدام از آن‌ها عدد منحصر به فرد ۰، ۱، ۲، ..... k-1 نسبت داده می‌شود. همان‌طورکه گفته شد این K کاراکتر می‌توانند حروف الفبا و علائم نوشتاری از قبیل علامت سوال (؟)، حروف فاصله (-)، کاما (،) و غیره باشند.

در این روش، برای رمزگشایی متنی که کدگذاری شده به یک ماتریس به نام ماتریس کلید A و وارون آن A^{-1} نیازمندیم بدیهی است که ماتریس کلید باید غیرمنفرد باشد و نیز خواص دیگری باید داشته باشد که به آن‌ها اشاره می‌کنیم.

در این مقاله روشی ساده برای معرفی ماتریس A و وارون آن ارائه خواهیم کرد.

۲- روش تحقیق

فرض کنیم $\alpha_k \dots, \alpha_2, \alpha_1$ تمامی کاراکترهایی باشند که در یک زبان به کار می‌روند به هر کدام از این کاراکترها اعداد ۰، ۱، ۲، ..... k-1 را به ترتیب نسبت می‌دهیم (البته می‌توان اعداد را به طور نامنظم و یا به پیمانه خاصی و .... نسبت داد).

اکنون فرض کنیم که $P = \alpha_1\alpha_2 \dots \alpha_l$ یک متن ۱ کاراکتری باشد که در آن، $1 \le l \le k$ می‌باشد.

ابتدا این متن را به یک رشته عددی به صورت زیر متناظر می‌کنیم:

$$P = 0,1,2, \dots, l-1$$

اکنون P را به صورت بردار ستونی $P_1, P_2, \dots, P_m$ می‌نویسیم که هرکدام از این بردارها دارای r سطر باشند. (r عددی دلخواه صحیح و مثبت است)

$$P_1 = [0,1,2, \dots, r-1]^t, P_2 = [r, r+1, \dots, 2r-1]^t, \dots$$

$$, P_m = [(m-1)r, (m-1)r+1, \dots l-1]^t$$

تذکر: چنان‌چه برای P_m کم‌تر از r مولفه باقی بماند، به عبارتی

*رایانامه نویسنده مسئول: s_mohammadian@Semanan.ac.ir

1- Hill Cipher

اگر r عدد l را عاد نکند(یعنی r بر l بخشپذیر نباشد) آن‌گاه عدد آخر را آن‌قدر تکرار می‌کنیم تا تعداد مولفه های P_m نیز r تا گردد.

در گام بعد باید ماتریسی مانند $A = [a_{ij}]_{r\times r}$ بیابیم به نام ماتریس کلید و آن‌را از چپ در P ضرب می‌کنیم.

$$\mathrm{Ap} = [AP_1, AP_2, \dots, AP_m] \quad (mod\ k)$$

ماتریس AP را ماتریس Hill r-cipher می‌نامیم. به عبارت دیگر، متن P توسط الگوریتم رمز هیل کدگذاری شده است و به منظور رمزگشایی AP ما نیازمند معکوس ماتریس کلید یعنی A^{-1} هستیم. با توجهبه آن‌که $A^{-1} = \frac{1}{|A|}adj(A)$ و از آن‌جایی‌که درایه‌های A^{-1} باید صحیح و متعلق به $\{0,1,2,\dots,k-1\}$ باشند به عبارت دیگر، چون درایه‌های A همگی صحیح و مثبت هستند لذا کافی است که $\frac{1}{|A|}$ را به پیمانه K محاسبه کنیم ابتدا به یک تعریف و یک قضیه اشاره می‌کنیم.

تعریف: اگر a عددی صحیح و غیرصفر باشد کوچک‌ترین عدد صحیح و مثبت x که در رابطه (ax≡ ۱ mod k) صدق کند وارون a به پیمانه k خوانده می‌شود. به عنوان مثال، از ۱۳x≡1(mod 32) نتیجه می‌شود که x=۵ بنابراین ۵=۱۳$^{-1}$ به پیمانه ۳۲ است.

قضیه: فرض کنیم $a, b, c \in \mathbb{Z}$ توأماً صفر نباشند آن‌گاه معادله $ax + by = c$ در Z دارای جواب است اگر و تنها اگر $d = (a, b)|c$، و اگر x_0 و y_0 یکی از جواب‌های معادله باشد آن‌گاه جواب عمومی آن را می‌توان از رابطه:

$$x = x_0 + \frac{b}{d}t$$
$$y = y_0 - \frac{a}{d}t$$

که $t \in \mathbb{Z}$ به دست آورد.

اکنون اگر a و k اعداد صحیح مفروض باشند آن‌گاه x وارون a به پیمانه k است. هرگاه $ax \equiv 1 \pmod k$ و یا به ازای $y \in \mathbb{Z}$ ax-1=ky و یا $ax - ky = 1$.

بنابر قضیه بالا، معادله اخیر دارای جواب است اگر و تنها اگر d=(a,k)|1 و یا (a,k)=1 لذا کافی است که ماتریس کلید $A = [a_{ij}]_{r\times r}$ دارای این خاصیت باشد که |A|=a و (|A|,k)=1

بدیهی است که چنین ماتریسی منحصر به فرد نیست و هر ماتریسی که دترمینان آن برای a باشد می‌تواند انتخاب گردد برای سهولت می‌توانیم ماتریس قطری در نظر بگیریم که حاصل ضرب درایه‌های روی قطر آن برابر a باشد، باید معادله $|A|x - ky = 1$ را حل کنیم و از آن‌جا:

$$x = \frac{ky + 1}{|A|} \qquad y \in \mathbb{Z}$$

با یافتن کوچک‌ترین عدد صحیح مثبت برای y و از آن‌جا:

$$\frac{1}{|A|} \equiv \mathrm{x} \pmod{\mathrm{k}}$$

سرانجام برای رمزگشایی Ap می‌توانیم از

$$A^{-1}(\mathrm{AP}) = \frac{1}{|A|}\ adj(A)(AP)$$

$$p = x\ (adj\ (A)(AP))\ (\mathrm{mod\ k})$$

استفاده کنیم.

مثال: فرض کنیم بخواهیم متن زیر را ابتدا رمزگذاری و سپس با Hill-3-cipher رمزگشایی کنیم.

P=That's life; feel it, live it & enjoy it.

a	b	c	d	...	z	&	.	⊔	;	,	.
0	1	2	3	...	25	26	27	28	29	30	31

با نمادهای بالا در این مثال داریم k=32 و l=41

t	h	a	t	,	s	⊔		i	f	e	;	⊔	f	e	e	l	⊔	i	t	,
19	7	0	19	31	18	28	11	8	5	4	29	28	5	4	4	11	28	8	19	30

$$\mathrm{P} = \begin{bmatrix} 19 & 19 & 28 & 5 & 28 & 4 & 8 & 28 & 21 & 8 & 26 & 13 & 14 & 19 \\ 7 & 31 & 11 & 4 & 5 & 11 & 19 & 11 & 4 & 19 & 28 & 9 & 28 & 27 \\ 0 & 18 & 8 & 29 & 4 & 28 & 30 & 8 & 28 & 28 & 4 & 14 & 8 & 27 \end{bmatrix}$$

با قراردادن r = 3 داریم:

$$\mathrm{P} = \begin{bmatrix} 19 & 19 & 28 & 5 & 28 & 4 & 8 & 28 & 21 & 8 & 26 & 13 & 14 & 19 \\ 7 & 31 & 11 & 4 & 5 & 11 & 19 & 11 & 4 & 19 & 28 & 9 & 28 & 27 \\ 0 & 18 & 8 & 29 & 4 & 28 & 30 & 8 & 28 & 28 & 4 & 14 & 8 & 27 \end{bmatrix}$$

حال باید ماتریس غیرمنفردی $A = [a_{ij}]_{3\times3}$ معرفی کنیم که ۱= (|A|,32) برای مثال قرار می‌دهیم |A|=15 (کاملاً اختیاری است و کافی است در شرط (|A|,32)=1 صدق کند.) و ماتریس A را به صورت زیر در نظر می‌گیریم:

$$\mathrm{A} = \begin{bmatrix} 3 & 0 & 0 \\ 0 & 5 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$|\mathrm{A}| = 15$$

برای کدگذاری متن P داریم:

$$\mathrm{AP} = \begin{bmatrix} 25 & 25 & 20 & 15 & 20 & 12 & 24 & 20 & 31 & 24 & 14 & 7 & 8 & 25 \\ 3 & 27 & 23 & 20 & 25 & 23 & 31 & 23 & 20 & 31 & 12 & 13 & 12 & 7 \\ 0 & 18 & 8 & 29 & 4 & 28 & 30 & 8 & 28 & 28 & 4 & 14 & 8 & 27 \end{bmatrix}$$

درایه‌های AP به پیمانه ۳۲ هستند بنابراین، متن مذکور به صورت زیر کدگذاری می‌گردد:

Zda. Suxipu; uzemxuy’, uxi’ uuy’u omehnoimizh.

حال فرض کنید بخواهیم متن اخیر را دی‌کد نمائیم:

$$adj(A) = \begin{bmatrix} 5 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 15 \end{bmatrix}$$

$$|A| = 15 \rightarrow 15x \equiv 1 \ (mod\ 32) \rightarrow 15x - 32y = 1$$

$$x = 15\ , (y = 7) \rightarrow \frac{1}{|A|} = 15 \ (mod\ 32)$$

$$A^{-1} = \frac{1}{|A|} adj(A) = \begin{bmatrix} 11 & 0 & 0 \\ 0 & 13 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$A^{-1}(AP) = \begin{bmatrix} 275 & 275 & 220 & 165 & 220 & 132 & 264 & 220 & 341 & 264 & 154 & 77 & 88 & 275 \\ 39 & 351 & 299 & 260 & 325 & 299 & 403 & 299 & 260 & 403 & 156 & 169 & 156 & 91 \\ 0 & 18 & 8 & 29 & 4 & 28 & 30 & 8 & 28 & 28 & 4 & 14 & 8 & 27 \end{bmatrix}$$

چنان‌چه ماتریس اخیر را به پیمانه ۳۲ بنویسم داریم:

$$p = \begin{bmatrix} 19 & 19 & 28 & 5 & 28 & 4 & 8 & 28 & 21 & 8 & 26 & 13 & 24 & 19 \\ 7 & 31 & 11 & 4 & 5 & 11 & 19 & 11 & 4 & 19 & 28 & 9 & 28 & 27 \\ 0 & 18 & 8 & 29 & 4 & 28 & 30 & 8 & 28 & 28 & 4 & 14 & 8 & 27 \end{bmatrix}$$

۵- نتیجه گیری

در رمز نگاری می توان به گونه های متفاوت علائم یک زبان را شماره گذاری کرد. به خصوص چنانچه بخواهیم احتمال کشف رمز را توسط افراد ناشناس کمتر کنیم، می توانیم شماره گذاری علائم آن زبان را تغییر دهیم.

۶- مراجع

[1] B. Acharya, G. SankarRath, S. Kumar Patra, and S. Kumar Panigrahy, “Novel Methods of Generating Self-invertible matrix for Hill cipher Algorithm,” International Journal of security, vol. 1.

[2] M. Eisenberg, “Hill cipher and modular linear algebra,” mimeographed notes, university of Massachusettsa, vol. 19 1998.

[3] D. Kahn, “The Codebreakers, The Story of Secret Writing,” Weiden-feld and Nicolson, London, pp. 404-410, 1967.

[4] S. H. Lester, “Cryptograph in an algebraic alphabet,” Amer. Math. Monthly, vol. 36, pp. 306-312, 1929.

[5] S. H. Lester, “Concerning certain linear transformation apparatus of cryptography,” Amer. Math. Monthly, vol. 38, pp. 135-154, 1931.

[6] W. stalling, “cryptography and network security,” 4th edition, printice Hall, 2005.

مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"
ویژه‌نامه کنفرانس بین‌المللی ترکیبیات، رمزنگاری و محاسبات، ص ۶۱ -۴۹

دسته‌بندی اهداف سوناری با استفاده از شبکه‌های عصبی مصنوعی آموزش دیده مبتنی بر جغرافیای زیستی

سید محمدرضا موسوی[1*]، محمد خویشه[2]، فلاح محمدزاده[3]، هومان علائیان[4]

۱- استاد، دانشگاه علم و صنعت ایران، ۲- دانشجوی دکتری، دانشگاه علم و صنعت ایران، ۳- مربی، دانشگاه علوم دریایی امام خمینی (ره) نوشهر
۴- دانشجوی کارشناسی مهندسی برق، دانشگاه علم و صنعت ایران،

(دریافت: ۹۵/۰۷/۰۵، پذیرش: ۹۶/۰۳/۰۶)

چکیده

هدف این مقاله، استفاده از الگوریتم بهینه شده مبتنی بر جغرافیای زیستی برای آموزش شبکه‌های عصبی چندلایه به منظور دسته‌بندی اهداف سوناری می‌باشد. به منظور آزمایش عملکرد این الگوریتم، دسته‌بندی‌کننده طراحی شده بوسیله دادگان سونار آزموده شده و نتایج بدست آمده با پنج الگوریتم تکاملی معروف مقایسه می‌شود. معیارهای مورد سنجش عبارتند از: سرعت همگرایی، احتمال گیر افتادن در بهینه‌های محلی و دقت دسته‌بندی. نتایج نشان می‌دهند که آموزش شبکه‌های عصبی چندلایه با استفاده از الگوریتم بهینه شده مبتنی بر جغرافیای زیستی نسبت به الگوریتم‌های تکاملی موجود و الگوریتم پس‌انتشار، در تمام زمینه‌ها نتایج بهتر و یا قابل مقایسه‌ای را ارائه می‌کند.

واژه‌های کلیدی: شبکه‌های عصبی، سونار، الگوریتم بهینه شده مبتنی بر جغرافیای زیستی، الگوریتم تکاملی

۱- مقدمه

اهداف آشکارسازی‌شده توسط سونار عبارتند از: هدف واقعی، نویز، طنین و اکوی بدون هدف. نویز دارای انواع مختلفی مانند نویز حرارتی، محیطی، قاره‌ای، لنگرگاه و غیره می‌باشد که چون از جنس صوت ارسالی توسط سونار نمی‌باشد، تمایز آن از هدف واقعی آسان است. اکوهای حاصل از برخورد پینگ ارسالی سونار با کف و سطح دریا را طنین گویند [۱]. با توجه به این‌که اکوهای حاصل از طنین دارای یک دامنه یکسان و همگن می‌باشند، علی‌رغم این‌که از جنس پینگ ارسالی هستند، تمایز آن‌ها از هدف واقعی آسان است. هنگامی‌که جنس بستر دریا دارای تغییرات زیادی است و در ابعاد کوچک، بستر با جنس‌های مختلفی وجود دارد، اکوهای برگشتی از بستر دارای ویژگی‌های هدف گونه خواهند بود، به صورتی که حتی تابع چگالی احتمال هدف واقعی و بستر بسیار باهم شبیه خواهند بود. این‌گونه اهداف کاذب را اکوی بدون هدف گویند [۲]. طبقه‌بندی اکوی بدون هدف و اهداف واقعی به خاطر تشابه بسیار زیاد اکوهای برگشتی از آن‌ها، کار بسیار دشواری است. دسته‌بندی‌کننده‌های متعارف آماری (که بیش‌تر بر مبنای نظریه بیزن[1] استوار هستند) به‌دلیل نیازمندی به محاسبه دانش قبلی و تابع چگالی احتمال[2] (PDF)، وابسته به آزمایشات گسترده بوده و در نتیجه هزینه، زمان و تجهیزات بسیار زیادی را احتیاج دارند. از طرف دیگر، با توجه به این‌که مشخصات انتشار صوت در هر نقطه از دریا و در هر باز زمانی از شب و روز متفاوت است، دسته‌بندی‌کننده‌ای باید انتخاب شود که هم به آزمایشات کم‌تر وابسته باشد و هم قابلیت تطبیق‌پذیری بالایی داشته باشد. از این‌رو، در این مقاله شبکه‌های عصبی مصنوعی برای دسته‌بندی هدف واقعی و اکوی بدون هدف انتخاب می‌شوند. این‌گونه شبکه‌ها می‌توانند با یک مجموع دادگان محدود آموزش ببینند و در سناریوهای آزمایش مختلف به کار برده شوند [۳]. صرف نظر از کاربردها، توانایی متمایز شبکه‌های عصبی مصنوعی چندلایه، یادگیری می‌باشد [۴]. یادگیری به‌این معنی است که این شبکه‌ها همانند مغز انسان می‌توانند از یک تجربه یا آزمایش یاد بگیرند. این ویژگی (یادگیری) بخش ضروری همه شبکه‌های عصبی است که ممکن است به دو نوع تقسیم گردد: یادگیری با نظارت[3] [۵] و یادگیری بدون نظارت[4] [۶]. برای شبکه‌های عصبی مصنوعی چندلایه (در بیش‌تر کاربردها)، از الگوریتم‌های پس‌انتشار[5] بهینه‌شده [۷] و یا استاندارد [۸]، به‌عنوان روش یادگیری استفاده می‌گردد که از خانواده یادگیری با نظارت می‌باشند. الگوریتم پس‌انتشار بر مبنای گرادیان است که اشکالاتی هم‌چون هم‌گرایی آهسته [۹] و

* رایانامه نویسنده مسئول: m_mosavi@iust.ac.ir

1- Bayesian Theorem
2 - Probability Density Function
3- Supervised Learning
4- Unsupervised Learning
5- Back-Propagation (BP) Algorithm

به‌کارگیری در یک محدوده کوچک [۱۰] را دارد و بنابراین برای کاربردهای عملی قابل اعتماد نیست.

هدف نهایی فرآیند یادگیری در شبکه‌های عصبی، پیداکردن بهترین ترکیب از یال‌های وزن‌دار و حد آستانه[1] آنها است به‌طوری‌که در آموزش شبکه و نمونه‌های آزمون، کم‌ترین مقدار خطا را داشته باشیم. اغلب خطای شبکه عصبی چندلایه، برای مدت زیادی در زمان فرآیند یادگیری، بزرگ خواهد بود و الگوریتم یادگیری آن را به‌سمت کم‌شدن هدایت می‌کند. این مسأله در فرآیندهای یادگیری مبتنی بر گرادیان، مثل الگوریتم پس‌انتشار، مشترک است. هم‌چنین هم‌گرایی الگوریتم پس‌انتشار به‌مقدار خیلی زیاد به مقادیر اولیه نرخ یادگیری و اندازه حرکت وابسته است. مقادیر نامناسب این متغیرها می‌تواند حتی سبب واگرایی الگوریتم گردد. مطالعات بسیار زیادی برای حل این مشکل الگوریتم پس انتشار انجام گرفته است [۱۱]، اما نتایج مورد انتظار به دست نیامده و هر روش فقط تأثیرات جانبی خودش را داشته است. مقاله [۱۲] نشان می‌دهد که الگوریتم‌های جستجوی ابتکاری یا اکتشافی[2] می‌تواند جایگزین الگوریتم‌های یادگیری مبتنی بر گرادیان باشد، زیرا ماهیت تصادفی این الگوریتم‌ها اجازه می‌دهد تا حداقل خطای بهتری نسبت به روش‌های مبتنی بر گرادیان داشته باشیم ولی اکتشاف تمام حالات، پیچیدگی زمانی و مکانی شبکه را افزایش می‌دهد که برای مسائل با ابعاد بالا این مشکل شدیدتر می‌شود [۱۳].

علاوه بر روش‌های مبتنی بر مشتق و روش‌های اکتشافی، در سال‌های اخیر روش‌های فراابتکاری گوناگونی از قبیل بهینه‌سازی گروهی ذرات[3] [۱۴]، الگوریتم ژنتیک[4] [۱۵]، الگوریتم اجتماع مورچه‌ها[5] [۱۶] و الگوریتم‌های تکامل‌پذیر[6] [۱۷] برای آموزش شبکه‌های عصبی به کار گرفته شده است. با استفاده از قضیه "هیچ نهاری مجانی نیست"[7]، ثابت شده است که الگوریتم‌های جستجوی اکتشافی الزاماً بهترین جواب را برای مسائل بهینه‌سازی تولید نمی‌کنند [۱۱ و ۱۹-۱۸]. این قضیه از یک طرف و مشکلات روش‌های مبتنی بر گرادیان از طرف دیگر، بسیاری از محققان را بر آن داشته است که درخصوص تأثیر الگوریتم‌های فرا ابتکاری متفاوت در یادگیری شبکه‌های عصبی مصنوعی تلاش‌های بسیاری را انجام دهند [۲۷-۲۰]. صرف‌نظر از تفاوت‌های بین روش‌های فراابتکاری مختلف، یک ویژگی مشترک بین آن‌ها تقسیم فرآیند جستجو به دو مرحله شناسایی و بهره‌برداری است [۲۹-۲۸]. پیداکردن یک موازنه مناسب بین این دو مرحله با توجه به ماهیت تصادفی روش‌های فراابتکاری، مسئله‌ای چالش‌برانگیز می‌باشد. یکی از الگوریتم‌های بسیار توانا در این زمینه بهینه‌ساز مبتنی بر جغرافیایی زیستی[8] (BBO) می‌باشد که با تعداد پارامترهای کم توانایی تطبیق برای مجموعه دادگان‌های مختلف را دارا می‌باشد. به عبارت دیگر با تنظیم خیلی ساده پارامترهای این الگوریتم، می‌توان الگوریتم بهینه‌ساز جدیدی را تولید کرد که برای آن مسأله خاص بهترین جواب ممکن را تولید کند. در این مقاله برای اولین بار الگوریتم BBO را برای دادگان سونار تغییر داده و نرخ‌های جدیدی برای مهاجرت به داخل[9] و خارج[10] معرفی می‌کنیم و هم‌چنین الگوریتم جدید را با نام IBBO[11] برای آموزش شبکه عصبی MLP به کار برده و توسط آن دسته‌بندی‌کننده جدیدی با نام MLPIBBO طراحی می‌نمایم.

در این مقاله، شبکه عصبی MLP توسط الگوریتم IBBO به منظور دسته‌بندی دادگان سونار (شامل هدف واقعی و هدف کاذب) آموزش داده شده است. دلیل استفاده از شبکه MLP و الگوریتم آموزشی IBBO به شرح ذیل می‌باشد:

- شبکه MLP به دلیل استفاده از توابع سیگموئید، توانایی منحصر به‌فردی در کار با دادگانی که به‌طور خطی قابلیت تفکیک ندارند را دارا می‌باشد. از طرفی دادگان سونار به‌صورت خطی قابل تفکیک نیستند و نیازمند دسته‌بندی‌کننده‌ای با ابعاد بالا می‌باشند.
- اکوی بدون هدف و هدف واقعی دارای ویژگی‌های بسیار شبیه هم می‌باشند. در نتیجه باید الگوریتمی انتخاب شود که فضای جستجو را به‌طور کامل اکتشاف کند.
- نقطه قوت الگوریتم IBBO نسبت به الگوریتم‌های فراابتکاری دیگر، قدرت اکتشاف فوق‌العاده آن می‌باشد. در مقایسه با روش‌های هوش گروهی[12] (از قبیل روش بهینه‌سازی ازدحام ذرات و روش بهینه‌سازی کلونی مورچه‌ها)، عملگر جهش الگوریتم ژنتیک توانایی اکتشاف بیش‌تری را فراهم می‌کند. این پتانسیل موجب می‌شود تا بهینه‌سازی مبتنی بر جغرافیای زیستی عملکرد بهتری در آموزش شبکه‌های عصبی مصنوعی چندلایه نسبت به تکنیک‌های هوش گروهی داشته باشد. به‌علاوه، در روش بهینه‌سازی مبتنی بر جغرافیای زیستی، داشتن ثابت‌های جهش مختلف برای هر فرد در یک جمعیت، نسبت به الگوریتم ژنتیک که فقط یک عملگر جهش برای کل جمعیت دارد، به ایجاد عملکرد بهتر کمک می‌کند.
- نقطه ضعف الگوریتم BBO سرعت کم در فاز بهره‌برداری است. از طرف دیگر در بسیاری از کاربردهای سونار فعال (از

1- Bias
2- Heuristic Optimization Methods
3- Particle Swarm Optimization (PSO)
4- Genetic Algorithm (GA)
5- Ant Colony Optimization (ACO)
6- Evolutionary Strategies (ES)
7- No Free Lunch Theorem (NFL)
8- Biogeography based Optimization Algorithm (BBO)
9- Immigration
10- Emigration
11- Improved-BBO
12- Swarm Intelligence (SI)

قبیل کاربردهای نظامی) نیاز به پردازش‌های بلادرنگ است و پیچیدگی زمانی یک نقطه ضعف بزرگ به‌شمار می‌آید. این ضعف توسط نرخ‌های جدید مهاجرت جبران می‌شود.

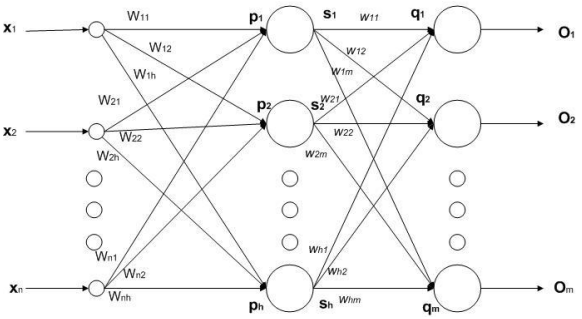
سازمان‌دهی مقاله بدین صورت می‌باشد که بخش ۲ به معرفی شبکه‌های عصبی مصنوعی چندلایه خواهد پرداخت. بخش ۳ به بحث در خصوص کلیات روش BBO، تنظیم نرخ‌های مهاجرت و نحوه تولید IBBO پرداخته است. شیوه اعمال IBBO به‌عنوان یک الگوریتم آموزش تکاملی در شبکه‌های عصبی مصنوعی چندلایه، در بخش ۴ توصیف گردیده است. نتایج در بخش ۵ مورد بحث قرار خواهند گرفت. در نهایت در بخش ۶ نتیجه‌گیری و محورهای مطالعاتی که می‌توان در خصوص آن‌ها به مطالعه پرداخت، بیان خواهد شد.

۲- شبکه‌های عصبی چندلایه

شکل (۱) یک شبکه عصبی چندلایه (۳ لایه) را نشان می‌دهد که در آن، n مبین تعداد گره‌های ورودی، h مبین تعداد گره‌های پنهان و m مبین تعداد گره‌های خروجی است. همان‌طورکه ملاحظه می‌شود، اتصال‌های یک طرفه بین گره‌های شبکه عصبی چندلایه که از خانواده شبکه‌های عصبی MLP است، وجود دارد. خروجی شبکه عصبی چندلایه به‌صورت رابطه (۱) محاسبه می‌گردد:

$$s_j = \sum_{i=1}^{n} (W_{ij} . X_i) - \theta_j , \quad j=1,2,...,h \qquad (۱)$$

که در آن، n مبین تعداد گره‌های ورودی، W_{ij} مبین وزن یال متصل‌کننده گره i-ام (در لایه ورودی) به گره j-ام (در لایه پنهان)، θ_j مبین بایاس گره j-ام (در لایه پنهان) و X_i مبین ورودی به گره i-ام (در لایه ورودی) است. خروجی هر گره پنهان با استفاده از یک تابع سیگموید و به‌صورت رابطه (۲) به دست می‌آید:



شکل (۱): یک شبکه عصبی مصنوعی چندلایه با یک لایه پنهان

$$S_j = sigmoid(s_j) = \frac{1}{(1+\exp(-s_j))}, \quad j=1,2,...,h \qquad (۲)$$

می‌توان بعد از محاسبه مقدار گره‌های پنهان، خروجی‌های نهایی را به‌صورت زیر تعریف نمود:

$$o_k = \sum_{j=1}^{h} (W_{jk} . S_j) - \theta'_k , \quad k=1,2,...,m \qquad (۳)$$

$$O_k = sigmoid(o_k) = \frac{1}{(1+\exp(-o_k))}, \quad k=1,2,...,m \qquad (۴)$$

که در آن، W_{jk} مبین وزن یال متصل‌کننده گره j-ام (در لایه پنهان) به گره k-ام (در لایه خروجی) و θ'_k مبین بایاس گره k-ام (در لایه خروجی) است. مهم‌ترین بخش‌های شبکه‌های عصبی چندلایه، وزن یال‌ها و بایاس گره‌ها می‌باشد. همان‌طورکه در روابط بالا مشاهده گردید، وزن یال‌ها و بایاس‌ها، مقدار خروجی نهایی را تعریف کردند. آموزش یک شبکه عصبی چندلایه، شامل پیداکردن بهترین مقدار برای وزن یال‌ها و بایاس‌ها، به‌منظور رسیدن به مقدار مطلوب خروجی در ازای ورودی‌های مشخص است.

۳- الگوریتم بهینه‌سازی مبتنی بر جغرافیای زیستی

الگوریتم بهینه‌سازی مبتنی بر جغرافیای زیستی برای اولین بار در سال ۲۰۰۸ توسط سیمون[1] [۳۰] پیشنهاد گردید. ایده اصلی این الگوریتم از رشته‌ای در زیست‌شناسی که درباره طرز انتشار و پخش حیوانات و نباتات (در زمان و مکان) بحث می‌کند، الهام گرفته شده است. در این الگوریتم، اکوسیستم‌های متفاوت (محل سکونت یا قلمروها)، برای یافتن ارتباط بین گونه‌های مختلف (ساکنین) بر حسب مهاجرت به بیرون، مهاجرت به داخل و جهش، بررسی می‌شوند. تکامل اکوسیستم‌ها با در نظر گرفتن انواع گونه‌های مختلف و تأثیر مهاجرت و جهش برای رسیدن به یک شرایط پایدار، زیربنای الگوریتم بهینه‌سازی مبتنی بر جغرافیای زیستی می‌باشد.

همانند الگوریتم ژنتیک، الگوریتم بهینه‌سازی مبتنی بر جغرافیای زیستی، از تعدادی عوامل جستجو به‌نام محل‌های سکونت[2] استفاده می‌کند. این محل‌های سکونت، مشابه کروموزوم‌ها در الگوریتم ژنتیک هستند. الگوریتم بهینه‌سازی مبتنی بر جغرافیای زیستی، هر محل سکونت را به‌صورت

1- Simon
2- Habitat

بردارهایی از ساکنین[1] (مشابه ژن‌ها در الگوریتم ژنتیک) در نظر می‌گیرد که متغیرهای مسأله را نشان می‌دهند. به‌علاوه، برای هر محل سکونت، شاخص مناسب‌بودن محل سکونت[2] نیز تعریف می‌گردد. بالابودن این شاخص به‌منزله داشتن شرایط بهتر می‌باشد. در هر زمان محل‌های سکونت بر اساس سه قانون اصلی به شرح زیر تعیین می‌گردند:

الف) ساکنینی که در مکان‌های با شاخص پایین اقامت دارند، بیش‌تر به مهاجرت به مکان‌هایی با شاخص بالاتر، تمایل دارند.

ب) ساکنینی که در مکان‌های با شاخص بالا اقامت دارند، تمایل بیش‌تری به جذب مهاجران از مکان‌های با شاخص پایین دارند.

ج) مکان‌ها بدون توجه به مقدار شاخص‌شان، باید به‌صورت تصادفی ساکنان‌شان را تغییر دهند.

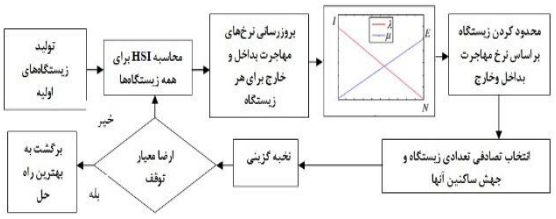
در طبیعت، این پدیده موجب ایجاد تعادل میان اکوسیستم‌های مختلف می‌گردد. به‌عبارت دیگر، طبیعت به بهبود پایداری نواحی زیستی مختلف تمایل دارد. الگوریتم بهینه‌سازی مبتنی بر جغرافیای زیستی، این مفاهیم را برای بهبود شاخص همه مکان‌های زیستی به‌کار می‌برد که نتایج آن در استخراج راه‌حل تصادفی اولیه برای یک مسأله خاص مورد استفاده قرار می‌گیرد.

با انتخاب تصادفی مجموعه‌ایی از محل‌های سکونت، الگوریتم بهینه‌سازی مبتنی بر جغرافیای زیستی آغاز می‌گردد. هر محل دارای n ساکن مختلف است که بر اساس متغیرهای یک مسأله خاص تعیین می‌گردند. به‌علاوه هر محل، نرخ‌های مهاجرت به بیرون، مهاجرت به داخل و جهش خاص خودش را دارد که از مکان‌های متمایز از نظر زیستی در طبیعت الگوبرداری شده است. مهاجرت به بیرون (μ_k) و مهاجرت به داخل (λ_k)، به‌عنوان توابعی از تعداد ساکنان آنان به‌صورت زیر تعریف می‌گردند:

$$\mu_k = \frac{E \times n}{N} \qquad (۵)$$

$$\lambda_k = I \times \frac{1-n}{N} \qquad (۶)$$

که در آن، n مبین تعداد ساکنین کنونی، N مبین حداکثر تعداد ساکنین مجاز که با استفاده از شاخص مناسب‌بودن محل سکونت افزایش می‌یابند (محل سکونت مناسب‌تر، تعداد ساکنین بیش‌تر)، E مبین بیش‌ترین نرخ مهاجرت به بیرون و I مبین بیش‌ترین نرخ مهاجرت به داخل است. در شکل (۲) بیش‌ترین نرخ مهاجرت به بیرون و بیش‌ترین نرخ مهاجرت به داخل، نشان داده شده است. با استفاده از این شکل می‌توان فهمید که تعداد زیادی از ساکنین، در یک زمان با احتمال زیاد به بیرون مهاجرت می‌کنند و با احتمال کم، به داخل مهاجرت می‌نمایند [۳۰].



شکل (۲): مراحل عمومی الگوریتم بهینه‌سازی مبتنی بر جغرافیای زیستی

سومین مولفه الگوریتم بهینه‌سازی مبتنی بر جغرافیای زیستی، جهش است که قدرت اکتشاف الگوریتم بهینه‌سازی مبتنی بر جغرافیای زیستی را بهبود داده و تنوع محل‌های سکونت را حفظ می‌کند. این مولفه به‌صورت رابطه (۷) تعریف می‌شود:

$$m_n = M \times \left(1 - \frac{p_n}{p_{\max}}\right) \qquad (۷)$$

که در آن، M مبین مقدار اولیه جهش است که به‌وسیله کاربر تعریف می‌گردد. p_n مبین احتمال جهش n-امین محل‌های سکونت و $p_{\max}$ مبین بیش‌ترین مقدار p_n است و به‌صورت رابطه (۸) تعریف می‌گردد:

$$p_{\max} = \arg\max\left(p_n\right) \qquad (۸)$$

در بلوک دیاگرام شکل (۲) مراحل کلی الگوریتم بهینه‌سازی مبتنی بر جغرافیای زیستی نشان داده شده است. این شکل نشان می‌دهد که الگوریتم بهینه‌سازی مبتنی بر جغرافیای زیستی با مجموعه‌ای از محل‌های سکونت تصادفی آغاز می‌گردد. بعد از محاسبه شاخص مناسب‌بودن زیستگاه[3] برای هر محل سکونت، نرخ‌های مهاجرت به بیرون، مهاجرت به داخل و جهش نیز به‌روز (محاسبه) می‌شود. مطابق با این نرخ‌ها، ساکنین معمولی (غیرنخبه) مهاجرت کرده و یا جهش پیدا می‌کنند. تعدادی از بهترین محل‌های سکونت که از قبل تعریف شده‌اند برای تولید نسل‌های بعد در نظر گرفته می‌شوند. سرانجام الگوریتم بهینه‌سازی مبتنی بر جغرافیای زیستی با برآورده‌شدن شرایط پایانی، به پایان می‌رسد. ذکر این نکته لازم است که نخبه‌گرایی مانع از خراب‌شدن بهترین محل سکونت با مهاجرت به داخل می‌گردد. با انجام این‌کار، ما تعدادی از بهترین محل‌های سکونت را در هر تکرار حفظ می‌کنیم. در مورد مجموعه دادگان سونار نرخ‌های خطی مهاجرت

1- Habitant
2- Habitat Suitability Index (HSI)
3- HSI

نمی‌تواند نتایج خوبی را ارائه کند. بنابراین، در قسمت بعد با توجه به ویژگی‌های این مجموعه دادگان یک مدل غیرخطی ارائه می‌شود. نتایج نشان خواهد داد که این مدل دارای توانایی منحصربه‌فردی در افزایش دقت دسته‌بندی دادگان سونار با حفظ پیچیدگی شبکه است.

۳-۱- الگوریتم BBO با نرخ مهاجرت بهبودیافته (IBBO)

در BBO استاندارد، پدیده‌های مهاجرت به داخل و خارج به صورت خطی و طبق روابط (۶-۵) مدل شده‌اند. این در حالی است که با توجه به سازوکارهای مهاجرت در بین حیوانات و پیچیدگی‌های فراوان این پدیده، نمی‌توان پدیده مهاجرت را به صورت خطی مدل کرد. در مراجع گوناگون [۳۲-۳۱] برای کاربردهای مختلف از مدل‌های غیرخطی مختلف استفاده شده است. در بعضی کاربردها که نیاز به پردازش بلادرنگ می‌باشد [۳۳]، از مدل‌هایی که به سرعت هم‌گرا شوند، استفاده شده است و در کاربردهایی که رسیدن به جواب بهینه و قطعی اولویت می‌باشد [۳۴]، از مدل‌های توسعه‌ای استفاده شده است. مسأله دسته‌بندی دادگان سونار تا حدودی با مسائل مطرح شده قبلی متفاوت می‌باشد. بدین صورت که در این مجموعه دادگان خاص، از یک طرف، با توجه به شباهت بسیار زیاد هدف واقعی و هدف کاذب، به تابعی نیاز است که فضای جستجو را به خوبی اکتشاف کرده و تمام بهینه‌های محلی را شناسایی کند تا در بهینه‌های محلی گیر نکند. از سوی دیگر، با توجه به نیاز به پردازش بلادرنگ، به تابعی نیاز است که در فاز بهره‌برداری رفتار کاملاً متفاوتی داشته باشد و به سرعت هم‌گرا شود. با توجه به مباحث مطرح‌شده در این مقاله، مهاجرت به داخل و خارج توسط روابط (۱۰-۹) تعریف می‌شوند. بعد از اصلاح BBO متناسب با نوع مجموعه دادگان سونار، از این پس در این مقاله این الگوریتم را IBBO[1] نام‌گذاری می‌کنیم. در ادامه مقاله، شبکه MLP برای اولین بار توسط IBBO آموزش داده می‌شود و نتایج با BBO استاندارد و الگوریتم‌های معیار استاندارد دیگر مقایسه خواهد شد.

$$\begin{cases}\mu_k = \mathrm{E} \times \mathrm{Ln}(\frac{k}{N}+1) \\ \lambda_k = \mathrm{I} \times \exp(-\frac{k}{N})\end{cases} \quad \mathrm{k} \le \mathrm{N/p} \qquad (۹)$$

$$\begin{cases}\mu_k = \mathrm{E} \times \exp(\frac{k}{N}-1) \\ \lambda_k = \mathrm{I} \times \mathrm{Ln}(2-\frac{k}{N})\end{cases} \quad \mathrm{k} > N/p \qquad (۱۰)$$

که در این روابط، N نشان‌دهنده جمعیت اولیه است و هم‌چنین $p \in \{2,3\}$ انتخاب شده است. در واقع ما توسط این روابط نرخ‌های مهاجرت موجودات را براساس میزان مقدار شاخص مناسب‌بودن محل سکونت (HSI) آن‌ها تنظیم می‌کنیم. همان‌گونه که در رابطه (۹) ملاحظه می‌شود، برای محل‌های سکونت با HSI پایین ($k \le N/p$) نرخ مهاجرت به خارج به صورت لگاریتمی افزایشی است، درحالی‌که نرخ مهاجرت به داخل به صورت نمایی کاهنده می‌باشد. عکس همین روابط را برای محل‌های سکونت با HSI بالا داریم. نحوه تنظیم این پارامترها هم براساس درک بالا از نحوه مهاجرت پرندگان و تاثیر مدل‌های ریاضی مختلف بر آن‌ها بوده است. به عبارت ساده‌تر، برای هر زیستگاه براساس مقدار HSI، نرخ‌های مهاجرت مختلف را در نظر گرفته و از سوی دیگر مدل ریاضی که این رفتار را به بهترین وجه توصیف کند با چند بار آزمایش به دست آورده‌ایم. به‌دست‌آوردن بهینه‌ترین مدل یکی از کارهایی است که می‌توان آن‌را به عنوان یکی از کارهای پیش‌رو در نظر گرفت.

در بخش بعدی، نخست الگوریتم IBBO به یک شبکه عصبی چندلایه اعمال و سپس با الگوریتم‌های BBO استاندارد، بهینه‌سازی ازدحام ذرات، ژنتیک، بهینه‌سازی کلونی مورچگان و جستجوی گرانشی روی دادگان سونار با ابعاد کاهش‌یافته، مقایسه می‌گردد.

۴- آموزش یک شبکه عصبی چندلایه با استفاده از الگوریتم بهینه‌سازی مبتنی بر جغرافیای زیستی

به‌طورکلی، از الگوریتم‌های تکاملی برای آموزش شبکه‌های عصبی چندلایه در سه حالت استفاده می‌شود. اولین روش عبارت است از به‌کارگیری شبکه‌های تکاملی به‌منظور یافتن ترکیب وزن یال‌ها و بایاس گره‌ها برای داشتن کم‌ترین مقدار خطا در یک شبکه عصبی چندلایه. دومین شیوه عبارت است از به‌کارگیری شبکه‌های تکاملی به‌منظور یافتن ساختار مناسب شبکه عصبی چندلایه در یک مسأله خاص و آخرین شیوه شامل به‌کارگیری شبکه‌های تکاملی به‌منظور یافتن پارامترهای الگوریتم یادگیری مبتنی بر گرادیان از قبیل نرخ یادگیری و اندازه حرکت است. در این مقاله، الگوریتم بهینه‌سازی مبتنی بر جغرافیای زیستی، با استفاده از شیوه نخست به یک شبکه عصبی چندلایه اعمال می‌گردد. به منظور طراحی یک الگوریتم آموزش‌دهنده برای شبکه‌های عصبی چندلایه، لازم است مراحل زیر انجام گردد:

1- Improved BBO

الف) راهبرد نمایش: در الگوریتم بهینه‌سازی مبتنی بر جغرافیای زیستی، باید وزن یال‌ها و بایاس گره‌ها به‌صورت مناسب نمایش داده شوند.

ب) شاخص مناسب‌بودن محل سکونت: برای ارزیابی زیستگاه‌ها، باید یک تابع مناسب خطای شبکه عصبی چندلایه تعریف گردد. در بخش‌های بعدی این مراحل با جزئیات تشریح خواهند شد.

۴-۱- نمایش مسأله آموزش شبکه‌ی عصبی چندلایه توسط الگوریتم بهینه‌سازی مبتنی بر جغرافیای زیستی

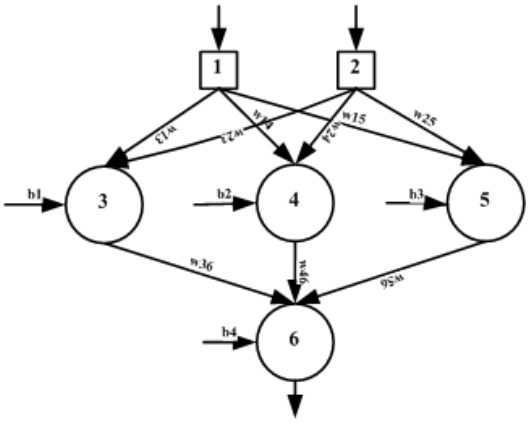
به‌طورکلی، سه روش برای نمایش وزن یال‌ها و بایاس گره‌ها وجود دارد: بردار، ماتریس و حالت دودویی [۳۵]. در نمایش برداری، هر پارامتر با یک بردار نمایش داده می‌شود. برای آموزش یک شبکه عصبی چندلایه، باید همه وزن‌ها و بایاس‌ها معلوم باشند. در نمایش ماتریسی، هر پارامتر به‌صورت یک ماتریس نمایش داده می‌شود. برای نمایش دودویی، هر پارامتر به‌صورت رشته‌ای از بیت‌های دودویی نمایش داده می‌شود. هر کدام از این شیوه‌های نمایش، مزایا و معایب خاص خود را دارد که می‌تواند در یک مسأله خاص مفید واقع گردد [۳۶].

در روش نخست، تبدیل پارامترها به بردار، ماتریس و یا رشته‌ای از بیت‌های دودویی آسان می‌باشد، اما فرآیند بازیابی آن‌ها پیچیده خواهد بود. به‌همین دلیل، اغلب این روش در شبکه‌های عصبی ساده مورد استفاده قرار می‌گیرد. در روش دوم برای شبکه‌های با ساختار پیچیده، بازیابی آسان‌تر از کدکردن پارامترها است. این روش برای الگوریتم‌های یادگیری در شبکه‌های عصبی عمومی بسیار مناسب است. در روش سوم، نیاز است که متغیرها به‌صورت دودویی نمایش داده شوند. در این حالت وقتی که ساختار شبکه پیچیده گردد، طول هر پارامتر نیز افزایش می‌یابد. بنابراین، فرآیند کدکردن و دی‌کدکردن خیلی پیچیده خواهد شد.

در این مقاله، چون با شبکه‌های عصبی چندلایه‌ی پیچیده سروکار نداریم، از روش برداری استفاده شده است. به‌منظور کاهش زمان اجرای برنامه شبکه‌های عصبی چندلایه، از جعبه ابزارهای عمومی Matlab استفاده نخواهد شد. به‌عنوان مثالی از این شیوه کدنویسی، بردار نهایی شبکه عصبی چندلایه نشان داده شده در شکل (۳)، در رابطه (۱۱) آورده شده است.

محل سکونت:

$$habitat = \left[w_{13} w_{23} w_{14} w_{24} w_{15} w_{25} w_{36} w_{46} w_{56} b_1 b_2 b_3 b_4 \right] \quad (۱۱)$$



شکل (۳): شبکه‌ی عصبی چندلایه با ساختار ۱-۳-۲.

بعد از نمایش شبکه‌های عصبی چندلایه به‌صورت بردارهای محل سکونت، برای ارزیابی هر کدام از آن‌ها (محل‌های سکونت)، لازم است که رابطه‌ای برای محاسبه شاخص مناسب‌بودن محل سکونت (تابعی مناسب) نوشته شود.

۴-۲- شاخص مناسب‌بودن زیستگاه (تابع شایستگی)

همان‌طورکه بیان شد، هدف نهایی روش‌های یادگیری، آموزش شبکه‌های عصبی مصنوعی است. مهم‌ترین بخش در یادگیری، فرآیند آموزش است. هر نمونه آموزش باید شامل، محاسبه شاخص مناسب‌بودن همه محل‌های سکونت باشد. در این مقاله، تابع شاخص مناسب‌بودن زیستگاه (برای همه نمونه‌های آموزش)، به روش میانگین مربعات خطا[1] و به‌صورت رابطه (۱۲) محاسبه می‌گردد:

$$E = \sum_{k=1}^{q} \frac{\sum_{i=1}^{m} \left(o_i^k - d_i^k \right)^2}{q} \quad (۱۲)$$

که در آن، q مبین تعداد نمونه‌های آموزش، m مبین تعداد خروجی‌ها، d_i^k مبین خروجی مطلوب از i-امین ورودی است وقتی که k-امین نمونه آموزش استفاده گردد و o_i^k مبین خروجی واقعی در ازای i-امین ورودی است وقتی که k-امین نمونه آموزش به ورودی اعمال می‌گردد. برای مثال، مقدار شاخص مناسب‌بودن محل سکونت برای i-امین محل سکونت به‌صورت رابطه (۱۳) محاسبه می‌گردد:

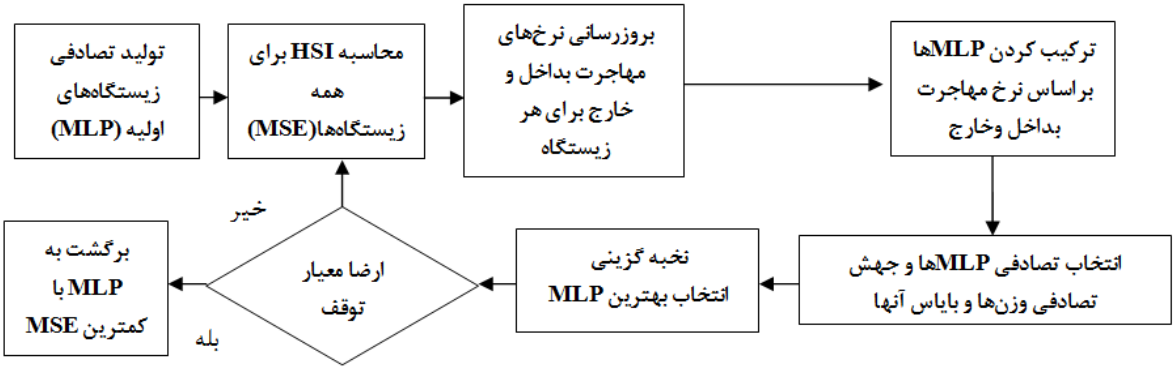
$$HSI\left(Habitat_i\right) = E\left(Habitat_i\right) \quad (۱۳)$$

می‌توان در دو مرحله با استفاده از الگوریتم بهینه‌سازی مبتنی بر جغرافیای زیستی، یادگیری در شبکه عصبی چندلایه را فرمول‌نویسی نمود. بلوک دیاگرام پیشنهادشده در شکل (۴) نشان داده شده است.

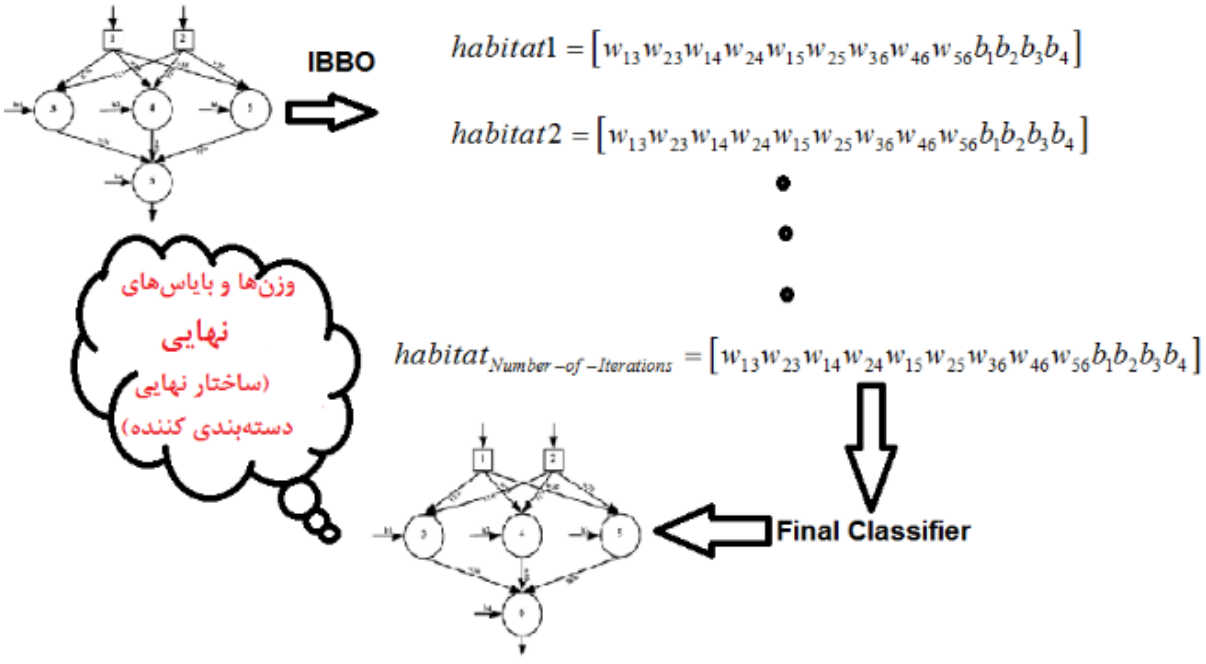
همان‌طوری‌که در شکل (۴) مشاهده می‌گردد، روش پیشنهادشده با تولید مجموعه‌های تصادفی از شبکه‌های عصبی

1- Mean Squared Error (MSE)

چندلایه بر مبنای تعداد محل‌های سکونت تعریف شده، آغاز می‌گردد. هر شبکه عصبی چندلایه متناظر با یک زیستگاه می‌باشد و هر وزن یا بایاس، با ساکنین آن زیستگاه متناظر است. بعد از گام آغازین، با استفاده از رابطه (۱۲) میانگین مربعات خطای هر شبکه‌های عصبی چندلایه محاسبه می‌گردد. درگام بعدی با استفاده از روابط (۶-۵)، نرخ‌های مهاجرت به بیرون، مهاجرت به داخل و جهش به‌روز می‌شوند. سپس شبکه‌های عصبی چندلایه براساس نرخ‌های مهاجرت به داخل و مهاجرت به بیرون با هم ترکیب می‌شوند. پس از آن هر شبکه عصبی چندلایه، بر مبنای نرخ جهش محل سکونتش تغییر می‌کند. انتخاب نخبه گام آخر روش پیشنهاد شده است، به‌طوری‌که بهترین شبکه‌های عصبی چندلایه به‌منظور جلوگیری از خرابی توسط عملگرهای جهشی و تکاملی در نسل بعدی، حفظ گردند. این مراحل (از محاسبه‌ی میانگین مربعات خطا تا انتخاب نخبه) تا ارضای شرایط پایانی ادامه می‌یابد. خلاصه مطالب بالا را می‌توان در شکل (۵) مشاهده کرد.



شکل (۴): بلوک‌دیاگرام روش پیشنهادشده.



شکل (۵): خلاصه روش پیشنهادشده.

پیچیدگی محاسبات روش پیشنهادشده به تعداد نمونه‌های آموزش گیرنده در مجموعه داده‌ها، ساختار شبکه عصبی چندلایه، تعداد محل‌های سکونت، سازوکار مهاجرت، مکانیزم جهش و مکانیزم نخبه‌گزینی وابسته است. پیچیدگی محاسباتی یک شبکه عصبی چندلایه با h گره پنهان، o خروجی و تعداد t نمونه آموزش، برابر است با $O\left(t\left(h+o\right)\right)$. در پیاده‌سازی انجام‌گرفته پیچیدگی محاسباتی مهاجرت برابر با $O\left(mn^2\right)$ است که در آن، m مبین تعداد ساکنین و n مبین تعداد محل‌های

سکونت است. ذکر این نکته لازم است که در بهترین حالت، پیچیدگی عملگر مهاجرت برابر است با $O(mn)$. پیچیدگی محاسباتی عملگر جهش در بدترین حالت برابر با $O(mn)$ است.

از آن‌جایی‌که در مرحله انتخاب نخبه، بهترین محل سکونت به روش مرتب‌کردن سریع[1] انتخاب می‌گردد، در بهترین حالت، پیچیدگی محاسباتی نخبه‌گزینی (انتخاب بهترین زیستگاه) برابر با $O(n.\log(n))$ و در بدترین حالت برابر با $O(n^2)$ خواهد بود. بنابراین پیچیدگی محاسباتی نهایی روش پیشنهادی به‌صورت رابطه (۱۴) محاسبه می‌گردد:

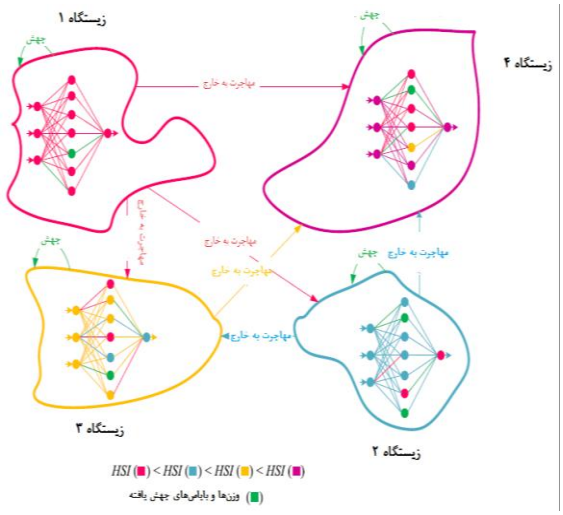
$$O(MLP,BBO)=O\left(g\left(t\left(h+o\right)+mn^2+nm+n^2\right)\right) \quad (۱۴)$$

که در آن، g مبین بیش‌ترین تعداد نسل‌ها، t مبین تعداد نمونه‌های آموزش، h مبین تعداد گره‌های پنهان، o مبین تعداد گره‌های خروجی، m مبین تعداد ساکنین و n مبین تعداد زیستگاه‌ها می‌باشد.

برای مشاهده چگونگی کار الگوریتم پیشنهادی، در شکل (۶) یک تصویر مفهومی از مهاجرت بین محل‌های سکونت برای یادگیری در یک شبکه عصبی چندلایه با استفاده از الگوریتم بهینه‌سازی مبتنی بر جغرافیای زیستی، نشان داده شده است. در این شکل، محل سکونت ۱ مناسب‌تر از محل‌های سکونت ۲، ۳ و ۴ می‌باشد، زیرا کم‌ترین شاخص مناسب‌بودن محل سکونت را دارد که نشان می‌دهد میانگین مربعات خطا برای همه نمونه‌های آزمایش، حداقل است.

همان‌طورکه ملاحظه می‌شود، زیستگاه ۱ بیش‌ترین مهاجرت به بیرون را دارد، درحالی‌که زیستگاه ۴ بیش‌ترین مهاجرت به داخل را دارد و در نتیجه ساکنین بیش‌تری (وزن‌ها و بایاس‌ها) را نسبت به محل‌های سکونت دیگر می‌پذیرد. این مهاجرت‌ها با رنگ‌های متفاوتی نشان داده شده‌اند. هم‌چنین گره‌های سبزرنگ و اتصالات آن‌ها جهش را نشان می‌دهند که برای همه ساکنین بدون درنظرگرفتن مقدار شاخص مناسب‌بودن محل سکونت اتفاق افتاده است. برای این‌که ببینید به‌صورت نظری چگونه الگوریتم بهینه‌سازی مبتنی بر جغرافیای زیستی، آموزش شبکه‌های عصبی چندلایه را بهبود می‌بخشد، مشاهدات زیر را در نظر بگیرید:

- مقادیر مختلف نرخ مهاجرت به بیرون و مهاجرت به داخل باعث ایجاد مکانیزم تکاملی برای هر محل سکونت می‌گردد که قدرت اکتشاف بیش‌تر را در پی دارد.
- قدرت اکتشاف بالاتر، الگوریتم بهینه‌سازی مبتنی بر جغرافیای زیستی را از گیرافتادن در حلقه‌های بهینه‌سازی محلی حفظ کرده و باعث رفع شرایط رکود (حالت ایستایی) در الگوریتم می‌گردد.
- از آن‌جایی‌که وزن‌ها و بایاس‌های شبکه‌های عصبی چندلایه بهتر تمایل به مهاجرت به‌سمت شبکه‌های بدتر دارند، درنتیجه میانگین‌های مربعات خطای (شاخص مناسب‌بودن محل سکونت) همه شبکه‌های عصبی چندلایه، بهبود می‌یابد و همین امر، هم‌گرایی روش پیشنهادشده را تضمین می‌نماید و همه شبکه‌های عصبی چندلایه را بهبود می‌بخشد.
- نرخ‌های جهش متفاوت هر محل سکونت به روش پیشنهادشده کمک می‌کند تا مکانیزم‌های بهره‌برداری متنوعی داشته باشد.
- نخبه‌گزینی (انتخاب بهترین محل سکونت) به روش پیشنهادشده کمک می‌کند، به‌طوری‌که این راه‌حل‌ها هرگز از بین نروند.



شکل (۶): مهاجرت بین محل‌های سکونت برای یادگیری یک شبکه MLP [۱].

۵- تشریح مطالب و نتایج

در این بخش الگوریتم بهینه‌سازی مبتنی بر جغرافیای زیستی روی دادگان سونار با ابعاد کاهش‌یافته، Lenses و Iris اعمال می‌گردد [۳۸]. هم‌چنین به‌منظور اطمینان از صحت عملکرد الگوریتم IBBO، مجموعه دادگان با الگوریتم‌های بهینه‌سازی ازدحام ذرات، ژنتیک، بهینه‌سازی کلونی مورچگان و جستجوی گرانشی مقایسه خواهند شد.

۵-۱- تنظیم پارامترها و انجام آزمایش

پارامترهای مورد نیاز و مقادیر اولیه در جدول (۱) آورده شده‌اند.

1- Quick-Sort

جدول (۱): پارامترهای اولیه الگوریتم‌ها.

الگوریتم	پارامتر	مقدار
BBO و IBBO	احتمال اصلاح ساکنین	۱
	محدوده احتمال مهاجرت به‌داخل	[۰,۱]
	اندازه پله برای انتگرال عددی احتمال	۱
	حداکثر ضریب مهاجرت به‌داخل (I) و مهاجرت به خارج (E)	۱
	احتمال جهش	۰/۰۰۵
	اندازه جمعیت	۲۰۸
	حداکثر تعداد تکرار	۲۵۰
PSO	جانمایی	اتصال کامل
	ثابت شناختی (C_1)	۱
	ثابت اجتماعی (C_2)	۱
	ثابت محلی (W)	۰/۳
	اندازه جمعیت	۲۰۸
GA	نوع	کدشده واقعی
	انتخاب	چرخ رولت
	ادغام	تک نقطه‌ای
	جهش	یکنواخت (۰/۰۱)
	اندازه جمعیت	۲۰۸
	حداکثر تعداد تکرار	۲۵۰
ACO	فرمون اولیه (τ_0)	۰/۰۰۰۰۰۱
	ثابت به‌روزرسانی فرمون (Q)	۲۰
	ثابت فرمون (q_0)	۱
	نرخ کاهش فرمون سراری (p_g)	۰/۹
	نرخ کاهش فرمون محلی (p_t)	۰/۵
	حساسیت فرمون (α)	۱
	حساسیت قابل رویت	۵
	اندازه جمعیت	۲۰۸
GSA	تعداد جرم‌ها	۶۰
	G_0	۱
	α	۲۰
	حداکثر تکرار	۵۰۰

هر شبکه ۱۰ بار آزمایش شده است. بهترین شبکه عصبی آموزش دیده از بین ۱۰ بار اجرا، انتخاب و برای مقایسه به‌کار گرفته می‌شود. نرخ دسته‌بندی و درصد خطای آزمون دو مقیاس برای مقایسه الگوریتم‌های ذکرشده می‌باشند. برای انجام یک مقایسه نسبتاً خوب، همه الگوریتم‌ها وقتی که حداکثر تعداد تکرار به ۲۵۰ رسید، متوقف می‌شوند. در نهایت، هم‌گرایی نتایج برای انجام مقایسه‌ای جامع بررسی خواهد شد. در دسته‌بندی مجموعه‌های داده، از آن‌جایی‌که برای انتخاب تعداد گره‌های پنهان استانداردی وجود ندارد. بنابراین، براساس ساختار شبکه‌های عصبی چندلایه، از پیشنهاد مطرح‌شده در [۳۷] و از رابطه (۱۵) استفاده خواهد شد.

$$H = 2\times N + 1 \qquad (۱۵)$$

که در آن، N مبین تعداد ورودی‌ها و H مبین تعداد گره‌های پنهان است.

در ابتدا دسته‌بندی‌کننده طراحی‌شده برروی دادگان Iris و Lenses (توصیف‌شده در جدول (۲)) اعمال شده و عملکرد دسته‌بندی‌کننده از نظر نرخ دسته‌بندی، اجتناب از گیرکردن در کمینه محلی و سرعت هم‌گرایی آزموده می‌شود. هر الگوریتم ۱۰ بار اجرا شده و نرخ دسته‌بندی، میانگین و انحراف معیار حداقل خطا و مقدار P-value در جداول (۴-۳) به ترتیب برای مجموعه دادگان Iris و Lenses نمایش داده شده است. نرخ دسته‌بندی، دقت دسته‌بندی‌کننده طراحی‌شده را نشان می‌دهد و مقادیر میانگین و انحراف معیار حداقل خطا و P-value نشان‌دهنده قدرت الگوریتم در اجتناب از بهینه محلی می‌باشد [۳]. نمونه‌ای از نتایج این مقایسه به‌ترتیب برای دادگان Iris و Lenses در اشکال (۸-۷) نمایش داده شده است. سپس در قسمت بعد دادگان سونار به‌طور مفصل توضیح داده‌شده و دسته‌بندی‌کننده‌های طراحی‌شده را بر روی این نوع دادگان نیز آزمایش می‌کنیم.

جدول (۲): دادگان مورد استفاده در این مقاله.

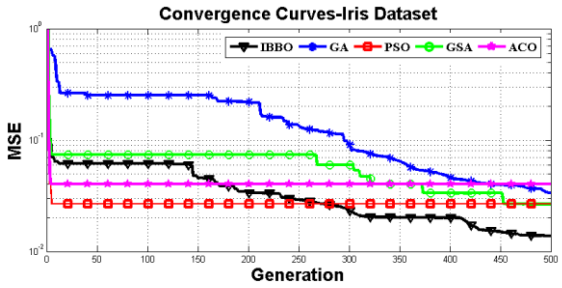
نام	وظیفه پیش‌فرض	ویژگی مشخصه	تعداد ویژگی	تعداد مثال	سال
Iris	دسته‌بندی	چندمتغیری	۴	۱۵۰	۱۹۸۸
Lenses	دسته‌بندی	چندمتغیری	۴	۲۴	۱۹۹۰

جدول (۳): نتایج حاصل از اعمال دسته‌بندی‌کننده‌های مختلف بر روی دادگان Iris.

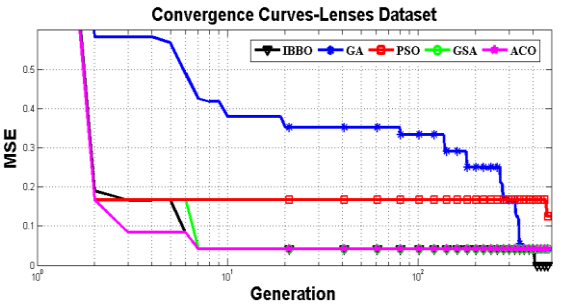
الگوریتم	نرخ دسته‌بندی	P-Values	MSE (AVE±STD)
MLPIBBO	**۸۸/٪۶۶۶**	**N/A**	**۰/۰۰۱۴±۰/۰۰۱۴۵**
MLPGA	۸۵/۳۵۲۲٪	۰/۰۰۱۱	۰/۱۲۲۵±۰/۱۲۴۷
MLPPSO	۸۷/۸۲۲۲٪	۰/۰۰۰۴۷	۰/۱۳۱۱±۰/۱۱۴۷
MLACO	۸۳/۶۳۳۳٪	۰/۰۰۰۱۷	۰/۱۷۲۹±۰/۲۳۳۳
MLPGSA	۸۵/۳۳۳۳٪	۰/۰۰۰۱۸	۰/۱۵۷۷±۰/۲۲۲۴

جدول (۴): نتایج حاصل از اعمال دسته‌بندی‌کننده‌های مختلف بر روی دادگان Lenses.

الگوریتم	نرخ دسته‌بندی	P-Values	MSE (AVE±STD)
MLPIBBO	**۸۹/۸۹۳۳٪**	**N/A**	**۰/۱۲۸۳±۰/۰۰۱۴**
MLPGA	۸۴/۲۲۲۲٪	۰/۰۰۴۷	۰/۱۵۱۹±۰/۰۲۶۹
MLPPSO	۸۲/۶۶۶۶٪	۰/۰۰۷۸	۰/۲۰۱۱±۰/۲۰۷۶
MLACO	۷۲/۲۲۳۳٪	۰/۰۰۰۷	۰/۳۱۴۹±۰/۲۹۶۵
MLPGSA	۷۳/۶۶۶۶٪	۰/۰۰۰۷	۰/۲۵۲۷±۰/۱۷۴۴



شکل (۷): مقایسه دقت دسته‌بندی و هم‌گرایی الگوریتم‌های مختلف اعمال‌شده به دادگان Iris.

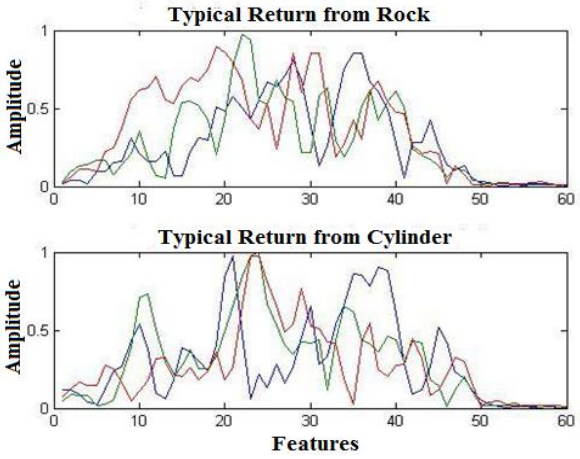


شکل (۸): مقایسه دقت دسته‌بندی و همگرایی الگوریتم‌های مختلف اعمال شده به دادگان Lenses.

۵-۲- دادگان سونار

دادگان مورد استفاده در این مقاله از آزمایش Gorman و Sejnowski موجود در مراجع [۳۹-۳۸] استخراج شده است. در این آزمایش یک سیلندر فلزی به طول ۵ فوت و یک صخره هم‌اندازه با آن در بستر شنی دریا قرار داده شده‌اند و یک پالس چیرپ FM خطی پهن باند[1] (ka=55/6) به سمت آن‌ها فرستاده شده است. اکوهای برگشتی در فاصله ۱۰ متری از آن‌ها جمع‌آوری شده است.

بر اساس SNR اکوی دریافتی از ۱۲۰۰ اکو، ۲۰۸ اکو که SNR آن‌ها بین ۴ dB تا ۱۵ dB است، انتخاب شده‌اند. از این ۲۰۸ اکو، ۱۱۱ عدد مربوط به سیلندر فلزی و ۹۷ عدد مربوط به صخره هستند. شکل (۹) نمونه‌هایی از اکوهای دریافتی از صخره و سیلندر فلزی را نشان می‌دهد.



شکل (۹): نمایش دامنه اکوهای برگشتی از سیلندر فلزی و صخره.

از نقطه نظر ریاضی، PCA سعی در پیداکردن یک نگاشت خطی به‌نام M می‌نماید که تابع هزینه رابطه (۱۶) را حداکثر نماید.

۵-۳- کاهش ابعاد دادگان با استفاده از روش تحلیل عناصر اصلی

تحلیل عناصر اصلی (PCA) یک روش خطی برای کاهش ابعاد دادگان می‌باشد. این روش به‌وسیله تعبیه دادگان در زیرفضاهای خطی با ابعاد پایین‌تر عمل می‌کند. در واقع این روش محورهای مختصات را به گونه‌ای می‌چرخاند که دادگان با حداکثر واریانس در راستای محورهای اصلی قرار بگیرند. اگرچه روش‌های زیادی برای کاهش ابعاد در سال‌های اخیر معرفی شده است، ما در این مقاله از روش PCA بدون ناظر و کلاسیک استفاده کرده‌ایم. همان‌گونه‌که در مرجع [۴۰] اثبات شده است، روش‌های جدید و ترکیبی برای دادگان مجازی دارای عملکرد بسیار بهتری نسبت

1- Wide-Band Linear FM

به روش‌های دسته یک هستند، اما روش‌های دسته یک مانند PCA برای داده‌گان دنیای واقعی دارای عملکرد بسیار بهتری می باشند. از طرف دیگر، برای سنجش عملکرد PCA طراحی‌شده دو روش وجود دارد که عبارتند از: الف) سنجش همراه با ناظر و ب) سنجش بدون ناظر. روش با ناظر از نظر دقت بسیار کارآمد می‌باشد، این در حالی است که از لحاظ زمانی بسیار پرهزینه می‌باشد. به‌دلیل نقصی که در روش اول وجود دارد (افزایش بار محاسباتی و پیچیدگی زمانی)، در این مقاله از روش دوم (بدون ناظر) استفاده کرده‌ایم.

$$trace(\mathbf{M}^T \, \mathrm{cov}(\mathbf{X})\mathbf{M}) \qquad (۱۶)$$

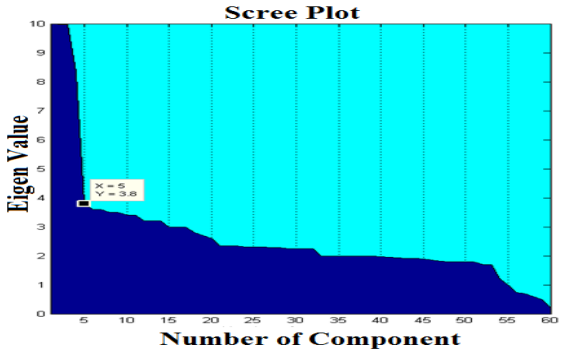
در این رابطه، $\mathrm{cov}(\mathbf{X})$ ماتریس کواریانس داده‌گان X می‌باشد. می‌توان نشان داد که این نگاشت خطی به‌وسیله d بردار ویژگی اصلی ماتریس کواریانس داده‌گان با میانگین صفر شکل می‌گیرد. از این رو این نوع PCA سعی در حل رابطه (۱۷) دارد.

$$\mathrm{cov}(\mathbf{X})\mathbf{M} = \lambda\mathbf{M} \qquad (۱۷)$$

با حل این رابطه می‌توان d مقدار ویژه λ را به‌دست آورد. داده‌گان اصلی x_i با ابعاد D (در این مقاله $D=60$) توسط نگاشت $\mathbf{M}$ و رابطه (۱۸) به داده‌گان جدید y_i با ابعاد d که $d<D$ است، تبدیل می‌شوند.

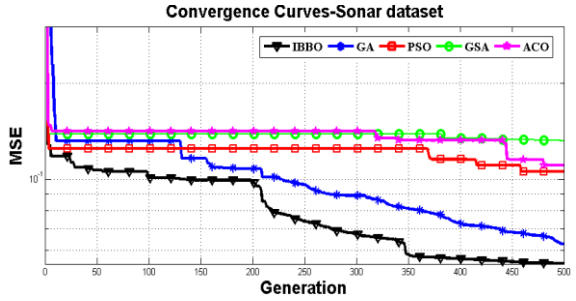
$$\mathbf{Y} = \mathbf{XM} \qquad (۱۸)$$

انتخاب مقدار d یکی دیگر از مسائل چالش‌برانگیز این روش می‌باشد. در این مقاله برای انتخاب d از روش Scree Test استفاده شده است. این روش [۴۱] برای انتخاب d از نمایش نزولی نمودار مقادیر ویژه استفاده می‌کند. بدین صورت که نقطه‌ای را که نمودار افت شدیدی دارد، ولی هنوز در مقادیر کوچک ثابت نشده است را به‌عنوان d انتخاب می‌کند. نتیجه این آزمایش در شکل (۱۰) نمایش داده شده است. همان‌گونه که در این شکل دیده می‌شود، برای داده‌گان سونار، $۶ < d < ۹$ می‌تواند انتخاب شود که برای دقت بیش‌تر d = ۹ انتخاب شده است.



شکل (۱۰): نتایج حاصل از انجام Scree Test بر روی داده‌گان سونار

از نقطه‌نظر آماری، الگوریتم بهینه‌سازی مبتنی بر جغرافیای زیستی، به‌اندازه کافی توانایی جلوگیری از گیرافتادن در حداقل‌های محلی را دارد. کارآیی بهتر الگوریتم IBBO در جستجوی همه فضای مسأله می‌باشد. به‌دلیل ماهیت طبیعی این الگوریتم‌ها و به‌خاطر مهاجرت و جهش در جلوگیری از گیرافتادن در حداقل‌های محلی این عمل به خوبی انجام می‌پذیرد. این عملگرها باعث تغییرات ناگهانی در انتخاب راه‌حل مسأله می‌گردند که در نتیجه توانایی شناسایی الگوریتم‌های بهینه‌سازی مبتنی بر جغرافیای زیستی و ژنتیک را به‌اندازه کافی بهبود می‌دهد.



شکل (۱۱): مقایسه دقت دسته‌بندی و هم‌گرایی الگوریتم‌های مختلف اعمال‌شده به داده‌گان سونار.

جدول (۵): نتایج حاصل از اعمال دسته‌بندی‌کننده‌های مختلف بر روی داده‌گان سونار

الگوریتم	نرخ دسته‌بندی	P-Values	MSE (AVE±STD)
MLPBBO	۸۸/۲۳۵۲٪	۰/۰۰۳۹	۰/۱۲۱۹±۰/۰۲۶۹
MLPGA	۶۵/۸۶۲۲٪	۰/۰۰۱۷	۰/۳۵۱۱±۰/۱۰۷۶
MLPPSO	۸۷/۳۳۳۳٪	۰/۰۰۰۱	۰/۱۳۴۵±۰/۰۹۶۵
MLACO	۷۳/۹۳۳۳٪	۰	۰/۱۷۲۲±۰/۱۰۶۴
MLPGSA	۸۰/۱۱۱۲٪	۰	۰/۲۰۱۹±۰/۱۴۲۳

نتایج ضعیف الگوریتم‌های بهینه‌سازی کلونی مورچگان و انبوه ذرات نیز به‌دلیل ماهیت طبیعی این الگوریتم‌ها است. این الگوریتم‌ها عملگری را برای تغییر ناگهانی راه‌حل مسأله ندارند و در نتیجه در حداقل‌های محلی گرفتار می‌شوند. علاوه براین، الگوریتم بهینه‌سازی کلونی مورچگان، از ماتریس فرومون که قدرت یادگیری و بهره‌برداری الگوریتم را افزایش می‌دهد، استفاده می‌کند که یک مزیت در مسائل ترکیبی است، ولی احتمال گیرافتادن در حداقل‌های محلی را افزایش می‌دهد. الگوریتم‌های انبوه ذرات به‌مقدار خیلی زیاد به نحوه توزیع اولیه ذرات و محرک‌های اولیه آن‌ها بر مبنای جاذبه بینشان، وابسته است. اگر تعداد زیادی از ذرات در حداقل‌های محلی گرفتار شوند، الگوریتم به‌مقدار کوچکی از گیرافتادن ذرات دیگر جلوگیری خواهد کرد.

دلیل کارآیی بهتر الگوریتم بهینه‌سازی مبتنی بر جغرافیای زیستی در مقایسه با الگوریتم ژنتیک در اکثر مسائل، نرخ‌های متفاوت مهاجرت به بیرون و مهاجرت به داخل هر محل سکونت است. الگوریتم بهینه‌سازی مبتنی بر جغرافیای زیستی در مقایسه با الگوریتم ژنتیک که برای همه محل‌های سکونت جامعه آماری آن، یک نرخ تولید مجدد کلی دارد، دو نرخ (مهاجرت به بیرون و مهاجرت به داخل) برای هر زیستگاه دارد. این مسأله باعث ایجاد رفتار تکاملی و قدرت شناسایی متفاوت می‌گردد. به‌طور خلاصه، می‌توانیم بگوییم در مسأله آموزش شبکه‌های عصبی چندلایه، توانایی اکتشاف، بسیار مهم است. بنابراین، در حل مسائل پیچیده با استفاده از شبکه‌های عصبی چندلایه، به گام‌های جستجوی تصادفی و ناگهانی برای جلوگیری از گیرافتادن در حداقل‌های محلی نیاز است.

این مقاله نشان داد که عملگرهای (مهاجرت) الگوریتم بهینه‌سازی مبتنی بر جغرافیای زیستی، برای این منظور بسیار مناسب هستند. در ادامه دلایل برتری کارآیی IBBO در مقایسه با الگوریتم پس‌انتشار و سایر الگوریتم‌های تکاملی آورده شده است:

- مقادیر متفاوت نرخ‌های مهاجرت به بیرون و داخل اطلاعات گوناگونی درخصوص تغییر محل‌های سکونت و در نتیجه آن، بهبود اکتشاف را در پی دارد.
- در مدت تولید، از آن‌جایی‌که ساکنین در محل‌های سکونت با شاخص بالا تمایل به مهاجرت به محل‌های سکونت با شاخص پایین دارند، شاخص مناسب‌بودن همه زیستگاه‌ها بهبود می‌یابد. این امر، هم‌گرایی الگوریتم بهینه‌سازی مبتنی بر جغرافیای زیستی را تضمین می‌کند.
- عملگرهای مهاجرت توانایی اکتشاف الگوریتم را افزایش می‌دهند و درنتیجه الگوریتم بهینه‌سازی مبتنی بر جغرافیای زیستی در حداقل‌های محلی گرفتار نمی‌شود.
- نرخ‌های جهش متفاوت باعث متنوع‌شدن محل‌های سکونت می‌گردد.
- نخبه‌گزینی به الگوریتم‌های بهینه‌سازی مبتنی بر جغرافیای زیستی کمک می‌کند تا بتوان راه‌حل‌های مناسب را ذخیره و دوباره مورد استفاده قرار داد و بنابراین هیچ‌گاه از روند محاسبات کنار نروند.

۶- نتیجه‌گیری

در این مقاله، یک شبکه عصبی چندلایه با استفاده از الگوریتم IBBO، آموزش داده شد. دادگان سونار با ابعاد کاهش‌یافته، به‌منظور بررسی تأثیر الگوریتم بهینه‌سازی مبتنی بر جغرافیای زیستی در آموزش شبکه‌های عصبی چندلایه، مورد استفاده قرار گرفت. نتایج آماری به دست آمده با نتایج حاصل از الگوریتم بهینه‌سازی گروهی ذرات، الگوریتم ژنتیک، الگوریتم کلونی مورچه‌ها و الگوریتم جستجوی گرانشی، جهت اثبات کارآیی، مقایسه گردید. نتایج حاصل نشان می‌دهد که الگوریتم بهینه‌سازی مبتنی بر جغرافیای زیستی به‌اندازه کافی توانایی جلوگیری از گیرافتادن در حداقل‌های محلی را در مقابل الگوریتم‌های معیار دارد. به‌علاوه، به‌وضوح کارآیی بهتر الگوریتم IBBO در آموزش شبکه‌های عصبی چندلایه بر حسب دقت نتایج و سرعت هم‌گرایی از نتایج به‌دست‌آمده دیده می‌شود.

۷- مراجع

[1] M. R. Mosavi, M. Khishe, and M. Aghababaie, "Modeling and Mitigation of Active Sonar Clutter," Noshahr University of Marine Science and Technology, 2015.

[2] M. R. Mosavi, M. Khishe, A. Ghamgosar and M. J. Ghalandari, "Classification of Sonar Data Set using the Gray Wolf Optimizer Algorithm", Journal of Electronics Industries, Vol.7, No.1, pp.27-41, 1395. (In Persian)

[3] M. R. Mosavi, M. Khishe, and E. Ebrahimi, "Classification of Sonar Targets using OMKC," Genetic Algorithm and Statistical Moments," Journal of Advances in Computer Research, vol.7, no.1, pp. 143-156, 2016.

[4] L. S. Nguyen, D. Frauendorfer, M. S. Mast, and D. Gatica-Perez, "Hire Me: Computational Inference of Hirability in Employment Interviews based on Nonverbal Behavior," IEEE Transactions on Multimedia, vol. 16, no. 4, pp. 1018-1031, 2014.

[5] M. R. Mosavi, M. Khishe, Y. Hatam Khani, and M. Shabani, "Training Radial Basis Function Neural Network using Stochastic Fractal Search Algorithm to Classify Sonar Dataset," Iranian Journal of Electrical and Electronic Engineering, vol. 13, no. 1, 2017.

[6] E. Oja, "Unsupervised Learning in Neural Computation," Theoretical Computer Science, vol. 287, pp. 187-207, 2002.

[7] N. Zhang, "An Online Gradient Method with Momentum for Two-Layer Feedforward Neural Networks," Applied Mathematics and Computation, vol. 212, pp. 488-498, 2009.

[8] D. R. Hush and B. G. Horne, "Progress in Supervised Neural Networks," IEEE Signal Processing Magazine, vol. 10, pp. 8-39, 1993.

[9] S. C. Ng, C. C. Cheung, S. H. Leung, and A. Luk, "Fast Convergence for Backpropagation Network with Magnified Gradient Function," IEEE Joint Conference on Neural Networks, vol. 3, pp. 1903-1908, 2003.

[10] G. Magoulas, M. Vrahatis, and G. Androulakis, "On the Alleviation of the Problem of Local Minima in Back-Propagation," Nonlinear Analysis, Theory, Methods & Applications, vol. 30, no. 7, pp. 4545-4550, 1997.

[11] Y. C. Ho and D. L. Pepyne, "Simple Explanation of the No-Free-Lunch Theorem and Its Implications," Journal of Optimization Theory and Applications, vol. 115, no. 3, pp. 549-570, 2002.

[12] P. Wang, X. Yu, and J. Lu, "Identification and Evolution of Structurally Dominant Nodes in Protein-Protein Interaction

Networks," IEEE Transactions on Biomedical Circuits and Systems, vol. 8, no. 1, pp. 87-97, 2014.

[13] V. G. Gudise and G. K. Venayagamoorthy, "Comparison of Particle Swarm Optimization and Backpropagation as Training Algorithms for Neural Networks," IEEE Swarm Intelligence Symposium, pp. 110-117, 2003.

[14] R. Mendes, P. Cortez, M. Rocha, and J. Neves, "Particle Swarms for Feedforward Neural Network Training," IEEE Joint Conference on Neural Networks, pp. 1895-1899, 2002.

[15] U. Seiffert, "Multiple Layer Perceptron Training using Genetic Algorithms," European Symposium on Artificial Neural Networks, pp. 159-164, 2001.

[16] C. Blum and K. Socha, "Training Feed-forward Neural Networks with Ant Colony Optimization: An Application to Pattern Classification," Hybrid Intelligent Systems Conference, pp. 6-14, 2005.

[17] G. Li, J. Na, D. Stoten, and X. Ren, "Adaptive Neural Network Feedforward Control for Dynamically Substructured Systems," IEEE Transactions on Control Systems Technology, vol. 22, no. 3, pp. 944-954, 2014.

[18] I. Boussaid, J. Lepagnot, and P. Siarry, "A Survey on Optimization Metaheuristics," Information Sciences, vol. 237, pp. 82-117, 2013.

[19] S. Mirjalili and S. Z. M. Hashim, "A New Hybrid PSOGSA Algorithm for Function Optimization," IEEE Conference on Computer and Information Application, pp. 374-377, 2010.

[20] S. Mirjalili, S. M. Mirjalili, and A. Lewis, "Grey Wolf Optimizer," Advances in Engineering Software, vol. 69, pp. 46-61, 2014.

[21] S. Mirjalili, S. M. Mirjalili, and X. S. Yang, "Binary Bat Algorithm," Neural Computing and Applications, vol. 25, no. 3-4, pp. 663-681, 2013.

[22] M. R. Mosavi and M. Khishe, "Training a Feed-Forward Neural Network using Particle Swarm Optimizer with Autonomous Groups for Sonar Target Classification," Journal of Circuits, Systems, and Computers (JCSC), vol. 26, no. 11, November 2017.

[23] M. Khishe, M. R. Mosavi, and M. Kaveh, "Improved Migration Models of Biogeography-based Optimization for Sonar Data Set Classification using Neural Network," Applied Acoustic, vol. 118, pp. 15-29, 2017.

[24] S. M. Mirjalili, S. Mirjalili, and A. Lewis, "A Novel Multi-Objective Optimization Framework for Designing Photonic Crystal Waveguides," Photonics Technology Letters, vol. 26, no. 2, pp. 146-149, 2014.

[25] S. M. Mirjalili, S. Mirjalili, A. Lewis, and K. Abedi, "A Tri-Objective Particle Swarm Optimizer for Designing Line Defect Photonic Crystal Waveguides," Photonics and Nanostructures Fundamentals and Applications, vol. 12, no. 2, pp. 152-163, 2014.

[26] S. Saremi, S. M. Mirjalili, and S. Mirjalili, "Unit Cell Topology Optimization of Line Defect Photonic Crystal Waveguide," Procedia Technolgy, vol. 12, pp. 174-179, 2014.

[27] S. Saremi, S. M. Mirjalili, and S. Mirjalili, "Chaotic Krill Herd Optimization Algorithm," Procedia Technology, vol. 12, pp. 180-185, 2014.

[28] M. R. Mosavi, M. Khishe, and M. Akbarisani, "Neural Network Trained by Biogeography-based Optimizer with Chaos for Sonar Data Set Classification," Wireless Personal Communications (WPC), pp. 1-20, 2017.

V. Abedifar, M. Eshghi, S. Mirjalili, and S. M. Mirjalili, "An Optimized Virtual Network Mapping using PSO in Cloud Computing," 21st Iranian Conference on Electrical Engineering, pp. 1-6, 2013.

[29] M. R. Mosavi, M. Kaveh, and M. Khishe, "Sonar Data Set Classification using MLP Neural Network Trained by Non-linear Migration Rates BBO," The Fourth Iranian Conference on Engineering Electromagnetic (ICEEM 2016), pp. 1-5, March 2016.

[30] W. Guo, L. Wang, and Q. Wu, "An Analysis of the Migration Rates for Biogeography-based Optimization," Information Science, vol. 254, pp. 111-140, 2014.

[31] M. R. Mosavi, M. Kaveh, M. Khishe, and M. Aghababaee, "Design and implementation a Sonar Data Set Classifier by using MLP NN Trained by Improved Biogeography-based Optimization," The Second National Conference on Marine Technology, MMT, 2016.

[32] M. Ergezer, D. Simon, and D. Du, "Oppositional Biogeography-based Optimization", IEEE Conference on Systems, Man and Cybernetics, San Antonio, Texas, pp. 1035-1040, 2009.

[33] R. Rarick, D. Simon, F. E. Villaseca, and B. Vyakaranam, "Biogeography-based Optimization and the Solution of the Power Flow Problem," IEEE Conference on Systems, Man and Cybernetics, San Antonio, Texas, pp. 1029-1034, 2009.

[34] J. R. Zhang, J. Zhang, T. M. Lok, and M. R. Lyu, "A Hybrid Particle Swarm Optimization-Back-propagation Algorithm for Feedforward Neural Network Training," Applied Mathematics and Computation, vol. 185, pp. 1026-1037, 2007.

[35] S. Mirjalili, S. Z. M. Hashim, and H. M. Sardroudi, "Training Feedforward Neural Networks using Hybrid Particle Swarm Optimization and Gravitational Search Algorithm," Applied Mathematics and Computation, vol. 218, pp. 11125-11137, 2012.

[36] S. Mirjalili, "Hybrid Particle Swarm Optimization and Gravitational Search Algorithm for Multilayer Perceptron Learning," University Teknologi Malaysia (UTM), 2011.

[37] http://archive.ics.uci.edu/ml/datasets/Connectionist+Bench+(Sonar,+Mines+vs.+Rocks).

[38] R. P. Gorman and T. J. Sejnowski, "Analysis of Hidden Units in a Layered Network Trained to Classify Sonar Targets," Neural Networks, vol. 1, pp. 75-89, 1988.

[39] S. C. H. Hoi, R. Jin, P. Zhao, and T. Yang, "Online Multiple Kernel Classification," Machine Learning, vol. 90, no. 2, pp. 289-316, 2013.

[40] R. K. Jade, L. K. Verma, and K. Verma, "Classification using Neural Network and Support Vector Machine for Sonar Data Set," International Journal of Computer Trends and Technology, vol. 4, no. 2, pp. 116-119, 2013.

مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"
ویژه‌نامه کنفرانس بین‌المللی ترکیبیات، رمزنگاری و محاسبات، ص ۶۷ -۶۳

اصول جدید برای الگوریتم‌های رمزنگاری

نوید عبودی[۱]، ناصر هاشمی[۲*]

۱- کارشناس ارشد، دانشکده ریاضی و علوم کامپیوتر دانشگاه امیر کبیر، ۲- استادیار، دانشکده ریاضی و علوم کامپیوتر دانشگاه امیر کبیر

(دریافت: ۹۵/۰۷/۰۵، پذیرش: ۹۶/۰۳/۰۶)

چکیده

با توجه به اهمیت اصول رمزنگاری، هدف ما در این مقاله این است که یک سری اصول جدید برای طراحی الگوریتم‌های رمزنگاری با حفظ اصول قبلی ارائه دهیم که با استفاده از این اصول، زمان لازم برای پیداکردن کلید بالاتر رفته و هم‌چنین منجر به افزایش سختی تحلیل الگوریتم‌ها شود و در نتیجه بتوانیم از امنیت حفظ اطلاعات بالاتری برخوردار باشیم.

واژه‌های کلیدی: رمزنگاری متقارن، اصول کرشهف، انتقال امن اطلاعات

۱- مقدمه[۱]

کرشهف در سال ۱۸۸۳، اصولی را برای رمزنگاری اطلاعات اعلام کرد که این اصول در شش بند ارائه گردید و تاکنون از آن‌ها در طراحی الگوریتم‌های رمزنگاری استفاده شده است. نکته قابل توجه این است که این اصول بیش از ۱۳۰ سال قبل نوشته شده است و بنا به پیشرفت سریع در علم و فناوری و افزایش سرعت رایانه ها و سریع‌ترشدن تجزیه و تحلیل الگوریتم‌های پیچیده در رایانه، نیازمند به افزودن اصول جدید در جهت تکمیل اصول قبلی است. برای به‌روزماندن الگوریتم‌ها با توجه به سرعت پیشرفت فناوری، روز به روز این اصول باید ارتقاء یابند و بر اساس آن‌ها، الگوریتم‌های جدیدی نوشته شوند به‌طوری‌که درجه سختی تحلیل الگوریتم‌ها پیچیده‌تر شود تا هم‌چنان از امنیت حفظ اطلاعات بالاتری برخوردار باشند.

در ادامه ابتدا به بیان اصول کرشهف پرداخته و سپس در بخش سه، اصول بهبودیافته رمزنگاری بیان خواهد شد و در بخش چهار، اصول جدید را تجزیه و تحلیل خواهیم کرد و با اصول کرشهف مقایسه کرده و دلایل اهمیت اصول جدید به صورت مجزا گفته خواهد شد و در انتها نتیجه‌گیری کلی صورت خواهد گرفت.

۲- اصول کرشهف

اصول کرشهف در شش بند ارائه شده است که این شش بند عبارتند از [۱]:

۲-۱) سیستم رمزنگاری از لحاظ تئوری و عملی غیرقابل شکست باشد.

۲-۲) سیستم رمزنگار باید هیچ نکته پنهان و محرمانه‌ای نداشته باشد بلکه تنها چیزی که باید سری نگه داشته شود کلید رمز است. طبق اصل اساسی کرکهافس، طراح سیستم رمزنگار نباید جزئیات سیستم خود را حتی از دشمنان مخفی نگاه دارد.

۲-۳) کلید رمز باید به گونه‌ای قابل انتخاب باشد که اولاً بتوان به راحتی آن را عوض کرد و ثانیاً بتوان آن را به خاطر سپرد و نیازی به یادداشت‌کردن کلید رمز نباشد.

۲-۴) متون رمزنگاری‌شده باید از طریق خطوط تلگراف قابل مخابره باشند.

۲-۵) دستگاه رمزنگاری یا اسناد رمزشده باید توسط یک نفر قابل حمل باشد.

۲-۶) سیستم رمزنگاری باید به سهولت قابل راه‌اندازی و کاربری باشد. چنین سیستمی نباید به آموزش‌های مفصل و رعایت فهرست بزرگی از قواعد و دستورالعمل‌ها نیاز داشته باشد.

۳- اصول بهبودیافته رمزنگاری

بعضی از اصول کرشهف مثل بندهای ۲-۴ الی ۲-۶ به‌خاطر پیشرفت فناوری و وسایل ارتباطی امروزه امری بدیهی است و اگر این اصول رعایت نشود الگوریتم نوشته‌شده کارایی خاصی نخواهد داشت و قابل اجرا نخواهد بود و هر الگوریتم کارایی این سه اصل را داراست. سه اصل مابقی یعنی ۲-۱ الی ۲-۳ در هر زمانی لازم-الاجرا است و باید در تمام الگوریتم‌های رمزنگاری رعایت شود تا الگوریتم نوشته‌شده حافظ امنیت داده‌ها باشد. امروزه به‌دلیل

* رایانامه نویسنده مسئول: nhashemi@aut.ac.ir

وجود رایانه و سرعت پیشرفت روزافزون فن‌آوری، این اصول و الگوریتم‌ها بیش از پیش نیازمند تغییر و بهبود هستند و باید متناسب با نیاز زمان نوشته شوند و به آن‌ها رفته رفته باید اصول جدیدی اضافه شده و بهبود یابند تا هم‌چنان امنیت حفظ اطلاعات بالاتری داشته باشیم و اطلاعات شخصی ما و دیگران به راحتی در اختیار فرد ثالث قرار نگیرد و متحمل ضررهای جانی و مالی نشویم.

در زیر مهم‌ترین اصول کرشهف همراه با اصول جدید آمده است که در آن، اصول ۳-۱ و ۳-۲ همان اصول قبلی ۲-۱ و ۲-۲ می‌باشند و اصل ۳-۳ تکمیل یافته اصل قبلی یعنی ۲-۳ است و بعد از آن اصول پیشنهادی جدید در سه بند ۳-۴ ، ۳-۵ و ۳-۶ ارائه شده است:

۳-۱) یک سیستم رمزنگاری از نظر تئوری و عملی باید غیرقابل شکست باشد.

۳-۲) سیستم رمزنگار باید هیچ نکته پنهان و محرمانه‌ای نداشته باشد بلکه تنها چیزی که باید سری نگه داشته شود کلید رمز است. طبق اصل اساسی کرکهافس، طراح سیستم رمزنگار نباید جزئیات سیستم خود را حتی از دشمنان مخفی نگاه دارد.

۳-۳) باید کلید رمز تصادفی باشد به‌طوری‌که با احتمال بالا قابل حدس‌زدن نباشد.

۳-۴) باید طول کلید ثابت و مشخص و محدود به الگوریتم رمزنگاری نبوده و به صورت تصادفی انتخاب شود و یا در اختیار رمزکننده باشد.

۳-۵) باید خود الگوریتم رمزنگاری تصادفی باشد به‌طوری‌که برای هر متن و کلیدی به‌صورت یکسان عمل نکند.

۳-۶) حتی‌الامکان از قطعه‌بندی متن اصلی به اندازه متن کلید پرهیز شده و از رمزنگاری گسسته و قطعه‌ای استفاده نشود بدین مفهوم که کل متن به‌صورت یک‌جا رمزنگاری شود و یا تعداد قطعات متن اصلی در کم‌ترین حد ممکن باشد (که تعداد این قطعات به سرعت و اندازه حافظه رایانه‌ها بستگی دارد و با پیشرفت فناوری و افزایش سرعت رایانه‌ها اندازه قطعه‌های انتخاب‌شده بیش‌تر می‌شود به‌طوری‌که طول قطعه انتخاب‌شده برابر طول متن اصلی می شود).

ملاحظه۱:

رعایت اصول بالا یک الگوریتم خوب برای رمزنگاری برای متونی با طول بیش‌تر از یک حد معین می‌دهد ولی برای متونی با طول کلید کم‌تر از آن دارای امنیت بالایی نیست و برای به‌دست‌آوردن این حد کران باید به مسئله زیر توجه کرد. با توجه به سرعت رایانه‌ها و تعداد حالات الگوریتم و طول کلید می‌توان به یک حد پایین مطلوب برای طول کلید رسید به‌طوری‌که با احتمال پایین در زمان طولانی الگوریتم شکسته شود و برای شکستن الگوریتم با احتمال بالای $\frac{1}{2}$ زمان زیادی لازم باشد. اگر p را برابر احتمال موفقیت و k برابر تعداد بیت‌ها و ۲^{k} تعداد حالات باشد و حالات طوری انتخاب شوند که حالت تکراری در انتخاب‌هایمان نداشته باشیم بنا به مسئله گوی و سکه و یا مسئله روز تولد داریم:

$$p > 1 - \frac{2^k}{2^k} * \frac{2^k - 1}{2^k} * \frac{2^k - 2}{2^k} * \dots * \frac{2^k - i}{2^k}$$

عبارت بالا برای iهـای بیش‌تر از $1.17 * 2^{k/2}$ احتمال p بالای ۵۰٪ نتیجه می‌دهد.

$$\text{مدت زمان جستجو} = \frac{\text{تعداد کل حالات جستجو}}{\text{سرعت هر رایانه} \times \text{تعداد رایانه}}$$

برای مثال، اگر از ۲۰۰۰ رایانه برای رمزگشایی استفاده شود و هر رایانه بتواند در هر ثانیه، ۱۰۰۰ حالت از کل حالات را برای پیداکردن کلید مسئله بررسی کند و حالت‌هایی که برای رایانه‌ها انتخاب می‌شوند حالت تکراری نداشته باشند برای شکست الگوریتم با احتمال ۵۰٪ در مدت زمان بیش از یک سال باید طول کلید حداقل برابر k بیت باشد.

اگر متن با کلیدی به‌طول k رمزنگاری شده باشد آن‌گاه در کل ۲^{k} حالت خواهیم داشت و برای پیداکردن کلید رمز با احتمال بالای ۵۰٪ باید حداقل $1.17 * 2^{\frac{k}{2}}$ حالت مختلف را جستجو کنیم. در مثال بالا اندازه حد پایین برای k به صورت زیر به‌دست می‌آید:

$$1\ year = 365 * 86400 = \frac{1.17 * 2^{k/2}}{2000 * 1000}$$

$$k = 2 * \log_2\left(\frac{365 * 86400 * 1000 * 2000}{1.17}\right) \approx 91.23 \approx 92$$

با توجه به مفروضات بالا، برای این که بخواهیم برای شکست الگوریتم با احتمال بالای ۵۰٪ مدت زمانی بیش‌تر از یک سال طول بکشد، باید طول کلید بیش از ۹۲ بیت باشد. که اگر تعداد رایانه‌ها و یا سرعت رایانه‌ها زیادتر شود باید بر این مقدار اضافه گردد تا احتمال شکست الگوریتم ما هم‌چنان کم باشد و با احتمال بالای ۵۰٪ به راحتی نشکند. در الگوریتم اولیه DES که از طول کلیدی برابر ۵۶ بیت استفاده می‌شد اگر بخواهیم با احتمال بالای ۵۰٪ متن رمز را پیدا کنیم، نیاز داریم که $۲^{۲۸}$ حالت را جستجو کرده و اگر از یک رایانه استفاده کنیم که در هر ثانیه ۱۰۰۰ حالت را بتواند جستجو کند، در مدت زمانی کم‌تر از ۲۵۶۰۰۰ ثانیه برابر کم‌تر از ۳ روز می‌توان کلید رمز را پیدا کرد و یکی از علل شکست الگوریتمی DES همین مسئله می‌تواند باشد.

۴- تجزیه و تحلیل اصول جدید و مقایسه با اصول کرشهف

اصولی که کرشهف اعلام کرد، اصول اولیه و کلی برای رمزنگاری است و رعایت این اصول برای هر الگوریتم رمزنگاری ضروری است و پایه و اساس الگوریتم‌های رمزنگاری است و شرط لازم برای ایجاد امنیت بالا است ولی شرط کامل و کافی نیست. به عبارت دیگر، اگر الگوریتم رمزنگاری این اصول را رعایت نکند قطعاً امنیت بالایی ندارد و برای حفظ اطلاعات مناسب نیست.

الگوریتم‌های موجود که در حال حاضر استفاده می‌شوند همگی بر اساس این اصول نوشته شده‌اند. الگوریتمی مثل الگوریتم DES که با استفاده از این اصول طراحی شده بود، از سال ۱۹۷۷ تا ۱۹۹۸ استفاده می‌شد ولی در سال ۱۹۹۸ Hellman و Diffie یک الگوریتم و سخت‌افزاری معرفی کردند که با این سخت‌افزار، الگوریتم DES شکسته شد و در عرض کم‌تر از هفت ساعت، کلیدرمز متن رمزشده پیدا گردید و رابطه‌ای بین متن رمزشده و متن اصلی با کلید پیدا شد. بعد از آن، این الگوریتم را تغییر دادند و به‌جای یک بار رمزنگاری، از سه بار با سه کلید متفاوت رمزنگاری کردند: در رمزنگاری DES جدید، ابتدا با کلید اول رمزنگاری می‌شود و بعد با کلید دوم رمزگشایی می‌شود و سپس با کلید سوم دوباره رمزنگاری می‌شود تا با این کار درجه سختی الگوریتم بالاتر رفته و به راحتی رابطه‌ای بین متن رمزشده و متن کلید پیدا نشود. این درحالی است که روش کلی این الگوریتم تغییر چندانی نکرده است و فقط تعداد تکرار آن زیاد شده است. الگوریتم‌های دیگر رمزنگاری که مهم‌ترین و مشهورترین آن‌ها الگوریتم AES است همانند الگوریتم DES، به صورت قطعه‌ای و گسسته رمزنگاری می‌شوند و طول متن رمز این الگوریتم‌ها ثابت است [۳-۲].

برای برطرف‌کردن مشکل‌های گفته‌شده و بهبود الگوریتم‌های رمزنگاری و بالابردن درجه سختی آن‌ها، اصول جدید را در بخش سه ارائه کردیم که در ادامه به بررسی و تحلیل این اصول جدید خواهیم پرداخت.

الف) اثبات درستی‌اصول ۳-۱ و ۳-۲

این دو اصل، همان اصول اصلی ۲-۱ و ۲-۲ کرشهف هستند که قبلاً اهمیت استفاده از این دو اصول برای برقراری امنیت بالا توسط خود کرشهف اثبات شده است.

ب) اثبات درستی‌اصل ۳-۳

اصل ۳-۳ اصلاح‌شده اصل ۲-۳ کرشهف است. در اصل ۲-۳ گفته شده بود که کلید رمز باید طوری نوشته شود که قابل حفظ‌کردن باشد که در این صورت متن کلید به متون زبان و اعداد وابستگی پیدا کرده و تعداد حالات کلید کم‌تر می‌شود و با احتمال زیاد، قابل حدس‌زدن خواهد بود. درحالی‌که امروزه از رایانه و وسایل الکتریکی در رمزنگاری استفاده می‌شود و خود این سیستم‌ها توانایی تولید کلید مجزا برای هر متن را دارند. امروزه چون از الگوریتم‌های شبه‌تصادفی در تولید کلید رمز استفاده می‌شود باید این الگوریتم‌ها طوری طراحی شوند که برای کلید، کل حالات موجود را با احتمال یکسان تولید کنند. برای هر متنی سعی شود کلید مجزایی تولید گردد، کلید دو متن یکسان انتخاب نشوند، متن آن‌ها ساده و وابسته به هم نباشند. در نتیجه حدث‌زدن کلید متون سخت‌تر می‌شود و تعداد حالات انتخاب‌شده برای کلید در رمزنگاری بیش‌تر خواهد شد و رمزنگاری امن‌تری خواهیم داشت.

ج) اثبات درستی اصل ۳-۴

اصل ۳-۴ گویای این است که باید طول متن کلید یکسان نباشد و یکی از دلایل شکست الگوریتم‌هایی مثل DES همین طول پایین و ثابت متن کلید است. برای مثال اگر طول متن اصلی ۱۰۲۴ بیت باشد و طول متن کلید الگوریتم‌های موجود ۱۲۸ بیت باشد چون این متن به قطعاتی به طول ۱۲۸ بیت تقسیم می‌شوند و از بین $۲^{۱۰۲۴}$ حالت موجود برای متن اصلی ما کافی است بین $۲^{۱۲۸}$ حالت مختلف به دنبال جملات با معنی بگردیم که تعداد جملات با معنی به این نسبت خیلی کم‌تر می‌شود و اگر طول کلید یکسان نباشد برای یک متن ۱۰۲۴ بیتی ما به تعداد زیر:

$$P = 2^1 + 2^1 + 2^3 + \cdots + 2^{1024} = 2^{2048} - 1$$

حالت خواهیم داشت که این عدد نسبت به $۲^{۱۲۸}$ یک عدد خیلی بزرگی است.

در الگوریتم‌های موجود برای هر طولی از متن اصلی به اندازه m کافی است ما بین $۲^{۱۲۸}$ حالت به دنبال جواب بگردیم درحالی که اگر طول متن رمز ثابت نباشد تعداد این حالات برابر $۲^{۲m}$ - ۱ حالت می‌شود یعنی کل بازه را می‌توانند در برگیرد و پیداکردن متن اصلی از روی متن رمزشده سخت‌تر می‌شود.

ه) اثبات درستی اصل ۳-۵

بنا به اصل ۳-۵، علاوه بر این که متن و طول کلید تصادفی است باید جزئیات الگوریتم نیز تصادفی باشد و در طراحی الگوریتم از الگوریتم‌های تولید شبه اعداد تصادفی استفاده کرد و الگوریتم را به‌صورت شبه تصادفی اجرا کرد. به‌عنوان مثال اگر الگوریتم AES دارای چهار مرحله a، b،c وd است و این مراحل شش بار به‌صورت زیر و با نظم و ترتیب عمل می‌کنند:

a1,b1,c1,d1,a2,b2,c2,d2,a3,b3,c3,d3,a4,b4,c4,d4,a5,b5,c5,d5,a6,b6,c6,d6

تصادفی‌شدن الگوریتم به این معنی است که این چهار مرحله با این نظم و ترتیب اجرا نشوند و به صورت تصادفی با هم جابه‌جا شوند و به‌جای یک راه و روش ثابت بتواند یکی از روش‌های موجود در زیر را طی کند:

1)a1,b1,c1,d1,a2,b2,c2,d2,a3,b3,c3,d3,a4,b4,c4,d4,a5,b5,c5,d5,a6,b6,c6,d6

2)b1,c1,d1a1,b2,c2,d2,a2,b3,c3,d3,a3,b4,c4,d4,a4,b5,c5,d5,a5,b6,c6,d6,a6

3) ,b1,c1,d1,a2, ,c2,d2,a3,b3, ,d3,a4,b4,c4, , ,b5,c5,d5,a6, ,c6,d

4)a1,b1, ,d1,a2,b2, ,d2,a3,b3,c3, ,a4,b4,c4,d4,a5, ,c5,d5,a6,b6,c6,d6

5)a1,b1,d1,c1,a2,b2,d2,c2,a3,c3,b3,d3,a4,c4,b4,d4,a5,b5,c5,d5,a6,b6,c6,d6

6)……

در این‌جا چون مراحل اجرای الگوریتم و خود این مراحل به صورت تصادفی، ثابت و منظم برای همه متن‌ها اجرا نمی‌شوند، درجه سختی الگوریتم بالاتر می‌رود و فردی که سعی در شکستن الگوریتم دارد دقیقاً نمی‌داند که متن داده‌شده با کدام روش از روش‌های موجود اجرا شده است و این کار مدت زمان شکسته‌شدن الگوریتم را بالاتر می‌برد.

الگوریتم برای متن و کلیدهای یکسان باید به یک صورت رمز شود تا فرد گیرنده بتواند متن رمزشده را به متن اصلی برگرداند و فرد گیرنده اعداد تصادفی تولیدشده توسط رمزکننده را بتواند به همان ترتیب تولید کند. مگر این‌که روش حل الگوریتم به طرقی بین فرستنده و گیرنده ردوبدل شده باشد و در این الگوریتم‌ها از الگوریتم‌های برگشت‌پذیر استفاده شود تا فرد گیرنده به متن اصلی دست پیدا کند.

و) اثبات درستی اصل ۳-۶

اصل ۳-۶ که مهم‌ترین اصل از اصول بالاست حائز این نکته است که باید در الگوریتم از قطعه‌بندی متن اصلی و رمزنگاری گسسته پرهیز شود. این کار دو نتیجه مهم دارد یکی این‌که معلوم نمی‌شود طول متن کلید چند بیت است و برای به‌دست‌آوردن یک حالت از حالات موجود باید به‌جای تحلیل یک قطعه باید کل متن رمزشده را تحلیل کرد تا به جواب رسید و نتیجه دوم این است که زمان لازم برای به‌دست‌آوردن کلید رمز برای فرد ثالث که قصد شکست الگوریتم را دارد، بالاتر می‌رود. برای مثال، اگر طول متن اصلی برابر ۱۰۰۰۰۰۰ بیت باشد و طول متن کلید برابر ۱۰۰ بیت باشد به‌جای تحلیل ۱۰۰ بیت باید ۱۰۰۰۰۰۰ بیت را تحلیل کرد و زمان لازم برای این‌کار ۱۰۰۰۰۰ برابر می‌شود.

ملاحظه ۲:

یکی از اصولی که در اصول کرشهف مطرح نشده است و با رعایت این اصل احتمال شکسته‌شدن الگوریتم و متن اصلی برابر صفر می‌شود و نمی‌توان از روی متن رمزشده به متن اصلی رسید، اصل ۳-۴ است. یعنی الگوریتمی که در آن بتوان کل حالات موجود را تولید کرد. وقتی که کل حالات موجود را بتوان تولید کرد دیگر نمی‌توان فهمید که متن اصلی با کدام یک از این متن‌ها رمز شده است، مگر با دانستن متن کلید. اصل جدید ۳-۴ این امکان را به فرستنده و گیرنده می‌دهد که طول متن کلید را هم‌اندازه طول متن کلید اصلی انتخاب کنند که این یک اصل مهم در رمزنگاری است. درحالی‌که الگوریتم‌های قبلی چنین امکانی را برای فرستنده فراهم نکرده بودند و این یکی از نواقص الگوریتم‌های موجود و اصول کرشهف است که به این نکته توجه نکرده است و الگوریتم‌هایی که ساخته شده‌اند، این اصل اساسی رمزنگاری را نادیده گرفته‌اند.

ملاحظه ۳:

سوالی که در این‌جا مطرح می‌شود این است که آیا متنی که با اصول جدید با طول کلید ۴۰ بیت رمز می‌شود دارای امنیت بالاتری نسبت به الگوریتم‌های ساخته‌شده با اصول قبلی با طول کلید ۶۴ بیت دارد یا نه؟

در جواب این سوال باید گفت که در الگوریتم‌های قبلی برای هر متن اصلی، به طول m بیت و متن رمز به طول k بیت نیاز داریم که به دنبال متن کلیدهایی بگردیم که طول آن‌ها به اندازه k بیت بوده و نیازی به جستجوی حالاتی به طول بیش‌تر و کم‌تر از k بیت نیست، چون k عددی معلوم و ثابت است ولی در اصول جدید این عدد k عدد ثابتی نیست و هر عددی بین ۱ تا m را می‌تواند به خود بگیرد. برای مثال، اگر طول کلید ۴۰ بیت باشد فرد ثالث که قصد شکستن الگوریتم را دارد دقیقاً نمی‌داند که طول کلید، چند بیت است و باید به‌دنبال کل حالات بگردد. اگر طول کلید ۴۰ بیت باشد باید کلیدهایی به طول ۳۰ بیت و ۳۸ بیت را هم بررسی کنیم. در الگوریتم‌های قبلی تعداد حالات کلید برابر ۲^{k} حالت بوده و در اصول جدید این تعداد حالات به تعداد $۲^{۲m}-۱$ حالت افزایش می‌یابد و در نتیجه، درجه سختی الگوریتم برای بعضی از حالات پیچیده و برای بعضی از حالات آسان است. ولی در کل چون تعداد حالات بیش‌تر است و ما دقیقاً این حالات سخت و آسان را نمی‌دانیم برای به‌دست‌آوردن جواب باید همه این‌ها را بگردیم که در بین حالات موجود، حالات سخت هم

انتخاب می‌شوند و در کل درجه سختی الگوریتم بالاتر از الگوریتم‌های دیگر می‌شود.

۵- نتیجه‌گیری

بنا به اصول اولیه رمزنگاری کرشهف، الگوریتم‌های نوشته‌شده با این اصول، به‌راحتی شکسته می‌شوند زیرا بعضی از نکات مهم رمزنگاری در آن نادیده گرفته شده است. یکی از این نکات این است که همه این الگوریتم‌ها به صورت قطعه‌ای و گسسته متن‌های اصلی را رمزنگاری می‌کنند و امروزه با احتمال بالا بعضی از این الگوریتم‌ها به‌راحتی شکسته شده‌اند. بنابرین، احتمال شکسته‌شدن الگوریتم‌های مشابه زیاد است. با پیشرفت فناوری و افزایش سرعت رایانه‌ها، لازم است که اصول رمزنگاری داده‌ها اصلاح شده و بهبود یابند و الگوریتم‌های جدید براساس اصول معرفی‌شده در این مقاله برای رمزنگاری طراحی شوند. امروزه باید سعی شود در تولید الگوریتم‌های جدید رمزنگاری، از الگوریتم‌های پیچیده ریاضی مثل الگوریتم‌های تصادفی و الگوریتم‌های کوانتومی در رمزنگاری استفاده شود تا درجه امنیت و حفظ اطلاعات هم‌چنان بالا باشد واحتمال شکسته‌شدن الگوریتم‌ها کم‌تر شود [۴].

۶- مراجع

[1] "Kerckhoffs' Law," WordNet 3.0, Farlex clipart collection, 2003-2008. Princeton University, Clipart.com, Farlex Inc. 23 May2016. http://www.thefreedictionary.com/Kerckhoffs%27+Law

[2] A. K. Mandal, C. Parakash, and A.Tiwari, Performance evaluation of cryptographic algorithms: DES and AES, In Electrical, Electronics and Computer Science (SCEECS), 2012 IEEE Students' Conference on, IEEE, pp. 1-5, March 2012.

[3] L. B. Kish, D. Abbott, and C. G. Granqvist, "Critical analysis of the Bennett–Riedel attack on secure cryptographic key distributions via the Kirchhoff-law–Johnson-noise scheme," PloS one, vol. 8, no. 12, p. e81810, 2013.

[4] T. Adamski, "Introduction to optical quantum cryptography," In Photonics Applications in Astronomy, Communications, Industry, and High-Energy Physics Experiments 2007, pp. 693723-693723, International Society for Optics and Photonics, October 2007.

مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"
ویژه‌نامه کنفرانس بین‌المللی ترکیبیات، رمزنگاری و محاسبات، ص ۷۷ -۶۹

محاسبات بر مبنای رایانه‌های کوانتومی و کاربرد آن برای تجزیه اعداد مرکب

علی جبار رشیدی[1*]، رحیم اصغری[2]، مصطفی اسلامی[3]

۱- دانشیار، ۲- استادیار، دانشگاه صنعتی مالک اشتر تهران ۳-استادیار، دانشگاه مازندران

(دریافت: ۹۵/۰۷/۰۵، پذیرش: ۹۶/۰۳/۰۶)

چکیده

در مقاله حاضر تبدیل فوریه کوانتومی به‌عنوان جزء کلیدی در الگوریتم تجزیه اعداد طبیعی به روش کوانتومی برای استفاده در الگوریتم شر معرفی می‌گردد. پیاده‌سازی کارای الگوریتم شر که تنها الگوریتم شناخته‌شده برای تجزیه اعداد با پیچیدگی زمانی چندجمله است، هدف اصلی این مقاله است. در این مقاله، پیچیدگی محاسباتی مراحل مختلف الگوریتم تجزیه اعداد طبیعی و مدارهای کوانتومی برای اجرای تبدیل فوریه کوانتومی ارائه شده‌اند. هم‌چنین، در این مقاله تبدیل فوریه کوانتومی تعمیم و برای انجام محاسبات بهبود یافته است. الگوریتم شر بهبودیافته در نرم‌افزار میپل با استفاده از کتابخانه محاسبات کوانتومی پیاده‌سازی شده است. با استفاده از این کتابخانه مفاهیم کوانتومی درهم تنیدگی و موازی در رایانه کلاسیک شبیه‌سازی شده‌اند. مثال‌هایی از شبیه‌سازی تخمین فاز به همراه جدول و نمودار برای نمایش قابلیت برنامه ارائه کرده‌ایم. در پایان مثال‌هایی به همراه نتایج برای محاسبات الگوریتم شر بهبود داده‌شده، آورده‌ایم.

واژه‌های کلیدی: محاسبات کوانتومی، تبدیل فوریه کوانتومی، الگوریتم شر، تخمین فاز، شبیه‌سازی

۱- مقدمه[1]

تا این لحظه مهم‌ترین یافته در محاسبات کوانتومی این است که رایانه های کوانتومی می‌توانند محاسباتی را که بر روی یک رایانه کلاسیک، در زمان چندجمله‌ای قابل پیاده‌سازی نیستند، به‌طور کارآمد اجرا کنند [۱]. به‌عنوان‌مثال، پیداکردن عامل‌های اول یک عدد صحیح n بیتی با استفاده از بهترین الگوریتم‌های کلاسیک شناخته‌شده به $\exp(O(n^{\frac{1}{3}}\log^{\frac{2}{3}} n))$ عملیات نیاز دارد [۲]. بنابراین، تجزیه اعداد به عامل‌های اول روی یک کامپیوتر کلاسیک، به‌عنوان یک مسئله سخت مورد توجه قرار می‌گیرد. اهمیت رایانه کوانتومی در این‌جاست که الگوریتم شر کوانتومی (که روی یک رایانه کوانتومی اجرا می‌شود) می‌تواند این کار را با استفاده از $O(n^2 \log n \log\log n))$ عملیات انجام دهد [۳]. تجزیه اعداد مرکب به عامل‌های اول از این نظر با اهمیت است که الگوریتم رمزنگاری RSA به عنوان یکی از پرکاربردترین الگوریتم‌های رمزنگاری مبتنی بر آن است. این الگوریتم رمزنگاری به دلیل کارایی بالا در محاسبه، سال‌هاست که در مهم‌ترین مراکز امنیتی، مراکز مالی تا نهادهای نظامی و ... ، مورد استفاده قرار می‌گیرد [۴]. هم‌چنین تبدیل فوریه کوانتومی که مهم‌ترین قسمت الگوریتم شر (بخش کوانتومی) را شامل می‌شود و البته در بسیاری از محاسبات کوانتومی دیگر هم ظاهر می‌شود از اهمیت ویژه‌ای برخوردار است که به آن می پردازیم. مسئله دیگر این است که در مقاله‌ها و کتاب‌های مختلفی در رابطه با تبدیل فوریه نوشته شده است [۵-۷] ولی درک عملکرد این الگوریتم موضوعی است که در اکثر این منابع کم‌تر مورد توجه قرار می‌گیرد. مقاله حاضر در تلاش است که به این زمینه بیش‌تر بپردازد.

براساس مشاهدات فاینمن[1] [۸]، شبیه‌سازی انجام محاسبات که باید در رایانه کوانتومی صورت بپذیرد، در رایانه‌های کلاسیک ناممکن است. این مسئله را طی انجام این مقاله به‌خوبی درک کردیم. با این حال، می‌توان برای انجام محاسبات جبری و محاسبات ماتریسی به شبیه‌سازی عملگرهای کوانتومی مانند کت‌ها، گیت‌ها و عملگرهای یکانی و درنتیجه تبدیل فوریه کوانتومی در رایانه های کوانتومی پرداخت.

در مقاله [۹]، الگوریتم شر در نرم‌افزار میپل[2] شبیه‌سازی شد، ولی در آن‌جا تنها به شبیه‌سازی بخش‌های کلاسیک نرم‌افزار اکتفا شده است. در آن مقاله، یافتن مرتبه با استفاده از نرم‌افزار مرتبه‌یاب میپل انجام گرفت و با محاسبه مرتبه شبیه‌سازی الگوریتم شر صورت پذیرفت. در الگوریتم شر ذکرشده درآن مقاله، در واقع برخی از جنبه‌های خاص این الگوریتم شبیه‌سازی شده است. به‌عنوان‌مثال، عملگرهای یکانی که در رایانه کوانتومی اعمال می‌شوند، شبیه‌سازی نشده ولی نتایج حاصل از آن تبدیل‌ها را در رایانه کلاسیک (به‌صورت احتمالی "تقریباً حتماً") ساخته است.

1- Von Neumann
2- Maple

* رایانامه نویسنده مسئول: Aiorashid@yahoo.com

در مقاله حاضر برای پیاده‌سازی، نرم‌افزار میپل را انتخاب کرده‌ایم زیرا این نرم‌افزار از یک‌سو دارای ابزارهای بسیار مناسب جبر خطی است و از طرفی دیگر، کتابخانه مناسبی را برای انجام محاسبات کوانتومی توسعه داده است [۱۲-۱۰]. کتابخانه‌ای که در این مقاله مورد استفاده قرار داده‌ایم Open QUACS است که توسط کریس مک کوبین توسعه داده شد [۱۳]. این کتابخانه با وجود محدودیتی که دارد، ابزارهای لازم جهت ایجاد کت‌ها و گیت‌های لازم شبیه‌سازی مدارهای کوانتومی را در اختیار ما قرار می‌دهد. با استفاده از این کتابخانه، می‌توان تبدیل فوریه مورد نظر را به‌صورت عملگر ماتریسی ساخت که برای اختصارنویسی، از ارائه کدها صرف‌نظر کرده‌ایم.

در این مقاله، تبدیل فوریه کوانتومی را که بخش کلیدی الگوریتم تجزیه اعداد صحیح به عوامل اول و بسیاری الگوریتم‌های کوانتومی دیگر است، مورد بررسی قرار می‌دهیم. تبدیل فوریه کوانتومی عبارت از یک الگوریتم کوانتومی مؤثر برای اجرای یک تبدیل فوریه است [۱۴]. به کمک تبدیل فوریه کوانتومی، تخمین فاز کوانتومی که تقریبی از مقادیر ویژه یک عملگر یکانی، تحت شرایط معین است، امکان‌پذیر می‌شود [۱۵]. این کار به ما اجازه می‌دهد که مسائلی مانند مسئله یافتن درجه و مسئله تجزیه اعداد صحیح به عامل‌های اول را مشابه آن‌چه در رایانه کوانتومی انجام می‌شود شبیه‌سازی کنیم. مثال‌هایی از تخمین فاز با استفاده از برنامه، ارائه شده است. در مقاله حاضر پیچیدگی زمانی مراحل مختلف الگوریتم ارائه‌شده و گام‌های الگوریتم شر برای تجزیه اعداد مرکب آورده شده‌اند.

ساختار مقاله به‌این‌ترتیب است: ابتدا در بخش ۲، تبدیل فوریه کوانتومی و نیز فرم تعمیم‌یافته آن را ارائه کرده و در بخش ۳، تخمین فاز کوانتومی براساس تبدیل فوریه کوانتومی تعمیم‌یافته، بیان شده است. در بخش ۴، مرتبه‌یابی کوانتومی را مطرح کرده و درنهایت در بخش ۵، الگوریتم شر برای تجزیه اعداد صحیح مثبت، به‌عنوان کاربردی از تبدیل فوریه کوانتومی تعمیم‌یافته، شبیه‌سازی و نتایج ارائه گردیده‌اند.

۲- تبدیل فوریه کوانتومی

یافته‌های جدید در محاسبه کوانتومی شامل انجام تبدیلاتی است که می‌توانند روی یک کامپیوتر کوانتومی، خیلی سریع‌تر از یک کامپیوتر کلاسیک اجرا شوند. این یافته، ساخت الگوریتم‌های سریع برای کامپیوترهای کوانتومی را ممکن ساخته است [۱۶]. تبدیل فوریه گسسته، یک بردار از اعداد مختلط را به عنوان ورودی و به صورت $x_0, \dots, x_{N-1}$ را (طول بردار N، یک پارامتر ثابت است) می‌گیرد. خروجی آن (داده تبدیل‌شده)، یک بردار از اعداد مختلط $y_0, \dots, y_{N-1}$ است که توسط رابطه (۱) تعریف می‌شود:

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi ijk/N} \qquad (۱)$$

تبدیل فوریه کوانتومی دقیقاً همان تبدیل فوریه گسسته است ولی نحوه نمادگذاری‌ها با توجه به نحوه نمادگذاری‌ها در فیزیک کوانتوم برای تبدیل فوریه کوانتومی، کمی متفاوت می‌شود. همان‌طورکه در رابطه (۲) نشان داده شده است، تبدیل فوریه کوانتومی روی پایه‌های $|0\rangle, \dots, |N-1\rangle$ تعریف می‌شود.

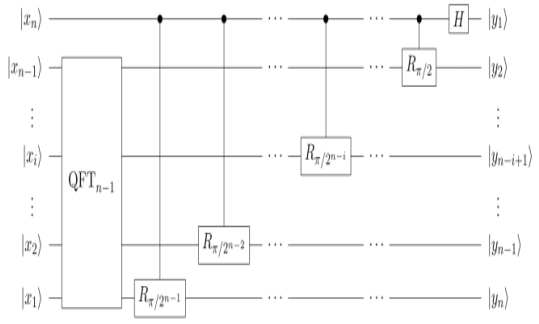
$$|j\rangle \to \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi ijk/N} |k\rangle \qquad (۲)$$

تبدیل بالا تبدیلی یکانی است و می‌تواند بر روی یک کامپیوتر کوانتومی پیاده‌سازی شود. در این رابطه، متغیر N که برابر با 2^n است را در نظر می‌گیریم که n در آن، عددی صحیح بوده و بردارهای $|0\rangle, \dots, |2^n-1\rangle$ هم پایه‌های محاسباتی برای یک رایانه کوانتومی n کیوبیتی محسوب می‌شوند. در این صورت می‌توان حالت $|j\rangle$ را با استفاده از نمایش باینری $j = j_1 j_2 \dots j_n$ نشان داد. هم‌چنین می‌توان حالت $0.j_L j_{L+1} \dots j_m$ را به‌صورت $\frac{j_L}{2} + \frac{j_{L+1}}{4} + \dots + \frac{j_m}{2^{m-L+1}}$ نیز نمایش داد.

به کمک خواص جبری، تبدیل فوریه کوانتومی می‌تواند به‌صورت رابطه (۵-۳) ارائه شود:

$$|j_1, \dots, j_n\rangle \to \frac{(|0\rangle + e^{2\pi i 0.j_n}|1\rangle) \dots (|0\rangle + e^{2\pi i 0.j_1 j_2 \dots j_n}|1\rangle)}{2^{n/2}} \qquad (۳)$$

این نمایش به ما اجازه پیاده‌سازی یک مدار کوانتومی کارآمد، جهت محاسبه تبدیل فوریه کوانتومی را می‌دهد. رابطه (۳)، استخراج یک مدار کارآمد برای تبدیل فوریه کوانتومی را آسان می‌سازد. یک چنین مداری در شکل (۱) نشان داده شده است [۵].



شکل (۱): مدار پیاده‌سازی تبدیل فوریه کوانتومی

گیت R_K (گیت چرخش شرطی)، بیانگر یک تبدیل یکانی است و ماتریس نظیر آن در رابطه (۴) ارائه گردیده است:

$$R_k = \begin{bmatrix} 1 & 0 \\ 0 & 2^{2\pi i/2^k} \end{bmatrix} \qquad (۴)$$

1- Cris macquin

در مدار شکل (۱)، ابتدا یک گیت هادامارد[1] و n-۱ چرخش شرطی، روی اولین کیوبیت اعمال می‌شود یعنی در مجموع n گیت مورد استفاده قرار می‌گیرد. سپس روی دومین کیوبیت، یک گیت هادامارد و n-۲ چرخش شرطی یعنی در مجموع n-۱ گیت اعمال می‌شوند.

به این ترتیب، تعداد گیت‌های مورد نیاز در این مدار برابر با $n+(n-1)+...+1=\frac{n(n+1)}{2}$ خواهد بود. البته این تعداد گیت، بدون احتساب گیت‌های جابه‌جایی است. از طرفی به تعداد $\frac{n}{2}$ گیت جابه‌جایی نیز مورد نیاز است که هر گیت جابه‌جایی با استفاده از سه گیت CNOT، پیاده‌سازی می‌شود. بنابراین، این مدار یک الگوریتم از مرتبه $\Theta(n^2)$ برای اجرای تبدیل فوریه کوانتومی فراهم می‌کند. برعکس، بهترین الگوریتم‌های کلاسیک برای محاسبه تبدیل فوریه گسسته عبارتند از: الگوریتم‌هایی مثل تبدیل فوریه سریع (FFT[2]) که تبدیل فوریه گسسته را با استفاده از $\Theta(n2^n)$ گیت، محاسبه می‌کند [۱۷].

در نتیجه، محاسبه تبدیل فوریه روی یک کامپیوتر کلاسیک نسبت به محاسبه تبدیل فوریه کوانتومی روی یک کامپیوتر کوانتومی، به‌طور نمایی به عملگرهای بیش‌تری نیاز دارد.

۳- تعمیم تبدیل فوریه

برای به‌دست‌آوردن کارایی بهتر، می‌توان الگوریتم فوریه کوانتومی را تعمیم داد. در این‌جا به‌طور خلاصه به نحوه تعمیم الگوریتم فوریه با استفاده از چندجمله‌ای‌های متعامد (مانند لاگور[3] و هرمیت[4]) می‌پردازیم. فرض کنید تابع $f\in H$ بوده که در آن H فضای هیلبرت است. هم‌چنین فرض کنید $\{\phi_n\}_{n\in\mathbb{N}}$ خانواده‌ای از بردارها در فضای هیلبرت H باشد، در این صورت می‌توان بر اساس خانواده بردارها یک عملگر به صورت زیر تعریف کرد:

$$\forall n\in\mathbb{N}, Uf[n]=\langle f,\phi_n\rangle \qquad (۵)$$

این عملگر، اساساً یک کار انجام می‌دهد و آن اختصاص مجموعه‌ای از اعداد به تابع f است، به این صورت که n امین عدد متناظر با ضرب داخلی تابع f در φ_n (می‌توان به‌جای ضرب داخلی روابط دیگری نیز تعریف نمود) است. برای ساخت مجدد تابع f از عملگر تعریف‌شده، باید عملگر ساخته‌شده (در اینجا U) وارون‌پذیر باشد (به‌عنوان‌مثال عملگری که با استفاده از توابع سینوسی و کسینوسی مانند تبدیل فوریه معمولی ساخته می‌شود). مطلب دوم این است که نمی‌توان هر تابع دلخواه f را بازسازی کرد. دنباله ساخته‌شده قابی از فضای هیلبرت خواهد بود اگر ثابت‌های مثبت a و b برای هر $f\in H$ وجود داشته باشند به‌طوری‌که رابطه زیر برقرار باشد: [۱۸]

$$a\|f\|^2\le\sum_{n\in\mathbb{N}}\left|\langle f,\phi_n\rangle\right|^2\le b\|f\|^2 \qquad (۶)$$

از طرفی، اگر $a=b$ باشد این قاب فشرده نامیده می‌شود و عملگر به‌دست‌آمده را عملگر قاب[5] می‌نامند و ثابت می‌شود که U عملگر قاب است اگر و فقط اگر در برد خود وارون‌پذیر متناهی باشد. اکنون فرمول‌بندی در فضای پیوسته را ارائه می‌کنیم که به‌سادگی قابل‌تعمیم به حالت گسسته خواهد بود. ایده تعمیم‌دادن تبدیل فوریه کوانتومی به تحلیل آنالیز فوریه برای معادلات دیفرانسیل معمولی در مجموعه اعداد حقیقی باز می‌گردد.

در حالت ساده معادله اشتروم لیوول[6] را در نیم‌صفحه $[0,\infty)$ به صورت زیر در نظر می‌گیریم:

$$Lf=-\frac{d^2f}{dx^2}+q(x)f(x)=g(x) \qquad (۸)$$
$$\cos\alpha f(0)+\sin\alpha f'(0)=0$$

که در آن، تابع q برای $t\ge 0$ و دربازه $[0,t]$ و نه لزوماً در $[0,\infty)$ انتگرال‌پذیر است. توابع f و g هم درمجموعه اعداد حقیقی پیوسته مشتق‌پذیر هستند. هم چنین در این‌جا ممکن است به‌شرط دومی نیاز داشته باشیم که در بی‌نهایت باید برقرار باشد.

برای هرعدد مختلط λ تابع ویژه و یکتای $\phi_\lambda(x)$ ای وجود دارد به‌طوری‌که در روابط زیر صدق می کند:

$$\begin{aligned}&L\phi_\lambda=\lambda\phi_\lambda\\&\cos\alpha\phi_\lambda(0)+\sin\alpha\phi_{\lambda'}(0)=0\\&-\sin\alpha\phi_\lambda(0)+\cos\alpha\phi_{\lambda'}(0)=1\\&\phi_\lambda\in L^2[0,\infty)\end{aligned} \qquad (۹)$$

$\phi_\lambda(x)$ ممکن است در بی‌نهایت شرایطی را برآورده نماید. اگر λ به u همگرا شود، این توابع تقریباً همه‌جا دارای حد نقطه‌ای λ خواهند بود که لزوماً در فضای هیلبرت $L^2[0,\infty)$ قرار ندارند، ولی برای $t\ge 0$ و در هر بازه متناهی $[0,t]$ دارای انتگرال مرتبه دوم خواهند بود. درصورتی‌که تابع ϕ_u یک تابع ویژه متناظر با u باشد، در فضای هیلبرت $L^2[0,\infty)$ قرار خواهد گرفت.

قضیه اشتروم لیوول [۱۹]: فرض کنید عملگر Γ در دامنه $D(\Gamma)$ ، که شامل توابع پیوسته مطلق موضعی در بازه $[0,\infty)$ هستند، قرار می‌گیرد. هم‌چنین فرض می‌کنیم که این توابع شروط مورد

1- Hadamard
2- Fast Fourier Transform
3- Laguerre
4- Hermit
5- Frame operator
6- Sturm-Liouville

نیاز در نقاط صفر و ∞ را برآورده می‌کنند. در این صورت انـدازه μ روی Γ که روی طیف $\sigma(L)$ از عملگـر توزیـع مـی‌شـود به‌طوری‌که تبدیل فوریه تعمیم‌یافتـه روی $L^2[\Gamma,\mu]$ مـی باشـد، به‌صورت حد زیر خواهد بود:

$$\hat{f}(u)=\lim_{r\to\infty}\int_0^r f(x)\phi_u(x)dx \qquad (۹)$$

پـس وارون تبـدیل فوریـه کوانتـومی تعمـیم‌یافتـه هـم در $L^2[0,\infty]$ برابر با رابطه زیر خواهد بود:

$$f(u)=\lim_{r\to\infty}\int_{-r}^{r}\hat{f}(x)\phi_u(x)d\mu(u) \qquad (۱۰)$$

علاوه بر آن، با استفاده از معادله پارسوال خواهیم داشت:

$$f_{L^2}\neq\hat{f}_{L^2} \qquad (۱۱)$$

یعنی:

$$\int_{-\infty}^{\infty}\left|\hat{f}(u)\right|^2 d\mu(u)=\int_{-\infty}^{\infty}\left|f(u)\right|^2 dx \qquad (۱۲)$$

درنتیجه، تابع $f\mapsto\hat{f}$ پوشا و یک به یـک بـوده و بنـابراین، وارون‌پذیری تبدیل فوریه کوانتومی به دسـت مـی‌آیـد. در واقـع، تبدیل فوریه، عملگر Γ را به یک‌ضرب با u تبـدیل مـی‌کنـد، بـه صورتی که $f\in D(\Gamma)$ اگر و تنها اگر داشته باشیم:

$$u\hat{f}(u)\in L^2[\Gamma,\mu] \qquad (۱۳)$$

و در این حالت، رابطه $\Gamma f(u)=u\hat{f}(u)$ برقرار می‌باشد.

درمجموع، اندازه μ می‌توانـد دارای مؤلفـه‌هـای گسسـته یـا پیوسته باشد (مانند تبدیل هنکل[1]). چنـین توسـیع‌هـایی بسـیار شبیه به توسیع تابع ویژه پیوسته است [۲۰]. به‌بیان‌دیگر، به‌جای رابطه زیر:

$$f=\sum_{\lambda_n}(f,\phi_{\lambda_n})\phi_{\lambda_n}\mu_n \qquad (۱۴)$$

رابطه زیر را داریم:

$$f=\int_{-\infty}^{\infty}(f,\phi_{\lambda_n})\phi_u(x)d\mu(u) \qquad (۱۵)$$

که درآن خواهیم داشت:

$$(f,\phi_u)=L^2_\mu\lim_{r\to\infty}\int_0^r f(x)\phi_u(x)dx \qquad (۱۶)$$

تبدیل فوریه $\hat{f}(u)=(f,\phi_u)$ چگالی طیفی f است و انـدازه آن به‌عنوان ضریب تابع ویژه ϕ_u تفسیر می‌شود که برای بازسازی f به کار می‌رود.

برای تعریف تابع دلتای دیراک[2] در حالت پیوسته داریم:

$$\sigma(x-y)=\int_{-\infty}^{\infty}e^{i2\pi\omega x}e^{i2\pi\omega x}d\omega \qquad (۱۷)$$

در نتیجه خواهیم داشت:

$$f(x)=\int_{-\infty}^{\infty}f(y)\delta(x-y)dy=$$
$$\int_{-\infty}^{\infty}e^{i2\pi\omega x}\int_{-\infty}^{\infty}f(y)e^{i2\pi\omega x}dyd\omega= \qquad (۱۸)$$
$$\int_{-\infty}^{\infty}e^{i2\pi\omega x}\hat{f}(\omega)d\omega$$

هم‌چنین، برای مقادیر ویژه عملگر دیفرانسیلی اشتروم-لیـوول، در حالت گسسته خواهیم داشت:

$$\sigma(x-y)=\sum_{n=0}^{\infty}\Psi_n(x)\Psi^*_n(y) \qquad (۱۹)$$

که در این صورت:

$$f(x)=\sum_{n=0}^{\infty}\Psi_n(x)\int_{-\infty}^{\infty}f(y)\Psi^*_n(y)dy \qquad (۲۰)$$

در این‌جا برای مقادیر $n\geq 0$، توابـع Ψ_n تـوابعی متعامـد پایه بوده و Ψ^*_n توابع دوگان آن‌ها محسوب می‌شوند. برای مثـال، با استفاده از توابع متعامد لاگور L^α_m از مرتبه α بـه‌جـای Ψ_n در حالت پیوسته خواهیم داشت:

$$\frac{(n+\alpha)!}{n!}\sigma_{mn}=\int x^\alpha e^{-x}L^\alpha_n(x)L^\alpha_m(x)dx \qquad (۲۱)$$

نتیجه می‌دهد:

$$f(x)=\sum_{n=0}^{\infty}\frac{n!L^\alpha_n(x)}{(n+\alpha)!}\hat{f}_n \qquad (۲۲)$$

$$\hat{f}_n=\int x^\alpha e^{-x}L^\alpha_n(x)f(x)dx \qquad (۲۳)$$

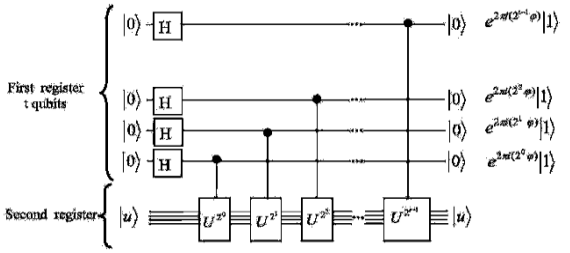
۴- تخمین فاز کوانتومی

پایه و اساس بسیاری از الگوریتم‌های کوانتومی، الگوریتم حداکثر تخمین فاز کوانتومی است [۲۱]. فرض کنید عملگر U، عملگـری یکانی می‌باشد که یک بردار ویژه $|u\rangle$ با مقدار ویژه $e^{2\pi i\phi}$ دارد. هدف الگوریتم تخمین فاز، تخمین مقدار φ است. روش تخمـین فاز کوانتومی از دو ثبات استفاده می‌کند. ثبات اول، در ابتدا t بیت کوانتومی را درحالت $|0\rangle$ دربرداردکه مقدار t وابسته به تعداد ارقام دقتی است که مـی‌خـواهیم در تخمـین داشـته باشـیم، انتخـاب می‌شود. ثبات دوم در حالت $|u\rangle$ قراردارد و تعداد بیت کوانتـومی

1- Henkel Transform

2- Dirac Delta

سه مرحله، اجرا می‌شود. ابتدا مدار نشان داده‌شده در شکل (۲) اعمال می‌شود.

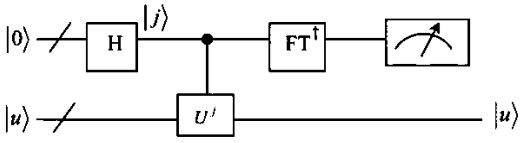


شکل (۲): مرحله اول روش تخمین فاز کوانتومی

در این مدار، ابتدا تبدیل هادامارد به اولین ثبات اعمال و سپس عملیات $Controlled-U^j$ از طریق ثبات دوم اجرا می‌گردد. بنابراین، حالت نهایی ثبات اول به‌صورت رابطه (۵) خواهد بود.

$$\frac{1}{2^{t/2}}\left(|0\rangle+e^{2\pi i 2^{t-1}\phi}|1\rangle\right)\left(|0\rangle+e^{2\pi i 2^{t-2}\phi}|1\rangle\right)\ldots\left(|0\rangle+e^{2\pi i 2^{0}\phi}|1\rangle\right)$$
$$=\frac{1}{2^{t/2}}\sum_{k=0}^{2^t-1}e^{2\pi i\phi k}|k\rangle \qquad (۲۴)$$

الگوریتم تخمین فاز کوانتومی، در شکل (۳) نشان داده شده است:



شکل (۳): مراحل الگوریتم تخمین فاز کوانتومی

الگوریتم تخمین فاز کوانتومی را در زیر مشاهده می‌کنید:

الگوریتم ۱: تخمین فاز کوانتومی	
ورودی‌ها:	
جعبه سیاه، حالت ویژه $\|u\rangle$ و t بیت کوانتومی خروجی‌ها: $\tilde{\phi}_u$ به‌عنوان تقریبی از مقدار ϕ_u	
گام‌های الگوریتم :	
حالت اولیه:	$\|0\rangle\|u\rangle$
ایجاد برهم‌نهی:	$\rightarrow \frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}\|j\rangle\|u\rangle$
اعمال جعبه سیاه :	$\rightarrow \frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}\|j\rangle U^j\|u\rangle$
خروجی جعبه سیاه:	$\rightarrow \frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}e^{2\pi i j\phi_n}\|j\rangle\|u\rangle$
اعمال تبدیل فوریه معکوس:	$\rightarrow \|\tilde{\phi}_u\rangle\|u\rangle$
اندازه‌گیری ثبات اول:	$\rightarrow \tilde{\phi}_u$

۴-۱- یافتن درجه

برای اعداد صحیح مثبت N و x که $x < N$ بوده و هیچ عامل مشترکی با هم ندارند، درجه x به پیمانه N شامل کوچک‌ترین عدد صحیح و مثبت r است که در رابطه $x^r = 1(\mathrm{mod}\, N)$ صدق می کند. مسئله یافتن درجه x عبارت از تعیین r مقدار به ازای مقادیر مشخص N است و این مسئله بر روی یک کامپیوتر کلاسیک به‌عنوان یک مسئله سخت مطرح به شمار می‌رود و این بدان معناست که حل آن بر روی یک کامپیوتر کلاسیک، از مرتبه نمایی است. در واقع، هیچ الگوریتم شناخته‌شده‌ای وجود ندارد که این مسئله را با استفاده از منابعی از مرتبه چندجمله‌ای حل نماید. به‌عبارت‌دیگر، اگر L بیت برای مشخص‌کردن N، مورد نیاز باشد هیچ الگوریتمی وجود ندارد که مسئله یافتن درجه را از مرتبه $O(L)$ حل نماید [۲۲]. در این قسمت خواهیم دید که چگونه تخمین فاز کوانتومی برای دست‌یابی به یک الگوریتم کوانتومی کارآمدیافتن درجه عدد x مورد استفاده قرار می‌گیرد.

الگوریتم کوانتومی برای یافتن درجه دقیقاً همان الگوریتم تخمین فاز است که به عملگر یکانی اعمال می‌شود. رابطه (۶) را در نظر بگیرید:

$$U|y\rangle \equiv |xy\ (\mathrm{mod}\ N)\rangle \qquad (۲۵)$$

که در آن، $y \in \{0,1\}^L$ است.

زمانی‌که $N \le y \le 2^L - 1$ باشد قرارداد می‌کنیم که $xy\ (\mathrm{mod}\ N)$ دقیقاً برابر y است.

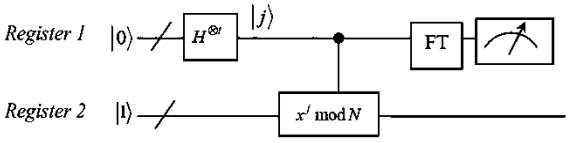
حالت‌هایی که به ازای عدد صحیح $0 \le s \le r-1$ در رابطه (۷) صدق نمایند، حالت‌های ویژه U می‌نامیم. در این رابطه، $\phi = \frac{s}{r}$ به دست می‌آید و ϕ ثابت می‌شود که رابطه (۸) برقرار است:

$$|u_s\rangle \equiv \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}\exp\left[\frac{-2\pi i s k}{r}\right]\left|x^k \bmod N\right\rangle \qquad (۲۶)$$

$$U|u_s\rangle \equiv \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}\exp\left[\frac{-2\pi i s k}{r}\right]\left|x^{k+1} \bmod N\right\rangle$$
$$= \exp\left[\frac{2\pi i s}{r}\right]|u_s\rangle \qquad (۲۷)$$

در اجرای روش تخمین فاز، اگر از t بیت کوانتومی، در ثبات اول استفاده مطابق شکل (۳) و ثبات دوم را در حالت $|1\rangle$ قرار دهیم در این صورت به ازای هر s در بازه 0 تا $r-1$، یک تخمین از فاز $\phi = \frac{s}{r}$ به دست می‌آوریم.

مدار کوانتومی الگوریتم یافتن درجه را در شکل (۴) مشاهده می نمایید:



شکل (۴): مدار کوانتومی الگوریتم یافتن درجه

۴-۱- الگوریتم کسرهای متوالی

تبدیل یافتن درجه به تخمین فاز، با توصیف چگونگی به دست آوردن پاسخ مطلوب r از نتیجه الگوریتم تخمین فاز $(\phi \approx s/r)$، کامل می‌شود. ϕ یک عدد گویا است (نسبت دو عدد صحیح معین) و اگر بتوانیم نزدیک‌ترین کسر متعارف به ϕ را محاسبه کنیم، دراین صورت قادر خواهیم بود که مقدار r را هم به دست آوریم. الگوریتم کسرهای متوالی، الگوریتم کلاسیکی است که در زمان چندجمله‌ای این کار را انجام می‌دهد.

فرض کنید $\frac{s}{r}$ عددی گویا است که در شرط $\left|\frac{s}{r}-\phi\right| \le \frac{1}{2r^2}$، صدق می‌کند. در این صورت، مقدار $\frac{s}{r}$ یکی از مقادیر حاصل از اجرای الگوریتم کسرهای متوالی برای ϕ است. به‌طور خلاصه، با فرض ϕ، الگوریتم کسرهای متوالی، اعداد s' و r' را بدون هیچ برگ خرید مشترکی تولید می‌کند. به‌طوری‌که رابطه $\frac{s'}{r'}=\frac{s}{r}$ برقرار است. حدس ما برای درجه عدد r' است. با محاسبه $x^{r'} \bmod N$ می‌توان بررسی کرد که آیا این مقدار یک درجه هست یا خیر؟ اگر حاصل عبارت برابر یک شود، r' درجه x به پیمانه N خواهد بود. در الگوریتم ۲، محاسبات کوانتومی برای یافتن درجه به طورخلاصه آورده شده است.

تعداد گیت‌های مورد نیاز برای اجرای تبدیل هادامارد از مرتبه $O(L)$ هست که در تبدیل فوریه معکوس، این تعداد از مرتبه $O(L^2)$ خواهد شد. عملگر $x^j \bmod N$ و الگوریتم کسرهای متوالی، هریک به $O(L^2)$ گیت نیاز دارند. بنابراین، بار محاسباتی در این مدار از مرتبه $O(L^3)$ است.

۵- الگوریتم شر

محاسبات کوانتومی، افزایش توان محاسباتی را نوید می‌دهند. پیتر شر[1] توانست از توازی موجود در کامپیوترهای کوانتومی به‌منظور عامل‌یابی اعداد استفاده کند [۱]. این الگوریتم، عملاً بسیار ساده بود. ابتدا یک عدد برای عامل‌یابی دریافت می‌شود (N) فرض این‌که N حاصل‌ضرب دو عدد اول است، این مقدار باید نسبت به N نیز اول باشد. به ازای مقادیر مختلف x، مقدار تابع $f(x)=(a^x \bmod N)$ محاسبه می شود که تمام این عملیات‌ها با توان محاسبات کوانتومی، می‌تواند در واحد زمان انجام گردد. در نتایج تابع، یک الگوی تکراری وجود دارد که دوره این تکرارها را باید پیدا کرد.

یافتن این دوره، معادل یافتن درجه است. در واقع، برای تجزیه اعداد به عوامل اول نیاز به استفاده از الگوریتم یافتن درجه داریم. خوشبختانه این کار را می‌توان به‌سرعت روی کامپیوترهای کوانتومی با یک تغییر شکل تبدیل فوریه کوانتومی انجام داد. این دوره را با نماد r نشان می‌دهیم. سپس مقادیر $\gcd(a^{r/2}+1, N)$ و $\gcd(a^{r/2}-1, N)$ محاسبه می‌شوند (تابع gcd بزرگ‌ترین مقسوم‌علیه مشترک می‌باشد). به دلیل برقراری تساوی $a' \bmod N$ خواهیم داشت:

$$a^r - 1 = (a^{r/2}-1).(a^{r/2}+1) = 0 \bmod N \qquad (۲۸)$$

به این صورت، $(a^{r/2}-1)(a^{r/2}+1)$ مضرب صحیحی از N است. در الگوریتم شر از خاصیت برهم‌نهی کوانتومی استفاده می‌شود که اجازه می‌دهد n کیوبیت در یک لحظه، تمام حالت ممکن را داشته باشند. پیتر شر نشان داد که کامپیوترهای کوانتومی قادر به محاسبه عوامل اول اعداد خیلی بزرگ، در یک‌زمان کوتاه هستند. این الگوریتم، وابسته به توازی کوانتومی و تبدیل فوریه کوانتومی است. مدارات کوانتومی، برای این الگوریتم با استفاده از کتابخانه Open QUACS [۱۱] در میپل طراحی‌شده‌اند. با انتخاب عدد صحیح N، مراحل پیاده‌سازی الگوریتم شر جهت پیداکردن عوامل اول آن به شرح زیر می‌باشند:

مرحله اول: پیداکردن عدد صحیح Q که توانی از ۲ بوده و $N^2 \le Q \le 2N^2$ باشد. این مرحله توسط رایانه‌های کلاسیک انجام می‌شود.

مرحله دوم: انتخاب عدد صحیح a که کوچک‌تر از N بوده و نسبت به آن اول باشد. این مرحله نیز توسط رایانه‌های کلاسیک انجام می‌شود.

مرحله سوم: ایجاد دو ثبات کوانتومی به نام ثبات ورودی و ثبات خروجی. ثبات ورودی باید دارای تعداد کافی کیوبیت، جهت نگهداری اعدادی به بزرگی Q-1 باشد و ثبات خروجی باید دارای تعداد کافی کیوبیت جهت نگهداری اعدادی به بزرگی N-1 باشد.

مرحله چهارم: بارگذاری ثبات ورودی با مقادیر صحیح 0 تا Q-1 و بارگذاری ثبات خروجی با مقدار 0.

مجموع حالت‌های اولیه ثبات‌های کوانتومی سیستم در این نقطه در رابطه (۲۹) بیان‌شده است.

1- Peter Shor

$$\frac{1}{\sqrt{Q}}\sum_{x=0}^{Q-1}|x\rangle|0\rangle \qquad (۲۹)$$

مرحله پنجم: اجرای تابع $a^x \bmod N$ برای هر عدد ذخیره‌شده در ثبات ورودی و ذخیره‌سازی نتایج آن در ثبات خروجی. به دلیل توازی کوانتومی، این مرحله در یک گام اجرا می‌شود. رایانه کوانتومی تابع $a^{|x\rangle} \bmod N$ را محاسبه می‌کند که $|x\rangle$، برهم‌نهی حالت‌های به‌دست‌آمده در مرحله چهارم است.

این مرحله، روی رایانه کوانتومی اجرا می‌شود. وضعیت ثبات‌های کوانتومی در این مرحله در رابطه (۳۰) نشان داده شده است:

$$\frac{1}{\sqrt{Q}}\sum_{x=0}^{Q-1}|x\rangle|a^x \bmod N\rangle \qquad (۳۰)$$

مرحله ششم: به دست آوردن ثبات خروجی با مقادیر K:

$$a^x \bmod N = K \qquad (۳۱)$$

این عمل به‌وسیله رایانه کوانتومی اجرا می‌شود. وضعیت ثبات‌های کوانتومی بعد از این مرحله عبارت است از:

$$\frac{1}{\sqrt{\|A\|}}\sum_{x'\in A}^{Q-1}|x'\rangle|k\rangle \qquad (۳۲)$$

که در آن، A مجموعه‌ای از x' است به‌طوری‌که خواهیم داشت:

$a^{x'} \bmod N = K$

و $\|A\|$ تعداد عناصر این مجموعه است.

مرحله هفتم: اعمال تبدیل فوریه کوانتومی روی ثبات ورودی. تبدیل فوریه کوانتومی باعث تغییر حالت $|x\rangle$ می‌شود همان‌طور که در رابطه (۳۳) نشان داده شده است:

$$|x\rangle \to \frac{1}{\sqrt{Q}}\sum_{c=0}^{Q-1}|C\rangle e^{2\pi ixc/Q} \qquad (۳۳)$$

این مرحله توسط رایانه کوانتومی، در یک گام به‌وسیله توازی کوانتومی اجرا می‌شود. بعد از تبدیل فوریه کوانتومی، وضعیت ثبات‌ها به‌صورت زیر است:

$$\frac{1}{\sqrt{\|A\|}}\sum_{x'\in A}^{Q-1}|C\rangle|k\rangle e^{2\pi ixc/Q} \qquad (۳۴)$$

مرحله هشتم: اندازه‌گیری ثبات ورودی. این مقدار m نامیده می‌شود. این مرحله توسط رایانه کوانتومی اجرا می‌شود.

مرحله نهم: با به کار بردن m روی رایانه‌های کلاسیک، مقدار دوره تکرار r توسط روش‌های مختلف به دست می‌آید.

مرحله دهم: با داشتن مقدار r ، عوامل اول عدد N توسط ب.م.م، مطابق رابطه (۳۵) به دست می‌آیند. این مرحله توسط رایانه‌های کلاسیک انجام می‌شود.

$$\left.\begin{aligned}\gcd(a^{r/2}+1, N) = p\\ \gcd(a^{r/2}-1, N) = q\end{aligned}\right\} \Rightarrow N = p.q \qquad (۳۵)$$

نتیجه جالبی که شر بدان دست یافت این بود که یک رایانه کوانتومی، در یک زمان از مرتبه چندجمله‌ای عمل تجزیه را انجام می‌دهد.

الگوریتم ۲: یافتن درجه به روش کوانتومی

ورودی‌ها:

۱- یک جعبه سیاه $U_{x,N}$

۲- t بیت کوانتومی که با $|0\rangle$ شروع می‌شود.

۳- L بیت کوانتومی که باحالت $|1\rangle$ شروع می‌شوند.

خروجی‌ها: یافتن درجه r

مراحل الگوریتم:

حالت اولیه: $|0\rangle|u\rangle$

ایجاد برهم‌نهی: $\frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}|j\rangle|u\rangle$

اعمال $U_{x,N}$ با رابطه زیر:

$$\to \frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}|j\rangle|x^j \bmod N\rangle \approx \frac{1}{\sqrt{r\,2^t}}\sum_{s=0}^{r-1}\sum_{j=0}^{2^t-1}e^{2\pi isj/r}|j\rangle|u_s\rangle$$

۴ - اعمال تبدیل فوریه معکوس به ثبات اول: $\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}\left|(\frac{\tilde{s}}{r})\right\rangle|u_s\rangle$

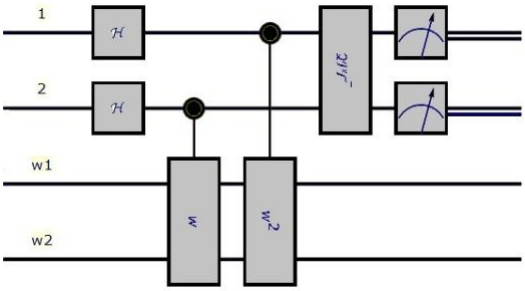
اندازه‌گیری ثبات اول: $\to (\frac{\tilde{s}}{r})$

اعمال الگوریتم کسرهای متوالی: $\to r$

۶- شبیه‌سازی در نرم‌افزار میپل

دراین بخش به عنوان مثال اول، ابتدا با درنظرگرفتن ثبات ثانویه با دو خروجی و ثبات اولیه با سه ورودی، یک مسئله ساده را در نظر گرفته‌ایم. مدار تخمین فاز برای این مثال را در شکل (۵) مشاهده می‌نمایید. در جدول (۱) نتایج مربوط به‌اندازه‌گیری با تبدیل فوریه کوانتومی و ابرحالت[1] متناظر ارائه شده است.

1- Superposition



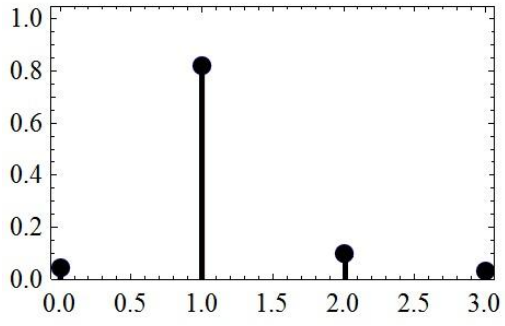
شکل (۵): مدار تخمین فاز برای مثال اول

جدول (۱): ابرحالت‌های به‌دست‌آمده در مثال اول

ابرحالت (سوپرپوزیشن)	اندازه‌گیری
$(0.0975452-0.490393i)\|0001\rangle+$ $(0.277785+0.415735i)\|0010\rangle+$ $(0.490393-0.975452i)\|0011\rangle+$ $(-0.490393+0.097545i)\|0000\rangle$	$(O_1 \quad O_2)$
$(0.415735-0.277785i)\|0101\rangle+$ $(0.0975452-0.490393i)\|0110\rangle+$ $(0.415735+0.277785i)\|0111\rangle+$ $(-0.415735-0.277785i)\|0100\rangle$	$(O_1 \quad l_2)$
$(0.0975452+0.490393i)\|1000\rangle+$ $(0.0.490393+0.0975452i)\|1001\rangle+$ $(0.415735-0.277785i)\|1010\rangle+$ $(0.0975452+0.490393i)\|1011\rangle$	$(l_1 \quad O_2)$
$-(0.277785+0.415735i)\|1101\rangle+$ $(0.490393-0.975452i)\|1110\rangle+$ $(0.277785-0.415735i)\|1111\rangle+$ $(-0.277785+0.415735i)\|1100\rangle$	$(l_1 \quad l_2)$

در شکل (۶)، احتمال متناظر با حالت‌های اندازه‌گیری‌شده در جدول (۱) نشان داده شده‌اند. حالت‌ها از بالا به پایین به ترتیب از چپ به راست با میله‌های نمودار متناظر شده‌اند.

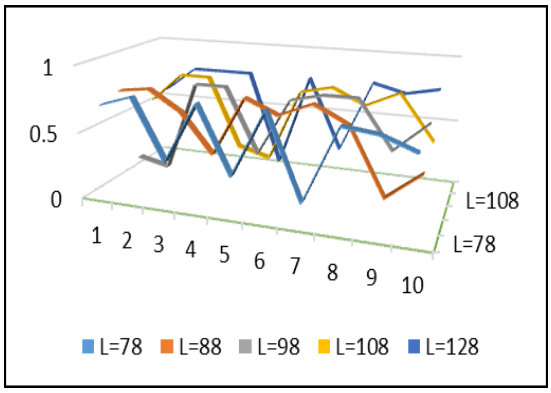
در مثال دوم، الگوریتم شر با استفاده از نرم‌افزار میپل پیاده‌سازی شده است. نتایج عددی ارائه‌شده در جدول (۲) تجزیه عدد مرکب ده رقمی N=2596466813=27751*93563 برای تعداد کیوبیت‌های درنظر گرفته‌شده در ثبات، جهت ۲ بار اجرای برنامه را نشان می‌دهد. هم‌چنین در این جدول تعداد تکرارها برای انتخاب عدد تصادفی اولیه و مرتبه به‌دست‌آمده نیز ارائه شده‌اند. نتایج تصادفی‌بودن زمان به‌دست‌آمده و هم‌چنین تعداد تکرارهای لازم برای انتخاب عدد تصادفی را که در جدول با * نشان داده شده، به‌خوبی نشان می‌دهد. الگوریتم تبدیل فوریه تعمیم‌یافته (با استفاده از چندجمله‌ای‌های متعامد) به‌خوبی الگوریتم تبدیل فوریه کوانتومی معمولی عمل می‌کند. درعین‌حال از لحاظ نظری اهمیت بیش‌تری برای تعمیم استفاده از تبدیل فوق خواهد داشت.



شکل (۶): احتمال متناظر با حالت‌های اندازه‌گیری‌شده جدول (۱)

جدول (۲): نتایج به‌دست‌آمده از اجرای الگوریتم

تکرار	۱		۲	
	زمان (*)	مرتبه	زمان (*)	مرتبه
L=78	42.510(2)	27750	25.459(3)	38850
L=88	11.560(3)	40098	79.077(8)	12950
L=98	119.075(12)	30750	203.113(19)	12062
L=108	36.692(7)	40750	70.856(6)	40750
L=128	29.859(8)	30750	52.291(3)	12062



شکل (۷): احتمال متناظر با فازهای تخمین زده‌شده

در شکل (۷)، احتمال متناظر با فازهای تخمین زده‌شده برای همه اجراها نشان داده شده‌اند. به این صورت که برای هر پنج شبیه‌سازی، بردار و مقدار ویژه حالت ظاهرشده به‌دست‌آمده و درنتیجه مقدار فاز تخمین زده‌شده برای فاز متناظر و اندازه حالتی که احتمال رخداد آن را نشان می‌دهد در جدول (۲) آورده شده است. با توجه به شکل می‌توان دید که با کاهش تعداد کیوبیت‌های درنظر گرفته‌شده در ثبات (L)، احتمال رخداد حالت در اجراها تغییر زیادی پیدا می‌کند. با افزایش L، احتمال رخداد

فاز بیش‌تر می‌شود و در اجراهای مختلف تفاوت کم‌تری نشان داده می‌دهد و این در واقع همان چیزی است که انتظار داریم، گرچه این موضوع را نمی‌توان در پنج اجرای متفاوت به‌خوبی و به‌طور کامل نشان داد.

باید توجه داشت با تغییر L نمی‌توان درباره سرعت انجام شبیه‌سازی اظهارنظر کرد. ولی به‌طورکلی با افزایش تعداد کیوبیت‌ها (مقدار L) زمان اجرای شبیه‌سازی افزایش می‌یابد.

۷- نتیجه‌گیری

در مقاله حاضر مسئله تجزیه اعداد مرکب صحیح و مثبت با استفاده از رایانه کوانتومی مورد مطالعه قرار گرفت. الگوریتم تجزیه که توسط پیتر شر برای رایانه‌های کوانتومی معرفی شد، از دو بخش کوانتومی و کلاسیک تشکیل می‌شود. بخش کوانتومی الگوریتم شر که شامل تخمین فاز کوانتومی و تبدیل فوریه کوانتومی و عملگرهای یکانی کوانتومی است برای پیاده‌سازی نیاز به رایانه کوانتومی دارد. تبدیل فوریه کوانتومی و تعمیم آن مورد مطالعه و بررسی قرار گرفت. در ادامه عملگرهای یکانی، به‌ویژه تبدیل فوریه کوانتومی را با کمک نرم‌افزار میپل و با استفاده از کتابخانه Open QUACS شبیه‌سازی کردیم. توازی و درهم تنیدگی دو ویژگی اساسی رایانه‌های کوانتومی است که در رایانه کلاسیک قابل پیاده‌سازی نیستند ولی با استفاده از کت‌هایی، نتیجه این دو پدیده را می‌توان شبیه‌سازی کرد. برای اندازه‌گیری نیز از توابع کتابخانه معرفی‌شده به‌کارگیری گردید. برخی نتایج شبیه‌سازی تخمین فاز و اندازه‌گیری‌های صورت گرفته‌شده در شکل‌ها و جدول‌ها ارائه شده‌اند. برای پژوهش‌های آینده می‌توان کتابخانه را با استفاده از تبدیل فوریه سریع نیز مجهز کرد و یا برنامه را برای تعداد کیوبیت‌های بیش‌تر توسعه بخشید.

۸- مراجع

[1] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," SIAM J. Comput., vol. 26, no. 5, pp. 1484-1509, 1997.

[2] R. Cleve, "The query complexity of order-finding," In Computational Complexity," 2000 Proceedings, 15th Annual IEEE Conference on IEEE, pp. 54-59, 2000.

[3] A. Y. Kitaev, A. Shen, and M. N. Vyalyi, "Classical and quantum computation," Providence: American Mathematical Society, 2002.

[4] A. Ekert and R. Jozsa, "Quantum computattion and Shor's factoring algorithm," Rev. Mod. Phys., vol. 68, pp. 733-53, 1996.

[5] M. L. Nielsen and I. L. Chuang, "Quantum Computation and Quantum Information," Cambridge University Press, New York, 2000.

[6] S. A. teane, "Quantum Computing," Rept. Prog. Phys., vol. 61, pp. 117-173, 1998.

[7] A. J. Menezes. P. C. Van Oorschot, and S. A. Vanstone, "Handbook of applied cryptography," CRC press, 1996.

[8] R. P. Feynman, "Simulating physics with computers," Int. J. Theor. Phys. 21, pp. 467-88, 1982.

[9] J. F. Schneiderman, M. E. Stanley, and P. K. Aravind, "A pseudo-simulation of Shor's quantum factoring algorithm," arXiv preprint quant-ph/0206101, 2002.

[10] T. Raditik, "Simulation of n-qubit quantum systems, I. Quantum registers and quantum gates," http://cpc.cs.qub.ac.uk/summaries/ADWE

[11] "List of QC simulators," http://web.archive.org

[12] Quantum information, "Controlled Quantum Dynamics," http://www3.imperial.ac.uk/ /research/downloads

[13] C. B. McCubbin, "Openquacs, an open-source quantum computation simulator in maple," Ph.D. dissertation, University of Maryland, Baltimore County, 2000.

[14] Y. S. Weinstein, M. A. Pravia, E. M. Fortunato, E. M. Lloyd, and D. G. Cory, "Implementation of the quantum Fourier transform," Phys. Rev. Letter., vol. 86, no. 9, pp. 18-89, 2001.

[15] L. Hales and S. Hallgren, "An improved quantum Fourier transform algorithm and applications," In Foundations of Computer Science, 2000.

[16] H. M. Ozaktas, Z. Zalevsky, and M. A. Kutay, "The fractional Fourier transform," Wiley, Chichester, 2001.

[17] J. S. Walker, "Fast fourier transforms," CRC press, 1996.

[18] S. Mallat, "A wavelet tour of signal processing," Academic press, 1999.

[19] A. Zettl, "Sturm-liouville theory," American Mathematical Society, 2010.

[20] M. A. Al-Gwaiz, "Sturm-Liouville theory and its applications," Springer, 2008.

[21] G. M. D'Ariano, C. Macchiavello, and M. F. Sacchi, "On the general problem of quantum phase estimation," Phys. Letter A, vol. 248, no. 2, pp. 103-108, 1998.

[22] S. Aaronson and A. Arkhipov, "The computational complexity of linear optics," In Proceedings of the forty-third annual ACM symposium on Theory of computing, ACM, pp. 333-342, 2011.

مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"
ویژه‌نامه کنفرانس بین‌المللی ترکیبیات، رمزنگاری و محاسبات، ص ۸۴ -۷۹

چندجمله‌ای غالب تام گراف‌ها

سعید علیخانی[1*]، نسرین جعفری[2]

۱- دانشیار، ۲- دانشجوی دکتری، دانشگاه یزد

(دریافت: ۹۵/۰۷/۰۵، پذیرش: ۹۶/۰۳/۰۶)

چکیده

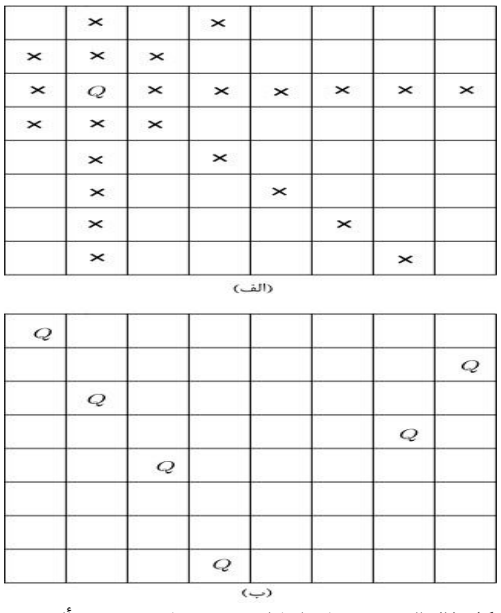
نظریه غالب، یکی از مهم‌ترین موضوعات موجود در علم گراف است که در بسیاری از زمینه‌ها هم‌چون شبکه‌های ارتباطی، نقشه‌برداری زمینی و مسیریابی کاربرد دارد. فرض کنید G=(V,E) گراف ساده با مرتبه n است. یک زیرمجموعه S از مجموعه V را مجموعه غالب تام گوییم، هرگاه هر راس u در V همسایه یک راس در S باشد. کوچک‌ترین اندازه مجموعه‌های غالب تام گراف G را عدد غالب تام می‌گوییم و آن را با $\gamma_t(G)$ نشان می‌دهیم. تعداد مجموعه‌های غالب و مجموعه‌های غالب تام با هر اندازه دلخواهی در گراف دلخواه G اخیراً مورد توجه قرار گرفته است. تابع مولد تعداد مجموعه‌های غالب تام گراف G با نماد $D_t(G,x)$، نشان داده شده و برابر با $D_t(G,x)=\sum_{i=\gamma_t(G)}^{n} d_t(G,i)x^i$ بوده که چندجمله‌ای غالب تام نامیده می‌شود که در آن $d_t(G,i)$، تعداد مجموعه‌های غالب تام با اندازه i از گراف G است. در این مقاله به مطالعه این چندجمله‌ای پرداخته و هم‌چنین ریشه این چندجمله‌ای را مورد بررسی قرار خواهیم داد.

واژه‌های کلیدی: عدد غالب، عدد غالب تام، چندجمله‌ای غالب تام

۱- مقدمه

نخستین دلیل تعریف و مطالعه مجموعه‌های غالب، یافتن راه‌حل برای مسأله n وزیر در یک صفحه شطرنج است. علاقه‌مندان شطرنج در اروپا در دهه 50 قرن نوزدهم، برای اولین بار این مسأله را مطرح کردند که چه تعداد وزیر در یک صفحه شطرنج می‌توان قرار داد به طوری که همه مربع‌های صفحه شطرنج یا با یک وزیر اشغال شوند یا حداقل با یک وزیر احاطه شوند و در عین حال وزیرها یک‌دیگر را نیز مغلوب نکنند. صفحه شطرنج در شکل (۱- الف)، یک صفحه شطرنج 8×8 استاندارد را نشان می‌دهد که در آن همه مربع‌های احاطه‌شده توسط وزیر داده‌شده با × علامت‌گذاری شده‌اند. مطابق قوانین بازی شطرنج، یک وزیر به هر تعداد مربع دلخواه در صفحه به صورت افقی، عمودی و قطری احاطه دارد. در شکل (۱- ب) صفحه شطرنج یک مجموعه از 6 وزیر را نشان می‌دهد که وزیرها به همه مربع‌های صفحه شطرنج احاطه دارند و هیچ‌کدام با دیگری مغلوب نمی‌شود.

به بیان دیگر مسأله مربع‌های غالب در صفحه شطرنج، معادل با مسأله رئوس غالب در یک گراف است. در گراف ساده G، به بیان دیگر مسأله مربع‌های غالب در صفحه شطرنج، معادل با مسأله رئوس غالب در یک گراف است. در گراف ساده G، $S\subseteq V(G)$ یک مجموعه غالب گراف G است، هرگاه هر رأس $v\in V(G)$ یا خودش متعلق به S باشد و یا همسایه حداقل یک رأس S باشد. کوچک‌ترین اندازه مجموعه‌های غالب گراف G را عدد غالب G می‌گوییم و آن را با نماد $\gamma(G)$ نشان می‌دهیم.



شکل (۱): الف) مربع‌های احاطه‌شده ب) پاسخی به مسأله ۸ وزیر

*رایانامه نویسنده مسئول: : alikhani@yazd.ac.ir

خانواده همه γ مجموعه‌های G را با $\Gamma(G)$ نشان می‌دهیم. هم‌چنین خانواده مجموعه‌های غالب گراف G با اندازه i را با $D(G,i)$ نشان می‌دهیم و $d(G,i)$ را $|D(G,i)|$ تعریف می‌کنیم. برای کسب اطلاعات بیش‌تر در مورد مجموعه‌های غالب و عدد غالب، مرجع [۱] پیشنهاد می‌شود. مفهوم مجموعه‌های غالب در بسیاری از زمینه‌های پژوهشی کاربرد دارد. یکی از این زمینه‌ها مسأله شبکه ارتباطی است. شبکه ارتباطی مجموعه‌ای از گره‌هاست که در آن یک گره با گره دیگر می‌تواند ارتباط برقرار کند، هرگاه این دو گره به طور مستقیم به هم متصل باشند. برای فرستادن یک پیام مستقیم از یک مجموعه گره به گره‌های دیگر، لازم است که این مجموعه به گونه‌ای انتخاب شود که گره‌های دیگر حداقل به یک گره از آن مجموعه متصل باشند. چنین مجموعه‌ای در گراف متناظر با شبکه، مجموعه غالب است. از کاربردهای دیگر مجموعه‌های غالب می‌توان به نقشه‌برداری زمینی، مسیریابی و... اشاره نمود [۲، ۳، ۴، ۵، ۶]. از دیگر انواع اعداد غالب که کاربرد نظامی هم دارد، عدد غالب رومی گراف است. تاریخچه عدد غالب رومی به قرن چهارم میلاد، زمان فرمانروایی کنستانتین، امپراتور روم باستان باز می‌گردد. در آن زمان، کنستانتین برای دفاع از شهرهای قلمرو خود دستوور داد تا هر شهر که فاقد ارتش است، در همسایگی آن شهری با دو ارتش وجود داشته باشد که اگر شهر اول مورد هجوم قرار گرفت، شهر دوم بتواند ارتشی برای دفاع از آن شهر گسیل دارد بدون آن که شهر خود آسیبی ببیند. حال موضوع کمینه کردن تعداد کل ارتش‌ها بود و این چنین عدد غالب رومی گراف‌ها مطرح شد [۱].

پیچیدگی طراحی الگوریتم برای پیداکردن کوچک‌ترین مجموعه‌های غالب در یک گراف منجر به بحث در مورد پیچیدگی محاسباتی و NP- کامل‌بودن این مسأله می‌شود. جانسون(Johnson) اولین کسی بود که نشان داد پیداکردن مجموعه غالب NP- کامل است [۱،۷].

مساله تعداد مجموعه‌های غالب یک گراف برای اولین بار توسط سعید علیخانی در پایان نامه دکتری ایشان مورد توجه قرار گرفت [۸]. وی چندجمله‌ای را معرفی کرد که ضرایبش تعداد مجموعه‌های غالب گراف است و آن‌را چندجمله‌ای غالب نامید. چندجمله‌ای غالب گراف G، $D(G,x)$، به صورت زیر تعریف می‌شود:

$$D(G,x)=\sum_{i=\gamma(G)}^{|V(G)|} d(G,i)x^i \qquad (۱)$$

که در آن، منظور از $d(G,i)$ تعداد مجموعه‌های غالب گراف با اندازه i است [۸-۱۱]. چندجمله‌ای غالب گراف G، $D(G,x)$، تابع مولد تعداد مجموعه‌های غالب آن گراف است. این چندجمله‌ای مشابه چندجمله‌ای‌های دیگر وابسته به گراف مورد توجه پژوهشگران قرار گرفته است. به طور کلی، محاسبه چندجمله‌ای غالب یک گراف G به دلیل NP- کامل‌بودن $\gamma(G)$ دشوار است. اما برای خانواده‌های خاص از گراف‌ها می‌توان فرمول صریحی برای چندجمله‌ای غالب به دست آورد. در گراف G ریشه‌های $D(G,x)$ را ریشه‌های غالب G می‌نامند [۹]. مجموعه ریشه‌های مجازی $D(G,x)$ را با $Z(D(G,x))$ نشان می‌دهیم. از آن‌جا که انواع مختلفی از اعداد غالب معرفی شده است، مشابه مساله تعداد مجموعه‌های غالب معمولی، می‌توان مساله تعداد مجموعه‌های غالب از انواع دیگر را مطرح نمود. در این مقاله تعداد مجموعه‌های غالب تام گراف را در نظر می گیریم و تابع مولد این اعداد که چندجمله‌ای غالب تام گراف نامیده شده و به صورت $D_t(G,x)=\sum_{i=\gamma_t(G)}^{n} d_t(G,i)x^i$ تعریف می‌شود را مورد مطالعه قرار خواهیم داد. هم‌چنین نتایجی در مورد ریشه‌های این چندجمله‌ای بیان خواهد شد.

۲- چندجمله‌ای غالب تام برخی گراف‌ها

در این بخش به مطالعه برخی از ویژگی‌های چندجمله‌ای غالب تام برخی از گراف‌ها خواهیم پرداخت. برای مطالعه بیش‌تر در ادامه مقاله از عمل‌های رأسی و یالی زیر برای گراف $G=(V,E)$ استفاده می‌کنیم که به طور مشترک در متن‌های مربوط به نظریه گراف یافت می‌شوند [۱۰، ۱۲ و ۱۳]. فرض کنید $v\in V$ یک رأس و $e=uv$ یک یال گراف G است.

حذف رأس $G-v$**:** نشان‌دهنده گراف به دست آمده از G با حذف رأس v و همه یال‌های واقع بر v است.

انقباض رأس G/v**:** نشان‌دهنده گراف به دست آمده از G با حذف رأس v و افزودن یال بین هر جفت از همسایه‌های غیرمجاور v است. به عبارت دیگر، گراف به دست آمده از G که همه رئوس در $N(v)$ به یک‌دیگر وصل شده‌اند و سپس رأس v حذف شده است.

برداشتن همسایگی بسته رأس $G-N[v]$**:** نشان‌دهنده گراف به دست آمده از G با حذف همه رئوس در همسایگی بسته v و همه یال‌های واقع بر آن‌هاست.

حذف یال $G-e$**:** نشان‌دهنده گراف به دست آمده از G با حذف یال e است.

انقباض یال G/e**:** نشان‌دهنده گراف به دست آمده از G با حذف یال e و یکی‌کردن پایانه‌های e برهم است.

تعریف: فرض کنید $G=(V,E)$ یک گراف ساده است. در این صورت زیرمجموعه S از مجموعه v را غالب تام گوییم، هرگاه هر راس u در v همسایه یک راس در S باشد.

کوچک‌ترین اندازه مجموعه‌های غالب تام گراف G را عدد غالب تام می‌گوییم و با $\gamma_t(G)$ نشان می‌دهیم.

تعریف: تعداد مجموعه‌های غالب تام با اندازه i از گراف G را با نماد $d_t(G,i)$، نشان داده و تابع مولد تعداد مجموعه‌های غالب تام گراف G، به صورت زیر تعریف می‌شود:

$$D_t(G,x)=\sum_{i=\gamma_t(G)}^{n} d_t(G,i)x^i \qquad (۲)$$

که آن‌را چندجمله‌ای غالب تام گراف G می‌نامیم.

قضیه ۱، اساسی‌ترین رابطه‌ای است که برای محاسبه چندجمله‌ای غالب تام گراف بیان شده است.

قضیه ۱: [۱۴]، فرض کنید $G=(V,E)$ یک گراف و $u\in V$ راسی از این گراف است. در این صورت خواهیم داشت:

$$D_t(G,x)=D_t(G-u,x)+xD_t(G/u,x)$$
$$+x^2\sum_{v\in N(u)} D_t(G-N[\{u,v\}],x)-(1+x)p_u(G,x)$$

که در آن، $p_u(G,x)$ یک چندجمله‌ای است که تعداد مجموعه‌های غالب تام گراف G-u که شامل هیچ همسایه‌ای از u نیستند را می‌شمارد.

قضیه ۲: [۱۴]، الف) فرض کنید $G=(V,E)$ یک گراف و $u,v\in V$ رئوسی از گراف G هستند به طوری که $N[v]\subseteq N[u]$ در این صورت رابطه بازگشتی زیر برای چندجمله‌ای غالب تام گراف برقرار است:

$$D_t(G,x)=D_t(G-u,x)+xD_t(G/u,x)$$
$$+x^2\sum_{w\in N(u)} D_t(G-N[\{u,w\}],x). \qquad (۳)$$

ب) اگر $u,v\in V$ دو رأس نامجاور با شرط $N(v)\subseteq N(u)$ از گراف G باشند. آن‌گاه داریم:

$$D_t(G,x)=D_t(G-u,x)+xD_t(G/u,x)$$
$$+x^2\sum_{w\in N(u)\cap N(v)} D_t(G-N[\{u,w\}],x). \qquad (۴)$$

با استفاده از روابط بازگشتی موجود در قضیه ۲، می‌توان چندجمله‌ای غالب تام گراف مسیر n رأسی P_n را محاسبه کرد.

قضیه ۳: برای گراف‌های مسیر از مرتبه $n\geq 5$ داریم:

$$D_t(P_n,x)=D_t(P_{n-1},x)+x^2D_t(P_{n-3},x)$$
$$+x^2D_t(P_{n-4},x). \qquad (۵)$$

اثبات: فرض کنید v برگی از گراف مسیر P_n و u همسایه v است. در این صورت بنابه قضیه ۲ داریم:

$$D_t(P_n,x)=D_t(P_n\cup K_1,x)+xD_t(P_{n-1},x)$$
$$+x^2\sum_{w\in N(u)} D_t(G-N[\{u,w\}],x). \qquad (۶)$$

بنابراین:

$$D_t(P_n,x)=D_t(P_{n-1},x)+x^2D_t(P_{n-3},x)$$
$$+x^2D_t(P_{n-4},x). \qquad (۷)$$

قضیه ۴: فرض کنید $G=(V,E)$ یک گراف از مرتبه n است. در این صورت خواهیم داشت:

$$D_t(G,x)=\sum_{S\subseteq V}(-1)^{|S|}(x+1)^{n-|N(S)|}. \qquad (۸)$$

اثبات: می‌دانیم که $(x+1)^n$ تابع مولد تعداد زیرمجموعه‌های رئوس G است. از طرف دیگر، برای هر زیرمجموعه $S\subseteq V$، $(x+1)^{n-|N(S)|}$ تابع مولد تعداد زیرمجموعه‌هایی از رئوس G است که هیچ همسایه‌ای در s ندارند. حال با استفاده از اصل شمول- طرد، اثبات کامل می‌شود.

قضیه ۵ رابطه بین چندجمله‌ای غالب تام یک گراف را با چندجمله‌ای غالب تام مکمل آن گراف، نشان می‌دهد.

قضیه ۵: برای هر گراف G از مرتبه n داریم:

$$D_t(G,x)+x^{n+1}D_t(\overline{G},\frac{1}{x})\geq x(x+1)^{n-1}. \qquad (۹)$$

که در آن، $\overline{G}$ نشان‌دهنده مکمل گراف G است.

اثبات: برای این منظور ضرایب x^k را در دو طرف نامساوی در نظر می‌گیریم. کافی است نشان دهیم:

$$d_t(G,k)+d_t(\overline{G},n-k+1)\geq\binom{n-1}{k-1}. \qquad (۱۰)$$

به ازای انتخاب هر $k-1$ رأس از $n-1$ رأس گراف G سه حالت ممکن است رخ دهد:

۱) این $k-1$ رأس با رأس دیگر گراف یک مجموعه غالب تام از گراف G است، در حقیقت در این حالت به یک مجموعه غالب تام k عضوی رسیده‌ایم که تعداد آن‌ها $d_t(G,k)$ خواهد بود.

۲) $n-k+1$ رأس دیگر، یک مجموعه غالب تام از گراف $\overline{G}$ است که در این صورت تعداد این‌گونه مجموعه‌ها، $d_t(\overline{G},n-k+1)$ خواهد بود.

۳) هر دو حالت رخ دهد.

بنابر اصل جمع حکم برقرار است.

هم‌چنین نتیجه مشابه‌ای را می‌توان برای چندجمله‌ای غالب گراف‌ها بیان نمود.

قضیه ۶: برای هر گراف G از مرتبه n داریم:

$$D(G,x)+x^{n}D(\overline{G},\frac{1}{x})\geq(x+1)^{n}. \qquad (۱۱)$$

که در آن، $\overline{G}$ مکمل گراف G است.

اثبات: مشابه با اثبات قضیه ۵ نشان می‌دهیم:

$$d(G,k)+d(\overline{G},n-k)\geq\binom{n}{k}.$$

برای این منظور به این نکته توجه کنید که به ازای انتخاب هر k رأس از گراف G سه حالت ممکن وجود دارد:

۱) این k رأس یک مجموعه غالب از گراف G است.

۲) $n-k$ رأس دیگر یک مجموعه غالب از گراف $\overline{G}$ است.

۳) حالت ۱ و ۲ با هم رخ دهند.

در نتیجه، حکم حاصل می‌شود.

توجه کنید که نامساوی قضیه ۶ دقیق است. به عنوان مثال، تساوی برای گراف‌های کامل رخ می‌دهد.

اگر در چندجمله‌ای غالب و یا غالب تام گراف به جای x مقدار ۱ را قرار دهیم تعداد کل مجموعه‌های غالب و یا غالب تام گراف به دست می‌آیند. از قضیه ۵ و ۶ نیز با قراردادن x=1 نتیجه زیر به دست می آید:

نتیجه ۷: الف) برای هر گراف G از مرتبه n داریم:

$$D_t(G,1)+D_t(\overline{G},1)\geq 2^{n-1}. \qquad (۱۲)$$

ب) برای هر گراف G از مرتبه n داریم:

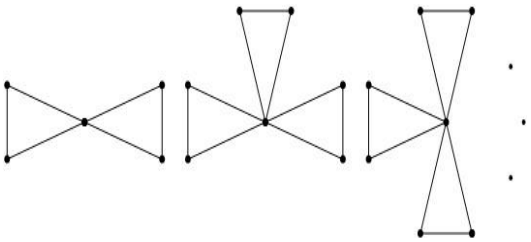
$$D(G,1)+D(\overline{G},1)\geq 2^{n}. \qquad (۱۳)$$

۲-۱- ریشه‌های چندجمله‌ای غالب تام برخی از گراف‌ها

ریشه‌های چندجمله‌ای‌های یک گراف منعکس‌کننده برخی اطلاعات مهم در مورد گراف هستند. در این بخش، ابتدا به محاسبه چندجمله‌ای غالب تام برخی از گراف‌ها و سپس به بررسی ریشه‌های آن‌ها می‌پردازیم. برای این منظور به تعاریف و قضایای زیر توجه کنید:

تعریف: در گراف G ریشه‌های چندجمله‌ای غالب تام گراف G، $D_t(G,x)$ را ریشه‌های غالب تام G می‌نامیم و مجموعه ریشه‌های مجزای $D_t(G,x)$ را با $Z(D_t(G,x))$ نشان می‌دهیم.

گرافی که از به هم پیوستن n نسخه از گراف دور C_3 با یک رأس مشترک ساخته می‌شود را گراف دوستانه (friendship) یا آسیاب بادی هلندی نامیده و آن را با نماد F_n نشان می دهیم. در شکل (۲) گراف‌های دوستانه F_2، F_3، F_4 و F_n را مشاهده می‌کنید.

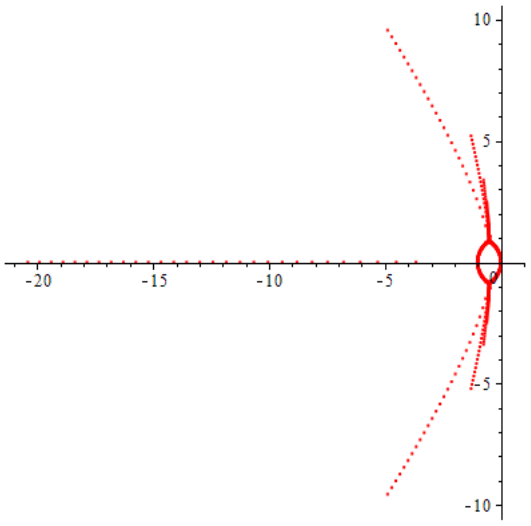


شکل (۲): گراف‌های دوستانه از چپ F_2، F_3 و F_n.

قضیه ۸: [۱۵] برای هر عدد طبیعی n، داریم:

$$D_t(F_n,x)=x(x+1)^{2n}+x^{2n}-x. \qquad (۱۴)$$

قضیه ۹: [۱۵] برای اعداد طبیعی به قدر کافی بزرگ n، گراف دوستانه F_n یک ریشه غالب تام حقیقی در بازه $(-n,-\ln(n))$ دارد.



شکل (۳): ریشه های غالب تام گراف دوستانه F_n برای $2\leq n\leq 30$

قضیه ۹ نشان می‌دهد که از لحاظ قدرمطلقی ریشه‌های غالب تام به اندازه کافی می‌تواند بزرگ شود. برای مطالعه بیش‌تر چندجمله‌ای‌های غالب تام و ریشه‌های آن مطالعه برخی از یال‌ها مفید خواهند بود. در این‌جا برخی از این گونه یال‌ها را مطالعه خواهیم کرد.

تعریف: یال $e\in E$ از گراف $G=(V,E)$ را یک یال بی‌اثر یا بی‌ربط برای چندجمله‌ای غالب تام می‌نامیم، هرگاه:

$D_t(G,x) = D_t(G-e,x)$.

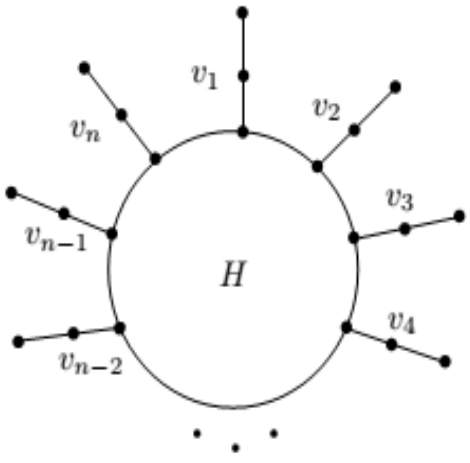
یال‌های بی اثر کار ما را در به دست آوردن چندجمله‌ای غالب تام برخی گراف‌ها ساده می‌کنند. قضیه ۱۰ شرطی کافی برای بی‌اثربودن یک یال از گراف G در چندجمله‌ای‌های غالب تام گراف است.

قضیه ۱۰: فرض کنید $G=(V,E)$ یک گراف و $e=\{u,v\}\in E$ یالی از گراف G است. در این صورت اگر u و v با رئوس تکیه‌گاهی مجاور باشند، آن‌گاه یال e یک یال بی‌اثر از گراف G است. (هر راس مجاور با رئوس درجه یک را رأس تکیه‌گاه می‌نامیم).

اثبات: فرض کنید $e=\{u,v\}\in E$ یالی از گراف G، u و v به ترتیب با رئوس تکیه‌گاه w_1 و w_2 مجاورند. در این صورت هر زیرمجموعه غالب تام از گراف G شامل رئوس w_1و w_2 است و در نتیجه رئوس واقع بر یال e، تحت هر مجموعه غالب دلخواه توسط رئوس w_1و w_2 پوشش داده می‌شوند و در نتیجه مجاورت بین u و v بی‌اثر است. بنابراین $D_t(G,x)=D_t(G-e,x)$ و یال e یالی بی‌اثر است.

در این قسمت، با استفاده از قضیه ۱۰، چندجمله‌ای غالب تام برخی از خانواده‌های گراف‌ها را محاسبه می‌کنیم.

تعریف: برای هر گراف دلخواه H از مرتبه n، گراف $H(3)$، گراف حاصل از چسباندن راس پایانی یک گراف مسیر P_3 به هر رأس گراف H است.



شکل (۴): گراف $H(3)$

قضیه ۱۱: برای هر گراف دلخواه H از مرتبه n، داریم:

$$D_t(H(3),x) = x^{2n}(x+2)^n. \qquad (۱۵)$$

اثبات: با توجه به قضیه ۱۰ و ساختار گراف $H(3)$، هر یال گراف H یک یال بی‌اثر است، زیرا رئوس گراف H با رئوس تکیه‌گاه v_i مجاورند (شکل ۴)، بنابراین داریم:

$$D_t(H(3),x) = (D_t(P_3,x))^n. \qquad (۱۶)$$

با توجه به این‌که $D_t(P_3,x) = x^3+2x^2$ حکم برقرار است حال به معرفی خانواده دیگری از گراف‌ها و محاسبه چندجمله‌ای غالب تام آن‌ها می‌پردازیم.

تعریف: یک (n,k)- ترقه، $f(n,k)$، گراف حاصل از لینک یک برگ از n عدد ستاره S_k با هم است (شکل ۵).

قضیه ۱۲: برای اعداد طبیعی n و $k\geq 3$ داریم:

$$D_t(f(n,k),x) = (x(x+1)^{k-1}-x)^n. \qquad (۱۷)$$

اثبات: تمام رئوس گراف $f(n,k)$، $(k\geq 3)$ که با هم لینک شده‌اند با رأس مرکزی گراف‌های ستاره مجاورند که رئوس تکیه‌گاه هستند و در نتیجه بنابه قضیه ۱۰ یال‌های بین آن‌ها بی‌اثر است و داریم:

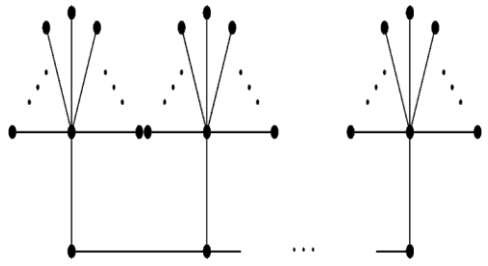
$$D_t(f(n,k),x) = (D_t(S_k,x))^n. \qquad (۱۸)$$

از طرفی داریم:

$$D_t(S_k,x) = x(x+1)^{k-1}-x$$

و لذا نتیجه حاصل می‌شود.

نتیجه: ریشه‌های غالب تام این خانواده از گراف‌ها ($f(n,k)$ ها برای $k\geq 3$) بر دایره‌ای به شعاع 1 و مرکز $(-1,0)$ واقع شده است.



شکل (۵): گراف (n,k)- ترقه، $f(n,k)$

۵- مراجع

[1] T. W. Haynes, S. T. Hedetniemi, and P. J. Slater, "Fundamentals of domination in graphs," Marcel Dekker, Inc., NewYork, 1998.

[2] S. Parsa, H. Saifi, M. H. Alaeian, "Providing a New Approach to Discovering Malware Behavioral Patterns Based on the Dependency Graph Between System Calls," J. Elect. & Cyber Defence, vol. 4, no. 3, pp. 47-60, 2016.

[3] J. N. Hooker, R. S. Garfinkel, and C. K. Chen, "Finite dominating sets for network location problems," Oper. Res., vol. 39, no. 1, pp. 100–118, 1991.

[4] L. L. Kelleher, "Domination in graphs and its application," to Social Network Theory, Ph.D. thesis, Northeastern University, 1985.

[5] L. L. Kelleher and M. B. Cozzens, "Dominating sets in social network graphs," Math. Social Sci., vol. 16, no. 3, pp. 267–279, 1988.

[6] P. J. Slater, "Maximin facility location," J. Res. Nat. Bur., Standards B 79, pp. 107–115, 1975.

[7] M. R. Garey and D. S. Johnson, "Computers and intractability: A guide to the theory of NP-completeness," Bull. Amer. Math. Soc. (N.S.) 3, vol. 2, pp. 898–904, 1980.

[8] S. Alikhani, "Dominating sets and domination polynomials of graphs," Ph.D. Thesis, University Putra Malaysia, March 2009.

[9] S. Akbari, S. Alikhani, and Y. H. Peng, "Characterization of graphs using domination polynomial," European J. Combin., vol. 31, no. 7, pp. 1714–1724, 2010.

[10] S. Alikhani, "Dominating sets and domination polynomials of graphs: Domination polynomial: A new graph polynomial," LAP LAMBERT Academic Publishing, 2012.

[11] S. Alikhani, and Y. H. Peng, "Introduction to domination polynomial of a graph", Ars Comb., vol. 114, pp. 257-266, 2014.

[12] T. Kotek, J. Preen, F. Simon, P. Tittmann, and M. Trinks, "Recurrence relations and splitting formulas for the domination polynomial," Electronic J. Combin., vol. 19, no. 3, p. 27, 2012.

[13] M. Walsh, "The hub number of a graph," Int. J. Math. Comput. Sci., vol. 1, no. 1, pp. 117–124, 2006.

[14] M. Dod, "The total domination polynomial and its generalization," Congr. Numer. 219, pp. 207-226, 2014.

[15] S. Alikhani and N. Jafari, "On the roots of total domination polynomial of graphs," submitted, Available at http://arxiv.org/abs/1605.02222.

[16] S. Alikhani and N. Jafari, "Total domination polynomial of graphs from primary subgraphs," submitted, Available at https://arxiv.org/abs/1609.07789.

مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"
ویژه‌نامه کنفرانس بین‌المللی ترکیبیات، رمزنگاری و محاسبات، ص ۸۹ -۸۵

رابطه امکان کنترل یک اختلال در سامانه و جواب ویسکوزیته یک معادله دیفرانسیل با مشتقات جزئی

سمیه سعیدی نژاد *

۱- استادیار، دانشگاه علم و صنعت ایران

(دریافت: ۹۵/۰۷/۰۵، پذیرش: ۹۶/۰۳/۰۶)

چکیده

در این مقاله ابتدا مقدمه‌ای از ارتباط مسائلی که امکان کنترل اختلال در آن‌ها و حفظ سامانه در یک فضای امن، می‌تواند به عنوان یک مدل ریاضی ارائه شده و ارتباط آنالیز امنیت سامانه با نوع خاصی از معادلات دیفرانسیل بیان می‌شود. سپس با جزئیات دقیق‌تر از یک مدل یک بعدی به ارتباط مجموعه انتخاب‌هایی که منجر به امنیت سامانه با آنالیز جواب‌های ویسکوزیته معادله‌ای خاص از نوع همیلتون- ژاکوبی دارد؛ می‌پردازیم.

واژه‌های کلیدی: نظریه دیفرانسیلی بازی‌ها، معادله دیفرانسیل با مشتقات جزئی، معادله دیفرانسیل همیلتون- ژاکوبی، جواب ویسکوزیته.

۱- مقدمه

نظریه بازی‌ها[1] حوزه‌ای از ریاضیات است که به مطالعه بهترین رفتار در قالب محدودیت‌های موجود در یک سامانه می‌پردازد. این رفتار زمانی اهمیت می‌یابد که انتخاب‌ها و رفتارهای خارج از پیش‌بینی سایرین، بتواند خروجی سامانه را تغییر دهد. این گویش از مسئله را می‌توان در بسیاری از مسائل کاربردی در اقتصاد، مسائل کنترل در مهندسی مکانیک و برق و هم‌چنین در برنامه‌ریزی غیرخطی مسائل مختلفی از شاخه‌های مختلف مهندسی صنایع و الگوریتم‌های برخط[2] که از جمله در بازی‌ها، سامانه های امنیتی و ... کاربرد دارند مطرح نمود. به عنوان مثال مقالات [۷-۱] را می‌توان به عنوان مسائلی مختلفی که در این قالب مطرح می‌شوند، معرفی نمود. هم‌چنین جهت اطلاع دقیق‌تر از نظریه بازی‌ها در سیستم‌های دینامیکی که به دنبال تعیین مسیری برای دریافت نتیجه مطلوب با لحاظ‌کردن تصمیمات، اختلالات و یا اقدامات سایرین در سامانه که مثلاً در حوزه‌های امنیتی این دخالت‌ها می‌تواند شامل حمله‌های هکر نیز باشد؛ به مرجع [۸] ارجاع می‌دهیم.

در ابتدا برای ورود دقیق‌تر به بحث، کلیت مسئله امنیتی الکترونیک مطرح‌شده در مرجع [۲] را به صورت عمومی زیر مطرح می کنیم. فرض کنید تراکنش پویای بین سیگنال رفت و برگشت در یک دستگاه کنترل هوشمند منتج به مجموعه‌ای از معادلات دیفرانسیل شده باشد که در آن سیگنال‌های ورودی از یک هکر یا خطاهای سیستمی و بنابراین تمهیدات کنترلی برنامه‌ریز را هم با پارامترهایی لحاظ کرده باشیم. مجموعه معادلات مورد بحث را به صورت دستگاه معادله‌ای به فرم $\frac{dX}{dt} = f(X,u)$ است که در آن t معرف زمان، $X:\mathbb{R}\to\mathbb{R}^n$ که $X(t) = (X_1(t),\dots,X_n(t))$، $u:\mathbb{R}\to\mathbb{R}^m$ که $u(t) = (u_1(t),\dots,u_m(t))$ و $f:\mathbb{R}^n\times\mathbb{R}^m\to\mathbb{R}^n$ نگاشتی معلوم می‌باشد. در این مدل مولفه‌های X_i ناظر به کمیت‌هایی است که در یک عملکرد مطلوب از سامانه در دامنه قابل قبولی که به آن فضای امن[3] سامانه می‌گوییم، تغییر می‌کند و u_i ها مربوط به انواع سیگنال‌های خارج از پیش‌بینی از سوی محیط یا هکرها و یا موارد کنترلی برنامه‌ریز است. اگر برای دستگاه معادلاتی $\frac{dX}{dt} = f(X,u)$ به ازای $x_0\in\mathbb{R}^n$ شرط اولیه $X(0) = x_0$ در نظر گرفته شده باشد که نشان‌دهنده وضعیت سیگنال‌ها در زمان راه‌اندازی سامانه است، مسئله امکان کنترل این‌گونه مطرح می‌شود که انتخاب این شرط اولیه در این که جواب دستگاه معادله در لحظات بعدی علی‌رغم مولفه‌های تابع u همواره در فضای امن قرار گیرد، چقدر است؟ آیا می‌توان شرط اولیه را در لحظه راه‌اندازی و یا حتی در لحظات بعدی به گونه‌ای انتخاب نمود در لحظات پس از آن جواب سامانه در فضای امن جواب ها قرار

* رایانامه نویسنده مسئول: Ssaiedinezhad@iust.ac.ir

1- Game theory
2- Online algorithm
3- Safe set

گیرد؟

تعبیر شهودی امکان کنترل و قرارگرفتن جواب دستگاه معادلاتی در فضای امن مورد نظر، در مسائل مختلف، متفاوت است. به طور مثال، اگر مسئله مطرح‌شده در مقاله [۴] را در نظر بگیریم که نیروهای واردشده بر چگالی جرم نقطه‌ای یک هواپیما است که مولفه‌های X_i مطرح شده در آن معرف ارتفاع و سرعت هواپیما است و مولفه‌های u_i شامل سرعت باد، زوایای هواپیما نسبت به زمین و جهت باد و تکانه موتور و ... است و مسئله امکان کنترل یعنی سرعت اولیه و ارتفاع مطلوب اولیه به گونه‌ای باشند که با کنترل مولفه‌هایی از u که امکان کنترل دارد، در تمام لحظات، پس از تثبیت نسبی ارتفاع هواپیما، علی‌رغم تاثیر نیروهای غیرقابل کنترل نظیر باد و جاذبه بر هواپیما، هواپیما با سرعت و ارتفاع متغیر در یک دامنه امن حرکت کند.

۲- مدل ریاضی

جهت امکان ادامه بحث از منظر ریاضی، تعاریف، مفروضات و محدودیت های دستگاه معادله با مشتقات جزئی از مرتبه اول $\frac{dX}{dt} = f(X,u)$ را به صورت زیر در نظر بگیرید:

۱) به ازای یک $T > 0$ ، $t \in [0,T]$

۲) $X = X(t): [0,T] \to \mathbb{R}^n ; (n \geq 1)$

۳) $f = f(X,u): \mathbb{R}^n \times U \to \mathbb{R}^n$ تابعی با خاصیت لیپشیتس[1] نسبت به مولفه اول و پیوسته نسبت به مولفه دوم خود است که در آن U زیر مجموعه فشرده‌ای از $\mathbb{R}^m$ است که $m \geq 1$.

۴) K زیرمجموعه فشرده‌ای از $\mathbb{R}^n$ است که از آن با عنوان فضای امن جواب‌ها یاد می‌کنیم.

۵) $\mathfrak{U}_{[t,T]}$ خانواده تمام توابع لبگ انتگرال‌پذیر[2] از بازه $[t,T]$ به U می باشد.

حال دستگاه معادله مرتبه اول زیر که وابسته به زمان اولیه t، تابع جواب اولیه x_t و تابع u است به صورت زیر در نظر بگیرید:

$$P(t,x_t,u): \begin{Bmatrix} \frac{dX(s)}{ds} = f(X(s),u(s)); \\ X(t) = x_t \end{Bmatrix} \qquad (۱)$$

با توجه به فرض (۳) از مبانی نظریه معادلات دیفرانسیل می‌دانیم به ازای هر $(t,x,u) \in [0,+\infty) \times \mathbb{R}^n \times \mathfrak{U}_{[t,T]}$ مسئله $P(t,x,u)$ دارای جواب منحصر به فردی چون، $X_{t,x,u} = X_{t,x,u}(s)$ است. لذا مجموعه شرایط اولیه‌ای را که مسئله $P(t,x,u)$ را غیرقابل آسیب‌پذیر می‌کنند (یعنی از لحظه t به بعد جواب‌ها در هر لحظه در فضای امن K قرار می‌گیرند)؛ با عنوان مجموعه $Inv(t,K)$ به صورت زیر تعریف می شود:

$$Inv(t,K) := \begin{Bmatrix} x \in \mathbb{R}^n;\ \forall u \in \mathfrak{U}_{[t,T]}, \forall s \geq t \\ : X_{t,x,u}(s) \in K \end{Bmatrix} \qquad (۲)$$

واضح است که اگر $t_1 < t_2$ آن‌گاه $Inv(t_1,K) \subseteq Inv(t_2,K)$ پس به ازای هر $t > 0$، $Inv(0,K) \subseteq Inv(t,K)$. به همین دلیل، در آنالیز کنترل صرفاً به محاسبه $Inv(0,K)$ اکتفا نمی‌کنند؛ چرا که با گذشت زمان انتظار می‌رود دامنه شرایط اولیه غیرقابل آسیب‌پذیر افزایش یابد و البته در بسیاری از موارد این توسعه از لحظاتی به بعد متوقف یا کند می‌شود.

لـــم ۲-۱: گـــزاره منطقـــی $x = (x_1, \dots, x_n) \in K$ کـــه در آن $K := [a_1,b_1] \times \dots \times [a_n,b_n] \subset \mathbb{R}^n$ را می‌توان با تعریـف تـابع $l_K(x) = \min_{1 \leq i \leq n} \min\{x_i - a_i, b_i - x_i\}$ به صـورت زیـر بیـان کرد:

$$x \in K \Leftrightarrow\ l_K(x) \geq 0 \qquad (۳)$$

تبصره ۲-۲: اگر بخواهیم تابع l_K تعریف‌شده در لم قبل کراندار باشد، می‌توان از یک جایی به بعد، در اطراف K تابع را به شکل پیوسته ثابت گرفت.

صورت کلی‌تر لم ۲-۱ را که در آن K لزوماً یک حجره n بعدی نباشد، صورت زیر بیان می‌شود.

لم ۲-۳: گزاره منطقی $x = (x_1, \dots, x_n) \in K$ که در آن $K \subset \mathbb{R}^n$ را می‌توان با تعریف تابع:

$$l_K(x) = -dist(x,K) = -inf(|x-y|; y \in K\}$$

به صورت زیر بیان کرد:

$$x \in K \Leftrightarrow\ l_K(x) \geq 0 \qquad (۴)$$

نتیجه ۲-۴: نتیجه به صورت زیر خواهد بود:

$$Inv(t,K) := \begin{Bmatrix} x \in \mathbb{R}^n;\ \forall u \in \mathfrak{U}_{[t,T]}, \forall s \geq t: \\ l(X_{t,x,u}(s)) \geq 0 \end{Bmatrix} \qquad (۵)$$

با توجه به نتیجه ۲-۴ و تعریف $V_K(x,t)$ قضـیه زیـر روشـن است.

قضیه ۲-۵: اگر

$V_K(x,t) := \inf_{u(.) \in \mathfrak{U}_{[t,T]}} \inf_{s \in [t,T]} l_K(X_{t,x,u}(s))$ آن‌گاه

$Inv(t,K) := \{x \in \mathbb{R}^n;\ V_K(x,t) \geq 0\}$

۳- ارتباط با نوع خاصی از معادله دیفرانسیل با مشتقات جزئی

در ادامه به‌شکل غافل‌گیرکننده‌ای تابع V_K را به صورت جواب‌های خاصی از یک معادله دیفرانسیل که به آن جواب ویسکوزیته می‌گویند؛ معرفی می‌کنیم. به منظور ورود به این بحث تعاریف و قضایای مقدماتی آن‌را بیان می‌کنیم.

1- Lipschitz
2- Lebesgue integrable

تعریف ۳-۱: تابع کراندار و پیوسته یک‌نواخت u را یک جواب ویسکوزیته از معادله با شرط اولیه:

$$\mathfrak{p}_0:\begin{Bmatrix} u_t(x,t)+H(\nabla u,x)=0; & (x,t)\in\mathbb{R}^n\times(0,+\infty) \\ u(x,0)=g(x); & x\in\mathbb{R}^n \end{Bmatrix} \quad (۶)$$

که در آن، $H:\mathbb{R}^n\times\mathbb{R}^n\to\mathbb{R}$ و $g:\mathbb{R}^n\to\mathbb{R}$ توابعی معلوم هستند، می‌نامیم هرگاه موارد (الف– ج) در زیر درست باشد:

(الف) تابع u شرط اولیه معادله را برقرار سازد، یعنی به ازای هر $x\in\mathbb{R}^n$ ؛ $u(x,0)=g(x)$.

(ب) به ازای هر تابع هموار $v\in C^\infty(\mathbb{R}^n\times(0,\infty))$، اگر $u-v$ دارای بیشینه موضعی در نقطه $(x_0,t_0)\in\mathbb{R}^n\times(0,\infty))$ است، آن‌گاه:

$$v_t(x_0,t_0)+H(\nabla v(x_0,t_0),x_0)\le 0 \quad (۷)$$

ج) به ازای هر تابع هموار $v\in C^\infty(\mathbb{R}^n\times(0,\infty))$ اگر $u-v$ دارای کمینه موضعی در نقطه $(x_0,t_0)\in\mathbb{R}^n\times(0,\infty))$ است، آن‌گاه:

$$v_t(x_0,t_0)+H(\nabla v(x_0,t_0),x_0)\ge 0 \quad (۸)$$

تبصره ۳-۲: بدیهی است که هر تابع جواب از معادله $\mathfrak{p}_0$ به این معنی که معادله را برقرار ساخته و کراندار و پیوسته یک‌نواخت باشد، یک جواب وسکوزیته از معادله است و بنابراین تعریف جواب ویسکوزیته تعریفی ضعیف‌تر از جواب کلاسیک و حتی جواب ضعیف معادله $\mathfrak{p}_0$ است. در این خصوص برای کسب جزئیات بیش‌تر، به [۹-۱۱] ارجاع می‌دهیم.

تبصره ۳-۳: اگر مسئله با شرط انتهایی بیان شده باشد یعنی مسئله $\mathfrak{p}_T$ به جای مسئله $\mathfrak{p}_0$ به صورت زیر مطرح باشد:

$$\mathfrak{p}_T:\begin{Bmatrix} u_t(x,t)+H(\nabla u,x)=0; & (x,t)\in\mathbb{R}^n\times(0,T) \\ u(x,T)=g(x); & x\in\mathbb{R}^n \end{Bmatrix}. \quad (۹)$$

آن‌گاه از آن‌جایی که u جواب ویسکوزیته معادله $\mathfrak{p}_T$ است اگر و فقط اگر $w(x,t):=u(x,T-t)$ جواب ویسکوزیته معادله با شرط اولیه،

(۱۰)

$$\begin{Bmatrix} w_t(x,t)-H(\nabla w,x)=0; & (x,t)\in\mathbb{R}^n\times(0,T) \\ w(x,0)=g(x); & x\in\mathbb{R}^n \end{Bmatrix}$$

باشد؛ پس در قسمت‌های (ب) و (ج) در تعاریف جواب ویسکوزیته نظیر معادله با شرط انتهایی $\mathfrak{p}_T$ جهت‌های نامساوی‌های موجود در بندهای (ب) و (ج) معکوس می‌گردد.

قضیه۳-۴: فرض کنید مفروضات ۵-۱ برقرار باشند؛ اگر $V=V_K(x,t)$ مطابق با تعریف ارائه‌شده در قضیه ۱-۱ باشد، آن‌گاه V جواب ویسکوزیته منحصر به فرد مسئله با شرط انتهایی زیر است:

(۱۱)

$$\begin{Bmatrix} v_t(x,t)+\min\{0,\inf_{u\in U}v_x(x,t).f(x,u)\}=0; & (x,t)\in\mathbb{R}^n\times(0,T) \\ V(x,T)=l_K(x); & x\in\mathbb{R}^n \end{Bmatrix}.$$

قضیه فوق را در مورد یک حالت خاص و ساده از مسئله کنترل امنیت دستگاه خطی که در بخش بعدی بیان می‌شود، ادامه می‌دهیم.

۴- آنالیز یک مسئله یک بعدی

مسئله یک بعدی زیر در نظر بگیرید:

$$p_{t,x,u}:\begin{Bmatrix} \frac{dX}{ds}=u(s); & s\in[t,T) \\ X(t)=x \end{Bmatrix} \quad (۱۲)$$

در این مسئله فرض کنید $U=[a,b]$ و $K=[c,d]$ که $a,b>0$. واضح است که مسئله $p_{t,x,u}$ دارای جواب منحصر به فرد $X_{t,x,u}(s)$ است که در واقع $X_{t,x,u}(s)=x+\int_t^s u(s)ds$. بنابراین داریم:

(۱۳)

$$l_K(X_{t,x,u}(s)=\min\{x+\int_t^s u(r)ds-c,d-x-\int_t^s u(r)dr\}$$

$$=\frac{d-c-|d+c-2(x+\int_t^s u(r)dr)|}{2}:=\frac{d-c}{2}-|A_x-B_t(s,u)|.$$

که در آن، $A_x=\frac{d+c-2x}{2}$ و $B_t(s,u)=\int_t^s u(r)dr$. واضح است که به ازای هر $u\in\mathfrak{U}_{[t,T]}$، $0\le B_t(s,u)\le\int_t^T u(r)dr$.

بنابراین داریم:

(۱۴)

$$Sup_{s\in[t,T]}|A_x-B_t(s,u)|=$$
$$\begin{Bmatrix} \int_t^T u(r)dr-A_x; & \int_t^T u(r)dr\ge 2A_x \\ A_x; & \int_t^T u(r)dr<2A_x \end{Bmatrix},$$

و لذا داریم:

$$\inf_{s\in[t,T]} l_K(X_{t,x,u}(s)) = \begin{cases} \frac{d-c}{2} + A_x - \int_t^T u(r)dr; & \int_t^T u(r)dr \geq 2A_x \\ \frac{d-c}{2} - A_x; & \int_t^T u(r)dr < 2A_x \end{cases}; \quad (۱۵)$$

به ازای x و t معلوم، قرار می دهیم:

$$\Gamma\Sigma := \mathfrak{U}_{[t,T]} \setminus \Gamma := \{u \in \mathfrak{U}_{[t,T]}; \int_t^T u(r)dr \geq 2A_x\} \quad (۱۶)$$

از آن‌جا که به ازای هر $r \in [t,T]$ ، $u(r) \in [a,b]$؛ واضح است اگر $a(T-t) \geq 2A_x$ آن‌گاه $\mathfrak{U}_{[t,T]} = \Gamma$ و اگر $b(T-t) \leq 2A_x$ آن‌گاه $\mathfrak{U}_{[t,T]} = \Sigma$ و در غیر این دو صورت $\Sigma, \Gamma \neq \emptyset$؛ لذا $u(r) \equiv a \in \Sigma$ و $u(r) \equiv b \in \Gamma$. بنابراین داریم:

(۱۷)

$$V_K(x,t) := \inf_{u(.)\in\mathfrak{U}_{[t,T]}} \inf_{s\in[t,T]} l_K(X_{t,x,u}(s)) =$$

$$\min\left\{\inf_{u(.)\in\Gamma}\inf_{s\in[t,T]} l_K(X_{t,x,u}(s), \inf_{u(.)\in\Gamma}\inf_{s\in[t,T]} l_K(X_{t,x,u}(s)\right)$$
$$= \min\left\{\frac{d-c}{2} + A_x - b(T-t), \frac{d-c}{2} - A_x\right\}$$
$$= \min\{d - x - b(T-t), x - c\}$$

همان‌طور که مشاهده می‌شود:

$$V_K(x,T) = l_K(x) = \min\{d-x, x-c\} \quad (۱۸)$$

حال تحقق شرایط (ب) و (ج) در تعریف ۳-۱ را برای تابع $V = V_K(x,t)$ بررسی می‌کنیم.

اگر $v - w$ در نقطه (x_0,t_0) دارای بیشینه موضعی باشد، پس به ازای (x,t)های به اندازه کافی نزدیک به (x_0,t_0) (مثلاً به ازای یک $\delta_1 > 0$ و (x,t)هایی که $(x-x_0)^2 + (t-t_0)^2 < \delta_1$) داریم:

$$v(x_0,t_0) - w(x_0,t_0) \geq v(x,t) - w(x,t) \quad (۱۹)$$

بنابراین داریم:

$$v(x,t) - v(x_0,t_0) \leq w(x,t) - w(x_0,t_0). \quad (۲۰)$$

فرض کنید به ازای یک $\theta > 0$ داشته باشیم:

$$w_t(x_0,t_0) + \min\{0, \inf_{u\in[a,b]} w_x(x_0,t_0)\, u\} \leq -\theta; \quad (۲۱)$$

داریم: $\inf_{u\in[a,b]} w_x(x_0,t_0)\, u < 0$ در این صورت اگر

$$w_t(x_0,t_0) + \inf_{u\in[a,b]} w_x(x_0,t_0)\, u \leq -\theta, \quad (۲۲)$$

که اگر $w_x(x_0,t_0) < 0$ آن‌گاه:

$$w_t(x_0,t_0) + b w_x(x_0,t_0) \leq -\theta, \quad (۲۳)$$

و اگر $w_x(x_0,t_0) \geq 0$ آن‌گاه:

$$w_t(x_0,t_0) + a w_x(x_0,t_0) \leq -\theta \quad (۲۴)$$

بدون این‌که به کلیت استدلال خللی وارد آید، نامساوی (۲۳) را درنظر می‌گیریم.

از آن‌جایی که تابع w هموار است، نامساوی (۲۳) در یک همسایگی به قدر کافی کوچک از (x_0,t_0) نیز برقرار است و لذا $\delta_1 > \delta_2$ را به گونه‌ای انتخاب می‌کنیم که اگر $(x-x_0)^2 + (t-t_0)^2 < \delta_2$ داشته باشیم:

$$w_t(x,t) + b w_x(x,t) \leq -\theta \quad (۲۵)$$

حال تابع پیوسته یک‌نواخت $X_{t_0,x_0,b}(s)$ را درنظر بگیرید که داریم: $\lim_{t\to t_0} X_{t_0,x_0,b}(t) = x_0$ پس به ازای tهای به قدر کافی نزدیک به t_0 داریم:

$$(X_{t_0,x_0,b}(t) - x_0)^2 + (t-t_0)^2 < \delta_2 \quad (۲۶)$$

و لذا:

$$w_t(X_{t_0,x_0,b}(t),t) + b w_x(X_{t_0,x_0,b}(t),t) \leq -\theta \quad (۲۷)$$

با توجه به رابطه (20) داریم:

$$v(X_{t_0,x_0,b}(t_0+h), t_0+h) - v(x_0,t_0)$$
$$\leq w(X_{t_0,x_0,b}(t_0+h), t_0+h) - w(x_0,t_0)$$
$$= \int_{t_0}^{t_0+h} \frac{dw(X_{t_0,x_0,b}(t),t)}{dt}\, dt$$
$$= \int_{t_0}^{t_0+h} w_t(X_{t_0,x_0,b}(t),t) + b w_x(X_{t_0,x_0,b}(t),t)\, dt$$
$$\leq -\theta\, h.$$

(۲۸)

از طرفی داریم:

(۲۹)

$$v(x_0,t_0) = \min\{d - x_0 - b(T-t_0), x_0 - c\} =$$
$$\min\{d - x_0 - b(T-(t_0+h)) - b((t_0+h)-t_0), x_0 - c\}$$
$$\leq \min\{d - x_0 - bh - b(T-(t_0+h)), x_0 + bh - c\}$$
$$= v(X_{t_0,x_0,b}(t_0+h), t_0+h)$$

که با رابطه (۲۸) در تناقض است بنابراین در این مرحله ثابت می‌شود:

$$w_t(x_0,t_0) + \min\{0, \inf_{u\in[a,b]} w_x(x_0,t_0)\, u\} \geq 0 \quad (۳۰)$$

تا این‌جا تحقق شرط (ب) را با فرض:

$$\inf_{u\in[a,b]} w_x(x_0,t_0)\, u < 0 \quad (۳۱)$$

ثابت کرده‌ایم. اما اگر $\inf_{u\in[a,b]} w_x(x_0,t_0)\ u > 0$ و (23) برقرار باشد خواهیم داشت: $w_t(x_0,t_0) \le -\theta$. لذا به ازای مقادیر به قدر کافی کوچک $0 < h$،

$$w_t(x_0, t_0 + h) \le -\theta \qquad (۳۲)$$

بنابراین با توجه به (20) داریم:

(۳۳)

$$v(x_0,t_0+h) - v(x_0,t_0) \le w(x_0,t_0+h) - w(x_0,t_0) = \int_{t_0}^{t_0+h} \frac{dw(x_0,t)}{dt}\,dt \le -\theta\, h.$$

از طرفی با توجه به تعریف $v(x,t)$، واضح است که تابع v نسبت به t صعودی است که با (33) در تناقض است. بنابراین اثبات تحقق شرط (ب) از تعریف 3-1 در این مرحله به اتمام می‌رسد.

به طریق مشابه می‌توان تحقق شرط (ج) را بررسی کرد که به جهت اختصار از ارائه اثبات آن چشم‌پوشی می‌کنیم.

۵- نتیجه‌گیری

بسیاری از مسائلی که در قالب یک مسئله کنترل مطرح می‌شوند، اگر توابع درگیر در رفتار دینامیک آن‌ها توابعی خوش‌رفتار باشند، مسئله امکان کنترل اختلال در سامانه آن‌ها را می‌توان با آنالیز نوع خاصی از جواب‌های معادله‌ای از نوع همیلتون- ژاکوبی[1] با شرط اولیه یا شرط انتهایی که به معادله و فضای امن آن نظیر می‌شود؛ بررسی نمود. یافتن مجموعه شرایط اولیه امن برای سامانه در مدل‌هایی با ابعاد بالا و دستگاه‌های غیرخطی بسیار سخت و دشوار است که در این صورت کارکرد معادلات دیفرانسیل که در قالب قضیه 3-4 در این مقاله مطرح شد، مشهود خواهد بود.

۶- مراجع

[1] P. Cardaliaguet, "A differential game with two players and one target," SIAM Journal on Control and Optimization, vol. 34, no. 4, pp. 1441-1460, 1996.

[2] Esfahani, P. Mohajerin, et al., "Cyber attack in a two-area power system: Impact identification using reachability," American Control Conference (ACC), 2010. IEEE, 2010.

[3] E. C. Lawrence, "Graduate studies in mathematics," Partial differential equations, vol. 19, 1998.

[4] T. L. Friesz, "Dynamic optimization and differential games," vol. 135, Springer Science & Business Media, 2010.

[5] J. Lygeros, "On reachability and minimum cost optimal control," Automatica, vol. 40, no. 6, pp. 917-927, 2004.

[6] S.-Y. Mu and Q. Zhu, "Power distribution algorithm based on game theory in the femtocell system," The Journal of China Universities of Posts and Telecommunications, vol. 20, no. 2, pp. 42-47, 2013.

[7] R. S. Sharma and S. Bhattacharya, "Knowledge dilemmas within organizations: Resolutions from game theory," Knowledge-Based Systems, vol. 45, pp. 100-113, 2013.

[8] E. C. Lawrence, and P. E. Souganidis, "Differential Games and Representation Formulas for Solutions of Hamilton-Jacobi-Isaacs Equations," no. Mrc-Tsr-2492. Wisconsin Univ-Madison Mathematics Research Center, 1983.

[9] M. G. Crandall, C. E. Lawrence, and P.-L. Lions, "Some properties of viscosity solutions of Hamilton-Jacobi equations," Transactions of the American Mathematical Society, vol. 282, no. 2, pp. 487-502, 1984.

[10] M. G. Crandall and P.-L. Lions, "Viscosity solutions of Hamilton-Jacobi equations," Transactions of the American Mathematical Society, vol. 277, no. 1, pp. 1-42, 1983.

[11] 11- E. C. Lawrence, "Graduate studies in mathematics," Partial differential equations, vol. 19, 1998.

1- Hamilton-Jacobi

مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"
ویژه‌نامه کنفرانس بین‌المللی ترکیبیات، رمزنگاری و محاسبات، ص ۹۸ -۹۱

رمز و رمزگرایی در جنگ نرم با تکیه بر ادبیات فارسی

سیدخلیل باقری*

مربی، عضو هیأت علمی دانشگاه علم و فناوری مازندران

(دریافت: ۹۵/۰۷/۰۵، پذیرش: ۹۶/۰۳/۰۶)

چکیده

تلاش برای بیان تعریفی مستقل از رمز همراه با دلایل و انگیزه آن در جنگ نرم تا حدودی مرهون رمزگرایی شاعران است. رویکرد رمزگرایی به جنگ نرم و سایبری از یک سو حاصل شرایط سیاسی و اجتماعی خاصی است که ما در آن زندگی می‌کنیم و از سویی دیگر حاصل نگاه شاعران و نویسندگان می‌باشد. رمزهای دشمن در جنگ نرم همراه با اهداف از موضوعاتی هستند که این مقاله در پی تفسیر و تبیین آن‌هاست. کوتاه سخن آن‌که در این پژوهش تلاش بر این است رمز و رمزگرایی در جنگ نرم با تکیه بر اشعار برخی شاعران همراه با راه‌کارها، هرچند کوتاه و مختصر، بررسی و به آن توجه شود. بنابراین، پژوهش پیش‌رو بر چند نمونه از رمز دشمن در جنگ نرم متمرکز شده است.

واژه‌های کلیدی: رمز، جنگ نرم، ادبیات، دشمن

۱- مقدمه

رمز یک کلمه عربی است که در زبان فارسی معانی گوناگونی دارد. رمز (نماد یا مظهر و با اندکی تسامح، سمبل لاتین) یکی از عناصر زیبایی سخن و از جمله صور خیال مستقل است و شاعران و نویسندگان بسیاری از این تصویر خیالی بهره گرفته‌اند. کلمه رمز به عنوان یکی از مهم‌ترین موضوعات در زبان و ادبیات فارسی در اصل مصدر مجرد از باب نَصَرَ - یَنصُرُ و به معنی اشاره به لب، چشم، ابرو، دست، دهن و یا زبان است. رمز در زبان فارسی به معنای اشاره، سرّ، ایما، نکته، دقیقه، علامت، اشاره‌کردن پنهان، نشانه‌ای مخصوص که مطلبی خاص از آن درک شود، بیان مقصود با نشانه‌ها و علایم قراردادی و... است. واژه رمز در قرآن [۱] تنها یک بار و آن هم در آیه ۴۱ سوره آل عمران آمده است:

قالَ رَبِّ اجْعَلْ لی آیَةً قالَ آیَتُکَ أَلاَّ تُکَلِّمَ النَّاسَ ثَلاثَةَ أَیَّامٍ إِلاَّ رَمْزاً

مفسرین رمز را در این آیه این‌گونه معنی کرده‌اند: صاحب ترجمه تفسیر طبری، رمز را در این آیه "اشارت" و راغب اصفهانی" اشارت با لب و صوت خفی" معنی کرده است. [۳-۲]

در علم بیان [۴]، رمز را این‌گونه تعریف کرده‌اند: رمز کنایه‌ای است که وسایط آن اندک باشد و معنی پنهان و احتیاج به قدری تامل دارد. در آثار متصوفه هم رمز این‌گونه معنی شده است:

رمز عبارت از معنی باطنی است که مخزون است تحت کلام ظاهری که غیر از اهل آن بدان دست نیابند. [۵]

قداقه ابن‌جعفر اولین کسی است که در کتاب "نقدالنثر" درباره رمز به عنوان یک اصطلاح صحبت کرده است:

" گویندگان آن‌گاه که می‌خواهند مقصود خود را از کافه مردم بپوشانند و فقط بعضی را از آن آگاه کنند در کلام خود رمز به کار می‌برند. بدین سان برای کلمه یا حرف، نامی از نام‌های پرندگان یا وحوش یا اجناس دیگر یا حرفی از حروف محجم را در رمز قرار می‌دهند و کسی را که بخواهد مطلب را بفهمد آگاهش می‌کنند. پس آن کلام در میان آن دو، مفهوم و از نظر دیگران مرموز است. "آن‌چه که در تمام این معانی مشترک است " عدم صراحت و پوشیدگی" است.

اما جنگ نرم، نوعی از جنگ است که در قرن بیست و یکم و در عصر ارتباطات، مورد توجه قدرت‌های استکباری قرار گرفته است. مفهوم جنگ نرم، در مقابل جنگ سخت است و تعریف واحدی که مورد پذیرش همگان باشد را ندارد. جنگ نرم در فرهنگ سیاسی به معنای، فروپاشی از درون، براندازی قانونی، براندازی خاموش، براندازی در سکوت، انقلاب مخملی، انقلاب رنگی، انقلاب سرخ و در حقیقت؛ شامل هرگونه اقدام روانی و تبلیغات رسانه‌ای است که "جامعه هدف" یا گروه هدف را نشانه می‌گیرد و با هدف گرفتن فکر و اندیشه ملت‌ها، تغییر ارزش‌ها، نقش مهمی در درست‌کردن حلقه‌های فکری و فرهنگی جوامع

* رایانامه نویسنده مسئول: kh_bagheri46@mazut.ac.ir

ایفا می‌کند و بدون درگیری نظامی، رقیب را به انفعال یا شکست وا می‌دارد. و به عبارت دیگر، با روش مسالمت‌آمیز و روش‌های قانونی موجود در قوانین نظام حاکم، به براندازی اقدام می‌کند. و تعریف دیگری که از جنگ نرم می‌توان به آن اشاره کرد عبارت است از: استفاده از ابزارهای فرهنگی و روش‌های نوین که به آرامی در بافت فرهنگی و هویتی یک نظام حرکت می‌کند. آثار عمیقی از خود به جای می‌گذارد، جبران اثرات آن به سادگی قابل جبران نیست و در نهایت موجب تغییر در مبانی یک نظام به سمت الگوهای مهاجم خواهد شد.

۲- دلایل و انگیزه رمز

در این بخش در مورد دلایل و انگیزه های رمز که به سه قسمت ۱) محدود بودن واژه ها در گستره زبان های بشری ۲) اسطوره سازی ۳) ترس از حکومت های خودکامه و ستم گر است تقسیم بندی می شود، بحث خواهد شد.

۲-۱- محدودبودن واژه‌ها در گستره زبان‌های بشری

نویسنده یا گوینده برای جبران این محدودیت زبان، می‌کوشد که با استفاده از کلمات موجود و بهره‌گیری از انواع صور خیال، کمبود واژگانی زبان را جبران کند. در این صورت به مجاز، رمز و کنایه ... روی می‌آورد. هر کدام از واژه‌ها و ترکیباتی چون نی، نیستان، ساقی، زلف، خط، ابرو، آب، کویر، زمستان، زندان، می، باغ هشت در، دیو، آیینه و ... در کنار معانی اصلی خود می‌تواند دست آویزی برای کاربرد معانی بلند عرفانی، غنایی، فلسفی، حماسی و انتقادی باشد. می‌توان به غزلیات حافظ[۶] ، مولانا [۷] یا غزل رمزآلود عراقی [۸] اشاره کرد.

نخستین باده کاندر جام کردند، ز چشم مست ساقی وام کردند
چو با خود یافتند اهل طرب را، شراب بی‌خودی در جام کردند
لب می‌گون جانان جام در داد، شراب عاشقانش نام کردند
ز بهر صید دل‌های جهانی، کمند زلف خوبان دام کردند...
ز بهر نقل مستان از لب و چشم، مهیا پسته و بادام کردند...
به غمزه صد سخن باز جان بگفتند، به دل ز ابرو دو صد پیغام کردند
جمال خویشتن را جلوه دادند، به یک جلوه دوعالم رام کردند

[۸] (عراقی ۱۳۳۸ : ۱۹۳)

۲-۲- اسطوره‌سازی

چرا که اسطوره نزد انسان‌های نخستین، بخش جدایی‌ناپذیری زندگی بوده است. بعد بشر به پروراندن رابطه خود با اسطوره پرداخته و به دنبال پیداکردن مظاهر خصلت‌ها و خلق‌وخوی خود در میان آن‌ها بوده است. در پایان -اسطوره‌زدایی- بشر با تکیه بر خود به چون و چرا در چگونگی و انکار اسطوره پرداخته است. گیلگمش، ایلیاد، ادیسه، آنه ید، شاهنامه و ... زاییده این دوره‌اند. با توجه به این مضامین دیوان، اژدهایان و رب‌النوع ها (خدایان) هر کدام رمز و نمادی می‌شود.

۲-۳- ترس از حکومت‌های خودکامه و ستم‌گر

یکی‌دیگر از راه‌های کشاندن ذهن و زبان شاعر و نویسنده به سوی رمزگرایی و استفاده از زبان حیوانات در داستان‌های فابل در آثاری چون کلیله و دمنه، مرزبان نامه، بهره‌گیری از عناصر طبیعی در آثار شاعرانی مانند: بهار، نیما، اخوان ثالث و دیگران است. انگیزه دیگر رمز، کهن الگو، فرصت بیش‌تر برای شکوفایی ذهن خوانندگان، نویسندگان نمادگزاری و از همه این‌ها مهم‌تر، غیرت عرفانی است که عرفا و صوفیه نسبت به حفظ اسرار خود دارند که نمی‌خواهند نامحرمان به دنیای اسرار آنان وارد شوند. این موضوع باعث می‌شود که عرفا با رمز، ایما و اشاره به بیان مقصود خود بپردازند.

۳- انواع رمز در ادبیات

در ادبیات رمز را می توان به چهار دسته خاص، عام، قراردادی و فرهنگ عمومی تقسیم بندی می شود [۹] که در ادامه، به اختصار در مورد آنها بحث خواهد شد.

۳-۱- رمز خاص

در ادبیات و فرهنگ هر کشور و قوم و یا پیروان مذهبی، پاره‌ای از نمادها خاص و حتی برای افراد بیرون آن مجموعه هم ناشناخته شده است. ازجمله: صلیب (مسیحیت)، هلال احمر (اسلام)، ترازو (عدالت)، کوه (مقاومت)، خر (تن و حماقت).

۳-۲- رمز عام

سیمرغ در شاه‌نامه بار اول (مربی و پروراننده)، بار دوم (طبیب و شفابخش)، بار سوم (در کنار دیگر مظاهر اهریمنی هفت خوان اسفندیار مظهر خوی اهریمنی) و بار چهارم (یاریگر خاندان زال و کشنده اسفندیار، نماد شخصیتی دو سویه) است. سیمرغ در داستان‌های عرفانی هم رمز حق است. البته این به معنی نادیده‌گرفتن کارکردهای واژه‌های رمزآلود در معانی وسیع نیست. گاهی واژه‌ای مانند شراب، از رموز کلیشه‌ای عرفانی است که از آن، تعبیر تابش انوار الهی در دل سالک می‌شود و درست در تقابل عقل به واسطه القای همین مفهوم است. در همین کلمه، گاهی در برابر رازداری قرار می‌گیرد و متناسب با مفهوم وجد و شوق حاصل از آن است و باز ممکن است در برابر هوشیاری و آگاهی قرار گیرد که با معنی غفلت‌آوربودن آن متناسب باشد و سرانجام در برابر جهل و ظلمت قرار گیرد که با اشراق حاصل از

آن تناسب دارد. پس عام‌بودن رمز ارتباطی به مفاهیم آن ندارد.

۳-۳- رمز قراردادی

بیش‌تر واژه‌ها و ترکیبات و درون مایه‌های ادبیات عرفانی، انتقادی، حماسی و غنایی ادب فارسی از این دسته‌اند. گاهی خود شاعر و نویسنده به رمزگشایی آن می‌پردازد و گویی با مخاطب خود قرار می‌گذارد که این واژه را در این‌جا با این مفهوم به کار ببرد. به عنوان نمونه، فردوسی دیو را مظهر مردم بد می‌داند:

تو مر دیو را مردم بدشناس کسی کو ندارد ز یزدان سپاس
هر آن کو گذشت از ره مردمی ز دیوان شمر،مشمر از آدمی
([۱۰]، ۳۱۰)

مولوی در داستان طوطی و بازرگان به رمزگشایی پاره‌ای از نمادهای خود می‌پردازد:

قصه طوطی جان زین سان بود کو کسی که محرم مرغان بود
تن قفس شکل است تن شد خارجان در فریب داخلان و خارجان
(همان/۱۸۴۹/۱)

من چو لب گویم لب دریا بود من چو لا گویم مراد الا بود
(همان/۱۷۵۹/۱)

شیخ محمود شبستری در گلشن راز، زلف، خط، خال، ابرو، ساقی، مغ، دیر، زنار، ...-که از رمزهای قراردادی است- را توضیح داده است. (شبستری ۱۳۶۵: ۹۹-۱۰۸)

۳-۳- رمز در فرهنگ عمومی

زبان ارتباطی و روزمره عامه مردم کاربرد حقیقی دارد و بیش‌تر کلمات در معنی به اصطلاح ما وُضع له خود به‌کار گرفته می‌شود. اما با تأمل و نگاهی دقیق در زندگی روزمره و ارتباطات مردم به خوبی عنصر رمز را می‌توان جست. گذشته از نشانه‌هایی مانند هلال احمر، ترازوی سر در دادگستری، صلیب آویخته به گردن یا روی لباس، انواع علایم در مکان‌های عمومی و یا طلوع و غروب خورشید در فرهنگ مردم بسیاری از کشورها، کوه، چشمه، آب و دریا، ابر، پرستو، کبوتر، شیر، روباه، خروس، طاووس، عقاب، و ... از رمزهای معروف روزمره مردم‌اند.

۴- تعریف مفاهیم جنگ نرم

تا سال ۱۹۴۵ میلادی، اغلب جنگ‌ها جنگ سخت بود[۱۱] . پس از آن، با توجه به قطبی‌شدن جهان به بلوک شرق و غرب، دور جدیدی از رقابت‌ها میان آمریکا و شوروی سابق آغاز شد که به "جنگ سرد" مشهور شد[۱۲]. جنگ سرد، ترکیبی از جنگ سخت و جنگ نرم بود که طی آن، دو ابرقدرت در عین تهدیدات سخت، از رویارویی مستقیم با یک‌دیگر پرهیز می‌کردند. (ماه-پیشانیان ، ۱۳۸۶: ۷۴-۵۴)

امروزه با کوچک‌تر و پیچیده‌ترشدن جهان به واسطه رشد روزافزون وسایل ارتباط جمعی از قبیل اینترنت و ماهواره، معادلات گذشته در تنظیم روابط بین کشورها تا حدود زیادی به هم خورده و جای خود را به معادلات جدیدی داده است؛ به گونه‌ای که به جای به کارگیری مستقیم زور، توجه قدرت‌ها به استفاده از قدرت نرم و ایجاد تغییرات از طریق مسالمت‌آمیز با به کارگیری شیوه‌های نوین مداخله در امور داخلی کشورها جلب شده است. [۱۳]

ویژگی های جنگ نرم: از ویژگی‌های جنگ نرم، آرام، تدریجی و زیرسطحی بودن، نمادساز بودن، پایدار و بادوام بودن، هیجان‌ساز بودن، پرتحرک و جاذبه‌دار بودن، آسیب‌محور بودن، چندوجهی بودن، تهدیدآفرین و تضادآفرین بودن، پیچیده بودن، فتنه‌آمیز بودن، پنهانی و سری بودن، جامعه‌محور بودن و بین رشته‌ای بودن را می‌توان نام برد. نیز در این جنگ از پیشرفته‌ترین روش‌های روز استفاده می‌گردد.

ابعاد جنگ نرم: جنگ نرم در چهار بعد فرهنگی، سیاسی، اجتماعی و اقتصادی قابل بررسی است که در بعد فرهنگی مهم‌ترین هدف آنان تضعیف و تغییر باورها و اعتقادات بنیادی در جامعه و هویت‌سازی‌های جدید فرهنگی و در بعد سیاسی هدف آنان بی‌اعتبارسازی، اعتمادزدایی و سلب مشروعیت نظام و شکاف بین نخبگان، مردم و حاکمیت و در بعد اجتماعی هدف آنان تضعیف و تخریب انسجام و مشارکت اجتماعی، روحیه و دلبستگی ملی و در بعد اقتصادی هدف آنان تضعیف و تخریب مدل و اندیشه اقتصادی و ناکارآمدسازی شیوه‌های مدیریت اقتصادی و ترویج رفاه‌طلبی است.

فرآیند جنگ نرم: اجتماعی مجازی کارآمدترین آنان می‌باشد و جنگ امواج همان رسانه‌های بیگانه مثل ماهواره و ... است و منظور از جنگ دیجیتال، رسانه های سطحی کم‌دانه می‌باشد. اگر فرهنگ شکل‌گیری جنگ نرم را بیان بکنیم باید جنگ نرم در حقیقت جنگ سایبری + جنگ دیجیتالی + جنگ امواج است که در حوزه سایبری شبکه‌های در دو دسته عرصه حکومت و عرصه جامعه (مردم) جدا بیان کنیم که در شکل (۱) به صورت کامل نشان داده شده است.

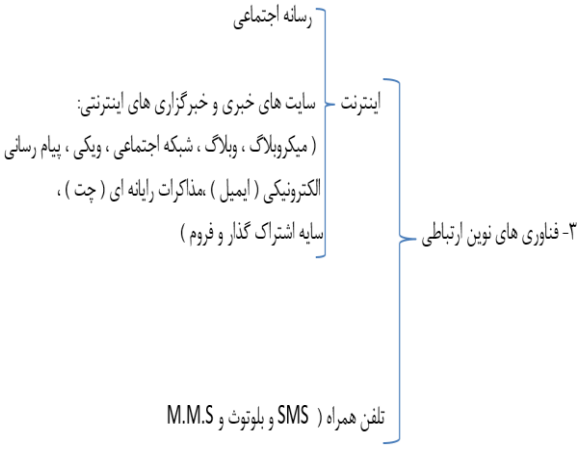
شکل (۱): جنگ نرم

ابزارهای جنگ نرم: خانم فاطمه مرسلی در کتاب "نبرد سایه‌ها" ابزارهای جنگ نرم را به سه دسته تقسیم می کنند.

۱- صنایع فرهنگی که شامل سینما، انیمیشن، ماهواره، اسباب‌بازی، بازی رایانه‌ای و موسیقی

۲- رسانه‌ها که شامل مطبوعات رادیو، تلویزیون، خبرگزاری‌ها و آژانس‌های خبری

۳- فن‌آوری‌های نوین ارتباطی که در شکل (۲) ساختار آن مشاهده می‌شود.



شکل (۲): ساختار فناوری های نوین ارتباطی

اما اگر بخواهیم مهم‌ترین اهداف جنگ نرم آمریکا و دنیای غرب را بیان کنیم عبارتند از:

۱- تغییر ایدئولوژی حاکم
۲- کاهش مشارکت سیاسی مردم
۳- القای ناکارآمدی حکومت
۴- تغییر هویت دینی و ملی شهروندان با تخریب پیشینه تاریخی آنان
۵- دست‌کاری افکار عمومی در جهت خواسته‌های خود و علیه نظام حاکم
۶- کاهش انسجام اجتماعی
۷- کاهش انسجام در حاکمیت و القای حاکمیت دوگانه
۸- تغییر ارزش‌های جامعه
۹- ایجاد استحاله فرهنگی
۱۰- تشدید و تقویت واگرایی قومی
۱۱- تغییر الگوی سیاسی حاکم

اهداف جنگ نرم از دیدگاه مقام معظم رهبری: مقام معظم رهبری در سخنرانی‌ها و دیدارهای خود هدف دشمن از جنگ نرم را این گونه بیان فرمودند که به برخی از آنان اشاره می‌کنم:

۱- بی‌اعتقادکردن نسل نو به دین و اصول انقلابی (دیدار با وزیر، معاونان، مشاوران و مدیران کل وزارت آموزش و پرورش، ۱۳۷۰/۱۰/۲۵)
۲- کشاندن نسل جوان جامعه به ابتذال و فساد اخلاقی (دیدار با اعضای شورای عالی انقلاب فرهنگی، ۱۳۷۱/۰۹/۱۹)
۳- تضعیف فرهنگ ملی و اسلامی ایران (دیدار با فرماندهان گردان‌های عاشورای نیروی مقاومت بسیج، ۱۳۷۱/۰۴/۲)
۴- ناامیدکردن جامعه در مبارزه علیه نظام سلطه (دیدار با کارگران و فرهنگیان کشور به مناسبت روز کارگر و روز معلم، ۱۳۷۲/۰۲/۱۵)
۵- جایگزین‌کردن فرهنگ بیگانه به جای فرهنگ، ارزش‌ها و باورهای مردم (دیدار با دانشگاهیان استان آذربایجان شرقی، ۱۳۷۲/۰۵/۰۹)
۶- خاموش‌کردن روحیه جهادی در صحنه‌های انقلاب و سازندگی (دهمین گردهمایی سراسری ائمه جمعه، ۱۳۷۳/۰۶/۲۱)
۷- ایجاد تصویری تاریک از آینده کشور برای مردم (بیانات رهبری در خطبه‌های نماز جمعه تهران؛ ۱۳۷۹/۰۲/۲۳)
۸- از حیثیت و اعتباراندختن مقاومت در میان ملت ایران (بیانات در دیدار با خانواده‌های شهدای نیروهای مسلح، ۱۳۸۰/۰۷/۰۴)
۹- ایجاد اختلاف و به جان هم انداختن فعالان سیاسی (دیدار با دانش‌آموزان و دانشجویان و تشکل‌های مختلف دانشگاهی در آستانه سال‌روز سیزده آبان، ۱۳۸۷/۰۸/۰۸)
۱۰- ایجاد شکاف میان ایران و دوست‌داران انقلاب اسلامی ایران (پیام رهبری به حجاج بیت‌الله الحرام، ۱۳۷۸/۱۲/۲۳)

راه‌کارهای مقابله با جنگ نرم از نظر مقام معظم رهبری: مقام معظم رهبری در دیدارهای خود با مسئولین، مردم، دانشجویان، نخبگان و... راه‌کارهای زیادی را بیان فرمودند که به شش راه‌کار ارائه‌شده از جانب ایشان می‌پردازیم:

۱- تقویت و پربارکردن فعالیت‌های فرهنگی و هنری. رهبر معظم انقلاب در دیدار با جمعی از شعرا، فرهیختگان و اهالی فرهنگ در مورخ ۱۳۸۸/۰۶/۱۴ فرمودند: هنر را بایستی تمام عیار توی میدان بیاورید. نباید کم گذاشت. جنگ نرم، راست است، این یک واقعیت است.

۲- امید به آینده و دیدی خوش‌بینانه همراه با اعتماد به نفس به دو راز ناامیدی مقام معظم رهبری در دیدار با رئیس و نمایندگان مجلس خبرگان رهبری مورخ ۱۳۸۸/۰۷/۰۲ فرمودند: مخدوش‌کردن نشانه‌های امید و تبدیل آن‌ها به نشانه‌های یاس و تردید و القای بن‌بست و سیاه‌نمایی، گرفتن پویایی جامعه یکی از خطوط مخالفان است. باز در دیدار با دانشجویان در سال ۱۳۸۸ فرمودند: نگاه من به آینده خوش‌بینانه است. نه از روی توهم، بلکه از روی بصیرت.

۳- راه‌اندازی کرسی‌های آزاداندیشی و نظریه‌پردازی آزاد (دیدار اساتید، نخبگان و رئوس دانشگاهی)

۴- بصیرت آحاد جامعه به ویژه نخبگان (دیدار با مردم چالوس و نوشهر)

۵- ایستادگی و عدم سازش در برابر دشمنان انقلاب و نظام اسلامی

۶- اتحاد مردم و جریان‌های سیاسی و دوری از اختلاف و تردید و بدبینی (دیدار با بسیجیان سراسر کشور) مورخ ۱۳۸۸/۰۹/۰۴

۵- رمزگرایی در جنگ نرم و سایبری

قرآن کریم [۱] در سوره بقره آیه ۱۹۴ می‌فرماید:

(فَمَنِ اعْتَدى عَلَيْكُمْ فَاعْتَدُوا عَلَيْهِ بِمِثْلِ مَا اعْتَدى عَلَيْكُمْ وَ اتَّقُوا اللّهَ وَ اعْلَمُوا أَنَّ اللّهَ مَعَ الْمُتَّقينَ)

یعنی هر کس به شما تجاوز کرد، همانند آن بر او تعدی کنید و از (مخالفت فرمان) خدا بپرهیزید (و زیاده‌روی ننمایید)؛ و بدانید خدا با پرهیزگاران است.

پس اگر دشمن به جنگ سخت روی آورد شما هم مثل آنان با جنگ سخت دفاع کنید و اگر دشمن در جنگ به شیوه نرم عمل کرد ما هم باید با جنگ نرم به سراغ دشمن برویم. امام علی (ع) در نهی از آغازنمودن جنگ، به سربازان خویش در جنگ صفین فرمودند:

نجنگید (شروع به جنگ ننماید) تا این‌که ایشان جنگ با شما را آغاز نمایند و....). این سیره ائمه معصومین (ع) می‌باشد. اما اگر جنگ چه سخت چه نرم ضرورت پیدا کند باید محکم و استوار وارد عرصه میدان نبرد شد. حکیم ابوالقاسم فردوسی می‌گوید:

در بی نیازی به شمشیر جوی به کشور شود شاه را آبروی

سپه را چه باید ستاره شهر به شمشیر جویند مردان هنر

چون زمانی که ضرورت پیدا کرد باید با زبان شمشیر وارد شد

پس رمز پیروزی در جنگ مقابله به مثل می‌باشد و به این نکته باید توجه ویژه داشت امروز چون دشمن بیش‌تر در عرصه جنگ نرم و حوزه سایبری فعال است ما هم باید به همین شیوه اما تکنیک و تاکتیک‌های مخصوص به خودمان وارد شویم. باید بادرنگ، آهستگی و با بصیرت وارد عرصه نبرد شد.

همی رفت با رأی و هوش و درنگ که تیزی پشیمانی آرد به جنگ

مکن هیچ در جنگ شتاب ز می دور باشد و مپیمای خواب

به تندی مجوی ایچ رزم از نخست همی باش تا خسته گردد درست

و در جای دیگر فردوسی می‌گوید:

که دانا به هر کار سازد درنگ / سر اندر نیارد به پیکار تنگ

سبک تندی نماید نخست / به فرجام کار انده آرد درست

پس حتی در جنگ سایبری (cyber war) که ادامه پروژه مهار ایران و جلوه‌ای از مقابله و جنگ نرمی است که از سوی منتقدان مخالفان جمهوری اسلامی ایران حمایت و هدایت می‌شود. رمز غلبه بر دشمن، شناخت، هوش و بصیرت می‌باشد. ما هم باید در همین حوزه به‌روز و فعال شویم گرچه به برکت نظام مقدس جمهوری اسلامی ایران طبق گزارش مرکز تکنولیتیکس، ما چهارمین ارتش سایبری بزرگ دنیا را در اختیار داریم. سربازان عرصه نبرد سایبری ویروس‌ها، کرم‌ها، اسب‌های تروا، بمب‌های منطقی و درهای پشتی و... هستند. پیامدهای مرگ‌بار و ویران‌گر جنگ سایبری باعث شده است تا از این گونه نبرد به نام نبرد هزاره سوم نام برده شود. سایبری که از آن به عنوان جهان دوم یا زندگی دوم یاد می‌کنند، در همه حوزه‌های زندگی وارد شده است و به سرعت، فرهنگ زندگی انسان‌ها را دستخوش تغییر قرار داده است. جمهوری اسلامی باید در مقابل تز جنگ نرم و سایبری آنتی‌تزهای مناسب را انتخاب کند تا از این طریق بتواند فرهنگ ایرانی اسلامی خود را در برابر تهاجم غرب حفظ کند.

رمز موفقیت جمهوری اسلامی، هوشیاری کامل در جنگ نرم می‌باشد. حماسه‌ساز ایران، حکیم فردوسی می‌گوید: جنگ‌جویان باید از بزم و آسایش در هنگام جنگ برحذر بوده و همواره در

حال آماده‌باش و هوشیاری کامل به سر برند و در هنگام خستگی دشمن، با استفاده از اصل غافل‌گیری بر دشمن حمله برند:

به جنگ آنگهی شد که دشمن ز جنگ/ بپرهیزد وسست گرددش چنگ
شما سر به آسایش و خوابگاه / سپردید و دشمن به رنج و به راه
تن آسان غم و رنج بار آورد / چو رنج آوری گنج بار آورد
چه گویم که روزی تن آسان شویم / ز تیمار ایران هراسان شویم

هم او گوید:

نباید که ایمن شوی از کمین سپه باشد اندر در و دشت کین

هوشیاری در هنگام مقابله با دشمن و رعایت جوانب احتیاط برای حفظ خود و ضربه‌زدن به دشمن، ژرف‌نگری همراه با استقامت و شیردلی، موضوع دیگری است که فردوسی در آیین نظامی جنگ به آن پرداخته است.

چو رزم آیدت پیش هوشیار باش تنت را ز دشمن نگهدار باش
چو بد خواه پیش تو صف بر کشید تو را رای و آرام باید گزید

هم‌چنین، دکتر شفیعی کدکنی که یکی از متعهدترین شاعران معاصر ماست [۱۵-۱۴] در شعر آیینه‌ای برای صداها، باغ را رمزی از جامعه خود می‌داند که در یأس و نامیدی به سر می‌برد و به علت نابسامانی‌های اجتماعی هیچ‌گاه خوشایند شاعر نیست.

باغ از نفس‌های گل و از بوی باران بیدار شد چشمان ز خواب ناز برداشت

بخوان به نام گل سرخ، در صحاری شب که باغ ها همه بیدار و بارور گردند.

و در شعر هزاره دوم آهوی کوهی گوید [۱۵]:
همه باغ در خموشی ست / نه آب جنبد این‌جا / و نه برگ و نه شکوفه / چه بهار و باغ باشد ؟
و یا دریا در شعر او رمزی می شود از مردم و جامعه خشمگین و توفنده.
همیشه دریا دریاست / همیشه دریا طوفان دارد. (آیینه‌ای برای صداها: ۲۹۸)
و گاه رمز جامعه می‌شود که هستی آن در گروه پرواز شهیدانش است:
می‌خواهم از نسیم بپرسم: / بی جزر و مد قلب شما / آه ، / دریا چگونه می تپد امروز ؟/
ای مرغ های طوفان! پروازتان بلند (همان :۳۰۴)

و یا حافظ شیرازی که از او به عنوان یک مصلح اجتماعی نام می‌بریم با همین شیوه جنگ نرم با استفاده از واژه‌ها و اشعارش با جنگ به حاکمان زمان خود می روند. حافظ محتسب را رمزی از انسان‌های ریاکار و مستبد می‌داند و دکتر شفیعی کدکنی هم به همین صورت از آن یاد می‌کند که این‌ها به عنوان نمونه بود.

۶- چند نمونه از رمزهای دشمن در جنگ نرم طی سال‌های اخیر

انتخابات سال ۱۳۸۸، جریان انحرافی و انقلاب رنگی از جمله رمزهای دشمن در جنگ نرم است که در ادامه به توضیح آنها خواهیم پرداخت.

۶-۱- انتخابات سال ۱۳۸۸

یکی از مهم‌ترین جنگ‌های نرم در سال‌های اخیر علیه نظام اسلامی، انتخابات سال ۱۳۸۸ بود که هنوز هم خوب رمزگشایی نشده است. در آن سال، دشمن هم در حوزه نرم‌افزار و هم در حوزه سخت‌افزاری سرمایه‌گذاری کرده است. از شبکه‌های ماهواره‌ای و فضای مجازی و شبکه‌های اجتماعی گرفته تا فن‌آوری دیجیتال استفاده کرده است.

لازم به ذکر است در چند سال دیگر، سونامی دیجیتالی اتفاق خواهد افتاد. در همان سال صدا و سیما از رسانه‌های معارض عقب افتاد چرا که نتوانستیم از رسانه خوب استفاده کنیم و تهدیدات نرم را کنترل و مهار کنیم و رصد و پیش‌بینی لازم انجام شود و از موفقیت دشمن پیشگیری کنیم. رسانه‌های ما نتوانستند کارکردهای خود را خوب انجام دهند. به طور مثال، دشمن در رسانه خود آخرین روش را به کار گرفت و این‌که چگونه با نمایش راست گویی دروغ بگوید. رسانه ها در جهان آن‌قدر مهم‌اند که آقای پتروس غالی می‌گوید:

CNN، عضو شانزدهم شورای امنیت است. در جریان حمله آمریکا به عراق خودشان گفتند: CNN عراق را اشغال کرد.

در آن سال، رمز استکبار در انتخابات "تقلب" بود. صحنه‌گردانان با رمز تقلب، فتنه را کلید زدند و دشمن موفق شد در آن سال اعتماد بخشی از مردم را خدشه‌دار کند و به وحدت ملی و انسجام اسلامی آسیب جدی وارد سازد. اما رمز جمهوری اسلامی شکست دشمنان، بصیرت افزایی، عنایات خاص الهی و قاطعیت و تدابیر دلسوزانه مقام معظم رهبری بود.

به قول حضرت حافظ :

حالی درون پرده بسی فتنه می رود تا آن زمان که پرده برافتد چه‌ها کنند

در آن فضای غبارآلود آن سال، شاعران متعهد احساس تکلیف کردند و در راستای پاسداری از ولایت به میدان آمدند و به روشن‌گری پرداختند. چرا که رهبری تکلیف را مشخص کرده بودند: ((گاهی سکوت، کنارکشیدن، حرف نزدن، خودش کمک به

فتنه است. در فتنه همه بایستی روشن‌گری کنند.))

۶-۲- جریان انحرافی

جریان موسوم به جریان انحرافی که قصد تقابل پنهان با ارکان نظام و مرجعیت در سال‌های اخیر را داشت با رمز شبه ناسیونالیسم با ستم‌گرایانه وارد عرصه سیاست، فرهنگ و حکومت شد تا از طریق باستان‌گرایی بتوانند به اهداف خود برسند. باستان‌گرایی رمز آنان بود که با تدبیر مقام معظم رهبری و بصیرت مردم و نخبگان سرکوب شد. باستان‌گرایی دارای مبانی و معانی متفاوتی است که در عین گرایش به ایران باستان، در انگیزه‌ها متفاوتند.

به طور مثال، باستان‌گرایی در شعر عصر مشروطه عبارت بود از احیای هویت ملی، خوش‌بینی افراطی به ایران باستان، اسلام ستیزی، انتقاد از اوضاع و اموال عصر، تحریک غرور ملی و شکست‌ناپذیری.

به عنوان نمونه، ملک الشعرای بهار در دیوانش می‌گوید:

هان ای ایرانیان! ایران اندر بلاست / مملکت داریوش دستخوش نیکلاست

مرکز ملک کیان در دهن اژدهاست / غیرت اسلام کوا جنبش ملی کجاست

برادران رشید! این همه سستی چراست/ایران مال شماست، ایران مال شماست

در همین عصر مشروطه میرزا فتحعلی آخوند زاده، میرزا آقاخان کرمانی، جلال الدین میرزا قاجار، اسلام را علت اصلی انحطاط ایران قلمداد کرده‌اند و راه نجات را بازگشت به ایران باستان می‌دانستند. به هر حال در دوره‌های مختلف انگیزه متفاوت می‌شوند. جریان انحرافی در حوزه اقتصادی با بزرگ‌نمایی نیازهای روزمره توده‌های مردم، عدالت توزیعی، مقابله با مفاسد اقتصادی و معرفی خود به عنوان منجی و در حوزه فرهنگ با حرکت در چارچوب عرفان‌های کاذب تکیه بر ادبیات اومانیستی، اتخاذ سیاست‌های تساهل و تسامح و سرمایه‌گذاری در پروژه‌های فرهنگی عامه‌پسند و در حوزه سیاسی با تاکید ظاهری بر تداوم روحیه استکبارستیزی و اسطوره‌سازی و مظلوم‌نمایی وارد عرصه شد که حرکت‌های آنان تا حدی مهار شد.

۶-۳- انقلاب رنگی گزینه تغییر رژیم در ایران

مایکل لدین، نومحافظه کار مشهور دستگاه بوش زمانی در مورد ایران گفته بود: بیست میلیون دلار به من بدهید تا انقلابی را که می‌خواهید راه بیندازیم! این انقلابی بیست میلیون دلاری در مقاله‌ای تحت عنوان "سریع‌تر لطفا!" با رمز طرح ملی رفراندوم پیشنهادی از داخل ایران مطرح شد که به طرح پیشنهادی رفراندوم (شصت میلیون دات کام) اشاره می‌کنند. همین طرح علیه چاوز در ونزویلا و انقلاب گل سرخ در گرجستان انجام شد. اما پشتوانه مردمی جمهوری اسلامی، رهبری فرهیخته و محبوب و فقدان وحدت در همراهان داخلی، موجب شکست آنان شده است.

از دیگر رمزهای دشمن که باید رمزگشایی شود، ایران‌هراسی، حقوق بشر، نفوذ، هسته‌ای و ... می‌باشد که در این مجال نمی‌گنجد. روحیه انقلابی و جهادی اوایل انقلاب، اقدام به هنگام و به موقع، حضور فعال در فضای مجازی و تهیه مطالب و محتوی تاثیرگذار و اقناعی، رصد و پیش‌بینی فعالیت‌های دشمن، وحدت و انسجام ملی و تقویت فرهنگ ایرانی اسلامی رمز موفقیت در جنگ نرم می‌باشددکه در ادبیات پایداری و مقاومت بازتاب خوبی داشته باشد.

۷- نتیجه گیری

حاصل سخن این‌که، رمز به عنوان یکی از مهم‌ترین موضوعات در ادبیات فارسی با کارکردهای متفاوت مورد نظر دشمنان در جنک نرم قرار گرفت. با توجه به این‌که یکی از ویژگی جنگ نرم نمادساز بودن و پنهانی و سری بودن می‌باشد، دشمن از طریق رمز و رمزگرایی حتی در حوزه سایبری توانست تا حدودی در انجام و مشارکت اجتماعی و تضعیف و تغییر باورها و اعتقادات با ابزارهای نوین خدشه‌ای وارد کند که نمونه آن را در درون نظام یعنی انتخابات سال ۸۸ و جریان انحرافی را به خوبی ببینیم، اما اگر درایت و بصیرت‌افزایی مقام معظم رهبری و روحیه انقلابی و جهادی نبود، نظام به کدام سمت رفته بود؟ که شاعران و نویسندگان هم به آن اشاره کرده‌اند.

۸- مراجع

[1] Quran, Al Omran:41

[2] T. Poornamdaran, “Codes and codic stories in Persian literature (an analysis of mystical stories, philosophical Ibn Sina and Suhrawardi).”, Scientific and Cultural, Secound edition, In Persion

[3] J. Satari, “Coding in psychoanalysis”, Toos, 1987, in persion.

[4] S. Shamisa, “Expression”, Ferdos, 1992, in persion.

[5] J. Satari, “Entrance to the mystical cryptology“, markaz, 1993, in persion.

[6] Hafez, "Divan-e Hafez.", Kharazmi, in persion.

[7] E. Satarzaaddeh, “Great comment on Masnavi”, Zarin, 1995, in persion.

[8] Sh. Araghi, ”Koliyat”, Sokhan, 2009, in persion.

[9] M.R. Nasresfahani, H. Hatami, “Mystical and mythological literature”, shiraz university, in persion.

[10] D. syaghi, “ferdowsi”, 2001, in persion.

[11] A. H. sharifi, "Soft war", Imam Khomeini Educational and Research Institute, 2010, in persion.
[12] A. Naeeini, "Principles of Soft War", Saghi, 2012, in persion.
[13] R. Seyedhassani, "World Literary research", Neghah, 1997, in persion.
[14] M. R. Shafiee KadKani, " A mirror for the sounds", Sokan, 2000, in persion.
[15] M. R. Shafiee KadKani, "Second millennium deer",Online: www.ensani.ir/storage/Files/20140624144158-9726-40.pdf, 2002, in persion,

مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"
ویژه‌نامه کنفرانس بین‌المللی ترکیبیات، رمزنگاری و محاسبات، ص ۱۰۲ -۹۹

بهبود روش تطبیق بخش توسط کد زنجیره ای در الگویابی هواپیما

محمّد سعید علمداری[1*]، محسن شاهرضایی[2]

۱- کارشناس ارشد، استادیار، دانشگاه جامع امام حسین (ع)

(دریافت: ۹۵/۰۷/۰۵، پذیرش: ۹۶/۰۳/۰۶)

چکیده

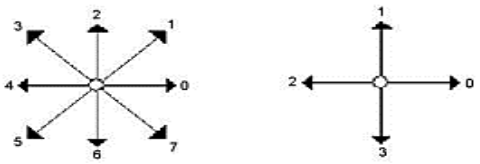
در این مقاله شناسایی الگو بر اساس روش فوریه و روش تطبیق بخش، انجام شده است که در آن ابتدا محیط مرزی هواپیما به چندین قسمت کوچک تجزیه می گردد و سپس مسیر بهینه ممکن شناسایی می شود که نتایج حاصل بر اساس مقایسه میان روش مفسر فوریه و روش تطبیق بخش مورد بررسی قرار گرفته اند.

واژه‌های کلیدی: کد زنجیره‌ای، جدول فاصله، کانتور، مفسر فوریه، مسیر کوتاه‌ترین فاصله، تبدیل فوریه گسسته.

۱- مقدمه

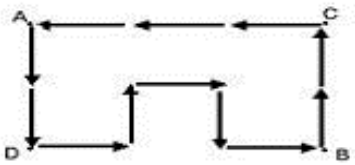
ابتدا به معرفی کد زنجیره ای [۱ و ۲] می‌پردازیم. کد زنجیره ای برگرفته از محیط مرزی یک جسم، شامل زنجیره بهم پیوسته ای از پاره خط هایی با طول و جهت مشخصی می باشند.

بر اساس تعداد جهت های مختلف این پاره خط ها کد زنجیره ای نوع ۴ تایی و نوع ۸ تایی تعریف می شود، شکل (۱) این دو نوع کد زنجیره ای را نمایش می دهد.



شکل (۱): کد زنجیره نوع چهارتایی (سمت راست) و کد زنجیره نوع هشت‌تایی (سمت چپ)

همانطور که مشاهده می شود، هر جهت با یک عدد بصورت یک کد مشخص شده است، به عنوان مثال ۳۳۰۱۰۳۰۱۱۲۲۲ کد زنجیره ای نوع ۴ تایی شکل (۲) می باشد که متناظر با نقطه شروع A می باشد.



شکل (۲): کدزنجیره‌ای نوع چهارتایی با توجه به نقطه شروع A

برای شروع کار، یک نقطه دلخواه بر روی مرز شکل انتخاب نموده و بر اساس کد زنجیره ۸ تایی در خلاف جهت عقربه های ساعت با توجه به جهت نسبی نقطه بعد نسبت به نقطه قبل، کدها را بدست می آوریم.

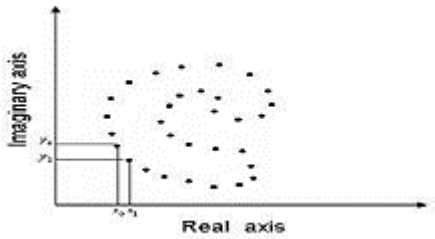
سپس این کد را به صورتی که نقطه شروع زنجیره بر روی مبدا مختصات قرار گیرد تنظیم می کنیم و سپس انتهای هر اتصال زنجیره را با یک نقطه مشخص کرده و با دنبال کردن کد زنجیره ای، مرز شکل بصورت مجموعه ای از نقاط بدست می آید.

برای تقسیم بندی شکل، ابتدا آن را به دو نیمه تقسیم کرده و با در نظر گرفتن یک نیمه، نقطه ای که از محیط دور ترین فاصله را دارد، تعیین می کنیم و با اتصال این نقطه به دو نقطه قبلی، هر نیمه به دو قسمت تقسیم شده و چهار ربع بدست می آید و با ادامه این کار سایر نقاط بدست می آید که همگی رئوس یک چند ضلعی می باشند.

پس از تکمیل چند ضلعی، نوبت به جدا کردن آن می رسد که با بکاربردن سری فوریه [۳، ۴ و ۵] و توسط ضرایب فوریه چند ضلعی را به بخش های مختلف تقسیم بندی کرده و در هر بخش ضریب فوریه [۶ و ۷] محاسبه می گردد.

برای تعریف سری فوریه، محیط مرزی که توسط N نقطه گسسته در دستگاه مختصات مطابق شکل (۳) نمایش داده شده است را در نظر بگیرید.

* رایانامه نویسنده مسئول: m.s.alamdari69@gmail.com



شکل (۳): نمایش یک منحنی به صورت نقاط گسسته

ابتدا نقطه شروع دلخواهی مانند (X,Y) را انتخاب می کنیم و از این نقطه درخلاف جهت عقربه ساعت محیط را می پیماییم تا مختصات نقاط دیگر بدست آیند که این مجموعه بصورت زیر نمایش داده می شود:

$$S(k) = (x_k, y_k) \quad s.t \quad k = 0,1,2, \dots, N-1$$

سپس هر نقطه بصورت یک عدد مختلط به صورت زیر تعریف می شود:

$$S(k) = x_k + \mathrm{j}\, y_k \quad s.t \quad k = 0,1,2, \dots, N-1$$

به این ترتیب محور x را محور حقیقی و محور y را محور موهومی فرض می کنیم که این کار موجب می شود تا مساله از حالت دوبعدی به حالت یک بعدی تبدیل گردد و سپس تبدیل فوریه گسسته برای تابع S(k) بصورت زیر تعریف می شود که ضرایب مختلط a(u) را اصطلاحاً ضرایب فوریه می نامند.

$$a(u) = \frac{1}{N} \sum_{k=0}^{k=N-1} S(k) \exp\left(\frac{-j2\pi uk}{N}\right) \quad s.t \quad u = 0,1,2, \dots, n-1$$

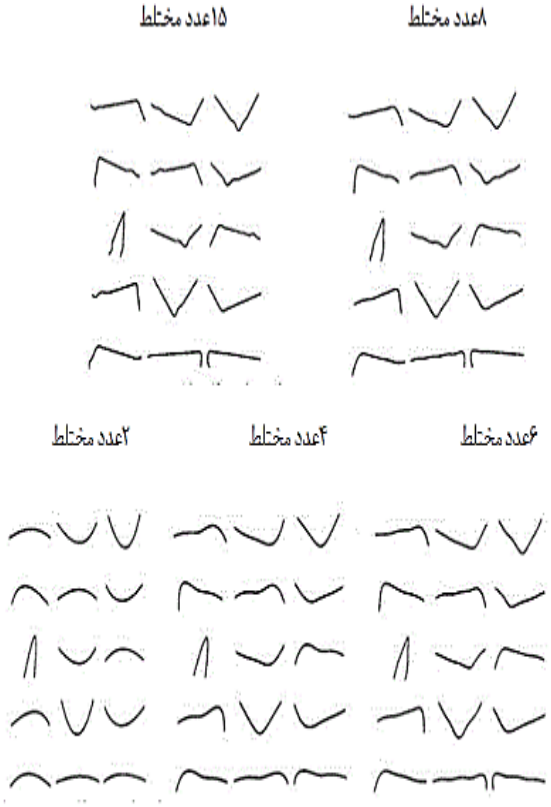
۲- به‌دست‌آوردن ضرایب فوریه

ضرایب فوریه بر اساس فرمول زیر محاسبه می شوند:
$t_P = \sum_{i=1}^{P} \Delta t_i$ و $t_0 = 0$ که k تعداد دوره کد زنجیره بوده و برابر با تناوب کانتورمی باشد، $\Delta\gamma_p, \Delta t_p$ از جدول (۱) متناسب با مولفه های کد زنجیره ای بدست می آیند:

جدول (۱): محاسبه مقادیر $\Delta\gamma_p, \Delta t_p$ بر اساس کدزنجیره‌ای

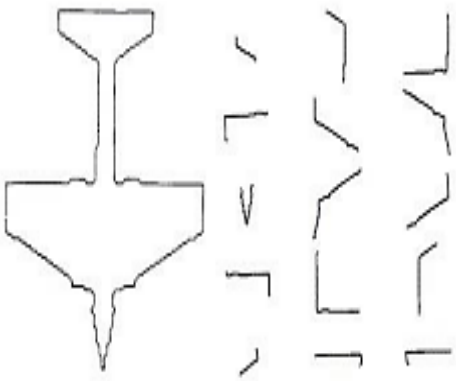
α_P	0	1	2	3	4	5	6	7
$\Delta\gamma_P$	1	1+i	i	-1+i	-1	-1-i	-i	1-i
Δt_P	1	$\sqrt{2}$	1	$\sqrt{2}$	1	$\sqrt{2}$	1	$\sqrt{2}$

درشکل(۴)، پاره‌منحنی‌هایی که از سری فوریه به دست آمده‌اند، برحسب تعداد اعداد مختلط به کار رفته، نمایش داده شده‌اند.



شکل (۴): تشکیل پاره‌منحنی‌ها براساس اعداد مختلط

به عنوان مثال، در شکل (۵)، هر زیرمجموعه از سه راس تشکیل شده است.



شکل (۵): تشکیل پاره‌منحنی‌ها براساس اعداد مختلط

حال فرض می‌کنیم X(i) و Y(i) تبدیل فوریه دو پاره‌منحنی باشند که در آن، i = -N,…,-1,0,1,…,N در این صورت فاصله دو منحنی را به صورت زیر تعریف می‌کنیم:

$$d^2 = \sum_{i=-N}^{i=N} |X(i) - Y(i)|^2$$

هنگامی که دو کانتور مقایسه می‌شوند لازم است کـه فاصـله بین هر بخش از کانتورها را بررسی نماییم که این کار بـا جـدول فاصله انجام می‌شود. شکل (۶) نشان‌دهنده جدول فاصـله در اثـر مقایسه بین بخش‌های شکل (۵) می‌باشد و مقادیر صفر روی قطر اصلی نشانگر تطابق بخش‌هاست و سایر درایه‌های غیرصفر نشانگر عدم تطابق بخش‌هاسـت. قسـمت‌هـایی از جـدول کـه بـا دایـره مشخص شده‌اند، مشخص‌کننده بهترین تطابق مجموعه کانتورهـا می‌باشد و به آن مسیر کوتاه‌ترین فاصله گویند.

0.	7.13	10.03	5.94	1.11	6.22	16.09	6.40	4.03	2.45	10.32	6.64	4.21	1.53	4.19
7.13	0.	4.68	9.31	7.21	3.80	18.80	1.73	7.26	8.35	5.32	4.04	7.66	6.46	6.98
10.03	4.68	0.	11.51	9.78	4.71	18.61	4.43	9.95	10.82	1.18	5.48	10.62	9.82	10.06
5.94	9.31	11.51	0.	5.44	8.44	14.20	8.24	2.62	6.34	11.86	9.23	2.78	6.50	4.02
1.11	7.21	9.78	5.44	0.	6.10	15.17	6.30	3.63	1.95	10.08	6.77	4.05	2.25	4.21
6.22	3.80	4.71	8.44	6.10	0.	17.51	2.96	6.69	7.46	4.68	1.91	7.23	6.19	6.45
16.09	18.80	18.61	14.20	15.17	17.51	0.	17.37	15.12	14.45	19.01	19.14	15.79	17.03	17.05
6.40	1.73	4.43	8.24	6.30	2.96	17.37	0.	6.27	7.54	5.07	3.91	6.81	6.04	6.34
4.03	7.26	9.95	2.62	3.63	6.69	15.12	6.27	0.	4.90	10.34	7.47	1.09	4.36	2.38
2.45	8.35	10.82	6.34	1.95	7.46	14.45	7.54	4.90	0.	11.16	8.18	5.30	3.24	5.67
10.32	5.32	1.18	11.86	10.08	4.68	19.01	5.07	10.34	11.16	0.	5.29	11.00	10.17	10.33
6.64	4.04	5.48	9.23	6.77	1.91	19.14	3.91	7.47	8.18	5.29	0.	7.81	6.42	6.65
4.21	7.66	10.62	2.78	4.05	7.23	15.79	6.81	1.09	5.30	11.00	7.81	0.	4.48	2.02
1.53	6.46	9.82	6.50	2.25	6.19	17.03	6.04	4.36	3.24	10.17	6.42	4.48	0.	4.20
4.19	6.98	10.06	4.02	4.21	6.45	17.05	6.34	2.38	5.67	10.33	6.65	2.02	4.20	0.

شکل (۶): جدول فاصله مقایسه پاره‌منحنی‌های شکل (۵)

۳- روش برنامه‌ریزی پویا

برای شروع فرموله‌کردن روش تطبیـق بخـش بـه عنـوان مسـئله مسیر کوتاه‌ترین فاصله، خاصیت‌های مورد نیاز مسیر مطلوب باید تعریف شده باشند که برای تعریف آن‌هـا، بـه صـورت زیـر عمـل می‌نماییم.

فرض کنید کانتور ناشـناخته ای M بخـش دارد کـه توسـط ستون های جدول فاصله نشان داده می شـود و کـانتور شـناخته شده ای N بخش دارد که توسط سطرهای جـدول فاصـله نشـان داده می شود.

درایه iامین سطر و jامین ستون از جدول فاصله، متناظر بـا بخش iام کانتور شناخته شده و بخش jام کانتور ناشناخته است که در آن، $i=1,2,\ldots,N$ و $j=1,2,\ldots,M$ می‌باشند.

معیار برای مسیر کامل این است که مسیر باید با اسـتفاده از تمام M بخش کانتور ناشناخه، ساخته شود یعنی مسیر بـا اولـین ستون از جدول فاصله شروع و با آخرین ستون تمام گردد.

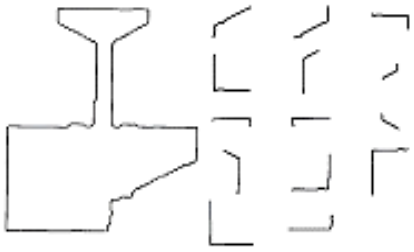
از آن جایی‌که در حـال بررسـی اشـکال جزئـی و بـه دنبـال تطبیق کانتور ناشناخته با کانتور شـناخته‌شـده هسـتیم، تعـداد بخش‌های کانتور شناخته‌شده کم‌تر یا برابر با تعـداد بخـش‌هـای کانتور ناشناخته خواهد بود لـذا بایـد تمـام بخـش‌هـای کـانتور شناخته‌شده را مورد بررسی قرار دهیم.

گام بعدی در شرح مسیر مـورد نظـر ایـن اسـت کـه جهـت حرکـت قـانونی را از طریـق جـدول فاصـله مشـخص کنـیم و حرکت‌کردن از طریق جدول در مسیرهای ممکن تنها بـه سـمت پایین و به سمت راست خواهد بود.

برای توصیف فرمول بنـدی برنامـه نویسـی پویـا [۸]، فـرض کنیـد $d(i,j)$ نشـان دهنـده ورودی سـطر i ام و سـتون j ام درجدول فاصله باشد، همچنین فرض کنیـد $D(i,j)$ کـل فاصـله روی مسیر کوتاهترین فاصله از (i,j) امین ورودی از جدول فاصله است که مقدار آن در هر نقطه بصورت زیر، مورد برآورد قرار مـی گیرد.

$$D(i,j) = min\begin{cases} d(i+1,j+1) + D(i+1,j+1) \\ d(i+1,j) + D(i+1,j) \\ d(i,j+1) + D(i,j+1) \end{cases}$$

شـکل (۷) کـه تغییریافتـه شـکل (۵) مـی‌باشـد را در نظـر می‌گیریم:



شکل (۷): محیط مرزی تخریب شده و بخش‌های مختلف آن

به عنوان مثال، جدول فاصله در شکل (۸) که در اثر مقایسـه بخش‌های نشان داده شده در اشکال (۵ و ۷) حاصل شده است را ملاحضه کنید.

5.35	4.03	2.45	10.32	6.64	4.21	1.53	4.19	0.	7.13	10.03	6.89	7.29	4.95
2.62	7.26	8.35	5.32	4.04	7.66	6.46	6.98	7.13	0.	4.68	11.91	12.21	8.34
6.08	9.95	10.82	1.18	5.48	10.62	9.82	10.06	10.03	4.68	0.	13.88	14.13	10.89
7.36	2.62	6.34	11.86	9.23	2.78	6.50	4.02	5.94	9.31	11.51	6.04	6.68	1.55
5.34	3.63	1.95	10.08	6.77	4.05	2.25	4.21	1.11	7.21	9.78	6.24	6.65	4.61
3.56	6.69	7.46	4.68	1.91	7.23	6.19	6.45	6.22	3.80	4.71	10.71	10.97	7.52
17.00	15.12	14.45	19.01	19.14	15.79	17.03	17.05	16.09	18.80	18.61	10.45	10.42	15.29
2.08	6.27	7.54	5.07	3.91	6.81	6.04	6.34	6.40	1.73	4.43	10.65	10.91	7.38
5.24	0.	4.90	10.34	7.47	1.09	4.36	2.38	4.03	7.26	9.95	6.36	6.36	1.65
6.47	4.90	0.	11.16	8.18	5.30	3.24	5.67	2.45	8.35	10.82	5.79	6.40	5.80
6.62	10.34	11.16	0.	5.29	11.00	10.17	10.33	10.32	5.32	1.18	14.27	14.52	11.20
4.33	7.47	8.18	5.29	0.	7.81	6.42	6.65	6.64	4.04	5.48	11.87	12.13	8.13
5.65	1.09	5.30	11.00	7.81	0.	4.48	2.02	4.21	7.66	10.62	6.66	6.62	1.51
4.88	4.36	3.24	10.17	6.42	4.48	0.	4.20	1.53	6.46	9.82	7.89	8.29	5.39
5.29	2.38	5.67	10.33	6.65	2.02	4.20	0.	4.19	6.98	10.06	8.02	8.05	2.53

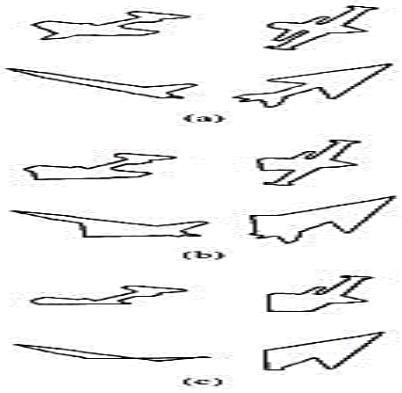
شکل (۸): جدول فاصله مقایسه پاره‌منحنی‌های اشکال (۵ و ۷)

شماره سطرهای این جدول متناظر با شماره کانتورهای شکل (۵) و شماره ستون‌ها متنـاظر بـا شـماره کانتورهـای شـکل (۷) می‌باشد، ملاحضه می‌شود که هرچه فاصله دو کانتور کم‌تر باشـد تطابق بیش‌تر است.

۴- آزمایش شناسایی شکل جزئی نتیجه‌گیری

برای آزمایش شناسایی شکل جزئی، مشابه داده‌های مورد استفاده توسط Dudani [۹و۱۰] کتابخانه با ۱۴۳ نمایش از شش کلاس هواپیما مورد استفاده قرار گرفت و برای هر کلاس از هواپیما ۵۰ نمایش ناشناخته در نظر گرفته شد و دو نوع کانتورهای شناخته‌شده و ناشناخته در رزولوشن تصویر ۱۲۸×۱۲۸ تولید شد.

برای ایجاد اشکال جزئی، کانتورهای ناشناخته به صورت ۱۰٪، ۲۰٪، ۳۰٪، ۴۰٪ و ۵۰٪ قطعه قطعه شده‌اند. برخی از کانتورهای نمونه در شکل (۹) نشان داده شده‌اند که قسمت a نشان‌گر چهار هواپیمای مختلف است که جهت‌گیری‌هایی متفاوتی دارند و قسمت b و c نشان‌گر کانتورهایی هستند که به ترتیب ۲۰٪ و ۴۰٪ قطعه قطعه شده‌اند.



شکل (۹): نمونه کانتور ناشناخته

۵- نتیجه‌گیری

شناسایی الگو بر اساس روش فوریه و روش تطبیق بخش صورت پذیرفت که در ابتدا محیط مرزی هواپیما به چندین قسمت کوچک تجزیه و سپس مسیر بهینه ممکن شناسایی شد.

جدول (۲) نشان‌گر مقایسه عملکرد روش تطبیق بخش با روش استفاده شده در توصیف‌گر فوریه است که با توجه به اطلاعات جدول مشخص می‌شود عملکرد روش تطبیق بخش برای کانتور قطعه قطعه‌شده نسبت به روشی که کل مرز را استفاده می‌کند تا حد زیادی بهبود یافته است زیرا هر چقدر ٪ کانتور افزایش می یابد، در روش فوریه طبقه بندی صحیح با کاهش چشم گیری مواجه می شود.

جدول (۲): بررسی طبقه‌بندی روش تطبیق بخش و روش فوریه

٪ کانتور	روش تطبیق بخش	روش فوریه
۰	۹۳/۰۰	۹۲/۰۰
۱۰	۵۸/۳۳	۸۳/۶۷
۲۰	۷۵/۰۰	۵۸/۰۰
۳۰	۷۱/۶۷	۳۰/۳۳
۴۰	۶۴/۶۷	۲۲/۰۰
۵۰	۵۱/۶۷	۱۲/۶۷

۶- مراجع

[1] F.Verdoja and M.Grangetto, "Efficient Representation of Segmentation Contours Using Chain Codes," IEEE International Conference on Acoustics Speech and Signal Processing(ICASSP), pp.1462-1466, 2017

[2] L. Daeha and K. Soon, "Chain code based object recognition,"IET Journals and Magazines, vol. 51, pp. 1996-1997, 2015.

[3] P.Wang and V.Patel, "Extracting Fourier Descriptors from Compressive Measurements," IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 4755-4759, 2017.

[4] J.Yang and Z.Lu, "A Shape Representation Based on Fourier Descriptors," 12th International Conference on Computational Intelligence and Security (CIS), pp 507-510, 2016.

[5] F.Timm, and T.Martinetz, "Statistical Fourier Descriptors for Defect Image Classification," Pattern Recognition ICPR, 20th International Conference, pp. 4190-4193, 2010.

[6] E.Sokic and S.Konjicija , "Area Function Fourier Descriptors Based on Contour," IEEE International Conference on Multimedia and Expo (ICME), pp 1-6, 2015.

[7] Z.Zhang, and M.Yang, "Area Function Fourier Descriptors Based on Contour," Communication Technology ICCT, IEEE 13th International Conference, pp 823-826, 2011.

[8] J.Ke,T.Bednarz and A.Sowmya, "Optimized GPU implementation for dynamic programming in image data processing,"IEEE 35th International Performance Computing and Communications Conference (IPCCC), pp 1-7, 2016.

[9] Z.Fang, G.Yao, S.Dudani, and K.Breeding, "Target Recognition of Aircraft Based on Moment Invariants," lEEE Transactions Computer, pp 1-5, 2012.

[10] M.Shahrezaei, and M.S.Alamdari, "The application of numerical analysis techniques to pattern recognition of helicopters by area method," Journal of Science Kharazmi University, vol. 17, pp. 1-2, 2016.

مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"
ویژه‌نامه کنفرانس بین‌المللی ترکیبیات، رمزنگاری و محاسبات، ص ۱۱۰ -۱۰۳

کاربرد چندجمله‌ای های برنولی در حل معادلات انتگرال– دیفرانسیل کسری

کبری ربیعی[۱]، یداله اردوخانی[۲*]

۱- دانشجوی دکتری دانشکده علوم ریاضی، دانشگاه الزهرا (س) ۲- استاد دانشکده علوم ریاضی، دانشگاه الزهرا (س)

(دریافت: ۹۵/۰۷/۰۵، پذیرش: ۹۶/۰۳/۰۶)

چکیده

در این مقاله، ماتریس عملیاتی انتگرال کسری ریمان- لیوویل برای چندجمله‌ای‌های برنولی معرفی می شود. سپس به کمک این ماتریس عملیاتی انتگرال، خواص دیگر چندجمله‌ای‌های برنولی و روش کم‌ترین مربعات، معادلات انتگرال -دیفرانسیل فردهلم - ولترای کسری به یک دستگاه جبری غیرخطی تبدیل می‌شود. روش استفاده‌شده برای حل این دستگاه، روش تکراری نیوتن می‌باشد. در ادامه، هم‌گرایی روش در حل معادلات مذکور بررسی شده و با ارائه نتایج عددی، دقت و کارایی روش مورد ارزیابی قرار می‌گیرد.

واژه‌های کلیدی: چندجمله‌ای‌های برنولی، ماتریس عملیاتی، تجزیه و تحلیل هم‌گرایی، معادلات انتگرال- دیفرانسیل کسری، تقریب کم-ترین مربعات.

۱- مقدمه

ایده اولیه حسابان از مرتبه کسری در سال ۱۶۹۵ طی نامه‌ای از هوپیتال[۱] به لایپ نیتز[۲] شکل گرفت و در آن، هوپیتال این‌گونه مطرح کرد که اگر در مشتق nام تابعی نسبت به متغیرش $n=\frac{1}{2}$ فرض شود، $\frac{d^n}{dx^n}$ چه مفهومی خواهد داشت؟ پس از این نقطه آغاز، مطالعاتی در این زمینه توسط دانشمندانی انجام شد و کتاب‌های جامعی توسط نویسندگان مختلف در این زمینه به چاپ رسید که یکی از مهم‌ترین منابع در این زمینه که به کاربردهای حسابان از مرتبه کسری می پردازد، در مرجع [۱] معرفی می‌شود. از آن‌جایی‌که مدل‌بندی بسیاری از پدیده‌های فیزیکی در حوزه وسیعی از علوم، نظیر پزشکی [۲]، اقتصاد [۳]، لرزه‌نگاری [۴] و ... منجر به تشکیل معادلات دیفرانسیل کسری می‌شود، اخیراً بررسی این معادلات توجه بسیاری از محققین را به خود جلب کرده است. علاوه بر این، پیداکردن حل تحلیلی و جواب دقیق برای این معادلات دیفرانسیل کسری به طور معمول پیچیده است، بنابراین، یافتن روش‌های عددی برای حل این معادلات از اهمیت ویژه‌ای برخوردار می‌باشد.

برای حل معادلات انتگرال-دیفرانسیل کسری روش‌های عددی گوناگونی به کار گرفته شده است. در مرجع [۵] روش تغییر پارامترها برای حل معادلات انتگرال- دیفرانسیل کسری به کار رفته است. روش تجزیه آدومیان[۳] توسط نویسندگان [۷-۶] استفاده شده است، در [۸] روش هموتوپی بر روی معادله انتگرال- دیفرانسیلی مرتبه چهار پیاده شده است، در مرجع [۹] کارایی روش موجک سینوس کسینوسی در حل معادله کسری انتگرال- دیفرانسیل فردهلم[۴] نشان داده شده است. نویسندگان در مرجع [۱۰] روش بسط تیلور را برای حل این نوع معادلات به کار گرفته‌اند و هم‌چنین کارایی روش‌های هم محلی و تبدیل دیفرانسیلی کسری در مراجع [۱۳-۱۱] به ترتیب بحث شده است.

قابل ذکر است که تعاریف متعددی برای انتگرال و مشتق کسری وجود دارد که توجه این مقاله بر روی مشتق کسری کاپوچو[۵] و انتگرال کسری ریمان- لیوویل[۶] معطوف می باشد. در بخش دوم، تعاریف این عملگرها و دیگر پیش‌نیازهای این مقاله ارایه می‌شود. در بخش سوم، چندجمله‌ای‌های برنولی[۷] و ماتریس عملیاتی انتگرال ریمان- لیوویل این چندجمله‌ای‌ها بیان خواهد شد. تجزیه و تحلیل هم‌گرایی در بخش چهارم بحث خواهد شد. بخش پنجم به بیان روش به کار گرفته‌شده برای حل این معادلات در این مقاله می‌پردازد و در بخش ششم نتایج عددی گزارش می‌شود. بحث و نتیجه‌گیری اجمالی از کل مباحث پیش-رو در بخش هفتم آورده شده است.

* رایانامه نویسنده مسئول: ordokhani@alzahra..ac.ir

1- Hopital
2- Leibniz
3- Adomian
4- Fredholm
5- Caputo
6- Riemann-Liouville
7- Bernoulli

۲- تعاریف اولیه

در این بخش تعاریف مورد نیاز در قسمت‌های بعدی مقاله به طور خلاصه بیان می‌شود.

۲-۱- مشتق و انتگرال ریمان- لیوویل

فرض کنید $\Omega = [a,b]$ یک بازه متناهی بر محور اعداد حقیقی R باشد، انتگرال چپ و راست ریمان- لیوویل از مرتبه کسری $\gamma > 0,$ برای $x: [a,b] \to R$ به ترتیب به صورت زیر تعریف می‌شود [۱۴]:

$$ {}_a I_t^{\gamma} x(t) = \frac{1}{\Gamma(\gamma)} \int_a^t (t-\tau)^{\gamma-1} x(\tau) d\tau, \quad (۱)$$

$$ {}_t I_b^{\gamma} x(t) = \frac{1}{\Gamma(\gamma)} \int_t^b (\tau-t)^{\gamma-1} x(\tau) d\tau, \quad (۲)$$

که در آن، $\Gamma(\gamma)$ تابع گاما است.

در حالت خاص $\gamma = n \in N$ انتگرال‌های n گانه زیر به دست می‌آیند:

$$ {}_a I_t^n x(t) = \int_a^t d\tau_1 \int_a^{\tau_1} d\tau_2 \dots \int_a^{\tau_{n-1}} x(\tau) d\tau = \frac{1}{\Gamma(n)} \int_a^t (t-\tau)^{n-1} x(\tau) d\tau, \quad (۳)$$

$$ {}_t I_b^n x(t) = \int_\tau^b d\tau_1 \int_{\tau_1}^b d\tau_2 \dots \int_{\tau_{n-1}}^b x(\tau) d\tau = \frac{1}{\Gamma(n)} \int_t^b (\tau-t)^{n-1} x(\tau) d\tau. \quad (۴)$$

مشتق چپ و راست ریمان- لیوویل از مرتبه کسری $\gamma > 0,$ به ترتیب به صورت زیر تعریف می‌شوند:

$$ {}_a D_t^{\gamma} x(t) = \frac{d^n}{dt^n} {}_a I_t^{n-\gamma} x(t) = \frac{1}{(n-\gamma)} \frac{d^n}{dt^n} \int_a^t (t-\tau)^{n-\gamma-1} x(\tau) d\tau, \quad (۵)$$

$$ n = [\gamma] + 1, \qquad t > a,$$

$$ {}_t D_b^{\gamma} x(t) = (-1)^n \frac{d^n}{dt^n} {}_t I_b^{n-\gamma} x(t) = \frac{(-1)^n}{(n-\gamma)} \frac{d^n}{dt^n} \int_t^b (\tau-t)^{n-\gamma-1} x(\tau) d\tau, \quad (۶)$$

$$ n = [\gamma] + 1, \; t < b.$$

و در صورتی‌که $\gamma = n \in N,$ باشد، به ترتیب برابر با $x^n(t)$ و $(-1)^n x^n(t)$ خواهند شد.

۲-۲- مشتقات از مرتبه کسری کاپوچو

در این قسمت مشتق کسری کاپوچو چپ و راست را به صورت زیر تعریف می‌کنیم [۱۴]:

$$ ({}_a^C D_t^{\gamma} x)(t) = ({}_a D_t^{\gamma} [x(t) - \sum_{k=0}^{n-1} \frac{x^k(a)}{k!} (t-a)^k]), \quad (۷)$$

$$ ({}_t^C D_b^{\gamma} x)(t) = ({}_t D_b^{\gamma} [x(t) - \sum_{k=0}^{n-1} \frac{x^k(a)}{k!} (t-a)^k]), \quad (۸)$$

که درآن، $n = [\gamma]$ برابر با کوچک‌ترین عدد صحیح بزرگ‌تر از γ است. با توجه به تعاریف فوق واضح است که این مشتق برای توابعی که دارای مشتق کسری ریمان- لیوویل باشند، قابل تعریف می‌باشد و می‌توان عبارات معادل این تعریف را به شکل زیر در نظر گرفت.

$$ {}_a^C D_t^{\gamma} x(t) = \frac{1}{\Gamma(n-\gamma)} \int_a^t (t-\tau)^{n-\gamma-1} x^{(n)}(\tau) d\tau = {}_a I_t^{n-\gamma} D^n x(t), \; n = [\gamma]+1, \; t > a, \quad (۹)$$

$$ {}_t^C D_b^{\gamma} x(t) = \frac{(-1)^n}{\Gamma(n-\gamma)} \int_t^b (t-\tau)^{n-\gamma-1} x^{(n)}(\tau) d\tau = (-1)^n \; {}_t I_b^{n-\gamma} D^n x(t), \; n = [\gamma]+1 \quad t < b. \quad (۱۰)$$

در مورد مشتقات کسری کاپوچو نیز در حالت $\gamma = \mathrm{n} \in \mathrm{N}$ داریم:

$$ ({}_a^C D_t^{n} x)(t) = x^{(n)}(t), \quad (۱۱)$$

$$ ({}_a^C D_t^{n} x)(t) = (-1)^{(n)} x^{(n)}(t). \quad (۱۲)$$

بررسی خواص بیش‌تر انواع مشتقات و انتگرال‌های کسری و نیز ارتباط و تاثیر مشتق کاپوچو و انتگرال کسری ریمان- لیوویل بر یک‌دیگر را می‌توان در مرجع [۱] مطالعه کرد.

۳- چندجمله‌ای‌های برنولی

چندجمله‌ای‌های برنولی از درجه m بر روی بازه $[0,1]$ به صورت زیر تعریف می‌شوند [۱۶]:

$$ \beta_m(t) = \sum_{i=0}^{m} \binom{m}{i} \alpha_{m-i} t^i . \quad (۱۳)$$

که در آن، α_i به ازای $i = 0, 1, \dots, m,$ اعداد برنولی بوده و به صورت زیر تعریف می‌شود:

$$ \frac{t}{e^t - 1} = \sum_{i=0}^{m} \alpha_i \frac{t^i}{i!}. \quad (۱۴)$$

چندجمله اول اعداد برنولی و چندجمله‌ای‌های برنولی به شکل

زیر می‌باشند:

$$\alpha_0 = 1, \quad \alpha_1 = \frac{-1}{2}, \quad \alpha_2 = \frac{1}{6}, \quad \alpha_4 = \frac{-1}{30}, \dots,$$
$$\alpha_{2i+1} = 0, \quad i = 0,1,2,3 \dots$$

و

$$\beta_0(t) = 1, \quad \beta_1(t) = t - \frac{1}{2}, \quad \beta_2(t) = t^2 - t + \frac{1}{6}, \dots$$

این چندجمله‌ای‌ها در رابطه زیر صدق می‌کنند:

$$\int_0^1 \beta_n(t)\beta_m(t)\, dt = (-1)^{n-1}\frac{m!n!}{(m+n)!}\alpha_{n+m}\,, \qquad (۱۵)$$

$n, m \geq 1$.

هم‌چنین یک پایه کامل روی فضای $L^2[0,1]$ تشکیل می‌دهند [۱۵].

۳-۱- تقریب توابع

چون $Y = span\{\beta_0(t), \beta_1(t), \dots, \beta_m(t)\}$ یک زیرمجموعه بسته و متناهی از فضای هیلبرت $H = L^2[0,1]$ می‌باشد، بنابراین، یک زیرفضای کامل است و درنتیجه برای هر $f \in H$ بهترین تقریب منحصر به فرد مانند $f_0 \in Y$ وجود دارد که در این صورت [۱۵]:

$$\forall y \in Y, \quad \|f - f_0\| \leq \|f - y\|.$$

از آن‌جایی‌که $f_0 \in Y$ پس می‌توان ضرایب یکتای $c_0, c_1, \dots, c_m$ را به نحوی پیدا کرد که رابطه زیر برقرار باشد:

$$f(t) \approx f_0(t) = \sum_{j=0}^{m} c_j\beta_j(t) = C^T\Psi(t), \qquad (۱۶)$$

که در آن، T نشان‌دهنده ترانهاده است و بردارهای $\Psi(t)$ و C به صورت زیر تعریف می‌شوند:

$$C = [c_0, c_1, \dots, c_m]^T,$$
$$\Psi(t) = [\beta_0(t), \beta_1(t), \dots, \beta_m(t)]^T. \qquad (۱۷)$$

حال با در نظر گرفتن رابطه زیر:

$$f_j = \langle f, \beta_j\rangle = \int_0^1 f(t)\beta_j(t)\, dt, \qquad (۱۸)$$

که $\langle , \rangle$ ضرب داخلی را نشان می‌دهد، به ازای $j = 0, \dots, m$ خواهیم داشت:

$$f_j = \sum_{i=0}^{m} c_i \int_0^1 \beta_i(t)\beta_j(t)\, dt = \sum_{j=0}^{m} c_i d_{ij} \qquad (۱۹)$$

که در آن، $d_{ij} = \int_0^1 \beta_i(t)\beta_j(t)\, dt, \ \ i,j = 0, \dots, m$. می‌باشد.

با در نظر گرفتن:

$$F = \langle f, \Psi\rangle = \begin{bmatrix} f_0 \\ f_1 \\ \cdot \\ \cdot \\ \cdot \\ f_m \end{bmatrix}, \qquad D = [d_{ij}],$$

عبارت زیر به دست می‌آید:

$$F^T = C^T D \qquad (۲۰)$$

حال با توجه به این که D ماتریس متقارن معرفی‌شده به صورت زیر است:

$$D = \int_0^1 \Psi(t)\Psi(t)^T\, dt \qquad (۲۱)$$

بردار ضرایب مجهول C از رابطه زیر محاسبه می‌شود:

$$C = D^{-1}\langle f(t), \Psi(t)\rangle, \qquad (۲۲)$$

۳-۲- ماتریس عملیاتی انتگرال کسری ریمان- لیوویل چندجمله‌ای‌های برنولی

در این بخش ماتریس عملیاتی $(m+1)\times(m+1)$ انتگرال کسری ریمان- لیوویل را برای چندجمله‌ای‌های برنولی معرفی کرده و آن را با $\boldsymbol{F}^{(\gamma)}$ نمایش می‌دهیم [۱۶].

$$ {}_0I_t^{\gamma}\Psi(t) \simeq \boldsymbol{F}^{(\gamma)}\Psi(t). \qquad (۲۳)$$

با استفاده از رابطه (۱۳) و خاصیت خطی انتگرال ریمان- لیوویل و هم‌چنین با توجه به رابطه [۱۷]:

$$ {}_0I_t^{\gamma}t^n = \frac{\Gamma(n+1)}{\Gamma(n+1+\gamma)}t^{n+\gamma}, \quad n > -1, \qquad (۲۴)$$

داریم:

$$ {}_0\mathrm{I}_t^{\gamma}\beta_{\mathrm{i}}(\mathrm{t}) = \ {}_0\mathrm{I}_t^{\gamma}\left(\sum_{\mathrm{r}=0}^{\mathrm{i}}\binom{\mathrm{i}}{\mathrm{r}}\ \alpha_{\mathrm{i}-\mathrm{r}}\mathrm{t}^{\mathrm{r}}\right) =$$
$$\sum_{\mathrm{r}=0}^{\mathrm{i}}\binom{\mathrm{i}}{\mathrm{r}}\ \alpha_{\mathrm{i}-\mathrm{r}}\ {}_0\mathrm{I}_t^{\gamma}\mathrm{t}^{\mathrm{r}} = \sum_{\mathrm{r}=0}^{\mathrm{i}}\binom{\mathrm{i}}{\mathrm{r}}\ \alpha_{\mathrm{i}-\mathrm{r}}\frac{\Gamma(\mathrm{r}+1)}{\Gamma(\mathrm{r}+1+\gamma)}\mathrm{t}^{\mathrm{r}+\gamma} =$$
$$\sum_{\mathrm{r}=0}^{\mathrm{i}}\mathrm{b}_{\mathrm{i},\mathrm{r}}\,\mathrm{t}^{\mathrm{r}+\gamma}. \qquad (۲۵)$$

که در آن:

$$b_{i,r} = \binom{i}{r}\alpha_{i-r}\frac{\Gamma(r+1)}{\Gamma(r+1+\gamma)}. \qquad (۲۶)$$

حال با بسط عبارت $t^{r+\gamma}$ بر حسب چندجمله‌ای‌های برنولی به دست می‌آوریم:

$$t^{r+\gamma} = \sum_{j=0}^{m} c_{r,j}\beta_j(t), \qquad (۲۷)$$

به طوری که ضرایب از فرمول زیر حاصل می‌شوند:

$$c_{r,j} = \frac{\langle t^{r+\gamma}, \beta_j(t)\rangle}{\langle \beta_j(t), \beta_j(t)\rangle}, \qquad (۲۸)$$

و با قراردادن تقریب به دست آمده در معادله (۲۵)، عبارت زیر حاصل می‌شود:

$$ {}_0I_t^{\gamma}\beta_i(t) = \sum_{r=0}^{i} b_{i,r}\sum_{j=0}^{m} c_{r,j}\beta_j(t) =$$
$$\sum_{j=0}^{m}\left(\sum_{r=0}^{i} b_{i,r}\, c_{r,j}\right)\beta_j(t), \qquad (۲۹)$$

بدون از دست دادن کلیت و برای نمایش ساده‌تر درایه‌های ماتریس عملیاتی مذکور، $\theta_{i,j,r} = b_{i,r}c_{r,j}$ را در نظر گرفته و معادله (۲۹) را به صورت زیر بازنویسی می‌کنیم:

$$I_t^{\gamma}\beta_i(t) \approx \left[\sum_{r=0}^{i}\theta_{i,0,r}, \sum_{r=0}^{i}\theta_{i,1,r}, \dots, \sum_{r=0}^{i}\theta_{i,m,r}\right]\Psi(t),$$
$$i = 0, \dots, m. \qquad (۳۰)$$

که در نهایت، ماتریس عملیاتی انتگرال به صورت زیر به دست می‌آید:

$$\boldsymbol{F^{(\gamma)}} = \begin{bmatrix} \theta_{0,0,0} & \cdots & \theta_{0,m,0} \\ \vdots & \ddots & \vdots \\ \sum_{r=0}^{m}\theta_{m,0,r} & \cdots & \sum_{r=0}^{m}\theta_{m,m,r} \end{bmatrix}. \qquad (۳۱)$$

۴- تجزیه و تحلیل هم‌گرایی

در این بخش، کران بالای خطا برای ماتریس عملیاتی انتگرال کسری ریمان- لیوویل معرفی‌شده در رابطه (۳۱)، به دست می‌آید. برای این منظور ابتدا قرار می‌دهیم:

$$E(t) = {}_0I_t^{\gamma}\Psi(t) - \boldsymbol{F^{(\gamma)}}\Psi(t), \qquad (۳۲)$$

و نشان می‌دهیم که اگر تعداد چندجمله‌ای‌های برنولی پایه‌ای به سمت بی‌نهایت میل کند، درایه‌های بردار خطای $E(t)$ به سمت صفر میل می‌کنند. برای اثبات این ادعا، ابتدا به بیان لم و قضایای زیر می‌پردازیم.

لم ۱:

فرض کنیم $f \in C^{m+1}[0,1]$ و Y زیرفضای تولیدشده توسط چندجمله‌های برنولی به صورت زیر باشد:

$$Y = span\{\beta_0(t), \beta_1(t), \dots, \beta_m(t)\}$$

آن‌گاه خواهیم داشت:

$$\|f - y_0\|_{L^2[0,1]} \le \frac{K}{(m+1)!\sqrt{2m+3}}, \qquad (۳۳)$$

که در آن، y_0 بهترین تقریب یکتای تابع f در مجموعه Y است و $K = Max_{t\in[0,1]}|f^{(m+1)}(t)|$.

اثبات:

مجموعه $\{1, t, \dots, t^m\}$ را به عنوان یک پایه برای فضای چندجمله‌ای‌های تا درجه m در نظر گرفته و فرض می‌کنیم:

$$y_1(t) = f(0) + t\acute{f}(0) + \acute{\cdots} + \frac{t^m}{m!}f^{(m)}(0). \qquad (۳۴)$$

لذا به کمک بسط تیلور داریم:

$$|f(t) - y_1(t)| = \frac{|f^{(m+1)}(\tau)t^{m+1}|}{(m+1)!}, \qquad (۳۵)$$

که در آن، $\tau \in (0,1)$. با توجه به این‌که y_0 بهترین تقریب یکتای تابع در مجموعه Y و هم‌چنین $y_1 \in Y$, و با درنظرگرفتن تساوی فوق می‌توان نتیجه گرفت:

$$\|f - y_0\|^2_{L^2[0,1]} \le \|f - y_1\|^2_{L^2[0,1]} =$$
$$\int_0^1 |f(t) - y_1(t)|^2 dt = \frac{K^2}{(m+1)!^2(2m+3)}. \qquad (۳۶)$$

با اعمال عملگر جذر در طرفین تساوی فوق، اثبات لم ۱ کامل می‌شود. □

قضیه ۱:

فرض کنیم که H یک فضای هیلبرت و Y یک زیرفضای بسته و متناهی آن باشد، $\{y_1, \dots y_n\}$ را پایه‌ای برای زیرفضای Y در نظر گرفته و برای هر عضو دلخواه از فضای H مانند x بهترین تقریب منحصر به فرد متعلق به زیرفضای Y را با y_0 نمایش می‌دهیم، بنابراین خواهیم داشت[۱۵]:

$$\|x - y_0\|_2^2 = \frac{G(x,y_1,\dots,y_n)}{G(y_1,\dots,y_n)}, \qquad (۳۷)$$

که G ماتریس گرام می‌باشد.

$$G(x,,y_1,\dots,y_n) = \begin{bmatrix} \langle x,x\rangle & \langle x,y_1\rangle & \cdots & \langle x,y_n\rangle \\ \vdots & & \ddots & \vdots \\ \langle y_n,x\rangle & \langle y_n,y_1\rangle & \cdots & \langle y_n,y_n\rangle \end{bmatrix} \qquad (۳۸)$$

قضیه ۲:

فرض کنید $f \in L^2[0,1]$ و $f(t)$ توسط $\sum_{i=0}^{m}c_i\beta_i(t)$ تقریب زده شود، آن‌گاه [۱۶]:

$$\lim_{m\to\infty}\|f(t) - \sum_{i=0}^{m}c_i\beta_i(t)\|_{L^2[0,1]} = 0.$$

□

حال با توجه به قضایای بیان‌شده، نشان می‌دهیم که ${}_0I_t^{\gamma}\beta_i(t) - \boldsymbol{F^{(\gamma)}}\beta_i(t)$ به سمت صفر میل کند.

چون $t^{r+\gamma} = \sum_{j=0}^{m}c_{r,j}\beta_j(t)$, و با به‌کارگیری قضیه ۱ داریم:

$$\left\|t^{r+\gamma} - \sum_{j=0}^{m}c_{r,j}\beta_j(t)\right\| = \left(\frac{G(t^{r+\gamma},\beta_0,\beta_1,\dots,\beta_m)}{G(\beta_0,\beta_1,\dots,\beta_m)}\right)^{\frac{1}{2}}, \qquad (۳۹)$$

و درنتیجه، به ازای $i = 0,1,\dots,m$, عبارت زیر حاصل می‌شود:

$$\left\| {}_0I_t^{\gamma}\beta_i(t) - \sum_{j=0}^{m}\left(\sum_{r=0}^{i}b_{i,r}\,c_{r,j}\right)\beta_j(t)\right\|$$
$$\le \sum_{r=0}^{i}\frac{i!\,\alpha_{i-r}}{(i-r)!\,\Gamma(r+1+\gamma)}\left\|t^{r+\gamma} - \sum_{j=0}^{m}c_{r,j}\beta_j(t)\right\|$$
$$\le \sum_{r=0}^{i}b_{i,r}\left(\frac{G(t^{r+\gamma},\beta_0,\beta_1,\dots,\beta_m)}{G(\beta_0,\beta_1,\dots,\beta_m)}\right)^{\frac{1}{2}}. \qquad (۴۰)$$

با عنایت به قضیه ۲ و هم‌چنین آخرین نامساوی به دست آمده در (۴۰)، می‌توان نتیجه گرفت که تفاضل $\boldsymbol{F^{(\gamma)}}\Psi(t)$ و

${}_0 I_t^{\gamma}\Psi(t)$ وقتی که m به سمت بی‌نهایت میل کند، به صفر هم‌گرا می‌شود.

۵- بیان مساله

معادله انتگرال- دیفرانسیل کسری زیر را در نظر می‌گیریم:

$$
\begin{aligned}
&{}_0^C D_t^{\gamma} x(t) = x(t) + g(t) \\
&+ \int_0^t K_1(t,s)\,(x(s))^{n_1}({}_0^C D_t^{\gamma_1} x(s))^{n_2} ds + \\
&\int_0^1 K_2(t,s)\,(x(s))^{n_3}({}_0^C D_t^{\gamma_2} x(s))^{n_4} ds. \qquad (۴۱)
\end{aligned}
$$

که در آن:

$$0 \le t,s \le 1\,, \quad n-1 \le \gamma \le n,$$

$$0 \le \gamma_1 \le \gamma_2 \le \gamma.$$

هم‌چنین، شرایط اولیه داده شده همراه با معادله به صورت زیر می‌باشد:

$$x^{(i)}(0) = \vartheta_i, \quad i = 0,1,\dots,n-1, \qquad (۴۲)$$

در معادله (۴۱)، K_1 و K_2 را هسته‌های جدایی‌پذیر در نظر گرفته و فرض می‌کنیم که $n_1,\ n_2,\ n_3,\ n_4$ اعداد صحیح مثبت بوده و تمامی مشتقات کسری ظاهرشده در این معادله از نوع کاپوچو می‌باشند. برای حل این مساله، ${}_0^C D_t^{\gamma} x(t)$ توسط توابع برنولی به شکل:

$${}_0^C D_t^{\gamma} x(t) = \sum_{i=0}^{m} c_i \beta_i(t) = C^T \Psi(t), \qquad (۴۳)$$

تقریب زده می‌شود که در آن $C = [c_0, c_1, \dots, c_m]^T$ بردار ضرایب و مجهول می‌باشد. با توجه به ارتباط زیر بین مشتق کسری کاپوچو و انتگرال کسری ریمان - لیوویل [۱۷] داریم:

$${}_0 I_t^{\gamma}\,{}_0^C D_t^{\gamma} x(t) = x(t) - \sum_{i=0}^{n-1} x^{(i)}(0)\frac{t^i}{i!}\,, \qquad (۴۴)$$

فرمول زیر را برای تابع مجهول $x(t)$ به دست می‌آوریم:

$$
\begin{aligned}
&x(t) = \sum_{i=0}^{m} c_i \;\; {}_0 I_t^{\gamma}\beta_i(t) + \sum_{i=0}^{n-1}\vartheta_i \;\; \frac{t^i}{i!} = C^T \boldsymbol{F}^{(\gamma)}\Psi(t) + \\
&d^T\Psi(t)\,, \qquad (۴۵)
\end{aligned}
$$

هم‌چنین برای مشتقات کسری کاپوچو کم‌تر از مرتبه $\boldsymbol{\gamma}$ روابط زیر طبق خواص و رابطه مشتق و انتگرال کسری حاصل می‌گردد:

$${}_0^C D_t^{\gamma_1} x(t) = C^T \boldsymbol{F}^{(\gamma-\gamma_1)}\Psi(t) + {d_1}^T\Psi(t), \qquad (۴۶)$$

و

$${}_0^C D_t^{\gamma_2} x(t) = C^T \boldsymbol{F}^{(\gamma-\gamma_2)}\Psi(t) + {d_2}^T\Psi(t)\,. \qquad (۴۷)$$

با توجه به فرض جدایی‌پذیری هسته‌ها می‌توان توابع $K_1(t,s)$ و $K_2(t,s)$ را نیز به شکل زیر نوشت:

$$K_1(t,s) = A_1(t)B_1(s), \qquad (۴۸)$$

$$K_2(t,s) = A_2(t)B_2(s), \qquad (۴۹)$$

و در نهایت انتگرال‌های معادله (۴۱) را به شکل زیر تقریب زد:

$$
\begin{aligned}
&\int_0^t K_1(t,s)\,(x(s))^{n_1}({}_0^C D_t^{\gamma_1} x(s))^{n_2} ds \approx \\
&A_1(t)\int_0^t B_1(s)\left(C^T \boldsymbol{F}^{(\gamma)}\Psi(s) + d^T\Psi(s)\right)^{n_1} \\
&\left(C^T \boldsymbol{F}^{(\gamma-\gamma_1)}\Psi(t) + {d_1}^T\Psi(t)\right)^{n_2} ds = H_1(t), \qquad (۵۰)
\end{aligned}
$$

به طور مشابه داریم:

$$
\begin{aligned}
&\int_0^1 K_2(t,s)\,(x(s))^{n_3}({}_0^C D_t^{\gamma_2} x(s))^{n_4} ds \\
&A_2(t)\int_0^1 B_2(s)\left(C^T \boldsymbol{F}^{(\gamma)}\Psi(s) + d^T\Psi(s)\right)^{n_3} \\
&\left(C^T \boldsymbol{F}^{(\gamma-\gamma_2)}\Psi(t) + {d_1}^T\Psi(t)\right)^{n_4} ds = H_2(t). \qquad (۵۱)
\end{aligned}
$$

حال با قراردادن تقریب‌های بیان‌شده در معادله (۴۱)، دستگاه معادله جبری زیر بر اساس درایه‌های مجهول بردار C به دست می‌آید:

$$
\begin{aligned}
&C^T\Psi(t) - C^T \boldsymbol{F}^{(\gamma)}\Psi(t) - d^T\Psi(t) - g(t) - H_1(t) - \\
&H_2(t) = 0. \qquad (۵۲)
\end{aligned}
$$

اکنون با به‌کارگیری روش کم‌ترین مربعات، تابعی زیر را برای پیداکردن ضرایب مجهول در نظر گرفته و بردار C به نحوی انتخاب می‌شود که مقدار تابعی کمینه شود:

$$
\begin{aligned}
&J[c_0, c_1, \dots, c_m] = \int_0^1 (C^T\Psi(t) - C^T \boldsymbol{F}^{(\gamma)}\Psi(t) \\
&-d^T\Psi(t) - g(t) - H_1(t) - H_2(t))^2 dt, \qquad (۵۳)
\end{aligned}
$$

شرایط لازم برای این منظور، تشکیل معادلات $\frac{\partial J}{\partial c_k} = 0$ و $k = 0,1,\dots,m.$ می‌باشد. این معادلات، تشکیل یک دستگاه غیرخطی از $m+1$ معادله و $m+1$ مجهول می‌دهند و در نهایت به کمک روش تکراری نیوتن حل شده است.

۶- نتایج عددی

در این قسمت برای نشان‌دادن درستی و دقت روش به‌کار برده‌شده برای حل معادله انتگرال- دیفرانسیل کسری مورد نظر نتایج مربوط به چند مثال را بررسی می‌کنیم:

مثال ۱:

معادله انتگرال- دیفرانسیل ولترای کسری زیر را در نظر می‌گیریم [۱۸]:

$$ {}_0^C D_t^{\frac{1}{2}} x(t) = x(t) + \frac{8}{3\Gamma\left(\frac{1}{2}\right)} t^{\frac{3}{2}} - t^2 - \frac{1}{3}t^3 + \int_0^t x(s)\, ds, $$

$$ 0 \le t \le 1, $$

$$ x(0) = 0, \qquad (۵۴) $$

جواب دقیق این معادله برابر با t^2 می‌باشد. با به کارگیری روش ارائه‌شده در بخش ۵، خطای مطلق جواب تقریبی در نقاط مختلف، در جدول (۱) مشاهده می‌شود.

همان‌طورکه از نتایج برمی‌آید، با افزایش تعداد چندجمله‌ای‌های پایه مقدار تقریبی جواب، به جواب واقعی در نقاط مختلف بازه مورد بررسی میل می‌کند.

جدول (۱): خطای مطلق مثال ۱

t	m=۵	m=۷
۰/۱	۴/۴×۱۰$^{-۵}$	۶/۹×۱۰$^{-۶}$
۰/۳	۳/۰×۱۰$^{-۵}$	۹/۹×۱۰$^{-۷}$
۰/۵	۲/۷×۱۰$^{-۶}$	۹/۷×۱۰$^{-۷}$
۰/۷	۲/۶×۱۰$^{-۵}$	۹/۲×۱۰$^{-۷}$
۰/۹	۴/۶×۱۰$^{-۵}$	۱/۰×۱۰$^{-۵}$

مثال ۲:

معادله کسری انتگرال- دیفرانسیل کسری فردهلم زیر را در نظر می‌گیریم [۱۹]:

$$ {}_0^C D_t^{\gamma} x(t) = 1 - \frac{t}{4} + \int_0^1 ts\, [x(s)]^2\, ds, $$

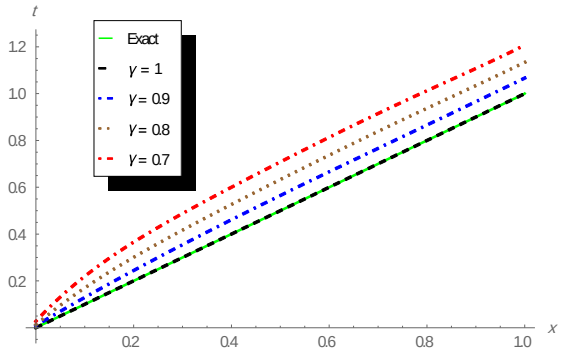
$$ x(0) = 0, \quad 0 \le t \le 1, \quad 0 \le \gamma \le 1, \qquad (۵۵) $$

مقدار دقیق این معادله برای $\gamma = 1$, برابر با $x(t) = t$, بوده و در جدول (۲) مقدار خطای مطلق برای این مساله به ازای mهای مختلف نشان داده شده است. در این مثال هم، نظیر مثال قبل با افزایش تعداد چندجمله‌ای‌های پایه‌ای تفاضل میان مقدار دقیق معادله و جواب تقریبی به دست آمده از روش پیشنهادی به سمت صفر میل می‌کند.

قابل توجه است که در شکل (۱) نیز نمودارهای به دست آمده برای تابع مجهول $x(t)$ به ازای مقادیر مختلف γ و $m = 3$ آورده شده است. همان‌طورکه از نمودارها مشخص است، زمانی که γ به سمت یک میل می‌کند، جواب به دست آمده برای تابع مجهول به مقدار دقیق نزدیک می‌شود. هم‌چنین شکل (۱) نشان‌دهنده هم‌گرایی بین جواب مساله به ازای مقادیر مختلف γ است که این نوع هم‌گرایی نشان‌دهنده کارایی روش بیان شده در حالت کسری نیز می‌باشد.

جدول (۲): خطای مطلق مثال ۲.

t	m=۲	m=۴
۰/۱	۳/۱×۱۰$^{-۱۳}$	۲/۲×۱۰$^{-۱۷}$
۰/۳	۹/۳×۱۰$^{-۱۳}$	۶/۶×۱۰$^{-۱۷}$
۰/۵	۱/۵×۱۰$^{-۱۲}$	۱/۱×۱۰$^{-۱۶}$
۰/۷	۲/۱×۱۰$^{-۱۲}$	۱/۵×۱۰$^{-۱۶}$
۰/۹	۲/۷×۱۰$^{-۱۲}$	۱/۹×۱۰$^{-۱۶}$



شکل (۱): نمودار x(t) به ازای γ مختلف

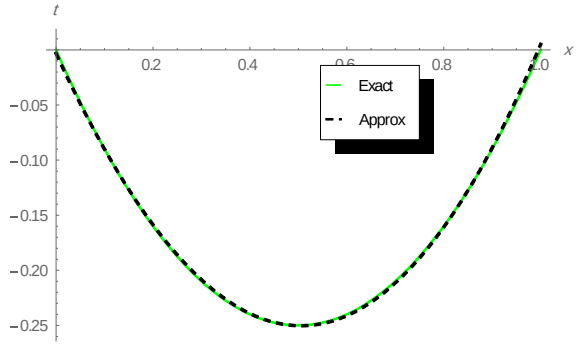
مثال ۳:

معادله دیفرانسیل کسری زیر را در نظر می‌گیریم [۲۰]:

$$ {}_0^C D_t^{\frac{1}{2}} x(t) = \frac{\left(\frac{8}{3}\right)t^{\frac{3}{2}} - 2t^{\frac{1}{2}}}{\sqrt{\pi}} + \frac{t}{12} + \int_0^1 ts\, [x(s)] \quad ds, $$

$$ 0 \le t \le 1, \quad x(0) = 0, \qquad (۵۶) $$

جواب دقیق این معادله برابر با $t^2 - t$ می‌باشد و نمودار مقدار دقیق و تقریبی این معادله در شکل (۲) برای $m = 3$, نشان داده شده است. خطای مطلق بین جواب دقیق و جواب عددی به دست آمده توسط روش پیشنهادی در نقاط مختلف در جدول (۳) مشاهده می‌شود. همان‌طورکه از نتایج برمی‌آید، افزایش تعداد چندجمله‌ای‌های پایه‌ای سبب کاهش خطای مطلق می‌شود.



شکل (۲): نمودار مقدار تقریبی و دقیق x(t) مثال۳.

جدول(۳): خطای مطلق مثال ۳

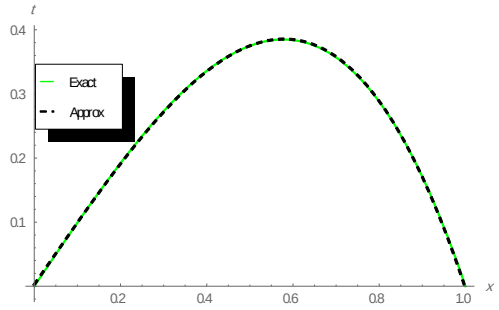
t	m=۲	m=۵
۰/۱	۲/۹×۱۰$^{-۳}$	۴/۶×۱۰$^{-۴}$
۰/۳	۲/۳×۱۰$^{-۳}$	۳/۵×۱۰$^{-۴}$
۰/۵	۳/۶×۱۰$^{-۳}$	۹/۲×۱۰$^{-۵}$
۰/۷	۸/۳×۱۰$^{-۴}$	۲/۸×۱۰$^{-۵}$
۰/۹	۶/۰×۱۰$^{-۳}$	۵/۱×۱۰$^{-۵}$

مثال ۴:

معادله انتگرال- دیفرانسیل کسری زیر را درنظر می‌گیریم [۲۰]:

$$ {}_0^C D_t^{\frac{5}{6}} x(t) = -\frac{3}{91}\frac{t^{\frac{1}{6}}\Gamma\left(\frac{5}{6}\right)(-91+216t^2)}{\pi} $$
$$ +(5-2e)t + \int_0^1 te^s\,[x(s)]\quad ds, $$
$$ 0 \le t \le 1, \quad x(0) = 0, \qquad (۵۷) $$

جواب دقیق این معادله برابر با $t - t^3$ می‌باشد. نمودار مقدار دقیق و تقریبی این معادله در شکل (۳) برای $m = 3$ مشاهده می‌شود.



شکل (۳): نمودار مقدار تقریبی و دقیق x(t) مثال ۴.

هم‌چنین خطای مطلق بین جواب دقیق و جواب عددی به دست آمده توسط روش پیشنهادی در نقاط مختلف بازه مورد بررسی، در جدول (۴) بیان شده است.

جدول (۴): خطای مطلق مثال ۴

t	m=۲	m=۵
۰/۱	۲×۱۰$^{-۳}$	۵/۵×۱۰$^{-۵}$
۰/۳	۲/۱×۱۰$^{-۳}$	۳/۵×۱۰$^{-۴}$
۰/۵	۱/۶×۱۰$^{-۳}$	۳/۶×۱۰$^{-۵}$
۰/۷	۲/۲×۱۰$^{-۳}$	۳/۳×۱۰$^{-۴}$
۰/۹	۶/۲×۱۰$^{-۳}$	۵/۲×۱۰$^{-۴}$

۷- نتیجه‌گیری

در این مقاله، از چندجمله‌ای‌های برنولی و خواص آن و ماتریس عملیاتی انتگرال، معادله انتگرال دیفرانسیل کسری را تبدیل به یک دستگاه از معادلات جبری غیرخطی نموده و با به کارگیری روش تکراری نیوتن، به جواب تقریبی مورد نظر دست یافته‌ایم. هم‌چنین تجزیه و تحلیل خطا مورد بحث قرار گرفته شده است و با ارائه مثال‌هایی کارایی روش را مورد بررسی قرار داده‌ایم.

۸- مراجع

[1] K. Oldham and J. Spanier, "The Fractional Calculus, Theory and Applications of Differentiation and Integration to Arbitrary Order," Mathematics in Science and Engineering, Academic Press, ۱۹۷۴.

[2] G. Gonzalez-Parra, A. J. Arenas, and B. M. Chen-Charpentier, "A fractional order epidemic model for the simulation of outbreaks of inuenza A (H1N1)," Mathematical Methods in the Applied Sciences, vol. 37, no. 15, pp. 2218-2226, 2014.

[3] R. T. Baillie, "Long memory processes and fractional integration in econometrics," J. Econom., vol. 73, pp. 5-59, 1996.

[4] J. H. He, "Nonlinear oscillation with fractional derivative and its applications," International conference on vibrating engineering98, China: Dalian, pp. 288-291, 1998.

[5] L. Boyadjiev, H. J. Dobner, and S. L. Kalla," A fractional integro-differential equation of Volterra type," Math. Comput. Model, vol. 28, no. 10, pp. 103-130, 1998.

[6] S. Momani and M. Noor, "Numerical methods for fourth order fractional integro-differential equations," Appl. Math. Comput. vol. 182, pp. 54-60, 2006.

[7] S. S. Ray, "Analytical solution for the space fractional diffusion equation by two-step Adomian decomposition method," Commun. Nonlinear Sci. Numer. Simulat. vol. 14, pp.129-306, 2009.

[8] Y. Nawaz, "Variational iteration method and homotopy perturbation method for fourth-order fractional integro-differential equations," Comput. Math. Appl., vol. 61, no. 8, pp. 2330-2340, 2011.

[9] H. Saeedi, M. Mohseni Moghadam, N. Mollahasani, and G. N Chuev, "A CAS wavelet method for solving nonlinear Fredholm integro-differential equations of fractional order," Commun. Nonlinear Sci. Numer. Simulat. vol. 16, no. 3, pp. 1154-1163, 2011.

[10] L. Huang, X. F. Li, Y. L. Zhao, and X. Y. Duan, "Approximate solution of fractional integro-differential equations by Taylor expansion method," Comput. Math. Appl., vol. 62, no. 3, pp. 1127-1134, 2011.

[11] E. A. Rawashdeh, "Numerical solution of fractional integro-differential equations by collocation method," Appl. Math. Comput. vol. 176, pp. 1-6, 2006.

[12] S. Sedaghat, Y.Ordokhani, and M. Dehghan, "On Spectral Method for Volterra Functional Integro-Differential Equations of Neutral Type," Numerical Functional Analysis and Optimization, vol. 35, no. 2, 2014.

[13] D. Nazari and S. Shahmorad, "Application of the fractional differential transform method to fractional-order integro-differential equations with nonlocal boundary conditions," J. Comput. Appl. Math., vol. 234, no. 3, pp. 883-891, 2010.

[14] I. Podlubny," Fractional Differential Equations," Academic Press, New York, 1999.

[15] E. Kreyszig, "Introductory Functional Analysis with Applications," John Wiley and Sons Press, New York, 1987.

[16] E. Keshavarz, Y. Ordokhani, and M. Razzaghi, "A numerical solution for fractional optimal control problems via Bernoulli polynomials," Journal of Vibration and Control, vol. 22, no. 18, pp. 3889-3903, 2016.

[17] K. Rabiei, Y. Ordokhani, and E. Babolian, "The Boubaker polynomials and their application to solve fractional optimal control problems," Nonlinear Dynamics, vol. 88, no. 2, pp. 1013-1026, 2016.

[18] F. Awawdeh, E. A. Rawashdeh, and H. M. Jaradat, "Analytic solution of fractional integro-differential equations," Annals of the University of Craiova, Mathematics and Computer Science Series, vol. 38, pp. 1-10, 2011.

[19] L. Zhu and Q. Fan, "Solving fractional nonlinear Fredholm integro-differential equations by the second kind Chebyshev wavelet," Commun. Nonl. Sci. Numer. Simulat. vol. 17, pp. 2333-2341, 2012.

[20] D. Sh. Mohammed, "Numerical Solution of Fractional Integro-Differential Equations by Least Squares Method and Shifted Chebyshev Polynomial," Mathematical Problems in Engineering, vol. 2014, 2014.

مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"
ویژه‌نامه کنفرانس بین‌المللی ترکیبیات، رمزنگاری و محاسبات، ص ۱۱۵ -۱۱۱

نهان‌نگاری تصویربا استفاده از الگوریتم توده ذرات

رضا سعادتی*

استادیار، دانشگاه علم و صنعت ایران

(دریافت: ۹۵/۰۷/۰۵، پذیرش: ۹۶/۰۳/۰۶)

چکیده

با رشد سریع اینترنت و فن‌آوری‌های چندرسانه‌ای دیجیتال در دهه اخیر، نسخه‌برداری و دست‌کاری داده‌ها بدون هیچ افت کیفیت و بدون رعایت حق نشر و با هزینه‌های بسیار اندک امکان‌پذیر شده است. در همین راستا هرروز نیازهای امنیتی متنوع‌تری مطرح می‌گردد. نهان‌نگاری داده در محصولات دیجیتال، به‌عنوان یک راه‌حل برای پیاده‌سازی و اثبات حق مالکیت، احراز اصالت محتوی و کنترل تعداد نسخه‌های چاپ‌شده از یک اثر را محقق ساخته است. نهان‌نگاری دیجیتالی یعنی قرار دادن یک سیگنال نامحسوس در بین داده‌های رسانه پوششی، به‌طوری‌که هیچ تغییری در داده‌های اصلی نداشته باشد ولی در صورت نیاز بتوان آن را استخراج کرده و به‌عنوان ادعا برای مالکیت اثر دیجیتالی استفاده نمود. نهان‌نگاری دیجیتال شامل دو بخش هست. بخش اول، مراحل قرار دادن تصویر نهان‌نگاری یا لوگو در داخل تصویر میزبان و بخش دوم مراحل استخراج تصویر نهان‌نگاری یا لوگو از تصویر نهان‌نگاری‌شده می‌باشد. در این مقاله، در مورد نقش الگوریتم PSO در استخراج تصویر watermark برای پیداکردن مقدار بهینه Scaling factor بحث و بررسی‌شده است.

واژه‌های کلیدی:نهان‌نگاری تصاویر دیجیتالی، حوزه تبدیل، الگوریتم توده ذرات

۱- مقدمه

نهان‌نگاری برای پنهان‌کردن یا اضافه‌کردن داده یا فایلی در فایل دیگر، به‌طوری‌که فقط افراد آگاه با ابزار لازم بتوانند به آن دست یابند و هم‌چنین یکی از راه‌های حفاظت از داده‌های چندرسانه‌ای در برابر نشرهای غیرقانونی و توزیع غیرقانونی آن‌ها است. تفاوت اصلی نهان‌نگاری با پنهان‌نگاری در این است که در نهان‌نگاری هدف اصلی حفظ محصول دیجیتال می‌باشد، درحالی‌که در پنهان‌نگاری، هدف اصلی، پیام پنهان‌شده می‌باشد. در این روش، یک سیگنال ثانویه یا الگو به تصویر، ویدئو و یا داده‌های صوتی جاسازی می‌شود که قابل کشف نیست و به‌صورت یک عضو جدایی‌ناپذیر به خوبی با داده‌های دیجیتال اصلی منطبق می‌باشد و در مقابل هر نوع پردازش سیگنال چندرسانه‌ای [۲-۱] بدون هیچ مشکلی باقی می‌ماند. این اطلاعات ثانویه تعبیه‌شده، علامت نهان‌نگاری دیجیتال است. علامت نهان‌نگاری دیجیتالی به‌طورکلی، یک کد شناسایی مرئی یا نامرئی است که ممکن است برخی اطلاعات مربوط به گیرنده قانونی و یا نویسنده داده‌های اصلی و قوانین حق نشر به شکل داده‌های متنی و یا تصویری در آن ذخیره‌شده باشد. این علامت نهان‌نگاری دیجیتال را می‌توان شناسایی و یا استخراج نمود و بعداً به‌عنوان یک ادعا در مورد مالکیت حقیقی داده‌ها از آن استفاده کرد. فقدان یک علامت نهان‌نگاری در تصویری که قبلاً نهان‌نگاری شده بود به این معنی است که محتوای داده دیجیتالی دچار تغییر شده است [۳]. در ادامه این بخش، در بخش دوم الگوریتم بهینه‌سازی ازدحام ذرات و در ادامه، روش پیشنهادی نهان نگاری در حوزه موجک در بخش سوم شرح داده می‌شود. در انتها در بخش چهارم با نتیجه گیری از پیاده‌سازی‌ها و نتیجه گیری نهایی در بخش پنجم، این مقاله را به پایان می‌رسانیم.

۲- الگوریتم بهینه‌سازی ازدحام ذرات

الگوریتم بهینه‌سازی ازدحام ذرات یاPSO[1]، که به نام الگوریتم پرندگان نیز شناخته می‌شود، یکی از الگوریتم‌های قدرتمند و پرطرفدار برای بهینه‌سازی است که بیش‌تر به خاطر سرعت هم‌گرایی نسبتاً بالایی که دارد، مورداستفاده قرار می‌گیرد. این الگوریتم باوجود عمر کمی که دارد، اما توانسته است در حوزه‌های کاربردی بسیاری، از الگوریتم‌های قدیمی‌تر، مانند الگوریتم ژنتیک، پیشی بگیرد و به‌عنوان انتخاب اول محسوب شود.

PSOیکی از روش‌های بهینه‌سازی الهام گرفته از طبیعت است که برای حل مسائل بهینه‌سازی عددی با فضای جستجوی بسیار بزرگ بدون نیاز به اطلاع از گرادیان تابع هدف ابداع‌شده

*رایانامه نویسنده مسئول: rsaadati@iust.ac.ir

1- Particle swarm optimization

است. در الگوریتمPSO از این نظر که جمعیتی از جواب‌ها به‌طور تصادفی توسط الگوریتم تولیدشده و با حرکت در دامنه مسئله به دنبال جواب می‌گردند، مشابه الگوریتم ژنتیک است. بااین‌حال در الگوریتم PSO برخلاف الگوریتم ژنتیک به هر یک از جواب‌های بالقوه مسئله بهینه‌ساز (ذرات) یک سرعت(Velocity) تصادفی نیز نسبت داده می‌شود به‌طوری‌که در هر تکرار هر ذره با توجه به مقدار سرعتش در فضای مسئله جابه‌جا می‌شود. هم‌چنین، برخلاف الگوریتم ژنتیک، در الگوریتمPSO باید بهترین جواب به‌دست‌آمده برای مسئله بهینه‌سازی (از آغاز اجرای برنامه تا آخرین تکرار) توسط هر یک از ذرات نیز ذخیره‌سازی شود. الگوریتم PSO نیز همانند الگوریتم ژنتیک ذاتاً برای حل مسائل بیشینه‌سازی بدون قید در حالت پیوسته مناسب است. بااین‌حال می‌توان انجام تغییراتی در نحوه تعریف تابع هدف، از آن برای حل مسائل بهینه‌سازی (اعم از کمینه‌سازی یا بیشینه‌سازی) در حالت تحت قید (پیوسته) نیز استفاده کرد. اساس کار الگوریتم PSO را می‌توان چنین توضیح داد:

ابتدا در فضای جستجوی موردنظر تعدادی نقطه به‌عنوان جمعت اولیه انتخاب می‌شود. نقاط بر اساس فاصله اقلیدسی در دسته‌های مختلف قرار می‌گیرند. به‌این‌ترتیب در هر دسته بهترین نقطه مشخص می‌گردد. از طرف دیگر با در دسترس بودن اطلاعات گذشته هر عامل، می‌توان بهترین نقطه‌ای که تاکنون توسط آن کشف‌شده است را مشخص کرد. به‌این‌ترتیب اطلاعات نقطه بهینه هر دسته و هر عامل مشخص می‌گردند. دانش اول متناظر با نقطه بهینه سراسر در هر گروه و دانش دوم متناظر با نقطه بهینه محلی است. با داشتن این اطلاعات، هر عامل در راستای بردار زیر حرکت داده می‌شود. این روش به‌وسیله ابعاد و غیرخطی بودن مسئله خیلی تحت تأثیر قرار نگرفته و نتایج خوبی در محیط‌های استاتیک، نویزی و محیط‌های به‌طور پیوسته در حال تغییر،به دست می‌آورد. این ویژگی‌ها به‌علاوه سادگی پیاده‌سازی، عدم الزام بر پیوستگی تابع هدف و توانایی وفق دادن به محیط پویا باعث شده که این الگوریتم در حوزه‌های بسیار مختلفی به‌کاربرده شود [۵-۴].

بر این اساس، می‌توان نتیجه گرفت که ماهیت رفتار هدفمند ذرات درروش PSO بر اساس دو اصل استوار است که این دو اصل عبارت‌اند از:

۱) دانش فردی: بر این اساس، هر فرد به سمت بهترین دانش قبلی خود حرکت می‌کند که دانش جدیدی به دست آورد.

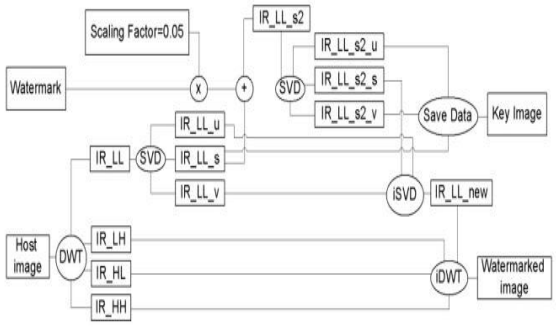
۲) دانش اجتماعی: بر این اساس، فرد برحسب نوع ارتباط خودش با جامعه از بهترین اطلاعات دیگران برای ادامه حرکت استفاده می‌کند.

۳- روش پیشنهادی نهان‌نگاری در حوزه موجک

در این تحقیق، یک روش نهان‌نگاری غیرقابل مشاهده و مبتنی بر روش SVD[1] چندگانه در حوزه موجک که از الگوریتم PSO جهت افزایش استحکام استفاده‌شده است، پیشنهاد می‌گردد. در الگوریتم پیشنهادی، تصویر میزبان I و تصویر نهان‌نگاری W و تصویر نهان‌نگاری‌شده I^w نامیده شده است و محدودیتی در اندازه تصویر میزبان و watermark وجود ندارد زیرا در هنگام قرار دادن تصویر نهان‌نگاری داخل تصویر میزبان، تصویر نهان‌نگاری تغییر اندازه داده و هم‌اندازه با زیرباند LL تصویر میزبان می‌گردد هم‌چنین در این روش، تصویر نهان‌نگاری و تصویر میزبان می‌تواند رنگی (RGB[2]) باشد[6,7].

۳-۱- الگوریتم جاسازی کردن تصویر نهان‌نگاری

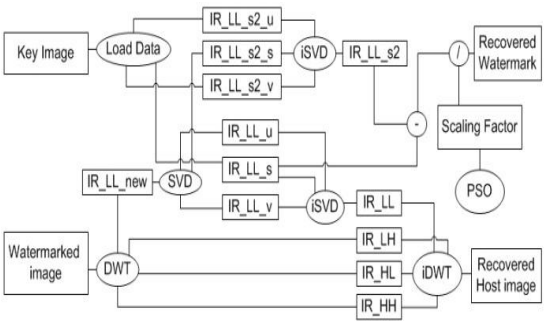
الگوریتم جاسازی کردن تصویر نهان‌نگاری در شکل (۱) نشان داده می‌شود.



شکل (۱):الگوریتم جاسازی watermark در تصویر میزبان

۳-۲- الگوریتم استخراج watermark

الگوریتم استخراج تصویر نهان‌نگاری در شکل (۲) نشان داده می‌شود.



شکل (۲): الگوریتم استخراج watermark از تصویر میزبان

فلوچارت الگوریتم پیشنهادی به همراه الگوریتم PSO جهت استخراج کردن watermark بر روی تصویر موردحمله قرارگرفته به‌صورت شکل (۳) است.

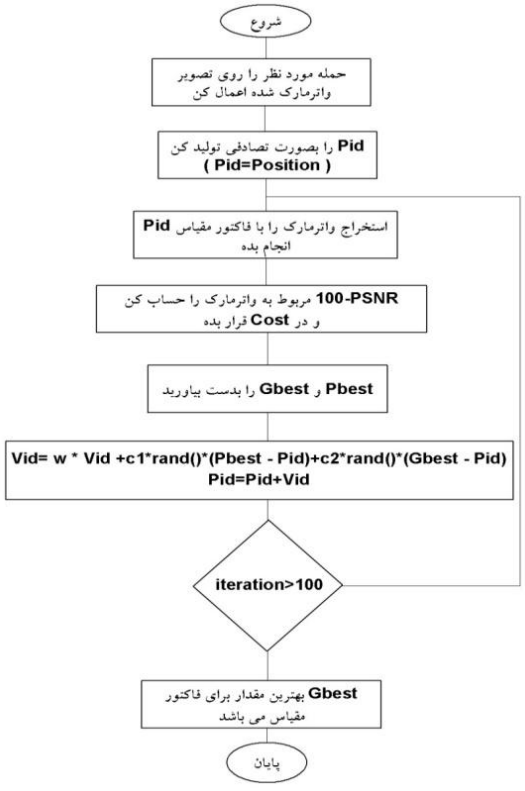
1- singular value decomposition
2- Red Green Blue

برای بررسی کیفیت تصاویر نهان‌نگاری پس از فرآیند نهان‌نگاری و اعمال حملات بر روی آن‌ها، روش‌های متعددی وجود دارد. یکی از روش‌های رایج اندازه‌گیری، PSNR[1] یا اوج نسبت وزن سیگنال به نویز و MSE[2] میانگین مربع خطاها است که در آن کیفیت بصری تصویر نهان‌نگاری استخراج‌شده W' و تصویر نهان‌نگاری اصلی موردبررسی قرار می‌گیرد. محاسبه PSNR با استفاده از رابطه زیر انجام می‌شود :

$$MSE(W,W') = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}(W(i,j) - W'(i,j))^2 \qquad (۱)$$

$$PSNR(W,W') = 10log_{10}\frac{255^2}{MSE(W,W')} \qquad (۲)$$

برای تصاویر با عمق ۸ بیت، مقدار معمول برای PSNRعددی بین ۳۰db و ۵۰db در واحد Decibel است. که این مقدار هرچه بیش‌تر باشد بهتر است. برای تصاویر با عمق ۱۶ بیت این مقدار بین ۶۰db تا ۸۰db است. درصورتی‌که تصویر watermark و تصویر watermark استخراج‌شده دقیقاً شبیه به هم باشند (اصلاً نویز وجود نداشته باشد) مقدار MSEبرابر صفر خواهد بود پس مقدار PSNRتعریف‌نشده است (تقسیم‌بر صفر) [۸].



شکل (۳): فلوچارت الگوریتم پرندگان در الگوریتم پیشنهادی.

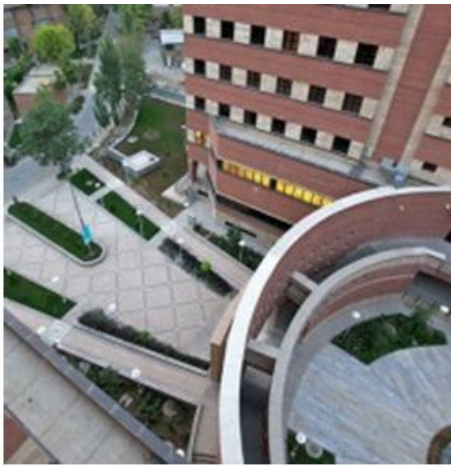
1- peak signal-to-noise ratio
2- Mean Square Error

۴- نتایج پیاده‌سازی

برای آزمایش طرح نهان‌نگاری مبتنی بر SVD چندگانه پیشنهادشده، از یک تصویر رنگی RGB شکل (۵) با اندازه ۵۱۲×۵۱۲ پیکسل به‌عنوان تصویر میزبان I و یک تصویر رنگی RGB شکل (۴) با اندازه ۶۴×۶۴ پیکسل به‌عنوان تصویر نهان‌نگاری W استفاده‌شده است.شکل (۶) تصویر نهان‌نگاری‌شده می‌باشد.

شکل (۴): تصویر نهان‌نگاری

شکل (۵): تصویر میزبان



شکل (۶): تصویر نهان‌نگاری‌شده

در این قسمت نقش الگوریتم PSO در روش پیشنهادی را در استحکام watermark در برابر انواع حملات موردبررسی قرار می‌دهیم. در این روش پیشنهادی، در زمان جاسازی تصویر نهان‌نگاری از فاکتور مقیاس ۰/۰۵ استفاده می‌کند ولی در زمان استخراج تصویر نهان‌نگاری، از الگوریتم PSO جهت به دست آوردن بهینه‌ترین مقدار فاکتور مقیاس کمک می‌گیرد. در جداول زیر نشان داده‌شده است که با استفاده از الگوریتم PSO می‌توان مقدار PSNR را افزایش داد و خروجی به نسبت بهتری را داشت.

جدول (۱): نقش الگوریتم PSO در روش پیشنهادی با حمله salt & pepper Noise ۰/۰۲

watermark	تصویر اصلی / تصویر موردحمله قرارگرفته	با استفاده از الگوریتم PSO			بدون استفاده از الگوریتم PSO		
		Watermark استخراج شده	PSNR	فاکتور مقیاس به دست آمده	Watermark استخراج شده	PSNR	فاکتور مقیاس
			30.5122	0.0462		26.4290	0.05
			30.5122	0.0450		26.0624	0.05
			27.2615	0.0484		26.3084	0.05

جدول (۲): نقش الگوریتم PSO در روش پیشنهادی با حمله Croping به اندازه ۱۰۰ پیکسل از چپ.

watermark	تصویر اصلی / تصویر مورد حمله قرار گرفته	با استفاده از الگوریتم PSO			بدون استفاده از الگوریتم PSO		
		Watermark استخراج شده	PSNR	فاکتور مقیاس به دست آمده	Watermark استخراج شده	PSNR	فاکتور مقیاس
			24.3508	0.0482		19.3012	0.05
			23.8884	0.0453		18.5847	0.05
			24.1934	0.0447		20.5383	0.05

جدول(۳): نقشه الگوریتم PSO درروش پیشنهادی باحمله Rotation 25°

watermark	تصویر اصلی / تصویر مورد حمله قرار گرفته	با استفاده از الگوریتم PSO			بدون استفاده از الگوریتم PSO		
		Watermark استخراج شده	PSNR	فاکتور مقیاس به دست آمده	Watermark استخراج شده	PSNR	فاکتور مقیاس
			25.8649	0.0482		25.1169	0.05
			24.9449	0.0470		24.0983	0.05
			25.4178	0.0499		25.4112	0.05

جدول (۴): نقش الگوریتم PSO در روش پیشنهادی با حمله ۰/۱ Gaussian Noise

watermark	تصویر اصلی / تصویر مورد حمله قرار گرفته	با استفاده از الگوریتم PSO			بدون استفاده از الگوریتم PSO		
		Watermark استخراج شده	PSNR	فاکتور مقیاس به دست آمده	Watermark استخراج شده	PSNR	فاکتور مقیاس
			28.6918	0.0450		11.7680	0.05
			29.4280	0.0440		13.3441	0.05
			25.0311	0.0485		12.7552	0.05

با توجه به جداول فوق و انواع مختلف حملاتی که بر روی تصاویر watermark شده اعمال‌شده، به این نتیجه می‌رسیم که با استفاده از الگوریتم PSO می‌توانیم بهینه‌ترین مقدار فاکتور مقیاس را پیداکرده تا بهترین مقدار PSNR به‌دست بیاید.

۵- نتیجه‌گیری

با توجه به جداول بخش ۴ مشاهده می‌شود که با استفاده از الگوریتم PSO می‌توانیم بهینه‌ترین مقدار فاکتور مقیاس را

پیداکرده تا بهترین مقدار PSNR به‌دست بیاید. در حالت کلی، هرچه مقدار PSNR بیش‌تر باشد شباهت بین تصویر نهان‌نگاری‌شده و تصویر نهان‌نگاری استخراج‌شده بیش‌تر است. پس انتخاب یک فاکتور مقیاس مناسب، نقش به‌سزایی در استحکام watermark دارد. هم‌چنین استحکام الگوریتم در حملات مختلف باهم فرق دارد ولی می‌توان مقدار فاکتور مقیاس را طوری انتخاب کرد که تصویر watermark شده در برابر انواع مختلف حملات بیش‌ترین استحکام را داشته باشد.

۶- مراجع

[1] N. Mahmoodabadi, V. VahidAbdolmaleki,and M. Mekdad, "Watermarking Confidential Information By Substitutions Permutations Least Significant Bit," The Fifth National Conference of Command and Control, 1392.(In Persian)

[2] A. Ghafoor and M. Imran, "A Non-blind Color Image Watermarking Scheme Resistent against Geometric Attacks," Radioengineering, vol. 21, no. 4, 2012.

[3] A. A. Mohammad, A. Alhaj, and S. Shaltaf, "An improved SVD-based watermarking scheme for protecting rightful ownership. Elsevier - Signal Processing," vol. 88, pp. 2158– 2180, 2008.

[4] A. Agarwal, N. bora, and N. Arora, "Goodput Enhanced Digital Image Watermarking Scheme Based on DWT and SVD," IJAIEM, vol. 2, Issue 9, 2013.

[5] A. K. Gupta, M. S. Raval, "A robust and secure watermarking scheme basedon singular values replacement," Sadhana, vol. 37, Part 4, pp. 425-440, 2012.

[6] H. Biao-Bing and T. Shao-Xian, "A contrast sensitive visible watermarking scheme," IEEE Multimedia, vol. 13, no. 2, pp. 60-67, 2006.

[7] S. Shanmugaprabha and N. Malmurugan, "A New Robust Image Watermarking Scheme Based On DWT With SVD," IJASCSE, vol. 3, Issue 4, 2014.

[8] HTTP://en.wikipedia.org/wiki/Peak_signal-to-noise_ratio

مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"
ویژه‌نامه کنفرانس بین‌المللی ترکیبیات، رمزنگاری و محاسبات، ص ۱۲۵ -۱۱۷

بهینه‌سازی محافظت از شبکه در برابر خط‌مشی‌های ممانعتی متنوع از طریق الگوریتم‌های تکاملی

وحید خرازی*

دانشگاه علم و صنعت ایران

(دریافت: ۹۵/۰۷/۰۵، پذیرش: ۹۶/۰۳/۰۶)

چکیده

هدف ما در این مقاله ارائه یک قالب بهینه‌سازی شبکه است که پایداری شبکه را برای یک جریان مورد نیاز عرضه و تقاضا بیشینه می‌کند. در قالب ارائه‌شده یال حالت تصادفی دارد که با درنظرگرفتن آسیب‌پذیری یال با استفاده از تابع میزان موفقیت مهاجم- مدافع مشخص می‌شود. در این قالب، هدف ممانعت‌کننده کاهش بیشینه جریان مورد انتظار شبکه از طریق تخریب یال‌های شبکه است. به‌علاوه، فرض می‌شود ممانعت‌کننده دارای منابع محدودی برای ممانعت از عناصر شبکه باشد. در این مطالعه به‌دنبال پیداکردن احتمال تخریب یک عنصر شبکه بوده و سپس می‌خواهیم منابع دفاعی در بین اقدامات دفاعی مختلف مثلاً جدایی، حفاظت و افزونگی به طور مطلوب توزیع کنیم به نحوی که پایداری سامانه حداکثر شود. رویکردهای متفاوتی که برای حل این قالب ممانعت مطرح شده‌اند غالباً برای شبکه‌های با ابعاد کوچک محدود می‌شوند. ما در این مقاله یک الگوریتم تکاملی برای حل این مسائل ارائه می‌دهیم. نتایج عددی به دست آمده نشان می‌دهد که این الگوریتم تکاملی فضای جواب را به طور قابل توجهی محدود می‌کند و بنابراین می‌توان آن را در شبکه‌های با ابعاد بزرگ به کار برد.

واژه‌های کلیدی: ممانعت در شبکه، محافظت از سیستم، پایداری شبکه، بهینه‌سازی تکاملی

۱- مقدمه

یک شبکه با پیکربندی معلوم و ثابت، تعدادی مصرف‌کننده محصول یا تحویل‌گیرنده خدمات را در نظر بگیرید به‌عنوان مثال در موارد قانونی، برق و ارتباطات و در موارد غیرقانونی مواد مخدر یا قاچاق اسلحه چنین شبکه‌ای را تشکیل می‌دهند. در این تحقیق تأثیر رویدادهای خارجی (به‌عنوان مثال، ۱۱ سپتامبر ۲۰۰۱ در مورد حمل و نقل و ۲۰۰۳ در مورد خاموشی در شبکه برق شمال غرب ایالات متحده) بر از کار افتادن اجزا در سطح شبکه بررسی می‌شود. زیر ساخت‌های حیاتی می‌توانند به‌عنوان شبکه‌های ارتباطی یا خدماتی تعریف شوند که برای اقتصاد و رفاه اجتماعی یک ملّت حیاتی هستند. به‌عنوان مثال، زیرساخت انرژی یکی از زیر ساخت‌های حیاتی است، بدون یک منبع انرژی پایدار، بهداشت و رفاه مورد تهدید است و اقتصاد کشور نمی‌تواند موثر باشد. بدیهی است برای بخش انرژی، عملکرد مناسب شبکه برق باید به‌طور مداوم بالا نگه داشته شود که این امر در مورد نگهداری و ایمنی شبکه حمل و نقل نیز درست است. در خارج از آمریکا، اتحادیه اروپا همراه با دیگر مدیران ملی و فرا ملی، درحال حاضر به اهمیت مهندسی قابلیت اطمینان و امنیت سیستم[1] که مرتبط با زیرساخت‌های حیاتی است پی برده و از طریق پیاده‌سازی سیاست‌ها و برنامه‌های خاص، (به خصوص برنامه اروپا برای حفاظت از زیرساخت‌های حیاتی) سعی در اجرای آن دارد. به‌طور خلاصه، از دیدگاه امنیتی، اختلال یا تخریب زیرساخت‌ها می‌تواند ضربه شدید و ناتوان‌کننده‌ای بر دفاع، امنیت اقتصادی و رفاه روانی کشور تحمیل کند. با توجه به این زیرساخت‌ها، می‌توان شبکه را قالب‌بندی کرد. به‌عنوان مثال، زیر ساخت‌های انرژی می‌تواند به‌عنوان جریان شبکه یا مخابرات به‌عنوان شبکه ارتباطی قالب‌بندی شود. تحقیق در زمینه قابلیت اطمینان و تجزیه و تحلیل خطر از طریق پیاده‌سازی خط‌مشی‌های محافظتی برای کاهش عدم جریان شبکه می‌تواند از اتفاقات ناخواسته در سطح شبکه که توسط شکست منابع داخلی ایجاد می‌شود جلوگیری کند.

مسائل ممانعت در شبکه تنوع بسیاری دارند و تعداد زیادی از این قالب‌ها تاکنون مطرح شده‌اند. تمامی قالب‌ها براساس سه رویکرد اصلی: بهینه‌سازی ترکیباتی، برنامه‌ریزی تصادفی و نظریه بازی می‌باشند. دراین قالب ممانعت که ما در این مقاله بررسی می‌کنیم ممانعت از هر یال به احتمال $p \leq 1$ موفق خواهد بود و هدف مهاجم کمینه کردن بیشینه جریان مورد انتظار است. برای این نوع مسائل، مک مسترز و ماستین[2] در [۱] یک روش حل مربوط به شبکه‌های مسطح (شبکه‌هایی که یال‌ها هم‌دیگر را قطع

* رایانامه نویسنده مسئول: kharazi@comp.iust.ac.ir

1- Reliability Engineering and System Safety

2- Mc Master and Mustin

نمی‌کنند) را براساس برنامه‌ریزی خطی ارائه کرده‌اند. این روش به شمارش مجموعه‌ای از اجزا نیاز دارد که شکست شبکه را تضمین می‌کنند و فقط در شبکه‌های با اندازه کوچک کاربرد دارد. برای این نوع شبکه‌ها، هلم بولد[1] [۲] یک روش برنامه‌ریزی پویا را پیاده‌سازی کرده که در آن مسطح‌بودن شبکه فرض شده است. بنابراین، قابلیت کاربرد آن به شبکه‌های با ابعاد کوچک محدود می‌شود. بویل[2] [۳] یک روش دوگان بسط‌یافته براین قالب در نظر گرفته است. این شیوه تمام مسیرهای s – t را که از بین می‌روند را می‌شمارد. هم‌چنین، وود[3] [۴] نشان داد که DNIP[4] یک NP- کامل است و یک قالب تازه از LP را ارائه کرد که توسط برنامه‌ریزی عدد صحیح حل می‌شود. با این‌حال این رویکرد در شبکه‌های با اندازه تقریباً کوچک اجرا شده بود. دای و پو[5] [۵] برای مواجه‌شدن با این محدودیت‌ها نخستین روش بهینه‌سازی تکاملی را برای حل مسائل DNIP ارائه کرده‌اند. این الگوریتم ژنتیک GA[6] می‌تواند جواب‌هایی برای شبکه‌های بزرگ تولید کند. با این‌حال، بایستی از مفاهیم مربوط به عملگر پیوند، جهش، جریمه و هم‌چنین پیش‌زمینه مناسبی در GA استفاده کرد. اخیراً راکو و رامیرز مارکز[7] در [۶]، PSDA[8] را ارائه کرده‌اند که یک الگوریتم تکاملی برای حل مسائل DNIP است. این الگوریتم فضای جواب را در یک جستجوی احتمالی مورد کاوش قرار می‌دهد.

۱-۱- تعریف مساله

اگرچه یکی از بی‌نهایت خط‌مشی‌های حمله‌ای توسط ممانعت‌کننده را می‌توان در نظر گرفت. در این تحقیق فرض بر این است که مهاجم منابع‌اش را به‌طور مساوی در میان تمام اجزای شبکه توزیع می‌کند. این فرض در مورد توزیع مساوی منابع در موارد زیر قابل توجیه است:

(a) مهاجم هیچ اطلاعی درباره ساختار شبکه و اهمیت یال‌های خاص ندارد و برای از بین‌بردن تمامی عناصر شبکه تلاش می‌کند.

(b) مهاجم هیچ توانایی برای هدایت حمله به یال‌های خاص را ندارد. به‌عنوان مثال، در استفاده از آلات موشکی با دقت پایین، مهاجم تلاش می‌کند به کل منطقه آسیب برساند و تنها بر حسب تصادف می‌تواند یالی را تخریب کند که تجهیزات زیادی در آن قرار گرفته است.

(c) سیستم نیازمند حفاظت در برابر بلایای طبیعی از قبیل سیل، طوفان و غیره است که کل منطقه را تخریب می‌کنند.

مفروضات این قالب به صورت زیر است:

- ظرفیت تمام یال‌ها مشخص است.
- تقاضای شبکه و پیکربندی- شبکه ثابت و مشخص است.
- بودجه مدافع و مهاجم معلوم است.
- بودجه حمله به‌طور مساوی در میان همه یال‌ها توزیع شده است.
- مهاجم یال‌های بدون محافظت را با احتمالی برابر با یک تخریب می‌کند.

جدول (۱): فهرست علائم و اختصارات استفاده‌شده در مقاله

$G(N,A)$	شبکه ظرفیت دار
$\boldsymbol{x}$	بردار خط‌مشی دفاعی= $\boldsymbol{x}=(x_{s1},\dots,x_{st},x_{12},\dots,x_{1n},\dots,x_{ij},\dots,x_{nt})$
x_{ij}	متغییر تصمیم‌گیری باینری، اگر یال شبکه بین گره‌های i و j دفاع شود $(x_{ij}=1)$ و در غیر این صورت $(x_{ij}=0)$
$\mathbf{x_u^h}$	h امین خط‌مشی دفاعی در چرخه u ام $\boldsymbol{x_u^h}=(x_{s1u}^h,\dots,x_{snu}^h,\dots,x_{12u}^h,\dots,x_{1nu}^h,\dots,x_{jhu}^h,\dots,x_{ntu}^h)$
$\boldsymbol{\gamma_u}$	بردار احتمال $\boldsymbol{\gamma_u}=(\gamma_{s1u},\dots,\gamma_{snu},\gamma_{12u},\dots,\gamma_{1nu},\dots,\gamma_{iju},\dots,\gamma_{ntu})$
γ_{ij}	احتمال این‌که از یال بین گره‌های i و j دفاع شود $P(x_{ij}=1)$
$\boldsymbol{k_{ij1}}$	مولفه جریان بین گره‌های i و j
v_{ij}	احتمال تخریب یال بین گره‌ها i و j
t_{ij}^m	منابع دفاعی اختصاص‌یافته برای هر یال بین گره‌های i و j
T_{ij}^m	منابع تهاجمی اختصاص‌یافته برای هر یال بین گره‌های i و j
m	پارامتر میزان درگیری
a	بردار وضعیت $\boldsymbol{a}=(a_{s1},\dots,a_{st},a_{12},\dots,a_{ij},\dots,a_{nt})$
b	بودجه تدافعی
B	بودجه تهاجمی
$\boldsymbol{\varphi(a)}$	جریان شبکه تحت بردار وضعیت a
$R(\boldsymbol{a}\|\boldsymbol{x'},d,v_{ij})$	پایداری شبکه تحت بردار خط‌مشی x' برای جریان داده شده d
d	جریان مورد نیاز شبکه
u	اندیس دور
S	اندازه مجموعه جواب
$\boldsymbol{x^*}$	بردار خط‌مشی دفاعی بهینه
$\vee$	عملگر یای منطقی

1- Helmbold
2- Boyle
3- Wood
4- Deterministic Network Interdiction Problem
5- Dai and Poh
6- Genetic Algorithm
7- Rocco and Ramirez-Marquez
8- Probabilistic Solution Discovery Algorithm

۱-۲- پیش‌زمینه حفاظت از شبکه‌ها

$G(N,A)$ را یک شبکه ظرفیتی با گره منبع s و گره تقاضا t در نظر بگیرید که N مجموعه‌ای از گره‌ها است و $A = A_1 \cup A_2$ که $A_1 = \{(s,i),(j,t)|1 < i,j < n\}$ و $A_2 = \{(i,j)|1 < i,j < n\}$ مجموعه‌ای از یال‌ها هستند. شبکه به ترتیب دارای بودجه تدافعی و تهاجمی b و B است. به علاوه، k_{ijv} یک عضو از $\boldsymbol{k_{ij}}$ است که بردار ظرفیت یال (i,j) را نمایش می‌دهد. برای این بردارها داریم $v = 0,1$ و $0 = k_{ij0} < k_{ij1}$. بردار وضعیت شبکه $\boldsymbol{a} = (a_{s1}, \dots, a_{st}, a_{12}, \dots, a_{ij}, \dots, a_{nt})$ ظرفیت جریان برای هر یال از شبکه است.

۱-۳- آسیب‌پذیری یال

آسیب‌پذیری یک یال شبکه v_{ij} (یعنی همان احتمال تخریب) به صورت نسبت تابع موفقیت [۸-۷] در رقابت مهاجم- مدافع به شکل:

$$v_{ij} = \frac{T_{ij}^m}{T_{ij}^m + t_{ij}^m}$$

تعریف می‌شود که در آن t_{ij}^m و T_{ij}^m به ترتیب بودجه تدافعی و تهاجمی اختصاص‌یافته به یال است و پارامتر m میزان درگیری به شرح زیر است:

۱) اگر $m = 0$، تلاش مهاجم و مدافع تأثیر یکسانی بر آسیب‌پذیری دارد.

۲) اگر $0 < m < 1$، نشان از یک عدم تناسب برتری ناشی از سرمایه‌گذاری کم‌تر از حریف دارد.

۳) اگر $1 < m < \infty$، نشان از یک عدم تناسب برتری برای سرمایه‌گذاری بیش‌تر از منابع حریف دارد.

۴) اگر $m = 1$، هر سرمایه‌گذاری تأثیر متناسب با آسیب‌پذیری اجزا دارد.

بنا بر توضیحات داده شده، در این قالب فرض بر این است که مهاجم منابعش را به طور مساوی در میان همه یال‌ها به طور مساوی توزیع می‌کند. بنابراین، $T_{ij} = B/|A|$. به‌علاوه بردار $\boldsymbol{x} = (x_{s1}, \dots, x_{st}, x_{12}, \dots, x_{1n}, \dots, x_{ij}, \dots, x_{nt})$ یک خط‌مشی دفاعی است به‌طوری‌که عنصر x_{ij} مقداری برابر با یک $(x_{ij} = 1)$ دارد اگر یال (i,j) به‌عنوان بخشی از خط‌مشی دفاعی تعریف‌شده باشد و مقدار صفر $(x_{ij} = 0)$ اگر دفاع نشود. در نتیجه، بردار خط‌مشی دفاعی مشخص می‌کند از کدام یال‌ها دفاع شود و چون در مفروضات این قالب بودجه دفاعی‌اش را به‌طور مساوی در میان یال‌های انتخاب‌شده برای دفاع پخش می‌کند، بنابراین داریم:

$$t_{ij}^m = \begin{cases} 0 & x_{ij} = 0 \\ \dfrac{b}{\sum_{ij} x_{ij}} x_{ij} & x_{ij} = 1 \end{cases}$$

جدول (۲): احتمال دقیق جریان s-t برای خط‌مشی‌های دفاعی مختلف

Defense strategy no.	Defense strategy (x_{s2}, x_{st}, x_{2t})	$(P(\varphi(a) = f\|x, v_{ij}\|)$				Expected flow
		$f = 0$	$f = 10$	$f = 100$	$f = 110$	
1	(0,0,0)	1	0	0	0	0
2	(1,0,0)	1	0	0	0	0
3	(0,1,0)	0.20	0.80	0	0	8
4	(0,0,1)	1	0	0	0	0
5	(1,1,0)	0.33	0.67	0	0	6.7
6	(1,0,1)	0.55	0	0.45	0	45
7	(0,1,1)	0.33	0.67	0	0	6.7
8	(1,1,1)	0.28	0.39	0.14	0.19	38.8

۱-۴- پایداری شبکه

تابع $\varphi(a): Z^{|A|} \to Z^+$ یک بردار حالت شبکه را به یک جریان شبکه بین $s-t$ می‌نگارد. بنابراین، پایداری شبکه تحت خط‌مشی دفاعی بردار x'، جریان داده‌شده d و آسیب‌پذیری‌های v_{ij} به‌صورت زیر تعریف می‌شود:

$$R(\boldsymbol{a}|\boldsymbol{x}', d, v_{ij}) = P(\varphi(\boldsymbol{a}) \geq d|\boldsymbol{x}', v_{ij})$$

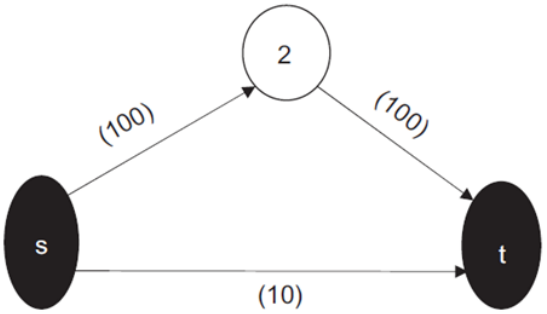
۱-۵- مثال تشریحی

برای روشن‌نمودن مفاهیم ذکرشده، همان‌طور که در شکل (۱) مشاهده می‌شود یک مثال در نظر گرفته‌ایم که در اصل توسط کرمیکن[1] و همکارانش در [۹] ارائه شده است. این شبکه ساده شامل یک گره منبع s و یک گره تقاضا t و گره میانی 2 است. مقدار بالای هر یال نشان‌دهنده ظرفیت آن یال است. فرض کنید برای این شبکه میزان درگیری $m = 1$ و بودجه تدافعی و تهاجمی به ترتیب b = ۴۰ و B = ۳۰ است.

برای این مثال، احتمال این‌که شبکه جریانی برابر با f داشته باشد را برای هر یک از خط‌مشی‌ها دفاعی ممکن نمایش می‌دهد.

1- Cormican

توجه داشته باشید که جریان شبکه تابعی از آسیب‌پذیری هریک از یال‌ها و نیز خط‌مشی دفاعی است. به‌عنوان مثال، برای خط‌مشی دفاعی نخست $T_{ij}^{m}=10$ و $t_{ij}^{m}=0$ به‌طوری‌که $v_{ij}=1$ برای هر یال (i,j) است. به طور مشابه در ششمین خط‌مشی دفاعی فقط دو یال حفاظت شده‌اند. در این دفاع، $T_{ij}^{m}=10$ و $t_{ij}^{m}=40/2=20$ به‌طوری‌که $v_{ij}=1/3$ برای یال‌های دفاع شده $(s,t$ و $2,t)$ و $v_{ij}=1$ برای یال دفاع نشده (s,t) است. در این مثال احتمال این‌که شبکه نتواند هیچ جریانی را انتقال دهد با درنظرگرفتن احتمال تخریب یال‌های x_{s2} و x_{2t} برابر با $1/3+1/3-1/9=0.55$ است. هم‌چنین احتمال این‌که جریان انتقالی برابر با ۱۰۰ واحد باشد را می‌توان به‌عنوان احتمال این‌که هر دو یال بعد از حمله باقی بمانند به دست آورد.



شکل (۱): مثال تشریحی

به‌علاوه، نتایج به ما اجازه مقایسه خط‌مشی‌های دفاعی مختلف و معیارهای بهینه‌سازی متفاوت را می‌دهد. به‌عنوان‌مثال، جواب بهینه می‌تواند s امین خط‌مشی باشد اگر هدف ماکزیمم کردن جریان مورد انتظار شبکه از گره منبع به گره مقصد باشد. بااین‌حال، اگر مدافع بخواهد خط‌مشی را انتخاب کند که جریان شبکه بیش‌تر یا مساوی ۱۰ واحد (به عنوان یک سطح اطمینان) باشد آن‌گاه سومین خط‌مشی، جواب بهینه است.

برای این قالب شبکه، محاسبه پایداری شبکه برای خط‌مشی دفاعی بردار x و جریان مورد نیاز شبکه d در $G(N,A)$ از طریق روش تحلیلی مشخص کرده مجموعه‌های مسیر/ برش کمینه ظرفیت‌دار [۱۱-۱۰] و یا یکی از روش‌های شبیه‌سازی [۱۳-۱۲] انجام می‌گیرد. چون محاسبه دقیق همه مجموعه‌های مسیر/ برش کمینه NP- سخت است و پیچیدگی محاسباتی با افزایش تعداد یال‌ها و گره‌های شبکه به طور نمایی افزایش می‌یابد. در این مقاله از شبیه‌سازی مونت‌کارلو برای تخمین $R(\boldsymbol{a}|\boldsymbol{x}',d,v_{ij})=P(\varphi(\boldsymbol{a})\geq d|\boldsymbol{x}',v_{ij})$ استفاده شده است.

به‌علاوه، نتایج به ما اجازه مقایسه خط‌مشی‌های دفاعی مختلف و معیارهای بهینه‌سازی متفاوت را می‌دهد. به‌عنوان‌مثال، جواب بهینه می‌تواند s امین خط‌مشی باشد اگر هدف ماکزیمم کردن جریان مورد انتظار شبکه از گره منبع به گره مقصد باشد. بااین‌حال، اگر مدافع بخواهد خط‌مشی را انتخاب کند که جریان شبکه بیش‌تر یا مساوی ۱۰ واحد (به عنوان یک سطح اطمینان) باشد آن‌گاه سومین خط‌مشی، جواب بهینه است.

۱-۶- قالب حفاظت بهینه از شبکه

تابع هدف در این قالب عبارت است از یک خط‌مشی دفاعی که پایداری شبکه را برای یک جریان به خصوص $s-t$ مورد نیاز شبکه در $G(N,A)$ به شکل:

$$\text{Max } R(\boldsymbol{a}|\boldsymbol{x}',d,v_{ij})$$
$$s.t.$$
$$(1)\ \ C(x)=b$$
$$(2)\sum_{i|x_{ij}}a_{ij}-\sum_{h|x_{jh}}a_{jh}=0\ \ \forall j\in N$$
$$(3)\ \ x_{ij}\in Bin(0,1)$$

را بیشینه می‌کند به طوری که:

۱) مجموعه هزینه دفاعی برای خط‌مشی دفاعی $\boldsymbol{x}$ برابر با بودجه دفاعی می‌باشد.

۲) جریان ورودی و خروجی هر گره تحت خط‌مشی دفاعی $\boldsymbol{x}$ باید برابر با صفر باشد.

۳) طبیعت دودویی متغیر تصمیم‌گیری $\boldsymbol{x}$ را نشان می‌دهد.

۲- روش تحلیل و ارائه نتایج

رویکرد تحقیق در این مسئله بر اساس سه گام زیر است:

۱) شبیه‌سازی مونت‌کارلو[1] برای به وجود آوردن خط‌مشی ممانعتی بالقوه؛

۲) الگوریتم فورد فولکرسون[2] [۱۴] برای ماکزیمم جریان $s-t$ شبکه؛

۳) الگوریتم تکاملی که ناحیه‌ای از فضای جواب را در هر چرخه براساس جستجوی احتمالی مورد کاوش قرار می‌دهد که از متناسب‌کردن جواب‌های تولیدشده به دست می‌آید؛

۲-۱- الگوریتم تکاملی PSDA

رویکرد بهینه‌سازی ارائه‌شده در این مقاله یک الگوریتم تکاملی (EA[3]) است که شباهت‌هایی با الگوریتم ژنتیک (GA) و بهینه‌سازی الگوریتم مورچگان (ACO[4]) دارد. در رابطه با الگوریتم ژنتیک،

1- Monte-Carlo Simulation
2- Ford-Fulkerson
3- Evolutionary Algorithm
4- Ant Colony Optimization Algorithms

تفاوت اساسی این است که الگوریتم حول محور مراحل مربوط به تولید نسل (انتخاب والدین، پیوند و جهش) نیست. در این الگوریتم ناحیه‌ای از فضای جواب براساس جستجوی احتمالی مورد کاوش قرار می‌گیرد که این احتمال از متناسب‌کردن جواب‌های تولیدشده در هر دور به دست می‌آید. هم‌چنان که روند الگوریتم پیش می‌رود ناحیه مورد جستجو به سمت جواب‌های بهتر سوق پیدا می‌کند. به عنوان تفاوت با الگوریتم مورچگان، الگوریتم ارائه‌شده فضای جواب را با استفاده از تابع جریمه و بهترین جواب‌های به‌دست‌آمده در هر دور به‌روزرسانی می‌کند. مانند دیگر الگوریتم‌های تکاملی PSDA برای تمامی مسائل هم‌گرا نیست [۱۵]. با این حال، طبیعت احتمالی PSDA باعث می‌شود ناحیه‌ای از فضای جواب را جستجو کند که جواب‌هایی با کیفیت بالا دارد. این الگوریتم تکاملی ثابت شده است که جواب‌هایی با کیفیت بالا برای انواع مختلف ممانعت در شبکه‌ها [۱۶]، تخصیص قابلیت اطمینان [۱۷]، بازرسی محتوا [۱۸] و شبکه‌های بی‌سیم [۱۹] دارد. در این رابطه برونز[1] [۲۰] یک شیوه مشابه برای کاوش فضای جواب از طریق تراکم مرزی برای حل مسائل بهینه‌سازی مقید ارائه کرده است. امتیاز PSDA این است که تنها به سه پارامتر برای به دست آوردن جواب بهینه نیاز دارد.

۲-۲- ایجاد خط‌مشی

در این گام، یک تعداد به خصوص (SAMPEL) از خط‌مشی‌های دفاعی $\boldsymbol{x_u^h} = (x_{s1u}^h, \dots, x_{snu}^h, \dots, x_{12u}^h, \dots, x_{1nu}^h, \dots, x_{jhu}^h, \dots, x_{ntu}^h)$ را با استفاده از شبیه‌سازی مونت کارلو و براساس احتمال دیکته‌شده توسط بردار احتمال:

$$\boldsymbol{\gamma_u} = (\gamma_{s1u}, \dots, \gamma_{snu}, \gamma_{12u}, \dots, \gamma_{1nu}, \dots, \gamma_{iju}, \dots, \gamma_{ntu})$$

تولید می‌کنیم. مؤلفه $\boldsymbol{\gamma_u}$ از γ_{iju} برابر با احتمال این است که یال (i,j) به عنوان بخشی از خط‌مشی دفاعی انتخاب شود، $\gamma_{iju} = p(x_{iju}^h = 1)$. این گام هم‌چنین تعیین می‌کند که الگوریتم چه موقع خاتمه یابد.

الگوریتم زمانی متوقف می‌شود که بردار γ_u دیگر نمی‌تواند به‌روزرسانی شود، یعنی همه مؤلفه‌های γ_u صفر یا یک هستند. شبه کد الگوریتم برای این گام به‌صورت زیر است:

Step 1—Strategy development:
For $h = 1, \dots,$ SAMPLE
{For $i = 1, \dots, n$ and $j = 1, \dots, n$ implement MC simulation and as dictated by γ_u generate a network defense design $\mathbf{x}_u^h = (x_{s1u}^h, \dots, x_{snu}^h, x_{12u}^h, \dots, x_{1nu}^h, \dots, x_{iju}^h, \dots, x_{ntu}^h)$
$h \to h+1$;}
if $(\gamma_{iju} = 1 \vee \gamma_{iju} = 0 \ \forall\ i, j) \vee u = U$, then Stop, $x^* = \arg\max\{K\}$.
else go to step 2.

۲-۳- تجزیه و تحلیل خط‌مشی

در گام دوم، الگوریتم تعداد یال‌ها دفاع‌شده برای هر $\mathbf{x_u^h}$ را بررسی می‌کند و سپس پایداری شبکه $R(\boldsymbol{a}|\boldsymbol{x_u^h}, d, v_{ij})$، را برای هر خط‌مشی دفاعی $\boldsymbol{x_u^h}$ بر اساس بردارهای k_{ij} و v_{ij} تخمین می‌زند. تعداد زیادی از روش‌ها برای به دست آوردن $R(\boldsymbol{a}|\boldsymbol{x_u^h}, d, v_{ij})$ وجود دارد. در این مقاله از روش شبیه‌سازی مونت کارلو همراه با الگوریتم فورد فولکرسون براساس مقاله [۱۴] برای تخمین پایداری یک خط‌مشی دفاعی استفاده شده است.

برای یک خط‌مشی دفاعی به خصوص $\mathbf{x_u^h}$، بردار تصادفی $\mathbf{x_u'^h}$ را با درنظرگرفتن این‌که کدام یال‌ها برای دفاع انتخاب شده‌اند و آسیب‌پذیری آن‌ها تولید می‌کنیم. سپس این بردار توسط الگوریتم فورد فولکرسون برای مشخص‌کردن ماکزیمم جریان مورد ارزیابی قرار می‌گیرد. وقتی‌که ماکزیمم جریان بیش‌تر یا برابر با مقدار جریان مورد نیاز برای پایداری شبکه d باشد، $\mathbf{x_u'^h}$ به عنوان یک وضعیت موفق محسوب می‌شود و شمارنده تعداد وضعیت‌های موفق سیستم یک واحد افزایش می‌یابد، در غیر این صورت، شمارنده بدون تغییر باقی می‌ماند. این روند $NSIMUL$ بار تکرار می‌شود. برای تخمین پایداری شبکه تعداد وضعیت‌های موفق سیستم را بر $NSIMUL$ تقسیم می‌کنیم. بعد از به‌دست‌آوردن پایداری شبکه برای هر خط‌مشی دفاعی، جواب‌های به‌دست‌آمده را از بزرگ به کوچک مرتب می‌کنیم. شبه کد الگوریتم برای این گام به‌صورت زیر است:

Step 2—Strategy Analysis and Penalization:
For $h = 1, \dots,$ SAMPLE
Obtain $t_{ij}^m = b/\Sigma_{ij}x_{ij}$ and estimate $R(\mathbf{a}|\mathbf{x}_u^h, d, v_{ij})$
List $R(\mathbf{a}|\mathbf{x}_u^h, d, v_{ij})$ by decreasing order of magnitude:
$R(\mathbf{a}|\mathbf{x}_u^{(1)}, d, v_{ij}) \geq R(\mathbf{a}|\mathbf{x}_u^{(2)}, d, v_{ij}) \geq \dots \geq R(\mathbf{a}|\mathbf{x}_u^{(\text{SAMPLE})}, d, v_{ij})$.

۲-۴- کاوش جواب

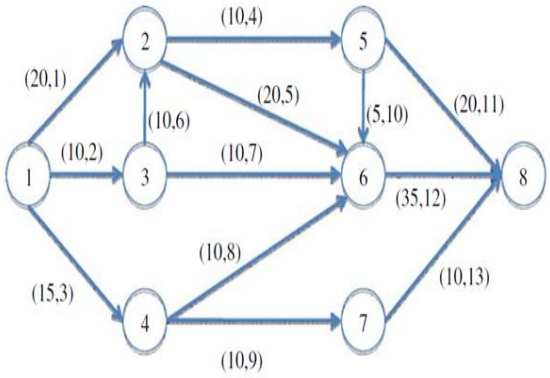
در سومین و آخرین گام از الگوریتم PSDA، یک زیرمجموعه مرتب از خط‌مشی‌های دفاعی برای به‌روز رسانی بردار احتمال γ_u مورد استفاده قرار می‌گیرد. این بردار جدید به گام نخست برای بررسی‌نمودن خاتمه الگوریتم یا برای هدایت کاوش تکاملی به سمت جواب‌های با کیفیت بالاتر فرستاده می‌شود. هم‌چنین در این گام تعداد به خصوص S از بهترین جواب‌های به‌دست‌آمده در چرخه در مجموعه K ذخیره می‌شود. شبه کد الگوریتم برای این گام به صورت زیر است:

Step 3—Solution Discovery
$\dots K \to K \cup R(\mathbf{a}|\mathbf{x}_u^{(1)}, d, v_{ij}) \geq R(\mathbf{a}|\mathbf{x}_u^{(2)}, d, v_{ij}) \geq \dots \geq R(\mathbf{a}|\mathbf{x}_u^{(\text{TOP})}, d, v_{ij}) \dots$
$u \to u+1$;
For $i = s,1, \dots, n$ and $j = 1, \dots, n$, t update vector γ_u as follows:
$\gamma_{iju} = (\Sigma_{k=1}^{S} x_{iju-1}^{(k)})/S$ where $S \ll$ SAMPLE;
Go to Step 1.

1- Berrones

۳- نتایج محاسباتی

برای نشان‌دادن رفتار PSDA برای مسئله حفاظت از شبکه از یک مثال استفاده می‌کنیم. شبکه‌ای که آن‌ها را مورد تجزیه و تحلیل قرار می‌دهیم در شکل (۲) مشاهده می‌شود، مقادیر بالای هر یال به ترتیب ظرفیت و اندیس آن‌ها نشان می‌دهد. برای مثال، یال بین گره‌های ۱ و ۲ دارای ظرفیت ۲۰ واحد و اندیس ۱ است. در این پیکربندی شبکه ماکزیمم جریانی که از گره منبع ۱ به گره چاهک ۲ می‌توان فرستاد ۴۵ واحد است. در این مثال فرض بر این است که مهاجم منابعش را میان تمام یال‌ها به طور مساوی تقسیم می‌کند و هیچ اطلاعی از پیکربندی شبکه و اهمیت یال‌های به خصوص ندارد. برای تشریح بهینه‌سازی قالب و راه‌حلش، سه جریان $d = (10,20,40)$، دو بودجه تهاجمی $B = (260,520)$، سه بودجه تدافعی $b = (130,650,1300)$ و سه میزان درگیری $m = (./3,1,3)$ در نظر گرفته شده است. برای این مثال پارامترهای مورد نیاز برای PSDA به صورت $SAMPEL = 50$، $U = 20$ و $S = 7$ در نظر گرفته شده است.



شکل (۲): یک مثال عددی برای تجزیه و تحلیل شبکه

نتایج به‌دست‌آمده از شرایط متفاوت در نظر گرفته‌شده در شکل (۲) نمایش داده شده است. این نتایج درک مناسبی از خط‌مشی دفاعی برای بیشینه‌کردن پایداری شبکه را فراهم می‌کنند. برای سه تقاضای شبکه نتایج به‌دست‌آمده بینش زیر را ارائه می‌دهند:

برای تقاضای ۱۰ واحد، پیکربندی شبکه افزونگی زیادی دارد و به مسیرهای گوناگون عرضه و تقاضا اجازه می‌دهد تا تقاضای شبکه را برآورده سازند. در این حالت، نتایج شکل (۲) نشان می‌دهند زمانی که بودجه تدافعی کم است، انتخاب خط‌مشی دفاعی بهینه براساس انتخاب یک مسیر عرضه و تقاضا (با اختصاص تمام منابع تدافعی به یال‌های این مسیر) و یا توزیع منابع در یال‌های گوناگون شبکه برای افزایش مختصر پایداری هریک از مسیرهای افزونه دیگر می‌باشد.

برای تشریح استدلال بالا سه حالت برای $B = 260$ در نظر می‌گیریم، اگر از تمام یال‌های شبکه حفاظت شود و $m = 1$ فرض شود. احتمال این‌که هر یال حفاظت‌شده تخریب نشود $(1 - v_{ij})$ به ترتیب بایستی برابر با ۰/۳۳۳۳، ۰/۷۱۴۳ و ۰/۸۳۳۳ باشد. براساس این آسیب‌پذیری‌ها، پایداری شبکه زمانی که از تمام یال‌های حفاظت شود به ترتیب برابر با ۰/۱۷۸۶، ۰/۸۵۸۹ و ۰/۹۶۹۸ است. طبق جدول (۳) پایداری شبکه برای خط‌مشی‌های دفاعی به ترتیب ۰/۳۳۱۵، ۰/۸۸۸۶ و ۰/۹۷۹۸ است. بنابراین جواب‌های به‌دست‌آمده توسط PSDA نشان می‌دهند که وقتی منابع تدافعی برای ایجاد افزونگی محدود هستند، منابع بایستی برای ماکزیمم‌کردن پایداری در یک مسیر عرضه- تقاضا (مسیر انتخابی شامل یال‌های شماره ۱، ۵ و ۱۲ برای b=۱۳۰) مورد استفاده قرار گیرند. هم‌چنان که منابع افزایش می‌یابند، چون آسیب‌پذیری عناصر (یال‌ها) کاهش می‌یابد، افزونگی پایداری تدافعی را بهبود می‌بخشد (همان‌طورکه مشاهده می‌کنید برای $b = 1300$ فقط از یال شماره ۱۰ حفاظت نشده است).

این استدلال هم‌چنین برای میزان بالای درگیری $m = 3$ نیز برقرار است. در این حالت وقتی منابع دفاعی یال افزایش می‌یابد، آسیب‌پذیری یال به‌سرعت کاهش می‌یابد. درنهایت برای حالتی که میزان درگیری پایین است، $m = 0.3$، زمانی که فقط از یک مسیر (به‌عنوان‌مثال ۱، ۵ و ۱۲) استفاده می‌کنیم آسیب‌پذیری یال‌ها بین ۰/۲۸۸۸ در بهترین حالت و ۰/۴۹۴۶ در بدترین حالت متغیر است، همواره از تخصیص منابع به یال‌های گوناگون به‌منظور ایجاد افزونگی استفاده می‌کنیم. در حقیقت وقتی میزان درگیری پایین است افزایش تلاش برای حفاظت از هر یال به خصوص تأثیر ناچیزی در کاهش آسیب‌پذیری آن یال دارد. بنابراین، فراهم‌نمودن افزونگی برای حفاظت از مسیرها (حفاظت از تعداد زیادی از یال‌ها) بسیار کاراتر از تخصیص منابع به تعداد کمی از یال‌ها است.

جدول (۳): نتایج محاسباتی به دست آمده در شرایط متفاوت

d	B	b	$m=1$			$m=0.3$			$m=3$	
			Non-defended links	Net.surv		Non-defended links	Net.surv		Non-defended links	Net.surv
۴۰	۵۲۰	۱۳۰	۸ ،۶	۰,۰۰۲۴		۴، ۶، ۸، ۱۰، ۱۱	۰/۰۰۲۴		NS*	۰,۰۰۰۰
		۶۵۰	۱۰ ،۶	۰,۰۲۷۴		۱۰	۰,۰۱۱۷		۴، ۶، ۸، ۱۰، ۱۱	۰,۴۱۹۹
		۱۳۰۰	۴، ۶، ۸، ۱۰، ۱۱	۰,۱۸۷۵		۱۰	۰,۰۲۲۵		۴، ۶، ۸، ۱۰، ۱۱	۰,۸۹۵۰
	۲۶۰	۱۳۰	۴، ۶، ۸، ۱۰، ۱۱	۰,۰۰۲۹		۱۰	۰,۰۰۴۶		NS*	۰,۰۰۰
		۶۵۰	۴، ۶، ۸، ۱۰، ۱۱	۰,۱۸۰۶		۱۰	۰,۰۲۴۱		۴، ۶، ۸، ۱۰، ۱۱	۰,۸۹۶۴
		۱۳۰۰	۴، ۶، ۸، ۱۰، ۱۱	۰,۴۰۶۲		۱۰	۰,۰۴۴۰		۴، ۶، ۸، ۱۰، ۱۱	۰,۹۸۹۳
۲۰	۵۲۰	۱۳۰	۲، ۳، ۴، ۶، ۷، ۸، ۹، ۱۰، ۱۱، ۱۳	۰,۱۵۲۰		۲، ۳، ۴، ۶، ۷، ۸، ۹، ۱۰، ۱۱، ۱۳	۰,۱۳۹۱		۲، ۳، ۴، ۶، ۷، ۸، ۹، ۱۰، ۱۱، ۱۳	۰,۱۸۲۸
		۶۵۰	۲، ۳، ۴، ۶، ۷، ۸، ۹، ۱۰، ۱۱، ۱۳	۰,۶۰۸۶		۴، ۶، ۹، ۱۰، ۱۱ ، ۱۳	۰,۲۲۹۰		۲، ۳، ۴، ۶، ۷، ۸، ۹، ۱۰، ۱۱، ۱۳	۰,۹۸۵۱
		۱۳۰۰	۲، ۳، ۴، ۶، ۷، ۸، ۹، ۱۰، ۱۱، ۱۳	۰,۷۷۷۶		۲، ۳، ۴، ۶، ۷، ۸، ۹، ۱۰، ۱۱، ۱۳	۰,۳۰۵۵		۲، ۳، ۴، ۶، ۷، ۸، ۹، ۱۰، ۱۱، ۱۳	۰,۹۹۸۹
	۲۶۰	۱۳۰	۲، ۳، ۴، ۶، ۷، ۸، ۹، ۱۰، ۱۱، ۱۳	۰,۳۲۷۰		۶، ۹، ۱۰، ۱۱، ۱۳	۰,۱۴۶۱		۲، ۳، ۴، ۶، ۷، ۸، ۹، ۱۰، ۱۱، ۱۳	۰,۷۶۷۰
		۶۵۰	۲، ۳، ۴، ۶، ۷، ۸، ۹، ۱۰، ۱۱، ۱۳	۰,۷۸۴۱		۱۰	۰,۳۰۲۶		۶، ۸، ۱۰	۰,۹۹۴۱
		۱۳۰۰	۲، ۳، ۴، ۶، ۷، ۸، ۹، ۱۰، ۱۱، ۱۳	۰,۸۸۰۰		۴، ۶، ۹، ۱۰، ۱۱ ، ۱۳	۰,۳۷۷۵		۲، ۳، ۴، ۶، ۷، ۸، ۹، ۱۰، ۱۱، ۱۳	۰,۹۹۹۸
۱۰	۵۲۰	۱۳۰	۱، ۲، ۴، ۵، ۶، ۷، ۹ ، ۱۰، ۱۱، ۱۳	۰,۱۴۱۲		۱۰	۰,۲۹۵۹		۱، ۲، ۴، ۵، ۶، ۷، ۹، ۱۰، ۱۱، ۱۳	۰,۱۸۲۳
		۶۵۰	۱۰ ،۶	۰,۶۴۲۶		۱۰	۰,۵۲۲۹		۱، ۲، ۴، ۵، ۶، ۷، ۹، ۱۰، ۱۱، ۱۳	۰,۹۸۴۶
		۱۳۰۰	۱۰ ،۶	۰,۸۸۶۴		۱۰	۰,۶۲۶۳		۱۰ ،۸ ،۶ ،۵	۰,۹۹۹۸
	۲۶۰	۱۳۰	۲، ۳، ۴، ۶، ۷، ۸، ۹ ، ۱۰، ۱۱	۰,۳۳۱۵		۱۰	۰,۳۸۶۸		۱، ۳، ۴، ۵، ۶، ۸، ۹، ۱۰، ۱۱،۱۳	۰,۷۶۳۰
		۶۵۰	۱۰ ،۶	۰,۸۸۸۶		۱۰	۰,۶۲۶۳		۱۰ ،۸ ،۶ ،۵	۰,۹۹۹۶
		۱۳۰۰	۱۰	۰,۹۷۸۷		۱۰	۰,۷۲۳۰		۱۰	۰,۹۹۹۹

زمانی‌که تقاضای شبکه ۲۰ واحد در نظر گرفته شود، تعداد مسیرهای افزونه برای تأمین این جریان کاهش می‌یابد. فقط دو مسیر مستقل وجود دارد که تقاضای شبکه را برآورده می‌سازند - اولی مسیر شامل یال‌های ۱، ۵ و ۱۲ درحالی‌که دومی شامل یال‌های ۲، ۳، ۴، ۶، ۹، ۱۱ و ۱۳ است. بنابراین خط‌مشی دفاعی یا بایستی یکی از این دو مسیرهای منبع- مقصد حفاظت کند و یا حول هر یک از آن‌ها افزونگی ایجاد کند.

نتایج به‌دست‌آمده برای هر یک از بودجه‌های تدافعی و تهاجمی زمانی که $m = 1,3$ است، رفتاری مشابه با بحث قبلی دارد. درنتیجه، بهترین خط‌مشی دفاعی مسیر ۱، ۵ و ۱۲ است، چون شامل تعداد کمی یال است و بنابراین آسیب‌پذیری یال‌ها کم است. تنها جوابی که از این رفتار تبعیت نمی‌کند یال‌های ۶، ۸ و ۱۰ را تعریف می‌کند که برای ایجاد افزونگی ضروری نیستند.

برای تقاضای $d = 40$ واحد تنها مسیر تأمین‌کننده جریان، شامل یال‌های ۱، ۲، ۳، ۵، ۷، ۹، ۱۲ و ۱۳ است. همان‌طورکه قبلاً بحث شد، بودجه منابع بایستی به این مسیر اختصاص یابد تا آسیب‌پذیری این مسیر کاهش یابد. جواب‌های بهینه برای $m = 1$ و $m = 3$ نشان می‌دهند که تنها از یال‌های ۴، ۶، ۸، ۱۰ و ۱۱ حفاظت نشده است.

برای این تقاضا، بالابردن افزونگی حداقل نیازمند سه یال اضافی دیگر است. بنابراین، به طور قابل توجهی منابع تخصیص‌یافته به سایر یال‌ها را کاهش می‌دهد. با این حال، در این مورد هنگامی‌که بودجه دفاعی کم است، منابع تهاجمی دفاع را در هم می‌شکنند. چون در شبیه‌سازی انجام‌شده مقادیر بسیار نزدیک به صفر بودند هیچ خط‌مشی دفاعی برای تأمین جریان موردنیاز وجود ندارد و PSDA جواب NS[1] را نمایش می‌دهد.

۳-۱- نتایج دای و پو

شبکه در نظر گرفته‌شده برای این مثال در واقع از دای و پو [۶] گرفته شده است. همان‌طور که در شکل (۲) مشاهده می‌کنید مقادیر بالای هر یال به ترتیب ظرفیت و اندیس آن یال را نشان می‌دهد. برای این پیکربندی شبکه ماکزیمم جریان از s به t برابر ۴۴ واحد است، زمانی که هیچ حمله‌ای وجود ندارد. جدول (۴) نتایج حاصل از حالت‌های مختلف قالب آسیب‌پذیری شبکه را نشان می‌دهد.

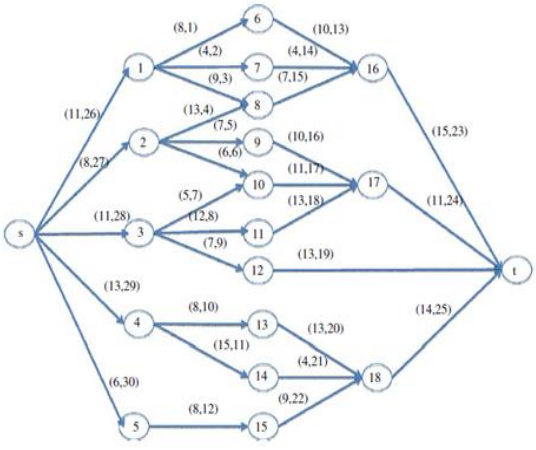
1- No Solution

جدول (۴). نتایج حاصل از حالت‌های مختلف قالب آسیب‌پذیری شبکه (دای و پو)

Net.surv	$m=5$ Non-defended links	Net.surv	$m=0.2$ Non-defended links	Net.surv	$m=1$ Non-defended links	b	B	d
۰,۷۲۳۵	۲، ۵، ۸، ۱۱، ۱۴، ۱۶، ۱۸، ۲۱	۰,۰۰۰۰	NS	۰,۰۰۵	۱۷	۱۰۰۰		
۰,۹۹۷۵	۲، ۶، ۷، ۱۱، ۱۴، ۱۷، ۲۱	۰,۰۰۰۵	۱۷، ۱۵	۰,۰۶۱۵	۲، ۱۱، ۱۴، ۲۱	۳۰۰۰	۶۰۰	
۰,۹۹۹۰	۵، ۱۴، ۱۶، ۲۱	۰,۰۰۱۰	۸، ۲	۰,۳۷۰۵	۲، ۱۱، ۱۴، ۲۱	۹۰۰۰		۴۴
۰,۹۹۵۰	۳، ۵، ۸، ۱۱، ۱۶، ۱۸، ۲۱	۰,۰۰۰۰	NS	۰,۰۴۹۰	۲، ۱۱، ۱۴، ۲۱	۱۰۰۰		
۰,۹۹۸۵	۶، ۱۱، ۱۴، ۱۷	۰,۰۰۱۵	۲۰	۰,۳۵۰۵	۲، ۱۱، ۱۴، ۲۱	۳۰۰۰	۲۱۰	
۰,۹۹۹۰	۱۴	۰,۰۰۳۰	۲۱، ۱۱	۰,۷۱۵۰	۲۱، ۱۱	۱۳۰۰		
0.9915	۲، ۴، ۶، ۸، ۱۲، ۱۴، ۱۸، ۲۲، ۳۰	۰,۰۰۶۵	۵، ۲	۰,۰۴۰۰	۶، ۷، ۱۷	۱۰۰۰		
۰,۹۹۹۵	۱۴، ۲	۰,۰۱۵۰	۶	۰,۴۹۱۰	۵، ۸، ۱۶، ۱۸	۳۰۰۰	۶۰۰	
۰,۹۹۹۵	۵، ۶، ۱۴، ۱۶، ۲۱، ۳۰	۰,۳۵۵۰	۶	۰,۹۱۸۵	۷	۹۰۰۰		۲۹
۰,۹۹۹۰	۷، ۱۱، ۲۱	۰,۰۱۵۰	۱۲، ۲۲، ۳۰	۰۴۷۷۰	۲، ۵، ۱۴، ۱۷	۱۰۰۰		
۰,۹۹۹۵	۱۵، ۱۶، ۱۸، ۲۱	۰,۰۳۲۵	۶	۰۹۱۲۰	۱۴، ۲	۳۰۰۰	۲۱۰	
۰,۹۹۹۸	۲۲، ۱۶	۰,۰۷۴۰	۱۶، ۵	۰,۹۹۳۵	۷	۹۰۰۰		
۰,۹۹۸۵	۲، ۵، ۶، ۷، ۱۲، ۱۴، ۱۶، ۱۷، ۲۲، ۳۰	۰,۲۸۳۵	۱۲، ۲۲، ۳۰	۰,۷۱۷۵	۴، ۵، ۶، ۷، ۹، ۱۰، ۱۱، ۱۲، ۱۶، ۱۷، ۱۹، ۲۰، ۲۱، ۲۲، ۲۵، ۲۷، ۲۹، ۳۰	۱۰۰۰		
۰,۹۹۹۰	۴، ۶، ۱۳، ۱۹، ۲۲، ۲۷، ۲۹	۰,۴۰۷۵	۶	۰,۹۷۵۵	۱۶، ۵	۳۰۰۰	۶۰۰	
۰,۹۹۹۵	۲، ۷، ۹، ۱۰، ۱۳، ۱۴، ۱۵، ۲۲، ۲۵، ۲۶، ۲۹	۰,۵۶۰۰	۶	۰,۹۹۵۰	۷، ۵	۹۰۰۰		۱۱
۰,۹۹۵۰	۵، ۶، ۷، ۱۱، ۱۲، ۱۳، ۱۵، ۱۶، ۳۰	۰۴۰۱۰	۲۱، ۱۱	۰,۹۷۱۰	۲، ۵، ۱۴، ۱۶	۱۰۰۰		
۰,۹۹۹۰	۱، ۲، ۳، ۱۱، ۱۳، ۱۴، ۱۶، ۱۷، ۲۱، ۲۲، ۲۶، ۲۷	۰,۵۵۰۵	۶	۰,۹۹۹۰	۷، ۵	۳۰۰۰	۲۱۰	
۰,۹۹۹۵	۱، ۱۰، ۱۳، ۱۴	۰,۶۸۹۰	۶	۰,۹۹۹۵	۸، ۶، ۳	۹۰۰۰		

در این جدول در کل ۱۸ حالت مختلف، برای میزان درگیری‌های $m=0.2,1,3$، سه جریان متفاوت $(d=44,29,11)$، سه بودجه تدافعی $(b=1000,3000,9000)$ و دو بودجه تهاجمی $(B=210,600)$ وجود دارد. برای این مثال پارامترهای مورد نیاز برای PSDA به صورت $SAMPEL=500$، $U=10$ و $S=71$ در نظر گرفته شده است.

تجزیه و تحلیل نتایج به‌دست‌آمده (جدول ۴) برای این شبکه بزرگ‌تر مانند مثال پیشین است. خط‌مشی دفاعی بهینه برای $m=1$، زمانی که بودجه تدافعی کم‌ترین $(b=1000)$ و بودجه تهاجمی بیش‌ترین $B=600$ مقدار است، فقط از ۱۲ یال حفاظت می‌شود با این امید که این یال‌ها افزونگی لازم برای فرستادن جریان مورد نیاز را فراهم کنند. هم‌چنان که بودجه تدافعی افزایش می‌یابد یا بودجه تهاجمی کاهش می‌یابد، یال‌های بیش‌تر می‌توانند برای فراهم‌نمودن افزونگی اضافه شوند و پایداری شبکه را افزایش دهند. به طور مشابه، وقتی تقاضا نیازمند یال‌های بیش‌تری است تا جریان مورد نیاز شبکه $d=40$ را تأمین کند. خط‌مشی دفاعی منابعش را به طور مساوی در میان یال‌های با اهمیت بیش‌تر توزیع می‌دهد.



شکل (۳): شبکه دای و پو

۴- نتیجه‌گیری و تحقیقات آینده

این مقاله قالب تدافعی از شبکه را نشان می‌دهد که مهاجم تلاش می‌کند جریان عرضه- تقاضا را با اختصاص منابع تخریبی به طور مساوی در میان یال‌های ظرفیت‌دار شبکه کاهش دهد. تحت این تهدید حمله، مدافع منابع‌اش را برای حفاظت از یال‌های شبکه اختصاص می‌دهد به طوری‌که احتمال تامین جریان مورد نیاز شبکه (همان پایداری شبکه) بیشینه شود. قالب بهینه‌سازی براساس آسیب‌پذیری یال‌ها با استفاده از تابع میزان موفقیت مهاجم- مدافع برای هر یال تعیین می‌شود. جواب‌های به دست آمده برای این قالب بر روی شبکه‌های مختلف نشان می‌دهد که موقعی که مدافع با توزیع مساوی منابع تهاجمی روبروست، خط‌مشی دفاعی بایستی براساس انتخاب میان بهبود قابل توجه پایداری یک مسیر عرضه- تقاضا به خصوص (با تخصیص تمام منابع دفاعی به یال‌های این مسیر)، یا توزیع منابع در میان یال‌های گوناگون شبکه برای افزایش مختصر پایداری چندین مسیر و بنابراین ایجاد افزونگی باشد. نتایج به دست آمده هم‌چنین نشان می‌دهد وقتی میزان درگیری افزایش می‌یابد انتخاب نخست سودمندتر است.

اگرچه این مقاله نخستین گام در فهمیدن رفتار خط‌مشی دفاعی می‌باشد، با این‌حال اگر به مدافع اجازه دهیم منابع‌اش را به طور نامساوی تقسیم کند، شاید موجب تخصیص بهتر و در نتیجه پایداری شبکه را در برابر سناریوهای متفاوت حمله‌ای افزایش دهد. هم‌چنین ممکن است مهاجم منابع‌اش را به طور بهینه در میان یال‌ها پخش کند تا بیش‌ترین آسیب را برای هر خط‌مشی دفاعی محتمل برساند. بنابراین، هریک از این موارد در تحقیقات آینده می‌تواند مورد بررسی قرار گیرد.

۵- مراجع

[1] A. W. McMasters and T. M. Mustin, “Optimal interdiction of a supply network,” Nav. Res. Logist. Q., 1970.

[2] R. L. Helmbold, “A countercapacity network interdiction model,” 1971.

[3] M. R. Boyle, “Partial-enumeration for planar network interdiction problems,” 1998.

[4] R. K. Wood, “Deterministic network interdiction,” Math. Comput. Model., 1993.

[5] Y. Dai and K. Poh, “Solving the network interdiction problem with genetic algorithms,” In Proceedings of the fourth Asia-Pacific conference on industrial engineering and management system, Taipei, pp. 18–20, 2002.

[6] J. E. Ramirez-Marquez, C. M. Rocco S, and G. Levitin, “Optimal protection of general source-sink networks via evolutionary techniques,” Reliab. Eng. Syst. Saf., 2009.

[7] G. Levitin and K. Hausken, “False targets vs. redundancy in homogeneous parallel systems,” Reliab. Eng. Syst. Saf., 2009.

[8] G. Levitin and K. Hausken, “Redundancy vs. protection vs. false targets for systems under attack,” IEEE Trans. Reliab., vol. 58, no. 1, pp. 58–68, 2009.

[9] K. J. Cormican, D. P. Morton, and R. K. Wood, “Stochastic Network Interdiction,” Oper. Res., 1998.

[10] B. A. Gebre and J. E. Ramirez-Marquez, “Element substitution algorithm for general two-terminal network reliability analyses,” IIE Trans. (Institute Ind. Eng.), 2007.

[11] J. E. Ramirez-Marquez and B. A. Gebre, “A classification tree based approach for the development of minimal cut and path vectors of a capacitated network,” IEEE Trans. Reliab., 2007.

[12] C. M. Rocco S and J. A. Moreno, “Network reliability assessment using a cellular automata approach,” Reliab. Eng. Syst. Saf., 2002.

[13] C. M. Rocco S and E. Zio, “Solving advanced network reliability problems by means of cellular automata and Monte Carlo sampling,” Reliab. Eng. Syst. Saf., 2005.

[14] L. R. Ford Jr and D. R. Fulkerson, “Flows in networks,” Princeton university press, 2015.

[15] Y. Rabinovich and A. Wigderson, “Techniques for bounding the convergence rate of genetic algorithms,” Random Struct. Algorithms, 1999.

[16] C. M. Rocco S and J. E. Ramirez-Marquez, “Deterministic network interdiction optimization via an evolutionary approach,” Reliab. Eng. Syst. Saf., 2009.

[17] J. E. Ramirez-Marquez, “New approaches for reliability design in multistate systems,” In Handbook of Performability Engineering, Springer, pp. 465–476, 2008.

[18] J. E. Ramirez-Marquez, “Port-of-entry safety via the reliability optimization of container inspection strategy through an evolutionary approach,” Reliab. Eng. Syst. Saf., 2008.

[19] J. L. Cook and J. E. Ramirez-Marquez, “Optimal design of cluster-based ad-hoc networks using probabilistic solution discovery,” Reliab. Eng. Syst. Saf., 2009.

[20] A. Berrones, “Stationary probability density of stochastic search processes in global optimization,” J. Stat. Mech. Theory Exp., 2008.

مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"
ویژه‌نامه کنفرانس بین‌المللی ترکیبیات، رمزنگاری و محاسبات، ص ۱۳۲ -۱۲۷

ارائه یک فرا-معماری سامانه‌ای از سامانه‌ها مبتنی بر ارزیابی فازی

هادی صالحی[۱]، محمدهادی علائیان[۲*]

۱- گروه مهندسی کامپیوتر، واحد ساری، دانشگاه آزاد اسلامی، ساری ۲- دانشکده مهندسی کامپیوتر دانشگاه علم و صنعت ایران

(دریافت: ۹۵/۰۷/۰۵، پذیرش: ۹۶/۰۳/۰۶)

چکیده

این مقاله ارائه‌دهنده یک مدل بهینه از معماری سامانه‌ای از سامانه‌ها (SOS) برای یک امداد و نجات دریایی است. سامانه‌ای از سامانه‌ها یک ساختار با ترکیب سامانه‌های مختلف است. همچنین، هر یک از سامانه‌ها دارای عملکرد و محدودیت‌های مستقل می‌باشند که با یکدیگر همکاری می‌کنند. مفهوم فرا معماری به معنی تولید معماری‌هایی است که هر یک بالقوه معماری مناسب برای سامانه موردنظر است. فرا معماری بیان می‌کند که چگونه تمام زیرمجموعه‌های احتمالی سامانه می‌تواند در ترکیب برای ایجاد یکSOS باهم همکاری کنند. ماهیت همکاری سامانه‌ها به شکلی است که عملکرد خروجی آن‌ها از جمع عملکرد سامانه‌های منفرد مناسب‌تر است. ازآنجایی‌که مؤلفه‌های سامانه، به‌طور مثال بودجه با توجه به شرایط تغییر می‌کند، نمی‌توان یک عدد مشخصی را به‌عنوان بودجه مطلوب در نظر گرفت. بنابراین، ارزیابی معماری‌های SOS به‌صورت فازی انجام می‌شود. هر یک از معماری‌ها توسط سامانه استنتاج فازی ارزیابی می‌شود و معماری ضعیف‌تر حذف می‌شود. در انتها، یک معماری به‌عنوان مناسب‌ترین معماری برای سامانه موردنظر انتخاب می‌شود.

کلیدواژه‌ها: سامانه‌ای از سامانه‌ها، امداد و نجات، الگوریتم ژنتیک.

۱. مقدمه

سامانه‌ای از سامانه‌ها مجموعه بزرگی از زیرسامانه‌ها و ارتباط‌های بین آن‌هاست. اگر این ساختار دارای رفتار پویای نوظهور باشد که از یک سامانه منفرد قابل بروز نباشد یک سامانه پیچیده نامیده می‌شود [۱]. یک سامانه پیچیده ویژگی‌هایی از خود بروز می‌دهد که در سامانه منفرد مشاهده نمی‌شود، به این ویژگی‌ها خواص نوظهور[۱] گویند [۲].

از سویی دیگر مهندسی سامانه‌ای از سامانه‌ها یک ساختار نظام‌مند در مهندسی است که تلاش دارد تا یک روشی اصولی برای سامانه‌ای از سامانه‌ها شکل دهد. اولین مسئله‌ای که باید در سامانه با مقیاس بزرگ مشخص شود این است که آیا این سامانه، سامانه‌ای از سامانه‌ها است یا خیر. مایر، در مقاله [۳]، پارامترها و شرایط لازم برای اینکه یک سامانه، SOS باشد را شرح می‌دهد. یکی از انواع بسیار مهم SOS نوع SOS تصدیقی[۲] است. این نوع SOS دارای اهداف مشخص و دارای یک هماهنگ‌کننده با اختیارات و منابع محدود است. SOS تصدیقی، صفات زیادی را هم از SOS همکار[۳] و هم از SOS مستقیم به اشتراک می‌گیرد.

به‌طورکلی SOS دارای چهار خاصیت اصلی زیر هست:

- هر یک از سامانه‌ها عملکرد و محدودیت‌های خاص خود را دارد که از پیش تعریف‌شده است.
- از مدل موج برای خلاصه‌سازی رفتار سامانه استفاده می‌شود. در ابتدا رفتار سامانه به شکل عناصر طناب بندی شده نمایش داده می‌شد که قادر به نمایش حالت پویای سامانه نبود. سپس با نمایش حالت موج برای نمایش حالت پویای سامانه استفاده شد.
- SOS اهداف خود را توسط ترکیب سامانه‌های موجود و اضافه کردن قابلیت‌های جزئی جدید به وجود می‌آورد.
- هر چرخه در مدل موج با (پیشنهاد - موافقت - مذاکره) ایجاد می‌شود.

برای یک ساختار با N سامانه، مدیر SOS از تعدادی از سامانه‌ها برای شرکت در SOS دعوت می‌کند. همچنین مدیر قادر به ارائه پیشنهادهای مالی یا.. به هر سامانه هست. هر سامانه می‌تواند با پذیرفتن پیشنهادها به سامانه SOS اضافه شود و در قبال آن، عملکرد مورد تقاضای SOS را انجام می‌دهد. همچنین با تغییر شرکت‌کننده‌ها (تغییر معماری) می‌توان به قابلیت جدیدی

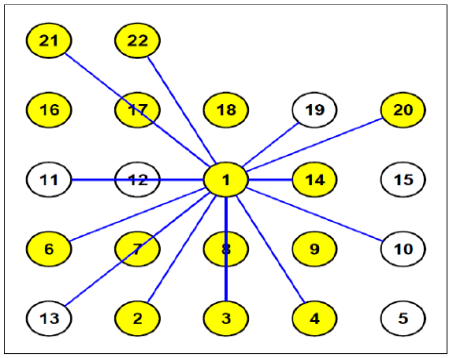
* رایانامه نویسنده مسئول: hadi_alaeiyan@comp.iust.ac.ir

1- Emergent
2- Acknowledged
3- Collaborative

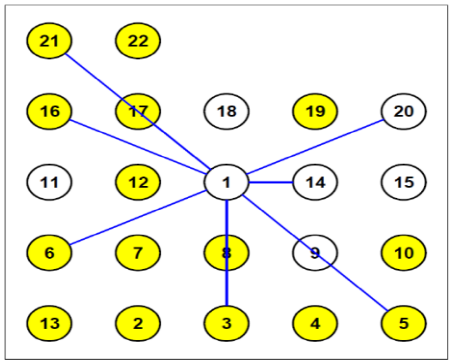
دست‌یافت که می‌تواند بالقوه سامانه مطلوب باشد. شکل (۱) مراحل انجام این کار را نشان می‌دهد. [۲]

شکل (۱): چگونگی دعوت به همکاری در SOS

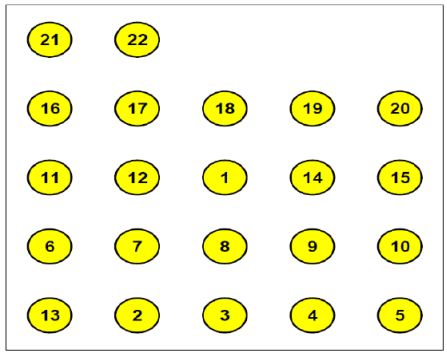
شکل (۲) و شکل (۳) نمونه‌ای از شرکت سامانه‌ها را در یک SOS نشان می‌دهند.



الف



ب



ج

شکل (۲): الف: SOS با ارتباط بالا ب: SOS با ارتباط متوسط ج: SOS بدون ارتباط.

شکل (۳): ساختار سه نوع سامانه SOS با خصوصیت‌ها، هزینه‌ها و ترکیب سامانه‌های مختلف.

با توجه به پیچیدگی و وسعت سامانه‌های جدید، استفاده از SOS جایگاه ویژه‌ای در میان معماران سامانه‌های مهندسی‌شده پیداکرده است. از روش‌هایی که در این زمینه استفاده شده‌اند، شامل روش مدل‌سازی جامع که ترکیبی از توانایی‌های پردازش اشیاء و پتری رنگی[1] است [۵]. همچنین، لویس پایب[2] و همکارانش برای تولید معماری‌های بالقوه و ارزیابی معماری‌ها، از الگوریتم‌های ژنتیک و مجموعه‌های فازی به‌طور گسترده استفاده کرده‌اند [۶]. لویس پایب و همکارانش با استفاده از سامانه SOS مدل‌هایی از همکاری سامانه‌ها را شبیه‌سازی نموده‌اند. آنها ادعا نموده‌اند اگر امریکا در جنگ خلیج‌فارس از چنین معماری‌هایی برای همکاری سامانه‌های نظامی خود استفاده می‌کرد، نقص‌های به وجود آمده در ره‌گیری موشک‌های عراق رخ نمی‌داد [۶-۱].

در این مقاله، ابتدا تعدادی از سامانه‌های موجود، توسط الگوریتم ژنتیک به‌عنوان معماری‌های اولیه به‌منظور امداد و نجات دریایی انتخاب می‌شوند. با توجه به استقلال سامانه‌ها ممکن است شرکت سامانه‌های مختلف در SOS صورت نگیرند. شبیه‌سازی شرکت یا عدم شرکت سامانه‌ها توسط الگوریتم مونت کارلو صورت می‌گیرد. سامانه استنتاج فازی با توجه به تعدادی از خصوصیات یک سامانه مطلوب، معماری را مورد ارزیابی قرار می‌دهد [۶-۱]. خصوصیت‌های مورد ارزیابی عبارت‌اند از کارایی، توان مالی، پایداری، پیمانه‌ای بودن و شبکه-مداری. معماری‌هایی که مقدار تابع هزینه بالایی داشته باشند در نسل‌های بعدی معماری شرکت داده نمی‌شوند. بعد از چند نسل از الگوریتم ژنتیک، معماری‌های مناسب‌تر تولید و ارزیابی می‌شوند. در انتها، معماری با مناسب‌ترین ساختار SOS ایجاد و ارزیابی می‌شود. در ادامه این مقاله در بخش دوم و سوم به ارائه الگوریتم‌های ژنتیک و روش پیشنهادی ارائه می‌شود. سپس، در بخش چهارم به شبیه‌سازی روش پیشنهادی می‌پردازیم. در انتها در بخش پنجم و ششم با نتیجه‌گیری و منابع، مقاله را به انتها می‌رسانیم.

1- Colored petri nets
2- Louis Pape

۲- الگوریتم ژنتیک

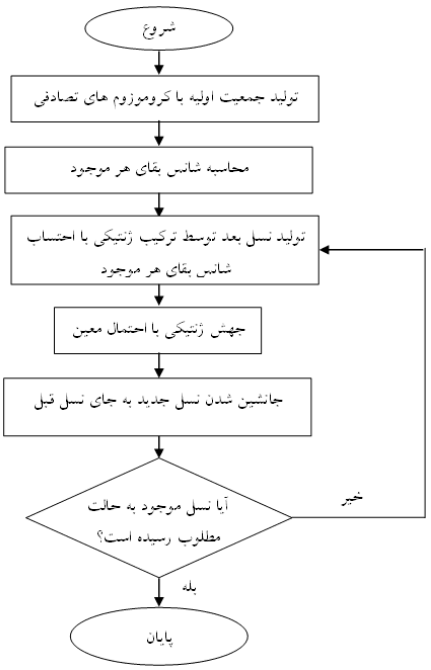
الگوریتم ژنتیک به‌منظور تولید معماری‌های بالقوه کاربرد دارد. مشارکت یا عدم مشارکت سامانه‌ها می‌تواند توسط بعضی از الگوریتم‌ها مدل شود. الگوریتم ژنتیک یکی از این الگوریتم‌ها است که می‌تواند این مشارکت یا عدم مشارکت را به شکل مناسبی پیاده‌سازی کند. الگوریتم ژنتیک در سال ۱۹۷۰ در ایالات‌متحده توسعه پیدا کرد و به‌طورمعمول برای بهینه‌سازی گسسته مورداستفاده قرار می‌گیرد. از ویژگی‌های این الگوریتم می‌توان به کند و سلسله مراتبی بودن آن اشاره کرد. در سامانه‌هایی که نیاز به‌نوعی خلاقیت و هوش باشد عملکرد مناسبی دارد. عملکرد الگوریتم ژنتیک به شکلی است که با ترکیب و جهش ژنتیکی والدین نسل جدیدی تولید می‌شود. همچنین الگوریتم GA از تعدادی پارامتر که در زیر نمایش داده‌شده برای تولید نسل جدید استفاده می‌کند. [۸-۷]

پارامترهایGA شامل:

GA(Fitness,Fitness_threshold,p,r,m)

- Fitness: تابع ارزیاب
- Fitness_threshold : آستانه توقف تولید نسل
- P : تعداد فرضیات
- r : نرخ ترکیب
- m : نرخ جهش

شکل (۴) دیاگرام عملکرد الگوریتم ژنتیک را به شکل مختصر نشان می‌دهد.



شکل (۴): دیاگرام تولید نسل GA

۳- روش پیشنهادی

روش پیشنهادی ایجاد سامانه‌ای باقابلیت تولید مناسب یک معماری با خصوصیت‌های موردنیاز است. به این منظور از روش‌های بهینه‌سازی هوش تکاملی استفاده‌شده است. گام‌های موردنیاز برای دستیابی به مناسب‌ترین معماری به شرح زیر است.

۳-۱- مشخصات سامانه

همان‌طور که در مقدمه ذکر شد، هدف از مدل‌سازی‌ها در این مقاله یافتن مناسب‌ترین معماری به‌منظور ایجاد یک سامانه SOS برای امداد و نجات تعدادی از افراد در حال غرق شدن در دریا است. تعدادی از متغیرهای اولیه این مأموریت در زیر ذکرشده است.

هدف از SOS: بهینه‌سازی عملکرد یک پاسگان ساحلی جستجو باقابلیت نجات جان مسافران یک کشتی در حال غرق شدن در دریای خزر انتخاب‌شده است.

ذی‌نفعان: پاسگان ساحلی یا ارتش دارای سامانه‌های متعدد باقابلیت‌های متفاوت (هواپیما، بالگرد، سامانه‌های ارتباطی و مراکز کنترل که با چندین ایستگاه در منطقه در دسترس هستند). علاوه بر این، کشتی‌های ماهیگیری، صنایع غیرنظامی و کشتی‌های تجاری برای ارائه کمک هنگامی که یک فاجعه اتفاق می‌افتد. مرکز هماهنگی و فرمان کنترل هدایت ترکیبی از کشتی‌های سرنشین دار و پهپادها. سامانه‌های ارتباطی هماهنگی سنجش و قابلیت‌های نجات.

بودجه: حدود ۱۰۰ میلیارد تومان.

ویژگی‌های کلیدی عملکرد

۱. کارایی
۲. توان مالی
۳. پایداری
۴. پیمانه‌ای بودن
۵. شبکه-مداری

تعدادی از سامانه‌هایی که به‌طور بالقوه شرکت دارند: N = 29.

مأموریت امداد و ردیابی شامل ۲۹ سامانه که هر یک قابلیت متفاوتی دارند.

۳-۲- تولید معماری‌ها

جمعیت اولیه یا فرضیات الگوریتم ژنتیک مجموعه محدودی از معماری‌های SOS می‌باشند. تولید معماری‌های مختلف توسط

الگوریتم ژنتیک صورت می‌گیرد. برای تعیین مناسب‌ترین SOS باید این فرضیات و معماری‌ها مورد ارزیابی قرار بگیرند. ارزیابی معماری‌ها با توجه به ویژگی‌های کلیدی عملکرد توسط سامانه استنتاج فازی صورت می‌گیرید. هرچه مقدار تابع تناسب در ارزیابی فازی بیشتر باشد عملکرد مناسب‌تری دارد. در ادامه، معماری‌های ضعیف‌تر حذف می‌شوند و معماری‌های مناسب‌تر به کمک ترکیب و جهش نسل جدیدی را شکل می‌دهند ارزیابی معماری‌ها در بخش ارزیابی معماری شرح داده‌شده است.

۳-۳-شبیه‌سازی استقلال سامانه‌ها

بعد از ایجاد معماری توسط الگوریتم ژنتیک، خودمختاری سامانه‌هایی که توسط الگوریتم ژنتیک دعوت به همکاری شده‌اند شبیه‌سازی می‌شود. مجموعه‌ای از سامانه‌های شرکت‌کننده یا عدم شرکت کردن سامانه می‌تواند توسط ۱ برای سامانه شرکت‌کننده و یا صفر برای شرکت نکردن سامانه مدل شود. برای مدل‌سازی این نوع سامانه، به‌احتمال شرکت کردن یک سامانه در SOS احتمال P که **(0 < p < 1)** نسبت داده می‌شود.

در ادامه برای شبیه‌سازی سامانه با کمک الگوریتم مونت‌کارلو و انتخاب عددی تصادفی بین صفر و یک می‌توان حضور یا عدم حضور سامانه را شبیه‌سازی نمود. وجود رابطه بین سامانه‌های مختلف توسط اعمال یک و عدم وجود چنین رابطه‌ای توسط صفر مشخص می‌شود. در اینجا نیز به‌احتمال وجود رابطه بین دو سامانه در SOS احتمال q که **(0 < q < 1)** نسبت داده می‌شود. در کنار هم قرار گرفتن این مجموعه صفر و یک‌ها، یک کروموزوم را شکل می‌دهد. اگر تمامی سامانه‌ها شرکت کنند حداکثر n(n-1)/2 ارتباط در SOS خواهیم داشت. همچنین اگر pn سامانه در SOS شرکت کنند و تمایل ایجاد برقراری ارتباط بین سامانه‌ها q باشد؛ تعداد $p^2qn(n-1)/2$ تعداد ارتباط‌های مورد انتظار می‌شود.

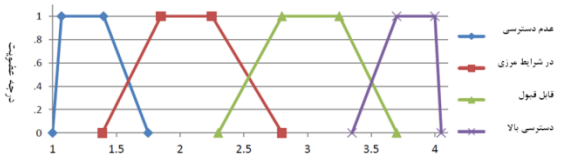
۴-۳- ارزیابی معماری

با توجه به شکل (۳)، تابع تناسب[1] در الگوریتم ژنتیک برای ارزیابی SOS ها کاربرد دارد. این ارزیابی نسبت به صفت‌های زیر صورت می‌گیرد:

- بودجه[2]
- کارایی[3]
- انعطاف[4]
- پایداری[5]
- پیمانه‌ای بودن
- شبکه-مداری

این صفت‌ها تا حدودی بر هم تأثیر دارند و نمی‌توان یک مقدار دقیق برای یک صفت با توجه به متغیر بودن صفت‌ها در شرایط مختلف و وابستگی صفت‌ها مشخص نمود. بنابراین ارزیابی صفت‌ها به شکل فازی صورت می‌گیرد.

هر یک از صفت دارای درجه‌بندی‌هایی از غیرقابل‌قبول[6]،قابل‌قبول[7]، خوب[8] و عالی[9] می‌باشند. تعیین مرز دقیقی بین این درجه‌بندی‌ها کار دشواری است، بنابراین این درجه‌بندی‌ها دارای ساختار فازی هستند [۱ و ۱۰]. شکل (۵) ساختار فازی این درجه‌بندی را به نمایش می‌گذارد.



شکل (۵): ساختار فازی درجه‌بندی.

همان‌طور که در شکل۵ مشخص است. مقادیر بین ۲,۳ و ۲,۸ به شکل فازی مشخص‌شده‌اند. برای هر یک از صفت‌ها درجه‌بندی خاص آن لحاظ می‌شود. درجه‌بندی با توجه به فرمول مورداستفاده برای آن صفت در نظر گرفته‌شده است. فرمول مورد استفاده برای درجه‌بندی هر یک از صفات به شکل زیر است.

کارایی : کارایی معمار به‌عنوان مجموع تعداد مردم نجات‌یافته از دریا است.

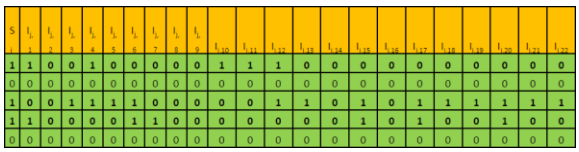
شبکه-مداری: شبکه مداری خاصیت آهنگ مربوط به توانایی در دسترس بودن برای به اشتراک گذاشتن اطلاعات است. مرکز-هایی که به این شکل عمل کنند، شبکه محور نامیده می‌شوند.(معادله ۱ و ۲)

$$\text{interoprerability} = \sum_{i=1}^{n}\sum_{j=1}^{n} A_{ii} * A_{jj} * A_{ij} \qquad (۱)$$

ماتریس توسط A با تبدیل رشته‌ای از بیت به یک ماتریس مجاورت محاسبه می‌شود و A_{ii} و A_{jj} مقادیر دودویی برای حضور سامانه‌ها (۱) و عدم وجود (۰) در معماری مشخص می‌شود. همچنین، Aij مشخص می‌کند آیا بین i و j ارتباطی وجود دارد یا خیر. اگر هر یک از دو سامانه وجود نداشته باشند، حاصل این معادله صفر می‌شود .همان‌طور در شکل (۶) مشخص است، نه سامانه باهم همکاری دارند، بعد از ستون نهم در موقعیت ستون ده تا نوزده مشخص‌کننده ارتباط سامانه اول با دیگر سامانه‌ها است. همچنین از موقعیت ستون بیست‌تا نه ستون بعد ارتباط

1- Fitness
2- Affordability
3- Performance
4- Flexibility
5- Robustness
6- unacceptable
7- marginal
8- acceptable
9- exceeds

سامانه دوم با دیگر سامانه‌ها را مشخص می‌کند و ... .



شکل (۶): مجموعه‌ای از ۹ سامانه و ارتباط بین سامانه‌ها.

توان مالی: بستگی به مجموع هزینه‌های عملیاتی (معادله ۲) و تعداد قابلیت‌هایی که برخوردار است. علاوه بر این، تعداد روابط (معادله 3) سامانه با دیگر سامانه‌ها.

$$\text{Operation cost} = \sum_{s=1}^{N} \text{Oc}^{\text{Ss}} * \sum_{i=1}^{M} \text{c}_i^{\text{Ss}} \qquad (2)$$

$$Interfasrs\ cost = \sum_{s=1}^{N} Ic^{Ss} * \sum_{k=1}^{N} k \neq s\ I_i^{SsSk} \qquad (3)$$

S_s : $_{s\in}\{1, 2, \dots N\}$.

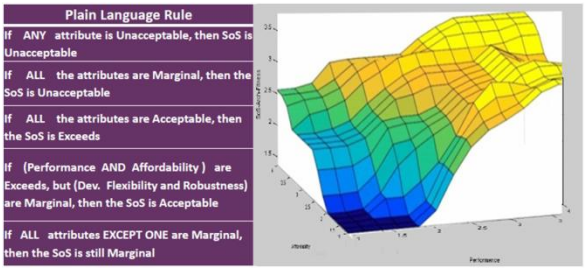
C_i : $_{i\in}\{1, 2, \dots N\}$.

I_i^{SsSk}: $_{s\in}\{1, 2, \dots N\}\&\ _{k\in}\{1, 2, \dots N\}; s.t. s \neq k$

به‌طوری‌که S_S نشان‌دهنده سامانه‌هایی است که در SOS مشارکت دارند. همچنین، C_i قابلیت‌هایی است که از یک سامانه به‌منظور امداد نجات استفاده می‌شود. I_i^{SsSk} نیز نشان‌دهنده ارتباط S_S با S_K است.

پیمانه‌ای: ساختار شبکه‌ها و گراف را اندازه‌گیری می‌کند. پیمانه‌ای عبارت است از، حداکثر تعداد قابلیت تفکیک ممکن در یک شبکه و الگوریتم نیومن[1] برای به دست آوردن آن [۹] استفاده‌شده است.

ارزیابی SOS نسبت به این صفات، توسط قوانین خاصی که در تابع فازی مشخص می‌شود صورت می‌گیرد. درنهایت خروجی فازی در این مقاله ملاک ارزیابی ما برای مناسب بودن SOS است. شکل (۷) این قوانین و خروجی سه‌بعدی این صفات را نمایش می‌دهد.



شکل (۷): مجموعه قوانین ارزیابی فازی

۳-۵- تولید نسل جدید

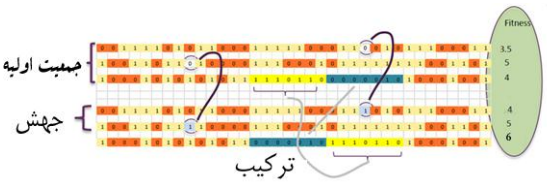
بعد از ارزیابی SOS ها به سه طریق نسل جدید ایجاد می‌شود.

۱. بهترین‌های نسل حاضر بدون تغییر وارد نسل جدید می‌شود

۲. تعدادی از کروموزوم‌های SOS در نسل حاضر باهم ترکیب شده و بخشی از نسل جدید را می‌سازند.

۳. تعدادی از کروموزوم‌های نسل جدید با جهش ژنتیکی وارد نسل بعد می‌شوند.

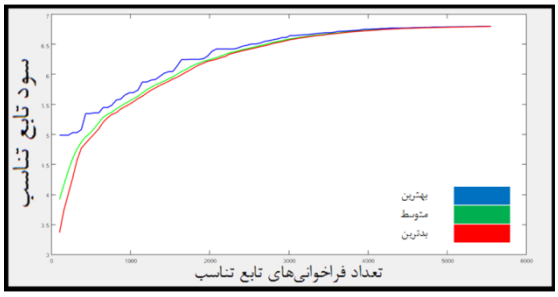
همچنین SOS ها با کمترین میزان تابع تناسب از نسل حاضر حذف می‌شوند. شکل (۸) روند تولید نسل جدید را نشان می‌دهد.



شکل (۸): روند تولید نسل جدید.

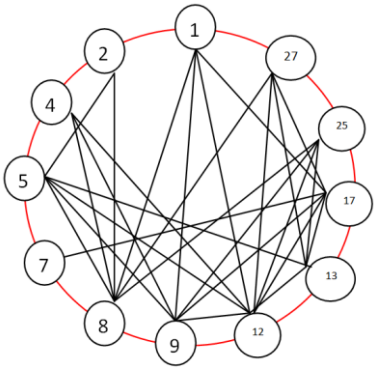
۴- شبیه‌سازی

برای به دست آوردن یک معماری مناسب، از ۱۰۰نسل معماری‌ها و در هر نسل از پنجاه تکرار از معماری‌های مختلف برای به دست آوردن مناسب‌ترین ترکیب سامانه‌ای استفاده‌شده است. افزایش نسل به ۳۰۰ هم تأثیری بر حداکثر کیفیت معماری ندارد. ازاین‌رو، معقول است همان کیفیت معماری در زمان شبیه‌سازی کمتر ثبت شود. نتایج ارائه‌شده در شکل (۹) ارزش تابع تناسب معماری را در سه حالت بیشترین، میانگین و بدترین تابع تناسب برای هر نسل، و این عملیات را در ۱۰۰ نسل با استفاده از الگوریتم ژنتیک نشان می‌دهد. بهترین مقدار تابع تناسب برای یک معماری ۶,۸ است که سامانه‌های تشکیل‌دهنده آن در جدول (۱) ذکرشده است. همچنین ارتباط‌های بین سامانه‌ها در این معماری در شکل (۱۰) مشخص‌شده است.



شکل (۱۰): نتایج ارائه‌شده توسط الگوریتم ژنتیک

1- Newman



شکل (۸): ارتباط‌های بین سامانه‌های معماری پیشنهادی

جدول (۱): ارتباط بین سامانه‌های پیشنهادی توسط الگوریتم ژنتیک

نوع سامانه	سامانه پیشنهادی الگوریتم ژنتیک
قایل تند رو	سامانه ۱
بالگرد	سامانه ۲
هواپیما	سامانه ۴ و ۵
پهپاد	سامانه ۷،۸،۹،۱۲ و ۱۳
کشتی ماهی گیری	سامانه ۱۷
مرکز کنترل	سامانه ۲۵
ارتباطات	سامانه ۲۷

۵- نتیجه‌گیری

این مقاله، یک روش یافتن مناسب‌ترین معماری برای یک مسئله جستجو و نجات است. مجموعه‌ای از معماری‌ها با یک تابع تناسب به‌دست‌آمده‌اند. معماری نهایی تولیدشده دارای قابلیت بالای نجات افراد با کمترین هزینه قابل پیش‌بینی هست. روش‌های اکتشافی تصادفی می‌تواند در فرایند سامانه معماری با ارائه سامانه‌های معمارانه با مجموعه‌ای از طرح‌های امکان‌پذیر که می‌توان به یک معماری مطلوب نزدیک باشد کمک کند. این سامانه‌ها می‌توانند با پیش‌بینی شرایط واقعی پیش از رخداد آن‌ها، باعث کاهش اتلاف هزینه و افزایش کارایی باشند. همچنین باعث افزایش میزان آمادگی پیش از وقوع رخداد غیرمترقبه شوند.

۶- مراجع

[1] Louis Pape, et al, (2013),“ A Fuzzy Evaluation method for System of Systems Meta-architectures”, CSER 2013: 245-254 .

[2] S.Agarwal et al. (2015)” Executable Architectures using Cuckoo Search Optimization coupled with OPM and CPN-A module: A new Meta-Architecture Model for FILA-SoS”, Springer International Publishing. , P 175-192.

[3] Maier, M. W. (1998),” Architecting principles for systems-of-systems”, Systems Engineering, 1(4), 267-284

[4] J. Dahmann, et al, (2011) “An Implementers’ View of Systems Engineering for Systems of Systems” Proceedings of IEEE International Systems Conference 2011, April 4-7, , Montreal, Quebec, Canada.

[5] Wang, R., & Dagli, C. H. (2011). Executable system architecting using systems modeling language in conjunction with colored Petri nets in a model-driven systems development process. Systems Engineering, 14(4), 383-409.

[6] Louis Pape, Siddhartha Agarwal, Kristin Giammarco, Cihan Dagli, Fuzzy Optimization of Acknowledged System of Systems Meta-architectures for Agent based Modeling of Development, Procedia Computer Science, Volume 28, 2014, Pages 404-411, ISSN 1877-0509.

[7] S. F. Galán, et al. (2013) “A novel mating approach for genetic algorithms,”Evolutionary Computation, vol. 21, no. 2, pp. 197–229.

[8] S. Li, H. Chen, and Z. Tang, (2011) “Study of Pseudo-Parallel genetic algorithm with ant colony optimization to solve the TSP,” IJCSNS International Journal of Computer Science and Network Security, vol. 11, no. 3.

[9] Newman, M. E. (2006). Modularity and community structure in networks. Proceedings of the National Academy of Sciences, 103(23), 8577-8582.

[10] R .ghaffarpour, A .A. pourmousa, A. ranjbar. Presenting an Index for Evaluation of Power Network Security Using Fuzzy Set Theory . 3; 7 (4) pp. 289-304. 2016. (In Persian)

مجله علمی - پژوهشی "پدافند الکترونیکی و سایبری"
ویژه‌نامه کنفرانس بین‌المللی ترکیبیات، رمزنگاری و محاسبات، ص ۱۴۲ -۱۳۳

ارائه یک فرا معماری پالایه دوطرفه چند وضوحی حذف نویز، مبتنی بر الگوریتم‌های فرا ابتکاری و ارزیابی فازی

جواد وحیدی[1*]، هادی صالحی[2]

۱- استادیار ،دانشگاه علم و صنعت ایران، ۲- دانشجوی دکترای مهندسی کامپیوتر، گروه مهندسی کامپیوتر، واحد ساری، دانشگاه آزاد اسلامی، ساری
(دریافت: ۹۵/۰۷/۰۵، پذیرش: ۹۶/۰۳/۰۶)

چکیده

تصاویر دریافتی با توجه عوامل محیطی دچار تداخل ناخواسته‌ای می‌شوند که به نویز شهرت دارند. در این مقاله، به‌منظور حذف این تداخل‌های ناخواسته دو سیستم حذف نویز باهم ترکیب می‌شوند و بر تصاویر شناورهایی که توسط پهپادها ارسال‌شده‌اند اعمال می‌گردند. ابتدا مدل‌های مختلف با ترکیب پالایه دوطرفه و تبدیل موجک، توسط الگوریتم ژنتیک تولید می‌شوند. مدل‌ها توسط اعمال پالایه دوطرفه در بخش‌های مختلف سطوح اول، دوم و سوم پالایه موجک پیاده‌سازی می‌شوند. با توجه به نیاز به ارزیابی تعداد زیاد معماری‌های مختلف و دقیق نبودن ارزیابی‌های شهودی، از یک تابع استنتاج فازی به‌منظور ارزیابی مدل‌های مختلف استفاده‌شده است. شبیه‌سازی و ارزیابی‌های ذکرشده در این مقاله بر سه تصویر ناو هواپیمابر، کشتی جنگی و زیردریایی صورت می‌گیرد. درنهایت، نتایج این سیستم در تمامی سطوح موردبررسی قرار می‌گیرد تا یک مدل با کمترین هزینه برای تمامی تصاویر ذکرشده یافت شود. به‌منظور درک بهتر کارایی این مدل، مقایسه‌ای بین مدل پیشنهادی و مدل‌های دیگر حذف نویز صورت می‌گیرد. نتایج نشان‌دهنده کارایی مناسب مدل پیشنهادی در مقایسه با دیگر مدل‌های حذف نویز است.

کلیدواژه‌ها: الگوریتم ژنتیک، حذف نویز، استنتاج فازی، پردازش تصویر،پالایه‌های موجک ، دوطرفه.

۱- مقدمه

علم پردازش تصویر یکی از علوم پرکاربرد در مهندسی است که در سال‌های اخیر پیشرفت قابل‌توجهی داشته است. یکی از مسائلی که در این علم وجود دارد، حذف اختلال‌های ناخواسته نظیر انواع نویزها و عوامل متعدد دیگر در تصاویر است. ، حذف این اختلال‌ها اغلب به‌عنوان مرحله پیش‌پردازش مورداستفاده قرار می‌گیرند. نویز یک سیگنال تصادفی است که موجب تخریب بسیاری از بخش‌های اصلی اطلاعات تصویر می‌شود. وجود نویز در تصویر یکی از مشکلات اصلی در پردازش تصویر است.

تصویر به علت انواع مختلفی از نویز مانند نویز گوسی[1]، نویز پواسون[2]، نویز نقطه[3]، نویز فلفل نمکی[4] و بسیاری دیگر انواع اساسی نویز دارای اعوجاج می‌شود. این نویز ممکن است از منابع نویز موجود در مجاورت دستگاه تصویربرداری، حافظه معیوب و یا ممکن است به علت نقص / عدم دقت در تصویر گرفتن دستگاه مانند دوربین، انحراف عدسی ، فاصله کانونی ضعیف، پراکندگی و دیگر شرایط نامطلوب رخ دهد[۲-۱].

پالایه‌های غیرخطی مانند پالایه میانه در حذف انواع نویزها مؤثر عمل می‌کنند. پالایه میانه قادر است نویزهای نقطه‌ای جدا از هم و یا نویزهای خطی جدا از هم را حذف کند، به‌طوری‌که در لبه‌های تصویر تغییری ایجاد نشود. یکی از معایب پالایه میانه هنگامی است که تصویر از یک حد آستانه‌بالای ۶۰ ٪ نویز بپذیرد که این پالایه قادر نیست پیکسل‌های بدون نویز ر ا از پیکسل‌های نویز دار تشخیص دهد.

استفاده از پالایه‌ها به‌طور ترکیبی منجر به یک همکاری هم‌افزا بین الگوریتم‌ها شده و موجب افزایش کارایی سیستم می‌شود. پالایه موجک قادر به بررسی تصویر در فرکانس‌های بالا و فرکانس‌های پایین است. پالایه دوطرفه نیز عملکرد مناسبی در فرکانس‌های بالا دارد. بنابراین، ترکیب این پالایه‌ها می‌تواند تأثیر مناسبی برای حذف نویز در تصاویر داشته باشند. ازاین‌رو استفاده از ترکیب پالایه‌ها در حال گسترش است. ازجمله می‌توان به ترکیب الگوریتم‌های حذف نویز موجک و پالایه دوطرفه تطبیقی

* رایانامه نویسنده مسئول: jvahidi@iust.ac.ir

1- Gaussian noise
2- Poisson noise
3- Spot noise
4- salt and pepper noise

توسط کارسی‌کیان[1] و همکارانش[۳] و براسو برامانین[2] و همکارانش در ترکیب پالایه میانه و موجک [۴] اشاره کرد. همچنین جو زانگ برای حذف نویز از تصاویر فراصوت از الگوریتم ترکیبی پالایه‌های دوطرفه و تبدیل موجک استفاده کرده است [۵] . جو زانگ[3] از پالایه دوطرفه به‌منظور حذف نویز در فرکانس پایین موجک و از آستانه دهی برای حذف نویز فرکانس بالا در تصویر موجک استفاده کرده است. در [۶] از ساختار مشابهی برای حذف نویز در تصاویر CT استفاده‌شده است. در مقالات ذکرشده، به کمک پالایه موجک، تصویر به مؤلفه‌های جزئیات و تقریبی تجزیه می‌شود. با توجه به تعداد سطوح استفاده‌شده از پالایه موجک تعداد موتلفه جزئیات افزایش می‌یابد اما تعداد مؤلفه تقریبی همواره یک است. بنابراین، تشخیص اینکه در کدام بخش از این مؤلفه جزئیات از پالایه دوطرفه استفاده شود دشوار است. لذا، در این مقالات، مؤلفه جزئیات توسط آستانه دهی موجک و مؤلفه تقریبی آن توسط پالایه دوطرفه تطبیقی حذف نویز می‌شنود. نیدهی چاندراکار[4] و همکاران در [۷] یک مدل جدید بر اساس ترکیب تبدیل موجک و پالایه دوطرفه برای حذف نویز ارائه داده‌اند. در این مقاله از نسبت اوج سیگنال به نرخ نویز (Peak signal-to-noise ratio[5]) و شاخص کیفیت تصویر (Image[6] quality indicator) برای ارزیابی استفاده‌شده است. در مقاله ذکرشده، ابتدا پالایه دوطرفه تطبیقی به تصویر اعمال‌شده است. سپس توسط موجک تصویر به موءلفه‌هایش تجزیه‌شده و آستانه دهی می‌شود. در ادامه تصویر بازسازی‌شده و بار دیگر از پالایه دوطرفه تطبیقی به‌منظور حذف نویز استفاده‌شده است. سوپیداروی[7] و همکارانش [۸] به بررسی تأثیر پالایه دوطرفه تطبیقی به بخش‌های مختلف مؤلفه‌های جزئیات و تقریبی پرداخته‌اند. نتایج این مقاله نشان‌دهنده این است که اعمال پالایه دوطرفه به ترتیب، پیش از اعمال پالایه موجک و بعد از اعمال پالایه موجک، مناسب‌ترین نتیجه را دارد. اما، ازآنجایی‌که ترکیب پالایه دوطرفه با موجک در چند سطح می‌تواند منجر به تولید حالات زیادی شود، این روش تنها به بررسی چند مدل و ترکیب پالایه دوطرفه با پالایه موجک در یک سطح نموده است.

در این مقاله تأثیر پالایه دوطرفه بر موءلفه‌های پالایه موجک در سه سطح موردبررسی قرار می‌گیرد.

به‌منظور ترکیب دو پالایه از الگوریتم فرا ابتکاری ژنتیک باینری که در ساختارهای گسسته عملکرد مناسبی دارد استفاده می‌شود. مدل‌های مناسب‌تر دارای قابلیت حذف نویز بهتر و هزینه حذف نویز کمتر می‌باشند. بنابراین، در نسل‌های بعدی الگوریتم ژنتیک باقی می‌مانند. به‌منظور بررسی دقیق پالایه موجک، تجزیه این پالایه در سه سطح صورت می‌گیرد و هر سطح به‌طور مجزا بررسی می‌شود تا مناسب‌ترین سطح تجزیه موجک برای اعمال پالایه دوطرفه مشخص شود. با توجه به اینکه بررسی درزمینه تأثیر پارامترها (از پارامترهای بهینه تا غیر بهینه) بر ترکیب بهینه پالایه‌ها انجام‌نشده بود، در این مقاله به بررسی مقادیر مختلف پارامترها در نویزهای مختلف پرداخته می‌شود. همچنین تأثیر تغییر پارامترها بر هزینه حذف نویز مدل بهینه موردبررسی قرار می‌گیرد. بهینه‌سازی پارامترهای این پالایه‌ها با توجه به پیوسته بودن پارامترها توسط الگوریتم فرا ابتکاری ازدحام ذرات صورت می‌گیرد.

به علت تعداد زیاد مدل‌های موردبررسی، نیاز به ارزیابی خودکار مدل‌ها است. لذا، یک تابع ارزیاب فازی به‌منظور ارزیابی مدل‌های مختلف پیشنهادشده است.

همچنین، با توجه به اینکه مقایسه مدل‌های به‌طور شهودی دارای دقت پایین است، استفاده از ارزیابی فازی منجر به ارزیابی یکپارچه مدل‌ها می‌شود. تابع ارزیاب فازی، به‌منظور ارزیابی عملکرد کیفیتی از سه معیار کیفیتی استفاده می‌کند.

در انتها، مدل با کمترین هزینه حذف نویز در تمامی تصاویر به دست می‌آید. عبارت فرا معماری به معماری‌هایی اشاره دارد که هر یک می‌توانند بالقوه معماری مناسب مدل برای حذف نویز در فرکانس‌های مختلف باشند [۱۱] مدل به‌دست‌آمده باید مناسب‌ترین عملکرد را در شرایط زیر داشته باشد.

- مناسب‌ترین عملکرد در نویزهای مختلف.
- پایین‌ترین هزینه تجمعی حذف نویز به ازای تمامی پارامترهای بهینه و غیر بهینه.
- پایین‌ترین هزینه در تمامی سطوح موجک.
- مناسب‌ترین مدل در تمامی تصاویر مورد آزمایش.

در انتها، مدل پیشنهادی با تعدادی از مدل‌های مفید و کارای دیگر مقایسه می‌شود. همان‌طور که در شکل ۱ و ۲ مشخص‌شده است، تصویرهای مورداستفاده و روش پیشنهادی نشان داده‌شده‌اند.

در ادامه مقاله در بخش‌های ۲ تا ۴ الگوریتم ژنتیک و پالایه‌های حذف نویز شرح داده می‌شود. سپس در بخش ۵ ، ۶ و ۷ روش پیشنهادی، شبیه‌سازی و نتیجه‌گیری بیان می‌شود.

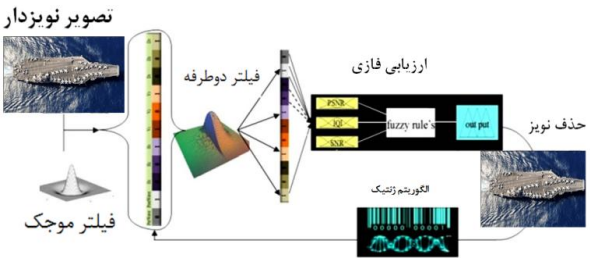
1- Karthikeyan
2- Balasubramanian
3- Ju Zhang
4- Nidhi Chandrakar
5- PSNR
6- IQI
7- Sudipta Roy

الف

ب

ج

شکل(۱): سه تصویر موردبررسی.



شکل(۲): روش پیشنهادی.

۲- الگوریتم ژنتیک

الگوریتم ژنتیک در سال ۱۹۷۰ در ایالات‌متحده توسعه پیدا کرد و به‌طورمعمول برای بهینه‌سازی گسسته مورداستفاده قرار می‌گیرد. از ویژگی‌های این الگوریتم می‌توان به کند و سلسله مراتبی بودن آن اشاره کرد که در سامانه‌هایی که نیاز به‌نوعی خلاقیت و هوش باشد عملکرد مناسبی دارد. عملکرد الگوریتم ژنتیک به شکلی است که با ترکیب و جهش ژنتیکی والدین، نسل جدیدی تولید می‌شود. اصطلاح‌های مهم به‌کاررفته در این الگوریتم در زیر بیان‌شده است.

- کروموزوم[1]: رشته‌ای از بیت‌ها را کروموزوم می‌نامند.
- ژن[2]: هر یک از بیت‌های درون کروموزوم را ژن می‌نامند.
- عملکرد ترکیب[3]: ترکیب کروموزوم دو یا چند والد برای تولید فرزندان.
- جهش: جهش[4] یک ژن در یک کروموزوم.

همچنین الگوریتم GA از تعدادی پارامتر برای تولید نسل جدید استفاده می‌کند. این پارامترها به ترتیب تابع ارزیاب برای ارزیابی فرضیات،آستانه توقف تولید نسل، تعداد فرضیات که جمعیت موردبررسی را تشکیل می‌دهند، نرخ ترکیب و نرخ جهش است.

۳. موجک و حذف نویز

یک روش پرکاربرد برای حذف نویز استفاده از موجک است. در تبدیل موجک یا به‌اختصار WT بدون اینکه اصل عدم قطعیت هایزنبرگ نقض شود، هم ر زولوشن فرکانسی و هم رزولوشن زمانی در نمودار زمان - فرکانس تغییر می‌کند. تفاوت تبدیل موجک با تبدیل فوریه زمان کوتاه این است که پهنای پنجره برای هر یک از اجزای طیفی تغییر می‌کند. این روش در فرکانس های بالا، رزولوشن زمانی خوب و رزولوشن فرکانسی ضعیف و در فرکانس‌های پایین، رزولوشن فرکانسی خوب و رزولوشن زمانی ضعیف به دست می‌دهد. در تبدیل موجک گسسته، سیگنال از یک سری پالایه‌های بالا گذر برای آنالیز[5] فرکانس‌های بالا و از یک سری پالایه‌های پایین گذر برای آنالیز فرکانس‌های پایین، عبور داده می‌شود. سیگنال به دو بخش تقسیم می‌شود بخش حاصل از عبور سیگنال از پالایه بالا گذر که شامل اطلاعات فرکانس بالا(ازجمله نویز) است و جزئیات نام دارد، و بخش حاصل از عبور سیگنال از پالایه پایین گذر که شامل اطاعات فرکانس پایین و دربرگیرنده مشخصات هویتی سیگنال است و کلیات نامیده می‌شود. درنهایت، گروهی از سیگنال‌ها را خواهیم داشت که همان سیگنال اولیه را نشان می‌دهند اما هر گروه سیگنال به باند فرکانسی متفاوتی مربوط است. در این حالت

1- Chromosome
2- Gene
3- Operator of crossover
4- Mutation
5- Resolution

می‌دانیم کدام سیگنال به کدام باند فرکانسی مربوط است و اگر همه آن‌ها را باهم در یک گراف سه‌بعدی نمایش دهیم، زمان را در یک محور، فرکانس را در محور دوم و دامنه را در محور سوم خواهیم داشت. در اینجا نیز با توجه به اصل عدم قطعیت هایزنبرگ[1] نمی‌توان مشخص کرد کدام فرکانس در کدام لحظه خاص وجود دارد، اما می‌دانیم کدام باند فرکانسی در کدام فاصله زمانی وجود دارد [۹-۸]. سپس با اعمال یک آستانه سازی بر فرکانس‌های موردنظر که الگوی فرکانسی نویز می‌باشند منجر به حذف نویزهای ناخواسته می‌شود.

۴- پالایه دوطرفه

می‌توان پالایه دوطرفه را به‌عنوان یک جایگزین مناسب پالایه موجک برای حذف نویز در نظر داشت. در پالایه دوطرفه یک وزن فضایی بدون نرم کردن لبه‌ها اعمال می‌شود. این پالایه به کمک ترکیب دو پالایه دیگر که یکی در حوزه مکانی و دیگری در حوزه شدت عمل می‌کند. بنابراین برای تعیین وزن‌های موردنیاز، به هردوی فاصله مکانی و شدت نیاز است. معادلات زیر خروجی یک پیکسل در نقطه x را مشخص می‌کند.

$$\bar{I}(x)=\frac{1}{c}\sum_{y\in N(x)} e^{\frac{-\|y-x\|^2}{2\sigma_d^2}} e^{\frac{-\|I(y)-I(x)\|^2}{2\sigma_r^2}} I(y) \qquad (۱)$$

به‌طوری‌که σ_d و σ_r انحراف از معیار برای دو پارامتر فضایی و شدت است. همچنین N(x) مشخص‌کننده پیکسل‌های همسایه پیکسل I(x) است. همچنین C ثابت نرمال ساز است. معادله ۲ این ثابت را نشان می‌دهد.

$$C=\sum_{y\in N(x)} e^{\frac{-\|y-x\|^2}{2\sigma_d^2}} e^{\frac{-\|I(y)-I(x)\|^2}{2\sigma_r^2}} \qquad (۲)$$

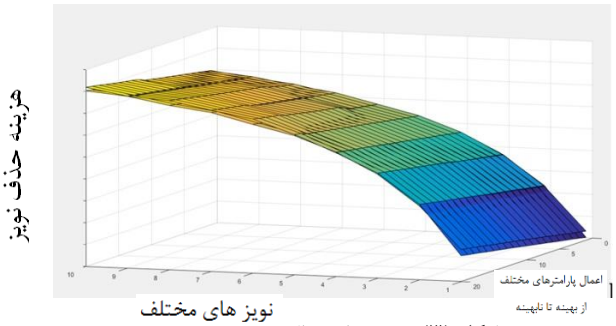
یکی از نقاط ضعف الگوریتم پالایه دوطرفه ، ناتوانی آن در حذف نویزهای فلفل نمکی است. مشکل دیگر این پالایه طبیعت وضوح یک‌طرفه آن است. برخلاف پالایه موجک، پالایه دوطرفه قادر به بررسی فرکانس‌های مختلف نیست. اگرچه این پالایه عملکرد خوبی در حذف نویزهایی با فرکانس بالا دارد ولی برای حذف نویزهای با فرکانس پایین با مشکل مواجه است. موضوع بااهمیت دیگر، نبود کار تحقیقاتی در مورد مقادیر بهینه پارامتر-های σ_d و σ_r است. [۸ و ۱۰].

۵- روش پیشنهادی

روش پیشنهادی به کمک پالایه موجک تصویر را به فرکانس‌های مختلف تجزیه و به مناسب‌ترین فرکانس، پالایه دوطرفه را اعمال می‌کند. به این منظور ابتدا هر دو پالایه در پارامترها و نویزهای مختلف بهینه می‌شوند.

۵-۱- بهینه‌سازی پالایه‌ها

ضرایب موجک و پارامترهای پالایه دوطرفه هر تصویر به‌طور جداگانه توسط الگوریتم فرا ابتکاری ازدحام ذرات بهینه می‌شوند. این بهینه‌سازی شامل پالایه موجک و پالایه دوطرفه از پارامترهای بهینه تا پارامترهای غیر بهینه و همچنین از نویز ۰,۰۱ تا ۰,۱ است. نمودار سه‌بعدی شکل ۳، بهینه‌سازی از سطح دوم موجک برای ناو هواپیمابر نشان داده‌شده است.



شکل (۳): بهینه‌سازی پالایه موجک و دوطرفه.

همان‌طور که مشخص است این دو نمودار سه‌بعدی تقریباً بر روی‌هم قرارگرفته‌اند. به‌منظور بررسی دقیق‌تر، تصویر نویز ۰,۰۱ همین نمودار را به جدول ۱ انتقال می‌دهیم.

جدول (۱): جدول بهینه سطح ۲ موجک، در تصویر ناو هواپیمابر

هزینه	مقادیر آستانه برای حذف ضرایب موجک						هزینه	پارامترهای فیلتر دوطرفه	
۲۶.۸۰	۰.۰۱۳۳	۱.۸۹۴۱	۲.۵۲۹۶	۰.۱۳۰۵	۱.۱۰۷۲	۰.۶۹۷۳	۲۶.۴۴	۰.۳۱۸	۱
۲۷.۳۵	-۰.۰۳۴۸	۲.۲۹۹۷	۲.۹۹۶۶	۰.۱۳۸۵	۱.۲۳۵۰	۰.۷۳۰۱	۲۷.۰۰	۰.۲۶۲	۱
۲۸.۵۱	-۰.۰۷۰۸	۱.۷۳۱۸	۲.۴۷۹۰	۰.۱۶۹۸	۱.۵۹۸۹	۱.۱۲۲۵	۲۸.۳۹	۰.۲۲۳	۱
۲۹.۰۰	-۰.۰۸۴۰	۱.۶۲۷۰	۲.۴۶۰۹	۰.۰۹۹۳	۰.۹۹۷۴	۰.۶۵۸۱	۲۹.۰۰	۰.۲۰۶	۲
۳۰.۰۱	۰.۱۱۰۹	۱.۹۸۵۹	۲.۴۱۲۲	۰.۰۸۴۰	۱.۲۳۱۱	۰.۲۲۴۰	۳۰.۰۲	۰.۲۲۴	۲
۳۱.۰۴	-۰.۱۱۴۶	۱.۷۷۷۷	۲.۱۱۲۴	۰.۶۱۹۸	۱.۲۹۷۸	۱.۰۱۸۰	۳۱.۰۰	۰.۱۶۹	۲
۳۲.۴۶	۰.۰۷۳۷	۲.۰۱۱۳	۲.۳۷۲۲	۰.۵۲۹۲	۰.۷۹۲۲	۰.۸۸۸۲	۳۲.۰	۰.۲۷۶	۲
۳۳.۳۹	۰.۱۵۲۳	۱.۶۹۶۱	۲.۴۶۹۷	۰.۰۵۵۱	۱.۲۱۹۹	۰.۶۵۴۴	۳۳.۰۴	۰.۳۰۹	۲
۳۴.۰۵	-۰.۱۴۱۹	۱.۸۸۳۱	۲.۴۸۳۱	۰.۰۷۸۵	۰.۷۶۴۰	۰.۷۴۲۱	۳۴.۰۲	۰.۳۸۳	۲
۳۵.۰۱	-۰.۱۴۸۴	۱.۷۵۶۰	۲.۵۱۹۱	۱.۱۵۵۹	۲.۱۲۳۶	۰.۷۷۰۲	۳۵.۰۰	۰.۳۲۵	۳

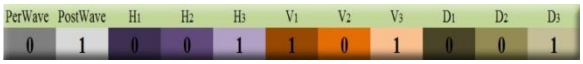
میزان هزینه‌های مدل‌های بهینه در سطح دوم و سوم پالایه موجک تقریباً برابر مقادیر هزینه بهینه پالایه دوطرفه است.

۵-۲- ارزیابی فازی مدل‌ها

هزینه بهینه‌سازی پالایه‌ها و هزینه مدل بهینه ترکیب پالایه‌ها توسط الگوریتم ژنتیک به دست می‌آید. این مدل‌ها می‌توانند به شکل ساختار ژن‌های یک کروموزوم کد شوند. شکل ۴ کد شدن ترکیب پالایه موجک سطح سوم و پالایه دوطرفه به یک کروموزوم با ۱۱ ژن را نشان می‌دهد. هر کروموزوم توسط ژن‌ها به دو ارزش علامت‌گذاری می‌شوند. این ارزش‌ها برابر ۰,۱ می‌باشند. عدد ۱ در هر ژن نشان‌دهنده اعمال پالایه دوطرفه در آن ژن است. از ۱۱ ژن، دو ژن اول مشخص‌کننده اعمال یا عدم اعمال پالایه دوطرفه پیش از اعمال موجک و بعد از اعمال

1- Uncertainty principle

موجک هستند. ژن‌های شماره‌های ۳ تا ۵ مشخص‌کننده ضرایب موجک افقی در سطح اول، دوم و سوم هستند. همچنین ژن‌های شماره ۶ تا۸ و ۹ تا ۱۱ به ترتیب مشخص‌کننده ضرایب موجک عمودی در سطح اول، دوم و سوم و ضرایب موجک قطری در سطح اول، دوم و سوم هستند.



شکل(۴): کد شدن یک مدل از پالایه‌های دوطرفه و موجک سه سطحی.

سپس، تصویر نهایی تولیدشده از مدل با تصویر بدون نویز مقایسه می‌شود. عمل مقایسه با توجه به ملاک‌هایی صورت می‌گیرد. این ملاک‌ها عبارت‌اند از PNSR، SNR و IQI. در معیارهای ذکرشده مقدار مناسب برای PSNR نشان‌دهنده این نیست که از دیدگاه بصری تصویر خوب به نظر می‌آید بنابراین، از مشخصه کیفیت تصویر به‌عنوان پارامتر دیگری برای تشخیص میزان کاهش نویز استفاده‌شده است[۷]. همان‌گونه که در رابطه ۳و۴ ملاحظه می‌شود فرمول میانگین مربعات خطا (Mean Squared Error[1]) و PSNR مشخص‌شده‌اند.

$$MSE = \frac{1}{M}\sum_{i=1}^{M}(g_i - f_i)^2 \qquad (۳)$$

$$PSNR = 10\,Log_{10}\left(\frac{(2^n-1)^2}{MSE}\right) \qquad (۴)$$

در معادله ۴، M نشان‌دهنده تعداد عناصر تصویر و n نشان‌دهنده تعداد بیت‌های هر علامت هستند. مشخصه کیفیت تصویر توسط سه عامل که در معادله ۵ مشخص‌شده‌اند تولید می‌شوند.

$$Q = \frac{\sigma_{fg}}{\sigma_f\sigma_g}.\frac{2\bar{f}\bar{g}}{\bar{f}^2+\bar{g}^2}.\frac{2\sigma_f\sigma_g}{\sigma_f^2\sigma_g^2} \qquad (۵)$$

همچنین پارامترهای آن در زیر مشخص‌شده است.

$$\bar{f} = \frac{1}{M}\sum_{i=1}^{M} f_i \qquad (۶)$$

$$\bar{g} = \frac{1}{M}\sum_{i=1}^{M} g_i \qquad (۷)$$

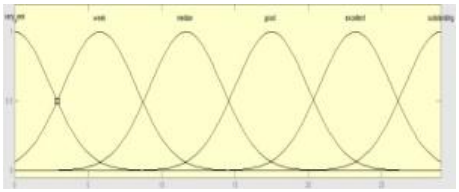
$$\sigma_{fg} = \frac{1}{M-1}\sum_{i=1}^{m}(f_i-\bar{f})(g_i-\bar{g}) \qquad (۸)$$

$$\sigma_f^2 = \frac{1}{M-1}\sum_{i=1}^{m}(f_i-\bar{f})^2 \qquad (۹)$$

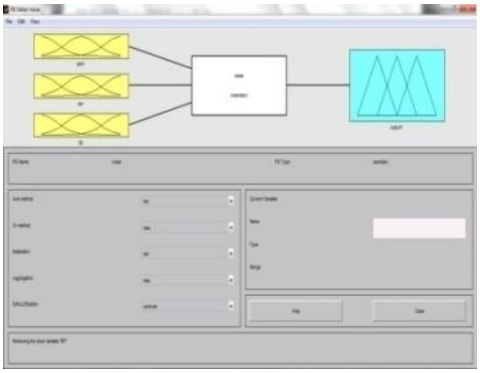
$$\sigma_g^2 = \frac{1}{M-1}\sum_{i=1}^{m}(g_i-\bar{g})^2 \qquad (۱۰)$$

جزء اول معادله (۵) مشخص‌کننده ضریب همبستگی بین f و g است، که اندازه‌گیری درجه همبستگی خطی بین f و g و محدوده دینامیکی آن در بازه [۱،۱-] است. جزء دوم معادله که مقدار شباهت شدت روشنایی بین f، g است با عددی بین [۰،۱] مشخص می‌شود. همچنین سومین جزء معادله میزان شباهت وضوح تصاویر را با عددی بین [۰،۱] مشخص می‌کند. معادله ۵ در دامنه مقادیر بین [۰،۱] در حال تغییر است و تنها زمانی یک می‌شود که gi=fi باشد. کمترین مقدار زمانی رخ می‌دهد که gi=2f-fi باشد.

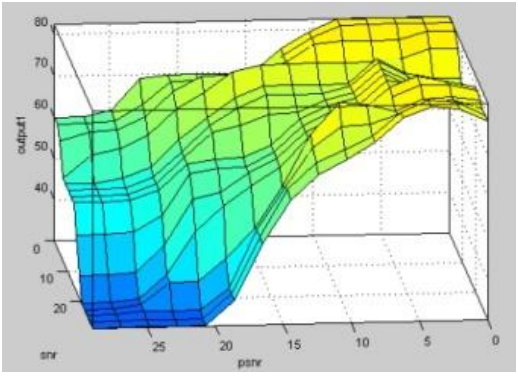
بعد از ارزیابی معیارهای کیفیتی، نتایج به سیستم استنتاج فازی ارسال می‌شوند. عمل فازی سازی برای هر ورودی صورت می‌گیرد. به‌طور مثال، برای PSNR مقدار ورودی عددی بین ۰-۳۰ است و این مقدار مطابق شکل (۵-الف) فازی می‌شود.



الف



ب



ج

شکل (۵): الف. فازی سازی مقدار ورودی PNSR ،ب. ترکیب مقادیر فازی شده توسط قوانین فازی، ج. خروجی تابع هزینه با مقدار ثابت IQI و متغیر SNR , PSNR.

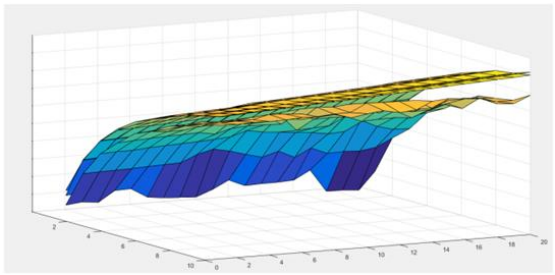
سپس مقدارهای فازی سازی شده توسط قوانین استنتاج فازی ترکیب می‌شود (۵.ب). ترکیب این مقادیر پاد فازی می‌شود و مقدار هزینه هر مدل را تولید می‌کند. شکل ۵.ج نشان‌دهنده

1- MSE

خروجی تابع هزینه با مقدار ثابت IQI و متغیر SNR , PSNR است

۵-۳- ترکیب پالایه‌ها توسط الگوریتم ژنتیک

پالایه‌های دوطرفه و موجک توسط الگوریتم ژنتیک باهم ترکیب می‌شوند. شکل۶ هزینه پالایه دوطرفه و موجک، همچنین هزینه مدل بهینه سطح دوم ناو هواپیمابر که توسط الگوریتم ژنتیک بهینه‌سازی شده است نشان می‌دهد.



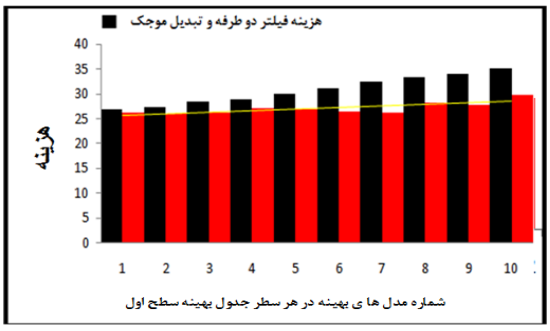
شکل(۶). هزینه پالایه‌های موجک (سطح دوم) و دوطرفه و هزینه بهینه ترکیب آن‌ها.

در ادامه بررسی، تصویر نویز ۰,۰۱ شکل (۶) در ادامه در نظر گرفته می‌شود. پارامترهایی از دو پالایه را که اعمال آن پارامترها بر پالایه، هزینه یکسانی برای پالایه‌ها ایجاد می‌کنند در یک سطح قرار داده‌شده‌اند (جدول ۲). انتخاب هزینه‌های برابر به‌منظور یکسان‌سازی میزان تأثیر پالایه‌ها بر تصویر نویز دار است. سطرهای بعدی به‌طور تقریبی با اختلاف یک هزینه مشخص‌شده‌اند.

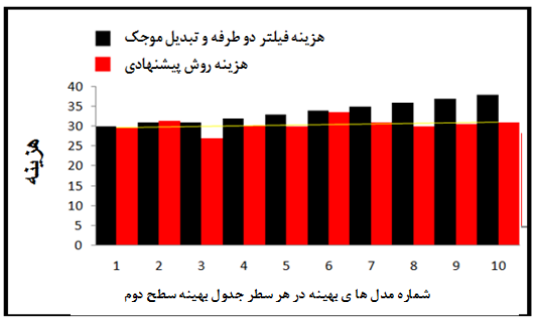
جدول (۲). تعیین مدل‌های بهینه با اعمال پالایه دوطرفه تطبیقی الف: در سطح دوم تبدیل موجک.

هزینه	موقعیت	هزینه فیلتر موجک	هزینه فیلتر دو ترفه تطبیقی
۲۶.۱۶۴۳	[۰ ۰ ۱ ۰ ۱ ۱ ۰ ۰]	۲۲.۴۱۳۴	۲۲.۴۱۹۱
۲۵.۹۷۴۷	[۰ ۰ ۰ ۱ ۱ ۱ ۰ ۱]	۲۳.۱۱۴۲	۲۳.۱۱۷۷
۲۶.۲۶۹۶	[۰ ۰ ۰ ۰ ۱ ۱ ۰ ۱]	۲۴.۰۷۶	۲۴.۰۵۰۳
۲۷.۱۳۱۷	[۰ ۰ ۰ ۰ ۱ ۱ ۱ ۱]	۲۵.۰۵۶	۲۵.۰۷۱۹
۲۶.۹۷۶۰	[۰ ۰ ۱ ۱ ۱ ۱ ۱ ۱]	۲۶.۰۷۷	۲۶.۰۷۳۷
۲۶.۴۲۵۰	[۰ ۰ ۰ ۱ ۱ ۱ ۱ ۰]	۲۷.۱۴۶	۲۷.۱۶۸۱
۲۶.۲۶۲۹	[۰ ۰ ۱ ۱ ۱ ۰ ۱ ۱]	۲۸.۰۴۳۵	۲۸.۰۴۱۶
۲۸.۲۸۰۸	[۰ ۰ ۱ ۱ ۱ ۱ ۱ ۱]	۲۹.۰۵۷۷	۲۹.۰۰۷۸
۲۷.۷۵۴۷	[۰ ۰ ۱ ۱ ۱ ۰ ۱ ۱]	۳۰.۲۳۵	۳۰.۱۵۵۳
۲۹.۷۶۴۰	[۰ ۰ ۱ ۱ ۱ ۱ ۱ ۱]	۳۱.۰۵۵۶	۳۱.۰۸۷۵
۲۶.۱۶۴۳	[۰ ۰ ۱ ۰ ۱ ۱ ۰ ۰]	۳۲.۳۲۴۵	۳۲.۱۱۹۷

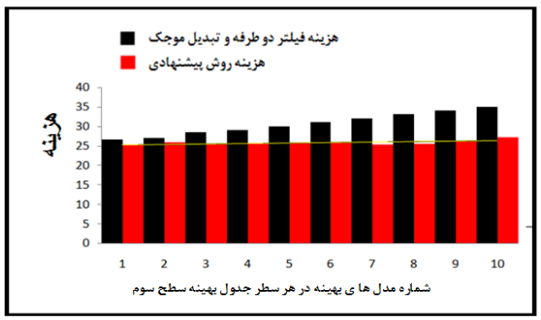
همان‌طور که از جدول(۲) مشخص است، مدل‌های روش پیشنهادی دارای هزینه کمتر و کارایی بیشتری از پالایه دوطرفه و تبدیل موجک هستند. شکل (۷) اختلاف مقدار هزینه بهینه پالایه دوطرفه و تبدیل موجک را با هزینه بهینه الگوریتم پیشنهادی در تصویر ناو هواپیمابر نشان می‌دهد.



الف



ب



ج

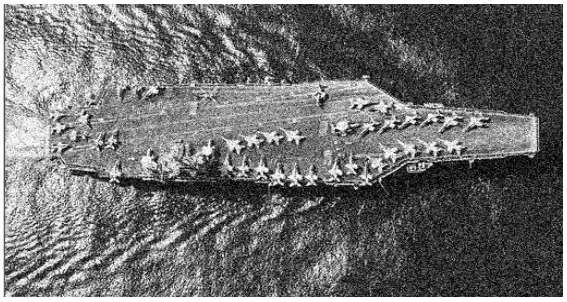
شکل (۷). اختلاف مقدار هزینه پالایه‌ها با هزینه الگوریتم پیشنهادی سطح.الف. اول، ب. دوم، ج. سوم.

نمودارهای شکل (۶ و ۷) و جدول (۲) نشان می‌دهند که مقدار بهینه الگوریتم پیشنهادی وابستگی کمی به مقادیر بهینه پالایه دوطرفه و تبدیل موجک دارد. همچنین در سطوح اول، دوم و سوم، خط روند[1] در الگوریتم پیشنهادی، به ترتیب به خط افقی نزدیک‌تر می‌شود. همچنین نزدیک‌ترین محل بین خط روند در الگوریتم پیشنهادی و پالایه‌ها، در محل بهینه پالایه‌ها رخ می‌دهد. این نشان می‌دهد که مقادیر بهینه الگوریتم پیشنهادی نمی‌تواند خیلی بهتر از حالت بهینه دو پالایه شود.

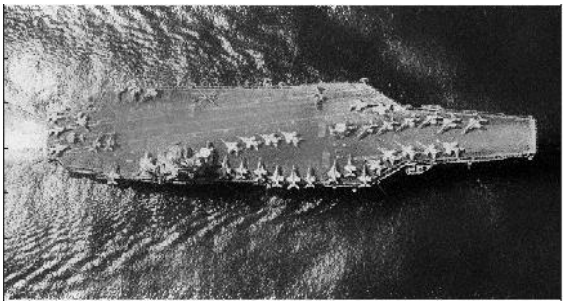
اما، نشان می‌دهد ترکیب پالایه‌ها بر مقادیر حتی غیر بهینه از پارامترهای دو پالایه می‌تواند هزینه‌ای مشابه باحالت بهینه تولید کند. شکل (۸) پنج تصویر بدون نویز، نویز دار، پالایه دوطرفه و پالایه موجک با مقدار هزینه حذف نویز ۳۰ و ترکیب آن‌ها توسط مدل [1 1 0 1 1 1 0 0] را نشان می‌دهد.

1- trend line

الف



ب



ج

د

ه

شکل (۸). الف. تصویر بدون نویز، ب. تصویر نویز دار، ج, د. تصویر بعد از اعمال پالایه دوطرفه و تبدیل موجک با هزینه حذف نویز ۳۰ ، ه. ترکیب دو پالایه با مدل [0 0 1 1 1 0 1 1] و هزینه حذف نویز ۲۷.

حال کم‌هزینه‌ترین مدل در تمامی تصاویر و سطح‌ها را به دست می‌آوریم. به‌منظور دستیابی به مدل با کمترین هزینه، مراحل زیر را به ترتیب انجام می‌گیرد.

- به دست آوردن کم‌هزینه‌ترین مدل در هر جدول مدل بهینه.
- به دست آوردن کم‌هزینه‌ترین مدل از جدول‌های مدل بهینه هم‌سطح در همه تصاویر.
- به دست آوردن کم‌هزینه‌ترین مدل از جدول مدل در تمامی سطوح و تصاویر.

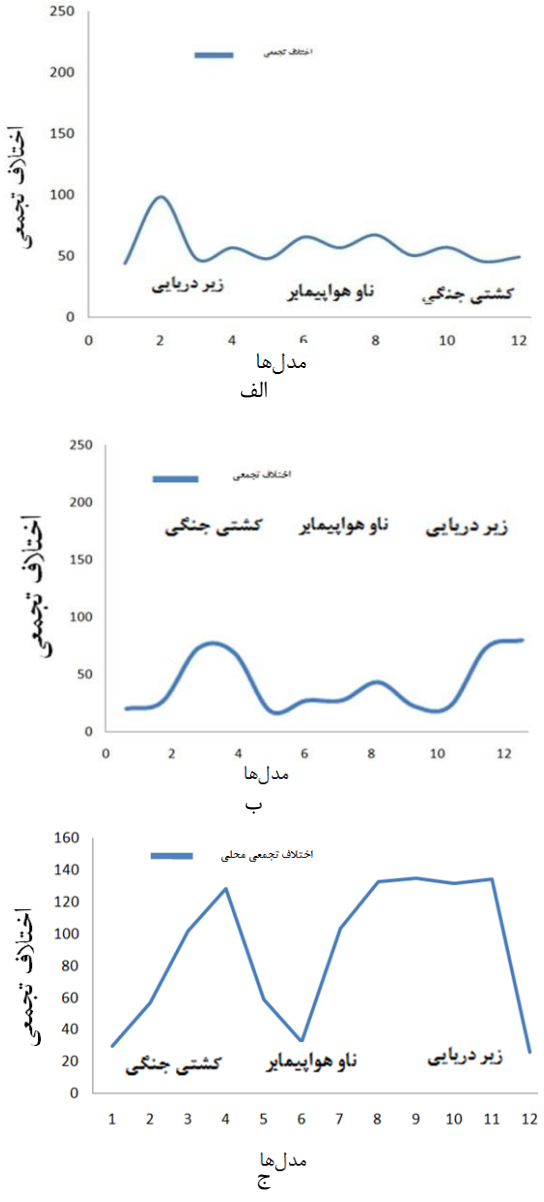
در مرحله اول مناسب‌ترین مدل‌های هر جدول را مشخص می‌شود. به این منظور هر یک از مدل‌های ستون موقعیت در جدول (۲) به ترتیب انتخاب می‌شود. مدل انتخاب‌شده جایگزین دیگر مدل‌ها از ستون موقعیت می‌شود. مدل جایگزین شده با متغیرهای σ_d و σ_r و همچنین آستانه حذف نویز سطری که وارد آن شده است ارزیابی می‌شود. سپس، هزینه مدل جایگزین شده با هزینه مدل بهینه همان موقعیت (پیش از جایگزینی) مقایسه می‌شود.

جمع اختلاف‌های یک مدل جایگزین شده با مدل‌های بهینه (پیش از جایگزینی) به دست آورده می‌شود. مدلی که در جایگزینی با پارامترهای مدل‌های دیگر کمترین اختلاف تجمعی را داشته باشد به‌عنوان کم‌هزینه‌ترین مدل آن جدول شناخته می‌شود.

در مرحله دوم، از هر جدول، چهار مدل با کمترین اختلاف تجمعی به‌عنوان مدل‌های بهینه در جدول (۳) قرار داده می‌شوند. عملیات مشابه برای تصاویر دیگر نیز انجام می‌شود. سپس عملیات جایگزینی مدل‌های جدول (۳)، در جدول هم‌سطح از سه تصویر انجام می‌گیرد (سی جایگزینی به ازای هر مدل). بنابراین، کم‌هزینه‌ترین مدل هر سطح در هر سه تصویر به دست می‌آید. سپس هزینه مدل‌ها در سه سطح مقایسه و کم‌هزینه‌ترین مدل در تمامی سطح‌ها مشخص می‌شود.

جدول (۳): مدل‌های با کمترین اختلاف تجمعی از میان تمامی تصاویر و در تمامی سطوح

		سطح سه	سطح دو	یک سطح
زیر دریایی	۱	[۰۰۱۱۱۱۱۰۰۱۱]	[۰۰۱۱۱۱۰۰۱]	[۱۰۰۱۰۱۰]
	۲	[۰۰۱۱۱۰۱۱۰۰۱]	[۰۰۱۱۱۱۱۰۱]	[۱۰۱۱۱]
	۳	[۰۰۰۱۱۱۱۱۰۰۱]	[۰۰۰۱۰۱۰۰۱]	[۱۰۱۱۱]
	۴	: [۰۰۱۱۱۱۱۱۰۰۱]	[۰۰۰۰۰۱۰۰۱]	[۰۰۱۱۰]
ناو هواپیمابر	۱	[۰۰۱۱۱۱۰۱۰۱۱]	[۰۰۱۱۱۱۰۱]	[۰۰۱۰۰]
	۲	[۰۰۱۱۱۰۱۰۱۰]	[۰۰۱۱۱۱۱۰]	[۰۰۱۱۰]
	۳	[۰۰۱۱۱۱۰۱۱۱۱]	[۰۰۱۱۱۱۱۱]	[۰۰۱۰۰]
	۴	[۰۰۱۱۱۱۰۰۱۱۱]	[۰۰۰۱۱۱۱۱]	[۱۰۱۱۱]
کشتی جنگی	۱	[۰۰۱۱۱۱۱۰۰۱۱]	[۰۰۱۱۱۱۰۱]	[۰۰۱۱۰]
	۲	[۰۰۱۱۱۱۱۰۱۱۱]	[۰۰۱۱۱۱۱۱]	[۰۰۱۱۰]
	۳	[۰۰۱۱۱۱۱۱۰۱۱]	[۰۰۱۱۱۰۰۱]	[۰۰۱۰۰]
	۴	[۰۰۰۱۱۱۱۰۰۱۱]	[۰۰۱۱۱۰۰۱]	[۰۰۰۰۰]

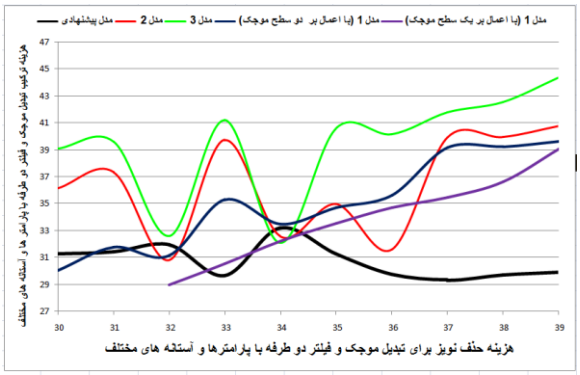


شکل (۹): نشان‌دهنده جمع تجمعی خطای مدل‌های مختلف الف. سطح سوم، ب. سطح دوم، ج . سطح اول.

نظر به نمودار شکل (۹)، مشاهده می‌شود که مدل شماره ۱ سطح دوم تصویر ناو هواپیمابر، کمترین هزینه تجمعی را دارد. بنابراین مدل با ساختار [1 0 1 1 0 01 0 0] مناسب‌ترین مدل برای تمامی تصاویر است.

۶- شبیه‌سازی

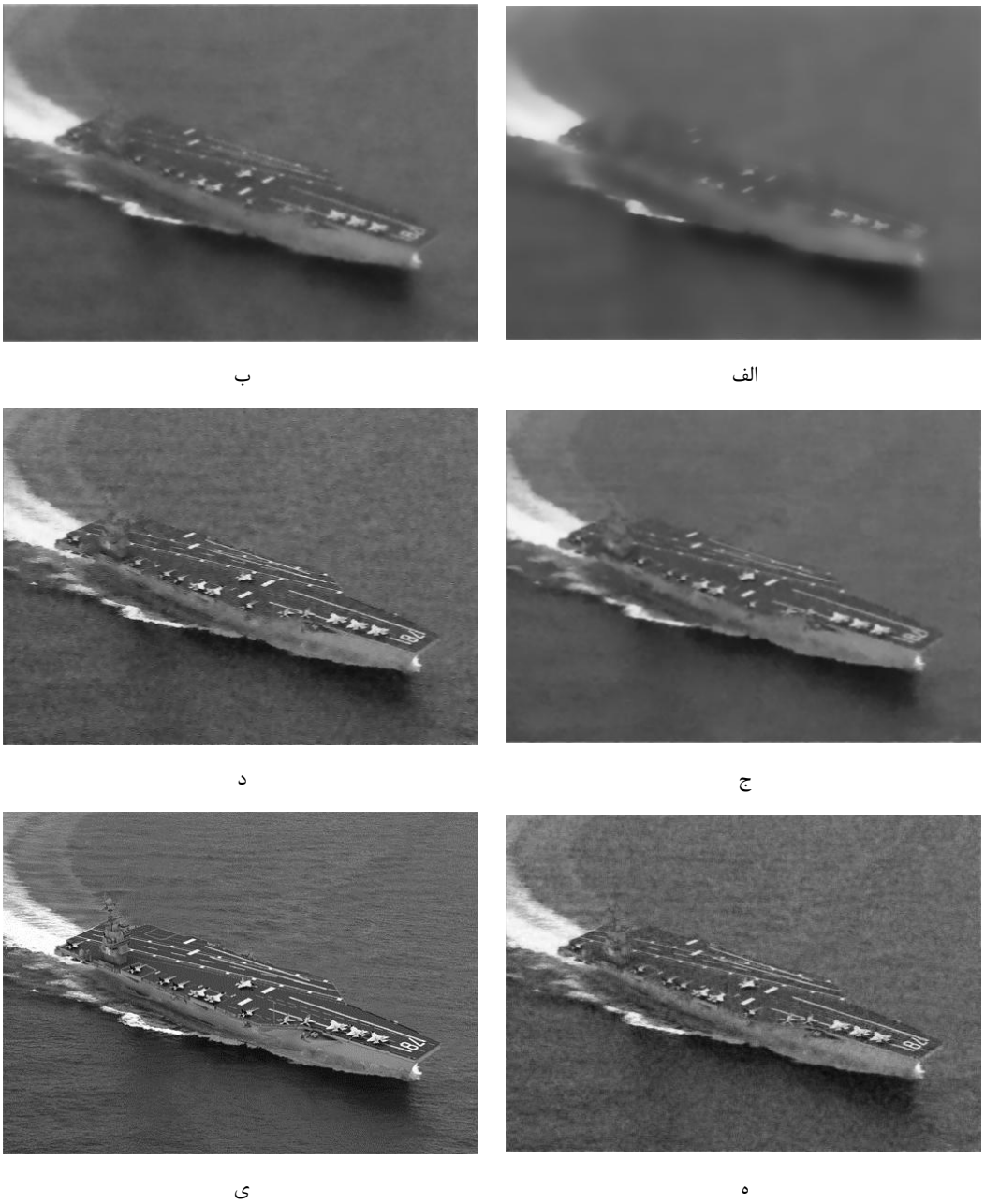
مدل یافت شده نشان‌دهنده اعمال پالایه دوطرفه بر ضرایب عمودی سطح اول و ضرایب افقی، عمودی و قطری سطح دوم است. مدل‌های شماره ۱ زیردریایی و ۱ کشتی جنگی دارای کمترین هزینه می‌باشند. هردوی این مدل‌ها در سطح دوم رخداده و ساختاری مشابه و به شکل[1 0 1 1 1 1 0 0] دارند. این مدل با تعدادی از مدل‌های مشابه مقایسه می‌شود. به این منظور، یک تصویر نمونه، مورد مقایسه مدل پیشنهادی و سه مدل دیگر قرار می‌گیرد. مدل‌های مورد ارزیابی علاوه بر مدل پیشنهادی به ترتیب بانام‌های مدل ۱ پیشنهادشده در [۵] و مدل‌های ۲ و ۳ به ترتیب پیشنهادشده در [۹-۸] مشخص می‌شوند.



شکل (۱۰): مقایسه مدل‌های مختلف حذف نویز.

مطابق شکل (۱۰)، مدل پیشنهادی دارای مناسب‌ترین هزینه و پایدارترین حالت در میان مدل‌های مورد مقایسه هست. شکل (۸) نتایج اعمال مدل پیشنهادی و دیگر مدل‌ها را بر تصویر مورد مقایسه، در حالتی که پالایه دوطرفه و تبدیل موجک هزینه ۳۹ رادارند، نشان می‌دهند(در انتهای تصویر یا بدترین وضعیت پارامترها).

همان‌طور که در شکل ۱۱ مشاهده می‌شود مدل پیشنهادی عملکرد مناسب‌تر و پایدارتری نسبت به دیگر مدل‌ها از خود نشان می‌دهد. همچنین، مدل ۱ با اعمال بر یک سطح از موجک عملکرد خوبی دارد، اما بر روی سطح آب دریا جزئیات بیشتری حذف‌شده است.



شکل(۱۱): مقایسه مدل‌های مختلف حذف نویز. الف) مدل ۳، ب) مدل ۲، ج) مدل ۱ با اعمال بر دو سطح از تبدیل موجک، د) مدل ۱ با اعمال بر یک سطح از تبدیل موجک، ه) مدل پیشنهادی، ی) تصویر بدون نویز.

۷- نتیجه‌گیری

این مقاله شامل بررسی یک ساختار تولید و ارزیابی فازی مدل‌های ترکیبی شامل پالایه موجک و دوطرفه تطبیقی است. ترکیب پالایه دوطرفه و موجک قابلیت حذف نویز چند وضوحی را به سیستم می‌دهد به‌طوری‌که می‌توان نویز را در فرکانس‌های مختلف تصویر تشخیص و حذف کند. هزینه‌های حذف نویز روش پیشنهادی و پالایه دوطرفه و موجک استخراج و به‌صورت فازی مورد ارزیابی قرارگرفته‌اند. نتایج مقایسه مدل پیشنهادی نشان‌دهنده کاهش هزینه و تولید تصاویر با نویز کمتر است.

همچنین با در نظر گرفتن زمان، پیچیدگی محاسبات و هزینه مدل‌های حذف نویز، سطح دوم هزینه‌های حذف نویز مطلوب‌تری را تولید می‌کند. در تمامی سطوح موردبررسی، هزینه حذف نویز بهینه روش پیشنهادی از هزینه حذف نویز پالایه دوطرفه و تبدیل موجک کمتر است.

همچنین، به کمک تغییر ترکیب مدل‌ها با پارامترهای غیر بهینه می‌توان هزینه در حدود هزینه بهینه پالایه‌ها تولید نمود. مدل بهینه فراگیر با ساختار [1 0 1 1 1 0 0 0] دارای مناسب‌ترین هزینه در هر سه تصویر به دست آمد. نتایج مقایسه مدل‌ها نشان از عملکرد مطلوب‌تر و پایداری بیشتر مدل فراگیر نسبت به دیگر مدل‌های مورد مقایسه دارد.

۸- مراجع

[1] Ajay Kumar Boyat1 and Brijendra Kumar Joshi,“ A REVIEW PAPER: NOISE MODELS IN DIGITAL IMAGE PROCESSING”,Signal & Image Processing : An International Journal (SIPIJ) Vol.6, No.2, pp. 1-18. 2015.

[2] alaee M, amiri R. Noise Cancellation of RADAR Reflected SignalUsing the Chirplet Transform. 3. Vol. 1, No.1, pp.33-42. 2010. (In Persian)

[3] Karthikeyan P, Vasuki S,” Multiresolution joint bilateral filtering with modified adaptive shrinkage for image denoising”, An International Journal Multimedia Tools and Applications, pp. 297-302. 2015.

[4] Balasubramanian Gopalan, A. Chilambuchelvan, S. Vijayan, and G. Gowrison,” Performance Improvement of Average BasedSpatial Filters through Multilevel Preprocessing using Wavelets”, IEEE Signal Processing Letters, Vol. 22, No. 10, October. pp. 1698-1702, 2015.

[5] Ju Zhang, Guangkuo Lin, Lili Wu, Chen Wang, Yun Cheng", Wavelet and fast bilateral filter based de-speckling method for medical ultrasound images”, Biomed. Signal Proc. and Control, Vol.18, pp.1-10, 2015.

[6] Manoj Diwakar, Sonam, Manoj Kumar,” CT image denoising based on complex wavelet transform using local adaptive thresholding and Bilateral filtering “,WCI '15 Proceedings of the Third International Symposium on Women in Computing and Informatics, pp. 297-302. 2015.

[7] Nidhi Chandrakar, Mr. Devanand Bhonsle,” A New Hybrid Image Denoising Method”, Journal of Engineering, Computers & Applied Sciences (JEC&AS), Volume 2, No.1, January, 2013.

[8] Sudipta Roy, Nidul Sinha, Asoke K. Sen, “An Efficient Denoising Model based on Wavelet and Bilateral Filters”, International Journal of Computer Applications (0975-8887), Vol. 53, No. 10, Sept. 2012.

[9] B. Ergen "Signal and Image Denoising Using Wavelet Transform", Advances in Wavelet Theory and Their Applications in Engineering, Physics and Technology, Dr. Dumitru Baleanu (Ed.), ISBN: 978-953-51-0494-0, InTech, 2012.

[10] C. Tomasi and R. Manduchi, “Bilateral Filtering for Gray and Color Images”, Proc. Int. Conf. Computer Vision, pp. 839–846, 1998.

[11] L. Pape, K. Giammarco, J M. Colombi, C H. Dagli, N H. Kilicay-Ergin, George Rebovich,“ A Fuzzy Evaluation method for System of Systems Meta-architectures”, CSER, pp. 245-254 ,2013.

مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"
ویژه‌نامه کنفرانس بین‌المللی ترکیبیات، رمزنگاری و محاسبات، ص ۱۵۰ -۱۴۳

درستی‌یابی پروتکل‌های رمزنگاری با استفاده از برنامه‌سازی منطق

مصطفی زارع خورمیزی*

استادیار، دانشکده ریاضی و علوم کامپیوتر دانشگاه دامغان

(دریافت: ۹۵/۰۷/۰۵، پذیرش: ۹۶/۰۳/۰۶)

چکیده

در [۱] برونو بلنچت روشی برای درستی‌یابی پروتکل‌های رمزنگاری براساس نمایش مجرد پروتکل‌ها با بندهای هورن ارائه داده است. این روش کاملاً خودکار و کارآمد است و توانایی بررسی تعداد نشست‌ها و فضای پیام نامحدود را دارد. این روش اولیه‌های رمزنگاری مختلف که با قواعد بازنویسی یا معادلات تعریف می‌شوند را پشتیبانی می‌کند. در این مقاله، این روش پیاده‌سازی شده است. اگرچه در این مقاله روی محرمانگی تمرکز می‌کنیم ولی این روش می‌تواند ویژگی‌های امنیتی دیگر نظیر احراز هویت و هم‌ارزی پردازه‌ها را نیز اثبات کند. آزمایش‌ها نشان می‌دهد با این ابزار بسیاری از پروتکل‌ها در زمان کم‌تر از یک ثانیه و با حافظه کمتر از دو مگابایت قابل درستی‌یابی است.

واژه‌های کلیدی: درستی‌یابی خودکار، پروتکل‌های رمزنگاری، بندهای هورن، محرمانگی

۱- مقدمه

پروتکل‌های رمزنگاری[۱] می‌توانند توسط یک رده‌یافت مبتنی بر بندهای هورن[۲] درستی‌یابی شوند؛ هدف اصلی این رده‌یافت اثبات خواص امنیتی پروتکل‌ها در مدل دولو-یائو[۳] به‌صورت کاملاً خودکار بدون محدودیت در تعداد نشست‌ها یا فضای پیام پروتکل‌هاست. برخلاف حالت تعداد نشست‌های محدود که در آن تصمیم‌پذیری قابل اثبات است، حالت تعداد نشست‌های نامحدود در مدل قابل قبولی از پروتکل‌ها تصمیم‌ناپذیر است [۲]. راه‌حل‌های ممکن برای حل این مشکل بر دخالت کاربر، مجاز دانستن عدم توقف و اعمال تقریب‌های دارای صحت تکیه دارند (در این حالت، روش تمامیت ندارد یعنی ویژگی‌های امنیتی درست همواره قابل اثبات نیستند). روش اثبات قضیه [۳] و روش‌های مبتنی بر منطق‌های شناختی نظیر منطق BAN [۴] بر دخالت کاربر یا اثبات‌های دستی تکیه دارند. روش تایپ[۴] [۵-۷] در حالت کلی بر تفسیر کاربر تکیه دارد و ناتمام است. روش فضاهای استرند[۵] [۸] و توابع رتبه [۹] نیز روش‌هایی را فراهم می‌آورند که می‌تواند تعداد نشست‌های نامحدود را پشتیبانی کند ولی ناتمام است.

روش‌های زیادی بر نمایش مجرد[۶] دارای صحت تکیه دارند [۱۰]: این روش‌ها معمولاً با محاسبه تقریب دست بالا از دانش مهاجم[۷] در بررسی امکان حمله‌ها دست بالا می‌گیرند. این کار دست‌یابی به روش‌های کاملاً خودکار ولی ناتمام را امکان‌پذیر می‌سازد. رده‌یافت بندهای هورن یکی از این روش‌هاست. این روش ابتدا توسط ویدن باخ[۸] [۱۱] معرفی شد. مقاله حاضر نسخه‌ای از این روش و توسیع‌های آن ارائه می‌کند که توسط بلنچت توسعه داده شده است. در این روش، پیام‌ها با عبارت M نشان داده می‌شوند؛ حقیقت attacker(M) به این معنی است که مهاجم می‌تواند پیام M را داشته باشد؛ بندهای هورن (یعنی قاعده‌های برنامه‌نویسی منطق) قواعد ایجابی بین این حقیقت‌ها را ارائه می‌کنند.

یک الگوریتم تجزیه کارآمد مشخص می‌کند که آیا یک حقیقت از بندها قابل استنتاج است یا نه، این می‌تواند برای اثبات خواص امنیتی به‌کار رود. به‌ویژه، هنگامی که attacker(M) از بندها قابل استنتاج نباشد، مهاجم نمی‌تواند M را داشته باشد، یعنی، M محرمانه است. این روش ناتمام است زیرا تعداد تکرارها از هر عمل در پروتکل را نادیده می‌گیرد. (بندهای هورن می‌توانند

* رایانامه نویسنده مسئول: mostafazaare@du.ac.ir

1- cryptographic protocols
2- Horn clause
3- Dolev-Yao
4- typing
5- strand space
6- abstrac representation
7- attacker
8- Weidenbach

هر تعداد از دفعات به‌کار برده شوند.) این نمایش مجرد کلید اجتناب از محدودیت در تعداد اجراهای پروتکل است. این روش دارای صحت است، به این معنی که اگر درست‌یاب رخنه‌ای در پروتکل پیدا نکند، آن‌گاه رخنه‌ای وجود ندارد. بنابراین، درست‌یاب تضمین امنیتی واقعی فراهم می‌سازد. در مقابل، ممکن است یک حمله نادرست علیه پروتکل ارائه دهد. اما، حمله‌های نادرست در عمل چنان‌که آزمایش‌ها نشان می‌دهد، نادر هستند. توقف در حالت کلی تضمین‌شده نیست، اما روی زیرکلاس خاصی از پروتکل‌ها تضمین می‌شود و با تقریب‌های اضافی می‌تواند در همه حالت‌ها به‌دست آید.

بدون این تقریب‌های اضافی، اگرچه این روش همواره متوقف نمی‌شود و ناتمام است، اما در عمل تعادل خوبی فراهم می‌آورد: این روش در بسیاری از حالت‌ها متوقف می‌شود و بسیار کارآمد و دقیق است. می‌تواند رده وسیعی از اولیه‌های رمزنگاری که با قواعد بازنویسی[1] یا معادلات تعریف می‌شوند نظیر رمزنگاری کلید- مشترک و کلید- عمومی (رمزگذاری و امضاءها)، توابع چکیده‌ساز و توافق کلید دفی-هلمن[2] را پشتیبانی کند. می‌تواند خواص امنیتی مختلف (محرمانگی، احراز هویت و هم‌ارزی پردازش‌ها) را ثابت کند. در این مقاله بر محرمانگی تمرکز می‌کنیم.

در بخش ۲ نمایش پروتکل با جزئیات ارائه می‌شود. در بخش ۳ الگوریتم تجزیه توصیف می‌شود. در بخش ۴ نتایج برخی آزمایش‌ها بیان می‌شود و بخش ۵، بخش نتیجه‌گیری است.

۲- نمایش مجرد پروتکل‌ها با بندهای هورن

یک پروتکل با مجموعه‌ای از بندهای هورن نمایش داده می‌شود؛ نحو این بندها در شکل (۱) نشان داده شده است.

عبارت‌ها	$M.N ::=$
متغیر	x
نام	
کاربرد تابع	$f(M_1. \dots . M_n)$
حقیقت	$F ::= p(M_1. \dots . M_n)$
بند هورن	$R ::= F_1 \wedge \dots \wedge F_n \Rightarrow F$

شکل (۱): نحو نمایش پروتکل

در این شکل، x روی متغیرها، a روی نام‌ها، fروی نمادهای تابعی و p روی نمادهای محمولی تغییر می‌کنند. عبارات M پیام‌هایی که بین شرکت‌کننده‌ها در پروتکل مبادله می‌شود را نمایش می‌دهند. یک متغیر می‌تواند هر عبارتی را نمایش دهد. نام‌ها مقدارهای اتمی نظیر کلیدها و نانس‌ها (اعداد تصادفی) را نمایش می‌دهند. هر شرکت‌کننده توانایی تولید نام‌های جدید را دارد: نام‌های جدید در هر اجرای پروتکل تولید می‌شوند. در این‌جا، نام‌های تولیدشده به‌عنوان تابع‌هایی از پیام‌هایی که قبلاً توسط شرکت‌کننده‌ای که نام را تولید می‌کند دریافت شده است، درنظر گرفته می‌شوند. بنابراین، نام‌ها تنها هنگامی‌که پیام‌های قبلی متفاوت باشند، متمایز هستند. کاربردهای تابع $f(M_1. \dots . M_n)$ عبارت‌ها را می‌سازد: مثال‌های تابع‌ها رمزگذاری و تابع‌های چکیده‌ساز هستند. یک حقیقت $F = p(M_1. \dots . M_n)$ یک خاصیت از پیام‌های M_1، ...، M_nرا بیان می‌کند. چندین محمول p می‌تواند به کار رود اما برای اولین مثال از محمول attacker استفاده می‌کنیم، به‌طوریکه حقیقت attacker(M) به این معنی است که «مهاجم می‌تواند پیام M را داشته باشد». بند $R = F_1 \wedge \dots \wedge F_n \Rightarrow F$ به این معنی است که، اگر همه حقیقت‌های F_1، ...، F_n درست باشند، آن‌گاه F نیز درست است. یک بند بدون هیچ فرضی $\Rightarrow F$ برای سادگی با F نشان داده می‌شود.

به‌عنوان مثال جاری در این مقاله، از پروتکل دست‌دادن[3] ساده زیر استفاده می‌کنیم:

پیام ۱. $A \to B: \{|[k]_{sk_A}|\}^a_{pk_B}$

پیام ۲. $B \to A: \{|s|\}^s_k$

sk_A کلید خصوصیA، pk_Aکلید عمومیA، sk_Bکلید خصوصی B و pk_B کلید عمومی B را نشان می‌دهد.

۲-۱- نمایش اولیه‌ها

اولیه‌های رمزنگاری با تابع‌ها نمایش داده می‌شوند. به‌عنوان مثال، رمزگذاری کلید عمومی را با تابع pencrypt$(m.pk)$ نشان می‌دهیم که دو شناسه دارد: پیام m که باید رمزگذاری شود و کلید عمومی.pk یک تابع pk وجود دارد که کلید عمومی را از روی کلید خصوصی می‌سازد. (هم‌چنین می‌توانیم دو تابع pk و sk داشته باشیم که از یک راز به‌ترتیب کلیدهای عمومی و خصوصی را می‌سازند.) کلید خصوصی با یک نام نمایش داده می‌شود که هیچ شناسه‌ای ندارد (یعنی، فقط یک نسخه از این نام

1- rewrite
2- Deffie-Hellman
3- handshake

وجود دارد)$sk_A[\,]$ برای A و $sk_B[\,]$ برایB. بنابراین $pk_A = \mathrm{pk}(sk_A[\,])$و $pk_B = \mathrm{pk}(sk_B[\,])$.

به‌طور کلی‌تر، دو نوع از تابع‌ها درنظر می‌گیریم: سازنده‌ها و مخرب‌ها. سازنده‌ها تابع‌هایی هستند که صریحاً در عبارت‌هایی که پیام‌ها را نمایش می‌دهند، ظاهر می‌شوند.

برای نمونه، pencryptو pk سازنده هستند. مخرب‌ها عبارت‌ها را دست‌کاری می‌کنند. یک مخرب g با یک مجموعه‌ی $\mathrm{def}(g)$ از قاعده‌های بازنویسی به‌صورت $g(M_1.\ldots.M_n) \to M$ تعریف می‌شود که M_1، ...، M_n و Mعبارت‌هایی هستند که تنها شامل متغیرها و سازنده‌ها هستند و متغیرهای M همگی در M_1، ...، M_n ظاهر می‌شوند. برای مثال، رمزگشایی pencrypt یک مخرب است که با

$$\mathrm{pencrypt}\big(\mathrm{pencrypt}\big(m.\mathrm{pk}(sk)\big).sk\big) \to m$$

تعریف می‌شود. این قاعده بازنویسی این‌که رمزگشایی یک متن رمز با کلید خصوصی متناظر، متن ساده را به‌دست می‌دهد، را مدل می‌کند.

تابع‌های دیگر به‌طور مشابه تعریف می‌شوند:

- برای امضاءها، از یک سازنده sign استفاده می‌کنیم و $\mathrm{sign}(m.sk)$ به معنای امضای پیام m با کلید خصوصی sk است. یک مخرب getmess که با $\mathrm{getmess}\big(\mathrm{sign}(m.sk)\big) \to m$ تعریف می‌شود پیام را بدون امضاء آن به‌دست می‌دهد، و $\mathrm{checksign}\big(\mathrm{sign}(m.sk).\mathrm{pk}(sk)\big) \to m$ پیام را برمی‌گرداند تنها اگر امضاء معتبر باشد.
- رمزگذاری کلید- مشترک یک سازنده sencrypt و رمزگشایی یک مخرب sdecrypt است که با $\mathrm{sdecrypt}(\mathrm{sencrypt}(m.k).k) \to m$

تعریف می‌شوند.

- یک تابع چکیده‌ساز یک- طرفه با یک سازنده h نمایش داده می‌شود (و هیچ مخربی ندارد).
- چندتایی‌های n موضعی با سازنده $(-.\ldots.-)$ نمایش داده می‌شوند و n مخرب $i\mathrm{th}_n$ با $i \in \{1.\ldots.n\}$ و $i\mathrm{th}_n((x_1.\ldots.x_n)) \to x_i$ تعریف می‌شوند. چندتایی‌ها می‌توانند برای نمایش ساختارهای داده مختلف در پروتکل‌ها به‌کار روند.

قواعد بازنویسی روش انعطاف‌پذیری برای تعریف اولیه‌های رمزنگاری بسیاری پیشنهاد می‌کنند که می‌تواند با استفاده از معادلات بیش‌تر گسترش یابد.

۲-۲- نمایش توانایی‌های مهاجم

فرض می‌کنیم که پروتکل در حضور یک مهاجم اجرا می‌شود که می‌تواند همه پیام‌ها را شنود کند، از پیام‌هایی که دریافت کرده است پیام‌های جدید محاسبه کند و هر پیامی که بتواند بسازد را ارسال کند. این مدل دولو-یائو [۱۲] نامیده می‌شود.

ابتدا توانایی‌های محاسباتی مهاجم را کدگذاری می‌کنیم. کدگذاری پروتکل در بخش ۲-۳ انجام می‌شود. مهاجم در طول محاسبات خود می‌تواند همه سازنده‌ها و مخرب‌ها را به‌کار برد. اگر f یک سازنده n موضعی باشد، بند زیر را خواهیم داشت:

$$\mathrm{attacker}(x_1) \wedge \ldots \wedge \mathrm{attacker}(x_n) \Rightarrow \mathrm{attacker}\big(f(x_1.\ldots.x_n)\big)$$

اگر g یک مخرب باشد، برای هر قاعده بازنویسی $g(M_1.\ldots.M_n) \to M$ در $\mathrm{def}(g)$، بند زیر را داریم:

$$\mathrm{attacker}(M_1) \wedge \ldots \wedge \mathrm{attacker}(M_n) \Rightarrow \mathrm{attacker}(M)$$

مخرب‌ها هرگز در بندها ظاهر نمی‌شوند، آن‌ها توسط تطابق الگو روی پارامترهایشان (در این‌جا M_1، ...، M_n) در فرضیات بند و تولید نتیجه آن‌ها در حکم کدگذاری می‌شوند. در حالت خاص رمزگذاری کلید- عمومی، به

$$\begin{aligned}&\mathrm{attacker}(m) \wedge \mathrm{attacker}(pk)\\ &\Rightarrow \mathrm{attacker}\big(\mathrm{pencrypt}(m.pk)\big).\\ &\mathrm{attacker}(sk)\\ &\Rightarrow \mathrm{attacker}(\mathrm{pk}(sk)).\\ &\mathrm{attacker}\Big(\mathrm{pencrypt}\big(m.\mathrm{pk}(sk)\big)\Big) \wedge \mathrm{attacker}(sk)\\ &\Rightarrow \mathrm{attacker}(m).\end{aligned} \qquad (۱)$$

منجر می‌شود که بندهای اول و دوم با سازنده‌های pencrypt و pk متناظر هستند و بند آخر با مخرب pdecrypt متناظر است. هنگامی‌که مهاجم پیام رمزگذاری‌شده $\mathrm{pencrypt}(m.pk)$و کلید رمزگشایی sk را دارد، آن‌گاه او هم‌چنین متن ساده m را دارد. (فرض می‌کنیم که رمزنگاری کامل است، بنابراین، مهاجم می‌تواند از پیام رمزشده به متن ساده دست یابد فقط اگر کلید را داشته باشد.)

بندهای مربوط به امضاءها (sign، getmess، checksign) و رمزگذاری کلید- مشترک (cencrypt، sdecrypt) در شکل (۲) ارائه شده است.

بندهای بالا توانایی‌های محاسباتی مهاجم را توصیف می‌کند. علاوه‌بر این، مهاجم در ابتدا کلیدهای عمومی شرکت‌کنندگان در

پروتکل را دارد. بنابراین، مهاجم بندهای (($\mathrm{attacker}(\mathrm{pk}(sk_A[\,]))$ و (($\mathrm{attacker}(\mathrm{pk}(sk_B[\,]))$را اضافه می‌کند. به‌ویژه، $a[\,]$کلید خصوصی هر شرکت‌کننده غیرامین را نمایش می‌دهد که کلید عمومی او $\mathrm{pk}(a[\,])$ است و مهاجم می‌تواند با استفاده از بندهای مربوط به سازنده pk آن را محاسبه کند.

۲-۳- نمایش پروتکل

حال، این‌که خود پروتکل چگونه نمایش داده می‌شود را توصیف می‌کنیم. فرض کنیم A و B قصد صحبت با یک شرکت‌کننده دلخواه A، Bیا هم‌چنین شرکت‌کنندگان بداندیش که با مهاجم نمایش داده می‌شوند، را دارند. بنابراین، اولین پیامی که توسط A ارسال می‌شود، می‌تواند

$$\mathrm{pencrypt}(\mathrm{sign}(k.sk_A[\,]).\mathrm{pk}(x))$$

برای هر x باشد. مهاجم مجاز است پروتکل را با هر شرکت‌کننده‌ای که بخواهد شروع کند، یعنی مهاجم یک پیام اولیه به A می‌فرستد که کلید عمومی شرکت‌کننده‌ای را مشخص می‌کند که A باید با او صحبت کند. این شرکت‌کننده می‌تواند B یا هر شرکت‌کننده دیگری باشد که با مهاجم نمایش داده می‌شود. بنابراین، اگر مهاجم یک کلید $\mathrm{pk}(x)$ را داشته باشد، می‌تواند پیام $\mathrm{pk}(x)$ را به A بفرستد؛ A با اولین پیام خود پاسخ می‌دهد که مهاجم می‌تواند آن‌را شنود کند، بنابراین، $\mathrm{pencrypt}(\mathrm{sign}(k.sk_A[\,]).\mathrm{pk}(x))$را به‌دست می‌آورد. در نتیجه، یک بند به صورت:

$$\mathrm{attacker}(\mathrm{pk}(x))$$
$$\Rightarrow \mathrm{attacker}\left(\mathrm{pencrypt}\left(\mathrm{sign}\left(k.sk_A[\,]\right).\mathrm{pk}(x)\right)\right)$$

خواهیم داشت. علاوه‌براین، در هر اجرای پروتکل یک کلید جدید تولید می‌شود. درنتیجه، اگر دو کلید متفاوت $\mathrm{pk}(x)$ توسط A دریافت شود، کلیدهای k تولید شده مطمئناً متفاوت هستند: k به $\mathrm{pk}(x)$ بستگی دارد. بند به

$$\mathrm{attacker}(\mathrm{pk}(x))$$
$$\Rightarrow \mathrm{attacker}\left(\mathrm{pencrypt}\left(\mathrm{sign}\left(k[\mathrm{pk}(x)].sk_A[\,]\right).\mathrm{pk}(x)\right)\right)$$

(۲)

تبدیل می‌شود.

هنگامی که B یک پیام دریافت می‌کند، آن را با کلید خصوصی خود sk_B رمزگشایی می‌کند، بنابراین B پیامی به صورت $\mathrm{pencrypt}(x'.\mathrm{pk}(sk_B[\,]))$ انتظار دارد. سپس، Bبررسی می‌کند که آیا A، x'را امضاء کرده است، یعنی، B، $\mathrm{checksign}(x'.pk_A)$را ارزیابی می‌کند و این تنها زمانی موفق است که$x' = \mathrm{sign}(y.sk_A[\,])$ اگر چنین باشد، او فرض می‌کند که کلید y را تنها A می‌داند، و یک راز s (یک ثابت که مهاجم آن را ندارد) که توسط y رمز شده است را می‌فرستد. فرض می‌کنیم مهاجم پیام فرستاده شده از طرف A را ذخیره می‌کند و پیام ارسال شده توسط B را شنود می‌کند. بنابراین بند حاصل به صورت

$$\mathrm{attacker}\left(\mathrm{pencrypt}\left(\mathrm{sign}(y.sk_A[\,]).\mathrm{pk}(sk_B[\,])\right)\right)$$
$$\Rightarrow \mathrm{attacker}\left(\mathrm{sencrypt}(s.y)\right)$$

است.

۲-۴- خلاصه

همان‌گونه که در شکل (۲) برای پروتکل جاری نشان داده شده است، یک پروتکل می‌تواند با سه مجموعه از بندهای هورن نمایش داده شود:

- بندهایی که توانایی‌های محاسباتی مهاجم را نمایش می‌دهند: سازنده‌ها، مخرب‌ها و تولید نام.
- حقیقت‌های متناظر با دانش اولیه مهاجم. در حالت کلی، حقیقت‌هایی وجود دارند که کلیدهای عمومی شرکت‌کنندگان و نام آن‌ها را به مهاجم می‌دهند.
- بندهایی که پیام‌های پروتکل را نمایش می‌دهند. برای هر پیام پروتکل یک مجموعه از بندها وجود دارد. در مجموعه‌ی متناظر با پیامi ام، ارسال شده توسط شرکت کنندهX، بندها به‌صورت

$$\mathrm{attacker}(M_{j_1}) \wedge \ldots \wedge \mathrm{attacker}(M_{j_n})$$
$$\Rightarrow \mathrm{attacker}(M_i)$$

است که M_{j_1}، ...، M_{j_n} الگوهای پیام‌های دریافت شده توسط X قبل از ارسالi امین پیام است و M_i الگوی پیام i است.

توانایی‌های محاسباتی مهاجم:

برای هر سازنده f با شناسه‌ی n:

$$\mathrm{attacker}(x_1) \wedge \ldots \wedge \mathrm{attacker}(x_n)$$
$$\Rightarrow \mathrm{attacker}\left(f(x_1.\ldots.x_n)\right)$$

برای هر مخرب g، برای هر قاعده بازنویسی $g(M_1.\ldots.M_n) \rightarrow M$ در$\mathrm{def}(g)$:

$$\mathrm{attacker}(M_1) \wedge \ldots \wedge \mathrm{attacker}(M_n) \Rightarrow \mathrm{attacker}(M)$$

یعنی

pencrypt	$\text{attacker}(m) \wedge \text{attacker}(pk)$ $\Rightarrow \text{attacker}(\text{pencrypt}(m.pk))$
pk	$\text{attacker}(sk) \Rightarrow \text{attacker}(\text{pk}(sk))$
pdecrypt	$\text{attacker}\left(\text{pencrypt}(m.\text{pk}(sk))\right) \wedge \text{attacker}(sk)$ $\Rightarrow \text{attacker}(m)$
sign	$\text{attacker}(m) \wedge \text{attacker}(sk)$ $\Rightarrow \text{attacker}(\text{sign}(m.sk))$
getmess	$\text{attacker}(\text{sign}(m.sk)) \Rightarrow \text{attacker}(m)$
checksign	$\text{attacker}(\text{sign}(m.sk)) \wedge \text{attacker}(sk)$ $\Rightarrow \text{attacker}(m)$
sencrypt	$\text{attacker}(m) \wedge \text{attacker}(k)$ $\Rightarrow \text{attacker}(\text{sencrypt}(m.k))$
sdecrypt	$\text{attacker}(\text{sencrypt}(m.k)) \wedge \text{attacker}(k)$ $\Rightarrow \text{attacker}(m)$

تولید نام:

$\text{attacker}(a[\,])$

دانش اولیه:

$\text{attacker}(\text{pk}(sk_A[\,])).\text{attacker}(\text{pk}(sk_B[\,]))$

پروتکل:

پیام اول:

$\text{attacker}(\text{pk}(x))$

$\Rightarrow \text{attacker}\left(\text{pencrypt}(\text{sign}(k[\text{pk}(x)].\, sk_A[\,]).\text{pk}(x))\right)$

پیام دوم:

$\text{attacker}\left(\text{pencrypt}(\text{sign}(y.\, sk_A[\,]).\text{pk}(sk_B[\,]))\right)$

$\Rightarrow \text{attacker}(\text{sencrypt}(s.y))$

شکل (۲). خلاصه نمایش پروتکل مثال جاری

۲-۵- محک محرمانگی

هدف ما مشخص کردن خواص محرمانگی است: برای مثال، آیا مهاجم می‌تواند راز s را به دست آورد؟ یعنی، آیا حقیقت $\text{attacker}(s)$از بندها قابل استنتاج است؟ اگر $\text{attacker}(s)$ قابل استنتاج باشد، دنباله‌ی بندهایی که برای استنتاج $\text{attacker}(s)$به‌کار می‌روند به توصیف یک حمله منجر می‌شوند. عبارت M محرمانه است اگر مهاجم نتواند با شنیدن و ارسال پیام‌ها و انجام محاسبات به آن دست یابد.

در مثال جاری، $\text{attacker}(s)$از بندها قابل استنتاج است. استنتاج به صورت زیر است. مهاجم نام جدید $a[\,]$ (به عنوان یک کلید خصوصی) را تولید می‌کند، سپس $\text{pk}(a[\,])$ را با استفاده از بند مربوط به pk محاسبه می‌کند و با استفاده از بند مربوط به پیام اول

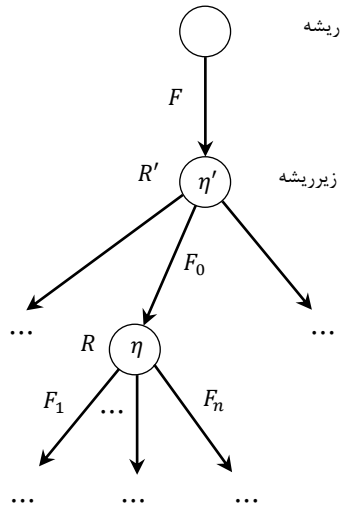
$$\text{pencrypt}(\text{sign}(k[\text{pk}(a[\,])].\, sk_A[\,]).\text{pk}(a[\,]))$$

را به دست می‌آورد. وی این پیام را با استفاده از بند مربوط به pdecrypt و آگاهی‌اش از $a[\,]$ رمزگشایی می‌کند و $\text{sign}(k[\text{pk}(a[\,])].\, sk_A[\,])$ را به دست می‌آورد. سپس امضاء را با استفاده از بند pencrypt و دانش اولیه‌اش از $\text{pk}(sk_B[\,])$ مجدداً رمزگذاری نموده و $\text{pencrypt}(\text{sign}(k[\text{pk}(a[\,])].\, sk_A[\,]).\text{pk}(a[\,]))$ را به‌دست می‌آورد. با استفاده از بند مربوط به پیام دوم، $\text{sencrypt}(s.k[\text{pk}(a[\,])])$ را به‌دست می‌آورد. از طرف دیگر، از $\text{sign}(k[\text{pk}(a[\,])].\, sk_A[\,])$ با استفاده از بند مربوط به getmess، $k[\text{pk}(a[\,])]$را به‌دست می‌آورد. بنابراین می‌تواند با استفاده از بند مربوط به sdecrypt، $\text{sencrypt}(s.k[\text{pk}(a[\,])])$را رمزگشایی و در نتیجه s را به‌دست آورد. به عبارت دیگر، مهاجم یک نشست بین A و یک شرکت‌کننده غیر امین با کلید خصوصی $a[\,]$ آغاز می‌کند. او اولین پیام $\text{pencrypt}(\text{sign}(k.\, sk_A[\,]).\text{pk}(a[\,]))$ را می‌گیرد، آن را رمزگشایی نموده و مجدداً با $\text{pk}(sk_B[\,])$ رمز نموده و آن را به B می‌فرستد. برایB، این پیام به صورت اولین پیام از یک نشست بین A و B به نظر می‌رسد، بنابراین B با $\text{sencrypt}(s.k)$ پاسخ می‌دهد، که مهاجم می‌تواند آن را رمزگشایی کند، زیرا او k را از اولین پیام به دست آورده است.

در نتیجه، استنتاج حاصل با حمله شناخته شده علیه این پروتکل متناظر است. در مقابل، اگر پروتکل را با افزودن کلید عمومی B در پیام اول $\left\{\left|\left[\langle \text{pk}_B.\, k\rangle\right]_{sk_A}\right|\right\}^{a}_{\text{pk}_B}$ اصلاح کنیم، $\text{attacker}(s)$ از بندها قابل استنتاج نیست. بنابراین، پروتکل اصلاح شده محرمانگی s را حفظ می‌کند.

در ادامه، این‌که چه هنگام یک حقیقت داده شده از یک مجموعه از بندها استنتاج می‌شود را به طور صوری تعریف می‌کنیم. فرض‌های یک بند به عنوان مجموعه‌های چندگانه درنظر گرفته می‌شوند. به این معنی که ترتیب فرض‌ها مهم نیست ولی تعداد تکرارهای یک فرض مهم است. از R برای بندها (قاعده‌های برنامه‌نویسی منطق)، H برای فرضیات و C برای حکم استفاده می‌کنیم.

تعریف ۱ (شمول) گوییم $H_1 \Rightarrow C_1$ شامل $H_2 \Rightarrow C_2$ است و می‌نویسیم$(H_1 \Rightarrow C_1) \supseteq (H_2 \Rightarrow C_2)$ ، اگر و تنها اگر جانشینی σ وجود داشته باشد به طوری که $\sigma C_1 = C_2$ و $\sigma H_1 \subseteq H_2$ (شمول مجموعه‌های چندگانه).



شکل (۳): استنتاج F

استنتاج به‌صورت زیر تعریف می‌شود، شکل (۳) را ببینید.

تعریف ۲ (استنتاج‌پذیری) فرض کنید F یک حقیقت بسته، یعنی، یک حقیقت بدون متغیر باشد. فرض کنید $\mathcal{R}$ یک مجموعه از بندها باشد. F از $\mathcal{R}$ استنتاج‌پذیر است اگر و تنها اگر یک استنتاج برای F از $\mathcal{R}$ وجود داشته باشد، یعنی، یک درخت متناهی که به صورت زیر تعریف می‌شود:

۱. رأس‌های (به‌جز ریشه) درخت با بندهای $R \in \mathcal{R}$ برچسب‌گذاری می‌شوند؛
۲. یال‌های درخت با حقیقت‌های بسته برچسب‌گذاری می‌شوند؛
۳. اگر درخت دارای رأسی باشد که با R برچسب‌گذاری شده است و یک یال وارد شونده به آن با F_0 و n یال خارج شونده از آن با F_1، ...، F_n نشانه‌گذاری شده‌اند، آن‌گاه $R \supseteq F_1 \wedge \cdots \wedge F_n \Rightarrow F_0$.
۴. ریشه یک یال خارج شونده دارد که با F نشانه‌گذاری شده است. تنها پسر ریشه، زیرریشه نامیده می‌شود.

۳- الگوریتم تجزیه

نمایش پروتکل، مجموعه‌ای از بندهای هورن و هدف تعیین این است که آیا یک حقیقت داده شده می‌تواند از این بندها استنتاج شود یا نه. این دقیقاً مسأله‌ای است که با سیستم‌های پرولوگ[1] معمول حل می‌شود. اما، در این‌جا، نمی‌توانیم از این سیستم‌ها استفاده کنیم، زیرا ممکن است متوقف نشوند. برای مثال، بند

$$\text{attacker}\left(\text{pencrypt}\left(m.\text{pk}(sk)\right)\right) \wedge \text{attacker}(sk) \Rightarrow \text{attacker}(m)$$

منجر به درنظر گرفتن بندهای پیچیده و پیچیده‌تر با تعداد نامحدودی رمزگذاری می‌شود. البته می‌توانیم برای حل مشکل، عمق عبارت‌ها را به دلخواه محدود کنیم، اما می‌توان بهتر از آن را انجام داد.

۳-۱. الگوریتم پایه

ابتدا تجزیه را تعریف می‌کنیم: هنگامی که حکم یک بند R با فرض بند دیگر (یا همان بند) R' متحد است، تجزیه، بند جدیدی استنتاج می‌کند که متناظر با کاربرد R و R' یکی پس از دیگری است. به‌طور صوری، تجزیه به صورت زیر تعریف می‌شود:

تعریف ۳ فرض کنید R و R' دو بند باشند، $R = H \Rightarrow C$ و $R' = H' \Rightarrow C'$. فرض کنید $F_0 \in H'$ موجود باشد به طوری‌که C و F_0 متحد باشند و σ کلی‌ترین متحدکننده[2] C و F_0 باشد. در این حالت، تعریف می‌کنیم

$$R \circ_{F_0} R' = \sigma\big(H \cup (H' \setminus \{F_0\})\big) \Rightarrow \sigma C'$$

برای مثال، اگر R بند (۲) و R' بند (۱) و حقیقت F_0 به‌صورت $F_0 = \text{attacker}\left(\text{pencrypt}\left(m.\text{pk}(sk)\right)\right)$ باشد، آن‌گاه $R \circ_{F_0} R'$،

$$\text{attacker}(\text{pk}(x)) \wedge \text{attacker}(x) \Rightarrow \text{attacker}\big(\text{sign}(k[\text{pk}(x)].sk_A[\,])\big)$$

است که در آن جانشینی

$$\sigma = \{sk \mapsto x.m \mapsto \text{sign}(k[\text{pk}(x)].sk_A[\,])\}$$

است. الگوریتم تجزیه در دو فاز کار می‌کند که در شکل (۴) توصیف شده است. فاز اول مجموعه‌ی اولیه از بندها را به یک بند جدید تبدیل می‌کند که حقیقت‌های یکسانی را استنتاج می‌کند. فاز دوم از یک جستجوی عمق-اول برای تشخیص این‌که یک حقیقت می‌تواند از بندها استنتاج شود یا نه استفاده می‌کند.

فاز اول: اشباع

$\text{saturate}(\mathcal{R}_0)=$

۱. $\mathcal{R} \leftarrow \emptyset$.

برای هر $R \in \mathcal{R}_0$، $\mathcal{R} \leftarrow \text{elim}(\{R\} \cup \mathcal{R})$.

۲. اعمال زیر را تا رسیدن به یک نقطه ثابت تکرار کن

برای هر $R \in \mathcal{R}$ به طوری که $sel(R) = \emptyset$،

برای هر $R' \in \mathcal{R}$، برای هر $F_0 \in sel(R')$ به طوری که $R \circ_{F_0} R'$ تعریف شده باشد،

1- Prolog

2- most general unifier

$\mathcal{R} \leftarrow \text{elim}(\{R \circ_{F_0} R'\} \cup \mathcal{R})$

۳. $\{R \in \mathcal{R} \mid sel(R) = \emptyset\}$ را برگردان.

فاز دوم: جستجوی عقب‌گرد عمق-اول

$$\text{deriv}\left(R, \mathcal{R}, \mathcal{R}_1\right) = \begin{cases} \emptyset & \text{اگر } R' \in \mathcal{R} \text{ وجود داشته باشد به طوری که } R' \supseteq R \\ \{R\} & \text{درغیر این صورت اگر } sel(R) = \emptyset \\ \cup\{\text{deriv}\left(R' \circ_{F_0} R, \{R\} \cup \mathcal{R}, \mathcal{R}_1\right) & \text{در غیر این‌صورت} \\ \mid R' \in \boldsymbol{R}, F_0 \in sel(R), & \{\text{به طوری که } R' \circ_{F_0} R \text{ تعریف شده باشد} \end{cases}$$

$$\text{derivable}\left(F, \mathcal{R}_1\right) = \text{deriv}(F \Rightarrow F, \emptyset, \mathcal{R}_1)$$

شکل (۴). الگوریتم تجزیه

۴- نتیجه آزمایش‌ها

این روش برای اثبات خواص محرمانگی و احراز هویت در بسیاری از پروتکل‌ها به‌کار رفته است، از جمله نسخه معیوب و صحیح پروتکل کلید عمومی نیدهام-شرودر[1] [۱۳، ۱۴]، پروتکل کلید مشترک نیدهام-شرودر [۱۳، ۴، ۱۵]، پروتکل کلید عمومی وو-لم[2] [۱۶، ۱۷]، پروتکل کلید مشترک وو-لم [۱۶، ۱۸، ۱۹، ۱۷، ۲۰]، پروتکل دنینگ-ساسکو[3] [۲۱، ۱۹]، پروتکل یالوم[4] [۴]، پروتکل اوتوی-ریس[5] [۲۲، ۴، ۳]، و پروتکل اسکیم[6] [۲۳]. هیچ حمله نادرستی در این آزمون‌ها رخ نداده است و تنها حالت عدم توقف در برخی نسخه‌های معیوب پروتکل کلید مشترک وو-لم بوده است. این پروتکل‌ها در کمتر از یک ثانیه روی یک کامپیوتر Intel Core i3-2310M 2.10GHz درستی‌یابی شده‌اند.

۵- نتیجه‌گیری

یک جنبه مهم رهیافت بندهای هورن توانایی اثبات خواص امنیتی پروتکل‌ها برای تعداد نامحدودی از نشست‌ها به روشی کاملاً خودکار است. این برای تصدیق پروتکل‌ها اساسی است. این رهیافت هم‌چنین رده‌ی وسیعی از اولیه‌های رمزنگاری را پشتیبانی می‌کند و می‌تواند رده‌ی وسیعی از خواص امنیتی را ثابت کند.

از طرف دیگر، مسأله درستی‌یابی پروتکل‌ها برای تعداد نامحدود از نشست‌ها تصمیم‌ناپذیر است، بنابراین این رهیافت ناتمام است یعنی همواره متوقف نمی‌شود و تقریب را به‌کار می‌گیرد، بنابراین پروتکل‌های امنی وجود دارند که امن بودن آن‌ها را نمی‌تواند اثبات کند، اگرچه در عمل بسیار دقیق و کارآ است.

1- Needham-Schroeder
2- Woo-Lam
3- Denning-Sacco
4- Yahalom
5- Otway-Rees
6- Skeme

۶- مراجع

[1] B. Blanchet, "An efficient cryptographic protocol verifier based on Prolog rules," In 14th IEEE Computer Security Foundations Workshop (CSFW-14), IEEE Computer Society, pp. 82–96, 2001.

[2] N. Durgin, P. Lincoln, J. C. Mitchell, and A. Scedrov, "Multiset rewriting and the complexity of bounded security protocols," Journal of Computer Security, vol. 12, no. 2, pp. 247–311, 2004.

[3] L. C. Paulson, "The inductive approach to verifying cryptographic protocols," Journal of Computer Security, vol. 6 (1–2), pp. 85–128, 1998.

[4] M. Burrows, M. Abadi, and R. Needham, "A Logic of Authentication," Proceedings of the Royal Society of London A, vol. 426, pp. 233–271, 1989.

[5] M. Abadi, "Secrecy by Typing in Security Protocols," Journal of the ACM, vol. 46, no. 5, pp. 749–786, 1999.

[6] L. Cardelli, G. Ghelli, and A. D. Gordon, "Secrecy and Group Creation," In C. Palamidessi, editor, CONCUR 2000: Concurrency Theory, volume 1877 of Lecture Notes on Computer Science, pp. 365–379. Springer Verlag, 2000.

[7] M. Hennessy and J. Riely, "Information Flow vs. Resource Access in the Asynchronous Pi-Calculus," In Proceedings of the 27th International Colloquium on Automata, Languages and Programming, Lecture Notes on Computer Science, pp. 415–427, Springer Verlag, 2000.

[8] F. J. Thayer Fabrega, J. C. Herzog, and J. D. Guttman, "Strand Spaces: Proving Security Protocols Correct," Journal of Computer Security, vol. 7, pp. 191-230, 1999.

[9] J. Heather and S. Schneider, "Towards automatic verification of authentication protocols on an unbounded network," In 13th IEEE Computer Security Foundations Workshop (CSFW-13), pp. 132–143, Cambridge, England, July 2000.

[10] P. Cousot and R. Cousot, "Systematic design of program analysis frameworks," In 6th Annual ACM Symposium on Principles of Programming Languages, pp. 269–282, 1979.

[11] C. Weidenbach, "Towards an automatic analysis of security protocols in first-order logic," In 16th International Conference on Automated Deduction (CADE-16), vol. 1632 of Lecture Notes in Artificial Intelligence, pp. 314–328, 1999.

[12] D. Dolev and A. C. Yao, "On the security of public key protocols," IEEE Transactions on Information Theory, IT, vol. 29, no. 12, pp. 198–208, 1983.

[13] R. M. Needham and M. D. Schroeder, "Using encryption for authentication in large networks of computers," Commun. ACM, vol. 21, no. 12, pp. 993–999, 1978.

[14] G. Lowe, "Breaking and fixing the Needham-Schroeder public-key protocol using FDR," In Tools and Algorithms for the Construction and Analysis of Systems, vol. 1055 of LNCS, pp. 147–166. Springer, 1996.

[15] R. M. Needham and M. D. Schroeder, "Authentication revisited," Operating Systems Review, vol. 21, no. 1, pp. 7, 1987.

[16] T. Y. C. Woo and S. S. Lam, "Authentication for distributed systems," Computer, vol. 25, no. 1, pp. 39–52, 1992.

[17] T. Y. C. Woo and S. S. Lam, "Authentication for distributed systems," In Internet Besieged: Countering Cyberspace Scofflaws, pp. 319–355, ACM Press and Addison-Wesley, 1997.

[18] R. Anderson and R. Needham, "Programming Satan's computer," In Computer Science Today: Recent Trends and Developments, vol. 1000 of LNCS, pp. 426–440, Springer, 1995.

[19] M. Abadi and R. Needham, "Prudent engineering practice for cryptographic protocols," IEEE Transactions on Software Engineering, vol. 22, no. 1, pp. 6–15, 1996.

[20] A. Gordon and A. Jeffrey, "Authenticity by typing for security protocols," Journal of Computer Security, vol. 11, no. 4, pp. 451–521, 2003.

[21] D. E. Denning, and G. M. Sacco, "Timestamps in key distribution protocols," Commun. ACM, vol. 24, no. 8, pp. 533–536, 1981.

[22] D. Otway and O. Rees, "Efficient and timely mutual authentication," Operating Systems Review, vol. 21, no. 1, pp. 8–10, 1987.

[23] H. Krawczyk, "SKEME: A versatile secure key exchange mechanism for Internet," In Internet Society Symposium on Network and Distributed Systems Security, 1996.

مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"
ویژه‌نامه کنفرانس بین‌المللی ترکیبیات، رمزنگاری و محاسبات، ص ۱۵۶ -۱۵۱

بعضی از ماتریس‌های پارامتر ۲–رانگ‌آمیزی تام گراف J(10,4)

مهدی علائیان[1*]، عفت علائیان[2]

۱- استاد، دانشگاه علم و صنعت ایران، ۲- دانشجو دکتری، دانشگاه علم و صنعت ایران

(دریافت: ۹۵/۰۷/۰۵، پذیرش: ۹۶/۰۳/۰۷)

چکیده

مفهوم کدهای کاملا منتظم، توسط دلسارته ارائه شده است. رنگ آمیزی تام گراف G با m رنگ، یک افراز از مجموعه رئوس G به m بخش $A_1, \ldots, A_m$ است که برای همه $i; j \in \{1,\ldots,m\}$، هر راس از A_i دارای تعداد یکسانی مجاور از A_j است که آن را a_{ij} و ماتریس $A = (a_{ij})\ i;j\in\{1,2,\ldots,m\}$ را ماتریس پارامتر نامگذاری می‌کنیم. ما در این مقاله ۲-رنگ آمیزی تام (افراز منصفانه به ۲ بخش) گراف J(10,4) را بررسی می‌کنیم.

واژه‌های کلیدی: گراف جانسون، ماتریس پارامتر، ۲-رنگ آمیزی تام

۱- مقدمه

در سال ۱۹۷۳ دلسارته اقدام به معرفی خانواده ای از کدها کرد که از خواص ترکیبیاتی جالبی برخوردار بودند. او این کدها را کدهای کاملا منتظم نامید و در همان زمان حدسی را مطرح کرد که هنوز یکی از سوال های اساسی در زمینه کدگذاریی و نظریه گراف می باشد؛ هیچ کد تام غیر بدیهی در گراف جانسون وجود ندارد. برای دانستن ارتباط بین حدس یاد شده و کدهای کاملا منتظم، ذکر این نکته کافیست که هر کد تام یک کد کاملا منتظم است. در واقع دلسارته برای اثبات حدس خود ترجیح داد که کدهای کاملا منتظم در گرافهای جانسون یافته و سپس نشان دهد که هیچ کدام از این کدها، کد تام غیر بدیهی نیست. اصطلاح افراز منصفانه ابتدا توسط هایناس وورس در مطالعه ماتریسهای منصفانه مطرح شد . همچنین ساکس و دیگران از افرازهای منصفانه به عنوان ابزاری برای محاسبه چند جمله‌ای مشخصه یک گراف استفاده کردند. نویمار نشان داد که هر زیر مجموعه از رئوس گراف یک کد کاملا منتظم است اگر و تنها اگر افراز فاصله آن، منصفانه باشد. تا کنون نتایج بسیاری در زمینه رده بندی ماتریس های پارامتر برای گرافهای مختلف بدست آمده است در این مقاله به ۲- رنگ آمیزی تام گراف J(10,4) می‌پردازیم.

۲- مفاهیم مقدماتی

در این بخش تعاریف، قضایا و مفاهیم اولیه را بیان می‌کنیم. E^n مجموعه تمام n تایی های ۰ و ۱ تعریف می‌شود:

$$E^{\mathrm{n}} = \{x = (x_1, x_2, \ldots, x_n)\ |x_i \in \{0,1\}\}$$

وزن n تایی x در E^{n}، تعداد مولفه های غیر صفر x است.

تعریف ۲-۱: گراف جانسون J(n,w) گرافی است که رئوس آن همه n تایی‌های با وزن w در E^{n} است و رئوسی مجاورند که دقیقا در دو مولفه با هم اختلاف داشته باشند که گرافی منتظم با درجه w(n-w) است که تعداد رئوس آن برابر است با $\binom{\mathrm{n}}{w}$.

تعریف ۲-۲: فرض کنیم $x\in E^{\mathrm{n}}$. در این صورت مجموعه اندیس مولفه‌های غیر صفر x را ساپورت x گوییم و آن را با supp(x) نشان می‌دهیم.

$$\mathrm{Supp(x)} = \{\mathrm{i} \in \{1,2,\ldots,\mathrm{n}\}|x_i \neq 0\}$$

تعریف ۲-۳: (n,k,λ)-t- طرح، فرض کنیم که v یک مجموعه n عضوی باشد. یک t-طرح روی v شامل گردایه‌ای از زیر مجموعه‌های مجزای k تایی v به نام بلوک است، با این ویژگی که هر زیر مجموعه t عضوی v دقیقا در λ بلوک قرار داشته باشند و آن را (n,k,λ)-t-طرح می‌نامیم.

تعریف ۲-۴: یک t طرح با λ = ۱ را یک دستگاه اشنایدر می‌نامیم و آن را با S(n,k,t) نشان می‌دهیم.

تعریف ۲-۵: گراف همبندG، فاصله منتظم نامیده می‌شود هرگاه منتظم از درجه k باشد و برای هر دو راس $x,y\in V(G)$ که در فاصله d(x,y)=i هستند، x دقیقا G_i همسایه در فاصله i+1 از y داشته باشند.

* رایانامه نویسنده مسئول: alaeiyan@iust.ac.ir

دنباله $E^n = \{b_1, b_2, \dots, b_{d-1}, c_1, c_2, \dots, c_d\}$ به‌طوری‌که d قطر G است را آرایه اشتراک G می‌نامیم. اگر $a_i = k - b_i - c_i$.

تعداد همسایه‌های x که در فاصله i از y هستند، باشد، آنگاه اعداد a_i, b_i, c_i اعداد اشتراک نامیده می‌شوند.

تعریف ۲-۶: هر رنگ آمیزی گراف G با m رنگ را یک m–رنگ آمیزی تام با ماتریس $A = [a_{ij}]_{m\times m}$ گوییم هرگاه هر راس به رنگ i، تعداد a_{ij} راس مجاور به رنگ j داشته باشد. به ماتریس A ماتریس پارامتر گوییم. در حالت m=2 رنگ اول را سفید و رنگ دوم را سیاه در نظر می‌گیریم.

نتیجه: هر m–رنگ‌آمیزی تام در گراف G را می‌توان به صورت یک نگاشت $T: V(G) \to \{1,2,\dots,m\}$ در نظر گرفت که خاصیت ذکر شده در تعریف را داشته باشد.

قضیه ۲-۷: [۲] اگر T یک رنگ‌آمیزی تام گراف G با m رنگ باشد، آنگاه هر مقدار ویژه T، یک مقدار ویژه ماتریس مجاورت G است.

قضیه ۲-۸: **[۴]** فرض کنیم G یک گراف k-منتظم و T یک m–رنگ‌آمیزی تام با ماتریس $A = [a_{ij}]_{m\times m}$ در گراف G باشد. در این صورت مجموع مقادیر هر سطر در ماتریس A برابر k است.

برهان. فرض کنیم v یک راس دلخواه به رنگ i باشد. تعداد رئوس مجاور v به رنگ j برابر a_{ij} است. از طرفی تعداد رئوس مجاور v برابر k می‌باشد. بنابراین $\sum_{j=1}^{m} a_{ij} = k$. در نهایت از آنجا که راس v دلخواه انتخاب شده بود، قضیه به اثبات می‌رسد.

قضیه ۲-۹: [۴] فرض کنیم T یک ۲-رنگ‌آمیزی تام با ماتریس $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ در گراف همبند G باشد. در این صورت b,c≠0.

برهان. فرض کنیم b=0 باشد. در این صورت هر راس به رنگ سیاه هیچ راس مجاوری به رنگ سفید ندارد. درنتیجه هر راس به رنگ سفید نیز هیچ راس مجاوری به رنگ سیاه ندارد. بنابراین رئوس به رنگ سیاه و سفید تشکیل دو مولفه همبندی می‌دهند که با همبندی گراف در تناقض است.

قضیه ۲-۱۰: چنانچه گراف G دارای یک ۲-رنگ‌آمیزی تام با ماتریس $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ باشد، آنگاه دارای ۲-رنگ‌آمیزی تام با ماتریس $\begin{bmatrix} d & c \\ b & a \end{bmatrix}$ نیز می‌باشد.

برهان. با تعویض رنگ‌های سفید و سیاه، حکم برقرار است.

قضیه ۲-۱۱: [۴] فرض کنیم R نشان‌دهنده مجموعه تمام رئوس سفید در یک ۲-رنگ‌آمیزی تام با ماتریس $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ در گراف همبند G باشد. در این صورت:

$$|W| = |V(G)|\frac{c}{b+c}.$$

برهان. با حذف یال‌های بین رئوس سفید و نیز حذف یال‌های بین رئوس سیاه، گراف دو بخشی به‌دست آمده با بخش‌های مجموعه رئوس سفید و مجموعه رئوس سیاه را در نظر بگیرید. در این گراف هر راس به رنگ سفید تعداد b راس مجاور به رنگ سیاه دارد. بنابراین تعداد یال‌ها در این گراف برابر |R|b است. از طرف دیگر هر راس به رنگ سیاه، تعداد c راس مجاور به رنگ سفید دارد. درنتیجه تعداد یال‌ها در این گراف برابر |B|c می‌باشد. از آنجا که |W|+|B|=|V(G)|، لذا

$$|V(G)| = |W| + |B|$$
$$= |W| + \frac{b}{c}|W|$$
$$= \left(\frac{b+c}{c}\right)|W|$$

درنتیجه حکم خواسته‌شده به سادگی به‌دست می‌آید.

نتیجه ۲-۱۲: فرض کنیم |B| نشان‌دهنده مجموعه تمام رئوس سیاه در یک ۲-رنگ‌آمیزی تام با ماتریس $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ در گراف همبند G باشد. در این صورت

$$|B| = |V(G)|\frac{b}{b+c}$$

قضیه ۲-۱۳: [۴] فرض کنیم T یک ۲- رنگ‌آمیزی تام با ماتریس پارامتر $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ در گراف k- منتظم G باشد. در این صورت مقادیر ویژه ماتریس پارامتر برابر k و a-c هستند.

برهان. از آنجا که می‌دانیم مجموع تمامی سطرها برابر k است به سادگی می‌توان دید که $\lambda_1 = 1$ یک مقدار ویژه با بردار متناظر $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ است. برای بدست آوردن مقدار ویژه دیگر λ_2 ابتدا توجه کنیم که $\lambda_1 + \lambda_2 = \text{tr } A = a + d$ لذا $\lambda_1 = a + d - k$ اما c+ d=k. در نتیجه

$$\lambda_2 = a + d - k = a + d - c = a - c.$$

قضیه ۲-۱۴: [۴] مقادیر ویژه J(n,w) دقیقا عبارتند از:

$$\theta_i = (n-w-i)(w-i)-I \qquad 0 \le i \le w.$$

نکته۲-۱۵: [۴]چند جمله‌ای زیر را در نظر بگیرید:

$$f(l,n,w,a_{11},a_{21}) = w(n-w-l)+a_{21}-a_{11}-l(n-w-l+1)$$

اگر k_1کوچکترین ریشه $f(l,n,w,a_{11},a_{21})$ به عنوان تابعی از l باشد آنگاه:

$$k_1 = \frac{n+1-\sqrt{(n-2w+1)^2+4(w+a11-a21)}}{2}.$$

گزاره۲-۱۶: [۴] فرض کنیم T یک ۲-رنگ آمیزی تام برای J(n,w) با ماتریس $A=[a_{ij}]_{i,j=1,2}$ باشد. در این صورت عدد

$\frac{a_{21}}{a_{12}+a_{21}}\binom{n-i}{n-i+j}$ برای هر i,j که $0\le i\le j\le k_1\text{-}1$ عددی صحیح است که در آن k_1 اندیس θ_{k1} مقدار ویژه J(n,w) و همچنین کوچکترین ریشه چندجمله‌ای $f(l,n,w,a_{11},a_{21})$ است.

تعریف۲-۱۷: گراف G فاصله انتقالی است هرگاه برای هر دو زوج x,y و همچنین u,v که d(x,y)=d(u,v) یک اتومورفیسم روی G باشید که یک زوج را به یک زوج دیگر می‌برد.

گزاره۲-۱۸: [۵] یک گراف فاصله انتقالی، فاصله منتظم است.

قضیه۲-۱۹: [۴] گراف جانسون J(n,w) با قطرd، فاصله انتقالی با آرایه اشتراک

$b_j=(w-j)(n-w-j)$

$c_j=j^2$

$a_j=k-b_j-c_j$

می‌باشد که در آن k درجه رئوس و $0\le j\le d$ است.

ساختار ۱۰: [۴] مؤلفه $i\in\{1,\dots,n\}$ را ثابت می‌گیریم. همه رئوس در J(n,w) که مؤلفه i ام آن صفر است را در w و بقیه را درB قرار می‌دهیم. در این صورت یک ۲-رنگ تام با ماتریس $\begin{bmatrix} w(n-w-1) & w \\ n-w & (w-1)(n-w)\end{bmatrix}$ برای J(n,w) به‌دست می‌آید.

قضیه۲-۲۰: [۴] دستگاه S(n,4,3) وجود دارد اگر و تنها اگر $n\equiv 1 \text{ or } 4 \bmod 6$.

ساختار ۱۲: [۴] دستگاه S(n,w,w-1) در گراف J(n,w) را در نظر بگیرید. رأس‌های دستگاه را در w و بقیه رئوس را در B قرار دهید. در این صورت یک ۲-رنگ آمیزی تام با ماتریس پارامتر $\begin{bmatrix} 0 & w(n-w) \\ w & w(n-w-1)\end{bmatrix}$ به‌دست می‌آید.

نکته۲-۲۱: [۴] هرگاه $q\ge 5$ عددی فرد باشد، آنگاه یک (q+1,4,3)-۳ طرح وجود دارد.

ساختار ۱۴: [۴] اگر یک (n,w,λ)-۱ طرح در J(n,w) وجود داشته باشد. آنگاه رأس‌های موجود در طرح را در w و دیگر راس‌ها را در B قرار می‌دهیم. ۲-رنگ‌آمیزی تام برای گراف با ماتریس پارامتر $\begin{bmatrix} w(\lambda-1) & w(n-w)-w(\lambda-1) \\ \lambda w & w(n-w)-\lambda w\end{bmatrix}$ به‌دست می‌آید.

۳- بعضی از ماتریس پارامترهای ممکن برای ۲-رنگ آمیزی تام گراف J(10,4)

در این بخش ماتریس‌های پارامتر و ساختارهای مرتبط به آن را برای گراف J(10,4) به‌دست می‌آوریم. گراف J(10,4)، ۲۴- منتظم و با قطر ۴ می‌باشد و تعداد رئوس آن ۲۱۰ رأس است که مقادیر ویژه آن عبارتند از:

$\theta_0=24,\ \theta_1=14,\ \theta_2=6,\ \theta_3=0,\ \theta_4=-4.$

برای پیدا کردن ۲-رنگ آمیزی‌های تام در J(10,4) ابتدا ماتریس‌هایی را پیدا می‌کنیم که شرط لازم قضیه ۲-۷ را داشته باشند. از آنجایی‌که J(10,4)، ۲۴منتظم است، لذا اگر $A=[a_{ij}]_{i,j=2}$ ماتریس پارامتریک ۲-رنگ‌آمیزی تام برای J(10,4) باشد آنگاه $a_{11}+a_{12}=a_{21}+a_{22}=24$ و ازآنجایی که درایه‌های اعداد صحیح نامنفی هستند، بنابراین $0\le a_{11}\le 24$. اکنون کار محاسبات را انجام می‌دهیم.

۱.حالت $a_{11}=24$. پس $A=\begin{bmatrix}24 & 0\\ a_{21} & a_{22}\end{bmatrix}$. لذا داریم:

$\theta_0=24-a_{21}=24\Rightarrow a_{21}=0$

$\theta_1=24-a_{21}=14\Rightarrow a_{21}=10$

$\theta_2=24-a_{21}=6\Rightarrow a_{21}=18$

$\theta_3=24-a_{21}=0\Rightarrow a_{21}=24$

$\theta_4=24-a_{21}=-4\Rightarrow a_{21}=28$

چون J(10,4)، ۲۴- منتظم است، درایه‌های A بیش از ۲۴ نمی‌توانند باشند. پس $a_{21}=28$ قابل قبول نیست. برای حالت‌های $a_{21}=10,18,24$ چون داریم $a_{21}\neq 0$ و $a_{12}=0$ پس این حالت‌ها امکان‌پذیر نیست و فقط حالت $a_{21}=0$ باقی می‌ماند که $A_{1-1}=\begin{bmatrix}24 & 0\\ 0 & 24\end{bmatrix}$.

۲.حالت $a_{11}=23$. پس $A=\begin{bmatrix}23 & 1\\ a_{21} & a_{22}\end{bmatrix}$. لذا داریم:

$\theta_0=23-a_{21}=24\Rightarrow a_{21}=-1$

$\theta_1=23-a_{21}=14\Rightarrow a_{21}=9$

$\theta_2=23-a_{21}=6\Rightarrow a_{21}=17$

$\theta_3=23-a_{21}=0\Rightarrow a_{21}=23$

$\theta_4=23-a_{21}=-4\Rightarrow a_{21}=27$

درایه‌های A باید نامنفی و همچنین بیشتر از ۲۴ نباشند پس مقادیری از A که باقی می‌مانند عبارتند از:

۳.حالت $a_{11}=22$. پس $A=\begin{bmatrix}22 & 2\\ a_{21} & a_{22}\end{bmatrix}$. لذا داریم:

$\theta_0=22-a_{21}=24\Rightarrow a_{21}=-2$

$\theta_1=22-a_{21}=14\Rightarrow a_{21}=8$

$\theta_2=22-a_{21}=6\Rightarrow a_{21}=16$

$\theta_3=22-a_{21}=0\Rightarrow a_{21}=22$

θ_4=22-a_{21} $= -4 \Rightarrow a_{21} = 26$

درایه‌های A باید نامنفی و همچنین بیشتر از ۲۴ نباشند پس مقادیری از A که باقی می‌مانند عبارتند از:

$A_{3-1}=\begin{bmatrix}22 & 2\\ 8 & 16\end{bmatrix}, A_{3-2}=\begin{bmatrix}22 & 2\\ 16 & 8\end{bmatrix},$

$A_{3-3}=\begin{bmatrix}22 & 2\\ 22 & 2\end{bmatrix}.$

۴.حالت a_{11}=21. پس $A=\begin{bmatrix}21 & 3\\ a_{21} & a_{22}\end{bmatrix}$ و در نتیجه داریم:

θ_0=21-a_{21} $= 24 \Rightarrow a_{21} = -3$

θ_1=21-a_{21} $= 14 \Rightarrow a_{21} = 7$

θ_2=21-a_{21} $= 6 \Rightarrow a_{21} = 15$

θ_3=21-a_{21} $= 0 \Rightarrow a_{21} = 21$

θ_4=21-a_{21} $= -4 \Rightarrow a_{21} = 25$

درایه های A باید نـامنفی و همچنـین بیشـتر از ۲۴ نباشـند پس مقادیری از A که باقی می‌مانند عبارتند از:

$A_{4-1}=\begin{bmatrix}21 & 3\\ 7 & 17\end{bmatrix}, A_{4-2}=\begin{bmatrix}21 & 3\\ 15 & 9\end{bmatrix},$

$A_{4-3}=\begin{bmatrix}21 & 3\\ 21 & 3\end{bmatrix}.$

تـا شـماره ۲۵ رونـد بـه صـورت فـوق مـی‌باشـد. لـذا فقـط ماتریس‌های بدست آمده را می‌نویسیم.

$A_{5-1}=\begin{bmatrix}20 & 4\\ 16 & 8\end{bmatrix}, \quad A_{5-2}=\begin{bmatrix}20 & 4\\ 14 & 10\end{bmatrix},$
$A_{5-3}=\begin{bmatrix}20 & 4\\ 20 & 4\end{bmatrix}, \quad A_{5-4}=\begin{bmatrix}20 & 4\\ 24 & 0\end{bmatrix},$

$A_{6-1}=\begin{bmatrix}19 & 5\\ 5 & 19\end{bmatrix}, A_{6-2}=\begin{bmatrix}19 & 5\\ 13 & 11\end{bmatrix},$

$A_{6-3}=\begin{bmatrix}19 & 5\\ 19 & 5\end{bmatrix}, \quad A_{6-4}=\begin{bmatrix}19 & 5\\ 23 & 1\end{bmatrix}.$

$A_{7-1}=\begin{bmatrix}18 & 6\\ 4 & 20\end{bmatrix}, \quad A_{7-2}=\begin{bmatrix}18 & 6\\ 12 & 12\end{bmatrix}$

$A_{7-3}=\begin{bmatrix}18 & 6\\ 18 & 6\end{bmatrix}, \quad A_{7-4}=\begin{bmatrix}18 & 6\\ 22 & 2\end{bmatrix}$

$A_{8-1}=\begin{bmatrix}17 & 7\\ 3 & 21\end{bmatrix}, \quad A_{8-2}=\begin{bmatrix}17 & 7\\ 11 & 13\end{bmatrix}$

$A_{8-3}=\begin{bmatrix}17 & 7\\ 17 & 7\end{bmatrix}, \quad A_{8-4}=\begin{bmatrix}17 & 7\\ 21 & 3\end{bmatrix}$

$A_{9-1}=\begin{bmatrix}16 & 8\\ 2 & 22\end{bmatrix}, \quad A_{9-2}=\begin{bmatrix}16 & 8\\ 10 & 14\end{bmatrix}$

$A_{9-3}=\begin{bmatrix}16 & 8\\ 16 & 8\end{bmatrix}, \quad A_{9-4}=\begin{bmatrix}16 & 8\\ 20 & 4\end{bmatrix}$

$A_{10-1}=\begin{bmatrix}15 & 9\\ 1 & 23\end{bmatrix}, \quad A_{10-2}=\begin{bmatrix}15 & 9\\ 9 & 15\end{bmatrix}$

$A_{10-3}=\begin{bmatrix}15 & 9\\ 15 & 9\end{bmatrix}, \quad A_{10-4}=\begin{bmatrix}15 & 9\\ 19 & 5\end{bmatrix}$

$A_{11-1}=\begin{bmatrix}14 & 10\\ 8 & 16\end{bmatrix}, \quad A_{11-2}=\begin{bmatrix}14 & 10\\ 14 & 10\end{bmatrix}$

$A_{11-3}=\begin{bmatrix}14 & 10\\ 18 & 6\end{bmatrix},$

$A_{12-1}=\begin{bmatrix}13 & 11\\ 7 & 17\end{bmatrix}, \quad A_{12-2}=\begin{bmatrix}13 & 11\\ 13 & 11\end{bmatrix}$

$A_{12-3}=\begin{bmatrix}13 & 11\\ 17 & 7\end{bmatrix}$

$A_{13-1}=\begin{bmatrix}12 & 12\\ 6 & 18\end{bmatrix} \quad A_{13-2}=\begin{bmatrix}12 & 12\\ 12 & 12\end{bmatrix}$

$A_{13-3}=\begin{bmatrix}12 & 12\\ 16 & 8\end{bmatrix}$

$A_{14-1}=\begin{bmatrix}11 & 13\\ 5 & 19\end{bmatrix} \quad A_{14-2}=\begin{bmatrix}11 & 13\\ 11 & 13\end{bmatrix}$

$A_{14-3}=\begin{bmatrix}11 & 13\\ 15 & 9\end{bmatrix}$

$A_{15-1}=\begin{bmatrix}10 & 14\\ 4 & 20\end{bmatrix} \quad A_{15-2}=\begin{bmatrix}10 & 14\\ 10 & 14\end{bmatrix}$

$A_{15-3}=\begin{bmatrix}10 & 14\\ 14 & 10\end{bmatrix}$

$A_{16-1}=\begin{bmatrix}9 & 15\\ 3 & 21\end{bmatrix} \quad A_{16-2}=\begin{bmatrix}9 & 15\\ 9 & 15\end{bmatrix}$

$A_{16-3}=\begin{bmatrix}9 & 15\\ 13 & 11\end{bmatrix}$

$A_{17-1}=\begin{bmatrix}8 & 16\\ 2 & 22\end{bmatrix} \quad A_{17-2}=\begin{bmatrix}8 & 16\\ 8 & 16\end{bmatrix}$

$A_{17-3}=\begin{bmatrix}8 & 16\\ 12 & 12\end{bmatrix}$

$A_{18-1}=\begin{bmatrix}7 & 17\\ 1 & 23\end{bmatrix}, A_{18-2}=\begin{bmatrix}7 & 17\\ 7 & 17\end{bmatrix},$

$A_{18-3}=\begin{bmatrix}7 & 1\\ 11 & 13\end{bmatrix}.$

$A_{19-1}=\begin{bmatrix}6 & 18\\ 6 & 18\end{bmatrix}, \quad A_{19-2}=\begin{bmatrix}6 & 18\\ 6 & 18\end{bmatrix}$

$A_{20-1}=\begin{bmatrix}5 & 19\\ 5 & 19\end{bmatrix}, \quad A_{20-2}=\begin{bmatrix}5 & 19\\ 9 & 15\end{bmatrix}$

$A_{21-1}=\begin{bmatrix}4 & 20\\ 4 & 20\end{bmatrix}, \quad A_{21-2}=\begin{bmatrix}4 & 20\\ 8 & 16\end{bmatrix}$

$A_{22-1}=\begin{bmatrix}3 & 21\\ 3 & 21\end{bmatrix}, \quad A_{22-2}=\begin{bmatrix}3 & 21\\ 7 & 17\end{bmatrix}$

$A_{23-1}=\begin{bmatrix}2 & 22\\ 2 & 22\end{bmatrix}, \quad A_{23-2}=\begin{bmatrix}2 & 22\\ 6 & 18\end{bmatrix}$

$A_{24-1}=\begin{bmatrix}1 & 23\\ 1 & 23\end{bmatrix}, \quad A_{24-2}=\begin{bmatrix}1 & 23\\ 5 & 19\end{bmatrix}$

$A_{25-1}=\begin{bmatrix}0 & 24\\ 4 & 20\end{bmatrix}.$

حال با استفاده از قضیه ۲-۱۰، نکتـه ۲-۱۵ و گـزاره ۲-۱۶ ماتریس هایی که شرط لازم را ندارنـد حـذف مـی‌کنـیم. پـس از انجام محاسبات ۲۰ ماتریس زیر باقی می‌مانند.

$A_{1-1}=\begin{bmatrix}24 & 0\\ 0 & 24\end{bmatrix}, \quad A_{2-1}=\begin{bmatrix}23 & 1\\ 9 & 15\end{bmatrix}$

$A_{3-1}=\begin{bmatrix}22 & 2\\ 8 & 16\end{bmatrix}$, $A_{4-1}=\begin{bmatrix}21 & 3\\ 7 & 17\end{bmatrix}$

$A_{5-1}=\begin{bmatrix}20 & 4\\ 16 & 8\end{bmatrix}$, $A_{5-4}=\begin{bmatrix}20 & 4\\ 24 & 0\end{bmatrix}$

$A_{6-1}=\begin{bmatrix}19 & 5\\ 5 & 19\end{bmatrix}$, $A_{7-1}=\begin{bmatrix}18 & 6\\ 4 & 20\end{bmatrix}$

$A_{7-2}=\begin{bmatrix}18 & 6\\ 12 & 12\end{bmatrix}$, $A_{8-1}=\begin{bmatrix}17 & 7\\ 3 & 21\end{bmatrix}$

$A_{9-1}=\begin{bmatrix}16 & 8\\ 2 & 22\end{bmatrix}$, $A_{9-4}=\begin{bmatrix}16 & 8\\ 20 & 4\end{bmatrix}$

$A_{10-1}=\begin{bmatrix}15 & 9\\ 1 & 23\end{bmatrix}$, $A_{10-2}=\begin{bmatrix}15 & 9\\ 9 & 15\end{bmatrix}$

$A_{13-1}=\begin{bmatrix}12 & 12\\ 6 & 18\end{bmatrix}$, $A_{13-2}=\begin{bmatrix}12 & 12\\ 12 & 12\end{bmatrix}$

$A_{13-3}=\begin{bmatrix}12 & 12\\ 16 & 8\end{bmatrix}$, $A_{17-3}=\begin{bmatrix}8 & 16\\ 12 & 12\end{bmatrix}$

$A_{21-2}=\begin{bmatrix}4 & 20\\ 8 & 16\end{bmatrix}$, $A_{25-1}=\begin{bmatrix}0 & 24\\ 4 & 20\end{bmatrix}$.

در ادامه ماتریس‌های فوق را بررسی می‌کنیم. از ساختار ۱۰ نتیجه می‌شود که ماتریس A_{5-1} یک ۲-رنگ‌آمیزی تام برای J(10,4) است. با جابجایی رنگ‌های سیاه و سفید که ماتریس A_{7-1} نیز یک ۲-رنگ‌آمیزی تام برای گراف J(10,4) است.

A_{25-1} نیز ماتریس پارامتر ۲-رنگ‌آمیزی تام برای J(10,4) است. زیرا $10 \equiv 4 \bmod 6$ و بنا به قضیه ۲-۲۰ داریم: S(10,4,3) وجود دارد و حال از ساختار ۱۲ حکم نتیجه می‌شود. با جابجایی رنگ‌های سفید و سیاه گره‌ها نتیجه می‌شود A_{5-4} نیز ماتریس پارامتر ۲- رنگ‌آمیزی تام برای گراف J(10,4) است.

A_{17-3} ماتریس پارامتر ۲- رنگ آمیزی تام برای گراف J(10,4) است. زیرا طبق نکته ۲-۲۱ یک (10,4,3)-3 طرح وجود دارد و از ساختار ۱۴ رنگ‌آمیزی تام به‌دست می‌آید. با جابجایی رنگ‌های سیاه و سفید که ماتریس A_{13-3} نیز یک ۲-رنگ‌آمیزی تام برای گراف J(10,4) است.

تا اینجا ۶ ماتریس از ۲۰ ماتریس فوق دارای ساختار هستند حال از ماتریس‌های باقی‌مانده آنهایی که ساختار ندارند را حذف می‌کنیم.

ماتریس A_{1-1} نمیتواند ماتریس پارامتر یک ۲- رنگ‌آمیزی تام برای گراف J(10,4) باشد زیرا بنا به قضیه ۲-۱۱، $|w|=0$ در حالی که $a_{11} \neq 0$.

با برهان خلف نشان می‌دهیم که ماتریس A_{2-1} نمی‌تواند ماتریس پارامتر یک ۲- رنگ‌آمیزی تام بترای گراف J(10,4) باشد. فرض کنیم که A_{2-1} ماتریس پارامتر یک ۲- رنگ‌آمیزی تام$T=\{W,B\}$ برای گراف J(10,4) باشد. با توجه به قضیه ۲-۱۱داریم که $|W|=189,|B|=21$. اگر x و y دو راس مجاور در B باشند، آنگاه با توجه به ماتریس مفروض، هرکدام دقیقا ۱۵ رأس همسایه در B دارند. حال از قضیه ۲-۱۹ داریم:

$$b_1 = 15, c_1 = 1, a_1 = 24 - 15 - 1 = 8.$$

بنابراین x و y، ۸ همسایه مشترک دارند. در بدترین حالت فرض کنیم این ۸ همسایه همگی در B قرار داشته باشند. در این صورت بنا بر این داریم: $|B| \geq 15+15-8=22$ که یک تناقض است. بنا براین ماتریس A_{2-1} و با توجه به جابجایی رنگ‌های سفید و سیاه ماتریس A_{10-1} نمی‌توانند ماتریس پارامتر یک ۲- رنگ آمیزی تام بترای گراف J(10,4) باشند.

حال با استدلال مشابه ماتریس‌های A_{4-1}، A_{8-1}، A_{3-1} و A_{9-1} نمی‌توانند ماتریس پارامتر یک ۲- رنگ‌آمیزی تام بترای گراف J(10,4) باشند. و تکلیف ۷ ماتریس A_{6-1}، A_{7-2}، A_{21-2}، A_{9-4}، A_{10-2}، A_{13-1} و A_{13-2} بعنوان مسئله باز هنوز تعیین تکلیف نشده است.

۴- مراجع

[1] Alaeiyan M, and Abedi AA, "Perfect 2-colorings of Johnson graphs J(4, 3), J(4, 3), J(6,3) and Petersen graph," Ars Combinatorial, (to apear).

[2] Alaeiyan M, Karami H, "Perfect 2-colorings of the generalized Petersen graph, " Proceedings Mathematical Sciences. vol 126. pp. 1-6, 2016.

[3] Alaeiyan M and Mehrabani A. "Perfect 3-colorings of cubic graphs of order 10, " Electronic Journal of Graph Theory and Applications (EJGTA), vol.5, no.2, pp. 194-206, 2017.

[4] Avgustinovich S. V., Mogilnykh I. Yu. "Perfect 2-colorings of Johnson graphs J(6, 3) and J(7, 3)," Lecture Notes in Computer Science. vol. 5228, pp.11-19, 2008.

[5] Avgustinovich S. V., Mogilnykh I. Yu. " Perfect colorings of the Johnson graphs J(8, 3) and J(8, 4) with two colors. Journal of Applied and Industrial Mathematics, vol. 5, pp.19-30, 2011.

[6] Fon-Der-Flaass D. G. "A bound on correlation immunity," Siberian Electronic Mathematical Reports Journal, vol. 4, pp. 133-135, 2007.

[7] Fon-Der-Flaass D. G. "Perfect 2-colorings of a hypercube, " Siberian Mathematical Journal, vol. 4, pp.923-930, 2007.

[8] Fon-Der-Flaass D. G, "Perfect 2-colorings of a 12-dimensional Cube that achieve a bound of correlation immunity". Siberian Mathematical Journal, vol. 4, pp. 292-295, 2007.

[9] Gavrilyuk A. L. and Goryainov S.V. On perfect 2-colorings of Johnson graphs J(v,3). Journal of Combinatorial Designs, vol. 21, pp. 232-252, 2013.

[10] Godsil C and Gordon R. Algebraic graph theory. Springer Science+Business Media, LLC, 2004.

[11] Godsil C., "Compact graphs and equitable partitions," Linear Algebra and Its Application, 1997.

The Prefect Coloring of J(10,2)

M. Alaeiyan*, E. Alaeiyan

*Iran University of science and technology

ABSTRACT

Delsarte presented the perfect coloring which is a generalization of the notion of completely regular codes. A perfect m-coloring of a graph G with m colors is a partition of the vertex set of G into m parts $A_1, A_2, A_3, \ldots, A_m$ such that, for all $i, j \in \{1, \ldots, m\}$ every vertex of A_i is adjacent to the same number of vertices, namely, a_{ij} vertices, of A_j. The matrix $A = (a_{ij})_{i,j \in \{1,\ldots,m\}}$ is called the parameter matrix. We study the perfect 2-colorings of the Johansson graphs J(10,2).

Keywords: prefect coloring, completely regular codes, Johansson graphs.

* Corresponding Author Email: alaeiyan@ iust.ac.ir

A logic programming approach to verifying cryptographic protocols

Mostafa Zaare*

*Damghan University

ABSTRACT

In [1], Bruno Blanchet has been introduced a method for verifying cryptographic protocols based on an abstract representation of protocols by Horn clauses. This method is fully automatic, efficient, and can handle an unbounded number of sessions and an unbounded message space. It supports various cryptographic primitives defined by rewrite rules or equations. In this paper, we have implemented it. Even if we focus on secrecy in this paper, this method can also prove other security properties, including authentication and process equivalences. The experimental results show that many examples of protocols of the literature can be verified by this tool with less than one second of time and 2 Mb of memory.

Keywords: Automatic verification, cryptographic protocols, Horn clauses, secrecy.

* Corresponding Author Email: mostafazaare@du.ac.ir

A meta-architecture of multi-resolution bilateral filter denoising based on meta-heuristic algorithms and fuzzy evaluation

Javad Vahidi*, Hadi Salehi

*Iran University of Science and Technology

ABSTRACT

Images received by considering environmental factors have unwanted interference. This interference is known noise. In this paper, in order to remove this unwanted interference, the two denoising systems combined. Different models by combining the bilateral filter and wavelet transformation are produced. Each model is evaluated. A fuzzy inference function is used to evaluate the different models.Different models are created by combining adaptive bilateral filters and wavelet transform. Finally, the results of this system at all levels will be analyzed to evaluate a model among the thousands of models with the lowest cost for all the pictures and all levels. Next, for more appropriate evaluation of the proposed model, the model is compared with similar models. The results show the effectiveness of the proposed model .

Keywords: Genetic algorithm, denoising, Fuzzy deduction system, image processing, wavelet transformation, adaptive bilateral filters.

* Corresponding Author Email: jvahidi@iust.ac.ir

A meta-architecture system based on fuzzy the evaluation

Hadi Salehi, Mohammadhadi Alaeiyan*

*Iran University of science and technology

ABSTRACT

This paper presents an optimal model system architecture of the system (SOS) for a marine rescue. Each function and restrictions of a system are independent. However, these systems work together. The concept of meta-architecture means that any potential architectures are suitable for SOS. Meta architecture defines how all possible system subsets can be combined to create an SOS system work together. The nature of system cooperation is so that the performance of SOS is better than individual systems. Since the system components, for example, the budget varies according to circumstances, cannot be considered a definitive number as the desired budget. Therefore, the evaluation of SOS architecture is in the form of fuzzy. Each of the architectures is evaluated by fuzzy inference system and weaker architecture is removed. Finally, an architecture as the most appropriate architecture for the SOS system is selected.

Keywords: System of systems, rescue, GA.

* Corresponding Author Email: hadi_alaeiyan@comp.iust.ac.ir

Optimal Network Protection against Interdiction Strategies via Evolutionary Algorithms

Vahid Kharazi*

*Iran University of Science and Technology

ABSTRACT

In this paper, we present an optimization technique for a network which maximizes the survivability of the network through the supply and demand. In the presented method, the links are in the random mode and the success ratio of attacker-defender is determined by a function considering the link vulnerability. Under this new setting, the target of interdictor is the reduction of maximal expected rate by demolition of the links. Moreover, we suppose that the interdictor has limited resources to prevent network components. In our investigation, we want to find the probability of demolition of a component and then distribute the defense resources ideally among the defensive measures such as separation, protection and redundancy so that the system survivability being maximized. We remark that many approaches have been introduced for solving this model of interdiction but more often are applied for the limited networks. We present an evolutionary algorithm for solving such problems. The obtained numerical results show that this algorithm considerably confines the solution space and therefore it can be used in high-dimensional networks.

Keywords: Network Interdiction, System Protection, Network Survivability, Graph Theory, Evolutionary Optimaztion.

* Corresponding Author Email: kharazi@comp.iust.ac.ir

Image watermarking algorithm using particle swarm optimization

Reza Saadati*

*Iran University of Science and Technology

ABSTRACT

With the rapid growth of the Internet and digital multimedia technology in the last decade, copy and manipulate data without any loss of quality and without respect for copyright and low cost is possible. In this regard, every day there is a variety of security needs. . Today watermarking in digital products, as a solution to implement and proof of ownership, and control the number of copies printed of a researcher's work. Watermarking is a subtle signal in the digital media data, so there is no change in the original data, but if necessary it can be extracted and used as a claim to ownership of digital effects. Digital watermarking consists of two parts. The first part of the image watermarking or logo within the host image and the second part involves the extraction of watermarking image or logo from the host image. In this paper, the role of the PSO algorithm to extract the watermark image to find the optimal value Scaling factor is discussed.

Keywords: particle swarm optimization, watermarking digital images, transforming fields, singular value decomposition.

* Corresponding Author Email: rsaadati@iust.ac.ir

The application of Bernoulli polynomials to solve fractional integro-differential equations

Kobra Rabiei, Yadollah Ordokhani*

*Alzahra University

ABSTRACT

In this paper, we introduce the Bernoulli operational matrix of Reimann-Liouville fractional integration. This matrix, the properties of Bernoulli polynomials and the least square method are used to reduce the fractional-order Fredholem-Volterra integro-differential equations to a systems of nonlinear algebraic equations which are solved through the Newton's iterative method. The convergence of the method is discussed and finally, some numerical examples are presented to show the efficiency and accuracy of our method.

Keywords: Bernoulli polynomials -Operational matrix-Convergence analysis-Fractional integro-differential equations-Least square method.

* Corresponding Author Email: ordokhani@alzahra..ac.ir

Improving Matching Section Method by Chain Code in Airplane Pattern

Mohammad Saeid Alamdari*, Mohsen Shahrezaee

*Imam Hossein University

ABSTRACT

In this paper, the identification method has been used based on Fourier method and matching Section method which the first airplane border area into several smaller parts and then identify the most optimal path possible. Results obtained based on comparison among Fourier method and matching section method.

Keywords: Chain Code, Distance Table, Contour, Fourier Interpreter, Distance Shortest Path, Discrete Fourier Transfor.

* Corresponding Author Email: m.s.alamdari69@gmail.com

Symbol and Symbolism in Soft War based on Persian Literature

Seyyed Khalil Bagheri*

*Mazandaran University of Science and Technology

ABSTRACT

Efforts for expressing an independent definition of a symbol along with its reasons and motivations behind it in the soft war require poets' symbolism. The symbolism approach in soft and cyber war on one hand is the consequence of the specific social and political situations in which we live and on the other hand is the outcome of poets and writers' perspectives. This paper aims at interpreting and specifying the enemy's symbols and their purposes in the soft war. In a nutshell, this study aims at investigating symbol and symbolism in soft war based on the poetry's of some poets along with some techniques. Therefore, the present study focuses on some symbols of the enemy in the soft war.

Keywords: symbol, soft war, literature, enemy.

* Corresponding Author Email: kh_bagheri46@mazut.ac.ir

The relation between the control of perturbation in a system and viscosity solution of a partial differential equation

Somayeh Saiedinezhad*

*Iran University of science and technology

ABSTRACT

In this article, firstly some concise comments about the real problems that follow a mathematical model for analysis the control of perturbation in theirs systems through differential game theory are presented. So we study the relation between the safe set of one dimensional sample with a viscosity solution of special type of partial differential equation which is called Hamilton- Jacobi equation.

Keywords: Differential game theory, partial differential equation, Hamilton- Jacobi equation, Viscosity solution.

* Corresponding Author Email: Ssaiedinezhad@iust.ac.ir

On the total domination polynomial of graphs

Saeid Alikhani*, Nasrin Jafari

*Yazd University

ABSTRACT

Domination theory is one of the most important subjects in graph theory which has applications in many areas such as communication networks, terrestrial mapping and routing. Let $G=(V,E)$ *be a simple graph of order n. The total dominating set of* G *is a subset* S *of* V *that every vertex of* V *is adjacent to some vertices of* D *. The total domination number of is equal to minimum cardinality of total dominating set in G and denoted by* $\gamma_t(G)$*. The number of dominating and total dominating sets of a graph with any cardinality has considered recently. The total domination polynomial of* G *is the polynomial ,* $D_t(G,x)=\sum_{i=\gamma_t(G)}^{n} d_t(G,i)x^i$ *where* $d_t(G,i)$ *is the number of total dominating sets of* G *of size i. In this paper, we study total domination polynomial of graph and also we investigate roots of this polynomial .*

Keywords: Domination number, Total domination number, Total domination polynomial.

* Corresponding Author Email: alikhani@yazd.ac.ir

Calculations based on quantum computers and their application for factoring

Ali Jabar Rashidi*, Rahim Asghari, Mostafa Eslami

*Malek-Ashtar University of Technology

ABSTRACT

This paper presents a quantum Fourier transform algorithm as a key component in the factoring by quantum method for use in Shor's algorithm is presented. Shor's algorithm implements an algorithm known only to parse numbers with polynomial time complexity is the main objective of this research is computationally efficient manner. The computational complexity of the factoring algorithm in the different stages is presented. The quantum Fourier transforms is extended and improved for computing. Shor's algorithm improved application using the library maple and quantum computing has been implemented. With these library concepts of entanglement and parallel computing in quantum is simulated on classic computers. Examples of simulation phase estimates with tables and graphs to display the program have offered. Finally, some examples with improved results are presented .

Keywords: Quantum computing, Quantum Fourier Transform, Shor's algorithm, Phase estimates, Simulation.

* Corresponding Author Email: Aiorashid@yahoo.com

New Principles for Cryptography Algorithm

Navid Oboudi, Naser Hashemi*

*Amir Kabir University of Technology

ABSTRACT

In this paper we present a number of new principles which are useful in cryptography, while the previous Kerckhoffs's principles are also maintained. Our proposed principles capture important characteristics by increasing the hardness of finding the keys and also make it more difficult to analyze the cryptographic algorithm.

Keywords: Symmetric Cryptography, Kerckhoffs's Principles, Information Secure Transportation

* Corresponding Author Email: nhashemi@aut.ac.ir

Classification of Sonar Targets using Multi-Layer Perceptron Trained by Biogeography Based Optimizer

Mohammadreza Mosavi*, Mohammad Khishe, Fallah Mohammadzadeh, Hooman Alaeiyan

*Iran University of Science and Technology

ABSTRACT

The aim of this paper is using the Biogeography Based Optimization (BBO) algorithm to train the MLP NNs for sonar dataset classification. To test the proposed method, this algorithm is compared to five well-known benchmark meta-heuristic algorithms using the sonar data set. Measured metrics are convergence speed, the possibility of trapping in local minimum and classification accuracy. The results show that the proposed algorithm in most cases provides better or comparable performance compared to the other mentioned algorithms.

Keywords: MLP NNs, BBO, Sonar, Meta-heuristic Algorithms

* Corresponding Author Email: m_mosavi@iust.ac.ir

A New Method For Finding Matrix Key And It's Inverse For Hill Cipher Algorithm

Saeid Mohammadian Semnani*

*Semnan University

ABSTRACT

Hill CIPHER algorithm is an application of linear algebra in cryptography.Cryptography is a science that use in coding and decoding the string texts.In this method we use a non singular matrix with integer numbers as noun key matrix. These matrices have some properties that we will want introduce them and calculate their inverse.

Keywords: matrix key, Coding, Decoding, Hill Cipher

* Corresponding Author Email: msafavi@aut.ac.ir

Image watermarking based on multiple SVD in wavelet domain using the PSO

Javad Vahidi[*]**,**

*Iran University of Science and Technology

ABSTRACT

Each day the number of those digital products, such as sounds, images and digital videos in their daily lives, grows On the other hand ability to copy these products, easily and without loss of quality has always been to design a system which could protect the goods and the rights of their owners, one of the serious needs of the field. Today watermarking in digital products, as a solution to implement and proof of ownership, and control the number of copies printed of a researcher's work. Watermarking is a subtle signal in the digital media data, so there is no change in the original data, but if necessary it can be extracted and used as a claim to ownership of digital effects. In this paper, a new hybrid method for watermarking images is peresented to extract the watermark that after the attacks, the Particle Swarm optimization (PSO) is used to find the most optimal amount of scaling factor.

Keywords: particle swarm optimization, watermarking digital images, transforming fields, singular value decomposition.

* Corresponding Author Email: jvahidi@iust.ac.ir

Modeling and solving multiobjective security game problem using multiobjective bilevel problem and its application in metro security system

Hamid Bigdeli*, Hassan Hassanpour

*University of Birjand

ABSTRACT

In this paper multiobjective security games between a defender and multiple attackers are studied. The aim of this paper is to select the optimal strategy for defender with limited security resources against the possible attacks of several types of attackers. The mentioned multiobjective security game is formulated as a multiobjective bilevel problem. Then the problem is reduced to a multiobjective single-objective problem by KKT optimality conditions and goal programming approach is proposed to solve it. Finally, an application of these games is presented to security in the metro stations.

Keywords: Game theory, Security game, Goal programming, Multiobjective bilevel optimization.

* Corresponding Author Email: h.bigdeli@birjand.ac.ir

Code obfuscation by Abstract interpretation

Mohammad Hadi Alaeiyan*, Saeed Parsa
Iran University of Science and Technology

ABSTRACT

The aim is to obfuscate codes which could not be easily analyzed by abstract interpretation. Abstract interpretation summarizes the code to extract the semantics of the code. In this way, abstract interpretation ignores all changes and transformations applied to obfuscate the code and extracts the code semantics. Then previous obfuscation methods are inefficient against abstract interpretation. In this article, we presented a new code obfuscation method preventing abstract interpretation of obfuscated executable codes. We utilize abstract interpretation to extract semantics and insert infeasible paths to provide a more complex code. The evaluation declares that obfuscated malware, which is not detected by anti-malware tools, applied their roguish aims and evaded the anti-malware tools.

Keywords: code obfuscation, Assembly language, Interval static analysis, Abstract interpretation.

* Corresponding Author Email: hadi_alaeiyan@comp.iust.ac.ir

A Note on Perfect Codes in Distance Balanced Graphs

Hassan Kharazi*, Mehdi Alaeiyan, Hossein Shabani

*Imam Hossein University

ABSTRACT

In this paper, we investigate the existence of the perfect codes in some classes of distance balanced graphs. Some results about the existence of perfect codes in these graphs as in direct product of cycle and the second power of the graphs are collected.

Keywords: Distance balanced graph, perfect code, power of graph

* Corresponding Author Email: hkharazi@ihu.ac.ir

New Differential-Linear Attack on Block Ciphers

Masohd Hadian Dehkordi*, Roghayeh Taghizadeh

*Iran University of Science and Technology

ABSTRACT

Differential and linear cryptanalysis are two important technique for evaluate the security of block ciphers. In this paper we introduce a new chosen text attack on block cipher that combine the differential and linear cryptanalysis. In this attack we use a differential characteristic over a part of the block cipher with probability of 1 and linear approximation with zero correlation, immediately following the differential characteristic.

Keywords: Block Cipher, Differential-Linear Cryptanalysis, Linear Approximation

* Corresponding Author Email: mhadian@iust.ac.ir

Some new bounds on the information ratio of the cartesian product of some classes of graphs

Abbas Cheraghi*, Mohammad Gholami

*Department of Mathematics, Khansar Faculty of Mathematics and Computer Science, Khansar, Iran

ABSTRACT

In this paper, we find a lower-bound for the information ratio of the cartesian product of an arbitrary tree with diameter at least 3 and a cycle C_m for every $m \geq 3$. Moreover, we determine the best information ratio of the perfect secret sharing scheme based on the graph C_6^d constructed from the cartesian product of a cycle of length with the -dimensional cube Q_d. More precisely, it is shown that for every $d \geq 1$, the information ratio of C_6^d is exactly $\frac{d(d+3)+3}{2(d+1)}$.

Keywords: Secret Sharing Scheme, Information Ratio, cartesian Product

* Corresponding Author Email: a.cheraghi@khn.ui.ac.ir

Constructing new functions

Mehdi Alaeiyan*, M. K. Hosseinipour

*Iran University of Science and Technology

ABSTRACT

A function $F:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$ is called almost perfect nonlinear (APN) if for every $a\neq o$ and every b in $\mathbb{F}_{2^n}$ the equation $F(x+a)+F(x)=b$ admist atmost 2 solutions. In this paper we get a new function $x^3+tr\left(x^9+x^3\right)$ over $\mathbb{F}_{2^n}$ for any positive integer .

Keywords: Almost Bent, Almost perfect nonlinear, Differential uniformity, S-box

* Corresponding Author Email: alaeiyan@iust.ac.ir

Editorial (sorted by name)

Consultants and Reviewers In This number of Journal

In The Name of Allah

Imam Khamenei:

Defence Electronics is very important to us.
Work on electronic stuff.

2010/02/19

1986
Imam Hossein Comprehensive University
Faculty Of Electronic Warfare
and Cyber Defence

Journal of
Electronic & cyber Defence

International Conference on Combinatorics,
Cryptography and Computing, 2016, ISSN: 2322-4347

Publisher: Imam Hossein Comprhensive University

Managing Director: Dr. Alireza Sadeghi

Editor-in-Chief: Dr. Abdolrasoul Mirghadri

Administrative Director: Saeid Zardar

- Rated - scientific research on a number 3/85595 Dated 2013/9/3 Ministry of Science, Research and Technology.
- Publishing license number: 91/27762 date: 2012.10.12 of Ministry of Culture and Islamic Guidance.
- **Lithography and printing**: Hadaf.
- **Press Address**: New Lalezar St. Hadaf Printing
- **Expert**: A. Tabarzadi
- **Copyeditor:** S. Zardar
- **Type Setting:** M. Esmaeilzadeh
- **Price:** 100,000 IRR

This journal is indexed in the following sites:

- ✓ *Iran Research Institute for information Science and Technology (www.irandoc.ac.ir)*
- ✓ *Database Bank of Scientific Publications (www.magiran.com)*
- ✓ *Islamic World Science Citation (www.isc.gov.ir)*
- ✓ *Scientific Information Database (www.SID.ir)*
- ✓ *Noor specialized magazines website (www.noormags.ir)*

The Journal of Faculty of Electronic Warfare and Cyber Defense Institute, is published.

Address: Office of Electronic & Cyber Defence Journal, Baqer-Al-Oloum Building, Imam Sadiq Site, Imam Hossein Comprehensive University, Shahid Babaee Highway, Tehran, I. R. Iran

P. O. Box: 16535-187 Phone: +98-21-73829200 Fax: +98-21-73829139

http://ecdj.ihu.ac.ir **Email: ecdjournal@ihu.ac.ir**