فصلنامه رویکردهای پژوهشی نوین در
مدیریت و حسابداری
سال چهارم، شماره ۳۰، بهار ۱۳۹۹- جلد چهارم، ص ۱۶۰-۱۴۳

Journal of New Research Approaches
in Management and Accounting
ISSN: 2588-4573
http://www.majournal.ir

سیستم های محافظ مصنوعی هوشمند برای تامین امنیت و محافظت از سیستم‌های اطلاعاتی حسابداری

ساجد داداشی [*1]

تاریخ دریافت: ۱۳۹۹/۰۱/۱۵ تاریخ چاپ: ۱۳۹۹/۰۲/۱۰

چکیده

سیستم‌های اطلاعاتی مدیریت و حسابداری حاوی داده‌های بسیار مهم با دقت بالا هستند و به همین خاطر، محافظت از این سیستم‌ها و تامین امنیت آنها در برابر هر گونه حمله یا تهدید از قبیل ویروس‌ها بیش از پیش لازم و ضروری است. سیستم‌های محافظ مصنوعی به عنوان یک شاخه از هوش محاسباتی دارای قابلیت بالقوه برای افزایش ایمنی سیستم‌های کامپیوتری و اطلاعاتی هستند. با افزایش مقدار داده ها، اتصال عمومی و ارتباط، حفظ امنیت سیستم‌ها از اهمیت بیشتری برخوردار شده‌است. از زمان ظهور تحمل پذیری خطا، تکنیک‌های بسیاری برای افزایش قابلیت اطیمنان ایجاد شده‌اند. در طبیعت، سیستم محافظ بدن، از یک فرم یادگیری برای بدست آوردن عملیات مطمئن در بدن حتی در حضور مهاجمان، استفاده می‌کند. سیستم‌های محافظ مصنوعی با راهکارهای الهام گرفته شده از مطالعه و تحلیل سیستم محافظ طبیعی، این امکان را فراهم می‌آورد که بتوان به نحوی کارآمد، امنیت سیستم‌های اطلاعاتی را فراهم کرده و همچنین، تحمل‌پذیری آنها در برابر خطا را افزایش داد.

واژگان کلیدی

سیستم اطلاعاتی مدیریت و حسابداری، سیستم محافظ مصنوعی، الگوریتم محافظ

[1] گروه مهندسی کامپیوتر، دانشگاه آزاد اسلامی واحد رودسر و املش، رودسر، ایران. (* نویسنده مسئول: sajed.dadashi@gmail.com)

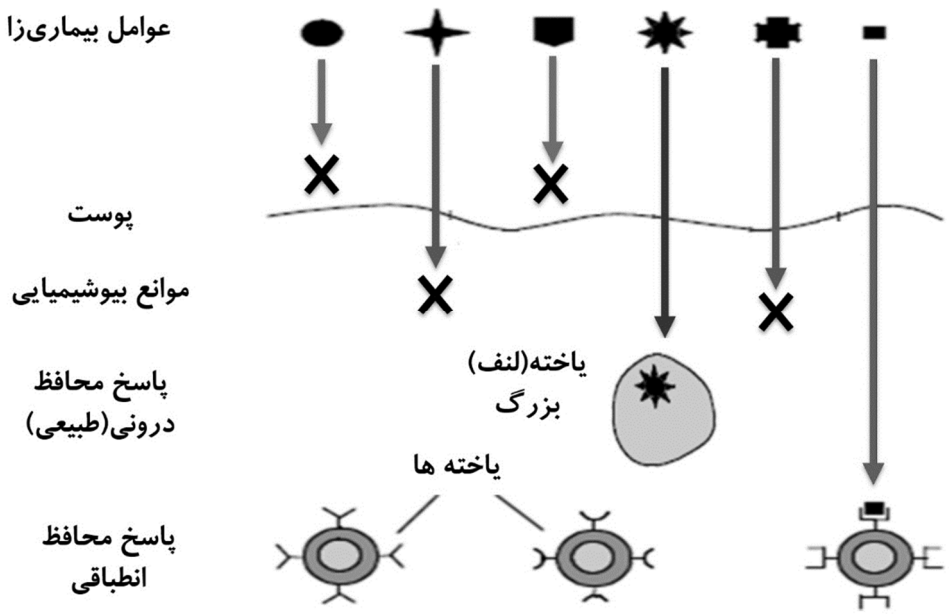
۱. مقدمه

سیستم محافظ مصنوعی کامپیوتر را با رشته های بیتی، شبیه سازی می کرد و قانون انطباق سست را به صورت درجه انطباق، استفاده می‌کند و آستانه‌ای را تعریف می‌کرد که بر اساس آن، انطباق صورت می گرفت، به این معنی که اگر تعداد انطباق در بیت‌ها، کمتر از حد آستانه بود، انطباقی صورت نمی گرفت و در واقع، برای اینکه عمل انطباق صورت گیرد، باید حداقل به اندازه حد آستانه، انطباق در سطح بیت انجام می‌شد (جانسون، ۲۰۰۷). همچنین، سطوح تجمعها را شبیه سازی کرده و بر اساس آن، رشته ها را ایجاد می کرد. مسلما، برای تولید رشته ها و مقایسه آنها، نیاز به حافظه بوده است. به تدریج، مدل‌هایی برای مسائل مختلف، از قبیل یادگیری، بهینه سازی و غیره به وجود آمدند که علاوه بر حل مسأله، سعی در افزایش سرعت و دقت کار داشتند.

همانند سیستم محافظ طبیعی، سیستم محافظ مصنوعی باید قادر به تشخیص بین خودی و غیرخودی باشد و در واقع، بتواند بین خودی و غیر خودی، تفاوت قائل شود و پاسخ‌های لازم را برای مقابله با غیرخودی (حالتهای غیر معتبر) تولید کند. سیستم محافظ مصنوعی، مدلی از سیستم محافظ طبیعی است که می‌تواند توسط زیست شناسان برای تفسیر استفاده شود. همچنین، فعالیت‌های آزمایشی و پیشگویی، به عنوان زیست شناسی محاسباتی، نامیده می‌شود. تعریف دیگر، این است که یک سیستم محافظ مصنوعی، یک انتزاع از یک فرآیند زیستی است که جانداران (انسان و حیوانات) را از ورود بدون اجازه مواد خارجی محافظت می‌کند که می‌تواند ایده بسیار سودمندی در زمینه تامین امنیت سیستم های کامپیوتری باشد.

طبیعت، اساسا، راهکارهای مختلفی برای حل مسائل پیچیده، نشان می‌دهد که در حال حاظر در زمینه‌های محاسبه و الکترونیک برای بهبود بسیاری از تکنیک‌های قدیمی استفاده شده‌اند. یکی از این زمینه‌ها، یعنی طراحی سیستم مطمئن با روشهای تکاملی از طریق سخت افزار نتیجه و توسعه سلولی چندگانه در مراحل جنینی، آزمایش شده‌است. گونه‌های مختلف حیات، مکانیزم‌های دفاعی خاص خود را دارا هستند که می‌توانند به عنوان یک سیستم محافظ به کار روند (تیمیس و همکاران، ۲۰۱۴). مهره‌داران، یک مکانیزم دفاع چند لایه و بسیار پیچیده را در فرم سیستم محافظ، برای فراهم کردن حفاظت از تأثیرات خارجی بالقوه، مانند تأثیرات باکتری و ویروس (آنتی ژن)، به کار می‌گیرند. فرآیند تشخیص آنتی‌ژن و خود تحمل پذیری، ضرورتا یکی از تفاوت‌های بین خودی و غیر خودی است که با یک دقت تقریبا نامحدود انجام می‌شود. شباهت‌ها بین نیازهای تحمل پذیری خطا و عمل مکانیزم‌های دفاع بدن، ارتباط سیستم محافظ را به عنوان یک مدل مفهومی، برای طراحی سیستم‌های مطمئن آینده، پررنگ کرده‌است.

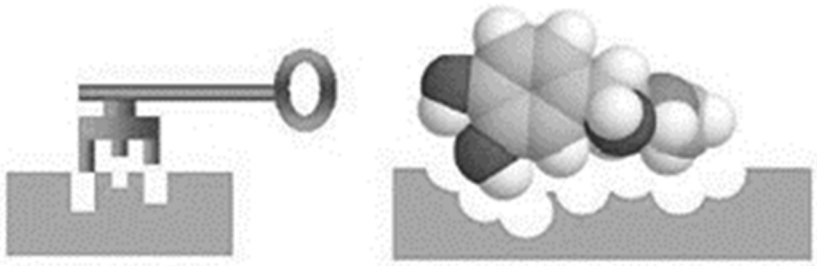
اندام سیستم محافظ زیستی، مستقل، توزیع شده و بدون پیوند به سیستم عصبی هستند. آنتی ژن‌ها، معمولا توسط سلول‌های عرضه کننده آنتی ژن، به سیستم محافظ و در داخل گره‌های لنف عرضه می‌شوند. لایه‌های مختلف موجود در سیستم محافظ، در شکل ۱، نشان داده شده‌اند:



شکل ۱. لایه‌های مختلف در سیستم محافظ

سلول‌های سیستم محافظ، به دو دسته سیستم محافظ داخلی و سیستم محافظ انطباقی تقسیم می‌شوند. در سیستم محافظ داخلی، یاخته درشت که یک سلول خونی سفید بزرگ است، عوامل مضر بالقوه و خارجی را نابود می‌کند، به این صورت که آنتی ژن‌ها را غرق می‌کند. در سیستم محافظ انطباقی، دو نوع لنفوسیت وجود دارند. سلول‌های B که در مغز استخوان تولید می‌شوند و سلول‌های T که توسط غذه تیموس تولید می‌شوند. سلول‌های T، آنتی ژن‌ها را به خاطر پوشش آنها تشخیص داده و پاسخ پیچیده‌ای را ایجاد می‌کنند. در واقع، سیستم محافظ زیستی می‌تواند به عنوان یک سیستم محافظتی چند لایه تصور شود که هر لایه، انواع مختلف مکانیزم‌های دفاع را برای تشخیص، مطابقت و پاسخ‌ها، فراهم می‌کند.

پادتن‌ها، در پاسخ محافظ لنفی تولید می‌شوند که توابع و الگوهای تطابق را دارا بوده و بنابراین به آنتی ژن‌های خارجی می‌پیوندند. این کار، به صورت یک مکانیزم قفل و کلید انجام می‌شود، به طوری که اگر پادتن‌ها، بتوانند به عنوان کلیدی برای باز کردن قفل آنتی ژن، عمل کنند، می‌توانند به آن بچسبند که این کار، با توجه به شکل سطح آنتی ژن صورت می‌گیرد. این فرآیند، در شکل ۲، نشان داده شده‌است.



شکل ۲. قفل و کلید: مولکول‌ها، توسط یک مکانیزم قفل و کلید و بر طبق اندازه و دیگر خصوصیات سطح مولکولی، به یکدیگر می‌پیوندند.

بسیاری از مدل‌های سیستم محافظ مصنوعی و طراحی الگوریتم‌های مورد نیاز، با استفاده از مدل‌های ساده شده از فرآیندهای زیستی مختلف و توابع عملیاتی به وجود می‌آیند؛ مانند دیگر تکنیک‌های الهام گرفته‌شده از طبیعت از قبیل شبکه‌های عصبی مصنوعی، الگوریتم‌های ژنتیک و اتوماتای سلولی، سیستم‌های محافظ مصنوعی نیز از طبیعت الهام گرفته شده‌اند. این سیستم‌ها در واقع از روی مکانیزم‌های سیستم محافظ زیستی به وجود می‌آیند. برای این کار، فرآیندهای طبیعی مربوط به سیستم محافظ زیستی و شبیه سازی رفتار پویای آن در حضور آنتی ژن‌ها/عوامل بیماری‌زا تحلیل و بررسی شده و در سیستم محافظ مصنوعی استفاده می‌شوند.

در بخش ۲، سیستم‌های محافظ مصنوعی و طرز عمل آنها، آمده‌است. در بخش ۳، الگوریتم‌های مختلفی که در سیستم‌های محافظ مصنوعی به کار می‌روند و قوانین انطباق، بحث شده‌اند. این الگوریتم‌ها، باعث تشخیص خطا شده و سیستم را در برابر خطا مصون می دارند. در بخش ۴، سیستم محافظ مصنوعی برای شناسایی و حذف ویروس در سیستم‌های اطلاعاتی، تحلیل و ارزیابی می‌شود. تشخیص خطای مبتنی بر مصونیت در بخش ۵ بررسی شده‌است و سرانجام در بخش ۶، نتایج عنوان شده‌است.

۲. سیستم‌های محافظ مصنوعی

سیستم‌های محافظ مصنوعی، به عنوان شاخه جدید در هوش محاسباتی به وجود آمدند. این سیستم‌ها در تشخیص الگو، تشخیص خطا، امنیت کامپیوتر و دسته متنوعی از کاربردها استفاده می‌شوند. در میان مکانیزم‌های متنوع در سیستم محافظ زیستی که به عنوان سیستم‌های محافظ مصنوعی، جستجو شده اند، انتخاب منفی، مدل شبکه محافظ و انتخاب تولید مثل، هنوز، معمول‌ترین مدل‌های قابل بحث هستند. راهکارهای زیستی در حال حاضر، برای امنیت کامپیوتر، تشخیص ویروس، تشخیص ناهنجاری، نظارت بر فرآیند، کنترل ربات و تحمل پذیری خطای نرم افزار، استفاده می‌شوند. (فارست و پلرسون)، از تحلیل نظری خصوصیات انطباق و پیوستن سیستم محافظ، الگوریتم انتخاب منفی را توسعه داده‌اند و از طریق آن، امنیت کامپیوتر، تشخیص ویروس و کاربردهای تشخیص بی قاعدگی ایجاد شده‌اند.

مدل‌های شبکه محافظ:

سیستم محافظ که شبکه‌ای از سلوله‌ای B متصل شده است، برای تشخیص آنتی ژن، نگهداری می‌شود. این سلول‌ها، یکدیگر را به طرق خاصی تحریک کرده و یا متوقف می کنند که منجر به پایداری شبکه می‌شود. دو سلول B، متصل هستند، اگر نزدیکی‌هایی که به اشتراک می‌گذارند، از یک آستانه مشخص تجاوز کند و قدرت اتصال، مستقیما متناسب با مقدار نزدیکی است که آنها به اشتراک می‌گذارند.

در مدل‌های شبکه محافظ مصنوعی، جمعیت یک سلول B، از دو زیر جمعیت ساخته شده است: جمعیت اولیه و جمعیت تولید مثل. مجموعه اولیه، از یک زیرمجموعه از داده آموزشی ردیفی برای ساختن شبکه سلول B، تولید شده است. باقیمانده‌ها، به عنوان اقلام آموزشی آنتی ژن، استفاده شده‌اند. آنتی‌ژنها، به صورت تصادفی از مجموعه آموزشی انتخاب شده و به ناحیه‌های شبکه سلول B، ارائه می‌شوند. اگر پیوستن، موفقیت آمیز بود، سلول B، تولید مثل کرده و تغییر پیدا می‌کند. تغییر، منجر به یک مجموعه متنوع از پادتن‌ها می‌شود که می‌توانند در یک زیرروال طبقه بندی، استفاده شوند. یکبار که یک سلول B جدید، ساخته می‌شود، تلاشی برای مجتمع کردن آن به شبکه، در نزدیکترین سلول‌های B، انجام می‌شود. اگر سلول B جدید، نتواند مجتمع شود، از جمعیت، حذف می شود. اگر هیچ پیوستنی، موفقیت آمیز نبود، یک سلول B با استفاده از آنتی ژن، به عنوان یک نمونه، تولید شده و سپس، به شبکه متحد می‌شود.

یک نسخه ارتقاء یافته، از توپ تشخیص مصنوعی، برای نمایش یک تعداد از سلولهای B مشابه (نه یک سلول B منفرد)، استفاده می‌کند. این، ایده توپ تشخیص در زیست شناسی را به یاد می‌آورد که به ناحیه‌هایی در فضای شکل آنتی‌ژن اشاره می‌کند که یک پادتن، می‌تواند تشخیص دهد. آن، یک قلم داده n بعدی را نشان می‌دهد که می‌تواند توسط فاصله اقلیدسی، به یک آنتی ژن یا یک توپ تشخیص مصنوعی دیگر، انطباق پیدا کند. یک پیوند بین دو سلول B ساخته می شود، اگر فاصله بین دو توپ تشخیص مصنوعی، در پایین آستانه نزدیکی شبکه باشد. نتایج، نشان می‌دهند که ترکیب نرمال سازی سطوح تحریک توپ‌های تشخیص مصنوعی در شبکه و مکانیزم تخصیص منابع، به بایاس کردن نسخه ارتقا یافته شبکه محافظ مصنوعی به سوی قویترین الگو در مجموعه داده، برای ظاهر شدن، منجر می‌شود.

اصل انتخاب تولید مثل:

اصل انتخاب تولید مثل، ویژگی‌های اصلی پاسخ مصنوعی را برای تحریک آنتی ژن شرح می‌دهد. آن، ایده‌ای را برقرار می‌کند که تنها آن سلول‌هایی را که آنتی ژن را تشخیص می‌دهند، تکثیر می‌شوند، بنابراین، این سلول‌ها، در مقابل آنهایی که این کار را انجام نمی‌دهند، انتخاب شده‌اند. ویژگی‌های اصلی تئوری تولید مثل، اینها هستند:

- سلول‌های جدید، کپی‌هایی از والدین خود هستند (تولید مثل) که به یک مکانیزم تغییر با نرخ‌های بالا (تغییر بسیار سریع سلول‌ها) شبیه است.
- حذف لنفوسیت‌های متفاوت جدید که گیرنده‌های عکس العمل خود را حمل می‌کنند.
- تکثیر و تفاوت روی سلول‌های بالغ رسیده، در اتصال سلول‌های بالغ با آنتی ژن‌ها

الگوریتم clonalg، مبتنی بر انتخاب تولید مثل و اصول بلوغ نزدیکی می‌باشد (داسگوپتا، ۲۰۰۶). آن، شبیه به الگوریتم‌های تکاملی مبتنی بر بلوغ می‌باشد و چند ویژگی جالب دارد: ۱) اندازه جمعیت، به صورت پویا، داده می‌شود، ۲) بهره برداری و شناسایی فضای جستجو، ۳) مکان بهینه چندگانه، ۴) قابلیت نگهداری راه حل‌های بهینه محلی و ۵) معیار توقف تعریف شده.

۳. الگوریتم‌های محافظ مصنوعی

الگوریتم‌های سیستم محافظ مصنوعی مبتنی بر جمعیت:

سه الگوریتم معمول در سیستم محافظ مصنوعی، انتخاب مثبت، منفی و تولید مثل هستند که همگی، مبتنی بر جمعیت عامل‌های آموزش دیده شده برای تشخیص جنبه‌های مشخص می‌باشند. شباهت‌هایی بین الگوریتم‌ها وجود دارد: به عنوان مثال، انتخاب مثبت و منفی، فقط دو طرف سکه مشابهی هستند. همچنین، تفاوت‌هایی وجود دارد: انتخاب مثبت و منفی، شامل تولید تصادفی تشخیص دهنده‌های کاندید هستند، در حالی که انتخاب تولید مثل، از یک شکل تقویت مبتنی بر انتخاب و جهش بهترین تشخیص دهنده‌ها، استفاده می‌کند.

الگوریتم‌های سیستم محافظ مصنوعی مبتنی بر شبکه:

تئوری شبکه محافظ اصلی، یک سیستم محافظ با یک رفتار پویا، حتی در حضور آنتی ژن‌ها را پیشنهاد می‌کند (بچمایر، ۲۰۰۷). این، از اساس زیستی الگوریتم‌های تولید مثل و انتخاب منفی، متفاوت است، به طوری که پیشنهاد می‌کند که سلول‌های B قادر به تشخیص یکدیگر هستند. این، روی الگوریتم سیستم محافظ مصنوعی اثر دارد: اگر زیست شناسی، درست نیست، پس باید یکی الگوریتم را دوباره امتحان کند تا بفهمد که در واقع، چه چیز است. این، نور امیدی را روی

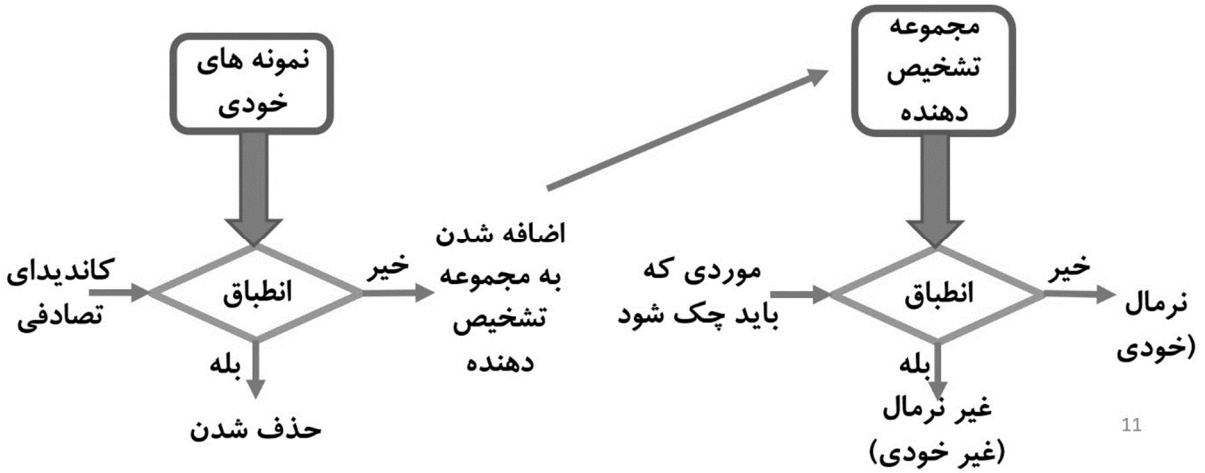
ماهیت بسیار پیچیده سیستم‌های محافظ و شبکه هایی که در حال حاضر، هستند، جاری می کند. برای بدست آوردن این فهم، در مرحله اول، باید سیستم زیستی را از جنبه تفسیر سیستم به عنوان یک شبکه از تعامل، همکاری و رقابت در مقابل مولکول‌ها، سلول‌ها، اندام‌ها و بافت‌ها، کاوش کرد. سپس، نتایج، برای فرمول بندی یک نگاشت مناسب بین خصوصیات زیستی و اجزاء ساختار استفاده می‌شود. سپس، این اجزاء می‌توانند به عنوان اساسی برای توپولوژی و پویایی مدل‌های زیستی جدید و همچنین آزمایش دوباره مدل‌های موجود استفاده شوند. مدل‌های جدید، فهم بیشتری از عمل چنین سیستم‌هایی برای توسعه در مفهوم مصنوعی را اجازه می دهند.

باید د ر مورد در مفهوم این مدل‌های شبکه محافظ جدید، آزمایش شود، به عنوان مثال، تئوری خطر، مفهوم پاسخ، مکانیزم‌های حافظه، پاسخ الارم عمومی یا پاسخ استرس، تشخیص خودی/غیر خودی و خود اثباتی را آزمایش می‌کند (آیکلین و همکاران، ۲۰۰۲). به علاوه، نقض سازنده نویز در سیستم‌های زیستی که یک ویژگی ذاتی در چنین سیستم‌هایی است، می‌تواند آزمایش شود. از این مدل‌های زیستی، تشبیهات محاسباتی جدید و ساختارهای تحلیلی، می‌توانند برای مشمول کردن نمایش‌های مناسب برای اجزاء، روش‌های شناسایی تعاملات بین اجزاء و فرآیندهای عمل کننده روی اجزاء، ساخته شوند. همچنین، این ساختارها به مدل‌های زیستی اجازه می‌دهد تا نمایش داده شده و در تعدادی از روش‌ها، دستکاری شوند. در یک پشتیبانی از ساختار، باید به ثبت خصوصیات مربوط به کاربردی که می خواهد توسعه پیدا کند، اجازه داده شود. در یک فرآیند تکراری، الگوریتم‌های ساختار، باید به منظور تست و توسعه تشابهات زیستی، با توجه به عملیات پیاده سازی و آزمایش ساختار پایه‌ای مفهوم، پیاده سازی و تست شوند.

الگوریتم‌های انتخاب منفی

یکی از اهداف سیستم محافظ، تشخیص تمام سلول‌ها (یا مولکول‌ها)، در بدن و طبقه بندی آن سلول‌ها به عنوان خودی و غیر خودی است. سلول‌های غیر خودی، اغلب، به منظور القاء یک نوع مناسب از مکانیزم دفاع است. سیستم محافظ، از طریق سیر تکاملی، یاد می‌گیرد تا بین آنتی ژن‌های خارجی (یعنی، باکتری، ویروس و غیره) و سلول‌های خودی بدن یا مولکول‌ها، تفاوت قائل شود. هدف انتخاب منفی، فراهم کردن تحمل (خطای مجاز، اختلاف مجاز) برای سلول‌های خود است. انتخاب منفی، با قابلیت سیستم محافظ برای شناسایی آنتی ژن‌های ناشناخته، بدون عکس العمل به سلول‌های خودی مربوط است. در طی تولید سلول‌های T، گیرنده‌ها، از طریق یک فرآیند مرتب سازی دوباره ژنتیک شبه تصادفی، ایجاد می‌شوند. سپس، متحمل یک فرآیند سانسور در غده تیموس، به نام انتخاب منفی می‌شوند؛ بنابراین، سلول‌های T که در مقابل پروتئین‌های خودی، عکس العمل نشان می‌دهند، نابود خواهند شد؛ بنابراین، تنها آن‌هایی که به پروتئین‌های خودی نپوسته‌اند، اجازه داده می‌شود تا غده تیموس را ترک کنند. سپس، این سلول‌های T بالغ، برای اجرای عملیات زیستی و حفاظت از بدن در مقابل آنتی ژن‌های خارجی، در تمام بدن می‌چرخند. در واقع، غده تیموس، سلول‌های T را آموزش می‌دهد. آن سلول‌هایی را که با خودی عکس العمل نشان می‌دهند را سانسور می‌کند. این الگوریتم، یکی از مدل‌های محاسباتی از تفکیک خودی/غیر خودی است که که در کاربردهای جهان واقعی متنوعی به کار رفته‌است. در تکامل و تنوع این روش، مشخصات اصلی یک الگوریتم انتخاب منفی شرح داده شده‌است (تیشودین، ۲۰۰۶). شکل ۳، مشابه با مفهوم اصلی، مراحل اصلی چنین الگوریتمی را نشان می‌دهند. در مرحله تولید، تشخیص دهنده‌ها توسط بعضی فرآیندهای تصادفی، تولید می‌شوند و با تلاش برای انطباق نمونه‌های خودی، سانسور می‌شوند. آنهایی که برای آن انطباق کاندید شده اند حذف شده و بقیه، به عنوان تشخیص دهنده‌ها، نگهداشته می‌شوند. در مرحله تشخیص، جمع آوری مجموعه تشخیص

دهنده ها برای چک کردن اینکه نمونه داده ورودی، خودی یا غیر خودی است، استفاده می‌شود. اگر آن، با هر تشخیص دهنده ای انطباق دهد، آن، به عنوان غیر خودی یا ناهنجاری، ادعا می‌شود.



شکل ۳. مفهوم اصلی الگوریتم انتخاب منفی

اصل اساسی الگوریتم انتخاب منفی به صورت زیر است:

– خودی را به عنوان یک مجموعه چندگانه S از رشته ها با طولی در یک الفبای محدود تعریف می کنیم که می خواهیم محافظت یا نظارت شود. به عنوان مثال، S، ممکن است یک فایل بخش بندی شده، یا یک الگوی نرمال از فعالیت بعضی سیستم‌ها یا فرآیندها باشد.

– تولید یک مجموعه R از تشخیص دهنده ها که هریک، برای انطباق هر رشته در S شکست می‌خورند. ما از یک قانون انطباق جزئی استفاده می‌کنیم که در آن، دو رشته، انطباق دارند، اگر و تنها اگر آنها در حداقل r موقعیت پیوسته یکسان هستند که r، یک پارامتر انتخاب شده مناسب است.

– نظارت S بر روی تغییرات، توسط انطباق پیوسته تشخیص دهنده‌ها در مقابل S. اگر هر تشخیص‌دهنده انطباق داد، یک تغییر باید اتفاق افتاده باشد.

قانون انطباق:

یک قانون انطباق جزئی مبتنی بر یک درجه از پیش مشخص شده از شباهت در نظر می‌گیریم. برای اندازه گیری این شباهت، ما از قانون انطباق پیوسته r بین دو رشته با طول مساوی استفاده می‌کنیم؛ بنابراین، برای هر دو رشته x و y، match(x,y) درست است اگر x و y روی حداقل r مکان پیوسته (r، کمتر یا مساوی l)، توافق یا انطباق دارند. با یک مثال می‌توان قانون انطباق را نمایش داد:

X:bcabcbad
Y: dcabdcba

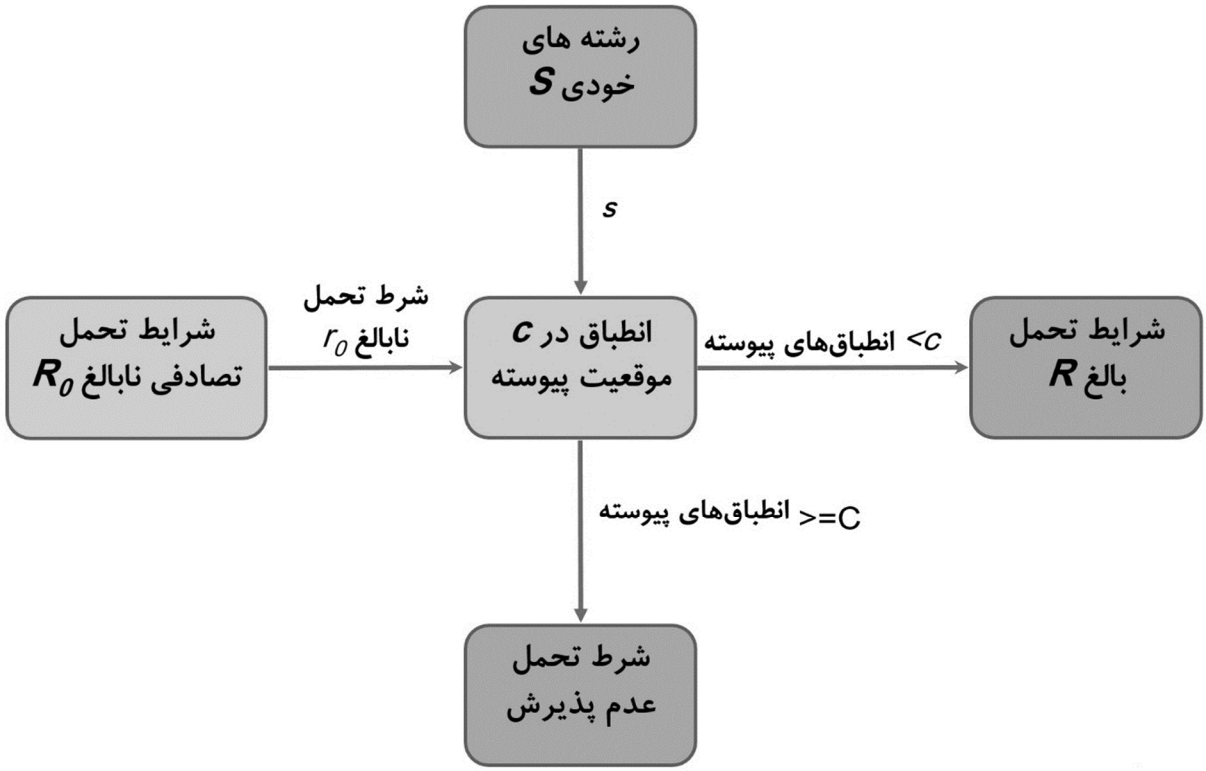
x و y، دو رشته تعریف شده حول الفبای ۴ حرفی a، b، c و d هستند. X و Y، در سه مکان پیوسته (زیر خط دار)، انطباق دارند؛ بنابراین، match(x,y)، برای $r \geq 3$ درست و برای $r > 3$ نادرست است.

یک قانون انطباق جزئی، یک تشخیص دهنده با قابلیت تشخیص رشته های نمونه در همسایگی خود، با توجه به مقدار آستانه r را فراهم می‌کند. پوشش یک رشته با طول تعریف شده، با کاهش r، به صورت نمایی افزایش می‌یابد. به هر حال پوشش ماکزیمم می‌تواند با r=l بدست آید، اما تشخیص دهنده‌های تولید شده، احتمالا با بسیاری از رشته‌های خودی در تشخیص نادرست انطباق دارند. از طرف دیگر، یک انطباق کامل (برای r=l)، دلالت بر این دارد که نمادها، در هر مکان در دو رشته، یکی هستند. در نتیجه تعداد بسیار بزرگی از تشخیص دهنده‌ها، برای تشخیص الگوها در فضای غیر خودی لازم هستند. یک مقدار بهینه r، یک اندازه منطقی مجموعه تشخیص‌دهنده را برای موفقیت این روش برقرار می‌کند. هنگامی که یک مجموعه غیر همپوشان از تشخیص دهنده‌ها با یک آستانه انطباق مناسب تولید شدند، هر تشخیص دهنده می‌تواند به عنوان یک کلاس الگوی جدید در فضای غیر خودی خدمت کند. به هر حال در حالت تشخیص دهنده‌های همپوشان، تشخیص دهنده‌های چندگانه ممکن است برای یک الگوی نمونه (غیر نرمال) فعال شوند و نیاز به تشخیص دهنده‌های بیشتر برای فراهم کردن پوشش کافی در فضای غیر خودی داشته باشند.

تولید تشخیص دهنده ها

راه‌های ممکن زیادی برای تولید تشخیص دهنده‌ها در فضای غیرخودی، وجود دارد. این راهکارها، معمولا پیچیدگی‌های محاسباتی مختلف دارند و پیچیدگی آنها بستگی به انتخاب قانون انطباق دارد. در توصیف اولیه الگوریتم انتخاب منفی، تشخیص دهنده‌های کاندید به صورت تصادفی تولید شده و سپس تست می شوند تا مشخص شود که با هیچ رشته خودی، انطباق نداده باشند. اگر یک انطباق پیدا شود، کاندید حذف می‌شود. این فرآیند تا زمانی تکرار می شود که تعداد مطلوب از تشخیص دهنده‌ها تولید شده باشند. یک تحلیل احتمالاتی برای تخمین تعداد تشخیص دهنده‌های مورد نیاز برای فراهم کردن سطوح داده شده از قابلیت اطمینان استفاده شده است. محدودیت اصلی راهکار تولید تصادفی، مشکل محاسباتی تولید کردن تشخیص دهنده‌های معتبر است که به صورت نمایی با اندازه خودی، رشد می‌کنند. همچنین، برای بسیاری از انتخاب‌های l و r و ترکیبات خودی، تولید تصادفی رشته‌ها برای تشخیص دهنده‌ها ممکن است منع کننده باشد.

در اینجا، مجموعه های تشخیص دهنده را با استفاده از الگوریتمی تولید می‌کنیم که در زمان خطی و با اندازه خطی اجرا می‌شود (ساکاناکا و همکاران، ۲۰۱۹). الگوریتم دو فاز دارد: ابتدا یک تکنیک برنامه نویسی پویا را برای شمارش تعداد مراحل بازگشتی، به منظور تعریف یک سرشماری از تمام رشته های غیر منطبق شده (یعنی تمام تشخیص دهنده‌های موجه)، به کار می گیرد. دوما، یک زیرمجموعه تصادفی از این سرشماری، برای تولید یک مجموعه تشخیص دهنده، انتخاب می‌شود. به بیان دیگر، با یک مجموعه داده شده از رشته های خودی S و آستانه انطباق r، فاز اول الگوریتم تعداد کل رشته‌های غیر منطبق‌شده را که برای self(S) تعریف شده، وجود دارند را تعیین می‌کند. سپس، در فاز دوم، بعضی از آنها برای تولید تشخیص دهنده‌ها، برای نظارت خودی (الگوهای نرمال)، به کار می‌روند. شکل ۴، الگوریتم را نشان می‌دهد.



شکل ٤. الگوریتم انتخاب منفی

الگوریتم انتخاب منفی، توسط انتخاب یک مجموعه از رشته‌های R (سلول‌های T کمک کننده بالغ)، با طول l، از یک مجموعه R_0 داده اولیه تولید شده تصادفی (سلولهای T نابالغ) که برای انطباق با هر رشته خودی $s_i \in S$ شکست خورده‌اند، شروع می‌شود. همچنین با طول l وحداقل r موقعیت متوالی، احتمال یک انطباق بین دو رشته توسط معادله زیر داده شده‌است:

$$P_M \approx m^{-r}\left[(l-r)(m-1)/m+1\right]$$

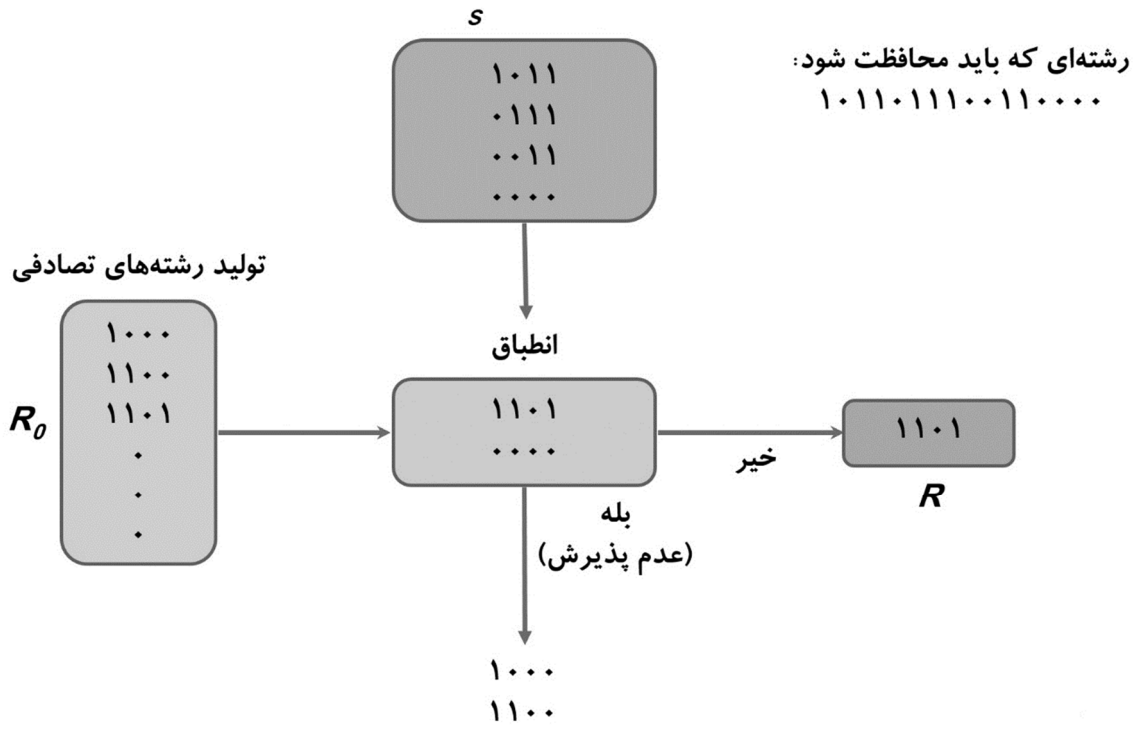
که m^{-r} 1 و m، تعداد نمادهای الفبا (۲، برای یک ماشین حالت متناهی دودویی) است. هر رشته ای که در حداقل c موقعیت پیوسته، انطباق داد حذف می‌شود. r، تعداد مطابقت‌های متوالی مورد نیاز برای یک تطبیق است. می‌توان دید که با افزایش تعداد نمادها در الفبا، احتمال تطابق به سرعت کاهش می‌یابد. به منظور ساختن R که به مجموعه شرایط تحمل پذیری با یک احتمال شکست به اندازه کافی کم مربوط است، تعداد رشته های خودی معتبر N_s، باید بسیار کمتر از تعداد رشته‌های نامعتبر N_e باشد. استفاده از یک روش تشخیص احتمالاتی، به این معنی است که یک مصالحه، می‌تواند بین تعداد شرایط تحمل پذیری، N_R و بنابراین، نیازهای حافظه و احتمال شکست تشخیص یک خطا، P_f،(احتمال تشخیص P_M، $1-P_f$، است) ایجاد شود. برای پیشگویی‌های نظری، این امر با معادله زیر، تعریف شده است:

$$P_{f_t} = \left(1-P_M\right)^{N_R} \qquad (2)$$

در طول مرحله عملیاتی فرآیند، داده از سیستم محافظت شده، گرفته شده و در مقابل لیستی از شرایط تحمل پذیری ذخیره شده R، مقایسه می‌شود. اگر هر انطباقی رخ دهد، سیستم، به یک بی قاعدگی/خطا، هشدار می‌دهد. مرحله عملیاتی از نظر

محاسباتی بسیار ساده‌تر است و پیاده سازی را برای یک سیستم سخت افزاری، بادوام می‌کند. در واقع، این الگوریتم برای تشخیص ناهنجاری در یک مجموعه از رشته ها توسعه یافته‌است که می‌تواند در checksum، طول و غیره تغییر یابد و توسط برنامه‌های مضر مانند یک ویروس، انجام شده باشد. در جهان واقعی، این رشته‌ها، یک برنامه کاربردی، داده یا هر بخش دیگر از سیستم کامپیوتری ذخیره شده در حافظه هستند (داسکوپتا و همکاران، ۲۰۰۲).

این، در یک پروسیجر به نام سانسور کردن و با برش دادن رشته محافظت شده به زیر رشته ها اتفاق می‌افتد که مجموعه S را از خود زیر رشته ها، تولید می‌کند. در مرحله بعدی، یک مجموعه از رشته های تصادفی، تولید می شود. آن دسته از رشته‌های تولید شده تصادفی که با خودشان مطابقت دارند، حذف شده و آنهایی که با هیچ رشته S مطابقت ندارند، یک عضو مجموعه تشخیصی R یا لیست نمایش می‌شوند. بعد از اینکه لیست نمایش، تولید شد، فاز نظارت می‌تواند با تطبیق پیوسته رشته‌ها از S در مقابل R، شروع شود. رشته‌ها، در همان ترتیبی که برای تطبیق تولید شده‌اند، انتخاب می‌شوند. ابتدا باید تشخیص دهنده‌ها تولید شوند که در شکل ۵ نشان داده شده‌است.



شکل ۵. تولید فهرست نمایش، با استفاده از الفبای (۰،۱) با r=2

یک مثال ساده، رشته ۰۰۱۱ است. اگر یک بیت، تغییر کند و مثلا رشته ۰۱۱۱ را بدهد، در بعضی نقاط در فرآیند نظارت، تشخیص داده خواهد شد که رشته تغییر یافته ۰۱۱۱(از S)، با رشته تشخیص دهنده ۰۱۱۱ از R، مطابقت دارد.

٤. تشخیص خطای مبتنی بر مصونیت

روش تشخیص خطا، یک الگوریتم انتخاب منفی مقدار دهی شده واقعی را به کار می‌گیرد که مبتنی بر اصل تفکیک خودی- غیرخودی در سیستم محافظ است. اساسا، خودی، الگوی نرمال داده و غیرخودی، الگوی غیر نرمال یا خطای داده است. الگوریتم انتخاب منفی، می‌تواند به صورت زیر خلاصه شود:

- تعریف خودی به عنوان یک مجموعه S از عناصر در یک فضای ویژگی U، یک مجموعه که نیاز به نظارت دارد. به عنوان نمونه، اگر U، مربوط به فضای حالت‌های یک سیستم و نمایش داده شده توسط یک لیست از ویژگی‌ها باشد، S، می‌تواند زیر مجموعه‌ای از حالت‌هایی را که به عنوان نرمال برای سیستم، در نظر گرفته می‌شوند را نشان دهد.

- تولید یک مجموعه F از تشخیص دهنده‌ها، هر یک، با انطباق به هر رشته در S، شکست می‌خورد. یک راهکار که سیستم محافظ را تقلید می‌کند، تشخیص دهنده‌های تصادفی را تولید کرده و آنهایی را که با هر عنصر در مجموعه خودی، انطباق دارند، حذف می‌کند.

- نظارت بر S، برای تغییرات، توسط انطباق پیوسته تشخیص دهنده‌ها در F، در مقابل S. اگر هر تشخیص دهنده، انطباق داد، نشان دهنده این است که یک تغییر، رخ داده است، به صورتی که تشخیص دهنده‌ها، برای انطباق ندادن با هیچ یک از نمونه های نمایش S، طراحی شده‌اند.

دو مرحله در تشخیص خطای مبتنی بر مصونیت وجود دارد، تولید تشخیص‌دهنده و تست کردن. در مرحله تولید تشخیص دهنده، الگوریتم RNS، یک مجموعه از تشخیص دهنده‌ها با اندازه متغیر که فضای غیر خودی را پوشش می‌دهند، بیرون می‌دهد (جیم و همکاران، ۲۰۱۹). یک تشخیص دهنده، به عنوان $d=(c,r_d)$ تعریف شده است که $c=(c_1,c_2,...c_m)$ ، یک نقطه m بعدی است که به مرکز یک فوق کره با شعاع r_d ، مربوط است.

فضای خودی، مربوط به حالت‌های عملیاتی نرمال سیستم تحت نظارت است؛ بنابراین، تشخیص ویژگیهای (نقطه m بعدی، c) مشخص کننده رفتار غیر نرمال سیستم و همچنین، ارائه انحرافات از امضاءهای صوری، در هنگامی که سیستم، off-nominal می باشد، مهم است. ویژگی‌ها، ممکن است اندازه گیری‌های سنسور یا کمیت‌های مشتق‌شده باشند. آنها، ممکن است همچنین، ویژگی‌های توسعه‌یافته با انتقال پنجره‌های همپوشانی از مراحل زمانی چندگانه، برای ثبت متغیرهای زمانی معمول باشند. مقادیر ویژگی‌ها، در رنج [۰,۰ ۱,۰]، به منظور تعریف فضای خودی- غیر خودی، با یک ابر مکعب واحد، مقیاس می‌شوند.

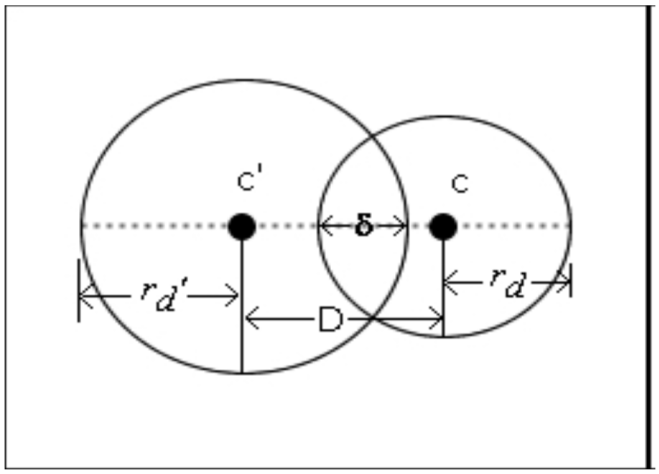
فرآیند تولید تشخیص دهنده، با یک جمعیت اولیه از تشخیص دهنده‌های کاندیدی که مکان‌های آنها، به صورت تصادفی انتخاب شده‌اند، شروع می‌شود. در تکرار اول، هنگامی که هیچ تشخیص دهنده بالغی وجود نداشته باشد، شعاع یک تشخیص دهنده کاندید خاص، با توجه به کمینه فاصله‌ها از آن، به نقاط خودی، تعیین می‌شوند. در تکرارهای زیردنباله، شعاع یک تشخیص دهنده کاندید، با توجه به کمینه فاصه ها از آن تا نقاط خودی و تشخیص دهنده های بالغ، تعیین می شود. محاسبات فاصله بین دو نقطه x و y، با استفاده از فاصله مینکووسکی، به صورت زیر تعریف می‌شوند:

$$D(x,y)=\left(\sum|x_i-y_i|^{\lambda}\right)^{\frac{1}{\lambda}} \qquad (1)$$

که $x=\{x_1,x_2,...x_N\}$ و $y=\{y_1,y_2,...y_N\}$ و $\lambda=N$. فاصله مینکووسکی با $\lambda=2$، معادل با فاصله اقلیدسی است.

اگر مکان تشخیص دهنده کاندید (یعنی مرکز تشخیص دهنده)، به نقطه خودی، نزدیکترین باشد، شعاع تشخیص‌دهنده، به صورت $r_d = (D - r_s)$، تنظیم می‌شود، جایی که D، فاصله بین مراکز تشخیص‌دهنده کاندید و نزدیکترین نقطه خودی و r_d، شعاع مجتمع شده با تغییر اجازه داده شده از یک نقطه خودی است. یک تشخیص دهنده کاندید رد می شود، اگر فاصله D، کمتر از مجموع کمینه شعاع تشخیص دهنده و شعاع نقطه خودی باشد، زیرا در آن حالت، تشخیص‌دهنده، بعضی از فضاهای شامل خودی را پوشش می‌دهد. اگر مکان تشخیص‌دهنده کاندید، به یک تشخیص دهنده بالغ نزدیک باشد، شعاع تشخیص‌دهنده، به صورت ساده، به فاصله D، تنظیم می‌شود. اگر این فاصله، کمتر از کمینه شعاع مجاز تشخیص‌دهنده باشد، تشخیص‌دهنده کاندید، رد می‌شود. به علاوه، اگر تشخیص‌دهنده کاندید، با یک تشخیص دهنده بالغ، بیشتر از یک آستانه تعریف شده کاربر، همپوشانی کرد، حذف می‌شود. مقدار همپوشانی، یعنی محدوده بین ۰ و ۱، به صورت زیر محاسبه می‌شود (پارامترها در شکل ۶ مشخص شده‌اند).

$$\sigma = \left(\frac{r_d + r_d' - D}{2r_d} \right) \qquad (2)$$



شکل ٦. نمایش همپوشانی تشخیص دهنده

بعضی از تشخیص‌دهنده‌های رد شده، برای انتقال و ارزیابی دوباره، در تکرار بعدی، انتخاب می‌شوند. فرض، $d^{rej} = (c^{rej}, r_d^{rej})$، یک تشخیص‌دهنده رد شده و $d^{nearest} = (c^{nearest}, r_d^{nearest})$، نزدیکترین تشخیص‌دهنده آن (یا نقطه خودی)، باشد، در این صورت، مرکز d^{rej}، به گونه ای حرکت داده می‌شود که

$$c^{new} = c^{rej} + \alpha \frac{dir}{\|dir\|}$$

که $dir = c^{rej} - c^{nearest}$ و $\|\bullet\|$، نُرم یک بردارm بعدی را نشان می‌دهد و پارامتری است که میزان حرکت مرکز را تعیین می‌کند. نکته اینکه، یک مکان مرکز جدید، برای تشخیص دهنده حرکت داده شده، مشخص شده است، اما شعاع در تکرار بعدی، محاسبه خواهد شد و به طور مشابه، از تشخیص‌دهنده اصلی، متفاوت خواهد بود.

در هر تکرار، بعضی از تشخیص‌دهنده های بهتر برای تکثیر انتخاب می‌شوند. فرض، $d = \left(c^{old}, r_d^{old}\right)$، یک تشخیص دهنده را مشخص کند که تکثیر شده است و $d^{clone} = \left(c^{clone}, r_d^{clone}\right)$، یک تشخیص دهنده تکثیر شده را نشان دهد که مرکز آن، در فاصله r_d^{old}، از d قرار دارد. مرکز d^{clone}، به صورت زیر محاسبه می‌شود.

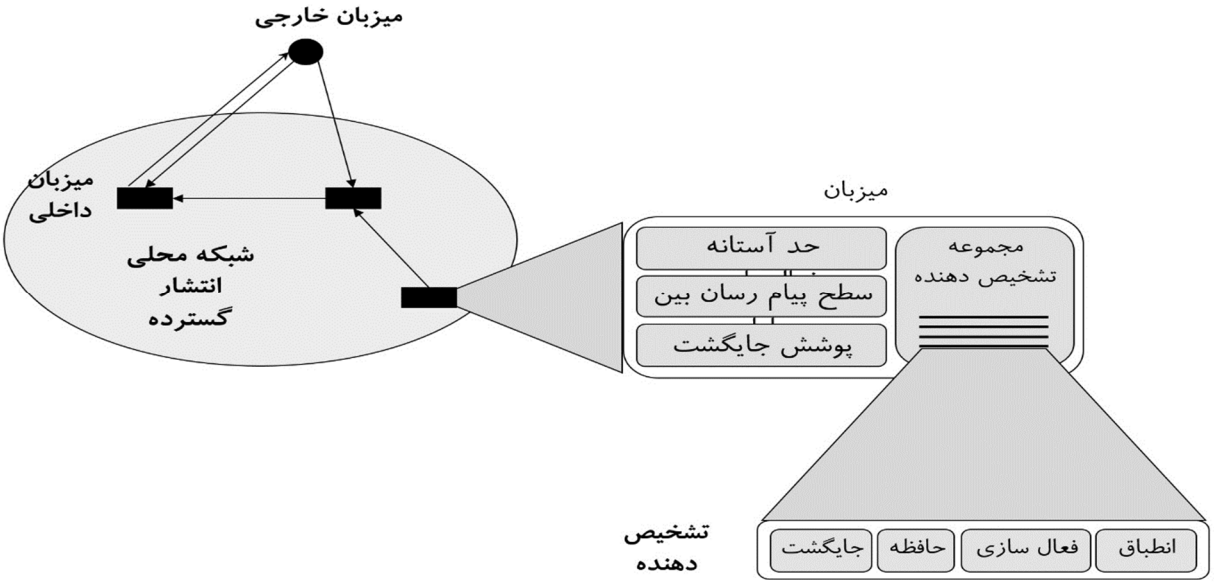
$$c^{clone} = c^{old} + r_d^{old} \frac{dir}{\|dir\|} \quad 3$$

که $dir = c^{old} - c^{rand}$ و c^{rand}، یک نقطه تصادفی در ابر مکعب واحد است. مشابه با عمل حرکت دادن، شعاع تشخیص دهنده تکثیر شده تا زمان تکرار بعدی، محاسبه نشده است و ممکن است شعاعی متفاوت از تشخیص دهنده قدیمی داشته باشد.

سرانجام، هر تکرار، بعضی مکان‌های تشخیص دهنده تصادفی برای اجازه دادن به شناسایی ناحیه‌های پوشش داده نشده از فضای غیر خودی را دارد. به طور خلاصه، بعد از تکرار اول (تنها مکان‌های تشخیص دهنده تصادفی، وجود دارند)، مجموعه مکان‌های تشخیص‌دهنده کاندید، از تولید تصادفی وحرکت دادن بعضی از تشخیص‌دهنده‌های ردشده در تکرار قبلی، همراه شده‌است. برای یک مکان تشخیص‌دهنده کاندید خاص، شعاع، به قبل محاسبه می‌شود. سپس، تشخیص‌دهنده کاندید، با یک مرکز و یک شعاع، کاملا مشخص شده است. اگر تشخیص دهنده، نقاط خودی را پوشش ندهد، اندازه مناسبی دارد و همپوشانی زیادی با تشخیص‌دهنده‌های موجود ندارد، آن مورد، نگهداری‌شده و به لیست تشخیص‌دهنده‌های بالغ، اضافه می‌شود. در غیر این صورت، رد شده و حرکت داده‌شده یا حذف می‌شود. این فرآیند تا زمانی که پوشش کافی از فضای غیر خودی، داده شود، ادامه می‌یابد.

۵. سیستم محافظ مصنوعی برای تشخیص ویروس در سیستم های اطلاعاتی

یک سیستم محافظ مصنوعی برای حفاظت یک سیستم در مقابل حمله‌های خارجی ارائه شده است که در واقع زیست شناسی طبیعی را به محاسبه نگاشت داده‌است (تیمس و همکاران، ۲۰۰۸). این طرح، در شکل ۷، نشان داده شده است:

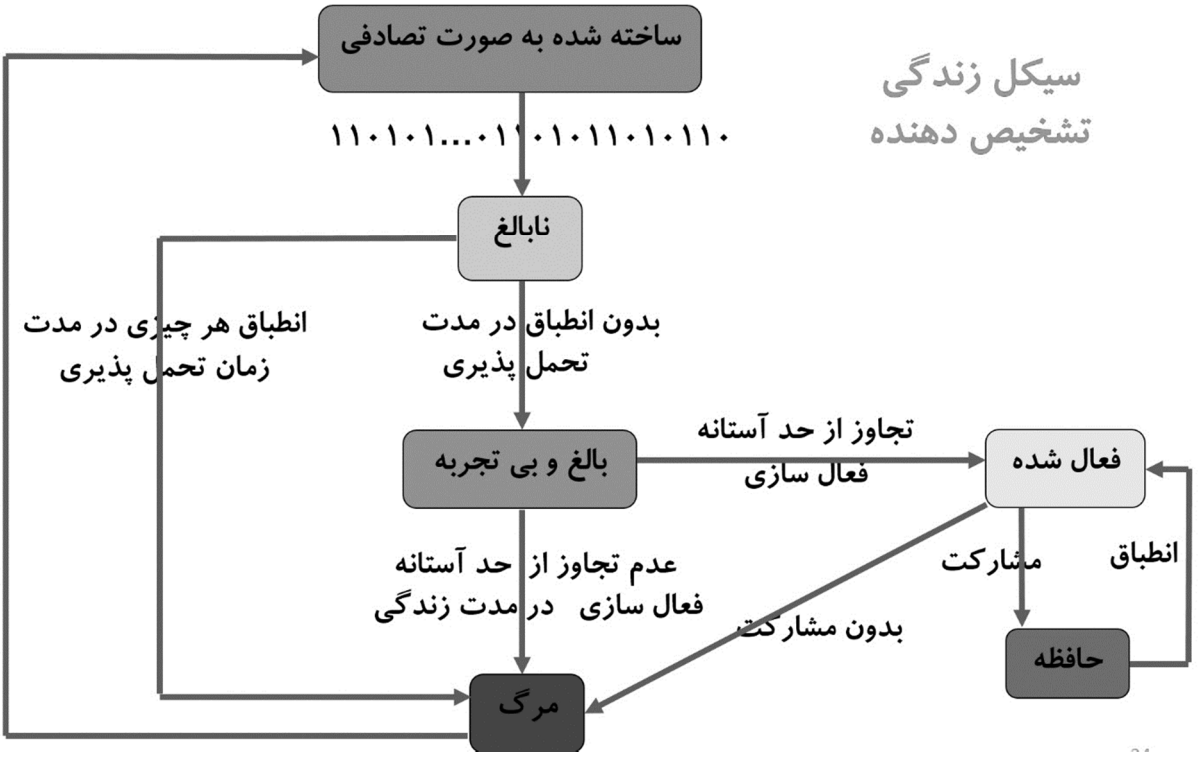


شکل ۷. معماری سیستم

در سیستم محافظ طبیعی، بسیاری از انواع مختلف سلول‌ها و مولکول‌ها مانند لنفوسیت‌ها،یاخته ها، سلول‌های کشنده طبیعی، سلول‌های درختی و بسیاری دیگر، وجود دارند. برای این سیستم محافظ مصنوعی، سیستم محافظ انتزاعی با استفاده از تنها یک نوع از انواع سلول تشخیص دهنده که خصوصیات مهم بسیاری را از سلول‌های مختلف ترکیب می‌کند و حالت‌های مختلفی دارد، کار می‌کند (اوجسکی و همکاران، ۲۰۱۹). هر سلول تشخیص‌دهنده از یک رشته بیت با طول ۴۹ بیت و از حالت‌های مختلف، تشکیل شده‌است که در شکل ۶، نشان داده شده‌است. در این ساختار، تشخیص به عنوان یک انطباق رشته، پیاده سازی شده‌است، جایی که هر تشخیص دهنده، یک رشته d است و تشخیص رشته s، هنگامی اتفاق می‌افتد که یک انطباق بین s و d، با توجه به قانون انطباق (که به عنوان مثال، می‌تواند فاصله همنیگ باشد)، وجود داشته باشد. قانون انطباق استفاده شده در اینجا، r بیت پیوسته نامیده می‌شود. این قانون می‌گوید که رشته‌های d و s، تحت r بیت پیوسته انطباق دارند، اگر d و s، نمادهایی مشابه در حداقل موقعیت‌های r بیت پیوسته داشته باشند. جایی که r، یک مقدار آستانه است و تشخیص‌دهنده‌ای را که نشانه‌ای از تعداد رشته‌های پوشش داده شده توسط یک تشخیص دهنده است را تعیین می‌کند. به عنوان مثال، اگر مقدار r مساوی با طول تشخیص‌دهنده باشد، فقط یک رشته، یعنی خودش را انطباق می‌دهد؛ بنابراین، نتیجه یک قانون انطباق این است که یک مصالحه بین تعداد تشخیص‌دهنده‌های استفاده شده و مشخصات آنها وجود دارد؛ بنابراین، اگر تعداد تشخیص دهنده‌های مشخص شده افزایش یابد، تعداد تشخیص‌دهنده های مورد نیاز برای پوشش دادن یک سطح مشخص از تشخیص نیز افرایش می‌یابد.

سیکل زندگی تشخیص‌دهنده:

تشخیص‌دهنده‌ها در گروه‌هایی طبقه بندی می‌شوند که مجموعه‌های تشخیص‌دهنده نامیده می‌شوند و در هر مجموعه، تشخیص دهنده‌های جدید به صورت غیر همزمان و تصادفی، مشابه با سیستم طبیعی، تولید می‌شوند. همانطور که شکل ۸ نشان می‌دهد، تشخیص دهنده‌های جدید تولید شده، باید از طریق یک انتخاب منفی بروند. تنها تشخیص دهنده‌هایی که انتخاب منفی را زنده نگه می‌دارند. تشخیص دهنده‌های نابالغ برای زمان مشخصی به نام پریود تحمل، حضور دارند. بعد از اینکه تشخیص‌دهنده از این زمان عبور کرد، یعنی با تعداد کافی از بسته‌های غیر خودی انطباق می‌دهد، تبدیل به یک تشخیص‌دهنده فعال شده و برای یک طول عمر متناهی وجود خواهد داشت، مگر اینکه آن با یک تشخیص دهنده جدید جایگزین شود. بعد از این طول عمر، اگر آستانه انطباق خود را عبور کرده باشد، یک تشخیص‌دهنده حافظه می‌شود، اگر اینگونه نباشد، حذف شده و جایگزین می شود.



شکل ۸. طول عمر تشخیص دهنده

مکانیزم‌های یادگیری

یکی از انواع مکانیزم‌های یادگیری، تولید مثل است. در ساده‌ترین شکل، تشخیص دهنده‌ها در مقابل یکدیگر برای بسته‌های غیر خودی رقابت می‌کنند (شیورز و همکاران، ۲۰۱۹)؛ بنابراین، اگر دو تشخیص دهنده به طور همزمان، بسته مشابهی را انطباق دهند، تشخیص‌دهنده با نزدیکترین انطباق، برنده می‌شود. در این راه، فشار بیشتری برای تمایز دقیق‌تر بین خودی و غیر خودی وجود دارد که باید از عکس العمل‌های محافظ اتوماتیک، اجتناب شود. تشخیص‌دهنده‌هایی که موفق هستند، خودشان را تکثیر می‌کنند.

یک مسأله در چنین سیستم محافظی، احتمال الارم‌های نادرست است که سیگنال‌های دوم استفاده شده، نامیده می‌شود. آنها همچنین، به روشی که لنفوسیت‌های کمک‌کننده T وجود دارند، در سیستم محافظ طبیعی وجود دارند. هنگامی که یک لنفوسیت B، یک سیگنال اول را اسیر می‌کند، یک سلول کمک کننده T، برای تحریک یک پاسخ محافظ لازم است که لنفوسیت‌های B را از عمل در مقابل خودشان، جلوگیری کند.

٦. بحث و نتیجه‌گیری

سیستم محافظ طبیعی، قابلیت‌های پردازش اطلاعات قدرتمندی دارد، با توجه به ماهیت توزیع شده حافظه آن، خود تحمل پذیری و مکانیزم‌های کنترل غیر متمرکز از دید اطلاعاتی و ساختن مدل‌های محاسباتی، می‌تواند بسیاری از مسائل علمی و مهندسی را بهتر حل کند. سیستم محافظ مصنوعی با اقتباس از سیستم محافظ طبیعی و تحلیل دقیق راهکارهای آن به وجود آمده است. الگوریتم انتخاب منفی، یک فرآیند مجزا در مقایسه با دیگر الگوریتم‌ها است و برای کاربردهای خاصی، بسیار مناسب است، البته الگوریتم انتخاب منفی برای استفاده به عنوان یک روش طبقه بندی عمومی،مناسب نیست، زیرا آنها

راهکار یک کلاس هستند. به هر حال الگوریتم انتخاب منفی می‌تواند برای تولید نمونه‌هایی برای کلاس زیر نمایش داده شده (یک کلاس با نمونه‌های کم) استفاده شود. جنبه هایی که باید به منظور ساختن سیستم محاف مصنوعی به عنوان یک تکنیک حل مسأله جهان واقعی، باید مورد توجه قرار گیرند، شامل بهبود در کارایی الگوریتم‌ها، پیشرفت در نمایش و معرفی دیگر مکانیزم‌های محافظ هستند.

هنگامی که یک مجموعه غیر همپوشان از تشخیص دهنده‌ها با یک آستانه انطباق مناسب تولید شدند، هر تشخیص‌دهنده می‌تواند به عنوان یک کلاس الگوی جدید در فضای غیر خودی خدمت کند. به هر حال در حالت تشخیص دهنده‌های همپوشان، تشخیص دهنده‌های چندگانه ممکن است برای یک الگوی نمونه (غیر نرمال) فعال شوند و نیاز به تشخیص دهنده‌های بیشتر برای فراهم کردن پوشش کافی در فضای غیر خودی داشته باشند. راه‌های ممکن زیادی برای تولید تشخیص‌دهنده‌ها در فضای غیرخودی، وجود دارد. این راهکارها، معمولا پیچیدگی‌های محاسباتی مختلف دارند و پیچیدگی آنها بستگی به انتخاب قانون انطباق دارد. در توصیف اولیه الگوریتم انتخاب منفی، تشخیص دهنده‌های کاندید به صورت تصادفی تولید شده و سپس تست می شوند تا مشخص شود که با هیچ رشته خودی، انطباق نداده باشند. اگر یک انطباق پیدا شود، کاندید حذف می‌شود. این فرآیند تا زمانی تکرار می شود که تعداد مطلوب از تشخیص دهنده‌ها تولید شده باشند.

با توجه به توانایی بسیار بالای سیستم محافظ مصنوعی و عملکرد حفاظت انطباقی در تامین امنیت سیستم‌ها و جلوگیری از ورود بدون اجازه عوامل مختلف خارجی مانند ویروس‌ها و همچنین دارا بودن الگوریتم‌های بسیار کارآمد از قبیل حفاظت تطبیقی، توانایی یادگیری رو به رشد و بهبود تشخیص عوامل خارجی می توان از سیستم‌های محافظ مصنوعی در حفظ امنیت سیستم‌های اطلاعاتی مدیریت و حسابداری استفاده کرد، زیرا این سیستم‌ها دارای اطلاعات بسیار زیادی هستند که به طور لحظه‌ای افزایش می‌یابد و از دقت و حساسیت بالایی برخوردار هستند و کوچکترین ایراد یا خطایی در صورت حمله عوامل خارجی می‌تواند آسیب جبران ناپذیری به کل سیستم وارد کند.

۷. منابع و مآخذ

1. Dasgupta, D. (2006). *Advances in Artificial Immune Systems*. IEEE Computational Intelligence Magazine, Volume: 1, Issue: 4.
2. Timmis, J., Knight, L.N. de Castro., & Hart, E. (2014). *An Overview of Artificial Immune Systems*.
3. Bachmayer, S. (2007). *Artificial Immune Systems*. Department of Computer Science, Gustaf Haellstroemin Katu Finland, University of Helsinki.
4. Tschudin, C. (2006). *Self-Protection and Artificial Immune System*. Autonomic Computer System, Computer Science Department, University of Basel.
5. Johnson, C. (2007). *Introduction to Intelligent Systems-Artificial Immune Systems*.
6. Aickelin, U., & Cayzer, S. (2002). *The Danger Theory and Its Application to Artificial Immune Systems*. Proceedings of the 1st Internal Conference on Artificial Immune Systems (ICARIS-2002), PP 141-148, Canterbury, UK.
7. Timmis, J., & Knight, T. (2008). *Artificial Immune Systems-Using the Immune Systems as Inspiration for Data Mining*. University of Kent at Canterbury, UK.
8. Dasgupta, D., & Forrest, S. (2002). *Artificial Immune Systems in Industrial Applications*. Proceedings of the Second International Conference on Intelligent Processing and Manufacturing of Materials.

9. Shivers, M., Llanes, C., & Sherman, M. (2019). *Implementation of an Artificial Immune System to Mitigate Cybersecurity Threats in Unmanned Aerial Systems*. IEEE International Conference on Industrial Internet (ICII).
10. Jim, L. E., & Gregory, M. A. (2019). *Improvised MANET Selfish Node Detection Using Artificial Immune System based Decision Tree*. 29th International Telecommunication Networks and Applications Conference (ITNAC).
11. Sakanaka. Y., & Aubert-Kato, N. (2019). *Surrogate-Assisted Optimization of the Opt-IA Artificial Immune System Algorithm*. IEEE Symposium Series on Computational Intelligence (SSCI).
12. Oujezsky, V., Skorpil, V., & Horvath, T. (2019). *GPON Frame Analysis with Artificial Immune System*. 11th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT).

Intelligent Artificial Immune Systems to Prepair Security and Protection of Accounting Information Systems

Sajed Dadashi [*1]

Date of Receipt: 2020/04/03 Date of Issue: 2020/04/29

Abstract

The management and accounting information systems contain very important and precise data; therefore, protection of these systems and prepair security against any attacks such as viruses are necessary. Artificial Immune Systems are a subset of computational intelligence. They have high capability to increase the security of computing and information systems. As the number of data, public connections and communications are increased, protecting systems against treats becomes very important. More techniques are created to increase the reliability. The human body immune system uses a learning form to get reliable operations in presence of threats. Artificial immune systems are based on the nature immune systems. They prepare the security and reliability of information systems effectively and increase the fault tolerance.

Keyword

Management and Accounting Information System, Artificial Immune System, Immune Algorithm

1. Department of Computer Engineering, Roudsar and Amlash Branch, Islamic Azad University, Roudsar, Iran ([*]Corresponding Author: sajed. dadashi@gmail.com).