مطالعات علوم کاربردی در مهندسی

دوره ۲، شماره ۳، پاییز ۱۳۹۵

صفحات ۸۸- ۹۸

Online ISSN: ٢٤٧٦-٤٥٠٧

Print ISSN: ٢٥٣٨-٢٠٥٥

www.irijournals.com

استفاده از سیستم تکاملی ایمنی مصنوعی برای امنیت شبکه‌های کامپیوتری

مجید جان نثاری لادانی[۱]، فاطمه خانی [۲]، محمدتقی فندهاری[۳]، محمد باقری دستگردی [۴]

[۱] عضو هیات علمی دانشگاه پیام نور، دانشگاه پیام نور دولت آباد، اصفهان، ایران
[۲] عضو هیات علمی دانشگاه پیام نور، دانشگاه پیام نور دولت آباد، اصفهان، ایران
[۳] عضو هیات علمی دانشگاه پیام نور، دانشگاه پیام نور دولت آباد، اصفهان، ایران
[۴] کارمند فولاد مبارکه سپاهان، فولاد، اصفهان، ایران

چکیده

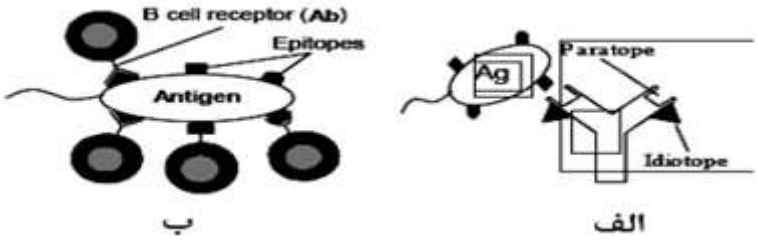
سیستم ایمنی بدن، یک سیستم محاسباتی جالب و کارا برای بسیاری از کاربردها در زمینه مهندسی وبخصوص تشخیص نفوذ است این سیستم دفاعی بر اساس عامل، بصورت توزیع شده و خود تطبیق است که بر اساس یک معماری لایه ای و سلسله مراتبی عمل می کند. در این مقاله ابتدا عناصرمعماری سیستم های های تشخیص ویروس که شامل چهار قسمت تبدیل داده، ایجاد و تشخیص ویروس و شناسایی سلول های حافظه می باشد با تمرکز بر عناصر شبکه‌های کامپیوتری بیان شده است. سپس چند نمونه سیستم ایمنی مصنوعی برای امنیت شبکه را مورد بررسی قرار داده ایم... از جمله سیستم ایمنی فورست که فقط ترافیک TCP/IP را در یک شبکه محلی مانیتور میکند. در انتها با توجه به ویژگی های الگوریتم های هوش محاسباتی نتیجه گیری و پیشنهاداتی برای استفاده موثر از این الگوریتم ها بیان شده اند.

واژه‌های کلیدی: سیستم تکاملی ایمنی مصنوعی، امنیت شبکه، ایمنی مصنوعی فازی

دوره ۲، شماره ۳، پاییز ۱۳۹۵، صفحات ۸۸- ۹۸

مقدمه

مهمترین هدف سیستم ایمنی بدن انسان حفاظت در مقابل عوامل بیرونی میکروب ها و ویروسهای بیماری زا است. ایمنی، از سلول ها مولکول ها و قوانینی تشکیل شده است که از اسیب رساندن عواملی همچون پاتوژن ها به بدن میزبان جلو گیری میکند. قسمتی از پاتوژن به نام انتی ژن توسط این سیستم قابل شناسایی است و موجب فعال شدن پاسخ سیستم ایمنی خواهد شد یک نمونه از پاسخ سیستم ایمنی میتوان ترشح انتی بادی توسط سلول های b و یا لنفوست های b باشد. انتی بادی ها مولکول های شناساگری به شکل yکه به سطح سلول های b متصل هستند و با قوانینی از پیش تعریف شده انتی ژن ها را شناسایی مینمایند و بهه ان ها متصل میشوند. مولکول های انتی بادی قسمتی از انتی ژن را به نام اپیتوپ شناسایی مینمایند. ناحیه ای از انتی بادی که وظیفه شناسایی و اتصال به انتی ژن را دارد پاراتوپ نامیده میشود. ایدوتایپ نیز مجموعه ای از ایدوتوپ است (همانند اپیتوپ است) که در سطح متغییر شکل انتی بادی قرار دارد. هر سلول b فقط توانایی تولید یک نوع انتی بادی را داراست به همین دلیل monospecific خوانده میشود اما هر انتی ژن چندین نوع گونه مختلف اپیتوپ دارد که موجب میشود چندین انتی بادی مختلف ان را شناسایی کنند. پاراتوپ با نام ناحیه vنیز شناخته میشود و به منظور ایجاد بیشترین تطابق با انتی ژن دها میتواند شکل خود را تغییردهد و به همین دلیل از ان به ناحیه متغیر نیز نام میبرند. میزان تعامل بین انتی بادی و انتی ژن ها با میزان تطابق و میزان شباهت در ناحیه داتصال بین ان ها سنجیده میشود شکل ۱ انتی ژن ها با چندین اپی توپ و انتی بادی را پاراتوپ و ایدوتوپش به تصویر کشیده شده است.



شکل۱: الف- سلول B، آنتی بادی، آنتی ژن، اپیتوپ، پاراتوپ و ایدوتوپ. ب- آنتی بادی و اتصال با آنتی ژن

سیستم ایمنی برای داشتن عملکردی صحیح باید بتواند بین سلول های خودی و سلول های بیگانه خارجی و غیر خودی تمایز قائل شود این پروسه تمایز خودی از غیر خودی نامیده میشود. ان سلول هایی که به عنوان خودی شناخته میشوند پاسخ سیستم ایمنی را فعال نمی کنند در حالی که دیگر سلول باعث تحریک پاسخ سیستم ایمنی خواهند شد. پس از ورود پاتوژن ان دسته از سلول های ایمنی که پاتوژن را شناسایی میکنند شروع به تولید و تکثیر مینمایند از بین سلول های شناساگر تولید شده دسته ای به عنوان سلول های حافظه انتخاب و نگه داری میشود تا در برخورد های بعدی با پاتوژن های همانند و یا با ساختاری مشابه پاسخ سریعتر و قویتر سییستم ایمنی ایجاد میشود.

تشخیص نفوذ، فرایند پیدا کردن بسته ها و برنامه های مخرب در شبکه‌های کامپیوتری است. عبارت ویروس های کامپیوتری اغلب برای کد های ناخواسته و فعالیت های نادرست در کامپیوتر میزبان به کار میرود. این خاصیت شبیه سیستم

ایمنی بدن است که بدن مارا شبیه عوامل بیماری زای خارجی محافظت میکند. خصیصه های سیستم ایمنی بدن که میتوان از ان در امنیت شبکه‌های کامپیوتری بهره برد عبارتند از:

۱- قابلیت یادگیری
۲- تنظیم تعداد سلول های ایمنی توسط سیستم ایمنی

۳- قابلیت تشخیص الگو توسط انتی بادی ها: این تشخیص الگو با استفاده از یک سطح استانه انجام میگیرد بدین صورت که هر گاه تحریک الگوی نفوذی از یک سطح استانه ای فراتر رفت ان به عنوان یک غیر خودی یا عامل مخرب تشخیص داده میشود

۴- تنوع و گوناگونی

۵- همکاری گروهی بین سلول ها

و ...

معماری

نگاهی کلی به سیستم

سیستم های تشخیص ویروس شامل چهار قسمت می شوند

۱- تبدیل داده ها

۲- ایجاد و پرورش تشخیص دهنده ها

۳- تشخیص ویروس

۴- شناسایی سلول های حافظه

در هر مرحله مفاهیم کم وزنی از سیستم های ایمنی طبیعی مورد استفاده قرارر گرفته است که به صورت زیر پیاده سازی می شوند.

۱- سلول های حافظه: یک ردیاب یا تشخیص دهنده در هنگام رویارویی یا عامل مخرب اطلاعات مربوطه را ذخیره می کند و باعث می شود در مواجهه بعدی سریعتر عمل کند این ذخیره سازی به عنوان سلول حافظه در نظر گرفته می شود

۲- ارائه ژن ها: تنوع بین ساختار تشخیص دهنده ها که از ترکیب تعداد زیادی از سلول های حافظه ایجاد می شود باعث افزایش کارایی انها می شود

البته قابل ذکر است که مفهوم ژن ها در فاز تست تشخیص دهنده ها و سلول های حافظه در قسمت شناسایی عامل مخرب مورد استفاده قرار می گیرد.

تبدیل داده ها

سیستمهای تشخیص دو نوع از مجموع داده ها را مورد استفاده قرار می دهند که شامل داده های خودی وغیرخودی یا مخرب می باشد داده ها از مجموع داده های DRAPAگرفته می شود (از مجموع داده های استاندهارد در ازمایشگاه لینکن انگلستان می باشد)

در تبدیل فیلد های مربوطه که باید در نظر گرفته شود به صورت زیر می باشد:

۱- Ip ادرس مقصد.

۲- Ip ادرس مبدا

۳- شماره پورت مقصد

۴- طول

۵- پروتکل

۶- شماره پورت مبدا

در خواست در ابتدا به صورت رشته ای دودویی که طول ان به صورت کلی ۱۳۴ بیت می باشد و با احتساب فیلد های ذکر شده تبدیل می شود و در عین حال اگر نیاز به نگاشت صفر باشد اینکار صورت میپذیرد. البته مقدار بیشینه و کمینه هر فیلد در جدول ۱ ذکر شده است.

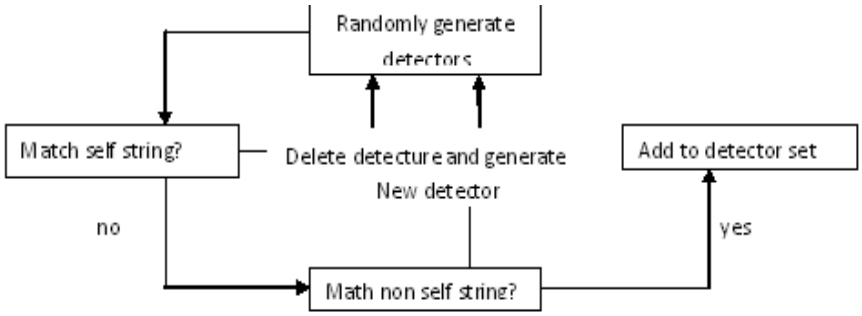
جدول ۱. مقدار بیشینه و کمینه

نا م فیلد ها	رشته (دودویی) طول	مقدار بیشینه و کمینه
Ip ادرس مقصد	38 bits	0.0.0.0-255.255.255.255
Ip ادرس مبدا	38 bits	0.0.0.0-255.255.255.255
شماره پورت مقصد	16 bits	0-65535
طول	10 bits	0-999 seconds
پروتکل	16 bits	0-65535
شماره پورت مبدا	16 bits	0-65535

تولید تشخیص دهنده ها

همانطور که ذکر شد تشخیص دهنده ها به عنوان مجموعه ای از رشته ها در نظر گرفته می شوند این رشته ها به صورت تصادفی تولید شده و برای شناخت تفاوت بین عوامل خودی و عوامل مخرب یا غیر خودی گسترش و پرورش می یابندپرورش و توسعه با استفاده از الگوریتم negative selection صورت می پذیردو به منظور تصحیح ساختار مجموعه تشخیص دهنده ها در مقابل عوامل مخرب و خودی می باشد. البته رویه انجام این کار در شکل ۲ نمایش داده شده است. این رویه از اختلاف تطابق الگویی استفاده می کند و به r-Contiguousتلقی می شود. در این رویه در واقع هر ردیاب پس از تطابق در صورت مشابهت با عوامل خودی ردیاب مربوطه حذف شده و ردیاب جدیدی جا یگزین می شود. در پایان خروجی ردیابی خواهد بود که با استفاده از همان الگوریتم گسترش پیدا خواهد کرد.

دوره ۲، شماره ۳، پاییز ۱۳۹۵، صفحات ۸۸- ۹۸



شکل ۲: تولید تشخیص دهنده ها

میزان سازگاری ردیابها توسط تعداد بیت تطابق یافته مشخص می شود و در طول این چرخه نیز مقدار به هم پیوستگی تشخیص دهنده ها و بیت های عوامل مخرب شناسایی می شود. و سرانجام وقتی تشخیص دهنده برای رویارویی با عومل مخرب اماده شد به شکل یک تشخیص دهنده کامل در می اید جز ردیاب هایی که مجددا تغییر میکنند نخواهد بود.

تشخیص عوامل مخرب (ویروس ها)

وقتی که تولید و پرورش تشخیص دهنده ها کامل شد انگاه برای رویارویی با عوامل مخرب اماده هستند در هنگام روبرو شدن با یک در خواست بیرونی یا عوامل مخرب سیستم مقدار سازگاری را مورد ارزیابی قرارمی دهدتا مخرب یا غیر مخرب بودنان را مشخص نماید. در صورتی که مقدار سازگاری یا تطابق بالا باشد انگاه به احتمال بسیار زیاد درخواستی از طرف دشمن است

اگر یک تطابق در ۱۳ منطقه به هم پیوسته یه وجود بیاید ان را به عنوان یک اصابت در نظر گرفته و ان منطقه به عنوان منطقه ویژه تلقی می شود اما سیستم زمانی فعال خواهد که فقط ۳ یا تعداد بیشتری از خواهر های تشخیص دهنده توسط

درخواست فعال شده باشد بنابراین درخواستی که در ۱۳ منطقه همجوار با ۳ یا تعدادبیشتری تشخیص دهنده منطبق شود به عنوان درخواست دشمن تلقی می شود.

شناسایی سلول حافظه

خاصیت انطباقی و تکاملی مربوط به الگوریتم ژنتیک برای فعال کردن تعداد بیشتری از خواهر های تشخیص دهنده ها در هنگام روبرویی با عامل مخرب مورد استفاده قرار می گیرد از این الگوریتم عملگرهای selection,cloning,crossover,mutation مورد استفاده قرار می گیرد. زمانی که یک عامل مخرب شروع به فعالیت می کند خواهر های ردیاب به عنوان شاخه ای از مجموعه تشخیص دهنده های فعال، فعال می شوندکه کاندیدی برای سلول های اساسی خواهند بود. پس از ان ردیاب هایی که یاید کلون شوند مشخص می شوند البته استانه تکثیر توسط فرمول زیر مشخص میشود:

تعداد کل ردیا بها /تعداد ردیاب های سازگار =استانه تکثیر

همانطور که می دانید ردیابهای فعال دارای مقدار سازگاری می باشندکه این مقدار بزرگتر یا برابر مقدار استانه تکثیر مربوط به تکثیر های تغییر یافته می باشد تعداد تکثیر که باید برای ردیاب های کاندید ایجاد شود از فرمول زیر بدست می اید:

[کل مقادیر سازگاری/مقدار سازگاری*۱۰]=تعداد تکثیر

دوره ۲، شماره ۳، پاییز ۱۳۹۵، صفحات ۸۸- ۹۸

وقتی که فرایند تکثیری کامل شد، تشخیص دهنده های باقیمانده به عنوان ردیاب های برنده تلقی می شوند

البته قرار دادن ردیاب های برنده در عملگر جهش و پیوند الگوریتم ژنتیک در تکامل انها کمک خواهند کرد. پس از ایجاد شماره اساسی ردیاب هایی که مقدار سازگاری انها از تمامی ردیا بهای برنده بیشتر باشد به عنوان سلول حافظه تلقی می شوند.

برخی سیستمهای ایمنی مصنوعی برای امنیت شبکه‌های کامپیوتری

سیستم ایمنی فورست:

این سیستم ایمنی که در پروژه (lisys) ارایه شده ترافیک (tcp/ip) را در یک شبکه محلی مانیتور میکند. ارتباط بین تمام پروتکل ها از طریق tcp است این ارتباط از طریق سه تایی: آدرس مبدا ومقصد وسرویس شبکه تعریف می شود. این سیستم به جریان ترافیکی کاری ندارد وتنها بسته های از نوع (tcpsyn) را مانیتور می کند در اینجا هر آنتی بادی یک چرخه حیات دارد وبر اساس انتخاب منفی کار می کند. بدین صورت که تمام عامل های خودی در ابتدا به آنتی بادی ارایه می شودو در صورتی که این آنتی بادی با یکی از آنها منطبق شود از بین میرود در این سیستم نشان داده شده است که هفت حمله معمول و شایع

که در سیتم اتفاق می افتد با کمتر از صد رشته بیتی تشخیص دهنده با طول چهل ونه بیت کشف می شود در این سیستم ایمنی عملیات ها در دو فاز انجام می شود: فاز آموزش و فاز تست (هارمر، ۲۰۰۰).

فاز آموزش:

در فاز آموزش تنها یکسری شناسنده ساخته می شوند و در بین میزبان های شبکه قرار می گیرند. الگوریتم تولید آنتی بادی در مرحله آموزش در این سیتم به صورت زیر است:

۱- تولید آنتی بادی به طور تصادفی:

این آنتی بادی ها آنتی بادی خام هستند که در مرحله اول به اندازه کافی و به تعداد مشخص تولید می شوند. با تولید هر آنتی بادی خام یک زمان سنج به آن تعلق می گیرد که در ابتدا مقدار آن صفر است.

۲- انتخاب منفی:

این عمل با استفاده از داده های آموزشی انجام می گیرد. داده های آموزشی همان مجموعه خودی ها هستند در صورتی که هر آنتی بادی خام با رشته ورودی خودی از داده های آموزشی انطباق حاصل کند آن آنتی بادی حذف می شود در غیر این صورت

به زمان سنج آن اضافه می گردد. اکر زمان سنج به یک حد قابل قبول رسیده باشد آنتی بادی خام تبدیل به آنتی بادی با تجربه می شود. برای هر آنتی بادی با تجربه یک زمان حیات در نظر گرفته می شود.

فازتست:

در این قسمت مرحله اصلی الگوریتم انجام می شود و غیر خودی ها شناسایی می گردند. الگوریتم شناسایی آنتی ژن ها و حملات و حیات هر آنتی بادی در این قسمت مشخص می شود. این الگوریتم به صورت زیر خلاصه می گردد:

۱-رشته ها از یک فایل ورودی تست به تربیتوارد می شوند.
۲-هر رشته ی ورودی به آنتی بادی های باتجربه تولید شده از مرحله آموزش ارایه می گردد و با آن مقایسه می شود

دوره ۲، شماره ۳، پاییز ۱۳۹۵، صفحات ۸۸- ۹۸

۱-۲-اگر رشته ورودی با آنتی بادی با تجربه انطباق حاصل کرد ویا به عبارتی شناسایی گردید. رشته ورودی به عنوان یک رشته غیر خودی تلقی می شود و آلارم ایجاد می گرددوبه کاربر هشدار داده می شود. به زمان حیات آن آنتی بادی نیز اضافه می گردد.

۲-۲-اگر رشته ورودی با آنتی بادی با تجربه انطباق حاصل نکرد از زمان حیات آنتی بادی با تجربه کم می شود بعد از این حالت این آنتی بادی با تجربه ای که زمان حیات آن سپری شده باشد حذف می شود و میمیرد.

۳-هر رشته ورودی آنتی بادی های خام موجود ارایه می گردد و با آن مقایسه می شود

۱-۳-اگر رشته ورودی با آنتی بادی خام انطباق حاصل کرد آنتی بادی خام حذف می گرددو دوباره یک آنتی بادی خام با زمان ستج صفر ایجاد می شود.

۲-۳-اگر رشته ی ورودی با آنتی بادی خام انطباق حاصل نکرد به زمان سنج آن اضافه می کردد بعد از آن اگر زمان سنج به حد قابل قبول رسیده بود آن آنتی بادی تبدیل به آنتی بادی با تجربه می شود.

سیستم ایمنی مصنوعی فازی:

این سیستم ایمنی بر اساس رشته های باینری ارایه می شود از الگوریتم های ژنتیک و فازی برای تکامل و بهبود آنتی بادی ها در سیستم استفاده میگردد. الگوریتم های ژنتیک هم چنین باعث تنوع آنتی بادی ها می شود به طوری که بر اساس انتخاب کلونی سلول هایی که آنتی ژن را تشخیص می دهند رشد کرده و سلول هایی که نمی توانند تشخیص دهند میمیرند (هارمر، ۲۰۰۲).

مشابه سیستم ایمنی فورست در سیستم ایمنی پیشنهادی نیز عملیات ها در دو فاز جداگانه آموزش و تست انجام می شوند.

در ابتدا آنتی بادی ها از یک تعداد ناحیه ژنی به طور تصادفی ساخته می شوند. مولفه های اصلی در این سیستم ایمنی یک مجموعه داده آموزشی و آنتی ژن و آنتی بادی ها و یکسری گوی تشخیص به نام (ARP) در حول هر سلول B است. هر (ARP) یک مجموعه فازی (n) بعدی می باشد. مقدار تطابق هر (ARB) با آنتی ژن با فاصله (d) نشان داده می شود. فاصله (d) مقدار تفاوت سلول (B) با آنتی ژن را نشان می دهد (یغمایی مقدم، ملکی، اکبر زاده توتونچی، ۱۳۸۴).

مقدار عضویت فازی هر آنتی ژن (j) به هر ARB(i)که با نماد w_{ij} مشخص می شود به صورت زیر به دست می آید: (۱)

$$w_{ij}=\exp(-d_{ij}^2/2\delta_i^2)$$

باتوجه به فرمول فوق شکل مجموعه فازی (ARB) یک تابع گوسی است که هر چه از مرکز (ARB) دور می شویم مقدار آن کاهش می یابد. سطح بر انگیختگی در هر (ARB) بصورت زیر بدست می آید: (۲)

$$S_i=\sum_j w_{ij}\Big/\delta_i^2$$

با ماکسیمم کردن سطح انگیزش در هر (ARB) ومشتق گیری از s خواهیم داشت (۳)

$$\delta_i^2=\frac{\sum_j d_{ij}^2 w_{ij}}{\sum_j w_{ij}}$$

دوره ۲، شماره ۳، پاییز ۱۳۹۵، صفحات ۸۸- ۹۸

در فرمول های فوقd_{ij} فاصله بین آنتی ژن j تا مرکز i(ARB و δ_i^2 شعاع گوی ARBi و S_i سطح انگیزش در هر ARBi می باشد.

نرمال سازی داده ها بر اساس شبکه ایمنی در فضای دو بعدی صورت می گیرد. در اینجا هر آنتی بادی می تواند به نسبت شعاع خود اپی توپ های آنتی ژن ها را در فضای دو بعدی تحت تاثیر قرار بدهد. چهار پارامتر مهم این سیستم عبارتند از:۱

۱- NAT یا حداکثر سطح آستانه که بین ۰ تا ۱ است.
۲- نرخ جهش (mutate)و احتمال (clone) که بین ۰ تا ۱ است.
۳- -حداکثر سطح انگیزش که بین ۰ تا ۱ است.
۴- حداکثر تعداد (clone) برای هر (ARB)

هر (ARB) یک رشته (n) بیتی است که این رشته ها در فضای دو بعدی نرمالیزه می شود به طوری که هر نقطه را در فضای دو بعدی دارد. در شکل ۱ نمایش داده هاو (ARB) در فضای دو بعدی آورده شده است.

در سیستم مورد بررسی از یک کنترلر فازی برای تصمیم گیری در تطبیق و تشخیص عامل در در عامل های آنتی بادی استفاده می شود. توابع عضویت بصورت گوسی و به عنوان یک گوی حول هر سلول (B) هستند. سلول های (B) سازنده آنتی بادی مربوطه می باشند. هر قدر رشته های کروموزوم از آنتی بادی ها دورتر باشد از مرکز (ARB) یا گوی تشخیص دورترند و آنتی بادی انگیزش کمتری برای تکثیر و تاثیر روی آن دارد. (ARB) ها به صورت حافظه دینامیک از سلول های (B) عمل می کنند این (ARB) ها می توانند به خوبی به روز آوری شوند واطلاعات گذشته را نیز به خوبی نگهداری کنند.

الگوریتم های ارایه شده عمل خوشه سازی داده های آموزشی یا داده های خودی را انجام می دهند و با توجه به آن آنتی بادی ها را می سازند. الگوریتم های ارایه شده دارای ساختار و مراحلی مشخص می باشند که در ادامه آورده شده است. این الگوریتم ها اجزای اصلی سیستم ایمنی هوشمند پیشنهادی را که بر مبنای سیستم ایمنی بدن طراحی شده است تشکیل می دهند.

فاز آموزش:

الگوریتم ارایه شده در قسمت فاز آموزش برای تولید یکسری آنتی بادی استفاده می شود. این الگوریتم خوشه سازی مجموعه خودی ها را به عهده دارد و بر اساس آن یکسری داده های آموزشی خودی انجام می گیرد. الگوریتم تولید آنتی بادی ها در سیستم مذکور به صورت زیر است:

۱-تولید جمعیت اولیه باینری بصورت تصادفی از (ARB) ها: به تعداد مشخص شده (ARB) اولیه تولید می شود که در ابتدا شعاع آن 0.1 است و تعداد سلول های (B) و شعاع هر (ARB) قدرت آن را در شناسایی آنتی ژن ها را نشان می دهند.

۲-مجموع خودی به سیستم ارایه می شود و تا زمان خاتمه وضعیت مراحل زیر انجام می شود:

۲-۱ رشته های خودی به هر (ARB) ارایه میشودو تابع هدف هر یک بدست می آید.

۲-۲-برای هر (ARB) موجود در شبکه مراحل زیر انجام می شود:

۲-۲-۱-سطح انگیزش (تابع هدف) در هر (ARB) محاسبه می شود.

۲-۲-۲ شعاع هر (ARB) محاسبه مجدد می شود.

۲-۳-برای هر (ARB) بر طبق سطح انگیزش بدست آمده برای آن سلول B(اختصاص می یابد...

۲-۴ (ARB) های ضعیف که هیچ سلولB(را شامل نیستند حذف می گردند.

۲-۵ عملیات های (clone) و ((mutate روی (ARB) ها انجام می شود.

۲-۶ مجموعه جمعیت (ARB) ها به صورت بهینه ویکپارچه می شوند:

۲-۶-۱-هر دو (ARB) ای که بسیار بهم نزدیک هستند و فاصله آن ها از هم بسیار کم است یا گوی ها با هم همپوشانی دارند آن دو (ARB) در هم ادغام می شوند ونتیجتا (ARB) جدیدی بدست می آید برابر با (cross-over) دو (ARB) قبلی.

۳-پایان

در این الگوریتم میزان انطباق یا نزدیکی بین ها (ARB) با داده ها و با دیگر (ARB) ها با فاصله اقلیدسی بین آن ها در فضای دو بعدی بدست می آید اگر دو با هم پوشانی یا تو رفتگی داشته باشد(یعنی :δi+δj<darbi آن ها را با عملیات crossover به یک ARB تبدیل می کنیم که با انجام عملیات درARB جدید داریم.

(۴)

$$\delta=(\delta+\delta)/2\alpha=(\alpha\delta+\alpha\delta)/(\alpha\delta+\alpha\delta)$$

در اینجا عملیات تکثیر یا cloneدر هر ARBبا جهش یا mutateانجام می شود و شعاعا نیز به ارث برده می شود.

فاز تست

در این فاز مرحله اصلی الگوریتم انجام می شود و حملات شناسایی می شوند شناسایی حملات به وسیله کنترلر فازی انجام می گیرد توابع عضویت در اینجا به صورت گوسی هستند هر چه قدر یک انتب بادی از یک رشته کروموزم دورتر باشد انتی بادی تاثیر کمتری روی ان دارد و برعکس. فاصله بین رشته های انتی بادی ها و کروموزم ها به مجموع طول های پیوسته یکسان در هر دو رشته محاسبه می گردد.

فرایند تصمیم گیری با یک کنترلر فازی انجام می گیرد سیستم های فازی دارای چهار ورودی و یک خروجی می باشند ورودی های کنترلر فازی چهار سیستم از مجموعه ARBدر نظر گرفته شده است. بر اساس خروجی کنترل کننده فازی وجود حمله یا عدم ان مشخص می شود.

هر سیستم انتی بادی های مربوط به خود را برای شناسایی دارد در این سیستم با در نظر گرفتن قابلیت های سیستم ایمنی در شناسایی غیر خودی ها از کنترلر فازی برای همکاری گروهی جهت تشخیص غیر خودی ها به شبکه استفاده شده است. سطح رفتار فازی با ۴ مجموعه فازی از توابع گوسی در ۴ سری ازARB ها به طور موازی انجام می شود در اینجا هر سیستم تشخیص

فاز اموزش و فاز تست مجزایی دارد. رفتار کلی انها با کنترلر فازی بررسی میشود. رفتار هر سیستم توسط دو مجموعه فازی low,high نشان داده می شود. همچنین خروجی کنترل کننه فازی با چهارمجموعه فازی -low,high,medium low,medium-high نمایش داده می گردد.

الگوریتم شناسایی انتی ژن ها و حملات و تکامل یافتن انتی بادی ها به صورت زیر خلاصه می شود

دوره ۲، شماره ۳، پاییز ۱۳۹۵، صفحات ۸۸- ۹۸

۱- مجموعه تست به سیستم ارائه می شود و برای هر رشته ورودی مراحل زیر انجام می گیرد

۱-۱- به تعداد n رشته به هر ARBارائه می گرددو بر اساس فاصله ای که ازARB دارندمشخص می شود ایا قابل شناسایی هستند یا نه ؟لذا مراحل زیر برای هرARB موجود در شبکه انجام می شود

۱-۱-۱- فاصله رشته ورودی با هر ARB محاسبه میشود.

۱-۱-۲- تابع عضویت برای رشته های ورودی محاسبه می شود مجموع سطح انگیزش ARB ها بدست می اید. شعاع هر ARB محاسبه مجدد می شود.

۱-۱-۳- ایا خطا یا واقعه ای اتفاق افتاده است یا نه؟

۱-۲- برای هر ARB بر طبق سطح انگیزش بدست امده برای ان سلول Bاختصاص می یابد.

۱-۳- ARB های ضعیف که هیچ سلول Bرا شامل نیستند حذف می گردند

۱-۴- عملیاتهای clone,mutate روی ARB انجام میشود.

۱-۵- مجموعه جمعیت ARB به صورت زیر بهینه و یکپارچه می شوند

۱-۵-۱ - هر رو ARB ای که بسیار به هم نزدیک بودند و فاصله انها ازهم بسیار کم بوده، ان دو ARB در ها ادغام می شوند ARB جدیدی که بدست می اید برابر با crossover دو ARB قبلی.

نتیجه گیری و پیشنهادات:

با توجه به نحوه عملکرد سیستم ایمنی بدن انسان در مقابل حملات ویروس ها و تطابق بین روند عملکرد حملات احتمالی در یک شبکه کامپیوتر ی با این سیستم الگوریتم های جالب وکارایی برای امنیت شبکه‌های کامپیوتری قابل ارایه است.

بطور کلی استفاده از الگوریتم های هوش محاسباتی در ابعاد امنیتی شبکه‌های کامپیوتری کارا به نظر میرسد. البته با توجه به اینکه نحوه ی عملکرد یک الگوریتم هوش محاسباتی بسیار وابسته به نحوه ی تعریف عملگر های مورد استفاده آن الگوریتم

است مهمترین قسمت تعیین دقیق پارامتر های الگوریتم است به نحوی که الگوریتم با استفاده از این پارامتر ها بتواند به خوبی در فضای حل مسله جستجو کند و انعطاف پذیری بالایی داشته باشد. با توجه به الگوریتم های بررسی شده به پیشنهاد میشود برای اینکه تنوع پذیری الگوریتم های ایمنی مصنوعی برای شناسایی حملات مختلف در شبکه‌های کامپیوتری بیشتر شود بهتر است در مرحله تولید تشخیص دهنده ها از فیلتر ها مناسب مثل فیلتر های ماتریسی که برای تشخیص الگو مورد استفاده قرار می گیرند استفاده شود تا در مرحله تشخیص عوامل مخرب، بصورت مناسب آنها را شناسایی کنیم. هدف ما اینست که در بررسی های آینده تلفیقی از روش های شناسایی الگو با روش های هوش محاسباتی برای امنیت شبکه‌های کامپیوتری ارایه دهیم.

منابع:

۱. جواد زاده، رامین؛ میبدی، محمدرضا (۱۳۸۵). بهبود کارایی الگوریتم سیستم ایمنی مصنوعی در مسایل بهینه سازی. دوره ۲، شماره ۴. ص ۲۲-۳۶.

۲. یغمایی مقدم، محمدحسین؛ ملکی، داوود؛ اکبرزاده توتونچی، محمدرضا (۱۳۸۴). طراحی یک سیستم ایمنی مصنوعی فازی برای امنیت شبکه‌های کامپیوتری. علوم و مهندسی کامپیوتر، دوره ۳، شماره ۳(الف). ص ۱-۱۲.

3. Furnell, S. (2004). *Enemies within: the problem of insider attacks*, Computer fraud & security. Volume 2004, issue 7.

4. Hofmeyr, S.Forrest, S.andSomayaji, A. (1998). Intusion Detection Using Sequences of System Call. Journal of Computer Security, vol.6, pp.151–180.
5. P. K. Hamer, P. D. williams, G. h. Gunsch and B. Lamont (2002). An Artificial Immune System Architecture for Computer security Applications, IEEE Transaction on Evolutionary Computation.
6. P. K. Harmer (2000). A distributed agent architecture for a computer virus immune system, M.S. thesis, Air Force Inst. Technol., Wright-Patterson-AFB, OH.
7. Rajesh,S.khurana (1999). NOMAD: Traffic-based Network Monitoring Framework for Anomaly Detection. Proceeding IEEE International Symposium on computers and communications, pp.442-451.