کاربرد سیستم ایمنی مصنوعی در مهندسی فن آوری اطلاعات

علیرضا نقش، الهه شکل آبادی، سارا عباس نژاد، بهناز گودرزی

شرکت سهامی ذوب آهن اصفهان ،دانشگاه آزاد اسلامی واحد نجف آباد، دانشگاه شهرکرد

E-mail: naghsh_@yahoo.com

چکیده - سیستم ایمنی بدن موجودات بسیار گسترده ،سازگار و خودسازمان یافته است برخوردهای قبلی را در حافظه نگه می دارد و توانایی یادگیری برخوردهای جدید را به طور دائمی داراست . آلگوریتم سیستم ایمنی مصنوعی حول این مفهوم توسعه یافته است . یک سیستم ایمنی مصنوعی می تواندبسیاری از ویژگی های کاربردی سیستم ایمنی طبیعی از جمله تنوع ، مقاومت در مقابل خطا ، یادگیری پویا وتطابق پذیری را ترکیب نمایند و از آن در سیستمهای مهندسی از جمله پردازنده ها و سیستمهای حفاظت و امنیت اطلاعات استفاده کند .این الگوریتم ها بسیاری از امور پیچیده مهندسی را میسر کرده اند که در این مقاله به بررسی آن پرداخته ایم .

کلید واژه- سیستم ایمنی مصنوعی ، فن آوری اطلاعات ، الگوریتم ژنتیک ، شبکه عصبی مصنوعی

۱- مقدمه

بدن انسان درمقابل مهاجم های خارجی به وسیله یک سیستم چند متغیره حفاظت شده است این سیستم ایمنی از موانع فیزیکی از قبیل پوست وسیستم تنفسی ، موانع شیمیایی از قبیل آنزیم های مخرب و اسیدهای معده وحتی سیستمهای بسیار پیچیده داخلی تشکیل شده است .

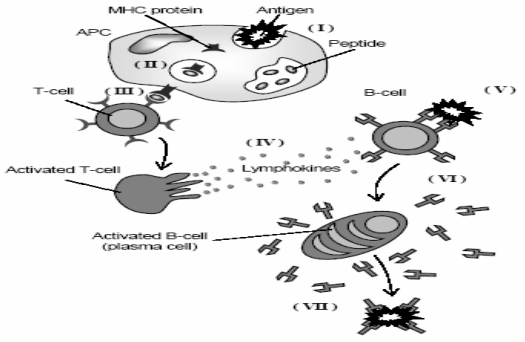
سیستم ایمنی بدن موجودات, یک سیستم دفاعی استادانه میباشد و بیش از میلیونها سال است که تکامل پیدا کرده و هنوز بسیاری از جزئیات و مکانیزم های آن حتی برای متخصصین ایمنی شناسی ناشناخته اند.بسته به نوع و نحوه ی رسیدن عامل خارجی وارد شده به بدن سیستم ایمنی از مکانیزمهای متفاوتی استفاده می کند.به عنوان مثال ایمنی ذاتی که توانایی محدود در تشخیص انواع میکرب ها و دفاع در مقابل آنها است.برخلاف ایمنی ذاتی مکانیسم های دفاعی تکامل یافته تری وجود دارند که بعد از برخورد با عوامل عفونی تحریک میشوند و شدت و قدرت دفاعی آنها بعد از هر بار برخورد با یک میکروب خاص افزایش میابد.به دلیل اینکه این مکانیزم ایمنی در پاسخ به عفونت تکامل پیدا میکند به آن ایمنی وفقی و یا اختصاصی می گویند[5] . اجزای ایمنی اختصاصی لنفوسیت ها هستند و محصولات آنها آنتی بادی ها هستند . مواد بیگانه ای که پاسخ های ایمنی اختصاصی را القا میکنند یا مورد هدف

این پاسخ ها قرار میگیرند آنتی ژن نامیده میشوند. پاسخ اختصاصی در ابتدا مکانیسم های حفاظتی ایمنی ذاتی را افزایش میدهد تا بتواند آنتی ژنهای بیگانه را به نحو بهتری از بین ببرد.سپس سیستم ایمنی اختصاصی جهت برتری بر مکانیسم های نسبتا ثابت ایمنی ذاتی درجه بالایی از اختصاصی بودن را کسب میکند و در نهایت این سیستم در هر بار برخورد با یک میکروب، آنتی ژن را به خاطر می سپارد به طوری که در برخوردهای بعدی مکانیسم دفاعی بسیار کاراتری را تحریک میکند.

در مقابل در دنیای تکنولوژی حملات متفاوت ومتعدد ویروسی ها در شبکه ها بسیار فراوان گشته به طوریکه انواع نفوذگریها برای سرورهای شرکت های معروف ساخته شده اند .این حملات ویروسی از سرویس های مانع و آنتی ویروسها عبور کرده و میتواند حتی اطلاعات مربوط به کارتهای اعتباری را خارج نمایند تا جایی که گاهی اوقات با خود تصور می کنیم که شاید هیچ سیستم مدافعی بر روی سرور نصب نشده است. با اینکه یک برنامه جلوگیری کننده مفید در برابر حملات و ویروسها ضروری می باشد اما تکنولوژی فعلی برای دفاع در مقابل حملات ویروسی ودفع کردن همه انواع آنها نا توان است . برای مقابله با این مشکل میتوان از ایده سیستهای ایمنی طبیعی استفاده کرد و نوعی سیستم ایمنی مصنوعی را به گونه ای طراحی نمود که در برابر نفوذگری کاراتر باشد.

۲- مقایسه سیستمهای ایمنی طبیعی با تکنولوژیهای مرسوم:

هنگامی که یک درگاه برای برقراری ارتباط با فضای اینترنتی باز می گردد دیگر کاری از دست سیستمهای جلوگیری کننده در دفاع از حملات ویروسی به درگاه ساخته نیست . حتی زمانی که یک درگاه برای دسترسی به اینترنت باز نباشد ویروس ها میتوانند باز هم از فضای داخل سازمان وارد سیستمها شوند و به هر حال در امان نخواهد بود. البته این مورد در جایی اتفاق می افتد که یک سیستم ردیا ب سر زده به داخل کامپیوتر راه پیدا نماید البته همانگونه که از نام این برنامه ها پیداست این سیستم ها برای شناسایی حملات با لقوه ویروسی و واکنش در مقابل آنها دسته بندی نشده اند و هدف اصلی این سیستمهای ردیاب سرزده مبارزه با استفاده های غیرقانونی ، از دست دادن فرصت بهره وری واستفاده نابه جا از سیستم های کامپیوتری چه از جانب سیستمهای داخلی و چه مداخله گرهای خارجی می باشد [7،8]. اکثر سیستمهای ردیاب سیگنال های مشکوک را که بنا بر مداخله گرهای شناسای شده قبلی شناسایی می کنند . اما محدودیت مشخص این کاوشگرها این است که آنها در مقابل مداخله گرهایی که از قبل برایشان تعریف نشده اند ناتوان می باشند . در مقابل سیستم دفاعی انسان در چنین مواقعی با ساختن سلولهای ایمنی جدید قادر به دفاع در مقابل ویروسهای جدید و از قبل تعریف نشده می باشد پس تا اینجا رقابت به نفع سیستمهای طبیعی می باشد .



شکل ۱: شماتیک سیستم ایمنی بدن موجودات

۳- دیدگاه های الگوریتم ژنتیک و شبکه‌های عصبی به سیستم ایمنی

الگوریتم ژنتیک و شبکه‌های عصبی در حقیقت دو دیدگاه مشترک در خصوص سیستم ایمنی مصنوعی دارند . این محاسبات تکاملی، اصول و نظریاتی مناسب در شیوه‌های مختلف سیستم ایمنی مصنوعی بیان می‌دارد. مدلها و طرحهای سیستم ایمنی مصنوعی که بر اساس شبکه‌های ایمنی طرح ریزی شده‌اند همانند ساختارها و فعل و انفعالات مدلهای پیوندگرا هستند. بعضی تحقیقات تفاوت‌ها و شباهت‌های میان سیستم ایمنی مصنوعی و شبکه‌های عصبی مصنوعی را نشان همچنین از سیستم ایمنی مصنوعی در سیستم‌های عصبی و ایجاد مجموعه‌ای مناسب از داده های وزن دار برای تغذیه شبکه‌های عصبی استفاده نمود. کاربردهایی که بر اساس الگوریتم تکوینی یا ژنتیک میباشد برای بهینه سازی و آنهایی که بر اساس شبکه‌های عصبی هستند برای طبقه‌بندی مورد استفاده قرار می‌گیرند[2].

۴- معرفی تئوری خطر

طول دهه اخیر ، یک تئوری جدید ، به نام تئوری خطر در میان ایمنی شناسان رشد یافته است. این تئوری هنوز کامل نیست و در مورد اینکه رفتار ویا ساختار سیستم تاچه حد تغییر می کند شک و تردیدهایی وجود دارد . با این وجود این تئوری به حدکافی در طبیعت وجود دارد تا کاربرد آن را به سیستم های ایمنی مصنوعی واردکنیم.

ایمنی شناسی کلاسیک قید می کند که وقتی بدن با چیزهای غیر خودی یا بیگانه مواجه می شو د یک پاسخ ایمنی تحریک می گردد.

مثالهایی که به نظر می رسد که با دیدگاه عرف سازگار نیست ، بیماریهای خود ایمنی و انواع معینی از تومورها هستند که توسط سیستم ایمنی مورد هجوم قرار می گیرند که در واقع حمله به خودی ها میباشد و همچنین پیوند موفق اعضا که عدم حمله به غیر خودی هااست.

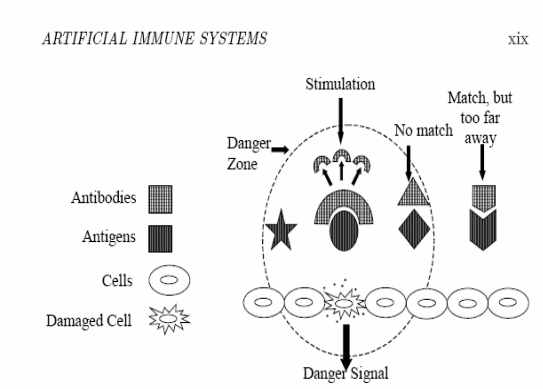
تئوری جدید اینطور استنتاج کرد که سیستم ایمنی در واقع برخی از خودی ها را از برخی غیر خودی ها تشخیص می دهد.و تنها بر چسب های جدید را شناسایی نمی کند بلکه روشی برای گریز از مشکلات معنایی خودی وغیر خودی فراهم می کند و بنابراین زمینه را برای پاسخ ایمنی مناسب فراهم می نماید . اگر تئوری خطر را به عنوان یک تئوری معتبر بپذیریم، می توانیم فقط به مهاجمان غیر خودی مضر وخودیهای مفید در سیستم مان توجه نماییم . برای پی بردن به این موضوع باید این تئوری را در جزئیات بیشتری امتحان کنیم.

نظر اصلی در تئوری خطر این است که سیستم ایمنی به غیرخودی ها پاسخ نمی دهد بلکه به خطر پاسخ می دهد.هر چند چیزی که در تئوری خطر بایدتشخیص داده شود با دیگر تئوری ها متفاوت است ولی در این تئوری نیز مثل تئوری کلاسیک نیاز به شناخت و تشخیص وجود

دارد . یعنی سیستم ایمنی به جای پاسخ به بیگانه، به خطر پاسخ می دهد . این تئوری از مشاهداتی به وجود آمده که در مواردی همچون پیوند اعضا که به آن اشاره شد، نیاز به حمله علیه عامل بیگانه وجود ندارد.

وقتی سلولها دراثر یک مرگ غیر طبیعی مانند استرس سلولی از بین می روند علامت خطر فرستاده می شود این علامت نشان دهنده ی آسیب به سلولها ست واز این طریق می توان خطر رااندازه گیری کرد . شکل۲ پاسخ ایمنی تئوری خطر را به ما نشان می دهد .

سلولی که آسیب دیده است یک علامت هشدار می فرستد ، در نتیجه آنتی ژن ها ی مجاور توسط سلولهای معرف آن آنتی ژن به گره های لنفاوی برده می شوند وتوسط لنفوسیت ها منهدم می شوند سیگنال خطرناک یک ناحیه ی خطر در اطراف خود به وجود می آورند . بنابراین پادتن هایی به وجود می آید که با آنتی ژن ها در ناحیه خطر هماهنگ می شوند .این پادتن ها تحریک می شوند و فرایند گسترش کلونی را بر عهده می گیرند .پادتن هایی که با آنتی ژن هماهنگ نمی شود ویا در فاصله ی دوری نسبت به ناحیه ی خطر قراردارند ، تحریک نمی شوند . هنوزماهیت دقیق سیگنال خطر واضح نیست . سیگنال خطر ممکن است سیگنال فعال کننده برای مثال آزاد کردن پروتئین هنگام شوک گرمایی ویا سیگنال مهار کننده مثل فقدان تماس سیناپسی با دنتریت سلولی که معرف آنتی ژن است باشد .



شکل ۲: شماتیک سیستم ایمنی بر مبنای سیستم خطر

۴-۱- پیاده سازی تئوری خطر در سیستم های ایمنی

تئوری خطر در مواردی که سیستمهای ایمنی مصنوعی باید دیتا ارائه دهند مناسب نمی باشد . در عوض ، این تئوری در مورد این که سیستم ایمنی مصنوعی کدام دیتا را باید ارائه دهد و با آن سروکار داشته باشد بسیار مناسب است [1].

سیستمهای ایمنی مصنوعی باید روی دیتای خطرناک متمرکز شوند. در این تئوری واژه غیر خودی را به خطر تغییر داده ایم. این مورد مناسب می باشد چون خطر یک سیگنال پایه است ولی غیرخودی نوعاً یک سری از بردارهای مشخصه هستند که اطلاعاتی در مور د اینکه آیا همه یا برخی ازاین ویژگیها در چه زمانی مورد نیاز هستند ندارند. سیگنال خطر به ما کمک می کند که زیرمجموعه هایی از بردار مشخصه که مورد نظر هستند را تشخیص دهیم.

یک سیگنال خطر تعریف شده مناسب می تواند به خیلی از محدودیت های انتخاب خودی از غیر خودی غلبه نمایدو حوزه غیر خودی ها را به یک سایز قابل کنترل

محدود می نماید و نیاز به واکنش در مقابل همه غیرخودی ها را از بین می برد در واقع به صورت وفقی به تغییرات بین خودی ها و غیرخودی هادلالت می نماید .

دستور شناسایی انتخاب و تعریف یک سیگنال خطر به طور واضح و مناسب است ، این انتخاب ممکن است یک نقطه بحرانی برای تابع برازندگی درالگوریتم ژنتیک باشد .به علاوه فاصله ی فیزیکی درسیستم زیستی باید به یک اندازه مناسب تعبیر شود تا یک سیستم ایمنی مصنوعی مطمئن داشته باشیم. این نوع پردازش بسیار با اهمیت می یاشد با این وجود اگر به شناخت کاملتری در مورد این تئوری برسیم کاربردهای سیستم ایمنی مصنوعی ممکن است مزایای قابل توجه وبینش جدیدی از تئوری خطر را به ویژه درسیستمهای کشف مزاحمت به کار گیرند .

۵- عملکرد سیستم ایمنی مصنوعی در امنیت اطلاعات

به طور شهودی واضح به نظر میرسد که سیستمهای ایمنی مصنوعی می بایست مناسب ترین سیستمها برای رفع مشکلات امنیتی کامپیوتر ها باشند.همانطورکه سیستم ایمنی انسانی ،بدن ما را فعال و پر انرژی نگه می دارد ما می توانیم همین را برای کامپیوترها با استفاده از سیستمهای ایمنی مصنوعی انجام دهیم.

هرچند ، برای فراهم کردن سیستمهای کشف مزاحمت عملی ، سیستمهای ایمنی مصنوعی می بایست یک سری از آشکارسازها را که به طور دقیق با آنتی ژن ها هماهنگ باشند بسازند. در روشی که سیستمهای کشف مزاحمت بر اساس سیستم خود ایمنی مصنوعی می باشند، آشکار سازها و اتصالات شبکه به عنوان رشته ها مدل شده اند.این آشکار سازها به طور تصادفی به وجود می آیند و سپس تاجایی که با اتصالات خوب حضور می یابند به مرحله ی بلوغ میرسند[3،4].

اگر آشکارسازها با هیچ یک از آنهایی که انتخاب شده اند سازگاری نداشته باشند آن ها به تکامل می رسندوشروع به کنترل اتصالات جدید در طول عمرشان می کنند . هرگاه این آشکار ساز تکامل یافته با اتصال دیگری هماهنگ شوند از مقدار آستانه معینی تجاوز کرده و فعال می شوند. این امر به یک اپراتور انسانی گزارش داده می شود واپراتور تصمیم می گیرد که آیا این یک ناهنجاری است یا نه ؟ اگر ناهنجاری وجود داشته باشد این آشکارسازها به آشکارسازهای حافظه با طول عمر نامحدود و حد آستانه فعال سازی مینیمم ترفیع داده می شوند. هر چند ا ین گزارش ها علائم مفیدی از مزاحمت های واقعی هستند ،اما آنها اغلب با هشدارهای اشتباه ترکیب می شوند و ظرفیت غیر قابل کنترل آنها متصدی امنیتی را مجبورمی کند که از اکثر اعلام خطرها چشم پوشی کند .به علاوه اعلام خطرهای سطح پایین،تشخیص مزاحمت های پیشرفته را ،که معمولا شامل مراحل مختلفی ازتهاجم است ،خیلی دشوار می کند.

برای بر طرف کردن این مشکلات سیستم های ایمنی مصنوعی بر پایه ایده هایی از تئوری خطر می تواند مورد استفاده قرار گیرد.

۶- نتیجه گیری

هر چند سیستم ایمنی در رابطه با سازگاری وبقا می باشند ،ولی در واقع یک تلاش دسته جمعی است که راه حل های چند گانه ای تولید می کنند و باهمکاری جواب را فراهم می کنند .بنابراین به نظر ما سیستم های ایمنی مصنوعی

در جایی که راه حلهای چند گانه سودمند هستند ،به عنوان یک بهینه ساز مناسب تر از روشهای مرسوم میباشند.به علاوه این سیستمها باید برخی از مفاهیم سازگاری را نیز برآورد سازد .و به دلیل اینکه آنها برخی از ویژگی های الگوریتم های تکاملی و شبکه های طبیعی را با هم ترکیب می نمایند به بکارگیری سیستم های ایمنی مصنوعی همراه با یادگیری توصیه ی خوبی برای مهندسی و مدیریت فن آوری اطلاعات در زمینه امنیتی میباشند .

سپاسگزاری

در پایان برخود لازم میدانیم ازهمکاری ونظرات شایسته جناب آقای مهندس قانونی معاونت محترم شرکت سهامی ذوب آهن اصفهان سپاسگزاری نماییم.

مراجع

[1] Aickelin, U., Bentley, P., Cayzer, S., Kim, J. and McLeod, J., 2003, Danger theory : The link between artificial immune systems and intrusion detection systems, in: Proc. 2nd Int. Conf. on Artificial Immune Systems (Edinburgh), Springer, Berlin, pp. 147–155.

[2]Aickelin, U., Greensmith, J. and Twycross, J., 2004, Immune system approaches to intrusion detection—a review, in: Proc. ICARIS-04, 3rd Int. Conf. on Artificial Immune Systems (Catania, Italy), Lecture Notes in Computer Science, Vol. 3239, pp. 316–329, Springer, Berlin.

[3]Esponda, F., Forrest, S. and Helman, P., 2004, A formal framework for positive and negative detection, *IEEE Trans. Syst., Man Cybernet.*,34:357–373

[4] Kim, J. and Bentley, P., 2001, Evaluating negative selection in an artificial immune systems for network intrusion detection, Proc. Geneticand Evolutionary Computation Conference 2001, pp.1330–1337.

[5]Ning, P., Cui, Y. and Reeves, S., 2002, Constructing attack scenarios through correlation of intrusion alerts, in: Proc. 9th ACM Conf. on Computer and Communications Security, pp. 245–254.

[6]Valdes, A. and Skinner, K., 2001, Probabilistic alert correlation, Proc.RAID'2001, pp. 54–68.

[۷] علیرضا نقش "طبقه بندی کالاهای صنعت و معدن توسط شبکه عصبی مصنوعی" همایش تحقیق و توسعه سالن اجلاس سران کشورهای اسلامی۱۳۸۴

[۸] علیرضا نقش بهاره بهمن پور "پیشگویی زلزله توسط شبکه عصبی مصنوعی" کنفرانس بین المللی زلزله دانشگاه شهید باهنر کرمان ۱۳۸۳