علوم و مهندسی کامپیوتر
نشریه علمی پژوهشی انجمن کامپیوتر ایران
مجلد ۳ شماره ۳ (الف)، پائیز ۱۳۸۴
صفحات ۱-۱۲
مقاله عادی

طراحی یک سیستم تکاملی ایمنی مصنوعی فازی برای امنیت شبکه های کامپیوتری

محمد حسین یغمایی مقدم[۱] داوود ملکی[۱] محمد رضا اکبرزاده توتونچی[۲]

[۱] گروه کامپیوتر، دانشگاه فردوسی مشهد، مشهد، ایران
[۲]گروه مهندسی برق، دانشگاه فردوسی مشهد، مشهد، ایران

چکیده

سیستم ایمنی بدن، یک سیستم محاسباتی جالب و کارا برای بسیاری از کاربردها در زمینهٔ مهندسی و بخصوص تشخیص نفوذ است. این سیستم دفاعی بر اساس عامل، به صورت توزیع شده و خود تطبیق است که بر اساس یک معماری لایه ای و سلسله مراتبی عمل می کند. در این مقاله، یک سیستم ایمنی مصنوعی بر اساس عامل ها و تکنیک های هوش محاسباتی شامل کنترل فازی والگوریتم های ژنتیکی، برای امنیت شبکه های کامپیوتری ارائه شده است. روش پیشنهادی از فرایند ذاتاً فازی بین عامل های آنتی ژن و آنتی بادی در سیستم ایمنی بدن استفاده می کند. همچنین از آلگوریتم های ژنتیک برای بهینه سازی و تکامل آنتی بادی ها استفاده می شود. ازشبیه ساز ns2 جهت شبیه سازی یک شبکه نمونه و تزریق حملات استفاده شده است. درقسمت ارزیابی عملکرد روش پیشنهادی، درفاز آموزش و تست از داده های استاندارد DARPA استفاده می شود. نتایج حاصل از شبیه سازی نشان دهنده برتری روش پیشنهادی نسبت به روش متداول فورست می باشد.

کلمات کلیدی: سیستم ایمنی مصنوعی فازی، آلگوریتم های ژنتیک ، عامل های هوشمند، تشخیص نفوذ، امنیت شبکه

۱- مقدمه

اخیراً با گسترده شدن اینترنت، تحقیق روی سیستم های ایمنی برای پیشگیری از نفوذ از اهمیت بالایی برخوردار شده است. بسیاری از سیستم های توسعه داده شده، امنیت را از طریق دیوارهای آتش و ضد ویروس ها برای حملات داخلی و خارجی فراهم می کنند [۱] . هر سیستم تشخیص نفوذ مبتنی بر شبکه عمدتاً سه هدف را دنبال می کند که عبارتند از: توزیع شدگی، خودتنظیمی و سربارکم [۲].
اخیراً فعالیت سیستم ایمنی بدن که بسیار پیچیده، هوشمندانه و مستقل از فرایند تفکر می باشد، بعلت شباهتهایی که با عملیات مرسوم کنترلی همچون شناسایی عامل های غیرخودی، حذف اغتشاش و صدور فرامین کنترلی دارد موردتوجه محققین قرار گرفته است. سیستم ایمنی بدن وظیفه حفظ سلامتی و دفاع بدن را بر عهده دارد، با بروز هر اختلال در سلامتی که می تواند بعلت ورود میکروارگانیسمهای مزاحم و یا دیگر عوامل محیطی باشد، مکانیزم های کنترلی این سیستم، عامل اخلالگر را شناسایی و فعالیت آن را محدود یا متوقف کرده و سپس آنرا منهدم می سازند. مولکول های شناسایی کننده عامل مزاحم ساختار پروتئینی دارند. علاوه بر این، ترکیبات مزاحم که آنتی ژن نامیده می شوند نیز اغلب ساختار پروتئینی دارند. عمل شناسایی بصورت اتصال مولکول های شناسایی کننده به قسمت هایی از پروتئین آنتی ژن که شاخص های آنتی ژنیک نامیده می شوند صورت می گیرد. پروتئین ها ملکول هایی بزرگ می باشند که از تکرار واحد های اسیدهای آمینه تشکیل شده اند. تعداد بیست اسید آمینه مختلف در ساختار پروتئینهای معمولی یافت می شوند که تفاوت آنها تنها در گروه متغیر جانبی آنهاست. اسیدهای آمینه به طرق مختلف با هم ترکیب شده و پیوندهای متفاوتی را ایجاد می کنند. با قرار گرفتن تعداد زیادی اسیدآمینه در کنار یکدیگر توسط پیوندهای ایجاد شده، پروتئین ها ایجاد می شوند.با توجه به تنوع موجود در پروتئین ها، بدیهی است که ساختار مولکولی و شکل پروتئین ها بسیار متنوع و پیچیده است.
دستگاه ایمنی انسان پس از برخورد اول با یک عامل عفتونت زا به تولید آنتی بادی می پردازد. این عامل عفونت زا ممکن است بار دیگر بدن را مورد حمله قرار دهد اما دستگاه ایمنی در برخورد اول با آن عامل هوشیار شده و آن را به خاطرمی سپارد. این خاطره به دستگاه ایمنی کمک می کند که در دفعات بعدی در مقابل

همان عامل عفونت زا با قدرت بیشتری عمل کند و مقادیر زیادی از آنتی بادی را در مدت کوتاه تری تولید کند. تشخیص آنتی ژنهای بیگانه که اساس عملکرد سیستم ایمنی بدن را تشکیل می دهد توسط دو نوع از مولکول ها به نام های ایمونوگلوبولین و گیرندهٔ آنتی ژن امکان پذیر می گردد. تنوع و گوناگونی که از مشخصات اساسی این ملکول هاست در نتیجه تغییرات ژنهای تولیدکنندهٔ آنها حاصل می شود. تنوع مولکولهای شناسایی کنندهٔ آنتی ژن های بیگانه، لازمهٔ مقابله با هر نوع عامل بیماری زا در بدن می باشد. برای این منظور ژنهای تولید کننده به طرق مختلف با یکدیگر تلفیق شده و در نهایت مولکول های متنوعی را پدید می آورند. بخشی از جایگاه نواحی متغیر آنتی بادی که با آنتی ژن برخورد می یابد پاراتوپ و قسمتی از آنتی ژن که در تماس با پاراتوپ واقع می شود اپی توپ نامیده می شوند[۴،۵،۶]. اصولاً پروتئینهای بزرگ به علت دارا بودن شاخصهای متعدد، بهتر از پروتئینهای کوچک می توانند دستگاه ایمنی راتحریک کنند. آنتی ژن هر چه بیگانه تر باشد(به این معنی که شباهت کمتری با آنتی ژن های خودی داشته باشد) بهتر می تواند پاسخ ایمنی را برانگیزد.

مهم ترین هدف یک مکانیزم سیستم ایمنی، محافظت بدن در مقابل نفوذ است. این کار بوسیله شناسایی مشخصات ملکولی میکروب ها و ویروس های حمله کننده به بدن انجام می شود. زمانی که ملکول های خارجی شناسایی شدند از طرق مختلف از بین می روند. شیوه ای که مکانیزم دفاعی بدن با شناسایی نوع آنتی ژن حمله کننده به بدن برمی گزیند مکانیزم"ایمنی اکتسابی اختصاصی" نام دارد. درآنتی ژن ها ملکول هایی هستند که قادرند پاسخ ایمنی اکتسابی را تحریک کنند. هر سلول در سیستم ایمنی از چندین ژن یا بیت تشکیل شده است[۶]. آنتی بادی ها به عنوان مشخصه شناسایی آنتی ژن ها یا غیر خودی ها معرفی می شوند. در سیستم ایمنی بدن زمانی که سطح انگیزش از یک سطح آستانه ای بیشتر شود، آنتی بادی ها به صورت فازی تکثیر و تولید می شوند.

اساس تصمیم گیری گروهی در سیستم ایمنی بدن بر اساس دو عامل انتخاب کلونی و شبکه ایدیوتایپ می باشد. بر اساس انتخاب کلونی، از نظر ژنتیکی سلول هایی که آنتی ژن را تشخیص می دهند رشد و تکامل می یابند، در حالی که سلول هایی که قادر به تشخیص آنتی ژن نیستند از بین می روند. این تشخیص بوسیلهٔ اتصال تقریبی صورت می گیرد. بنابراین اساس تنوع و گوناگونی، انتخاب کلونی است. بر اساس شبکهٔ ایدیوتایپ، آنتی بادی ها نه تنها بوسیله آنتی ژن ها تحریک می شوند بلکه بوسیلهٔ آنتی بادی های دیگر نیز تحریک می گردند[۶،۷].

تشخیص نفوذ، فرایند پیدا کردن بسته ها و برنامه های مخرب در شبکه های کامپیوتری است. عبارت ویروس های کامپیوتری اغلب برای کدهای ناخواسته و فعالیت های نادرست در کامپیوتر میزبان به کار می رود. این خاصیت شبیه سیستم ایمنی بدن است که بدن ما را در مقابل عوامل بیماریزای خارجی محافظت می کند.

یک مدل و نگاشت بین سیستم های محاسباتی و زیستی به صورت زیر است:

ویروس های کامپیوتری و نفوذها در شبکه، معادل آنتی ژن ها در سیستم ایمنی بدن هستند.

عامل های کشف و شناسایی در شبکه، معادل سلول های B، T و آنتی بادی ها در سیستم ایمنی بدن هستند.

بیت ها، کلمات و رشته ها در کامپیوتر، معادل پروتئین ها در سیستم ایمنی بدن انجام وظیفه می کنند.

انطباق الگو در شناسایی حملات در کامپیوتر، معادل اتصال آنتی بادی ها وآنتی ژن ها در سیستم ایمنی بدن است.

خصیصه های سیستم ایمنی بدن که می توان از آنها در امنیت شبکه های کامپیوتری بهره برد عبارتند از:

۱) قابلیت تشخیص الگو توسط آنتی بادی ها: این تشخیص الگو با استفاده از یک سطح آستانه انجام می گیرد. بدین صورت که هر گاه تحریک الگوی نفوذی از یک سطح آستانه ای فراتر رفت، آن به عنوان یک غیرخودی تشخیص داده می شود.

۲) تطبیقی بودن سیستم ایمنی بدن با رخدادها و محیط

۳) قابلیت یادگیری: سیستم ایمنی بدن قادر است ویروس های جدیدی که می بیند به خاطر بسپارد.

۴) همکاری گروهی بین سلول ها: این خاصیت به صورت موازی و توزیع شده در سیستم ایمنی بدن برای تشخیص و انهدام نفوذها است.

۵) تنظیم تعداد سلول های ایمنی توسط سیستم ایمنی

۶) چند لایه ای بودن: هیچ موجودیتی در بدن، یک مکانیزم کامل امنیتی را فراهم نمی کند بلکه هر لایه به صورت مستقل عمل کرده و با بقیه لایه ها نیز در ارتباط است.

۷) تنوع و گوناگونی: سیستم ایمنی بدن در برابر انواع مختلفی از نفوذها مقاومت کرده و تسلیم نمی شود.

۸) بهینه بودن منابع: با ایجاد مرگ سلولی و تکثیر سلولی، همواره یک نمونه فضای کوچکی از فضای جستجوی آنتی ژن ها در هر زمان نگه داری می شود.

۹) پاسخ انتخابی: در سیستم ایمنی بدن بعد از شناسایی یک آنتی ژن پاسخ های متفاوتی به آن داده می شود و همواره به یک شکل عمل نمی کند[۸،۹] .

دراین مقاله از سیستم ایمنی طبیعی بدن برای شناسایی الگوهای ترافیکی غیرنرمال استفاده شده است. این مقاله روی مکانیزم های تشخیص عامل های خودی و غیرخودی در سیستم ایمنی و روش های محاسباتی مانند فازی و آلگوریتم ژنتیک تکیه دارد. الگوریتم ژنتیک با استفاده از اپراتورهای جهش و انتخاب، عمل اتصال را بهبود می بخشد[۱۱،۱۰] . در نتیجه این مکانیزم سطح بالایی را برای آنتی ژن ها ایجاد می کند. همچنین الگوریتم ژنتیک درسیستم ایمنی پیشنهادی با عمل تقاطع متقابل همراه است که آلگوریتم ژنتیک تکاملی را مدل سازی می کند. سیستم پیشنهادی بر اساس انتخاب منفی کار می کند وقادر به شناسایی حملات شناخته شده و ناشناخته می باشد.

دراین مقاله از چندین خاصیت سیستم ایمنی شامل: انتخاب منفی برای شناسایی الگوهای غیرنرمال، تطبیق جزئی با روش فازی و الگوریتم های ژنتیک استفاده شده است. سیستم تشخیص نفوذ پیشنهادی به صورت توزیع شده می باشد. در سیستم توزیع شدهٔ پیشنهادی، فرض براین است که درنقاط مختلف شبکه کامپیوترهایی وجود دارند که موظف به آنالیز ترافیک شبکه و تشخیص نفوذ احتمالی می باشند. تشخیص نفوذ درسیستم پیشنهادی، به کمک چندین عامل توزیع شده هوشمند انجام می شود. این عامل های توزیع شده، درکناریکدیگر هوشمندی و توان زیادی را برای تشخیص نفوذ فراهم می کنند[۱۲،۱۳،۷].

ساختار باقیمانده مقاله به صورت زیر می باشد. در بخش۲سیستم ایمنی و کارهای مرتبط در این زمینه ارائه شده است. دراین بخش سیستم ایمنی فورست بررسی می گردد؛ در بخش ۳ سیستم امنیتی پیشنهادی توضیح داده می شود. ارزیابی عملکرد سیستم پیشنهادی و مقایسه آن با سیستم فورست دربخش ۴ آورده شده است. در بخش ۵ نتیجه گیری از مقاله ارائه گردیده است.

۲- کارهای مرتبط

از روش های ایجاد امنیت و تشخیص نفوذ، می توان روشهای ایجاد نماهای عادی شبکه، شبکه های عصبی، کنترل فازی و سیستم های خبره را نام برد. بیشتر پروژه ها در این زمینه تنها به بررسی حملات بر روی فقط یک سیستم متمرکز شده اند، در حالی که حوادث و رخدادها در حملات چندین سیستم را مورد آسیب قرار می دهند. از آنجاییکه سیستم پیشنهادی مبتنی برسیستم دفاعی بدن می باشد، دراین بخش کارهای قبلی درزمینه استفاده از سیستم ایمنی بدن درامنیت شبکه های کامپیوتری بررسی می شوند.

در زمینهٔ بکارگیری از خواص سیستم ایمنی بدن در امنیت شبکه های کامپیوتری، اولین تحقیقات را فورست برای تشخیص خودی و غیر خودی دریک سیستم ایمنی شبکه انجام داده است[۱۴-۱۶]. فورست با ساخت یک سیستم ایمنی کامپیوتر برای تشخیص خودی و غیر خودی، توانست نفوذها رادر شبکه شناسایی کند و از فایل ها حفاظت نماید. درادامه کار فورست، هافمیر[۷،۸،۱۰]، یک سیستم ایمنی مصنوعی به نام ARTIS [۱] طراحی کرد و آن را برای امنیت یک شبکه کامپیوتری با ۵۰ کامپیوتر به کار گرفت . در این سیستم مسئله همکاری و تبادل اطلاعات بین عامل ها در نظر گرفته نشده است و تشخیص نفوذگر در هر کامپیوتر جداگانه انجام می گردد لذا سیستم کارایی چندانی ندارد.

پروژه هایی که از سیستم ایمنی بدن برای امنیت شبکه های کامپیوتری استفاده کرده اند به نام سیستم های ایمنی مصنوعی یا CIS [۲] معروفند. از دیگر کارهایی که از سیستم ایمنی بدن برای امنیت شبکه استفاده کرده اند می توان به روش ذکر شده در[۱۷] اشاره کرد. در این پروژه یک برنامه، شبیه سلول های B در سیستم ایمنی، اتصالات شبکه را مشاهده می کند. یک سری از برنامه ها نیز شبیه سلول هایT در سیستم ایمنی، فرآیندهای در حال اجرا رامی بینند. یک سری از توابع نرم افزاری نیز به طور اتوماتیک سلول های B و T می بینند و یکسری از توابع نیز اطلاعات را در شبکه بین سلول های مختلف مبادله می کنند. سیستم در صورت تشخیص تهاجم یا فرآیندهای غیر نرمال، واکنش لازم را انجام می دهد. سایرکارهای دیگر که از سیستم ایمنی یا CIS برای امنیت شبکه های کامپیوتری بکارگرفته شده است در مراجع [۱۸-۲۲] آورده شده است.

در این مقاله یک سیستم ایمنی مصنوعی طراحی و شبیه سازی شده است. سیستم پیشنهادی بر اساس زیر ساختارهای سیستم های ایمنی مصنوعی در پروژه های Lisys [۳] [۱۵] و CDIS [۴] [۲۳،۱-۲۷] ساخته شده است. Lisys یکی از اولین ساختارها برای سیستم های ایمنی مصنوعی است که برای مسئله تشخیص نفوذ در شبکه به کار می رود. این سیستم توسط فورست از دانشگاه نیو مکزیکو ارائه شده است. Lisys برای یک شبکهٔ محلی ساده طراحی شده و می تواند ترافیک شبکه را یاد گرفته و بسته های غیر عادی را تشخیص دهد و برای حفاظت یک شبکه محلی از حملات شبکه ای مناسب است. در اینجا خودی به عنوان یک مجموعهٔ نرمال از ارتباطات در سطح TCP/IP بین کامپیوترها تعریف می شود و غیرخودی یک مجموعه از ارتباط های غیرنرمال درشبکه محلی است که شبیه نفوذهای شبکه ای می باشند. هر ارتباط به صورت سه تایی: آدرس مبدأ، آدرس مقصد و سرویس کامپیوترها نشان داده می شود. یک مجموعه شناسنده [۵] در Lisys وجود دارد که برای تشخیص غیرخودی ها به کار می رودویک زندگی محدودی دارند و در صورتی که عمر آنها سپری شده باشد و یا فاقد انگیزه شوند از بین می روند. این مجموعه شناسنده به صورت تصادفی تولید می شود و در بین میزبان های شبکه قرار می گیرد.

CDIS نیز یک ساختار سیستم ایمنی مصنوعی دیگری است که برای تشخیص ویروس ها و تهاجم های کامپیوتری طراحی شده است. CDIS به عنوان توسعهٔ پروژهٔ Lisys است و در اصول مشابه آن می باشد. این سیستم طوری طراحی شده تا هم ویروس ها و هم نفوذهای شبکه ای را کشف کند. CDIS یک سیستم ایمنی محاسباتی توزیع شده، چند لایه و چند عامله است که بسیار شبیه به Lisys است و چرخهٔ حیات آنتی بادی ها در هر دو یکسان می باشد. آنتی بادی ها یا همان شناسنده ها درهر دو به طور تصادفی تولید می شوند. ازجمله مشکلات ساختار CDIS این است که تنها یک بسته را در هر زمان بررسی و آنالیز می کند.

۲-۱ سیستم ایمنی فورست

این سیستم ایمنی که در پروژهٔ Lisys ارائه شده است[۱۰،۱۵] ترافیک TCP/IP را در یک شبکه محلی مانیتور می کند.

ارتباط بین تمام پروتکل ها از طریق TCP است. این ارتباط از طریق سه تایی: آدرس مبدأ، آدرس مقصد و سرویس شبکه تعریف می شود. این سیستم به جریان ترافیکی کاری ندارد و تنها بسته های از نوع TCP SYN را مانیتور می کند. در اینجا هر آنتی بادی یک چرخهٔ حیات دارد و بر اساس انتخاب منفی کار می کند. بدین صورت که تمام عامل ها ی خودی در ابتدا به آنتی بادی ارائه می شود و در صورتی که این آنتی بادی با یکی از آنها منطبق شود از بین می رود. در این سیستم نشان داده شده است که هفت حملهٔ معمول و شایع که در سیستم اتفاق می افتد با کمتر از ۱۰۰ رشتهٔ بیتی تشخیص دهنده با طول ۴۹ بیت کشف می شود. در این سیستم ایمنی عملیات ها در دو فاز انجام می شود: فاز آموزش و فاز تست.

- **فاز آموزش**

در فاز آموزش تنها یکسری شناسنده ساخته می شوند و در بین میزبانهای شبکه قرار می گیرند. آلگوریتم تولید آنتی بادی در مرحلهٔ آموزش در این سیستم به صورت زیر است:

۱- تولید آنتی بادی به طور تصادفی: این آنتی بادی ها، آنتی بادی های 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 گیردکه 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 رشتهٔ 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. اگر زمان سنج به یک حد قابل قبول رسیده باشد، آنتی بادی خام تبدیل به آنتی بادی با تجربه می شود. برای هر آنتی بادی باتجربه یک زمان حیات در نظر گرفته می شود.

- **فاز تست**

در این قسمت مرحلهٔ اصلی آلگوریتم انجام می شود و غیرخودی ها شناسایی می گردند. آلگوریتم شناسایی آنتی ژن ها و حملات و حیات هر آنتی بادی در این قسمت مشخص می شود. این آلگوریتم به صورت زیر خلاصه می گردد:

۱- رشته ها از یک فایل ورودی تست به ترتیب وارد می شوند.

۲- هر رشتهٔ ورودی به آنتی بادی های با تجربه تولید شده از مرحله آموزش ارائه می گردد و با آن مقایسه می شود؛

۲-۱- اگر رشتهٔ ورودی با آنتی بادی با تجربه انطباق حاصل کرد و یا به عبارتی شناسایی گردید، رشتهٔ ورودی به عنوان یک رشتهٔ غیرخودی تلقی می شود و آلارم ایجاد می گردد وبه کاربر هشدار داده می شود. به زمان حیات آن آنتی بادی نیز اضافه می گردد.

۲-۲- اگر رشتهٔ ورودی با آنتی بادی با تجربه انطباق حاصل نکرد، از زمان حیات آنتی بادی با تجربه کم می شود .بعد از این حالت هر آنتی بادی با تجربه ای که زمان حیات آن سپری شده باشدحذف می شود و می میرد.

۳- هر رشتهٔ ورودی به آنتی بادی های خام موجود ارائه می گردد و با آن مقایسه می شود؛

۳-۱- اگر رشتهٔ ورودی با آنتی بادی خام انطباق حاصل کرد؛ آنتی بادی خام حذف می شود و دوباره یک آنتی بادی خام با زمان سنج صفر ایجاد می شود.

۳-۲- اگر رشتهٔ ورودی با آنتی بادی خام انطباق حاصل نکرد؛ به زمان سنج آن اضافه می گردد. بعد از آن اگر زمان سنج به حد قابل قبول رسیده بود، آن آنتی بادی تبدیل به آنتی بادی باتجربه می گردد.

۳- سیستم ایمنی پیشنهادی

در این قسمت یک سیستم ایمنی بر اساس رشته های باینـری ارائــه می شود که

ازالگوریتم های ژنتیک و فازی برای تکامل و بهبود آنتی بادی ها در سیستم استفاده می گردد. الگوریتم های ژنتیک همچنین باعث تنوع آنتی بادی ها می شود، بطوری که بر اساس انتخاب کلونی سلول هایی که آنتی ژن را تشخیص می دهند رشد کرده و سلول هایی که نمی توانند تشخیص دهند می میرند.مشابه سیستم ایمنی فورست ، در سیستم ایمنی پیشنهادی نیز عملیات ها در دو فاز جداگانه انجام می شود: فاز آموزش و فاز تست.

در ابتدا آنتی بادی ها ازیک تعداد ناحیهٔ ژنی به طور تصادفی ساخته می شوند. مؤلفه های اصلی در این سیستم ایمنی؛ یک مجموعه دادهٔ آموزشی، آنتی ژن و آنتی بادی ها و یکسری گوی تشخیص به نام $ARB^{۶}$ در حول هر سلول B است. هر ARB یک مجموعهٔ 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.

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

$$w_{ij} = \exp(-\frac{d_{ij}^2}{2d_i^2}) \qquad (۱)$$

با توجه به فرمول فوق، شکل مجموعهٔ فازی ARBیک تابع گوسی است که هر چه از مرکز ARBدور می شویم مقدار آن کاهش می یابد.

سطح برانگیختگی در هر ARB به صورت زیر بدست می آید:

$$S_i = \frac{\sum_j w_{ij}}{d_i^2} \qquad (۲)$$

با ماگزیمم کردن سطح انگیزش در هر ARB و مشتق گیری از S خواهیم داشت:

$$d^2{}_i = \frac{\sum_j w_{ij} d_{ij}^2}{\sum_j w_{ij}} \qquad (۳)$$

درفرمول های فوق، d_{ij} فاصلهٔ بین آنتی ژنj تا مرکز $ARB(i)$، $d_i{}^2$ شعاع گوی $ARB(i)$ و S_i سطح انگیزش در هر $ARB(i)$ می باشد.

نرمال سازی داده ها بر اساس شبکهٔ 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 تأثیر قرار بدهد. چهار پارامتر مهم این سیستم عبارتند از:

۱- NAT[۷] 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 cloneها برای هر ARB

هر ARB، یک رشتهٔ n بیتی است که این رشته ها در فضای دو بعدی نرمالیزه می شوند بطوریکه هر رشته حکم یک نقطه را در فضای دو بعدی دارد. در شکل ۱ نمایش داده ها و ABR ها درفضای دو بعدی آورده شده است.

درسیستم پیشنهادی ازیک کنترلر فازی برای تصمیم گیری در تطبیق و تشخیص عامل 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 سازندهٔ آنتی بادی مربوطه می باشند. هرقدر رشته های کروموزوم از آنتی بادی ها دورتر باشند از مرکز ARB یا گوی تشخیص دورترند و آنتی بادی انگیزش کمتری برای تکثیر و تأثیر روی آن دارد.ARB ها به صورت حافظهٔ دینامیک از سلول های B عمل می کنند. این ARB ها می توانند به خوبی به روز آوری شوند و اطلاعات گذشته را نیز به خوبی نگهداری کنند.

الگوریتم های ارائه 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 ارائه شده دارای ساختار و مراحلی مشخص می باشند که در ادامه آورده شده است. این الگوریتم ها اجزای اصلی سیستم ایمنی هوشمند پیشنهادی راکه برمبنای سیستم ایمنی بدن طراحی شده است، تشکیل می دهند.

• فاز آموزش

آلگوریتم ارائه شده در قسمت فاز آموزش برای تولید یکسری آنتی بادی استفاده می شود. این آلگوریتم، خوشه سازی مجموعهٔ خودی ها را به عهده دارد و بر اساس آن یکسری آنتی بادی تولید می کند. هر ARB شامل یک رشته داده ای و تعدادی سلول B با شعاع مربوطه می باشد. فازآموزش با استفاده از یکسری داده های آموزشی خودی انجام می گیرد. آلگوریتم تولید آنتی بادی ها در مرحله آموزش در سیستم پیشنهادی به صورت زیر است:

۱- تولید جمعیت اولیه باینری بصورت تصادفی از ARBها: به تعداد مشخص شده ARB اولیه تولید می شود که در ابتدا شعاع آنها 1/. است و تعداد سلول های B و سطح انگیزش هر یک ۰ می باشد. تعداد سلول های B و شعاع هر ARB قدرت آن را در شناسایی آنتی ژن ها نشان می دهند.

۲- مجموع خودی به سیستم ارائه می شود و تا زمان خاتمهٔ وضعیت مراحل زیر انجام می گردد:

۲-۱- رشته های خودی به هر ARB ارائه می شود و 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 هرARB بر طبق سطح انگیزش بدست آمده برای آن، سلول B اختصاص می یابد.

۲-۴- ARB های ضعیف که هیچ سلول B را شامل نیستند حذف می گردند.

۲-۵- عملیاتهای Clone و Mutate روی ARB ها انجام می شود.

۲-۶- مجموعهٔ جمعیت ARB ها به صورت زیر بهینه و یکپارچه می شوند:

۲-۶-۱- هر دو ARB ای که بسیار به هم نزدیک هستند و فاصلهٔ آنها از هم بسیار کم است؛ یا گوی ها با هم همپوشانی دارند، آن دو ARB در هم ادغام می شوند. نتیجتاً ARB جدیدی که بدست می آید برابر است با crossover دو ARB قبلی.

۳- پایان

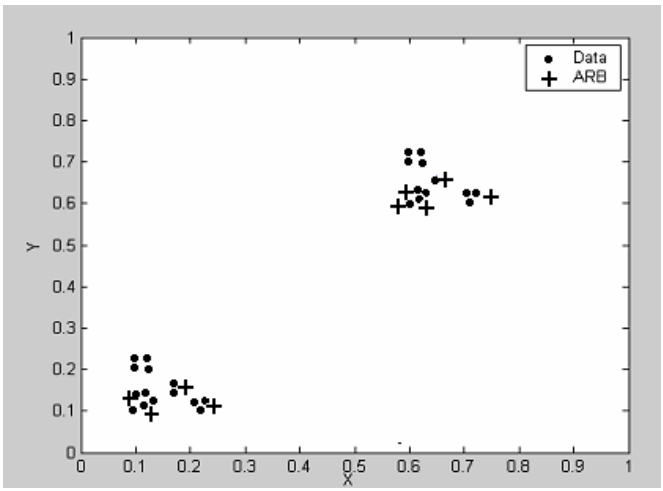
در این آلگوریتم، میزان انطباق یا نزدیکی بین ARB ها با داده ها و یا دیگر ARB ها، با فاصله اقلیدسی بین آنها در فضای دو بعدی بدست می آید. اگر دو ARB با هم همپوشانی یا تورفتگی داشته باشند(یعنی: $d_i + d_j < d_{ARBi} + d_{ARBj}$) آنها را با عملیات crossover به یک ARB تبدیل می کنیم که با انجام عملیات crossover درARB جدید داریم:

$$d = (d_i + d_j)/2, c = (c_i d_i + c_j d_j)/(d_i + d_j) \qquad (۴)$$

در اینجا عملیات تکثیر یا *clone* در هر *ARB* با جهش یا *mutate* انجام می شود و شعاع نیز به ارث برده می شود.

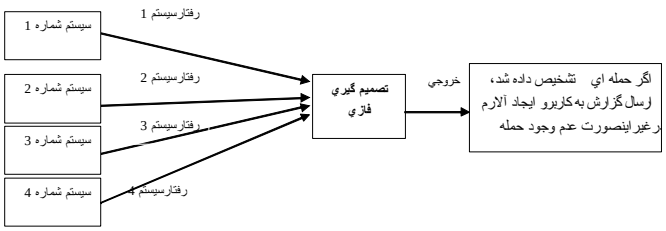
• فاز تست

در این فازمرحلهٔ اصلی آلگوریتم انجام می شود و حملات شناسایی می گردند. شناسایی حملات بوسیلهٔ کنترلر فازی انجام می گیرد. توابع عضویت در اینجا بصورت گوسی هستند. هر چه قدر یک آنتی بادی از رشتهٔ کروموزوم دورتر باشد آنتی بادی تأثیر کمتری روی آن دارد و برعکس. فاصلهٔ بین رشته های آنتی بادی و کروموزوم ها بصورت مجموع طول های پیوسته یکسان در هر دو رشته محاسبه می شود.



شکل ۱- نمایش داده ها و ARBها در فضای دو بعدی

فرایند تصمیم گیری با یک کنترلر فازی انجام می گیرد. سیستم فازی دارای چهار ورودی ویک خروجی می باشد. ورودی های کنترلرفازی چهار سیستم از مجموعهٔ *ARB* در نظر گرفته شده است. براساس خروجی کنترل کننده فازی ، وجود حمله و یا عدم وجود حمله مشخص می شود. کنترلر فازی پیشنهادی درشکل ۲ آورده شده است.

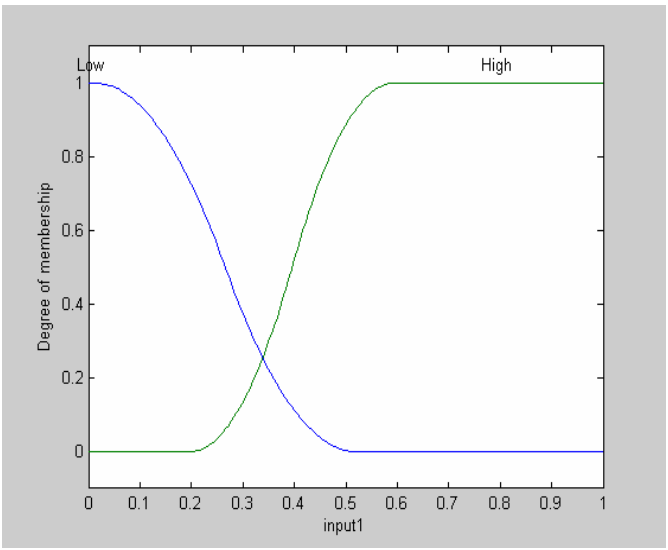


شکل ۲- ساختار سیستم فازی پیشنهادی تشخیص نفوذ

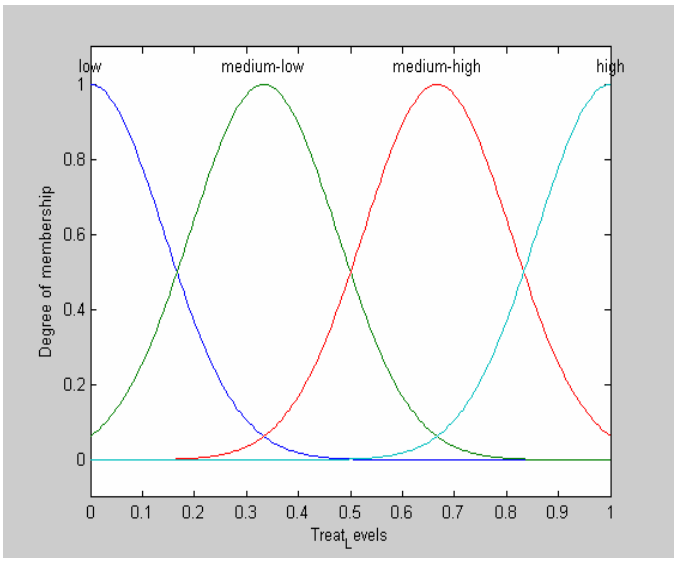
هر سیستم، آنتی بادی های مربوط به خود را برای شناسایی دارد. درسیستم پیشنهادی با در نظر گرفتن قابلیت های سیستم ایمنی در شناسایی غیرخودی ها، از کنترلر فازی برای همکاری گروهی جهت تشخیص غیرخودی ها به شبکه استفاده شده است.

سطح رفتار فازی با ۴ مجموعهٔ فازی از توابع گوسی در ۴ سری از *ARB* ها به طور موازی انجام می شود. در اینجا هر سیستم تشخیص، فاز آموزش و فاز تست مجزا دارد. رفتار کلی آنها با کنترلر فازی بررسی می شود. رفتار هر سیستم توسط دو مجموعه فازی low، High نشان داده می شود. همچنین خروجی کنترل کننده فازی با چهار مجموعه فازی low، Medium-Low، Medium-High و High نمایش داده می گردد.

تمام توابع عضویت به صورت گوسی بوده که درشکل ۳ و ۴ نمایش داده شده اند. درشکل ۵ نمایش سه بعدی قوانین فازی با درنظر گرفتن دو سطح انگیزش ورودی آورده شده است.



شکل ۳- تابع عضویت ورودی کنترلرفازی برای هرسیستم



شکل ۴- توابع عضویت خروجی

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

۱- مجموعه تست به سیستم ارائه می شود. برای هر رشته ورودی مراحل زیر انجام می گردد:

۱-۱- به تعداد n رشته به هر *ARB* ارائه می شود و بر اساس فاصله ای که از هر *ARB* دارند مشخص می شود آیا قابل شناسایی هستند یا نه؟ لذا مراحل زیر برای هر *ARB* موجود در شبکه انجام می شود:

۱-۱-۱- فاصلهٔ رشتهٔ ورودی با هر *ARB* محاسبه می شود.

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

۱-۱-۳- آیا خطا یا واقعه ای اتفاق افتاده است یا نه؟(در صورت رخداد خطا کنترلر فازی آنرا بررسی می کند.)

۱-۲- برای هر *ARB* برطبق سطح انگیزش بدست آمده برای آن، سلول *B* اختصاص می یابد.

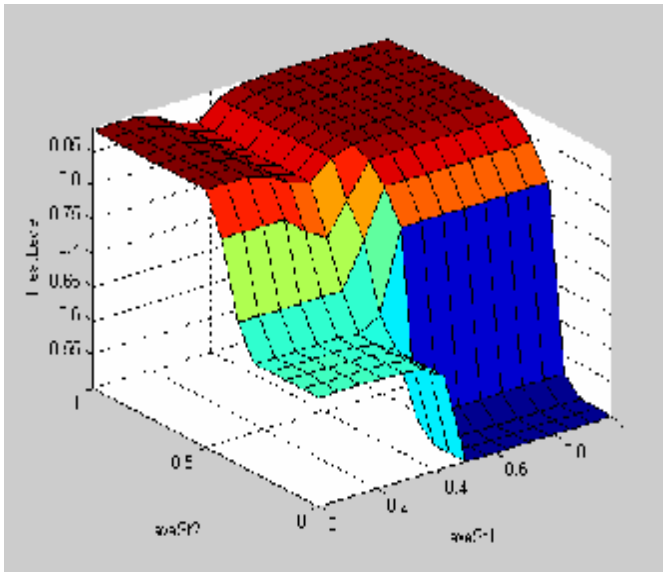
۱-۳- *ARB* های ضعیف که هیچ سلول *B* را شامل نیستند حذف می گردند.

۱-۴- عملیاتهای Clone و Mutate روی *ARB* ها انجام می شود.

۱-۵- مجموعهٔ جمعیت *ARB* ها به صورت زیر بهینه و یکپارچه می شوند:

۱-۵-۱- هر دو *ARB* ای که بسیار به هم نزدیک بودند و فاصلهٔ آنها از هم بسیار کم بود؛ آن دو *ARB* در هم ادغام می شوند. *ARB* جدیدی که بدست می آید برابر است با crossover دو *ARB* قبلی.

۲- پایان



شکل ۵- نمایش سطح ۳ بعدی قوانین فازی

۴- ارزیابی عملکرد

دراین قسمت به بررسی ارزیابی عملکرد سیستم پیشنهادی و مقایسه آن با سیستم متداول فورست می پردازیم. برای ارزیابی الگوریتم ارائه شده، دو مجموعه داده استفاده شده است که عبارتند از: ۱) داده های استاندارد مجموعهٔ DARPA [28] که شامل یکسری داده برای فاز آزمایش و یکسری داده برای فاز تست با حملات مشخص می باشد ۲) داده های ترافیکی شبکهٔ شبیه سازی شده درمحیط شبیه سازns2[29] که آن نیزشامل دو مجموعه داده می باشد، یک مجموعه داده برای فاز آموزش و یک مجموعه داده برای فاز تست با حملات مشخص. توپولوژی شبکهٔ شبیه سازی شده درمحیط ns2 شامل یک شبکه محلی با یکسری کامپیوتر داخلی و خارجی است که از سه سرور، دو مسیریاب و تعدادی client و حمله کنندهٔ داخلی و خارجی تشکیل شده است. برای بررسی کارایی روش ارائه شده تحت حملات مختلف، برخی از حملات متداول در این شبکه شبیه سازی شده است. این حملات درادامه آورده می شوند. بر روی داده های ترافیکی این شبکه و داده های DARPA آنالیز مورد نظر انجام گرفته و کلیه مشخصات مورد نظر از سرآیند بسته ها و اتصالات در شبکه استخراج گردیده وبر اساس سیستم ایمنی کد گردیده شده اند و رشته های باینری مورد نظر ساخته شده است. درمرحله بعد با استفاده از آلگوریتم های سیستم ایمنی انواع حملات شناسایی گردیده است. سیستم ایمنی مصنوعی فورست و سیستم پیشنهادی شبیه سازی شده است و بر روی داده های باینری کد شده، الگوریتم های مورد نظر پیاده سازی شده و سپس نتایج مورد بررسی قرارگرفته اند. هر آزمایش ده بار تکرار گردیده است و میانگین نتایج بدست آمده درنمودارها نشان داده می شود.

۴-۱ کدینگ پیشنهادی اتصالات شبکه بر اساس سیستم ایمنی

حملات و کلیهٔ اتصالات در شبکه بصورت رشته های باینری کد می شوند. روش فورست تنها بسته های از نوع TCP SYN را درنظر می گیرد و به بقیهٔ جریان ترافیک کاری ندارد. رشته های باینری از یک فایل ورودی به نام TcpDump ساخته می شوندوسپس بر اساس جدول ۱کدسازی انجام می گردد. اگر طول رشته، ۴۹ بیت باشد کدسازی فشرده انجام می شود. اگر طول رشته ۷۵ بیت باشد کدسازی فشردهٔ کم انجام می شود وچنانچه طول رشته ۸۲ بیت باشد، کدسازی غیر فشرده اما بدون آدرس مبدأ اعمال می شود. اگر طول رشته ۹۸ بیت باشد کدسازی غیر فشرده انجام می شود.

جدول۱- جدول کدسازی داده ها

حالت ۱: کد سازی فشرده ۴۹ بیتی	**پورت مقصد**	**ورود/خروج**	**آدرس دور**	**آدرس محلی**	-	-
	۸ بیت	۱ بیت	۳۲ بیت	۸ بیت	-	-
حالت ۲: کدسازی ۷۵ بیتی	**پورت مقصد**	**پورت مبدا**	**نوع پروتکل اتصال**	**ورود/خروج**	**آدرس دور**	**آدرس محلی**
	۱۶ بیت	۱۶ بیت	۲ بیت	۱ بیت	۳۲ بیت	۸ بیت
حالت۳: کدسازی ۸۲ بیتی	**پورت مقصد**	**نوع پروتکل اتصال**	**آدرس مقصد**	**آدرس مبدا**	-	-
	۱۶ بیت	۲ بیت	۳۲ بیت	۳۲ بیت	-	-
حالت ۴: کدسازی ۹۸ بیتی	**نوع پروتکل اتصال**	**پورت مقصد**	**آدرس مقصد**	**پورت مبداء**	**آدرس مبداء**	-
	۲ بیت	۱۶ بیت	۳۲ بیت	۱۶ بیت	۳۲ بیت	-

در حالت کلی تر کدسازی اتصالات و آنتی بادی ها به رشته های باینری بر اساس مشخصات کاملتری از پروتکل های ارتباطی نشان داده شده درجدول۲ انجام می شود. کد کردن رشته ها برای پروتکل های اصلی TCP،IP ، UDP، ICMP انجام می گیرد. حالت عمومی کدسازی بسته های TCP،IP، UDP و ICMP، ۳۲۰ بیت است که از روی مشخصات فیلدهای پروتکل ها بدست می آید . این ۳۲۰ بیت از روی ۲۸ مشخصهٔ فیلدهای سرآیند بسته ها بدست می آیند. آنتی بادی ها و رشته های مربوطه در سیستم ایمنی از روی این مشخصه ها ساخته می شوند. آنتی بادی ها از روی این ۲۸ مشخصه، آنتی ژن ها را بوسیلهٔ قوانین انطباق (match_rule) در سیستم ایمنی تشخیص می دهند.

تعدادی از مشخصه های مهم فیلدهای پروتکل ها در جدول۲ آمده است.

در این جدول برای هر فیلد موارد زیر عنوان گردیده است:

۱- مشخصهٔ ژن؛ که نشان می دهد آن ژن چه مشخصه ای از فیلد در پروتکل مربوطه دارد مثلاً آدرس مبدأ یا مقصد و ...

۲- مقادیر ممکن عددی برای فیلد؛

۳- طول ژن یا تعداد بیت های مربوطه هر فیلد؛

۴- مکان شروع آن فیلد در رشته یا کروموزوم؛

۵- توضیحات برای هر ژن؛ که در ستون آخر جدول قرار دارد.

حملات مشخص و شناخته شده نیز بر اساس جداول فوق کد شده ومشخص می شوند.

۴-۲ حملات آزمایش شده

سیستم تشخیص نفوذپیشنهادی بر اساس مشخصات بسته های پروتکلی یا با مشخص کردن اتصالات در شبکه قادر به کشف حملات می باشد. این سیستم قادر به شناسایی حملات و ویروس های متعدد است.

جدول ۲- قوانین کدینگ پیشنهادی برای انطباق الگوی بسته های شبکه و آنتی بادی های سیستم ایمنی (برای بسته های IP)

شماره ژنی	فیلد	مقادیر ممکن	تعداد بیت های ژن	مکان شروع	توضیحات
۱	Protocol Type	TCP, UDP, ICMP	۲	۰	مقادیر ۱و۲و۳ به ترتیب برای پروتکل های TCP ، UDP و ICMPبه کارمی روند. عدد ۰ نشان دهنده حالت بی اهمیت است
۳	IP Time To Live (TTL)	۰-۲۵۵	۸	۱۸	معمولاً کمتر از ۱۲۸ می باشد
۴	IP Flags	۰- ۶۵۵۳۵	۱۶	۲۶	فقط مقادیر ۲ و ۴ قانونی می باشند
۶	IP Source Address A	۰-۲۵۵	۸	۵۸	--
۱۰	IP Dest. Address A	۰-۲۵۵	۸	۹۰	--
۱۴	TCP Src Port	۰- ۶۵۵۳۵	۱۶	۱۲۲	--
۱۵	TCP Dest.Port	۰- ۶۵۵۳۵	۱۶	۱۳۸	--
۲۵	TCPReset	Boolean	۱	۲۶۳	--
۲۶	TCPSyn	Boolean	۱	۲۶۴	--
۲۷	TCPFin	Boolean	۱	۲۶۵	--
۱۴	UDPSrcPort	۰- ۶۵۵۳۵	۱۶	۱۲۲	--
۱۵	UDPDesPort	۰- ۶۵۵۳۵	۱۶	۱۳۸	--
۱۴	ICMPType	۰-۲۵۵	۸	۱۲۲	--

یکی از راههای توسعه سیستم های ایمنی انجام عملیات موازی و همکاری بین آنتی بادی ها در تشخیص حملات می باشد که در این پروژه انجام گرفته است.

حالت ساده ای از این سیستم تشخیص نفوذ، بررسی تنها مسیرها و اتصالات ایجاد شده بین کامپیوترهاست که این کار بوسیله فورست با بررسی تنها بسته های TCP SYNدر شبکه انجام گرفته است. در این حالت از آنالیز بقیهٔ بسته های شبکه صرف نظر می شود. طول رشته یا طولDatapath برابر ۴۹ بیت قرار داده شده است. از پورت های مشهور TCP که دراین مقاله بررسی می شوند عبارتند از:

۱- سرویس FTP با شمارهٔ پورت ۲۱.
۲- سرویس Telnet با شماره پورت ۲۳.
۳- سرویس SMTP(e-mail) با شماره پورت ۲۵.
۴- سرویس DNS با شماره پورت ۵۳.
۵- سرویس SNMP با شماره پورت ۱۶۱.
۶- سرویس IMAP باشماره پورت ۱۴۳.
۷. سرویس Login با شماره پورت ۵۱۳.
۸- سرویس SSH با شماره پورت ۲۲.
۹- سرویس POP3 با شماره پورت ۱۱۰.
۱۰- سرویس finger با شماره پورت ۷۹.
۱۱- سرویس HTTP با شماره پورت ۸۰.

حملاتی که مورد آزمایش قرار گرفته اند عبارتند از:

۱- Address Probing(AP) یا حملهٔ جستجوی آدرس: بدین ترتیب که یک نفوذگر با استفاده از یک کامپیوتر در شبکه داخلی، تعداد زیادی حوزهٔ آدرس خارجی را کشف می کند. همهٔ این جستجوها روی پورت شمارهٔ ۲۳، Telnet انجام می گیرد.

۲- PortScanning (PS) یا پویش پورت ها: بدین صورت انجام می گیرد که یک کامپیوتر خارجی، کامپیوترهای داخلی را با تلاش برای ارتباط به همهٔ پورت هادر شبکه داخلی، پویش و بررسی می کند.

۳- Limited Probing (LP) یا پویش پورت های محدود : در اینجا یک کامپیوتر خارجی سعی در ارتباط با چهار پورت Telnet(23)، SMTP(25)، DNS(53) و POP(110) روی کامپیوتر های داخلی دارد.

۴- Single Port Probing (SP) یا پویش تنها یک پورت: که در اینجا یک کامپیوتر خارجی، پورت Telnet(23) را روی کامپیوترهای داخلی پویش می کند.

۵- Synthetic Internal(SI): این آزمایش روی ۱۰۰۰ اتصال تصادفی بین کامپیوترهای داخلی انجام شده است. آدرس مبدأ و مقصد بین کامپیوترها به طور تصادفی، از کامپیوترهای داخلی انتخاب شده است. سرویس ها و پورت ها نیز به طور تصادفی از بین FTP(21)، Telnet(23)، SMTP(25) و finger(79) انتخاب گردیده است. این آزمایش می تواند مدلی از حملاتی که حمله کننده حداقل به یک کامپیوتر داخلی دسترسی دارد، باشد.

۶- Synthetic External(SE): این آزمایش روی ۱۰۰۰ اتصال تصادفی بین کامپیوترهای داخلی و خارجی انجام شده است و سرویس ها به طور تصادفی از (finger، SMTP، Telnet، FTP) انتخاب گردیده است. این آزمایش مدلی از حملات هماهنگ و توزیع شده می باشد.

۷- Random(RN) یا تصادفی: آزمایش روی ۱۰۰۰ رشتهٔ تصادفی به طول ۴۹ بیت انجام شده است.

با ورود هر بسته، بر اساس جدول کدسازی ارائه شده عملیات مشخصی برروی آن انجام می شود. در نهایت از هر بسته یک رشتهٔ دودویی با مشخصات ژنی ساخته می شود. بعد از کدکردن وقایع و ایجاد رشته های ژنی، بر اساس قوانین انطباق در صورت تشخیص حمله به آن پاسخ مناسب داده می شود.

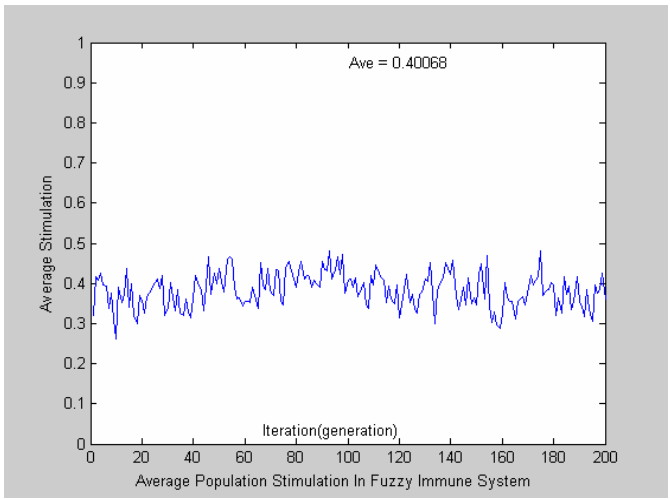
۴-۳ نتایج ارزیابی

دراین قسمت به ارائه نتایج ارزیابی بدست آمده از شبیه سازی می پردازیم.شکل ۶ مراحل تولید آنتی بادی را در فاز آموزش آلگوریتم ارائه شده نشان می دهد. در نهایت تعداد بهینه ای از آنتی بادی های مناسب تولید می شوند که در فاز تست مورد استفاده قرار می گیرند. این آنتی بادی ها بر اساس داده های آموزشی ورودی ساخته می شوند. همچنانکه در شکل مشخص است تعداد ***ARB*** ها نمی تواند تا بینهایت رشد کند و به یک حد قابل قبول می رسد و عمل خوشه سازی روی ورودی ها انجام می گیرد. شکل ۷ تکامل میانگین سطح انگیزش آنتی بادی ها را در هر مرحله در فاز آموزش آلگوریتم ارائه شده نشان می دهد.

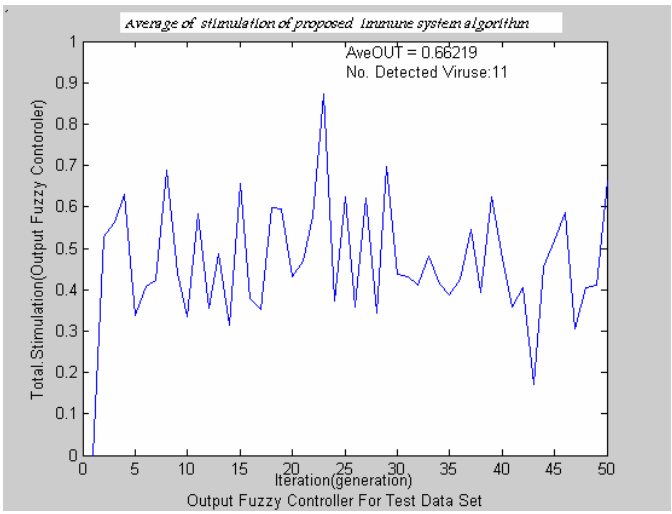
همانطور که درشکل مشاهده می شود میانگین سطح انگیزش تکامل می یابدودر نهایت به یک حد مناسب می رسد. تعداد و نوع آنتی بادی ها بر اساس این مقادیر تغییر می کند. در شکل بیشترین و کمترین میانگین سطح انگیزش آنتی بادی ها معلوم است. الگوریتم پیشنهادی، در نهایت چند دسته از داده ها با سطح انگیزش شبیه به هم را ارائه می دهد.

نمودار شکل ۸ میانگین سطح انگیزش در هر تکرار برای فاز تست الگوریتم پیشنهادی را نشان می دهد. سیستم کنترلر فازی با توجه به این مقادیر، ویروس های داده های تست را پیدا می کند و گزارش می دهد.

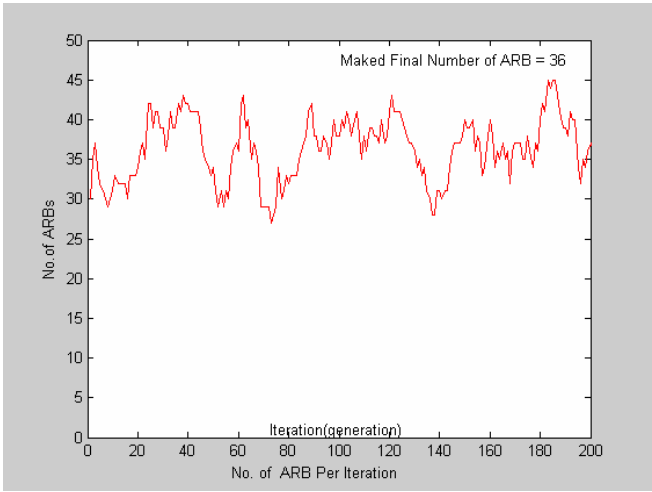
در نمونهٔ آزمایش شده با داده های تست ورودی تعداد ۱۱ ویروس توسط سیستم فازی گزارش شده است.



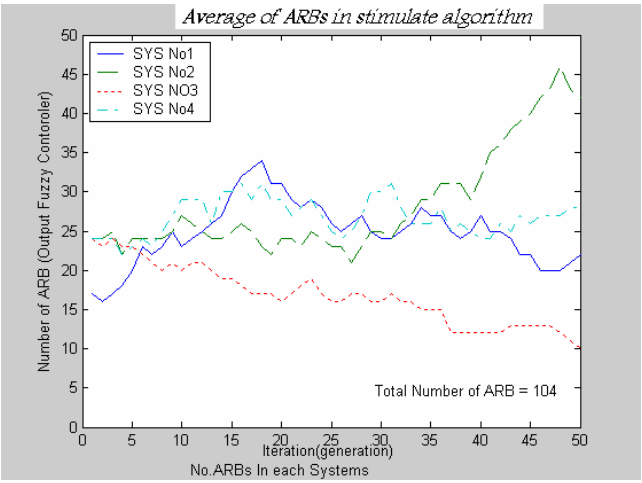
شکل ۶- تعداد آنتی بادی ها در هر تکرار



شکل ۸- میانگین سطح انگیزش در هر تکرار



شکل ۷- میانگین سطح انگیزش در هر تکرار



شکل۹- تعداد آنتی بادی ها در هر تکرار.

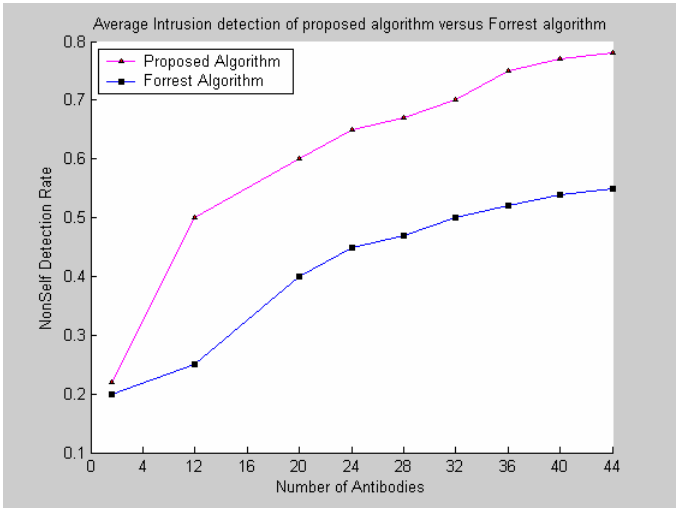
نمودار شکل ۹ تعدادآنتی بادی های هر سیستم تشخیص نفوذ را نشان می دهد. همچنان که در شکل مشخص است سیستم پیشنهادی شامل ۴ سیستم تشخیص نفوذ است. در اینجا هر سیستم بعد از هر تکرار به روزآوری می شود و یکسری آنتی بادی تولید و یکسری از بین می روند.در نهایت هر سیستم سعی می کند تعداد بهینه ای از آنتی بادی های مناسب را در تکرار های بعدی نگه دارد.

حملات توضیح داده شده در قسمت قبل، شبیه سازی و ساخته شده اند. رشته های باینری و آنتی ژن ها و آنتی بادی ها مربوط به هر یک با استفاده از کدینگ ارائه شده ساخته گردیده اند. سپس حملات توسط هر دو الگوریتم معمول فورست و پیشنهادی در شرایط یکسان آزمایش شده اند. نتایج آزمایش با تولید اولیهٔ ۲۰ آنتی بادی در هر الگوریتم در فاز آموزش، درجدول۳ آورده شده است. همچنانکه درجدول۳ مشاهده می شود الگوریتم پیشنهادی در همهٔ موارد حملات بیشتری را کشف می کند. درسیستم پیشنهادی با استفاده از روش های سیستم ایمنی فازی و ژنتیک آنتی بادی ها در هر مرحله بهینه می شوند.

شکل ۱۰ نرخ کشف غیرخودی ها را به تعداد آنتی بادی ها در هر دو روش نشان می دهد. چنانکه در شکل مشخص شده است هر چقدر تعداد آنتی بادی ها در سیستم بیشتر باشد حملات بیشتری کشف می شود اما در الگوریتم پیشنهادی نرخ تشخیص با افزایش آنتی بادی ها بسیار بیشتر از الگوریتم فورست افزایش می یابد.

جدول ۳- مقایسه درصد حملات کشف شده در الگوریتم فورست و الگوریتم پیشنهادی (با تعداد ۲۰ آنتی بادی اولیه در هر کدام)

مجموعه حملات تست شده	تعداد رشته ها	بخش غیر خودی	بخش غیر خودی کشف شده توسط الگوریتم فورست	بخش غیر خودی کشف شده توسط الگوریتم پیشنهادی
AP	۱۰۰۰	٪۵۴	٪۳۴	٪۴۴
PS	۱۰۲۴	٪۴۳	٪۳۰	٪۳۵
LP	۱۰۲۴	٪۶۰	٪۳۰	٪۴۵
SP	۵۰۰	٪۱۰	٪۵	٪۷
SI	۲۰۲۴	٪۲۰	٪۱۳	٪۱۸
SE	۲۰۲۴	٪۴۰	٪۲۵	٪۳۵
RND	۲۰۲۴	٪۵۰	٪۳۰	٪۴۸



شکل ۱۰- نرخ کشف غیر خودی ها به تعداد آنتی بادی های

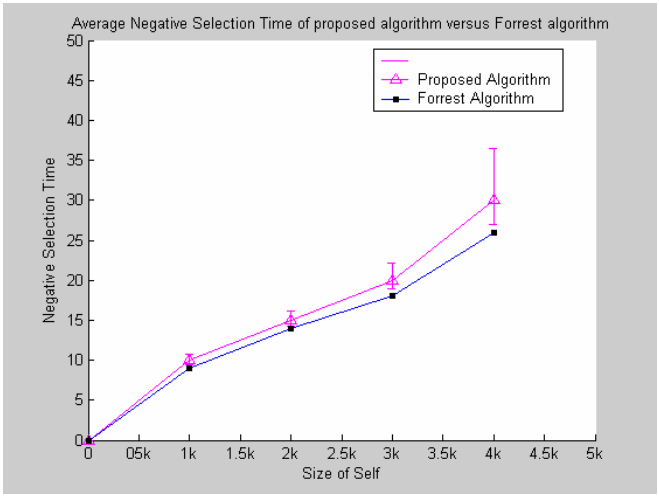
نمودارهای شکل۱۱ و۱۲ برای مقایسهٔ سیستم ایمنی ارائه شده با سیستم های ایمنی معمول فورست در فاز آموزش یا مرحله یادگیری آنتی بادی ها است که هر دو بر اساس انتخاب منفی کار می کنند. بدین ترتیب که یک مجموعه از خودی ها در داده های آموزشی به سیستم ارائه می شود و نتیجتاً یک سری آنتی بادی حاصل می شود.

نمودار شکل ۱۱ زمان انتخاب منفی بر حسب اندازه فایل آموزشی را نشان می دهد. برای انجام این آزمایش فایل ورودی با اندازه های 1k, 2k, 3k, 4k, 5k به سیستم های ایمنی معمول فورست و سیستم پیشنهادی داده شده و زمانهای انتخاب منفی در هر دو آلگوریتم اندازه گیری شده است. دیده می شود که زمان انتخاب منفی هردوروش تقریبا یکسان می باشد. لذا در پردازش فایل ورودی و انجام آلگوریتم انتخاب منفی، سیستم پیشنهادی سرعت لازم را دارا می باشد. وجود آلگوریتم های فازی و ژنتیک تأثیری در کاهش سرعت پردازش در این سیستم ندارد و سرعت لازم را نسبت به آلگوریتم فورست دارا می باشد.

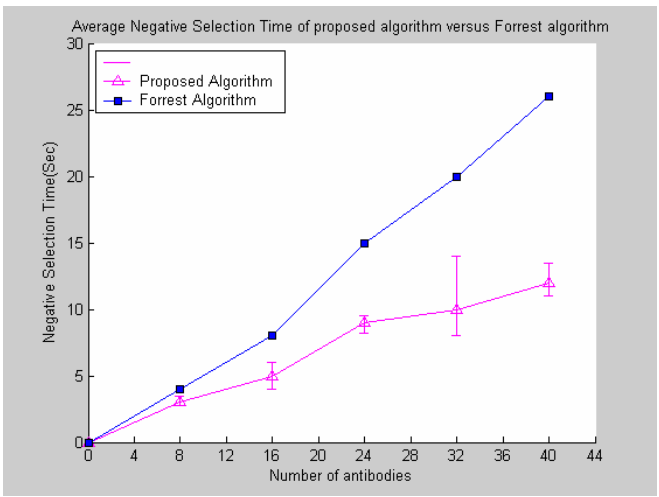
نمودار شکل۱۲ زمانهای انتخاب منفی را بر حسب تعداد آنتی بادی های تولیدی در هر آلگوریتم نشان می دهد. درهر الگوریتم به ترتیب ۲، ۴، ۶و ...آنتی بادی به طور تصادفی تولید شده و با یک فایل 1k آموزشی زمانهای انتخاب منفی در هردو الگوریتم اندازه گیری شده و در نمودار شکل ۱۲ ارائه گردیده است. همچنانکه در شکل ۱۲ مشخص است زمانهای انتخاب منفی در آلگوریتم پیشنهادی کمتر از الگوریتم معمول فورست می باشد. این کاهش زمان انتخاب منفی به خاطر وجود آلگوریتم ژنتیک و فازی در آلگوریتم پیشنهادی است و موجب بهینه سازی تعداد و نوع آنتی بادی ها می گردد.

نمودارهای شکل های ۱۳، ۱۴، ۱۵ و۱۶ برای ارزیابی و مقایسه سیستم ایمنی مصنوعی پیشنهادی با سیستم ایمنی معمول فورست درفاز تست ارائه شده است. این نمودارها مربوط به فاز تست و تشخیص آنتی ژنها و غیر خودی ها در شبکه می باشند. در اینجا از یک مجموعه دادهٔ تست که از شبکه شبیه سازی شده با داده های DARPA فراهم آمده است برای تست سیستم های ایمنی در شناسایی حملات استفاده شده است. مجموعه داده تست شامل یک سری داده از رشته های باینری است که با استفاده از سیستم های ایمنی خودی ها و غیر خودی های در آن مشخص می شوند

نمودار شکل۱۳ نرخ خطاها را بر حسب تعداد آنتی بادی ها در هر دو سیستم ایمنی نشان می دهد. خودی هایی که به عنوان غیرخودی و نفوذ تشخیص داده می شود، به عنوان خطا درنظر گرفته شده است.



شکل ۱۱- زمان انتخاب منفی به اندازهٔ فایل ورودی

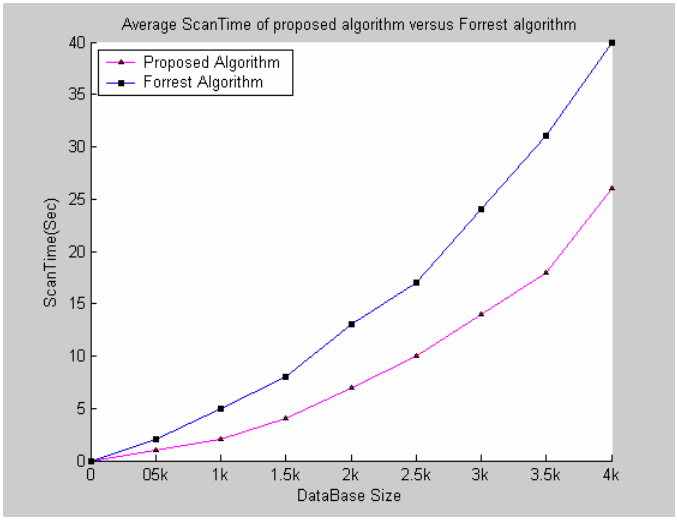


شکل ۱۲- زمان انتخاب منفی به تعداد آنتی بادی ها.

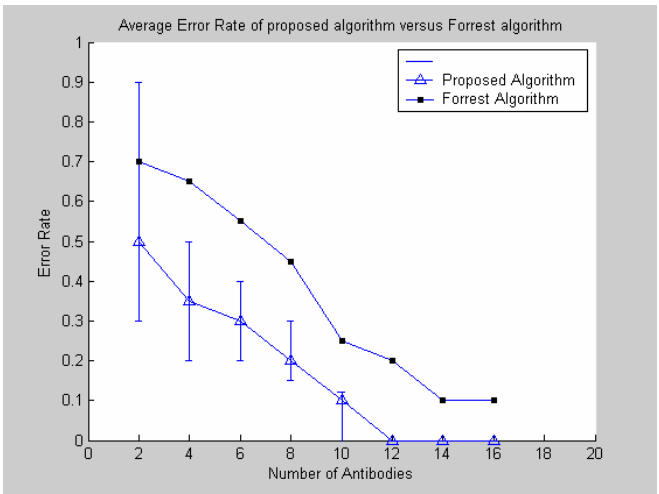
نرخ خطا به صورت درصد تعداد خطاها به تعداد حملات کشف شده محاسبه می شود. چنانچه در شکل مشخص است نرخ خطا در سیستم پیشنهادی کمتر از سیستم متداول فورست است. این موضوع به خاطر وجود آلگوریتم های فازی و ژنتیک در شناسایی غیرخودی ها در سیستم پیشنهادی است. بدین ترتیب روش پیشنهادی، روشی کاراتر و بهتر در شناسایی غیر خودی ها ارائه می دهد.

نمودار شکل ۱۴ زمان پویش و آنالیز فایل تست را بر حسب اندازهٔ فایل ورودی تست نشان می دهد . فایل پایگاه داده ای که برای آزمایش مورد استفاده قرار گرفته است در اندازه های 4k،3k،2k،1k می باشد. زمان پویش در هر دو سیستم اندازه گیری شده و در نمودارها مشخص شده است. همانطورکه در نمودارها مشخص است زمان اسکن در سیستم پیشنهادی بهتر می باشد و وجود آلگوریتم های فازی و ژنتیک باعث کندی و اخلال در سیستم نمی شود بلکه به سرعت تشخیص می انجامد، در صورتی که در آلگوریتم فورست مراحل بیشتری برای آنالیز فایل تست ورودی باید انجام گیرد.

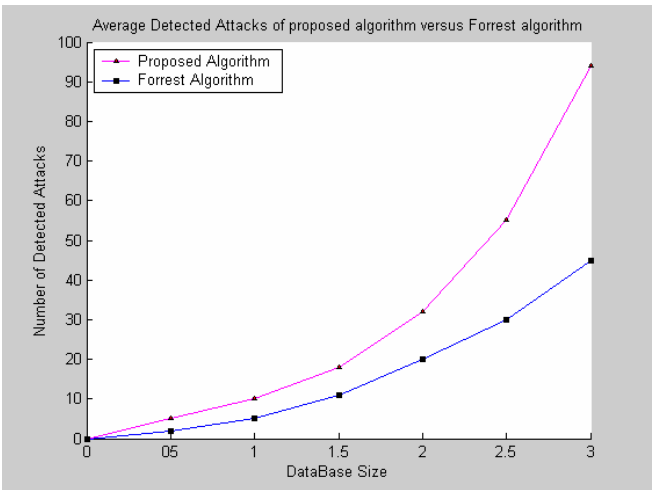
نمودار شکل ۱۵ یکی از مهمترین نمودارهای بدست آمده است. وجود آلگوریتم های ژنتیک در سیستم ایمنی پیشنهادی موجب تنوع در کشف حملات مختلف می گردد. ادغام سیستم فازی با آلگوریتم های ژنتیک نیز به این امر کمک می کند. این نمودار، تعداد حملات کشف شده بر حسب اندازهٔ فایل ورودی در سیستم را نشان می دهد.



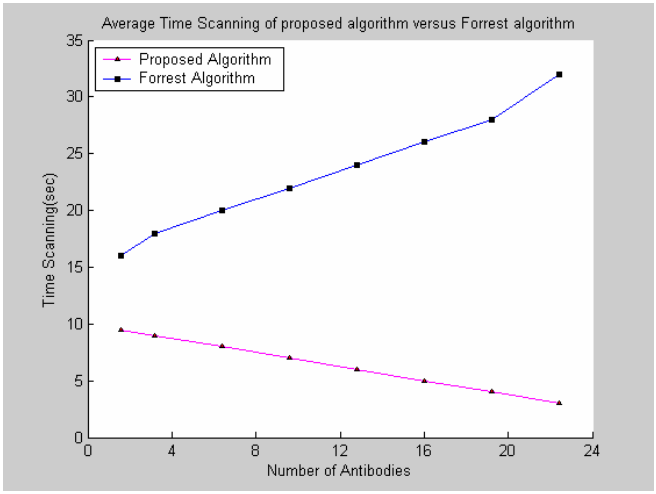
شکل ۱۳- نرخ خطا به تعداد آنتی بادی ها



شکل ۱۴- زمان پویش برای تشخیص نفوذ به اندازهٔ فایل.



شکل ۱۵- تعداد حملات کشف شده به اندازهٔ فایل



شکل ۱۶- زمان پویش در تشخیص نفوذ به تعداد آنتی بادی ها

نمودار شکل ۱۶، مهم ترین نمودار در فاز تست می باشد. این نمودار زمان اسکن و پویش یک فایل ورودی به اندازهٔ 1k را بر حسب تعداد آنتی بادی ها در هر دو سیستم نشان می دهد. وجود آلگوریتم های ژنتیک و فازی در این شکل مشهودتر است زیرا که وجود این دو آلگوریتم باعث بهینه سازی آنتی بادی ها و در نتیجه کاهش زمان پویش می شود.

۵- نتیجه گیری

این مقاله از مکانیزم تشخیص خودی و غیر خودی سیستم ایمنی و مکانیزم انتخاب کلونی در این سیستم ، برای تشخیص نفوذ در شبکه های کامپیوتری استفاده کرده است. همچنین دراین مقاله نوع جدیدی از آنتی بادی ها با استفاده از عامل های تصمیم گیرنده و آلگوریتم های ژنتیک و فرایند فازی توسعه داده شده است. آزمایش ها نشان می دهد که سیستم ایمنی مصنوعی پیشنهادی نتایج خوب و مطلوبی در امنیت شبکه دارد. درسیستم پیشنهادی الگوریتم های ژنتیک باعث تنوع در آنتی بادی ها شده و قابلیت یادگیری را برای سیستم بوجود می آورد. سیستم ایمنی پیشنهادی تلاش دارد تا قابلیت ها ی سیستم های تشخیص نفوذ را در شبکه های کامپیوتری بهبود ببخشد و تکنیک جدیدی در حل امنیت سیستم های کامپیوتری باشد. در این مقاله از مکانیزم تشخیص خودی و غیرخودی سیستم ایمنی بدن و بر اساس اصل انتخاب کلونی در میان آنتی بادی ها استفاده شده است ویک روش جالب و کارا، برای تولید آنتی بادی ها در شناسایی ویروس ها و نفوذهای شبکه ای ارائه می دهد. نتیجتاً اینکه استفاده از آلگوریتم های سیستم ایمنی، در شناسایی نفوذها در شبکه های کامپیوتری وسیستم های توزیع شده، بسیار کارا و قابل استفاده می باشد. نتایج حاصل از شبیه سازی با کمک داده های استاندارد DARPA نشان می دهد که سیستم ایمنی ارائه شده دراین مقاله نتیجه بهتری نسبت به سیستم متداول فورست دارد. از کارهای انجام شده در این مقاله، ایجاد ارتباط و همکاری بین سلول ها و آنتی بادی ها بر اساس شبکهٔ ایدیوتایپ سیستم ایمنی بدن در ساخت تصمیمات بهینهٔ گروهی برای مقابله با حملات است. برای رسیدن به این هدف در این مقاله از آلگوریتم های تکامل جمعی در ساختار آنتی بادی ها استفاده شده است. بدین مفهوم که یک گروه از سلول هابا هم تکامل می یا بند به طوریکه با هم همکاری و ارتباط دارند تا به اهداف خود برسند و حملات را شناسایی کنند. از کارهای آینده دراین تحقیق توسعه الگوریتم های تکامل جمعی برای فرایند سلولی سیستم ایمنی می باشد.

مراجع

[1] P. K. Harmer, P. D. Williams, G. H. Gunsch and B. Lamont, " An Artificial Immune System Architecture for Computer Security Applications," *IEEE Transaction On Evolutionary Computation*, 2002.

[2] M. Roesch, "Writing Snort Rules: How to Write Snort Rules and Keep your Sanity," http://www.snort.org/writing_snort_rules.htm.

[3] Rajesh, S. Khurana, "NOMAD: Traffic-based Network Monitoring Framework for Anomaly Detection," *Proceedings IEEE International Symposium on Computers and Communications*, ,pp. 442-451, 1999.

[4] B. Alberts, D. Bray, J. Lewis,M. Raff, K. Roberts and J. D. Watson, *Molecular Biology of the Cell (2nd Edition)*, Garland publishing. Inc., New York,1994.

[5] Roitt, M. Ivan, *Essential immunology* 9nd Edition Oxford : Blackwell Scientific, 1997.

[6] J. D. Farmer, N. H. Packard and A. S. Perelson. "The Immune System, Adaptation and Machine Learning". *Physica 22D* pp. 187-204, North-Holland, Amsterdam, 1986.

[7] F. M. Burnet, *The Clonal Selection Theory of Acquired Immunity*. Cambridge University Press. 1959.

[8] S. A. Hofmeyer, *An Immunological Model of Distributed Detection and Its Application to Computer Security* PhD. Thesis New Mexico: University of New Mexico, 1999.

[9] J. Kim and P.Bentley, "An Evaluation of Negative Selection in an Artificial Immune Model for Network Intrusion Detection," *Proc. Genetic and Evolutionary Conference 2001 (GECCO-2001),* San Francisco, CA, pp. 1330-37, 2001.

[10] S. A. Hofmeyer and S. Forrest, "Immunity by Design: An Artificial Immune System," *Proc. of the Genetic and Evolutionary Computation.Conference.* San Mateo, CA Morgan Kaufmann, pp.1289-1296, 1999.

[11] S. Forrest, B. Javornik, R. E. Smith and A. S., "Using Genetic Algorithms to Explore Pattern Recognition in the Immune System," *Perelson. Evolutionary Computation*, vol. 1, no. 3, pp. 191-211, 1993.

[12] P. Harmer, P. Williams, G. Grunsch and G. Lamnot," Distributed Agent Based Architecture for Computer Security Applications," *IEEE Transactions on volutionary Computation, Special Issue on Artificial Immune Systems*, 2002.

[13] O. Nasaroui, F. Gonzalez, et al. "The Fuzzy Artificial Immune System: Motivations, Basic Concepts and Application to Clustering and Web Profiling." *International Joint Conference on Fuzzy Systems*: pp. 711-717 , 2002.

[14] S. Forrest, A. S.Perelson, L.Allen, and Cherukuri, "Self-- Nonself Discrimination in a Computer," *Proc. IEEE Symposium on Research in Security and Privacy*, Oakland, CA, pp. 202- 212.

[15] J. Balthrop, S. Forrest and M. Glickman. "Revising lisys: Parameters and Normal Behavior," *In CEC-2002. Proceeding of the Congress on Evolutionary Computing*, 2002.

[16] S. Forrest, B. Javornik, R. E. Smith and A. S. Perelson. "Using Genetic Algorithms to Explore Pattern Recognition in the Immune System," *In Evolutionary Computation* vol.1, no.3, pp. 191-211, 1993.

[17] H. Nishiyama and F. Mizoguchi, "Design of Security System Based on Immune System," *IEEE Faculty of Sci. and Tech., Science University of Tokyo .Noda, Chiba*, PP. 278-8510, 2001.

[18] D. Dasgupta, "Immunity-Based Intrusion Detection System A General Framework," *Proc. of the 22nd National Information Systems Security Conference(NISSC)*, 1999.

[19] L. N. D. Castro and F. J. V. Zuben," Artificial Immune Systems: PartII-A Survey of Applications," *Technical Report DCA-RT* 02/00, 2000.

[20] N. Mitsumoto and T. Fukuda, "The Immune Mechanism, Adaptation, Learning for the Multi Agent System," *Proc. of IEEE Symposium on Emerging Technologies & Faculty Automation*, pp. 446-453, 1994.

[۲۱] ر. جلیلی، « طراحی و پیاده سازی یک سیستم تشخیص تهاجم مبتنی بر توصیف»، **مجموعه مقالات هشتمین کنفرانس بین المللی سالانه انجمن کامپیوتر ایران**، دانشگاه فردوسی مشهد،۱۳۸۱.

[۲۲] م. نیلی احمد آبادی، **بررسی نقش سیستم های چندعامله به منظور مدیریت امنیت** ، پایان نامهٔ کارشناسی ارشد، دانشگاه تهران، گروه مهندسی برق و کامپیوتر- هوش و رباتیک، ۱۳۸۰.

[23] P. D. Williams, "Warthog: Towards a Computer Immune System for Detecting “Low and Slow” Information System Attacks," M.S. thesis, AFIT/GCS/ENG/01M-15, Graduate School of Technology (AU) , Wright- Patterson AFB, OH, 2001.

[24] J. Kim and P. Bentley, "Toward an Artificial Immune System for Network Intrusion Detection: An Investigation of Clonal Selection With a Negative Selection Operator," *Proc. of Congress on Evolutionary Computation (CEC-2001),* Seoul, Korea, pp.1244-1252, 2001.

[25] K. P. Acchore, P. D. Williams, G. H. Gunsch, " The Computer Defense Immune System: Current and Future Research in Intrusion Detection," *Graduate School of Engineering and Management Air Force Institute of Technology*. 0-7803-7282-4/02/$10.0,IEEE, 2002.

[26] P. D. Williams, *Toward an Artificial Immune System for detecting Low and Slow Information System Attacks*, M.S. thesis, Air Force Instite.Technol., Wright-Patterson AFB, OH, 2001.

[27] P. D. Williams, K. P. Anchor, J. L. Bebo, G. H. Gunsch, and Lamont, "CDIS: Toward a Computer Immune System for Detecting Network Instrusions, " *Proc. Foutth Int. Symp. Recent Advances in intrusion Detection*, pp.117-133, 2001.

[28] R. P. Lippmann, D. Fried, I. Graf, et al. "Evaluating Intrusion Detection Systems: The 1998 DARPA Off-Line Intrusion Detection Evaluation," in press Proceedings of the DARPA Information Survivability Conference & Exposition (DISCEX'00)

[29] Ns web page, http://www.isi.edu/nsnam/ns/, 2000.

[1] Artificial Immune System
[2] Computational Immune System
[3] Light Weight Intrusion Detection System
[4] Computer Defense Immune System
[5] Detector
[6] Artificial Recognition Ball
[7] Network Threshold Affinity

محمد حسین یغمایی مقدم درسال ۱۳۵۰ درشهر مشهد متولد گردید. ایشان مدرک کارشناسی مهندسی برق مخابرات را درسال ۱۳۷۲ از دانشکده مهندسی برق دانشگاه صنعتی شریف دریافت نمود. همچنین مدارک کارشناسی ارشد و دکترای تخصصی خود را دررشته مهندسی برق- مخابرات درسال های ۱۳۷۴ و ۱۳۷۸ از دانشکده مهندسی برق دانشگاه صنعتی امیرکبیر دریافت کرد. محمد حسین یغمایی از سال ۱۳۷۱ تا ۱۳۷۸ درمرکز تحقیقات مخابرات ایران درپروژه های متعددی همکاری داشته است. ایشان به مدت یک سال درمرکز تحقیقات تکنولوژی های شبکه شرکت NEC ژاپن دوره فرصت مطالعاتی خود را گذراند. دکتر محمد حسین یغمایی مقدم ازسال ۱۳۷۸ تاکنون عضو هیئت علمی گروه مهندسی کامپیوتر دانشگاه فردوسی مشهد بوده است و هم اکنون دانشیار این گروه می باشد. ایشان تاکنون حدود ۳۵ مقاله کنفرانس بین المللی داخلی و خارجی و ۱۰ مقاله ژورنال درمجلات علمی پژوهشی به چاپ رسانده است. همچنین ایشان نویسنده یک کتاب با عنوان شبکه های رایانه ای و اینترنت می باشد.
آدرس پست الکترونیکی عبارتست از:

hyaghmae@um.ac.ir

داوود ملکی فارغ التحصیل کارشناسی ارشد مهندسی کامپیوتر گرایش نرم افزار از دانشگاه فردوسی مشهد در سال ۱۳۸۳ می باشد. ایشان عنوان پایان نامه کارشناسی ارشد خود را درزمینه امنیت شبکه های کامپیوتری با استفاده از محاسبات نرم و الگوریتم های تکاملی با راهنمایی آقایان دکتر محمد حسین یغمایی و دکتر محمد رضا اکبرزاده به پایان رسانید. مهندس داوود ملکی از سال ۱۳۸۳ با مرکز تحقیقات مخابرات ایران درپروژه های مرتبط با امنیت شبکه همکاری داشته است و هم اکنون نیز به عنوان پژوهشگر دراین مرکز مشغول به فعالیت می باشد.

محمد رضا اکبرزاده توتونچی عضو ارشد IEEE و استادیار گروه مهندسی برق دانشگاه فردوسی مشهد می باشد. درطی سال های ۱۳۷۵ تا ۱۳۸۱ ایشان دردانشگاه نیومکزیکو با سازمان ناسای آمریکا همکاری داشته است و درسال ۱۳۷۷ مدرک دکترای خود را درزمینه بهینه سازی تکاملی وکنترل فازی سیستم های پیچیده از این دانشگاه دریافت نمود. ایشان تاکنون چندین حکم دریافت نموده اند که برخی از آنها عبارتنداز: حکم شایستگی فرصت تحصیلی ISDB درسال ۱۳۸۴، عضو هیئت علمی برجسته در حمایت از فعالیت های علمی دانشجویان درسال ۱۳۸۲، عضو هیئت علمی برجسته درسال ۱۳۸۰ و فارغ التحصیل برجسته تحصیلات تکمیلی درسال ۱۳۷۷. علاقه تحقیقاتی ایشان شامل : الگوریتم های تکاملی، کنترل و منطق فازی، محاسبات نرم، سیستمهای چند عامله، سیستمهای پیچیده و رباتیک می باشد. ایشان بیش از ۱۲۰ مقاله درزمینه های تحقیقاتی فوق منتشر نموده اند. دکتر اکبرزاده درحال حاضر در حال گذراندن فرصت مطالعاتی در دانشگاه برکلی آمریکا می باشند.
آدرس پست الکترونیکی عبارتست از:

akbarzadeh@ieee.org