سیستم تشخیص تهاجم مبتنی بر شبکه عصبی ART

رسول جلیلی
دانشکده مهندسی کامپیوتر
دانشگاه صنعتی شریف تهران
تلفن: ۶۱۶۴۶۱۷-۲۱-۹۸+
jalili@sharif.edu

مرتضی امینی
دانشکده مهندسی کامپیوتر
دانشگاه صنعتی شریف تهران
تلفن: ۶۱۶۴۶۳۲-۲۱-۹۸+
m_amini@ce.sharif.edu

چکیده : در این مقاله یک سیستم تشخیص تهاجم مبتنی بر شبکه‌های عصبی بدون سرپرست با نام UNNID معرفی می‌گردد که قادر به شناسایی و تشخیص حملات و تهاجم‌های روی‌داده در شبکه‌های کامپیوتری می‌باشد. این سیستم امکان آموزش، تست، تنظیم و به‌کارگیری شبکه‌های عصبی بدون سرپرست را در یک سیستم تشخیص تهاجم فراهم می‌آورد. با استفاده از این سیستم، کارایی دو نوع شبکهٔعصبیART با نامهای ART-1 وART-2 در تشخیص تهاجم مورد ارزیابی قرار گرفت و با نتایج حاصله از به‌کارگیری شبکهٔ عصبی خودسازماندهSOM در این سیستم، مقایسه گردید. نتایج حاصله نشان داد که شبکه‌های ART قادر به دسته‌بندی درست بیش از ۹۰ درصد ترافیک شبکه به دسته‌های نرمال و حمله می‌باشند. از آنجاییکه در طراحی سیستمUNNID از ترکیب روشهای تشخیص سوءاستفاده و تشخیص ناهنجاری استفاده شده است، لذا قادر است نه تنها حملات شناخته شده بلکه حملات جدید ناشناخته، که نوعی ناهنجاری محسوب می‌شوند، را نیز شناسایی نماید.

کلمات کلیدی: *امنیت کامپیوتر، تشخیص تهاجم، شبکه عصبی بدون سرپرست، شبکه ART.*

۱- مقدمه

یکی از ابزارهای مهم در تامین امنیت شبکه‌های کامپیوتری، سیستمهای تشخیص تهاجم یا IDS[۱]ها می‌باشند،که با تحلیل داده‌های ممیزی سیستمها و یا شبکه، بروز تهاجم و یا حمله را تشخیص می‌دهند. سیستمهای تشخیص تهاجم بر اساس منبع تامین کنندهٔ داده‌های ورودی، به دو دستهٔ سیستمهای IDS مبتنی بر میزبان و سیستمهای IDS مبتنی بر شبکه تقسیم می‌گردند. بر اساس روش تحلیل و تشخیص نیز این سیستمها به دو دستهٔ اساسی سیستمهای تشخیص سوءاستفاده و سیستمهای تشخیص ناهنجاری تقسیم می‌شوند. سیستمهای تشخیص سوءاستفاده، با داشتن اطلاع از الگوهای حمله، به تشخیص حملات شناخته شده می‌پردازند، درحالیکه سیستمهای تشخیص ناهنجاری ابتدا نمایه‌هایی از رفتارهای نرمال و هنجار (از سیستم، شبکه و یا کاربران آن) را تشکیل داده، سپس هرگونه تخطی و یا انحراف از این نمایه‌های نرمال را به عنوان رفتاری ناهنجار و مهاجمانه تلقی می‌نمایند [۳، ۱۲].

یکی از روشهای مطرح در تشخیص تهاجم، بهره‌گیری از شبکه‌های عصبی مصنوعی می‌باشد و در سالهای اخیر بسیاری از کارهای انجام شده در زمینهٔ تشخیص تهاجم، بر روی این موضوع تمرکز نموده‌اند. سیستمهای تشخیص تهاجم مبتنی بر شبکه‌های عصبی ابتدا بر اساس رفتارهای نرمال و یا حمله و یا ترکیبی از هر دوی آنها آموزش یافته،

۱- Intrusion Detection System

سپس جهت تشخیص تهاجم به کار برده می‌شوند. در IDSهای تولید شده تاکنون، هر دو نوع شبکه‌های عصبی با سرپرست و شبکه‌های عصبی بدون سرپرست به کار برده شده‌اند. با وجود اینکه در سیستمهای IDS، شبکه‌های عصبی با سرپرست از دقت بیشتری نسبت به شبکه‌های عصبی بدون سرپرست برخوردار می‌باشند، ولی با گذشت زمان برای بهبود و ارتقاء سطح تشخیص حملات در شبکه‌های با سرپرست، لازم است که این شبکه‌ها با کل داده‌های قبلی به انضمام داده‌های جدید آموزش مجدد بیابند که این امر هزینهٔ بسیار بالایی را در پی خواهد داشت، لذا شبکه‌های بدون سرپرست، که همواره می‌توانند خود را با وضعیت و داده‌های جدید سازگار نمایند، مورد توجه خاصی در این کاربرد قرار گرفته‌اند [۴].

شبکه عصبی ART یکی از انواع شبکه‌های عصبی است که می‌تواند به صورت بدون سرپرست آموزش یابد و به صورت کارایی به دسته‌بندی و کلاستربندی داده‌های ورودی بپردازد. در این تحقیق با توجه به قابلیتهای شبکه‌های عصبی بدون سرپرست، یک سیستم تشخیص تهاجم مبتنی بر این نوع از شبکه‌های عصبی با نام UNNID طراحی گردید. سیستم UNNID قابلیت استفاده از انواع شبکه‌های عصبی بدون سرپرست را داشته و از انعطاف‌پذیری مطلوبی جهت تغییر ساختار و پارامترهای مطرح در هر کدام از انواع این شبکه‌ها برخوردار است. در این مقاله سعی بر معرفی این سیستم و نحوهٔ به کارگیری شبکه‌های ART (ازجمله ART-1 و ART-2) در آن را داریم، تا بتوانیم ترافیک شبکه را به دسته‌های نرمال و حمله دسته‌بندی نموده و رویداد حملات از قبل شناخته شده، به همراه نوع آن و همچنین حملات ناشناختهٔ جدید را تشخیص دهیم. به منظور ارزیابی قابلیتهای شبکه‌های ART-1 و ART-2 و مقایسه با کارهای مشابهی که بیشتر بر روی شبکه‌های خودسازمانده SOM تمرکز نموده‌اند، از شبکهٔ SOM نیز در سیستم UNNID بهره برده و نتایج حاصله از شبکه‌های ART-1، ART-2 و SOM را با هم مقایسه نموده‌ایم.

در ادامهٔ مقاله در بخش ۲، کارهای مرتبط انجام شده در زمینهٔ استفاده از شبکه‌های عصبی در سیستمهای تشخیص تهاجم معرفی می‌گردند. در بخش ۳، معماری سیستم UNNID و مؤلفه‌های اصلی آن تشریح می‌گردند. در بخش ۴، به بیان مشخصات و ویژگیهای شبکه‌های عصبی ART و نحوهٔ به کارگیری آن در سیستمهای تشخیص تهاجم شبکه‌ای پرداخته می‌شود. در بخش ۵، نتایج آزمایشات و ارزیابیهای انجام شده بر روی سیستم تشخیص تهاجم مبتنی بر شبکه‌های ART-1 ، ART-2 و SOM و نتیجهٔ مقایسهٔ آنها با یکدیگر ارائه می‌گردد و نهایتاً در بخش ۶، جمع‌بندی و نتیجه‌گیری از مقاله و سوی کارهای آتی پروژه بیان می‌گردد.

۲- کارهای انجام شده در تشخیص تهاجم مبتنی بر شبکه‌های عصبی

از سال ۱۹۹۰ تاکنون تحقیقات زیادی بر روی به‌کارگیری شبکه‌های عصبی هم در سیستمهای تشخیص سوءاستفاده و هم در سیستمهای تشخیص ناهنجاری به انجام رسیده است. سیستمهای تشخیص تهاجم حاصله در طی این سالها را می‌توان بر اساس معیارهای مختلفی دسته‌بندی نمود، که اگر بخواهیم بر اساس نوع شبکهٔ عصبی به کار برده شده در آنها این دسته‌بندی را انجام دهیم، سه دسته را خواهیم داشت.

دستهٔ اول سیستمهایی هستند که بر اساس شبکه‌های عصبی پیشخور چند لایه (MLFF) و شبکه‌هایی همچون MLP وBP ایجاد شده‌اند، که به عنوان نمونه می‌توان به [۱، ۴، ۹، ۱۶] اشاره نمود.

دستهٔ دوم، سیستمهایی هستند که بر اساس شبکه‌های عصبی بازگشتی(recurrent) و شبکه‌های عصبی تطبیقی مانند ELMAN وCMAC بـنا شده‌اند و با دریافت بازخورد از خروجی شبکه و یا خود سیستم تحت حفاظت، همبستگی بین ورودیهـای فعلـی سیستم را با ورودیها و حالات قبلی آن، در خود حفظ می‌نمایند. نمونه‌هایی از سیستمهای این دسته در [۲، ۵، ۶] ارائه گردیده اند.

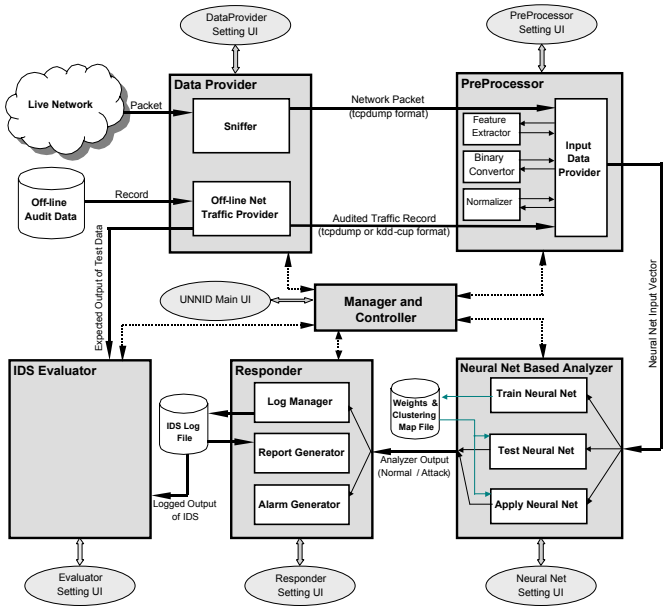
دسته سوم ، سیستم‌های تشخیص تهاجمی هستند که با استفاده از شبکه‌های عصبی بدون سرپرست، به دسته‌بندی و بصری‌سازی(visualization) ورودیهای سیستم و تفکیک رفتارهای نرمال از رفتارهای ناهنجار (که می توانند حمله باشند) می‌پردازند. اکثر سیستمهای دسته سوم از شبکه‌های خود سازمانده SOM استفاده نموده‌اند و تنها تعداد اندکی از آنها از روشهای دیگر بهره برده‌اند، که در ادامه به معرفی گزیده‌ای از سیستمهای این دسته خواهیم پرداخت. در سال ۱۹۹۰، Fox [۸] اولین فردی بود که از شبکه SOM برای مشخص نمودن حالت نرمال ماشین و سپس تشخیص سوء استفاده‌های تاثیرگذار بر پردازه‌ها و منابع سیستم استفاده نمود. Cannady در [۱۷] نیز از شبکه‌هایSOM چندگانه برای تشخیص تهاجم استفاده نموده است. در این سیستم پردازش و تحلیل ترافیک شبکه بر عهدهٔ مجموعه‌ای از نقشه‌های کوهنن می‌باشد که هر نقشه موظف است بسته‌های مربوط به یک پروتکل خاص شبکه را تحلیل نماید. Gardian در [۱۰] از SOM برای بصری‌سازی فعالیت شبکه استفاده نمود و بدین ترتیب راه جدیدی را برای مدیران شبکه جهت کاوش، پیگیری و تحلیل مهاجمان، با تکیه بر فاکتورهای انسانی، فراهم نموده است. Jrapummin در [۱۱] نیز متدلوژی دیگری را جهت بهره‌گیری از شبکه‌های عصبی ترکیبی پیشنهاد نموده که در آن از شبکه SOM برای بصری‌سازی تهاجمات شبکه و از شبکه RPROP برای دسته بندی تهاجمات استفاده می‌گردد.

تعداد کثیری از تحقیقات جدید انجام شده در دسته سوم سعی نموده‌اند که چند شبکه عصبی بدون سرپرست را به‌طور توام در یک سیستم تشخیص تهاجم و در ساختاری سلسله مراتبی به کار برند تا بدین‌ترتیب به دقت بیشتر و نتایج بهتری دست یابند. از این جمله در [۲۰] یک سیستم تشخیص تهاجم سلسله مراتبی به نام HIDE معرفی شده است که قادر است با پیش پردازش آماری و دسته بندی مبتنی بر شبکه عصبی به تشخیص حملات شبکه‌ای بپردازد. با استفاده از این سیستم، پنج نوع مختلف شبکه‌های عصبی (به عنوان دسته بندی کننده)، در تشخیص تهاجم به کاربرده شده و کارایی آنها در تشخیص تهاجم با یکدیگر مقایسه گردیده است. در [۱۵] نیز از شبکهSOM به صورت سلسله مراتبی در ساختاری دولایه برای تشخیص تهاجم استفاده شده است. تاکید این سیستم، بیشتر برروی در نظر گرفتن زمان و توسعه تدریجی سلسله مراتب در آن می‌باشد. سیستمی که در [۱۳] تحت عنوان NSOM تولید گردیده نیز از یک شبکه SOM ساختیافته برای دسته‌بندی بلادرنگ داده‌های یک شبکه اترنت و تشخیص حملات انکار سرویس (DoS) استفاده می‌نماید.

بررسی کارهای انجام شده در این زمینه نشان می‌دهد که تنها کارهای انجام شده در [۱۸] و[۲۰] از نوعی شبکه ART با سرپرست به نام Fuzzy ARTMAP استفاده نموده و آنرا مورد ارزیابی قرار داده‌اند و در هیچ یک از کارهای دیگر با وجود تمام قابلیتها و مزایای شبکه‌هایART در مقابل SOM، استفاده چندانی از این نوع شبکه عصبی به عمل نیامده است. تنها کاری که در آن از شبکه‌های ART بدون سرپرست (شبکه ART-2) آن هم به صورت غیر مستقیم در تشخیص تهاجم استفاده شده، مقاله مربوط به پایان نامه کارشناسی ارشدی است که در [۱۴] ارائه گردیده است. در سیستم ارائه شده در [۱۴]، از متدهای آماری برای تشخیص ناهنجاری استفاده می‌شود. در این سیستم نمایه هر کاربر فعال با نمایه‌های تاریخی نرمال کاربران مقایسه می‌گردد و در صورتی که با نمایه نرمال مربوط به همان کاربر تطابق داشته باشد، کاربری مجاز و نرمال تشخیص داده می‌شود و در غیر اینصورت ناهنجار تلقی می‌گردد. در این سیستم به‌منظور بهبود تشخیص هویت کاربران، از شبکه ART-2 برای دسته بندی کاربران براساس نمایه‌های مربوط به فرامین صادره از سوی آنها، استفاده شده است که بدین شکل نرمال بودن و یا نبودن کاربر با تطابق یا عدم تطابق آن با کلاستر مربوط به نمایهٔ آن کاربر تعیین می‌گردد.

۳- معماری سیستم UNNID

معماری و مولفه‌های اصلی سیستم UNNID در شکل ۱ نشان داده شده است. این سیستم به گونه‌ای طراحی شده



شکل ۱. معماری سیستم تشخیص تهاجم مبتنی بر شبکه‌های عصبی بدون سرپرست UNNID

است کـه اولا امکان آموزش، تست، تنظیم و ارزیابی شبکه‌های عصبی بدون سرپرست مختلف را برای تشخیص تهاجم فـراهم آورد و ثانـیا امکـان بـه‌کارگـیری شبکه‌های عصبی بدون سرپرست را جهت تحلیل ترافیک شبکه هم به صورت بـرخط و بلادرنـگ و هم به صورت برون از خط و غیر بلادرنگ با دسته بندی ترافیک شبکه به دو دسته نرمال و حمله فراهم نماید. سیستمUNNID می‌تواند در چهار مد مختلف مورد استفاده قرار گیرد: ۱) مد آموزش برون از خط، ۲) مد تسـت بـرون از خـط، ۳) به عنوان یکIDS واقعی در حالت برون از خط و ۴) به عنوان یکIDS واقعی در حالت برخط. در ایـن مقالـه، سـعی بر استفاده از سیستم UNNID برای آموزش و تست و تنظیم شبکه‌های عصبی ART و SOM و بررسـی قابلیتهای شبکه‌های ART، را داریم، لذا در ادامه به بیان جزئیات عملکرد هر یک از مولفه‌های فوق در راستای هدفمان خواهیم پرداخت.

۳-۱- Data Provider (فراهم کنندهٔ داده‌ها): این مولفه خـود دارای دو زیر مولفه دیـگر می‌باشـد: یکی Sniffer و دیگـریOff-line Net Traffic Provider. زیر مولفه Sniffer در مد برخط استفاده شده و می‌تواند با گوش دادن به یک شـبکه فعال بسته‌های شبکه را (با فرمت tcpdump) جمع‌آوری و در صورت لزوم فیلتر نماید. زیر مولفه Off-line Net Traffic Provider نیـز وظیفـه مدیـریت فایـلهای ممیـزی (با فرمت tcpdump و یا kddcup) را برعهـده دارد. در این بررسی از مجمـوعه داده‌هـایKDD Cup's 99 که دارای فـرمت kddcup می‌باشـند، جهت آمـوزش و تست شـبکه‌های عصبی استفـاده شده است. داده‌های KDD Cup's 99 یک مجمـوعه دادهٔ استاندارد برای ارزیابی سیستمهای تشخـیص تهاجم می‌باشد که در سال ۱۹۹۹فراهم گردیده است. این مجموعه، شامل اطلاعات اتصالات شبکه محلی نیروی هوایی آمـریکا بـه انضـمام انـواع گسترده‌ای از تهاجمات شبیه‌سازی شده می‌باشد. برای هر اتصال در این مجموعه داده‌ها، ۴۱ مشخصـه تعـریف گـردیده که این مشخصه‌ها به ۴ دستهٔ مشخصه‌های اولیه TCP، مشخصه‌های محتوایی، مشخصه‌های ترافیک مبتنی بر زمان و مشخصه‌های ترافیک مبتنی بر میزبان تقسیم بندی می‌شوند [۱۵]. هر اتصال دارای برچسبی اسـت که مشخص می‌کند اتصال مذکور نرمال است و یا یکی از انواع حملات. این مجموعه داده‌ها شامل ۲۴ نوع حمله شـناخته شـده مختلف در داده‌های آموزشی و همچنین ۱۴ نوع حمله ناشناخته اضافی دیگر است که فقط در داده‌های تست گنجانده شده‌اند. کل این حملات به ۴ دسته زیر قابل تقسیم می‌باشند[۲۱]:

- حملات انکار سرویس (DoS): که در آن درخواستهای مشروع کاربر توسط سیستم برآورده نمی‌شوند.
- حملات از راه دور (R2L): که در آن از یک ماشین راه دور دسترسیهای غیرمعتبر به یک سیستم محلی

صورت می‌پذیرد.

- حملات کاربر به ریشه (U2R): که در آن با تصاحب مجوزهای کاربر ریشه، دسترسیهای غیر معتبر و غیر مجاز به سیستم صورت می‌پذیرد.
- حملات پویش(probe): که شامل بررسی و پویش بر روی سیستم برای یافتن راههای نفوذ به آن می‌باشد.

بـرای آمـوزش سیستم UNNID، ۱۰۰۰۰ اتصال از مجموعه داده‌های آمـوزشی KDD Cup's 99 به صورت تصادفی به گونـه‌ای انـتخاب شـد کـه شـامل ۲۲ نـوع حملـه شـناخته شده باشد و برای تست نیز ۵۰۰۰ اتصال از میان مجموعه داده‌هـای تست به گونه‌ای انتخاب شد که شامل ۲۲ نوع حمله موجود در مجموعه داده‌های آموزشی به انضمام ۱۴ نوع حمله جدید ناشناخته باشد.

۳-۲- PreProcessor (پیش‌پردازنده): وظیفهٔ پیش‌پردازنده دریافت داده‌های مربوط به ترافیک شبکه از مولفهٔ Data Provider، استخراج مشخصه‌های مناسب و تبدیل مشخصه‌ها به فرمت عددی مناسب جهت ورود به سنسورهای ورودی شبکهٔ عصبی در مولفهٔ Neural Net Based Analyzer می‌باشد. داده‌های ورودی به شبکهٔ عصبی بر حسب نوع شبکهٔ عصبی می‌توانند به یکی از دو شکل باینری و یا پیوسته باشند. لذا در پیش‌پردازنده پس از تبدیل مشخصه‌ها از فرمت متنی به فرمت عددی، مسالهٔ اصلی تبدیل داده‌ها به فرم باینری و یا به فرم پیوستهٔ نرمال شده، می‌باشد. برای نرمال سازی مشخصه‌ها، ابتدا یک بررسی آماری بر روی هر یک از مشخصه‌ها بر اساس داده‌های موجود از KDD Cup's 99 صورت پذیرفت و یک مقدار ماکزیمم برای مقادیر هر مشخصه تعیین گردید. سپس بر اساس فرمول سادهٔ زیر این نرمال سازی در بازهٔ[1 , 0] انجام پذیرفت.

$$\begin{aligned} &If\ (f > MaxF) \quad Nf=1; \\ &Otherwise \quad Nf = (f / MaxF) \end{aligned} \qquad \text{(فرمول ۱)}$$

(مقدار نرمال شده یا محدود شدهF :*Nf* ، ماکزیمم مقدار قابل قبولF :*MaxF*، مقدار مشخصه :*f* ، مشخصه :*F*)

جهت تبدیل مشخصه‌ها به فرم باینری، در صورتیکه بازهٔ تغییرات مقادیر مشخصه موردنظر کم و نوع آن نیز عدد صحیح باشد، این تبدیل مستقیماً از دهدهی به باینری انجام می‌پذیرد. در غیر اینصورت بازهٔ [0,MaxF] بر اساس میزان پراکندگی مقادیر مشخصه F، به زیر بازه‌هایی تقسیم می‌گردد و به هرکدام از این زیربازه‌ها یک کد باینری اختصاص می‌یابد. سپس مقدار مشخصه F در هر زیربازه‌ای که قرار گیرد، کد باینری آن زیربازه به آن نسبت داده می‌شود. قاعدتاً هرچه این زیربازه‌ها کوچکتر و تعدادشان بیشتر گردد، دقت سیستم نیز افزایش خواهد یافت. ولی این افزایش دقت، افزایش تعداد ورودی باینری شبکهٔ عصبی را به دنبال دارد که این مساله نیز منجر به افزایش زمان آموزش و همچنین زمان پاسخ شبکه می‌گردد. شاید بهترین راه تقسیم این بازه به زیربازه‌های کوچکتر این باشد که در قسمتهایی که تراکم مقادیر بیشتر است، از تفکیک پذیری بالاتر و زیربازه‌های کوچکتر استفاده شود و دربقیهٔ قسمتها، از تفکیک‌پذیری پایین‌تر و زیربازه‌های بزرگتر استفاده گردد. با فرض نرمال بودن توزیع مقادیر یک مشخصه، می‌توان محل تجمع بیشتر مقادیر را در محدودهٔ [Fm-δ , Fm+δ] (که Fm میانگین مقادیر مشخصه F وδ انحراف معیار آن می‌باشد) در نظر گرفت.

مولفهٔ پیش‌پردازنده علاوه بر امکان پیش‌پردازش داده‌های kddcup، امکان پیش‌پردازش سرآیند بسته‌های با فرمت tcpdump و همچنین تبدیل بسته‌های با فرمت tcpdump به اتصالات شبکه با فرمت kddcup را نیز دارا می‌باشد که در این کار، ما از این قابلیتها استفاده‌ای ننموده‌ایم.

۳-۳- Neural Net Based Analyzer (تحلیلگر مبتنی بر شبکهٔ عصبی): این مؤلفه مهمترین مؤلفهٔ سیستم UNNID می‌باشد که وظیفهٔ تحلیل و تشخیص تهاجم را با استفاده از شبکهٔ عصبی در زمان کاربرد به عهده دارد. این

مؤلفه امکان آموزش شبکه‌های عصبی بدون سرپرست وتست آنها را قبل از بکارگیری نیز فراهم می‌نماید. داده‌های ورودی به این مؤلفه از مؤلفهٔ پیش‌پردازنده به صورت بردارهای عددی فراهم و خروجی حاصله نیز به مؤلفهٔ Responder ارسال می‌گردد. لازم به ذکر است که شبکه‌های عصبی بدون سرپرست با توجه به شباهت بین داده‌های ورودی، می‌توانند آنها را دسته‌بندی نمایند، که در این کاربرد نیز هدف ما، استفاده از این نوع شبکه‌های عصبی در دسته‌بندی ترافیک شبکه به دو دستهٔ نرمال و تهاجمی می‌باشد. یکی از انواع شبکه‌های عصبی بدون سرپرست، شبکه‌های عصبی ART می‌باشد، که در بخش ۴ به تشریح بیشتر خصوصیات این نوع شبکه‌های عصبی و نحوهٔ به کارگیری آنها در تشخیص تهاجم خواهیم پرداخت. در این مقاله جهت ارزیابی کارایی شبکهٔ ART در مقایسه با شبکهٔ خودسازمانده SOM که در بسیاری از کارهای قبلی از آن استفاده شده است، شبکهٔSOM نیز در تحلیلگر سیستم استفاده شده و کارایی آن مورد ارزیابی قرار گرفته است.

۳-۴- Responder (پاسخ‌ده): وظیفهٔ این مؤلفه پاسخ‌دهی سیستم تشخیص تهاجم بر اساس خروجی دریافتی از مؤلفهٔ تحلیلگر سیستم می‌باشد. برای این منظور این مؤلفه امکاناتی جهت رویدادنگاری، تولید هشدار به گونه‌های مختلف (از جمله ارسال e-mail، نمایش پیغام بر روی صفحه و...) و همچنین تولید گزارشهای مختلف را در خود دارا می‌باشد.

۳-۵- IDS Evaluator (ارزیاب سیستم تشخیص تهاجم): این مؤلفه جهت ارزیابی عملکرد سیستم تشخیص تهاجم در طی تست آن، در این معماری گنجانده شده است. ارزیاب سیستم، با مقایسهٔ خروجی حاصله از سیستم در زمان تست با خروجی مورد انتظار آن (که در مجموعه داده‌های آموزشی مشخص گردیده است)، معیارهای ارزیابی زیر را استخراج می‌نماید:

- درصد تشخیص صحیح نوع (تفکیک صحیح ترافیک نرمال از حمله و تشخیص صحیح نوع حملهٔ شناخته شده در موارد رویداد آن) که به اختصار آن را ETTR نامیم؛
- درصد تشخیص درست (تنها تفکیک صحیح ترافیک نرمال از حمله بدون در نظر گرفتن نوع حملهٔ تشخیص داده شده) که به اختصار آن را TR گوییم.
- درصد خطای مثبت غلط (تشخیص حمله درحالیکه حمله‌ای روی نداده) که به اختصار آن را FPR گوییم؛
- درصد خطای منفی غلط (عدم تشخیص حمله در زمان بروز حمله) که به اختصار آن را FNR گوییم.

۴- دسته‌بندی کننده مبتنی بر شبکهٔ ART

شبکه عصبی ART در سال ۱۹۷۶ توسط Stephan Grossberg بنا نهاده شد. بعد از آن اشکال و مدلهای مختلفی از شبکه ART هم از نوع با سرپرست و هم از نوع بدون سرپرست ابداع و ایجاد شد. از انواع شبکه‌های ART بدون سرپرست می‌توان به ART-1، ART-2، ART-3 و Fuzzy ART اشاره نمود [۱۹] و از انواع شبکه‌های ART با سرپرست که پسوند "MAP" نیز معمولاً دارند، می‌توان به ARTMAP، Fuzzy ARTMAP و Gussian ARTMAP اشاره نمود [۱۹]. تمرکز اصلی این مقاله بر روی شبکه‌های ART بدون سرپرست می‌باشد که قبل از انواع با سرپرست آن توسعه یافته‌اند. در شبکه‌های ART بدون سرپرست، الگوهای ورودی ممکن است چندین بار و با ترتیب مختلف به شبکه داده شوند. در هربار که یک الگو به عنوان ورودی به شبکه داده می‌شود، یک واحد کلاستر مناسب انتخاب و وزنهای مربوط به آن تغییر می‌یابند. در این شبکه‌ها انتخاب واحد برنده بر اساس تفاضل مطلق بردارها (که در شبکه‌های SOM مطرح است) نبوده، بلکه شباهت نسبی بردار ورودی با بردار وزن یک واحد کلاستر، معیار انتخاب واحد برنده می‌باشد [۷].

شبکه‌های ART به گونه‌ای طراحی شده‌اند که به کاربر این امکان را می‌دهند که درجهٔ شباهت الگوهایی که در یک

کلاستر قرار می‌گیرند را با تنظیم پارمتر vigilance کنترل نماید. همچنین در این شبکه‌ها نیازی نیست که تعداد کلاسترها از قبل تعیین شده باشد و می‌توان در آنها از پارمترvigilance برای تعیین تعداد مناسب کلاسترها استفاده نمود. چرا که هر چه این پارامتر افزایش یابد، تعداد کلاسترها نیز افزایش و هر چه کاهش یابد، تعداد کلاسترها نیز کاهش می‌یابد. قاعدتاً در این کاربرد، تعداد کلاسترها باید به اندازه‌ای تعیین گردد که انواع حملاتی که تا حدودی شبیه به هم هستند در یک کلاستر یکسان قرار نگیرند. علاوه بر خصوصیت اساسی فوق، شبکه‌های ART دو خصوصیت مهم دیگر را نیز دارا می‌باشند که عبارتند از:

۱. پایداری(stability): یعنی عدم نوسان یک الگو در مراحل مختلف آموزش بین کلاسترهای مختلف.
۲. انعطاف‌پذیری (plasticity) : یعنی توانایی شبکه در یادگیری الگوهای جدید در هر یک از مراحل یادگیری.

پایداری و انعطاف‌پذیری شبکه‌های ART و قابلیت آنها در دسته‌بندی الگوهای ورودی با میزان شباهت تحت کنترل کاربر، آنها را مناسب‌تر از سایر شبکه‌های عصبی بدون سرپرست برای استفاده در سیستمهای تشخیص تهاجم نموده است. برای این منظور در این مقاله دو نوع از شبکه‌های ART با نامهای ART-1 و ART-2 به کار برده شده‌اند که شبکه ART-1 اولین شبکهٔ مطرح در مجموعه شبکه‌های ART بوده و تنها ورودی باینری می‌پذیرد و شبکه ART-2 نیز شبکه‌ای است مشابه ART-1 که بردارهای با مقادیر پیوسته را نیز می‌پذیرد.

در سیستم UNNID، بردار ورودی مناسب (بردار باینری برای ART-1 و بردار با مقادیر پیوسته نرمال شده برای ART-2) توسط مولفه پیش پردازنده (PreProcessor) فراهم شده و به شبکهٔ عصبی در مولفه Neural Net Based Analyzer داده می‌شود. در فاز آموزش، ابتدا داده‌های ورودی بدون توجه به ماهیت آنها (نرمال و یا حمله) توسط شبکه ART دسته‌بندی می‌گردند. بعد از اتمام آموزش، سیستم باید واحدهای مربوط به هر یک از کلاسترها را مشخص و با استفاده از برچسب داده‌های آموزشی نام مناسبی را به آنها اختصاص دهد. نام هر کلاستر معادل نام واحدهایش بوده و نام هر واحد معادل است با نوع اکثریت داده‌هایی که با اعمال آنها به ورودی سیستم، واحد مورد نظر به عنوان واحد برنده انتخاب گردیده است. نتیجه این کار ایجاد یک نقشه کلاستربندی (Clustering Map) است. دراین نقشه تعدادی از واحدها با یکدیگر تشکیل کلاستری را می‌دهند که بیانگر ترافیک نرمال است. تعدادی دیگر با یکدیگر تشکیل کلاستری را می‌دهند که بیانگر یکی از انواع حملات شناخته شده می‌باشد و بقیه نیز تشکیل کلاستری را می‌دهند که نه بیانگر ترافیک نرمال می‌باشد و نه نشانگر ترافیک حملات شناخته شده و لذا بیانگر ترافیک حملات جدید می‌باشد.

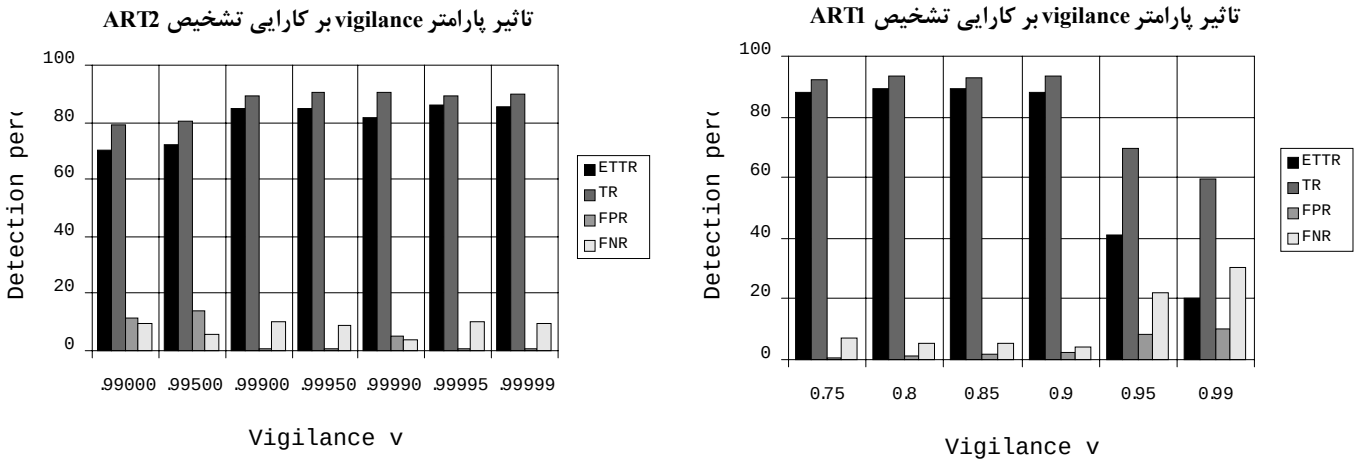
باتوجه به توضیح فوق برای آموزش تحلیلگر مبتنی بر شبکه عصبی نیاز داریم که از هر دو ترافیک نرمال و حمله، در این سیستم استفاده نماییم تا بوسیلهٔ آن توانایی تشخیص انواع حملات شناخته شده و همچنین حملات جدید روی‌داده در شبکه را داشته باشیم. بنابراین سیستم UNNID دو روش تشخیص سوء استفاده و تشخیص ناهنجاری را با به‌کارگیری شبکه‌های عصبی بدون سرپرست با یکدیگر ترکیب نموده است و لذا می‌تواند مزایا و فواید هر دو روش را در تشخیص حملات شناخته شده و حملات جدید درخود دارا باشد.

۵- نتایج آزمایشات

پیاده‌سازی سیستم UNNID، تحت سیستم عامل RedHat Linux 9.0 و با استفاده از زبان C++ انجام پذیرفته است. برای ارزیابی شبکه‌های ART وSOM با استفاده از این سیستم، ابتدا مقادیر پارامترهای مهم شبکه‌های عصبی (ازجمله تعداد واحدهای لایهٔ خروجی، تعداد دفعات تکرار بردارهای ورودی در آموزش شبکه و پارامتر vigilance در شبکه‌های ART) تعیین گردید و سپس قابلیتهای این شبکه‌ها از جنبه‌های مختلف با یکدیگر مقایسه شدند. با بررسی‌های انجام

شـده، تعداد واحدهای لایهٔ خروجی در شبکهٔ ART-1 برابر با ۲۵۰۰، در ART-2 برابر با۵۰۰ و در SOM برابر با ۲۵۰۰ عـدد انـتخاب گـردید. تعـداد دفعـات تکـرار بردارهای ورودی در مرحلهٔ آموزش نیز برای هر سه شبکه، ۱۰۰ بار تعیین گـردید. لازم بـه ذکـر است که برای تعیین مقادیر فوق در شبکهART-1، مقدار پارامتر vigilance برابر ۰/۹ و در شبکهٔ ART-2 مقـدار آن برابـر۰/۹۹۹ در نظـر گرفـته شـد. در شبکهٔ SOM نیز واحدهای لایهٔ خروجی به صـورت دوبعدی با همسـایگی مربعـی در نظر گرفته شدند و برای ضریب یادگیری و شعاع همسایگی نیز به ترتیب مقادیر ۰/۸ و ۷ در نظر گرفته شد.

بـرای تعییـن مقـدار مناسـب پارامـتر vigilance و همچنیـن بررسی تاثیر آن در کارایی شبکه‌های ART در تشخیص تهاجم، سیستم موردنظر با مقادیر vigilance مختلف آموزش داده شد و هر یک از معیارهای ETTR، TR، FPR، FNR در آنها مورد محاسبه قرار گرفت که نتایج حاصله از این آزمایشات در شکل ۲ آمده است.



شکل ۲. ارزیابی کارایی شبکه‌های ART در تشخیص تهاجم و تاثیر پارامتر vigilance برکارایی آنها

بررسـی نمودارهـای شکل ۲ نشان می‌دهدکه بالاترین کارایی در تشخیص ترافیک نرمال از حمله، در شبکهٔ ART-1، با مقـدار ۰/۹ بـرای پارامتر vigilance و در شبکهٔART-2 با مقدار ۰/۹۹۹۵ برای این پارامتر حاصل گردیده است. پس از تعییـن مقادیر مناسب برای پارامترها، کارایی شبکه‌هایART با نتایج حاصله از بکارگیری شبکه‌های SOM در سیستم UNNID مقایسه گردید، که نتایج آن به طور خلاصه در جدول ۱ نشان داده شده است.

بـرای هر یک از شبکه‌های ART-1، ART-2 و SOM، میزان تشخیص صحیح هر یک از ۴ دسته حملات DoS، U2R، R2L و Probe نـیز مـورد محاسـبه قرار گرفت و با بهترین نتیجه‌ای که در [۱۸] با استفاده از روشهای یادگیری ماشین

جدول ۱. کارایی شبکه‌های ART با پارامترهای مناسب در مقایسه با کارایی شبکهٔ SOM.

	ETTR	*TR*	*FPR*	*FNR*
UNNID ART-1	89.26	93.14	1.64	5.22
UNNID ART-2	84.88	90.40	0.74	8.86
UNNID SOM	87.64	92.64	0.96	6.40

جدول ۲. درصد تشخیص شبکه‌هایART وSOM به تفکیک نوع حمله در مقایسه با بهترین نتیجهٔ حاصله در [۱۸].

	DoS	*R2L*	*U2R*	*Probe*
UNNID ART-1	100	88.69	17.41	99.48
UNNID ART-2	96.17	36.31	10.71	96.88
UNNID SOM	99.04	53.57	12.50	93.23
Best result of [18]	97.3	9.6	29.28	88.7

حاصل گردیده، مقایسه گردید. نتایج نشان می‌دهد که هر دوشبکهٔ ART-1 وART-2 قادرند به خوبی حملات DoS و Probe را تشخیص دهند ولی شبکهٔART-2 قادر نیست به خوبی حملاتR2L را تشخیص دهد و در مورد حملات U2R نیز توانایی این دوشبکه همانند همهٔ روشهای تشخیص تهاجم شبکه‌ای چندان قابل قبول نیست.

مقایسهٔ بین شبکه‌های ART-1، ART-2 و SOM نشان می‌دهد که شبکهٔART-1 در بین سه شبکهٔ فوق بالاترین کارایی را در تشخیص تهاجم دارامی‌باشد، ولی با در نظر گرفتن زمان پاسخ، شبکهٔART-2، ۸ تا ۱۰ برابر سریعتر از شبکه‌هایART-1 و SOM می‌باشد که این ویژگی آن را برای سیستمهای IDS بلادرنگ بسیار مناسب می‌نماید.

۶- نتیجه گیری

در این مقاله یک سیستم تشخیص تهاجم مبتنی بر شبکه‌های عصبی بدون‌سرپرست با نام UNNID معرفی گردید. با معرفی معماری و نحوهٔ عملکرد مؤلفه‌های این سیستم، توانایی و انعطاف پذیری این سیستم در بکارگیری انواع شبکه‌های عصبی بدون سرپرست، تشریح گردید. جهت ارزیابی کارایی شبکه‌های عصبی ART در تشخیص تهاجم از سیستمUNNID برای تنظیم، آموزش و تست دو نوع معروف از شبکه‌های ART با نامهای ART-1 و ART-2 بهره گرفته شد و نتایج حاصل از ارزیابی آنها با نتایج حاصل از بکارگیری شبکهٔ خودسازمانده SOM مقایسه گردید. نتایج نشان داد که شبکهٔART-1 در بیش از ۹۳ درصد موارد و ART-2 در بیش از ۹۰ درصد موارد قادر به تفکیک صحیح ترافیک نرمال از حمله می‌باشند، که در مقایسه باART-1،SOM کارایی بیشتر وART-2 کارایی کمتری را از خود نشان می‌دهند. ولی آنچه که موجب برتری ART-2 نسبت بهART-1 و SOM می‌گردد، سرعت بسیار بالا و زمان پاسخ بسیار کم آن است، که همین ویژگی آن را برای IDSهای بلادرنگ در شبکه‌های کامپیوتری با ترافیک بالا مناسب می‌نماید.

بکارگیری شبکه‌های عصبی بدون سرپرست در تشخیص تهاجم، مزایای زیادی نسبت به نوع باسرپرست آن دارد که دلیل اصلی آن قابلیت این نوع شبکه‌ها در یادگیری مستمر و تطابق با داده‌های جدید، بدون نیاز به آموزش مجدد (با کل داده‌های قدیم و جدید) می‌باشد. لذا با تجربهٔ حاصله از این کار، در مرحلهٔ بعد از تحقیقمان قصد داریم، از یک دسته‌بندی کنندهٔ چندگانه که ترکیبی از چند شبکهٔ عصبی بدون سرپرست می‌باشد، به گونه‌ای استفاده نماییم که هر یک از آنها با توجه به قابلیتشان، بخشی از ترافیک شبکه را جهت کشف حملات، مورد تحلیل و دسته‌بندی قرار دهند.

۷- سپاسگزاری

در اینجا لازم است از جناب آقای دکتر باقری از دانشگاه صنعتی شریف، که ما را در مراحل مختلف این پروژه یاری نموده‌اند و همچنین بانک رفاه و مرکز تحقیقات مخابرات ایران که بخشی از پشتیبانی مالی این پروژه را تقبل نموده‌اند، تشکر و قدردانی نماییم.

۸- مراجع

[1] Bonifacio, J.M., "Neural Networks Applied in Intrusion Detection Systems", Neural Networks Proceedings, IEEE World Congress on Computational Intelligence, vol. 1, pp. 205-210, 1998

[2] Cannady, J., "Applying CMAC-based Online Learning to Intrusion Detection", Neural Networks, Proceeding of the IEEE-INNS-ENNS International Joint Conference, vol. 5, pp. 405-410, 2000

[3] Coolen, R. and Luiijf, H.A.M., "Intrusion Detection: Generics and State-of-the-Art", Research and Technology Organization (RTO) Technical Report 49, 2002

[4] Cannady, J., "Artificial Neural Networks for Misuse Detection", In Proceedings of National Information Systems Security Conference, 1998

[5] Debar, H. and Dorizzi, B., "An Application of Recurrent Network to An Intrusion Detection System", In Proceeding of the International Joint Conference on Neural Networks, pp. 478-483, 1992
[6] Debar, H., Becker, M. and Siboni, D., "A Neural Network Component for An Intrusion Detection System", IEEE Computer Society Symposium, pp. 240-250, 1992
[7] Fausett, L., "Fundamentals of Neural Networks", Prentice-Hall, 1994
[8] Fox Kevin, L., Henning Rhonda, R. and Reed Jonathan, H., "A Neural Network Approach Towards Intrusion Detection", In Proceeding of 13th National Computer Security Conference, 1990
[9] Ghosh, A. K. and Schwartzbard, A., "A Study in Using Neural Network For Anomaly and misuse Detection", In Proceedings of the 8th USENIX Security Symposium, 1999
[10] Girardin, L., "An Eye on Network Intruder-Administrator Shootouts", In Proceedings of the First USENIX Workshop on Intrusion Detection and Network Monitoring, Santa Clara, USA, 1999
[11] Jirapummin, C., Wattanapongsakorn, N. and Kanthamanon, P., "Hybrid Neural Networks for Intrusion Detection System", The 2002 International Technical Conference on Circuits / Systems, Computers and Communications (ITC-CSCC 2002), pages: 928-931, Thailand, July 2002
[12] Kummar, S., "Classification and Detection of Computer Intrusions", PhD thesis Purdue University, 1995
[13] Labib, K. and Vemuri, R., "NSOM: A Real-Time Network-Based Intrusion Detection System Using Self-Organizing Maps", Networks and Security, 2002
[14] Li, T., "Behavioral Clustering and Statistical Intrusion Detection", M. S. Dissertation, Florida State University, Spring 1997
[15] Lichodzijewski, P., Zincir-Heywood, A.N. and Heywood, M.I., "Dynamic Intrusion Detection Using Self-Organizing Maps", The 14th Annual Canadian Information Technology Security Symposium, CITSS, 2002
[16] Lippmann, R.P. and Cunningham, R.K., "Improving Intrusion Detection Performance Using Keyword Selection and Neural Networks", RAID99, Computer Networks, Vol. 34, Number 4, 2000
[17] Rhodes, B.C., Mahaffey, J.A. and Cannady, J.D., "Multiple Self-Organizing Maps for Intrusion Detection", In Proceedings of 23rd National Information Systems Security Conference, 2000
[18] Sabhnani, M. and Serpen, G., "Application of Machine Learning Algorithms to KDD Intrusion Detection Dataset within Misuse Detection Context", http://www.eecs.utoledo.edu/~serpen/professional/Research/Publication/MLMTA 2003 Manuscript Submission Version.pdf, July 2003
[19] Tauritz, D., "ART: An overview of the field", http://web.umr.edu/~tauritzd/art/overview.html, April 2003
[20] Zhang, Z., Li, J., Manikopoulos, C.N., Jorgenson, J. and Ucles, J., "HIDE: A Hierarchical Network Intrusion Detection System Using Statistical Preprocessing and Neural Network Classification", In Proceedings of the 2nd Annual IEEE Systems, Mans, Cybernetics Information Assurance Workshop, West Point, NY, June 2001
[21] The 3rd International Knowledge Discovery and Data Mining Tools Competition, http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html, April 2003