طراحی سیستم تشخیص نفوذ با استفاده از شبکه عصبی GFF

حسین کریمی[۱]، محمد علی منتظری[۲]

[۱]دانشگاه آزاد اسلامی،واحد لامرد، گروه کامپیوتر، لامرد، ایران
Karimi.h87@gmail.com

[۲]دانشگاه صنعتی اصفهان، گروه آموزشی کامپیوتر، اصفهان، ایران
montazeri_ma@yahoo.com

چکیده

سیستم تشخیص نفوذ[۱] (IDS) یک ابزار مؤثر برای جلوگیری از دستیابی های غیر مجاز به منابع شبکه است. یک سیستم تشخیص نفوذ خوب باید دارای میزان تشخیص بالا[۲] و میزان خطای پایین[۳] باشد. این مقاله یک روش جدید برای طراحی سیستم تشخیص نفوذ با استفاده از شبکه های عصبی پیشنهاد می‌دهد، به این صورت که آموزش شبکه های عصبی بکار رفته در آن به صورت دو مرحله ای و متوالی انجام می‌شود. ما این مدل جدید را بر روی شبکه عصبی پیش خور تعمیم یافته[۴] (GFF) آزمایش و کارآیی آن را با مدل‌هایی که فرآیند آموزش در آنها به صورت یک مرحله‌ای است مقایسه کردیم. آزمایش ها و ارزیابی ها با استفاده از پایگاه داده KDD CUP 99 انجام شده و از تمامی رکوردهای شبکه برای آموزش و تست شبکه استفاده شده است. نتایج نشان می‌دهد که مدل پیشنهادی بهبود قابل توجهی از نظر میزان تشخیص و میزان خطای مثبت در مقایسه با سیستم ساده داشته به گونه‌ای که این سیستم همان سطح کارآیی یا در مواردی بهتر در مقایسه با سیستم‌های مشابه دیگر دارد.

کلمات کلیدی

سیستم تشخیص نفوذ، میزان تشخیص، میزان خطای مثبت، شبکه عصبی GFF

[1]Intrusion Detection System
[2]Detection Rate
[3]False Positive Rate
[4]Generalized Feed Forward

۱-مقدمه

رشد سریع کامپیوترها روش های ذخیره سازی اطلاعات و داده‌ها را دگرگون ساخته است. با استفاده از این شیوه های جدید برای دستیابی به داده ها، امنیت اطلاعات بوسیله کاربران غیر مجاز در معرض خطر و آسیب جدی قرار می‌گیرد. از سوی دیگر کامپیوترها به یک مولفه اساسی در زندگی روزمره ما تبدیل شده اند؛ روزانه میلیون‌ها تراکنش در اینترنت انجام می‌شود و حجم عظیمی از اطلاعات و داده ها بوسیله کاربران وب در سراسر جهان به اشتراک گذاشته شده است. اما مساله محافظت از این اطلاعات و داده ها بیش از پیش حایز اهمیت است چرا که اندازه شبکه های کامپیوتری به طور شگفت انگیزی روزانه در حال افزایش است. از نظر هدف مهاجم در حمله و از نظر اینکه چه بعدی از امنیت مورد حمله قرار گرفته است، حملات را در چهار دسته حملات کاربر به ریشه[۱]، حملات از راه دور[۲]، حملات پویش[۳] و حملات قطع سرویس[۴] تقسیم بندی می‌کنند. حملات کاربر به ریشه (U2R) دسته ای از حملات هستند که در آن حمله کننده تلاش می‌کند مجوزهای کاربر نرمال را تصاحب کند. در حملات از راه دور (R2L) ازیکماشیناهدوردسترسی‌هایغیر معتبربهیکسیستممحلی صورتمیپذیرد. حملات پویش (Probe) شاملبررسیوپویشبررویسیستمبرایییافتنراه‌هایاینفوذبهآناست. حملات قطع سرویس (DoS) یا از کار اندازی سرویس حملاتی هستند کهدرآندرخواست هایمشروعکاربرتوسطسیستمبرآوردهنمی‌شود.

سیستم‌های تشخیص نفوذ سیستم‌هایی هستند که برای نظارت بر فعالیت شبکه-های کامپیوتری و به منظور سیاست‌های امنیتی طراحی شده اند. براساس نوع تجزیه و تحلیل سیستم های تشخیص نفوذ به دو گروه عمده تقسیم بندی می‌شوند؛ تشخیص ناهنجاری[۵] و تشخیص سوء استفاده[۶]. به طور کلی سیستم های تشخیص ناهنجاری، ابتدا نمایه‌هایی از رفتارهای نرمال و هنجار را تشکیل داده، سپس هرگونه تخطی و یا انحراف از این نمایه‌های نرمال را به عنوان رفتاری ناهنجار و مهاجمانه تلقی می-نمایند. لذا قابلیت اصلی این سیستم ها تشخیص حملات جدید و ناشناخته است. سیستم های تشخیص سوء استفاده با داشتن اطلاع از الگوهای حملات مختلف، به تشخیص حملات شناخته شده می‌پردازند و لذا قادر به تشخیص حملات ناشناخته و جدید نمی باشند. با توجه به حجم عظیم اطلاعات برای پردازش محتوای اطلاعات به روش های خاصی مورد نیاز است و همچنین به دلیل ماهیت غیرالگوریتمی روشهای نفوذ به شبکه‌های کامپیوتری، روش‌های مطرح شده برای مقابله با حملات نیز باید دارای ماهیت غیر الگوریتمی باشد. بنابراین طرح یک روش جهت مقابله با نفوذ، عموماً درصورت کشف و شناخت سناریوی آن امکان پذیر است. تشخیص نفوذ با استفاده از داده‌های ممیزی در حجم بالا به منابع و زمان اجرای بسیار زیادی نیاز دارد که الگوریتم های داده کاوی سنتی با این شرایط پیچیدگی زیادی دارند. از این رو تحقیقات فعلی در IDSبه خصوص در زمینه تشخیص ناهنجاری و تشخیص بر اساس ویژگی های مشخصاتبیشتربر روش های مدل سازی آماری[۷]، مدل های فرآیند مارکوف[۸]، الگوریتم‌های بر اساس قاعده[۹]، روش‌های داده کاوی[۱۰] و استفاده از شبکه‌های عصبی و سایر روش‌ها و الگوریتم‌های هوشمند تمرکز یافته است [۱].

در [۲] یک شیوه جدید در طراحی تشخیص نفوذ که بر اساس تشخیص ناهنجاری بوده و از منطق فازی به همراه ترکیبی از چندین SOMاستفاده می‌کند توسط جَزَر و جاناتان در سال ۲۰۰۸ ارایه شده است. میزان تشخیص و خطا در این روش به ترتیب ۹۰ درصد و ۱۰/۲۹ درصد است.

یک روش جدید با استفاده از فیلتر فیشر برای انتخاب صفات و دسته‌بندی حملات توسط بِغداد در سال ۲۰۰۷ پیشنهاد شده است. این روش از چهار شبکه عصبی مختلف استفاده می‌کند و نتایج نشان می‌دهد که میزان تشخیص و میزان دسته‌بندی[۱۱] رشد داشته است [۳].

یک سیستم تشخیص ترکیبی که از ترکیب تشخیص ناهنجاری و تشخیص سوء استفاده با استفاده از منطق فازی استفاده می‌کند در [۴] توسط شانموگام و ادریس در سال ۲۰۰۷ گزارش شده است. نتایج نشان می‌دهد که میزان تشخیص برای همه انواع حملات افزایش یافته است و دقت تشخیص حملات نیز ۹۹/۹۰ درصد بدست آمده است.

در یک تحقیق جدید کارآیی شبکه های عصبی مختلف زمانی که از تمام رکوردهای پایگاه داده موجود در امر آموزش شبکه استفاده شده توسط بِغداد در سال ۲۰۰۷ بررسی شده است. در این تحقیق پنج نوع شبکه عصبی مختلف بررسی شده است: شبکه عصبی پرسپترون چند لایه[۱۲] (MLP) ، شبکه عصبی مبتنی بر نگاشت ویژگی‌ها به شیوه

1 User to Root
2 Remote to Local
3 Probe
4 Denial of Service
5 Anomaly detection
6 Misuse detection

7 statistical model
8 Markov process models
9 Rule-based algorithms
10 Data mining techniques
11 Classification Rate
12 Multilayer Perceptron Neural Network

خود سازماندهی شده[1] (SOFM) ، شبکه عصبی جردن- المان[2]، شبکه شبکه عصبی بازگشتی و شبکه عصبی تابعی مبتنی بر شعاع[3] (RBF). نتایج نشان داد که میزان تشخیص درستی برای این شبکه‌ها به ترتیب ۹۹/۱۶ ، ۹۸/۲۸ ، ۹۸/۳۶ ، ۹۸/۴۴ و ۷۹/۲۳ به صورت درصد است [۵].

در [۶] یک سیستم تشخیص نفوذ بر اساس شبکه های عصبی و فازی طراحی شده است. این سیستم بهبود قابل توجهی در مقایسه با روش‌های درخت تصمیم گیری[4] و روش‌های دیگر دارد و در سال ۲۰۱۰ به چاپ رسیده است.

در [۷] از یک روش ترکیبی و بهینه سازی اجتماع ذرات[5] استفاده شده است. در بخش اول سعی می‌کند مناسب ترین ویژگی‌ها مربوط به ترافیک شبکه را انتخاب کند و در بخش بعد به طبقه‌بندی حملات مختلف می‌پردازد. دقت طبقه‌بندی در این مقاله که در سال ۲۰۱۲ چاپ شده است ۹۳/۳ درصد است.

نویسنده در [۸] سعی می‌کند میزان خطای مثبت، خطای منفی[6] و زمان آموزش شبکه عصبی برای تشخیص نفوذ را با استفاده از شبکه عصبی SOMبهبود یافته کاهش دهد. میزان تشخیص در این مقاله که در سال ۲۰۱۲ چاپ شده است برای حملات DoS،U2R،R2Lو Probeبه ترتیب ۹۹/۶ ، ۶۹ ، ۹۵/۹ و ۹۲/۶ و میزان خطای مثبت ۱/۲ به صورت درصد است.

در [۹] یک الگوریتم طبقه بندی تشخیص نفوذ جدید در سال ۲۰۱۴ معرفی شده است. در این الگوریتم ماشین بردار پشتیبان[7] با تئوری کلونی مورچه‌ها[8] ترکیب شده است. نتایج نشان از دقت طبقه-بندی و کارآیی زمان اجرا در این الگوریتم دارد. درصد تشخیص در این روش ۹۴/۸۶ و میزان خطای مثبت ۶/۰۱ درصد است.

در [۱۰] یک روش تولید ویژگی دیداری بر اساس ستاره چهار گوشه به منظور ارزیابی فاصله بین نمونه ها برای طبقه‌بندی پنج کلاس مختلف در سال ۲۰۱۴ پیشنهاد شده است. دقت طبقه‌بندی در این روش ۹۴/۳۵ درصد است.

[1]Self-Organizing Feature Maps
[2]Jordan- Elman Neural Network
[3]Radial Basis Function
[4]Decision tree
[5]Particle swarm optimization
[6]false negative rate
[7]Support Vector Machine
[8]Ant Colony Optimization

علاوه بر تحقیقات فوق، استاندارد ها، یادداشت ها و رهنمود های فراوانی در زمینه ایمن سازی شبکه ها توسط شرکت های معتبر، موسسات بین المللی استاندارد و کارشناسان ایمنی منتشر شده است. علیرغم بکارگیری مکانیزم‌های امنیتی مختلف هنوز شاهد حملات جدیدی علیه شبکه های کامپیوتری هستیم. بخصوص حملات قطع سرویس به دلیل سادگی در اجرا و عدم راه حل قطعی جهت مقابله با آنها رو به افزایش است. به هرحال با همه این تلاش‌ها به منظور بهبود و بدست آوردن نتایج بهتر در تشخیص لازم است تلاش‌های بیشتری انجام شود.

در این مقاله سعی می‌شود یک سیستم تشخیص نفوذ مبتنی بر شبکه طراحی شود به گونه‌ای که کارآیی بالاتر و خطای کمتری داشته باشد.

دلیل اصلی برای استفاده از شبکه های عصبی در تشخیص نفوذ قابلیت تعمیم دهی آنهاست که سبب تشخیص حملات ناشناخته می-شود. در سیستم‌های تشخیص می‌توان از شبکه‌های عصبی به صورت ساده یا ترکیبی از شبکه های عصبی و یا ترکیب شبکه‌های عصبی با روش‌های دیگر استفاده کرد.

سیستم پیشنهادی لایه‌های مختلفی دارد و آموزش شبکه عصبی در دو مرحله انجام می‌شود. بعد از پیش پردازش بر روی داده‌های اصلی این رکوردها در پنج دسته طبقه‌بندی می‌شوند. در اولین مرحله پنج شبکه عصبی GFFبرای هر دسته از رکوردها وجود دارد. در هر شبکه عصبی GFFتنها رکوردهای مربوط به همان دسته وجود دارد و آموزش داده می‌شود. خروجی این مرحله به یک شبکه عصبی GFFدیگر به عنوان دومین مرحله داده می‌شود. بعد از این دو مرحله آموزش شبکه عصبی به پایان می‌رسد. بکارگیری این دو مرحله در آموزش و ترکیب شبکه عصبی سبب بهبود و افزایش کارآیی در مقایسه با سیستم های موجود می‌شود.

درادامهٔمقالهدربخش۲،شبکه عصبی GFF و مزایای آن بیان می شود. دربخش۳به توصیف پایگاه داده استفاده شده برای انجام شبیه سازی پرداخته می شود.دربخش۴،سیستم پیشنهادی برای تشخیص نفوذ معرفی می شود. پارامترهای ارزیابی برای بررسی کارآیی سیستم پیشنهادی دربخش۵ارایه می شود. بخش ۶، آزمایشات انجام شده را نشان می دهد. مقایسه سیستم پیشنهادی با سیستم ساده در بخش ۷ و مقایسه کارآیی آن با سیستم های تشخیص نفوذ دیگر در بخش ۸

تشریح می گردد و نهایتاًدربخش۹، نتیجه‌گیریازمقالهوپیشنهادات برای کارهایآیندهبیانمیگردد.

۲-شبکه عصبی GFF

شبکه‌های عصبی به دلیل توانایی یادگیری و سازگاری در اکثر سیستم‌های تشخیص نفوذ استفاده می‌شوند. تفاوت شبکه‌های عصبی مختلف در ساختار آنها یعنی تعداد لایه های ورودی، میانی، خروجی و همچنین در نحوه آموزش و الگوهای یادگیری است. الگوهای یادگیری می‌توانند به صورت بانظارت، بدون نظارت و یا ترکیبی از هردو باشند. در یادگیری با نظارت جواب مطلوب سیستم یادگیرنده از قبل آماده است یعنی به خطای یادگیری که همان خطای بین مقدار مطلوب و مقدار واقعی است دسترسی خواهد داشت. در یادگیری بدون ناظر جواب مطلوب برای سیستم یادگیرنده موجود نیست.

شبکه عصبی GFFنمونه خاصی از پرسپترون چند لایه است به طوری‌که اتصالات آن می‌تواند در جریان یک یا چندین لایه پرش کند. شبکه عصبی GFFشامل یک لایه ورودی، حداقل یک لایه میانی و یک لایه خروجی است.

در تئوری هر نمونه مساله ای که شبکه عصبی GFFآن را حل می‌کنند به وسیله MLPقابل حل است. اما در عمل این شبکه ها اغلب مسایل را با کارآیی بیشتری حل می‌کنند یک نمونه مشخص از این مسایل، مساله دو مارپیچ است. بدون این که بخواهیم به بیان این مساله بپردازیم تنها به بیان این مساله اکتفا می‌کنیم که یک MLPاستاندارد برای حل این مساله به صدها تکرار بیشتر برای آموزش نسبت به این شبکه عصبی نیاز دارد (برای شبکه ای به همان اندازه). امتیاز شبکه های GFFتوانایی برای پیش بردن فعالیت ها بوسیله بای پاس کردن لایه‌ها است. نتیجه اینکه آموزش لایه‌های نزدیک‌تر به ورودی مؤثرتر است.

آموزش این شبکه همراه با نظارت است. این شبکه توانایی تعمیم دارد و می‌تواند خروجی مناسب را برای ورودی هایی که آموزش ندیده است، تولید کند.

۳-توصیف پایگاه داده

ارزیاب تشخیص نفوذ ۱۹۹۸ اولین مجموعه از ارزیاب‌ها بود که بوسیله آزمایشگاه MITدر لینکولن و تحت نظارت DARPAو آزمایشگاه تحقیقاتی نیروی هوایی ایجاد شد. این ارزیاب ها نقش مؤثری در جهت دهی تلاش‌های محققان در زمینه تشخیص نفوذ به عهده دارند. برای توصیف یک اتصال شبکه ۴۲ ویژگی مرتبط به هم وجود دارد. ۴۱ مورد اول، ویژگی‌های اتصال و آخرین فیلد نوع اتصال را نشان می‌دهد.

برای انجام آزمایشات از پایگاه داده KDD Cup 99 استفاده می-شود که نسخه دیگری از ارزیاب ۱۹۹۸ است. اینمجموعه،شاملاطلاعاتاتصالاتشبکهمحلینیرویهوایی آمریکابهانضمامانواعگستردهایازحملاتشبیهسازیشده است. برایهراتصالدر اینمجموعهدادهها، ۴۱ مشخصهتعریفگردیدهکهاینمشخصههابه۴دستهٔمشخصههایاصلی، مشخصه‌هایمحتوایی،مشخصه‌های ترافیکمبتنیبرزمانومشخصه هایترافیکمبتنیبرمیزبانتقسیمبندیمی‌شوند. هراتصالدارایبرچسبی استکهمشخصمی‌کنداتصالمذکورنرمالاستویایکیازانواعحملات.در این پایگاه داده مجموعه‌های مختلفی برای آموزش و تست وجود دارد. برای آموزش از پایگاه داده‌ای تحت عنوان kddcup.data_10_percent و برای تست از پایگاه داده‌ای به نام correctedاستفاده می‌شود. انواع حملاتی که در این دو پایگاه داده وجود دارد به همراه تعداد آنها به تفکیک نوع حمله در جدول (۱) آورده شده است. همچنین در این جدول تعداد حملات به درصد نیز درج شده است. در داده‌های تست حملات جدیدی نیز وجود دارد. منظور از حملات جدید حملاتی است که در مجموعه داده آموزش وجود ندارد اما در پایگاه داده تست به دلیل ماهیت آنها این حملات قرار داده شده است. یک سیستم تشخیص نفوذ خوب باید بتواند این حملات جدید را شناسایی کند.

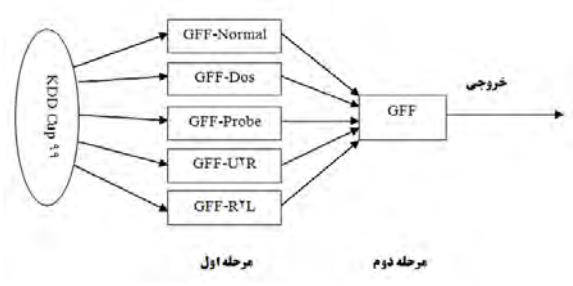
جدول (۱) : توزیع انواع حملات مختلف در پایگاه داده آموزش و تست

دسته	آموزش		تست	
	تعداد	درصد	تعداد	درصد
Normal	۹۷۲۷۸	۱۶/۹۸	۶۰۵۹۳	۱۹/۴۸
DoS	۳۹۱۴۵۸	۷۹/۲۴	۲۲۹۸۵۳	۷۳/۹۰
Probe	۴۱۰۷	۰/۸۳	۴۱۶۶	۱/۳۴
U2R	۵۲	۰/۰۱	۲۲۸	۰/۰۷
R2L	۱۱۲۶	۰/۲۲	۱۶۱۸۹	۵/۲
مجموع	۴۹۴۰۲۱	۱۰۰	۳۱۱۰۲۹	۱۰۰

۴-طرح سیستم پیشنهادی

با الهام از سیستم آموزشی که به صورت مرحله ای است و یادگیرنده در هر مرحله اطلاعات جدیدی کسب می‌کند یک سیستم تشخیص نفوذ دو مرحله ای پیشنهاد می‌شود. در مرحله اول از پنج شبکه عصبی که هر یک بخشی از پایگاه داده را آموزش می‌بینند و در مرحله دوم از یک شبکه عصبی مشابه شبکه‌های عصبی مرحله اول به منظور نتیجه

گیری و تشخیص نهایی استفاده می‌شود. انگیزه ما برای استفاده از چنین روشی این بود که ضمن بدست آوردن نتایج مطلوب در مرحله پیش بینی این روش را با روش آموزش معمول برای شبکه های عصبی نیز مقایسه کنیم. این مدل در شکل (۱) نشان داده شده است.



شکل (۱): ساختار مدل پیشنهادی مورد استفاده برای سیستم تشخیص نفوذ

همانطور که در شکل مشاهده می‌کنید در مرحله اول آموزش پنج شبکه عصبی و در مرحله دوم یک شبکه عصبی وجود دارد. در مرحله اول تمامی شبکه ها از ساختار یکسانی برخوردارند. ۴۱ عنصر در لایه ورودی، ۵ عنصر در لایه میانی و ۵ عنصر در لایه خروجی که این ساختار به اختصار به صورت [41, 5, 5] نمایش داده می‌شود. در این مرحله پنج شبکه عصبی مختلف که هر یک برای آموزش یکی از دسته های حملات و نرمال بکار می‌روند وجود دارد. یعنی GFF-Normal[41; 5; 5] برای آموزش اتصالات نرمال، GFF-DoS[41; 5; 5] برای آموزش اتصالات DoS، GFF-Probe[41; 5; 5] برای آموزش اتصالات Probe، GFF-U2R[41; 5; 5] برای آموزش اتصالات U2Rو GFF-R2L[41; 5; 5] برای آموزش اتصالات R2Lبکار می‌رود. با توجه به تعداد عناصر هر یک از پنج دسته، ماتریس های ورودی برای هر یک از شبکه ها متفاوت است. ماتریس ورودی برای شبکه اول ۴۱×۹۷۲۷۸ و ماتریس خروجی آن ۵× ۹۷۲۷۸، ماتریس ورودی برای شبکه دوم ۴۱×۳۹۱۴۵۸ و ماتریس خروجی آن ۵×۳۹۱۴۵۸، ماتریس ورودی برای شبکه سوم ۴۱× ۴۱۰۷ و ماتریس خروجی آن ۵×۴۱۰۷ ، ماتریس ورودی برای شبکه چهارم ۴۱×۵۲ و ماتریس خروجی آن ۵×۵۲ و ماتریس ورودی برای شبکه پنجم ۴۱×۱۱۲۶ و ماتریس خروجی آن ۵×۱۱۲۶ است. این مرحله می‌تواند هم به صورت متوالی و هم به صورت موازی انجام داد که ما به صورت متوالی این عمل را انجام دادیم. در پایان این مرحله یک شناخت جزیی نسبت به مجموعه داده ها بدست می‌آید و انتظار می‌رود وزن های شبکه ها به گونه ای تنظیم شوند که برای مرحله دوم مناسب شوند. پس از جمع آوری خروجی های مرحله اول یک ماتریس ۴۹۴۰۲۱×۵ تشکیل می‌شود که به عنوان ورودی به یک شبکه عصبی دیگر در مرحله دوم داده می‌شود. ساختار این شبکه به صورت GFF [5; 30; 30; 5] است. در پایان این مرحله آموزش شبکه ها به منظور سیستم تشخیص نفوذ به پایان می‌رسد.

۵-پارامترهای ارزیابی

برای ارزیابی و مقایسه سیستم های مختلف در زمینه تشخیص نفوذ پارامترهای مختلفی استفاده می‌شود اما در این مقاله سعی کرده ایم از تمامی پارامترهای ارزیابی موجود استفاده کنیم. در این بخش چهار پارامتر ارزیابی برای مقایسه این روش با روش های دیگر معرفی می-شود.

میزان تشخیص:نسبت بین تعداد حملاتی که درست تشخیص داده شده و تعداد کل نمونه های تست است[۱۱] .

میزان دسته بندی:بیان کننده نسبت بین تعداد نمونه‌های تست یک دسته که درست تشخیص داده شده و تعداد کل نمونه‌های همان دسته است.[۱۱].

خطای مثبت:بیانگر نسبت بین تعداد نمونه اتصالاتی است که اشتباهاً در یک دسته قرار گرفته اند و تعداد کل نمونه‌هایی که در این دسته قرار گرفته اند[۱۱].

هزینه روش[1]: پارامتر CPEبا استفاده از فرمول (۱) محاسبه می-شود.

$$CPE = \frac{1}{N}\sum_{i=1}^{m}\sum_{j=1}^{m} CM(i,j) * C(i,j) \quad (۱)$$

که CMو Cبه ترتیب نشان دهنده ماتریس مجاورت و ماتریس هزینه، Nتعداد کل نمونه تست‌ها و mتعداد دسته‌های مختلف است. ماتریس هزینه نیز به این صورت تعریف می‌شود که هر عنصرC(i , j) نشان دهنده هزینه جریمه برای تعداد نمونه‌هایی است که متلق به دسته iام بوده‌اند اما اشتباهاً در دسته jام قرار گرفته‌اند. ماتریس هزینه در جدول (۲) آمده است.

جدول (۲) : مقادیر ماتریس هزینه برای محاسبه CPE

خروجی مطلوب / خروجی شبکه	Normal	DoS	Probe	U2R	R2L
Normal	۰	۲	۱	۲	۲

[1]Cost Per Example

DoS	۲	۰	۱	۲	۲
Probe	۱	۲	۰	۲	۲
U2R	۳	۲	۲	۰	۲
R2L	۴	۲	۲	۲	۰

۶-آزمایش‌ها

برای بررسی نحوه عملکرد این شیوه آموزشی و تفاوت آن با سیستمی که آموزش آن به صورت یک مرحله ای انجام می‌شود یک سیستم تشخیص نفوذ مبتنی بر فرآیند آموزش یک مرحله ای نیز طراحی شده است. آزمایش ها با استفاده از نرم افزار NeuroSolutionبر روی یک پردازنده T5500 (1.66 GH) و با ۰/۹۹ گیگا بایت حافظه انجام شده است. این شبکه عصبی را یک بار در سیستم تشخیص نفوذ پیشنهادی و بار دیگر در سیستم تشخیص نفوذ ساده استفاده می‌کنیم. سیستم تشخیص نفوذ ساده در شکل (۲) نشان داده شده است.

شکل (۲) : سیستم تشخیص نفوذ که شیوه آموزش شبکه عصبی در آن به صورت یک مرحله ای است.

در جداول (۳) و (۴) نتایج آزمایشات با استفاده از دو مدل آمده است. در هر جدول مقادیر میزان دسته بندی (CR)، میزان تشخیص (DR)، میزان خطای مثبت (FP) و میزان هزینه (CPE) آمده است. ستون های جداول نشان دهنده خروجی شبکه و سطرها بیان کننده خروجی مطلوب شبکه است.

جدول (۳): ماتریس مجاورت برای GFF ساده

خروجی مطلوب / خروجی شبکه	Normal	DoS	Probe	U2R	R2L
Normal	۵۸۸۲۵	۱۶۳	۶۹۵	۷۳۲	۱۷۸
DoS	۷۴۷۲	۲۲۲۰۰۵	۲۵۱	۳۹	۸۶
Probe	۵۹۶	۸۵	۳۴۵۷	۱۰	۱۸
U2R	۱۹	۲	۱۴۰	۵۷	۱۰
R2L	۱۴۳۴۶	۲	۶۸	۶۷۲	۱۱۰۱
FP (%)	۲۷/۶۱	۰/۱۱	۲۵/۰۳	۹۶/۲۳	۲۰/۹۶
DR (%)			۹۱/۷۷		
CPE			۰/۲۵۲		

جدول (۴): ماتریس مجاورت برای GFF با روش پیشنهادی

خروجی مطلوب / خروجی شبکه	Normal	DoS	Probe	U2R	R2L
Normal	۶۰۵۹۱	۰	۲	۰	۰
DoS	۰	۲۲۹۸۳۸	۱۵	۰	۰
Probe	۰	۰	۴۱۶۶	۰	۰
U2R	۱	۰	۶	۲۲۱	۰
R2L	۰	۰	۳	۰	۱۶۱۸۶
FP (%)	۰/۰۰۲	۰	۰/۶۲۰	۰	۰
DR (%)			۹۹/۹۹۲		
CPE			۰/۰۰۰۱۲۲		

۷-مقایسه سیستم تشخیص نفوذ پیشنهادی با سیستم تشخیص نفوذ ساده

به منظور مقایسه بهتر سیستم طراحی شده با روش پیشنهادی و روش ساده نتایج ارایه شده در جداول بالا را به صورت خلاصه در جدول (۵) می‌آوریم. در این جدول روشی که در فرآیند آموزش شبکه عصبی استفاده شده و همچنین درصد خروجی سیستم (میزان دسته بندی) آمده است.

جدول (۵) : **مقایسه نتایج سیستم تشخیص نفوذ در دو روش ساده و پیشنهادی**

روش آموزش شبکه عصبی	میزان دسته بندی شبکه عصبی				
	Normal	DoS	Probe	U2R	R2L
روش پیشنهادی با GFF	۹۹/۹۹۷	۹۹/۹۹۳	۱۰۰	۹۶/۹۳۰	۹۹/۹۸۱
روش ساده با GFF	۹۷/۰۸	۹۶/۵۹	۸۲/۹۹	۲۵	۶/۸

همانطور که از روی جدول قابل مشاهده است، روش جدیدی که برای آموزش سیستم تشخیص نفوذ بکار رفته است نتایج قابل توجه و

بسیار بهتری نسبت به روش آموزش یک مرحله ای دارد. به این صورت که با توجه به جداول (۳) ، (۴) و (۵) میزان تشخیص در روش جدید به ۹۹/۹۹۲ درصد رسیده که نسبت به ۹۱/۷۷ درصد روش ساده بسیار بهبود داشته است. همچنین میزان CPE نیز در روش جدید به میزان بسیار زیادی کاهش یافته است.

نکته دیگری که باید به آن توجه داشته باشیم در مورد سه دسته Probe، U2Rو R2Lاست. با توجه به اینکه درصد حملات جدید در این سه دسته به ترتیب ۴۲/۹۴ ، ۸۲/۸۹ و ۶۲/۹۸ بوده و همچنین تراکم رکوردها به منظور آموزش در این سه دسته بسیار کم است اما مشاهده می‌شود که سیستم جدید با درصد بالا به شخیص این حملات می‌پردازد و بهبود قابل توجهی نسبت به روش ساده داشته است.

۸-مقایسه سیستم پیشنهادی با سیستم های دیگر

در این بخش سیستم طراحی شده با روش پیشنهادی را با سیستم های طراحی شده دیگر مقایسه می‌کنیم. این نتایج در جدول (۶) آمده است.

اگر بخواهیم نتایج را از نظر میزان دسته بندی مقایسه کنیم مساله اصلی پایین بودن میزان دسته بندی در دسته های U2Rو R2Lدر اکثر سیستم های تشخیص نفوذ است که این امر به دلیل پایین بودن تعداد رکوردهای این دسته‌ها، U2R(۵۲ رکورد) و R2L(۱۱۲۶ رکورد)، در پایگاه داده است. اما در روش پیشنهادی این مقادیر به بالاترین حد خود یعنی ۱۰۰ در صد رسیده اند. دلیل این بهبود، شیوه آموزش دو مرحله‌ای در سیستم طراحی شده است. در روش ما این مقادیر از همه سیستم‌های دیگر بالاتر است.

از نظر میزان تشخیص درستی نوع حملات با توجه به جدول بالا بهترین نتیجه در بین کارهای دیگر ۹۹/۹۰ درصد است که در روش پیشنهادی نیز به همین خوبی جواب می‌دهد.

یک سیستم تشخیص نفوذ خوب باید از خطای مثبت بسیار پایینی برخوردار باشد. در روش ما این میزان در حدود ۰/۰۰۳ درصد بود که در مقایسه با سایر روش‌ها بسیار پایین است.

مقدار CPEدر همه کارها محاسبه نشده است اما با توجه به مقادیر میزان دسته بندی مشخص است که در روش پیشنهادی ما این میزان بسیار کم است.

۹-نتیجه گیری و پیشنهادها

بر خلاف بسیاری از سیستم های تشخیص نفوذ، سیستم پیشنهادی در این مقاله به صورت سلسله مراتبی عمل می‌کند. این سیستم تشخیص نفوذ با استفاده از شبکه های عصبی به دلیل قابلیت تعمیم آنها طراحی شده است و آموزش شبکه عصبی بکار رفته در آن به صورت دو مرحله ای و متوالی انجام می‌شود. رمز موفقیت این سیستم در این است که در طی دو مرحله به شناسایی حملات مختلف می‌پردازد به این صورت که در مرحله اول یک شناخت جزیی نسبت به داده ها و حملات مختلف بدست می‌آورد و در مرحله بعد به تشخیص کامل آنها می-پردازد.

در سیستم پیشنهادی شبکه عصبی استفاده شده در هر دو لایه مشابه است اما می‌توان این سیستم را با شبکه های عصبی مختلف نیز طراحی کرد. در این صورت می‌توان از خصوصیات چندین شبکه عصبی مختلف استفاده کرد.

در این سیستم به منظور آموزش شبکه های عصبی از همه رکوردهای پایگاه داده استفاده شده است که این مساله باعث افزایش حجم محاسبات و همچنین افزایش زمان آموزش شبکه شده است. می‌توان با انجام پیش پردازش بیشتر و عملیات آماری مثل نمونه گیری و استفاده از الگوریتم های هوشمند و ترکیب آنها با یکدیگر ویژگی هایی از رکوردها که تاثیر بیشتری دارند را انتخاب و به منظور آموزش شبکه عصبی استفاده کرد.

جدول (۶) : مقایسه نتایج سیستم پیشنهادی با سیستم های دیگر

سیستم	میزان دسته بندی شبکه عصبی					پارامترهای ارزیابی		
	Normal (%)	DoS (%)	Probe (%)	U2R (%)	R2L (%)	DR (%)	FP (%)	CPE
این مقاله	۹۹/۹۹۷	۹۹/۹۹۳	۱۰۰	۹۶/۹۳۰	۹۹/۹۸۱	۹۹/۹۹۲	۰/۰۰۲	۰/۰۰۰۱۲۲

[۲]	۹۹/۵۱	۹۸/۳۷	۸۸/۴	۸۴/۳۳	۷۱/۱۳	۹۰	۱۰/۲۹	–
[۳]	۹۴/۹	۹۹/۴۶	۹۵/۱۷	۰	۹۰/۷۶	۹۸/۴۹	–	–
[۴]	۹۹/۷۰	۹۹/۹۵	۹۹/۴۵	۷۹/۹۶	۱۰۰	۹۹/۹۰	–	–
[۵]	۹۹/۸۵	۹۹/۳۶	۹۲/۴۵	۰	۰	۹۲/۱۶	–	–
[۷]	–	–	–	–	–	۹۳/۳	–	–
[۸]	–	۹۹/۶	۹۲/۶	۶۹	۹۵/۹	–	۱/۲	–
[۹]	–	–	–	–	–	۹۴/۸۶	۶/۰۱	–
[۱۰]	–	–	–	–	–	۹۴/۳۵	–	–
[۱۱]	۹۸/۲	۹۹/۵	۸۴/۱	۱۴/۱	۳۱/۵	۹۵/۳	۱/۹	۰/۱۵۷۹

مراجع

[1] Ioannis, X., Aide à la surveillance de l'application d'une politique de sécurité dans un réseau par prise de connaissance d'un graphe de fonctionnement du réseau Thèse dirigée par le Professeur Dimitri PLÉMÉNOS Coencadrement Pierre-Francois Bonnefoi M.C. et Professeur Djamchid GHAZANFARPOUR, UNIVERSITE DE LIMOGES ECOLE DOCTORALE Science Technologie – Santé FACULTE des Sciences et Techniques Laboratoire XLIM, 2007

[2] Jazzar M., Jantan A., "A Novel Soft Computing Inference Engine Model for Intrusion Detection", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.4, pp. 1-8, April 2008

[3] Beghdad R., "Applying fisher's filter to select KDD connections features and using neural network to classify and detect attacks", Neural Network World, ProQuest Science Journals, pp 1-16, 2007

[4] Shanmugam B., Idris N. B., "Improved hybrid intelligent intrusion detection system using AI technique", Neural Network World, ProQuest Science Journals, pp. 351, 2007

[5] Beghdad R., "Training all the KDD data set to classify and detect attacks", Neural Network World, ProQuest Science Journals, pp. 81, 2007

[6] G.Wang, J.Hao, J.Ma, L.Huang ,"A new approach to intrusion detection using Artificial Neural Networks and fuzzy clustering", Expert Systems with Applications,Vol 37,pp. 6225–6232,2010

[7] Chung ,Yuk Y., Wahid ,N.," A hybrid network intrusion detection system using simplified swarm optimization (SSO)" Applied Soft Computing, Vol. 12, pp. 3014–3022,2012

[8] Jiang, X., Liu, K., Yan J., Chen ,W.," Application of Improved SOM Neural Network in Anomaly

Detection", Physics Procedia,Vol 33 ,pp. 1093 – 1099 ,2012

[9] Feng, W., Zhang Q., Hu G., Huang, Jimmy X.," Mining network data for intrusion detection through combining

SVMs with ant colony networks", Future Generation Computer Systems,Vol 37,pp. 127–140,2014

[10] Luo ,B., Xia ,J.," A novel intrusion detection system based on feature generation with visualization strategy", Expert Systems with Applications,Vol 41,pp. 4139–4147,2014

[11] Toosi A. N., Kahani M. M., "A new approach to intrusion detection based on an evolutionary soft computing model using neuro-fuzzy classifiers", computer connections, Science Direct, pp 2201-2212, 2007