رهیافت جدیدی برای طراحی سیستمهای تشخیص نفوذ: ادغام سیستمهای تشخیص سوءاستفاده و تشخیص ناهنجاری با به‌کارگیری ترکیب جدیدی از شبکه‌های عصبی پس انتشار خطا و کوهونن

احمدرضا شرافت[1*]، مهدی راستی[2]

۱- استاد مهندسی برق و کامپیوتر، دانشگاه تربیت مدرس

۲- دانشجوی دکترای مهندسی برق و کامپیوتر، دانشگاه تربیت مدرس

*** تهران صندوق پستی: ۴۸۳۸-۱۴۱۵۵**

sharafat@isc.iranet.net

(دریافت مقاله: آذر ۱۳۸۲، پذیرش مقاله: اردیبهشت ۱۳۸۶)

چکیده- بار پردازشی زیاد، نیاز متناوب به به‌روزرسانی، پیچیدگی و خطای زیاد در تشخیص، برخی از مشکلات و ضعفهای موجود در طراحی سیستمهای تشخیص ناهنجاری و تشخیص سوءاستفاده است. هدف این تحقیق، طراحی نوعی سیستم تشخیص نفوذ مبتنی بر شبکه است که این ضعفها را تا حد امکان کم کند. برای رسیدن به این هدف، سیستمهای تشخیص سوءاستفاده و تشخیص ناهنجاری را ادغام کرده‌ایم. این رویکرد تاکنون در طراحی سیستمهای تشخیص نفوذ به‌کار برده نشده است. برای ادغام سیستمهای تشخیص ناهنجاری و تشخیص سوءاستفاده در سیستم ترکیبی تشخیص نفوذ، از ساختار ترکیبی جدیدی از شبکه‌های پس انتشار خطا و کوهونن که برای کاربردهای بازشناسی الگو و دسته‌بندی پیشنهاد شده - استفاده کرده‌ایم. نتایج به‌دست آمده نشانگر اثر بسیار مثبت این ادغام سیستمهای تشخیص ناهنجاری و سوءاستفاده و همچنین توانایی ساختار شبکه عصبی پیشنهادی در بهبود عملکرد سیستم ترکیبی تشخیص نفوذ است.

کلید واژگان: امنیت شبکه، تشخیص ناهنجاری، تشخیص سوءاستفاده، تشخیص نفوذ، شبکه عصبی.

۱- مقدمه

علی‌رغم به‌کارگیری سازوکارهای امنیتی، رمزنگاری و دیوار آتش، هنوز شاهد حملات جدیدی بر علیه شبکه‌های کامپیوتری هستیم. سیستمهای عامل و برنامه‌های کاربردی، همواره اشتباهات و ضعفهای غیرقابل اجتنابی دارند که در کنار ضعف پروتکل‌های شبکه، مورد استفاده مهاجمان قرار می‌گیرند.

سیستم تشخیص تهاجم، حمله‌هایی را که علی‌رغم مواظبتهای امنیتی اتفاق می‌افتد، تشخیص می‌دهد. سیستمهای تشخیص تهاجم سه جزء اصلی دارند که عبارتند از: منبع اطلاعات، موتور تحلیل و پاسخ‌دهنده. منبع اطلاعات، وقایع اتفاق افتاده در سیستم را ثبت می‌کند؛ موتور تحلیل علائم تهاجم را پیدا می‌کند؛ و

[Downloaded from mjee.modares.ac.ir on 2024-04-30]

پاسخ‌دهنده، براساس خروجی موتور تحلیل، عکس‌العملهای لازم و ممکن را از خود نشان می‌دهد.

از نظر نوع منبع اطلاعات استفاده شده، سیستمهای تشخیص تهاجم به دو دسته: مبتنی بر میزبان و مبتنی بر شبکه تقسیم‌بندی می‌شوند. سیستمهای مبتنی بر میزبان، بر روی اطلاعات جمع‌آوری شده در داخل یک کامپیوتر مجزا عمل می‌کنند، در حالی‌که سیستمهای مبتنی بر شبکه، بر ترافیک شبکه نظارت می‌کنند.

سیستمهای تشخیص تهاجم، از دید روش تشخیص نفوذ نیز به دو دسته: تشخیص سوءاستفاده[1] و تشخیص ناهنجاری[2] تقسیم می‌شوند. سیستمهای تشخیص سوءاستفاده، تهاجم را براساس الگوهای از پیش تعریف شده‌ای از حملات شناخته شده تشخیص می‌دهند و سیستمهای تشخیص ناهنجاری، رفتار غیرمعمول یا غیرنرمال را در میزبان یا در شبکه تشخیص می‌دهند. این روش، بازتاب دیدگاهی در تحقیقات تشخیص تهاجم است که می‌گوید: تهاجم، زیرمجموعه‌ای از فعالیتهای غیرنرمال است. سیستمهای تشخیص سوءاستفاده، فقط حملات شناخته شده را تشخیص می‌دهد؛ اما سیستمهای تشخیص ناهنجاری، توانایی شناسایی حملات جدید و ناشناخته را نیز دارند. در این سیستمها داشتن پایگاه داده‌ای از الگوهای حمله ضروری نیست؛ اما در عوض به آموزش وسیعی از وقایع سیستم یا شبکه نیاز است تا بتوان الگوهای رفتار عادی را به‌خوبی از آنها استخراج کرد.

طراحی سیستمهای تشخیص ناهنجاری نسبت به سیستمهای تشخیص سوءاستفاده، مشکل‌تر و نیازمند روشهای پیچیده‌تری است. در سیستمهای تشخیص نفوذ از نوع تشخیص ناهنجاری، با استخراج ویژگیهای رفتار عادی، هر رفتاری که ویژگیهای آن متفاوت از این ویژگیها باشد، به‌عنوان رفتار غیرعادی شناخته می‌شود. برای آموزش رفتار عادی، به مجموعه‌ای از داده‌های واقعی عاری از حمله نیاز است. در سیستمهای تشخیص نفوذ از نوع تشخیص سوءاستفاده، با آموزش رفتار غیرعادی، رفتارهای شبیه به آن به‌عنوان رفتار غیرعادی و رفتارهای متفاوت با آن به‌عنوان رفتار عادی تشخیص داده می‌شود. برای آموزش رفتار غیرعادی نیز به مجموعه‌ای از داده‌های فاقد رفتار عادی (مجموعه داده‌های حمله) نیاز است.

در این مقاله، نوعی سیستم تشخیص نفوذ ترکیبی معرفی شده است. علاوه بر این، ساختار ترکیبی جدیدی از شبکه‌های پس انتشار خطا و کوهونن را برای کاربردهای بازشناسی الگو و دسته‌بندی ارائه کرده‌ایم. در سیستم تشخیص نفوذ ترکیبی پیشنهادی، دو سیستم تشخیص ناهنجاری و تشخیص سوءاستفاده ادغام شده‌اند. در قسمت موتور تحلیل این سیستمها، از ساختار شبکه عصبی پیشنهادی برای بازشناسی الگوی رفتار عادی و غیرعادی ترافیک شبکه‌های کامپیوتری استفاده کرده و شبکه عصبی پیشنهادی را برای طراحی سه نوع سیستم تشخیص نفوذ به‌کار برده‌ایم. این سه نوع سیستم عبارتند از: سیستم تشخیص ناهنجاری، سیستم تشخیص سوءاستفاده و سیستم ادغام شده تشخیص ناهنجاری و سوءاستفاده.

در بخش دوم مقاله به بیان مسأله می‌پردازیم. در بخش سوم سابقه تحقیقات مرتبط مرور می‌شود. در بخش چهارم رهیافت پیشنهادی را شرح می‌دهیم و بلوک دیاگرام پیشنهادی برای سیستم تشخیص نفوذ و همچنین ساختار کلی شبکه عصبی مورد استفاده در موتور تحلیل سیستم تشخیص نفوذ را شرح می‌دهیم. در بخش پنجم سیستمهای طراحی شده تشریح می‌شود. نتایج به‌دست آمده را در بخش ششم نشان می‌دهیم. در بخش هفتم به نتیجه‌گیری و پیشنهادهایی برای ادامه کار می‌پردازیم.

1. Misuse
2. Anomaly

[Downloaded from mjee.modares.ac.ir on 2024-04-30]

۲- بیان مسأله

سیستم خوب تشخیص نفوذ باید ویژگیهای زیر را داشته باشد:

- خطای مثبت و خطای منفی کوچکی داشته باشد.
- در شرایط مختلف، مصالحه میان خطای مثبت و خطای منفی را بتوان به‌دلخواه انجام داد.
- بار پردازشی کمی داشته باشد.
- مرحله آموزش سیستم تشخیص نفوذ به‌طور کامل خودکار بوده و به تحلیل و تفسیر توسط انسان نیازی نداشته باشد.

متأسفانه نرخ خطا یا تشخیص نادرست در سیستمهای تشخیص نفوذ زیاد است. این خطاها دو نوع هستند. خطاهای منفی[1] (FN) هنگامی رخ می‌دهد که سیستم تشخیص نفوذ با فعالیتی روبرو می‌شود که تهاجم است اما غیرعادی نیست. خطاهای مثبت[2] (FP) هنگامی رخ می‌دهد که تشخیص دهنده ناهنجاری با فعالیتی روبه‌رو می‌شود که غیرعادی است اما تهاجم نیست. در حالت اخیر، سیستم تشخیص ناهنجاری، وقوع تهاجم را به اشتباه تشخیص می‌دهد. هر چه این دو نوع خطا کمتر باشند، سیستم تشخیص نفوذ عملکرد بهتری دارد. در عمل، کمتر کردن یکی از این دو نوع خطا منجر به افزایش دیگری می‌شود و لذا با توجه به هدف طراحی، باید مصالحه‌ای میان آنها ایجاد کرد. این مصالحه ممکن است در شرایط خاصی به سمت کوچکتر کردن مقدار FN باشد یا بعکس. اما از آنجاکه تشخیص نادرست وقوع حمله، موجب اعمال محدودیتها یا پاسخهای خاصی می‌شود، بهتر است این مصالحه به سمت کمتر کردن خطای مثبت باشد تا اعتبار اعلام خطر بیشتر شود؛ البته این مصالحه، به مقدار خطای منفی بزرگتری منجر می‌شود و تشخیص برخی حملات (اغلب جدید) ناممکن می‌شود. اما در حالت کلی بهتر است ساختار و پیکربندی سیستم تشخیص ناهنجاری به نوعی باشد که بتوان مصالحه میان این دو خطا را در شرایط خاصی و بنا به نظر مدیر شبکه، به سمت کمتر کردن هر یک از آنها سوق داد.

در تمامی روشهای تشخیص تهاجم، داده مورد استفاده[3] بسیار زیاد است و این باعث سربار پردازشی زیادی می‌شود [۱]. به‌عنوان مثال سیستمهای قاعده‌پی به‌دنبال نشانه‌های[4] خاص میان داده‌های مورد استفاده می‌گردند. روش آماری تشخیص ناهنجاری نیز با مشاهده رفتار هر کاربر، به دنبال نشانه‌های رفتار غیرعادی جستجو می‌کند. متأسفانه این سیستمها بار پردازشی سیستم را زیادتر می‌کنند. یکی از هدفهای این تحقیق، طراحی نوعی سیستم تشخیص ناهنجاری مبتنی بر شبکه است که رفتار عادی و غیرعادی شبکه را تشخیص دهد، بدون آنکه بار پردازشی زیادی داشته باشد.

یکی از ضعفهای بالقوه در سیستمهای تشخیص نفوذ، پیچیدگی به‌روزرسانی آنها است. به‌دلیل اضافه شدن سرویسها، کاربردها و کاربران جدید و همچنین کشف حملات جدید، سیستمهای تشخیص نفوذ را باید به‌روز کرد. به‌روزرسانی سیستمهای تشخیص قاعده‌پی و تشخیص آماری، به‌دلیل آنکه نیاز به دانش و تحلیل انسان دارد، پیچیده بوده و با مشکلات زیادی همراه است [۲].

۳- سابقه تحقیق

در اغلب تحقیقات سیستمهای تشخیص نفوذ، از روشهای قاعده‌پی استفاده شده است [۲]. این روشها شامل مجموعه قواعدی هستند که حملات را به‌طور کامل تشریح می‌کنند. سیستمهای خبره از معمولترین روشهای قاعده‌پی هستند [۲]. نیاز متناوب به به‌روزرسانی و در عین حال پیچیدگی انجام آن [۳]، بار پردازشی زیاد و عدم

1. False Negative
2. False Positive
3. Monitoring Data
4. Signatures

[Downloaded from mjee.modares.ac.ir on 2024-04-30]

توانایی در تشخیص حملات جدید، ضعفهای سیستمهای خبره محسوب می‌شود.

بسیاری از سیستمهای تشخیص ناهنجاری از مؤلفه‌های آماری استفاده می‌کنند. رفتار کاربر یا سیستم، به‌وسیلهٔ تعدادی از متغیرها که در طول زمان نمونه‌برداری شده، سنجیده می‌شود. مدلهای پیچیده‌تر، از نمایهٔ کاربران در فعالیتهای کوتاه‌مدت و بلندمدت همراه با همبستگی متغیرها استفاده می‌کنند [٤]. با توجه به تغییر فعالیت کاربران، نمایه‌ها باید به‌طور متناوب تغییر کنند. مثالهایی از این متغیرها عبارتند از: زمان ورود و خروج هر نشست و مدت در اختیارگیری منبع (پردازنده، دیسک سخت، حافظهٔ اصلی و غیره). مدت زمان نمونه‌برداری می‌تواند کوتاه (چند دقیقه) یا طولانی (حدود یک ماه) باشد. نیاز متناوب به به‌روزرسانی و در عین حال پیچیدگی انجام آن و بار پردازشی زیاد از ضعفهای عمده سیستمهای تشخیص آماری است.

تحقیقات اندکی نیز در زمینه استفاده از شبکه عصبی در سیستمهای تشخیص نفوذ انجام شده است [٢]. شبکه‌های عصبی به‌عنوان جایگزینی برای سیستمهای قاعده‌پی و تشخیص آماری برای غلبه بر ضعفهای موجود در این سیستمها مطرح شده‌اند [٢]. در [٥، ٦] برای اولین بار شبکه عصبی به‌عنوان جایگزین روشهای آماری در تشخیص ناهنجاری مطرح شد. تحقیقات [١] و [٧] تا [١٤] نیز در ادامه کار در زمینه طراحی سیستمهای تشخیص ناهنجاری با استفاده از شبکه عصبی انجام شده است. در [٣] برای اولین بار شبکه عصبی به‌عنوان جایگزین روشهای قاعده‌پی در تشخیص سوءاستفاده پیشنهاد شد. این تحقیقات نشان داده است که چنانچه این شبکه‌ها به‌درستی طراحی و پیاده‌سازی شوند، مزیتهای مهمی مانند بار پردازشی کمتر، یادگیری بهتر رفتار عادی به‌طور خودکار و تشخیص رفتار غیرعادی، در مقایسه با سایر روشهای تشخیص تهاجم دارند.

در [١٩، ٢٠] نشان داده شده است که ادغام خروجیهای طبقه‌بندی‌کننده‌ها[1] برای کاربردهای بازشناسی الگو می‌تواند به عملکرد بهتری، در مقایسه با استفاده از هر یک از طبقه‌بندی کننده‌ها به‌طور جداگانه، منجر شود. همچنین در [٢١، ٢٢] نشان داده شده است که اگر مجموعه‌ای از شبکه‌های عصبی، خطاهای متفاوت[2] (غیرهمبسته) داشته باشند، ادغام آنها می‌تواند عملکرد بهتری از نظر دقت طبقه‌بندی نسبت به شبکه عصبی با بیشترین دقت در آن مجموعه داشته باشد. ایجاد شبکه‌های عصبی با خطای متفاوت به‌راحتی امکان‌پذیر نیست [٢١]. با وجود این روشهایی برای ایجاد چنین شبکه‌هایی پیشنهاد شده است [٢٣]. در این روشها، معمولاً از: تفاوت در پارامترهای مربوط به طراحی و آموزش شبکه‌های عصبی، شامل تعیین تصادفی وزنهای اولیه؛ یک نوع شبکه عصبی با معماریهای متفاوت؛ شبکه‌های عصبی متفاوت؛ و از داده‌های آموزشی متفاوت استفاده می‌شود. در [٢٣] به‌طور تجربی نشان داده شده که تفاوت در نوع شبکه‌های به‌کار رفته و تفاوت در داده‌های آموزشی مورد استفاده، نسبت به سایر روشها کارایی بهتری دارد. اساس روش پیشنهادی ما نیز بر استفاده از دو نوع متفاوت شبکه عصبی یعنی شبکه‌های پس انتشار خطا و کوهونن و همچنین بر استفاده از داده‌های آموزشی متفاوت (داده‌های مربوط به کلاسهای متفاوت)، برای بازشناسی الگوی حملات و غیرحملات استوار است. به‌خلاف سیستمهای طراحی شده در [٥، ٦] و [٣] که سیستم منفرد تشخیص سوءاستفاده یا سیستم منفرد تشخیص ناهنجاری هستند، اساس روش پیشنهادی این مقاله، ادغام این دو سیستم، به‌عنوان ادغام دو طبقه‌بندی کننده است.

1. Fusion of Multiple Classifiers' Outputs
2. Diverse Errors

[Downloaded from mjee.modares.ac.ir on 2024-04-30]

٤- روش پیشنهادی

به‌منظور استفاده از شبکه‌های عصبی در تشخیص نفوذ، ابتدا باید ساختار و نوع شبکه عصبی مشخص و سپس مجموعه ویژگیهای ترافیک شبکه - که ورودی شبکه عصبی محسوب می‌شود - انتخاب شود. در ادامه، ابتدا ساختار شبکه عصبی پیشنهادی و سپس مجموعه ویژگیها و پایگاه داده مورد استفاده برای آموزش و آزمودن شبکه آورده می‌شود.

برای دستیابی به ویژگیهایی که برای سیستم تشخیص ناهنجاری برشمردیم، دو ایده زیر را مطرح می‌کنیم.

۱- ترکیب سیستم تشخیص تهاجم و ناهنجاری (آموزش توأم رفتار غیرعادی و رفتار عادی).

۲- ارائه ترکیب جدید شبکه عصبی کوهونن (با اندکی تغییر) و شبکه عصبی پس انتشار خطا به‌منظور بازشناسی الگوهای (رفتارهای) عادی و غیرعادی.

تاکنون برای تشخیص نفوذ، یا از سیستم تشخیص سوءاستفاده یا از سیستم تشخیص ناهنجاری استفاده شده است. ما نشان می‌دهیم که با ادغام سیستمهای تشخیص ناهنجاری و تشخیص سوءاستفاده، می‌توان از تواناییهای این دو سیستم به‌طور همزمان استفاده کرد. علاوه بر این، با استفاده از سیستم ترکیبی تشخیص ناهنجاری و سوءاستفاده، می‌توان بر ضعفهایی که در طراحی هر یک از این سیستمها (به‌طور مستقل) وجود دارد غلبه کرد. این رویکرد تاکنون در سیستمهای تشخیص نفوذ مدنظر قرار نگرفته است.

در این مقاله ساختار ترکیبی جدیدی از شبکه‌های عصبی پس انتشار خطا و کوهونن برای کاربردهای بازشناسی الگو ارائه می‌کنیم. از این ساختار به‌عنوان موتور تحلیل در سیستمهای تشخیص نفوذ استفاده می‌کنیم.

٤-۱- ساختار شبکه عصبی با استفاده از شبکه‌های پس انتشار خطا و کوهونن

در این بخش ساختار شبکه عصبی متشکل از شبکه‌های پس انتشار خطا و کوهونن را به‌طور کلی برای کاربردهای بازشناسی الگو و دسته‌بندی پیشنهاد می‌کنیم. از این ساختار پیشنهادی به‌عنوان موتور تحلیل سیستم تشخیص نفوذ استفاده می‌کنیم. ابتدا ساختار سنتی دو نوع شبکه عصبی پس انتشار خطا و کوهونن را به‌اختصار شرح می‌دهیم.

٤-۱-۱- شبکه عصبی کوهونن

شبکه عصبی مصنوعی کوهونن که در سال ۱۹۹۵ ارائه شد [۱۵]، برای تحلیل و به تصویر کشیدن تحلیل داده‌های با ابعاد زیاد مناسب است. شبکه عصبی کوهونن شبکه ای رقابتی مبتنی بر یادگیری بدون نظارت است که داده‌های ورودی با ابعاد زیاد را به ساختار یک‌بُعدی، دوبُعدی یا سه‌بُعدی نگاشت می‌کند.

این نگاشت حفظ‌کننده توپولوژی است، به این‌معنا که نقاط نزدیک به هم در فضای ورودیها به واحدهای نزدیک به هم در فضای خروجی نگاشته می‌شود [۷]. در پایان آموزش، این نگاشت، تابع چگالی احتمال الگوهای ورودی با ابعاد زیاد را تقریب می‌زند. دو گام در آموزش شبکه کوهونن طی می‌شود. ابتدا با اعمال هر الگوی آموزشی، فاصله بردار وزن هر واحد i در لایه رقابتی با بردار الگوی ورودی محاسبه می‌شود، سپس نورونی که دارای کمترین فاصله است به‌عنوان نورون برنده انتخاب می‌شود. مقدار فعالیت نورون برنده را یک و بقیه نورونها را صفر در نظر می‌گیریم. سپس وزنهای نورون برنده و نورونهای واقع در همسایگی آن را، با رابطه زیر اصلاح می‌کنیم:

$$\Delta w_{i,j} = \eta(x_j - w_{i,j})$$
$$w_{i,j}^{\text{new}} = w_{i,j}^{\text{old}} + \Delta w_{i,j} \qquad (۱)$$

[Downloaded from mjee.modares.ac.ir on 2024-04-30]

که η ضریب یادگیری و $\mathbf{w}_j=[w_{1,j}, w_{2,j}, \ldots, w_{n,j}]$ بردار وزنهای نورون j در لایه رقابتی و $\mathbf{x}=[x_1, x_2, \ldots, x_n]$ بردار الگوی ورودی است. وزنهای بقیه نورونها نیز تغییر داده نمی‌شود. این اصلاح به‌نحوی است که فاصله بردار وزنهای نورون برنده و همسایه آن، با بردار ورودی کمتر شود. در واقع، بردار وزنهای اصلاح شده به الگوی ورودی شبیه‌تر می‌شوند. در هنگام آموزش پارامتر η و تابع تعیین‌کننده همسایگی باید مشخص شود. مقدار اولیه η معمولاً بزرگ است و در طی دوره آموزش، مقدار آن به‌طور خطی با زمان کوچک می‌شود.

شبکه کوهونن به‌دلیل معماری موازی و فراهم کردن ترتیب ارتباط الگوها به‌صورت گرافیکی بر روشهای سنتی شناسایی الگو مزیت دارد. برای پردازش بی‌درنگ داده‌ها در کاربردهای طبقه‌بندی، شبکه کوهونن به‌دلیل سرعت و کارایی زیاد آن در مقایسه با سایر روشهای یادگیری، بهترین انتخاب است [۱۱]. به همین دلیل شبکه کوهونن را برای یادگیری مشخصه‌های رفتار عادی و غیرعادی ترافیک شبکه‌های کامپیوتری بر سایر روشهای یادگیری ترجیح داده و از آن در لایه اول شبکه پیشنهادی خود استفاده می‌کنیم. انتظار داریم که با آموزش رفتار عادی و غیرعادی به شبکه کوهونن، بردار وزنهای به‌دست آمده در فضای ورودیها، بیانگر محدوده رفتار داده‌های آموزش داده شده (عادی و غیرعادی) باشد.

٤-١-٢- شبکه پس‌انتشار خطا

شبکه پس‌انتشار خطا، یک لایه ورودی، حداقل یک لایه میانی و یک لایه خروجی دارد. آموزش این شبکه، همراه با نظارت است. این شبکه توانایی تعمیم دارد و می‌تواند خروجی مناسب را برای ورودیهایی که آموزش ندیده تولید کند. ضعف آن در پیچیدگی محاسباتی و صرف وقت زیاد در مرحله آموزش است. آموزش بدین روش است که ابتدا ورودی به آن داده می‌شود. سپس مقدار فعالیت نورونهای هر لایه به‌ترتیب تا لایه خروجی محاسبه می‌شود. آنگاه مقدار نورونهای لایه خروجی با مقدار مطلوب آنها مقایسه و از ضرب اختلاف آنها در مشتق تابع فعالیت نورونهای خروجی، خطا در لایه خروجی محاسبه می‌شود. خطا در لایه میانی نیز با ضرب خطای لایه خروجی در وزنهای اتصالات لایه میانی به لایه خروجی و ضرب در مشتق تابع فعالیت نورونهای میانی به‌دست می‌آید. با محاسبه خطا در هر لایه، وزنهایی را که از نورونهای لایه قبل به آن لایه آمده، بر طبق رابطه زیر اصلاح می‌شود:

$$\Delta w_{i,j} = \eta \delta_j a_i$$
$$w_{i,j}^{\text{new}} = w_{i,j}^{\text{old}} + \Delta w_{i,j} \qquad (۲)$$

که η ضریب یادگیری و δ_j خطای نورون jام آن لایه و a_i مقدار فعالیت نورون i ام لایه قبل است. محاسبه خطا و اصلاح وزنها از سمت خروجی به‌سمت ورودی، دلیل نام پس‌انتشار خطا است.

دسته‌بندی، تخمین و تقریب زدن توابع، تعدادی از کاربردهای شبکه پس‌انتشار خطا است. استفاده از شبکه پس‌انتشار خطا، در تشخیص ناهنجاری به‌منظور یادگیری رفتار عادی و غیرعادی مناسب نیست، زیرا فرایند پیچیده یادگیری رفتار عادی در این شبکه، نیازمند چند لایه میانی یا حداقل نیازمند تعداد زیادی نورون در لایه میانی و همچنین در لایه ورودی [۹] است. این باعث بسیار طولانی شدن دوره آموزش شبکه و افزایش پیچیدگی محاسبات می‌شود. اما چنانچه ویژگیهای رفتار عادی و غیرعادی را تا حدودی در اختیار داشته باشیم، این شبکه می‌تواند با یک لایه میانی با تعداد کمتری نورون اختلاف رفتار فعلی شبکه را با رفتار عادی یا غیرعادی آشکار کند.

[Downloaded from mjee.modares.ac.ir on 2024-04-30]

٤-۱-۳- ساختار شبکه عصبی پیشنهادی برای کاربردهای بازشناسی الگو

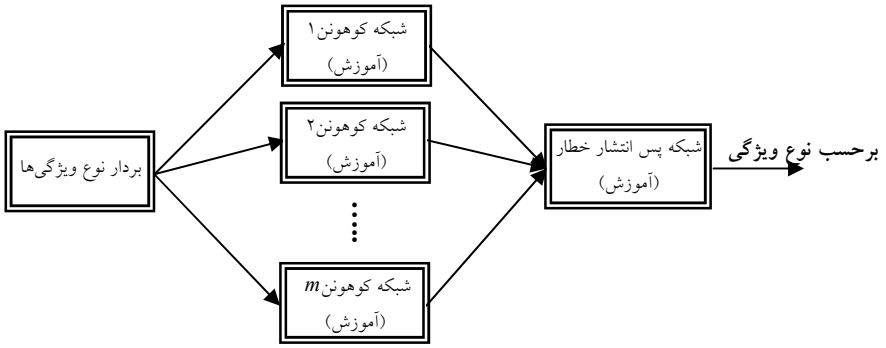
الگو با بردار ویژگی n بعدی بیان می‌شود که آن را با $\mathbf{x}=[x_1,x_2,...,x_n]$ نشان می‌دهیم. فرض کنید می‌خواهیم M کلاس را شناسایی کنیم و داده‌هایی کافی و مناسب، متعلق به هر یک از این الگوها را نیز در دست داریم. مجموعه برچسب‌های تمام کلاسها را با $\mathrm{C}=\{c_1,c_2,...,c_m\}$ نشان می‌دهیم. مجموعه تمام داده‌های آموزشی (الگوهایی که کلاس آنها معلوم است) مربوط به کلاس iام را با $\mathcal{D}_i$ نشان می‌دهیم. اجتماع تمام این زیرمجموعه‌ها را با $\mathcal{D}$ نمایش می‌دهیم. ساختار شبکه عصبی پیشنهادی در شکل ۱ نشان داده شده است. آموزش شبکه عصبی پیشنهادی در دو مرحله و به‌طور جداگانه انجام می‌شود. در مرحله اول، تعداد m شبکه عصبی کوهونن طراحی می‌شود. هر یک از شبکه‌های کوهونن به‌طور جداگانه و مستقل از هم با داده‌های مربوط به یک کلاس متفاوت از M کلاس ($m \le M$) آموزش داده می‌شوند. در واقع برای آموزش اولیه ویژگیهای هر کلاس، یک شبکه کوهونن جداگانه به‌کار برده می‌شود. در مرحله دوم با آموزش شبکه پس انتشار خطا با استفاده از تمام مجموعه داده آموزشی، تفاوتهای الگوها آشکار می‌شود.

مرحله اول:

۱- تعداد m شبکه کوهونن ($m \le M$)، یعنی $\mathrm{S}=\{S_1,S_2,...,S_k,...,S_m\}$، هر یک با n ورودی و یک صفحه نگاشت خروجی با ابعاد $p_k = z_k \times y_k$ ایجاد می‌کنیم.

۲- بر طبق الگوریتم سنتی آموزش شبکه کوهونن، هر شبکه S_k را با $\mathcal{D}_k$ آموزش می‌دهیم.

مجموعه بردار وزنهای شبکه S_k را با $\mathcal{W}^k=\{\mathbf{w}_1^k,\mathbf{w}_2^k,...,\mathbf{w}_j^k,...,\mathbf{w}_{p_k}^k\}$ نشان می‌دهیم که در آن w_j^k بردار وزن نورون jام از شبکه S_k است، یعنی $\mathbf{w}_j^k=[w_{j,1}^k,w_{j,2}^k,...,w_{j,l}^k,...,w_{j,n}^k]$ که در آن $w_{j,l}^k$ مقدار وزن اتصال بین مؤلفه lام از بردار ویژگی ورودی و نورون j در صفحه نگاشت خروجی شبکه K/م کوهونن، است. در پایان آموزش مرحله اول انتظار داریم که مجموعه بردار وزنهای شبکه S_k (یعنی $\mathcal{W}^k$) بیانگر ویژگیهای کلاسی باشد که به آن آموزش داده شده است. به بیان دیگر بردار وزنهای S_k بیانگر فضای ویژگیهای کلاس K/م در فضای ورودی است. یعنی برحسب موقعیت نورون jام در صفحه نگاشت خروجی شبکه S_k و همچنین میزان اختلاف بردار ویژگی ورودی به بردار $\mathbf{w}_j^k$، بتوان میزان شباهت یا تفاوت الگوی ورودی به الگوی کلاس kام را آشکار کرد. آشکارسازی خودکار ویژگیهای کلاس kام از روی مقدار



شکل ۱ (ساختار پیشنهادی برای بازشناسی الگو): هر شبکه کوهونن با داده‌های آموزشی مربوط به یک کلاس متفاوت با استفاده از روش معمول آموزش داده شده، سپس از شبکه های کوهونن آموزش داده شده، (با قرار دادن مقدار هر یک از نورونهای خروجی شبکه کوهونن برابر با تفاوت بردار وزنهای آن نورون و بردار ویژگی ورودی) برای آموزش داده‌های آموزشی مربوط به تمام کلاسها به شبکه پس انتشار خطا استفاده می‌شود. بعد از اتمام دو مرحله آموزش به‌صورت فوق، از ترکیب شبکه های پس انتشار خطا و کوهونن به‌عنوان تشخیص‌دهنده الگو استفاده می‌شود.

[Downloaded from mjee.modares.ac.ir on 2024-04-30]

اختلافی که بردار ورودی با هر یک از بردارهای وزنهای شبکه S_k (با توجه به موقعیت نورونهای مختلف در صفحه خروجی S_k) دارد و همچنین مقدار اختلاف بردار ورودی با بردار وزنهای نورونهای شبکه‌های کوهونن دیگر، در مرحله دوم انجام می‌شود.

مرحله دوم:

۱- یک شبکه عصبی پس انتشار خطا با تعداد $\sum_{k=1}^{m} x_k \times z_k$ ورودی، تعداد K نورون در لایه میانی و تعداد L نورون در لایه خروجی ایجاد می‌کنیم. تعداد نورونهای ورودی شبکه پس انتشار خطا برابر با مجموع نورونهای صفحه نگاشت‌های خروجی تعداد m شبکه کوهونن است.

۲- شبکه پس انتشار خطا را روی تمامی داده‌های مجموعه $\mathcal{D}$ به روش زیر آموزش می‌دهیم:

برای هر بردار از مجموعه $\mathcal{D}$، یعنی داده مربوط به کلاس i، خروجی مطلوب d_i را که متناظر با کلاس c_i است (c_i برچسب کلاسی که x متعلق به آن است)، اختصاص می‌دهیم. در واقع مجموعه مقادیر d_i برای $i = 1,2,...,M$، مجموعه برچسب تمام کلاسها را مشخص می‌کند. هر بردار از مجموعه $\mathcal{D}$ به‌عنوان ورودی به نورونهای ورودی شبکه‌های کوهونن اعمال می‌شود. آنگاه مقدار فعالیت هر نورون خروجی شبکه‌های کوهونن را (به‌جای اختصاص مقدار صفر یا یک) برابر با اختلاف بردار ورودی با بردار وزنهای آن نورون قرار می‌دهیم. به بیان دیگر مقدار فعالیت نورون jام شبکه S_k (یعنی a_j^k) برابر با $a_j^k = \left\|\mathbf{x}-\mathbf{w}_j^k\right\| = \sqrt{\sum_{i=1}^{n}\left(x_i - w_{j,i}^k\right)^2}$ است. سپس خروجی این نورونها را به‌عنوان ورودی به شبکه پس انتشار خطا اعمال می‌کنیم. در واقع، مقادیر خروجی این نورونها بیانگر اختلاف یا شباهت الگوی ورودی با الگوی مربوط به کلاس K ام از مجموعه m کلاس است.

آنگاه با توجه به مقدار مطلوب d_i، برطبق الگوریتم سنتی آموزش شبکه پس انتشار خطا، وزنهای شبکه پس انتشار خطا را اصلاح می‌کنیم. در پایان آموزش این مرحله، انتظار داریم شبکه پس انتشار خطا بتواند با دانشی که از شبکه‌های کوهونن می‌گیرد، وزنهای خود را طوری اصلاح کند که با آشکارسازی تفاوتهای الگوها از هم بتواند کلاس بردار ورودی را تشخیص دهد.

نوآوری ساختار پیشنهادی برای کاربردهای بازشناسی الگو، در روش آموزش و چگونگی ادغام شبکه‌های عصبی پس انتشار خطا و کوهونن است. هر یک از شبکه‌های کوهونن با داده‌های آموزشی متعلق به یک کلاس متفاوت، به‌طور جداگانه آموزش داده می‌شوند و سپس از شبکه های کوهونن آموزش داده شده برای آموزش داده‌های آموزشی مربوط به تمام کلاسها به شبکه پس انتشار خطا استفاده می‌شود.

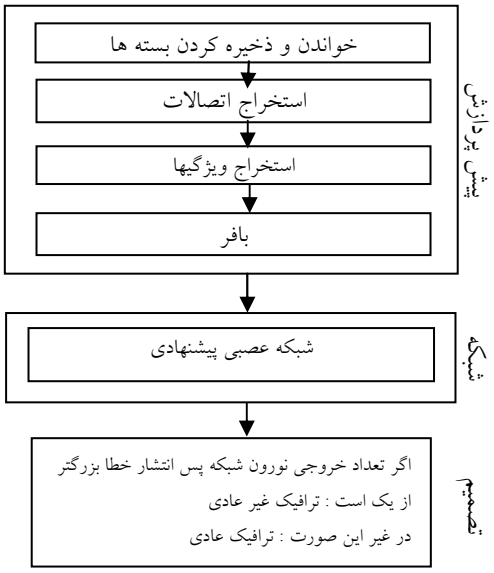
٤-٢- تشخیص نفوذ با استفاده از شبکه عصبی پیشنهادی

شکل ۲، بلوک ساختار سیستم را برای سیستم تشخیص نفوذ نشان می‌دهد. بر طبق شکل ۲ ابتدا بسته‌های شبکه خوانده و نگهداری می‌شوند. از روی این بسته‌ها، اتصالات را هر یک به‌طور جداگانه استخراج می‌کنیم. آنگاه ویژگیهای تعیین شده برای هر اتصال استخراج می‌شود (تعداد F ویژگی برای هر اتصال). از آنجاکه تعداد زیادی از حملات با ترتیبی از اتصالات انجام می‌شود و ساختار شبکه عصبی پیشنهاد شده توانایی حفظ و یادآوری اطلاعات زمانی را ندارد، باید به‌نحوی مفهوم زمان (یعنی ترتیب اتصالات) را به‌طور ضمنی در ورودی شبکه عصبی وارد کنیم. لذا داده‌های مربوط به ویژگیهای تعداد S اتصال، با حفظ ترتیب، در یک بافر ذخیره می‌شوند. آنگاه ویژگیهای تعداد S اتصال را به‌طور همزمان به شبکه عصبی پیشنهادی، اعمال می‌کنیم. لذا بردار

[Downloaded from mjee.modares.ac.ir on 2024-04-30]

ورودی شبکه عصبی پیشنهادی، F×S عضو دارد. سپس چنانچه مقدار نورون خروجی شبکه از مقدار آستانه T بزرگتر باشد، سیستم، ترافیک را ناهنجار تشخیص می‌دهد، در غیر این‌صورت ترافیک عادی اعلام می‌شود.

در تشخیص نفوذ با استفاده از شبکه عصبی با دو مسأله روبه‌رو هستیم. یکی انتخاب مجموعه ویژگیهایی از ترافیک شبکه که باید به‌عنوان ورودی به شبکه عصبی داده شود و دیگری انتخاب ساختار شبکه عصبی. در ادامه، مجموعه داده استفاده شده برای آموزش و ارزیابی سیستم تشخیص نفوذ طراحی شده، عملیات پیش‌پردازش و ساختار شبکه عصبی و آموزش آن را شرح می‌دهیم. با طراحی سه سیستم و ارائه نتایج در آخرین بخش، قدرتمندی ساختار شبکه عصبی پیشنهاد شده و همچنین اثر ترکیب سیستم تشخیص ناهنجاری (آموزش رفتار غیرعادی) و سیستم تشخیص سوءاستفاده (آموزش رفتار عادی) را بررسی می‌کنیم.



شکل ۲ ساختار سیستم پیشنهادی تشخیص نفوذ

٤-۲-۱- مجموعه داده‌ها

گروه فناوری سیستمهای اطلاعاتی آزمایشگاه لینکلن دانشگاه ام آی تی با حمایت آژانس پروژه های تحقیقاتی پیشرفته (DARPA) [١٦]، در سال ۱۹۹۸ با فراهم کردن مجموعه‌ای شامل حدود ۵ میلیون اتصال برچسب‌دار برای آموزش سیستمهای تشخیص نفوذ و حدود ۲ میلیون اتصال برای آزمایش آنها، برای اولین بار ارزیابی سیستمهای تشخیص تهاجم را امکان‌پذیر ساخت. ابتدا در محیط آزمایشگاهی، ترافیک عادی و غیرعادی روی شبکه‌ای با هزاران میزبان یونیکس و صدها کاربر شبیه‌سازی شده و ترافیک شبیه ترافیک واقعی که میان سایتهای دولت امریکا و شبکه جهانی اینترنت جریان داشت، تولید شد. هر یک از حملات شبیه‌سازی شده، در یکی از چهار دسته حملاتR-L[1] ، U-R[2]، DoS[3] ، وP[4] قرار می‌گیرند. با برچسب زدن به تمامی بسته‌های ترافیک – برای مشخص کردن نوع آنها (حمله است یا خیر) – و ذخیره‌سازی داده‌های موجود در تمامی بسته‌ها، پایگاه داده‌ای را برای ابداع، آموزش و ارزیابی سیستمهای تشخیص نفوذ ایجاد کردند. در سومین مسابقه بین‌المللی استخراج دانش و داده‌کاوی [١٧] در سال ۱۹۹۹، پردازش بیشتری روی این داده‌ها، صورت گرفت و حدود هفت میلیون اتصال TCP از آن استخراج شد. هر اتصال با چهار دسته ویژگیهای اساسیTCP[5]، ویژگیهای محتوایی[6]، ویژگیهای مبتنی بر زمان[7] و ویژگیهای مبتنی بر میزبان[8] (در مجموع ٤١ ویژگی) توصیف شده است.

٤-۲-۲- پیش‌پردازش: مجموعه ویژگیها و ورودیهای شبکه عصبی

تعیین ویژگیهایی که مقادیر آنها در ترافیک عادی و غیرعادی به اندازه کافی متفاوت باشند، برای طراحی سیستم تشخیص نفوذ با عملکرد مطلوب، بسیار مهم و

1. Remote-to-Local
2. User-to-Root
3. Denial of Service
4. Probing
5. Basic TCP Features
6. Content Features
7. Time-Based Features
8. Host-Based Features

[Downloaded from mjee.modares.ac.ir on 2024-04-30]

اساسی است. هر چه ترافیک عادی و غیرعادی در این ویژگیها متفاوت‌تر باشند، سیستم عملکرد بهتری در تشخیص تهاجم دارد. مشابه [۲]، ما نیز فقط از شش ویژگی اساسی TCP (F=٦) (از میان ٤١ ویژگی ذکر شده برای هر اتصال) برای آموزش و ارزیابی استفاده می‌کنیم. این ویژگیها در جدول ۱ آورده شده است. این شش ویژگی به‌سادگی از ترافیک شبکه (لایه شبکه) استخراج می‌شوند و لذا به آسانی در مسیریابها قابل استخراج [۲] و لذا برای تشخیص حملات بر علیه شبکه مناسب هستند. در حالی‌که برای استخراج بقیه ویژگیها (مانند ویژگیهایی که مربوط به Process برنامه‌های

جدول ۱ ویژگیهای در نظر گرفته شده برای هر اتصال

نام ویژگی	شرح	نوع
duration	مدت اتصال به ثانیه	پیوسته
protocol_type	نوع پروتکل (TCP، UDP، و غیره)	گسسته
service	سرویس شبکه در مقصد (http، telnet، و غیره)	گسسته
src_bytes	تعداد بایت‌های ارسالی از منبع به مقصد	پیوسته
dst_bytes	تعداد بایت‌های ارسالی از مقصد به مبداء	پیوسته
flag	وضعیت عادی یا غیر عادی اتصال	گسسته

کاربردی (لایه کاربرد) هستند) به اطلاعات لایه‌های بالاتر (در مقایسه با لایه شبکه) نیاز است که در مسیریابها قابل استخراج نیستند. برای هر اتصال، این شش ویژگی را استخراج کرده و به‌عنوان بردار ویژگیهای آن اتصال می‌شناسیم. مقدار هر یک از ویژگیها را با یک عدد نشان می‌دهیم. برای نشان دادن ویژگیهایی که متنی هستند (مانندTCP یا HTTP)، کد ASCII معادل کارکترهای آن را - حداکثر تا پنج کارکتر - با هم جمع کرده و به‌عنوان مقدار عددی آن ویژگی درنظر می‌گیریم. در نتیجه بردار ویژگی با شش مؤلفه برای هر اتصال به‌دست می‌آید.

آخرین مرحله در پیش‌پردازش، فراهم ساختن مفهوم زمان است. بدین‌منظور بردار عددی ویژگیهای اتصالات را به‌ترتیب در انتهای بافر ذخیره کرده و بردار ویژگیهای شش اتصال (S=٦) ابتدای بافر را همزمان به‌عنوان ورودی به شبکه عصبی اعمال می‌کنیم. در نتیجه ورودی شبکه عصبی، الگوهای ٣٦ بعدی (٦×٦) هستند.

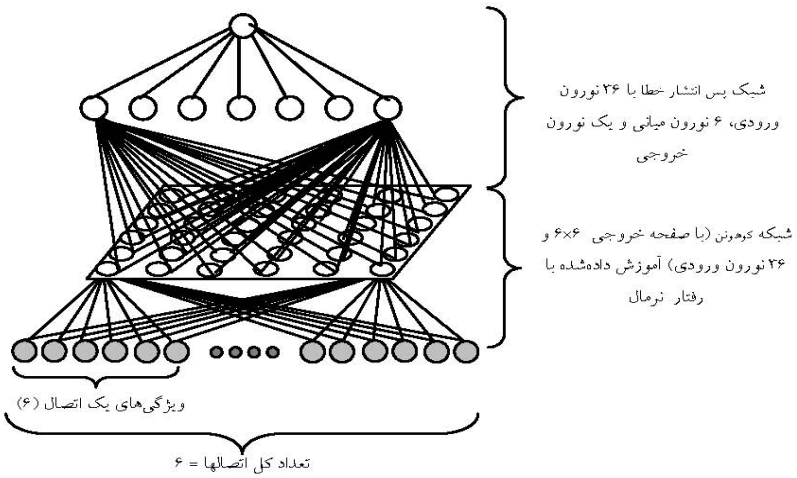
۵- سیستمهای طراحی شده

برای بررسی عملکرد شبکه عصبی پیشنهادی، همچنین بررسی اثر ترکیب سیستمهای تشخیص ناهنجاری و تشخیص نفوذ در بهبود عملکرد سیستم تشخیص نفوذ، سه نوع سیستم را طراحی می‌کنیم. در این سه نوع سیستم، از ساختار نشان داده شده در شکل ۳-۱ و برای هر سیستم، از شبکه عصبی متفاوتی استفاده می‌کنیم. در واقع می‌خواهیم دو الگوی رفتار عادی و غیرعادی را تشخیص دهیم (M=٢). در سیستم اول فقط از شبکه عصبی کوهونن برای آموزش رفتار عادی استفاده می‌کنیم (m=١). در سیستم دوم فقط رفتار غیرعادی آموزش داده می‌شود (m=١). در سیستم سوم با استفاده از دو شبکه کوهونن، هم رفتار عادی و هم رفتار غیرعادی، آموزش داده می‌شود (m=٢).

۵-۱- (سیستم اول): طراحی سیستم تشخیص ناهنجاری (آموزش رفتار عادی) (شکل۳)

به شبکه کوهونن براساس الگوریتم ارائه شده، رفتار عادی را آموزش می‌دهیم. از مجموعه داده‌های آموزشی فقط نمونه‌هایی را که در آنها هیچ اتصال حمله‌ای وجود ندارد، انتخاب کرده و آنگاه شبکه کوهونن را با این مجموعه عاری از حمله، آموزش می‌دهیم. در این مرحله انتظار داریم که بردارهای وزنهای شبکه کوهونن در فضای ورودی، معرف ناحیه رفتار عادی ترافیک شبکه‌های کامپیوتری باشد. سپس از این شبکه کوهونن آموزش داده شده، در شبکه عصبی پیشنهادی (m=١) استفاده می‌کنیم. در مرحله دوم آموزش، شبکه پس‌انتشار خطا را روی تمام مجموعه داده آموزشی،

[Downloaded from mjee.modares.ac.ir on 2024-04-30]



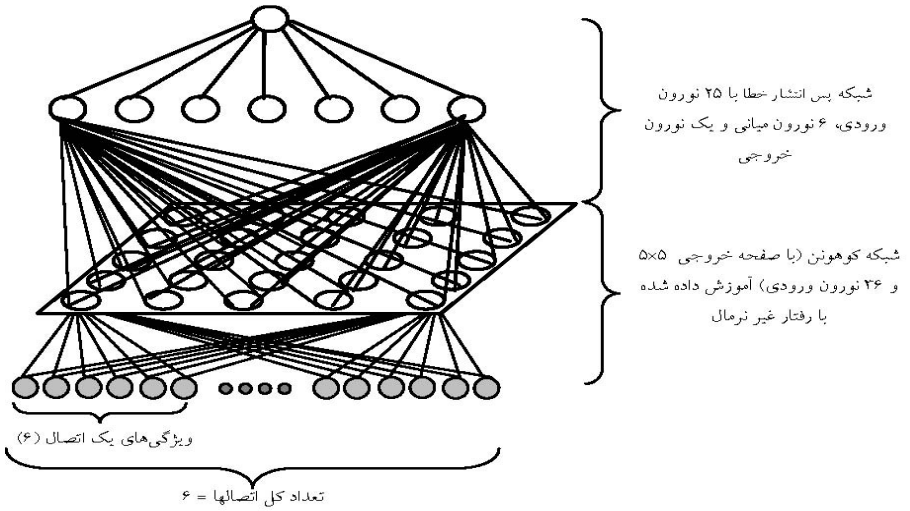
شکل ۳ (سیستم اول): طراحی سیستم اول با استفاده از شبکه عصبی کوهونن با صفحه خروجی ٦×٦ و شبکه عصبی پس انتشار خطا با ۳٦ نورون ورودی، ٦ نورون در لایه میانی و یک نورون در لایه خروجی

آموزش می‌دهیم. بدین‌ترتیب که تمامی مجموعه آموزشی،شامل اتصالات حمله و غیرحمله را به ورودی شبکه کوهونن آموزش دیده - که آموزش آن فقط با داده‌های عادی انجام شده - اعمال می‌کنیم. سپس به‌جای آنکه با اعمال ورودی، مقدار فعالیت نورون برنده را برابر یک و بقیه نورونها را برابر صفر بگیریم، مقدار فعالیت هر نورون در صفحه خروجی دو شبکه کوهونن را برابر با مقدار فاصله‌ای که بردار ورودی با بردار وزنهای متصل به آن نورون دارد، قرار می‌دهیم. در واقع، مقادیر این نورونها در صفحه خروجی کوهونن بیانگر مقدار فاصله‌ای است که ورودی از رفتار عادی دارد. سپس نورونهای صفحه خروجی شبکه کوهونن را به‌عنوان ورودی به شبکه پس انتشار خطا اعمال می‌کنیم. خروجی مطلوب را برای نمونه‌هایی که حداقل یک اتصال آن در حمله شرکت داشته، برابر ۱+ و برای نمونه‌هایی که هیچ اتصال آن در حمله‌ای شرکت نداشته، برابر ۱- تعریف می‌کنیم (d_1=۱ و d_2=-1). شبکه پس انتشار خطا، با استفاده از ورودیهای خود - که برابر با اختلاف بردار ورودیهای اصلی از بردار وزنهای کوهونن (رفتار عادی) است - و خروجی مطلوب، وزنهای خود را طوری تنظیم می‌کند که بتواند رفتار ناهنجار را تشخیص دهد.

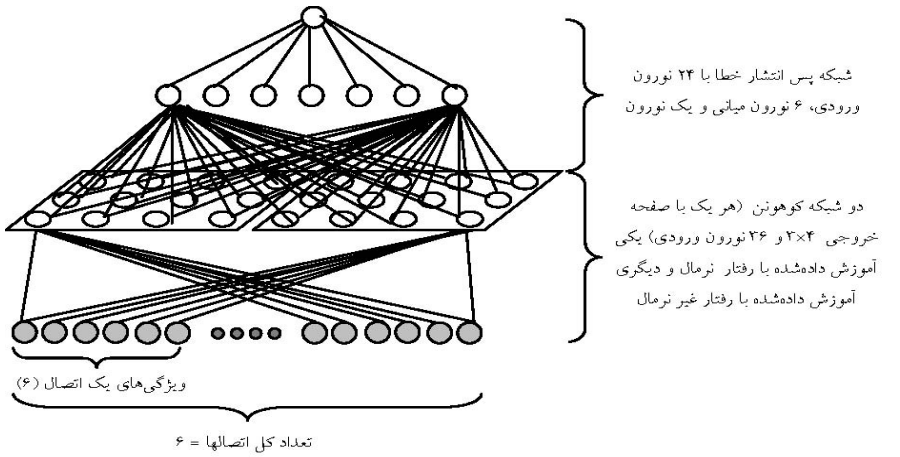
۵-۲- (سیستم دوم): طراحی سیستم تشخیص سوءاستفاده (آموزش رفتار غیرعادی) (شکل٤)

این سیستم مانند سیستم اول طراحی می‌شود، با این تفاوت که به‌جای رفتار عادی، رفتار غیرعادی (یعنی حمله) به شبکه کوهونن آموزش داده می‌شود. با آموزش شبکه کوهونن، با مجموعه نمونه‌هایی که حداقل یک اتصال حمله در آن وجود دارد (مجموعه عاری از اتصال عادی)، انتظار داریم که بردارهای وزنهای شبکه کوهونن در فضای ورودی، معرف ناحیه ترافیک غیرعادی باشد. سپس از این شبکه پس انتشار خطا آموزش داده شده در شبکه عصبی پیشنهادی استفاده کرده و مرحله دوم آموزش را دقیقاً مانند مرحله دوم آموزش در سیستم اول، با تمامی مجموعه داده،

[Downloaded from mjee.modares.ac.ir on 2024-04-30]



شکل ۴ (سیستم دوم): طراحی سیستم دوم با استفاده از شبکه عصبی کوهونن با صفحه خروجی ۵×۵ و شبکه عصبی پس انتشار خطا با ۲۵ نورون ورودی، ٦ نورون در لایه میانی و یک نورون در لایه خروجی



شکل ۵ (سیستم سوم): طراحی سیستم سوم با استفاده از شبکه عصبی کوهونن با صفحه خروجی ۳×٤ و شبکه عصبی پس انتشار خطا با ٢٤ نورون ورودی، ٦ نورون در لایه میانی و یک نورون در لایه خروجی

شامل داده‌های عادی و غیرعادی انجام می‌دهیم.

۵-۳- (سیستم سوم): طراحی سیستم ترکیبی تشخیص ناهنجاری - تشخیص سوءاستفاده (آموزش رفتار عادی و غیرعادی) (شکل۵)

در این سیستم دو شبکه کوهونن را برای آموزش رفتار عادی و غیرعادی انتخاب می‌کنیم. مانند سیستم اول، رفتار عادی را به یک شبکه کوهونن و مانند سیستم دوم، رفتار غیرعادی را به شبکه کوهونن دیگری، آموزش می‌دهیم. در این مرحله انتظار داریم که بردارهای وزنهای شبکه کوهونن اول، در فضای ورودی معرف ناحیه ترافیک عادی و بردارهای وزنهای شبکه کوهونن دوم، معرف

[Downloaded from mjee.modares.ac.ir on 2024-04-30]

جدول ۲- الف مقادیر مشترک پارامترهای شبکه کوهونن در هر سه سیستم

تعداد یا نام اختصاری	نام تابع یا پارامتر
Topology function	تابع ساختار
Distance function	تابع فاصله ای
Learning rate function	تابع نرخ یادگیری
Ordering phase learning rate	تابع یادگیری مرحله بترتیب و توالی
Tuning phase learning rate	نرخ یادگیری مرحله تنظیم

جدول ۲ - ب مقادیر مشترک پارامترهای شبکه پس انتشار خطا در هر سه سیستم

تعداد یا نام اختصاری	نام تابع یا پارامتر
Backprop network training function	تابع آموزش
Backprop weight/bias learning function	تابع یادگیری / بایاس
Transfer function	تابع تبدیل
Performance function	تابع عملکرد
Number of Hidden Neurons	تعداد نورون میانی
Number of Output Neurons	تعداد نورون خارجی

جدول ۳- الف پارامترهای شبکه کوهونن سیستم اول

نام تابع یا پارامتر	مقدار یا نام اختصاری
تعداد خروجی	٦×٦
تعداد دفعات	۵۰

جدول ۳- ب پارامترهای شبکه پس انتشار خطا سیستم اول

نام تابع یا پارامتر	مقدار یا نام اختصاری
تعداد ورودی	۲۵
تعداد دفعات	۲۰۰۰۰

جدول ٤- الف پارامترهای شبکه کوهونن سیستم دوم

نام تابع یا پارامتر	مقدار یا نام اختصاری
تعداد خروجی	۵×۵
تعداد دفعات	۱۰۰

جدول ٤- ب پارامترهای شبکه پس انتشار سیستم دوم

نام تابع یا پارامتر	مقدار یا نام اختصاری
تعداد ورودی	۳٦
تعداد دفعات	۲۰۰۰۰

جدول ۵ – الف پارامترهای شبکه کوهونن سیستم سوم

نام تابع یا پارامتر	مقدار یا نام اختصاری
تعداد خروجی	۳×٤
تعداد دفعات	۵۰

جدول ۵- ب پارامترهای شبکه پس انتشار خطا سیستم سوم

نام تابع یا پارامتر	مقدار یا نام اختصاری
تعداد ورودی	۲٤
تعداد دفعات	۱۰۰۰۰

ناحیه ترافیک غیر عادی شبکه های کامپیوتری باشد، سپس از این دو شبکه کوهونن آموزش داده شده، در شبکه عصبی پیشنهادی استفاده می‌کنیم. مرحله دوم آموزش را نیز دقیقاً مانند دو سیستم قبل انجام می‌دهیم. بدین‌ترتیب که تمام مجموعه آموزشی، شامل اتصالات حمله و غیرحمله، را به ورودی دو شبکه کوهونن آموزش دیده – که آموزش آنها به‌طور جداگانه و فقط با داده‌های عادی و غیرعادی انجام شده – اعمال می‌کنیم. سپس به جای آنکه با اعمال ورودی، مقدار فعالیت نورون برنده را یک و بقیه نورونها را صفر بگیریم، مقدار فعالیت هر نورون در صفحه خروجی دو شبکه کوهونن را برابر با مقدار فاصله‌ای که بردار ورودی با بردار وزنهای متصل به آن نورون دارد، قرار می‌دهیم. در واقع، مقادیر این نورونها در صفحه خروجی شبکه کوهونن بیانگر مقدار فاصله‌ای است که ورودی از ترافیک عادی و غیرعادی دارد. سپس نورونهای صفحه خروجی دو شبکه کوهونن را به عنوان ورودی به شبکه پس انتشار خطا اعمال می کنیم. شبکه پس انتشار خطا از روی ورودیهای خود – که برابر با اختلاف

[Downloaded from mjee.modares.ac.ir on 2024-04-30]

بردار ورودیهای اصلی از بردار وزنهای شبکه کوهونن اول (یعنی رفتار عادی) و شبکه کوهونن دوم (یعنی رفتار غیرعادی) است – و خروجی مطلوب (یعنی ۱+ برای ترافیک غیرعادی و ۱- برای ترافیک عادی)، وزنهای خود را طوری تنظیم می‌کند که بتواند رفتار ناهنجار را تشخیص دهد.

خروجی شبکه پس انتشار خطا مقادیری پیوسته در بازه [۱۱] است. همانطور که قبلاً نیز ذکر شد، برای آنکه مشخص کنیم حمله‌ای رخ داده یا در حال وقوع است، مقدار آستانه T را در نظر می‌گیریم. چنانچه خروجی شبکه پس انتشار خطا از مقدار آستانه بیشتر شود، ترافیک جاری شبکه را به‌عنوان حمله و چنانچه کمتر باشد، به‌عنوان ترافیک عادی تشخیص می‌دهیم. جهتگیری مصالحه میان خطای منفی و مثبت، برای مقادیر آستانه متفاوت، تغییر می‌کند.

در هر سه سیستم، توانمندی شبکه عصبی پیشنهادی در مقایسه با روشهای ارائه شده توسط دیگران را بررسی می‌کنیم. علاوه بر این، اثر به‌کارگیری توأم آموزش رفتار عادی و غیرعادی در سیستم سوم را که در آن به‌خلاف رویکرد سیستمهای سنتی تشخیص نفوذ، از ترکیب سیستم تشخیص ناهنجاری و سوءاستفاده، استفاده شده نیز بررسی می‌کنیم.

٦- نتایج

حدود ۳۰۰۰۰۰ اتصال از مجموعه داده‌های سال ۱۹۹۸ مربوط به ارزیابی سیستمهای تشخیص نفوذ را (۲۷ درصد اتصالات، حمله و بقیه، اتصال عادی) به‌عنوان مجموعه داده آموزشی انتخاب کردیم. حمله‌ها، هر چهار دسته حمله‌های پایگاه داده DARPA را در بر می‌گیرد. برای رسیدن به مقادیری از پارامترها که منجر به بهترین نتیجه شود، هر یک از سیستمها را چندین بار با مقادیر مختلف پارامترها طراحی کرده‌ایم. در هر یک از سیستمها، فرایند آموزش در دو مرحله جدا از هم با استفاده از نرم‌افزار MATLAB و به روش گفته شده انجام شد. مقادیر نهایی پارامترها برای شبکه‌های پس انتشار خطا و کوهونن در شبکه عصبی پیشنهادی در جدولهای ۳، ٤ و ٥ به‌ترتیب برای سه سیستم آورده شده است. مقادیر پارامترهایی که در سه سیستم یکسان بوده، در جدول ۲ آورده شده است. توجه شود که مقادیر مشترک و غیرمشترک پارامترها، پس از مشاهده نتایج چندین سیستم به‌دست آمده است.

برای ارزیابی عملکرد سیستم تشخیص نفوذ، حدود ۲۰۰۰۰۰ اتصال (۱۹ درصد اتصالات، حمله و بقیه، اتصال عادی) متفاوت با مجموعه داده‌های آموزشی را به‌عنوان مجموعه داده‌های آزمون انتخاب کرده‌ایم. حدود ٤۰ درصد از حمله‌های مجموعه داده‌های ارزیابی، عضو مجموعه آموزشی نیستند. این نوع حمله‌ها را به‌عنوان حمله‌های جدید در نظر می‌گیریم که هر چهار دسته حمله‌های پایگاه داده DARPA را در برمی‌گیرند. نتایج این سه سیستم را براساس نرخ خطای مثبت و منفی برای مقادیر متفاوت آستانه و همچنین میزان پیچیدگی بیان می‌کنیم. نرخ خطا بر طبق روابط ۳ و ٤ محاسبه می‌شود. پیچیدگی را برابر با تعداد عملیات ضرب و جمعی که لازم است تا مقدار فعالیت نورون خروجی به‌دست آید، تعریف می‌کنیم.(۵) که معیاری برای بیان بار پردازشی سیستم تشخیص نفوذ است. نتایج مربوط به سیستم اول در شکل ٦ و جدول ۷، سیستم دوم در شکل ۷ و جدول ۸ و سیستم سوم در شکل ۸ و جدول ۹ آورده شده است. در جدول ۱۰ نتایج برحسب پیچیدگی و کمترین خطای مثبت و منفی آورده شده است.

[Downloaded from mjee.modares.ac.ir on 2024-04-30]

جدول ۷ مقادیر خطا برحسب مقادیر آستانه (سیستم اول)

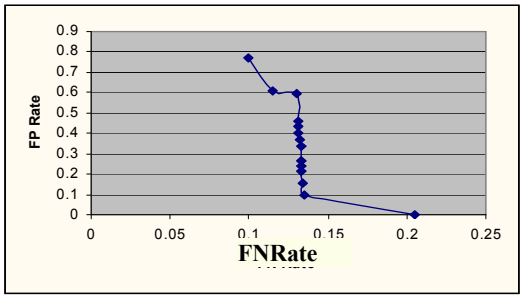
Threshold	FN Rate	FP Rate
−۰/۵	۰/۰۹۹۱٤	۰/۷۷۰٤٤
−۰/٤	۰/۱۱۵۲۳	۰/٦۱۰۰۱
−۰/۳	۰/۱۳۰۱۰	۰/۵۹۵۱
−۰/۲	۰/۱۳۱۰۹	۰/٤٦۱۲۳
−۰/۱	۰/۱۳۱٤۵	۰/٤۳۱۸۱
۰	۰/۱۳۱٦۱	۰/٤۰۳۱۳
۰/۱	۰/۱۳۲۰۱	۰/۳۷۱۲۳
۰/۲	۰/۱۳۲۷۵	۰/۳۳۸۱۱
۰/۳	۰/۱۳۳۱۱	۰/۲٦۵۱۵
۰/٤	۰/۱۳۳۲۰	۰/۲۳۷٦۱
۰/۵	۰/۱۳۳٤۱	۰/۲۱٤٤۵
۰/٦	۰/۱۳۳۸۷	۰/۱۵۵۵۵
۰/۷	۰/۱۳٤۷۷	۰/۰۹۸۵۵
۰/۸	۰/۲۰٤۹۵	۰/۰۰۲۵۹

جدول ۸ مقادیر خطا برحسب مقادیر آستانه (سیستم دوم)

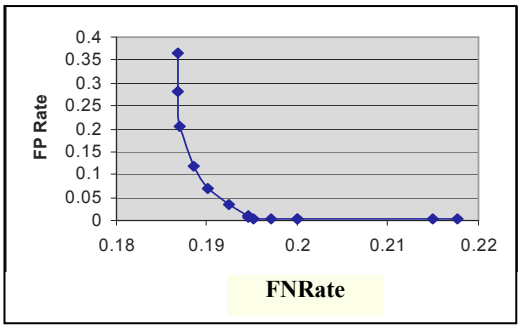
Threshold	FN Rate	FP Rate
−۰/۵	۰/۱۸٦۸۷	۰/۳٦۵۰۱
−۰/٤	۰/۱۸٦۸۷	۰/۲۸۱۰۱
−۰/۳	۰/۱۸٦۹۰	۰/۲۰٦۱۳
−۰/۲	۰/۱۸۸٤۵	۰/۱۱۹۱٤
−۰/۱	۰/۱۹۰۱۱	۰/۰۷۱۱۲
۰	۰/۱۹۲۵۰	۰/۰۳٦۱۱
۰/۱	۰/۱۹٤۵۱	۰/۰۱۰۱۲
۰/۲	۰/۱۹٤٦۳	۰/۰۰۵٤٤
۰/۳	۰/۱۹۵۱۹	۰/۰۰٤۵۳
۰/٤	۰/۱۹۷۰۵	۰/۰۰۳۵۱
۰/۵	۰/۱۹۹۹٦	۰/۰۰۲۳۲
۰/٦	۰/۱۹۹۹۹	۰/۰۰۲۱۲
۰/۷	۰/۲۱۵۰٤	۰/۰۰۲۱۳
۰/۸	۰/۲۱۷٦۵	۰/۰۰۲۱٤

جدول ۹ مقادیر خطا بر حسب مقادیر آستانه (سیستم سوم)

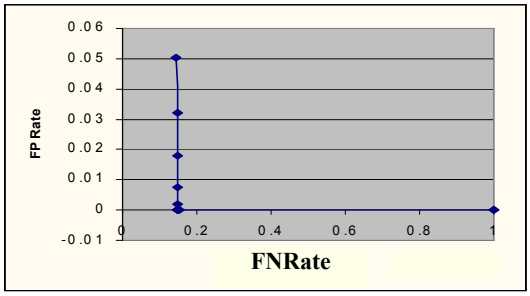
Threshold	FN Rate	FP Rate
−۰/۵	۰/۱٤۲۹۵	۰/۰۵۰۲۵
−۰/٤	۰/۱٤۷۹۵	۰/۰۳۲۱۹
−۰/۳	۰/۱٤۷۹۵	۰/۰۱۸۰۱
−۰/۲	۰/۱٤۷۹۵	۰/۰۰۷۳۲
−۰/۱	۰/۱٤۷۹۵	۰/۰۰۲۱۰
۰	۰/۱٤۷۹۵	۰
۰/۱	۰/۱٤۷۹۵	۰
۰/۲	۰/۱٤۷۹۵	۰
۰/۳	۰/۱٤۷۹۵	۰
۰/٤	۰/۱٤۷۹۵	۰
۰/۵	۰/۱۵۰۸۹	۰
۰/٦	۰/۱۵۰۸۹	۰
۰/۷	۱	۰
۰/۸	۱	۰



شکل ٦ نرخ خطای مثبت برحسب نرخ خطای منفی (سیستم اول)



شکل ۷ نرخ خطای مثبت برحسب نرخ خطای منفی (سیستم دوم)



شکل ۸ نرخ خطای مثبت برحسب نرخ خطای منفی (سیستم سوم)

[Downloaded from mjee.modares.ac.ir on 2024-04-30]

جدول ۱۰ نتایج برحسب مقادیر خطای مثبت و منفی و پیچیدگی برای سه سیستم

پارامتر ارزیابی	پیچیدگی	خطای مثبت	خطای منفی
سیستم ۱	۲۹۹۳	۰/۰۰۲۵	۰/۲۰۴۹
سیستم ۲	۲۰۸۰	۰/۰۰۲۱	۰/۲۱۷۶
سیستم ۳	۱۹۹۷	۰	۰/۱۴۷۹

$$FN = \frac{No.\ of\ attack\ \ patterns\ \ with\ \ scores\ \ smaller\ \ than\ \ T\ (Detected\ \ as\ normal\ )}{Total\ \ No.\ of\ attack\ \ patterns} \quad (۳)$$

$$FP = \frac{No.\ of\ normal\ \ patterns\ \ with\ \ scores\ \ greater\ \ than\ T\ (Detected\ \ as\ attack\ )}{Total\ \ No.\ of\ normal\ \ patterns} \quad (۴)$$

$$\begin{aligned} Complexity = {} & No.\ of\ SOM\ \ Output\ Neurons \times (2 \times No.\ of\ Input\ Neurons - 1) + \\ & No.\ of\ BP\ Hidden\ Layer\ Neurons \times (2 \times No.of\ SOM\ Output\ Neurons - 1) + \\ & No.\ of\ BP\ \ Output\ Neurons \times (2 \times No.\ of\ BP\ Hidden\ Layer\ Neurons - 1) \end{aligned} \quad (۵)$$

۷- نتیجه‌گیری و پیشنهاد برای ادامه کار

نتایج به‌دست آمده بیانگر توانمندی شبکه عصبی معرفی شده در تشخیص ترافیک عادی و ترافیک غیرعادی، مناسب بودن ساختار ارائه شده برای سیستم تشخیص نفوذ مبتنی بر شبکه و همچنین اثر ترکیب سیستمهای تشخیص ناهنجاری و تشخیص سوءاستفاده در بهبود عملکرد سیستمهای تشخیص نفوذ است.

برای مقایسه عملکرد سیستمهای تشخیص نفوذ طراحی شده با سیستمهای موجود، می توان از چهار ویژگی مطرح شده در این مقاله استفاده کرد. ابتدا نتایج سیستمهای به دست آمده را مقایسه کرده و نتیجه گیری می کنیم، آنگاه نتایج سیستم پیشنهادی را با کارهای مشابه دیگران مقایسه می کنیم.

در میان سه سیستم، سیستم سوم به دلیل استفاده همزمان از آموزش ترافیک عادی و غیرعادی، بهترین نتیجه را به دست می دهد. سیستمهای دوم و سوم تقریباً از نظر خطای مثبت و منفی نتایج مشابهی دارند،اما سیستم دوم، پیچیدگی کمتری نسبت به سیستم اول دارد. لذا مشخص می‌شود که آموزش رفتار غیرعادی در کنار رفتار\دوم، پیچیدگی کمتری نسبت به سیستم اول دارد. لذا مشخص می‌شود که آموزش رفتار غیرعادی در کنار رفتار عادی، باعث کمتر شدن خطای مثبت و منفی و همچنین کمتر شدن بار پردازشی می‌شود. روش پیشنهادی ما برای سیستم تشخیص نفوذ، هر چهار ویژگی مطرح شده برای سیستم خوب تشخیص نفوذ را دارد؛ یعنی:

۱- برای سیستم سوم توانستیم با بهره‌گیری از توانمندی شبکه عصبی پیشنهادی و همچنین با استفاده از آموزش رفتار غیرعادی برای مجموعه داده‌های ارزیابی، خطای مثبت را به صفر و خطای منفی را به ۰/۱۴۷۹ برسانیم. این مقادیر برای مجموعه داده ارزیابی – که متفاوت از مجموعه داده آموزشی انتخاب شد – به‌دست آمده و نشانه خوبی از توانمندی روش پیشنهادی است.

[Downloaded from mjee.modares.ac.ir on 2024-04-30]

۲- سیستم سوم پیچیدگی کمتری نسبت به کارهای دیگران و همچنین دو سیستم اول و دوم دارد و بار پردازشی زیادی نیز ندارد.

۳- از آنجاکه در هر سه سیستم، فرایند یادگیری به‌طور خودکار توسط شبکه عصبی انجام می‌شود، درصورت نیاز به آموزش مجدد، فقط به‌روز کردن مجموعه داده‌های آموزشی نیاز است و نیازی به به‌دست آوردن مجدد قوانین نیست.

۴- همچنین ازآنجا که در ساختار پیشنهادی، تصمیم‌گیری براساس مقدار آستانه از پیش تعیین شده‌ای انجام می‌شود، می‌توان با تغییر مقدار آستانه، جهتگیری مصالحه میان خطای منفی و مثبت را به‌دلخواه تعیین کرد.

هر سه سیستم نشان می‌دهند که شبکه عصبی پیشنهادی نسبت به کارهای مشابه ارائه شده توسط دیگران، برتری قابل‌توجهی دارد. در بهترین نتیجه موجود از کارهای دیگران [۱۸] که از کل مجموعه داده و از تمامی ٤١ ویژگی مجموعه داده‌های DARPA برای آموزش استفاده کرده (در مقایسه، ما فقط از شش ویژگی استفاده کرده‌ایم) و همچنین ارزیابی آن روی تمام مجموعه داده‌های ارزیابی، نرخ خطای منفی تقریباً برابر ۰/۳۳ و نرخ خطای مثبت برابر ۰/۰۰۲ بوده است. در [۱] نیز در بهترین حالت - که با بار پردازشی زیادی همراه است - نرخ خطای منفی برابر ۰/۳٤۹۳ و نرخ خطای مثبت برابر ۰/۰۰۲۰ بوده است. در این مرجع، ترکیبی از روش شبکه عصبی و قاعده‌پی به‌کار گرفته شده است. لذا در آموزش مجدد علاوه بر آموزش شبکه عصبی، قواعد را باید دوباره به‌دست آورد. اگر چه در [۱]، سازوکاری برای مصالحه میان خطای مثبت و منفی وجود دارد، اما در حالتی که مصالحه به‌سمت کمتر شدن خطای مثبت باشد، به ذخیره‌سازی و تحلیل تعداد بیشتری از اتصالات و خروجیهای قبلی شبکه عصبی نیاز است که این به افزایش بار پردازشی و همچنین مقدار حافظه منجر می‌شود.

اکنون برای ادامه کار انجام شده، پیشنهادهایی را مطرح می‌کنیم: در سیستمهای تشخیص نفوذ طراحی شده، فقط از شش ویژگی ترافیک شبکه برای تشخیص نفوذ در شبکه استفاده شده است. پیشنهاد می‌شود در ادامه این کار، سایر ویژگیها (مانند ویژگیهای دیگر تهیه شده در پایگاه داده DARPA) نیز استفاده و تأثیر این ویژگیها در عملکرد سیستم تشخیص نفوذ بررسی شود. همچنین ویژگیهای مؤثر در تشخیص هر یک از انواع حمله‌های کامپیوتری شناسایی شوند. در صورت انجام این کار، مشخص می‌شود که برای شناخت هر دسته از حملات بهتر است از کدام ویژگیهای ترافیکی شبکه استفاده شود. در این حالت طراحی سیستمهای تشخیص ناهنجاری به سمتی سوق داده می‌شود که به تشخیص حمله‌های خاصی متمرکز شوند و از ویژگیهایی که امکان تشخیص آن نوع حمله را بیشتر می‌کند، استفاده کنند. این‌گونه سیستمها احتمالاً خطای کمتری دارند.

۸- منابع

[1] P. Lichodzijewski, A. N. Zincir-Heywood, and M. I. Heywood, "Dynamic intrusion detection using self-organizing maps", Proc. of the 14th Annual Canadian Information Technology Security Symp.- CITSS 2002, pp. 127-131, Canada, 2002.

[2] J. Cannady, "Applying CMAC-based online learning to intrusion detection", Proc. of the Int. Joint Conf. on Neural Networks, pp. 405 – 410, Italy, 24 – 27 July 2000.

[3] J. Cannady, "Applying neural networks to misuse detection," Proc. of the 21st

[Downloaded from mjee.modares.ac.ir on 2024-04-30]

National Information Systems Security Conf., 1998.

[4] H. Debar, M. Dacier, and A. Wespi, "Towards a taxonomy of intrusion-detection systems," Computer Networks, pp. 805 - 822, 1999.

[5] H. Debar and B. Dorizzi, "An application of a recurrent networks to an intrusion detection system," Proc. of the Int. Joint Conf. on Neural Networks, pp.78-83, June 1992.

[6] K. L. Fox, R. R. Henning, J. H. Reed, and R. P. Simonian, "A neural network approach towards intrusion detection," Proc. of the 13th National Computer Security Conf., pp. 125-134, Washington D. C. , 1990.

[7] B. V. Nguyen, "Self organizing map (SOM) for anomaly detection," Available [Online]: http://132.235.28.162/bnguyen/papers/IDS-SOM.pdf.

[8] P. Lichodzijewski, A. N. Zincir-Heywood, and M. I. Heywood, "Host-based intrusion detection using self organizing maps," Proc. of the 2002 IEEE world Congress on Computational Intelligence, pp. 1714-1719, Hawaii, 2002.

[9] A .K. Ghosh, J. Wanken, and F. Charron, "Detecting anomalous and unknown intrusion against programs," Proc. of the IEEE Conf. on Security Applications, pp. 259-267, December 1998.

[10] K. Labib and R. Venmuri, "NSOM: a real-time networked based intrusion detection system using self-organizing maps," Available [online]: http://www.cs.ucdavis .edu /~vemuri/ papers/som-ids.pdf.

[11] B. Rahodes, J. Mahaffey, and J. Canady, "Multiple self organizing maps for intrusion detection system," Proc. of the NISSC Conference, Baltimore, MD, 2000.

[12] K. Tan, "The application of neural networks to UNIX computer security," Proc. of the IEEE Int. Conf. on Neural Networks, vol. 1, pp. 476-481. 1995.

[13] A. R. Sharafat and M. Rasti, "Real time anomaly detection in computer networks using self organizing maps and back propagation neural networks," Proc. of IST 2003, pp. 552-555, Isfahan, Iran, 2003.

[14] A. R. Sharafat and M. Rasti, and A. Yazdian, "Neural network based dynamic anomaly detection in computer networks: a novel training paradigm using abnormal behavior," Proc. of ICAINE 2003, Nevada USA, pp. 50-53, 2003.

[15] T. Kohonen, Self Organizing Maps, Vol. 30 of Springer Series in Information Science, Springer, Berlin, Heidelberg, 1995.

[16] DARPA Off-Line Intrusion Detection Evaluation Schedule, Available [online]: http://www.ll.mit.edu/IST/ideval/docs/1998/schedule.html.

[Downloaded from mjee.modares.ac.ir on 2024-04-30]

[17] The Third International Knowledge Discovery and Data Mining Tools Competition, Available [online]: http://kdd.ics.uci.edu/databases/kddcup99 .kddcup99.html.

[18] W. Lee, S. J. Stolfo, and K. W. Mok, "Mining in a data-flow environment: experience in network intrusion detection," Knowledge Discovery and Data Mining Journal, pp. 114-124, 1999.

[19] M. Petrakos, J. A. Benediktsson, and I. Kanellopoulos, "The effect of classifier agreement on the accuracy of the combined classifier in decision level fusion," IEEE Trans. on Geoscience and Remote Sensing, vol. 39, No. 11, pp. 2539-2546, November 2001.

[20] K. Turner and J. Ghosh, "Error correlation and error reduction in ensemble classifiers", Connection Science, vol. 8, pp. 385-404, December1996.

[21] A. J. C. Sharkey, "On combining artificial neural nets", Connection Science, vol. 8, pp. 299-314, December 1996.

[22] A. J. C. Sharkey and N. E. Sharkey, "Combining diverse neural nets," The Knowledge Engineering Review, vol. 12, pp. 231-247, June 1997.

[23] D. Patridge and W. B. Yates, "Engineering multiversion neural-net systems," Neural Computation, vol. 8, pp. 869-893, May 1996.

[Downloaded from mjee.modares.ac.ir on 2024-04-30]