مقایسه فن های طبقه بندی مورد استفاده برای تشخیص و طبقه بندی نفوذ شبکه

چکیده

در تحقیق قبلی، یک سیستم ایمنی مصنوعی چندگانه برای شناسایی و طبقه‌بندی نفوذ شبکه پیشنهاد و آزمایش شد که در آن یک فرایند تشخیص و طبقه‌بندی چندلایه روی هر عامل برای هر میزبان در شبکه اجرا شد. در این مقاله، ما آزمایش‌هایی را انجام می‌دهیم که با طبقه‌بندی‌های مختلف طبقه‌بندی‌های مناسب را انتخاب کرده و آن‌ها را مقایسه می‌کنیم تا دقت تشخیص را افزایش دهیم و اطلاعات بیشتری در مورد ناهنجاری‌های تشخیصی به دست آوریم. نشان داده خواهد شد که به دلیل نرخ‌های مختلف طبقه‌بندی به‌دست‌آمده، هیچ طبقه‌بندی نمی‌بایست برای تمام انواع حملات استفاده شود. این به خاطر نمایش حملات در مجموعه سلسله و وابستگی بین ویژگی‌های مورداستفاده برای شناسایی آن‌ها است. همچنین نشان داده خواهد شد که یک طبقه‌بندی کننده ساده و اساسی مانند Naive Bayes دارای نتایج طبقه‌بندی بهتر در مورد حملات کم نشان داده‌شده است و درخت تصمیم‌گیری اولیه مانند درخت Naive-Bayes Tree و Best-First نتایج بسیار خوبی نسبت به J48 معروف (اجرای وکا C4.5) و درخت تصمیم‌گیری Random Forest ارائه می‌دهد. بر اساس این آزمایش‌ها و نتایج آن‌ها، طبقه‌بندی کننده‌های Naive Bayes و Best-First برای طبقه‌بندی ترافیک ناشناخته انتخاب شدند. نشان داده‌شده است که در مرحله تشخیص 90٪ ناهنجاری‌ها شناسایی‌شده و در مرحله طبقه‌بندی 88٪ از مثبت‌های کاذب با موفقیت به‌عنوان اتصالات ترافیکی عادی برچسب‌گذاری شده و 79٪ از حملات DoS و Probe به‌درستی توسط NB، NBTree و طبقه‌بندی کننده BFTree برچسب‌گذاری شده‌اند.

کلید واژه ها: تشخیص نفوذ. سیستم های ایمنی مصنوعی. طبقه بندی نفوذ. فراگیری ماشین

1. معرفی

امروزه دستگاه‌های کامپیوتری معمولاً به هم متصل هستند که به دستگاه‌های توزیع‌شده بزرگ وصل هستند که در دنیای محاسبات صنعتی ضروری هستند. دستگاه‌های نرم‌افزاری امروز نیازمند روندهایی مانند اتصالات، هوش و فراگیری هستند که همگی منجر به ایجاد دستگاه‌های چند عامل شد. دستگاه‌های چندگانه رفتار هوشمندانه انسان و نحوه ارتباط انسان‌ها با یکدیگر و با محیط آن‌ها برای دستیابی به اهداف خاص را تقلید می‌کند. یکی از دستگاه‌هایی که می‌تواند به‌صورت موفقیت‌آمیز و کارآمد به‌عنوان یک سیستم‌عامل چندگانه اجرا شود، دستگاه‌های ایمنی مصنوعی (AIS) است. سیستم ایمنی مصنوعی یک منطقه پژوهشی است که شامل ایمنی‌شناسی، علوم رایانه و مهندسی است. با الهام از دستگاه‌های ایمنی طبیعی، سه زمینه اصلی تحقیق تحت AIS قرار می‌گیرند: مدل‌سازی ایمنی، AIS های نظری و AIS های کاربردی. مدل‌سازی ایمن در مورد مدل‌های ایمنی و شبیه‌سازی سیستم ایمنی است. پژوهش AIS های نظری در مورد توضیح و نفوذ به جنبه‌های نظری الگوریتم‌های AIS، مدل‌های ریاضی و عملکرد و تجزیه‌وتحلیل پیچیدگی آن‌ها است. درنهایت، تحقیق AIS های کاربردی در مورد توسعه و اجرای الگوریتم‌ها و دستگاه‌های کامپیوتری الهام گرفته از دستگاه‌های ایمنی است که از آن‌ها برای انواع برنامه‌های کاربردی دنیای واقعی استفاده می‌شود.

با توجه به دستگاه‌های کامپیوتری می‌توانیم بفهمیم که مفهوم خود/ غیر خود در قالب فعالیت‌ها و عناصری معمولی/ غیرعادی اعمال می‌شود. دستگاه‌های تشخیص نفوذ (IDS) دستگاه‌های امنیتی قدرتمندی هستند که انواع مختلفی برای اهداف حفاظتی دارند. آن‌ها ابزار امنیتی خاصی را جایگزین نمی‌کنند، بلکه به‌جای آن، یک خط دفاعی در برابر نفوذها و تهدیدات از داخل سیستم (یک کامپیوتر یا یک شبکه) و همچنین از خارج- درست مانند سیستم ایمنی اضافه می‌کنند. IDS ها می‌توانند به روش‌های مختلف دسته‌بندی شوند، اما اساساً می‌توان آن‌ها را به IDS هایی مبتنی بر سوءاستفاده و ناهنجار تقسیم کرد. IDS های سوءاستفاده که همچنین به‌عنوان مبتنی بر امضا یا دانش شناخته می‌شوند، بستگی به تشخیص نفوذ با استفاده از الگوهای نشان‌دهنده حملات شناخته‌شده دارد. این الگوها یا امضاها با رویدادها برای یافتن نفوذهای ممکن مقایسه می‌شوند. IDSهای غیرمتعارف که همچنین به‌عنوان IDS های مبتنی بر رفتار شناخته می‌شود، به ساخت یک نمایه بستگی دارد که رفتار طبیعی یک سیستم

را با نظارت بر فعالیت‌های آن در طول زمان نشان می‌دهد. سپس هر انحراف از آن نمایه، یک ناهنجاری است. نمایه‌ها می‌توانند ایستا یا پویا باشند و با استفاده از بسیاری از ویژگی‌های سیستم توسعه می‌یابند.

با تنوع و پیچیدگی فن‌های حمله، بسیاری از مسائل در رابطه با IDS ها رایج هستند که باید در هنگام ساخت IDS موردتوجه قرار گیرند [17]. شایع‌ترین مسئله، استخراج مجموعه‌ای از قوانین تخصصی است که در اغلب موارد از طریق یک متخصص انسانی به‌خصوص با استفاده از IDS سوءاستفاده به‌روز می‌شود. با تشخیص ناهنجاری، چنین مسئله‌ای با استفاده از نمایش مناسب و تعریف حملات حل می‌شود، بنابراین انواع مختلف حملات می‌تواند با استفاده از مجموعه‌ای محدود از قوانین با تغییرات این قوانین شناسایی شود. یکی دیگر از مسائل، مربوط به آموزش مدل‌های رفتاری است که معمولاً اطلاعات عادی یا دو مجموعه داده‌های عادی و غیرعادی برای آموزش استفاده می‌شود. فن‌های یادگیری ماشینی بیشتر برای آموزش و یادگیری استفاده می‌شود.

در تلاش برای غلبه بر مسائل ذکرشده در بالا، ما یک الگوریتم طبقه‌بندی دولایه با چندعاملی را پیشنهاد کردیم که ناهنجاری‌ها را در یک شبکه تشخیص می‌دهد و طبقه‌بندی می‌کند. IDS سیستم پیشنهادی ترکیبی از الگوریتم ژنتیک با روش انتخاب منفی به‌عنوان اولین لایه شناسایی ناهنجاری‌ها است. سپس طبقه‌بندی کننده‌های انتخاب‌شده برای ترسیم ناهنجاری‌های شناسایی‌شده در هر دو ترافیک نرمال و غیرطبیعی آموزش داده می‌شود و به‌کاربرده می‌شود. سیستم ایمنی یک سیستم توزیعی از سلول‌های تخصصی متفاوتی است که دارای تعامل بالا بین اجزای آن برای یک پاسخ هماهنگ است. با توجه به این، بسیاری از رویکردها، اجرای یک AIS را به‌عنوان یک سیستم‌عامل چندگانه پذیرفته‌اند.

در تحقیقات قبلی که به‌نوعی به سیستم پیشنهادشده شبیه هستند، هر نوع طبقه‌بندی کننده خاص برای هر نوع حمله مورداستفاده قرار می‌گیرد، یا طبقه‌بندی کننده‌ها- که با استفاده از داده‌های برچسب‌گذاری شده آموزش داده‌شده‌اند- به‌طور مستقیم به مجموعه داده‌ها برای تشخیص نفوذ و برچسب‌گذاری حملات بدون برچسب اعمال می‌شود. سهم این مقاله این است که برخی تجزیه‌وتحلیل تطبیقی را برای پاسخ به سؤالات در مورد چگونگی عملکرد سیستم در پارامترهای مختلف انجام دهد و این‌که چه فن‌هایی برای بهترین نتایج و دلیل استفاده می‌شود. همچنین بررسی خواهد کرد که آیا تغذیه ترافیک عادی به طبقه‌بندی کننده‌ها اهمیت دارد یا خیر.

در یک گزارش از قبل منتشرشده [8] یک سیستم ایمنی مصنوعی چندگانه برای تشخیص و طبقه‌بندی نفوذ شبکه اعمال شد. الگوریتمی که به‌عنوان یک فن سیستم ایمنی مصنوعی اعمال‌شده است، روش انتخاب منفی است که از الگوریتم ژنتیک استفاده می‌کند. به‌عنوان یک سیستم هوشمند، داده‌کاوی در طول فرایند برای بهترین نتایج استفاده می‌شود. دو طبقه‌بندی کننده برای طبقه‌بندی‌های ناهنجاری، طبقه‌بندی کننده‌های Bayes Naive Bayes و Best-First استفاده شد. طبقه‌بندی کننده Bayes Naive برای حملاتی استفاده شد که ارائه کمی در مجموعه داده‌های آموزشی دارند، زیرا آن‌ها ثابت کرده‌اند که نتایج بهتری نسبت به سایر طبقه‌بندی کننده‌ها در آزمایش قبلی داشته‌اند. طبقه‌بندی کننده BFTree برای طبقه‌بندی حملات باقی‌مانده مورداستفاده قرار گرفت، زیرا آن‌ها نتایج بهتری را نسبت به سایر طبقه‌بندی کننده‌های پیچیده‌تر در آزمایش‌ها این مقاله نشان دادند.

مقاله به‌صورت زیر مرتب‌شده است. بخش 2 زمینه‌ای راجع به اصول فن‌های طبقه‌بندی ارائه می‌دهد. در بخش 3 رویکرد پیشنهادی و مدل سیستم با اجزا و مرحله‌های مختلف آن توضیح داده‌شده است. بخش 4 شامل جزئیات آزمایش و تنظیمات است. نتایج در بخش 5 ارائه‌شده و موردبحث قرار می‌گیرد. درنهایت، نتیجه‌گیری باکار بیشتر در بخش 6 ارائه می‌شود.

2. فن‌های طبقه‌بندی داده‌ها

طبقه‌بندی فرآیند اختصاص یک برچسب طبقه به شیء (اشیاء) طبقه‌بندی نشده بر اساس مجموعه‌ای از ویژگی‌های تعریف‌شده است. یک طبقه‌بندی کننده ابتدا باید آن دانش را با یادگیری ارائه دسته‌ها با استفاده از یک مجموعه داده‌شده از نمونه‌های طبقه‌بندی‌شده پیشین دریافت کند. یک طبقه‌بندی کننده می‌تواند به‌عنوان یک پیش‌بینی کننده برای اشیاء طبقه‌بندی نشده یا یک توصیفگر برای اشیاء طبقه‌بندی‌شده عمل کند. رویکردهای بسیاری مانند درختان تصمیم‌گیری، رویکردهای مبتنی بر قانون، طبقه‌بندی‌های بیزی، شبکه‌های عصبی، طبقه‌بندی کننده‌های ژنتیک، ماشین‌های بردار پشتیبانی و بسیاری دیگر وجود دارد. یک طبقه‌بندی کننده با دقت پیش‌بینی آن، سرعت، استحکام، مقیاس‌پذیری، تفسیرپذیری، سادگی و شاخص‌های کیفیت وابسته به دامنه ارزیابی می‌شود.

2.1. طبقه‌بندی کننده Bayes Naïve

این مطلب تئوری Bayes را با فرضیه‌های استقلال قوی به‌عنوان یک طبقه‌بندی کننده ساده احتمالی اعمال می‌کند. فرض بر این است که وجود یا فقدان یک ویژگی مستقل از وجود یا فقدان ویژگی‌های دیگر است - ویژگی‌ها نامرتبط هستند که اجرای آن‌ها ساده، بهینه و درست است. اگر برخی اطلاعات و داده‌های آموزشی داشته باشیم، می‌توان از طبقه‌بندی کننده NB استفاده کرد و ما باید احتمالات را از داده‌های محدود برآورد کنیم. مزیت اصلی آن این است که زمان زیادی برای آموزش نیاز ندارد.

2.2. درختان تصمیم‌گیری

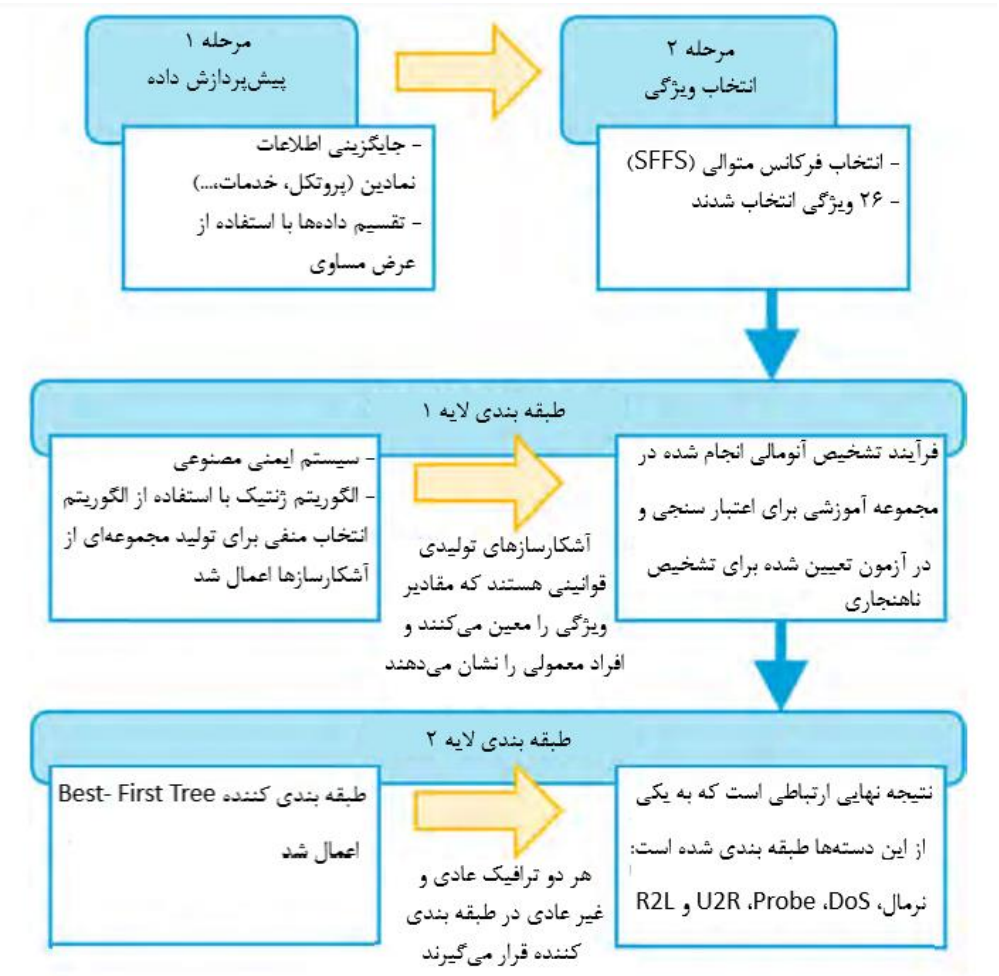
درختان تصمیم‌گیری نمایش ساختاری یک مجموعه داده را تشکیل می‌دهند. یک گره یک تصمیم را از تعدادی از گزینه‌ها می‌سازد و هر گره نهایی یک طبقه‌بندی خاص را نشان می‌دهد. DT ها (درختان تصمیم‌گیری) ابزارهایی بسیار قدرتمند هستند زیرا آن‌ها سریع هستند و عملکرد معقولی دارند. DT های مورداستفاده در این تحقیق BFTree، NBTree، J48 و RFT هستند.BFTree (Best-First Tree) گره‌های خود را در بهترین حالت اول، برخلاف DT های استاندارد گسترش می‌دهد که در حالت عمق اول گسترش می‌یابد. بهترین گرهی که همیشه برای اولین بار گسترش‌یافته است، گرهی است که منجر به حداکثر کاهش ناخالصی می‌شود. NBTree (Naive Bayes Tree) از یک تابع نقشه‌برداری برای فهرست داده‌های با ابعاد بزرگ استفاده می‌کند و باید یک تابع محاسباتی سبک و کم باشد؛ بنابراین، این مقادیر می‌تواند مرتب‌شده و بعداً در ساختار یک‌بعدی نهایی استفاده شود.J48 (نشان‌دهنده وکا C4.5 DT) گره‌های خود را در حالت عمق اول گسترش می‌دهد. این یک الگوریتم یادگیری تحت نظارت است که نقشه‌برداری را از مقادیر ویژگی به طبقات می‌آموزد و سپس این نقشه‌برداری به نمونه‌های ناشناخته جدید اعمال می‌شود. RFT (Forests Forest Random) شامل ایجاد مجموعه‌ای از درختان طبقه‌بندی است که بر اساس مجموعه‌های تصادفی داده‌ها محاسبه می‌شوند. این کار با استفاده از پیش‌بینی کننده‌های انتخاب‌شده به‌صورت تصادفی برای هر تقسیم در هر درخت انجام می‌شود.

2.3. فرایندهای چندلایه

اگر نمونه‌های ارائه‌شده را نتوان به‌صورت خطی جدا کرد، فرایندهای چندلایه (MLP) مورداستفاده قرار می‌گیرند. MLP ها شبکه‌های عصبی ارسالی هستند که شامل تعداد زیادی از عصب‌های متصل شده هستند که به واحدهای ورودی، واحدهای خروجی و واحدهای مخفی در بین آن‌ها تقسیم می‌شوند. وزن‌های اختصاص داده‌شده برای ارتباطات با استفاده از الگوریتم بازگشت عقب (BP) برآورد می‌شود. مقادیر وزن، عملکرد شبکه عصبی را تعریف می‌کنند.

3. سیستم تشخیص و طبقه‌بندی دولایه

سیستم چندلایه‌ای که قبلاً پیشنهادشده بود از دولایه تشکیل‌شده است که پیش از یک مرحله پیش‌پردازش می‌آیند. لایه اول - لایه تشخیص - روش انتخاب منفی را با استفاده از الگوریتم ژنتیک برای تشخیص نفوذ انحراف استفاده می‌کند، جایی که ردیاب‌ها برای شناسایی فعالیت‌های طبیعی آموزش می‌بینند تا هرگونه تفاوت (بیش از یک آستانه مشخص) را به‌عنوان یک ناهنجاری تشخیص دهند. لایه دوم - لایه طبقه‌بندی - از یک طبقه‌بندی کننده برای برچسب‌گذاری ترافیک با طبقه مناسب برای دسته‌های حمله و به حداقل رساندن هشدارهای نادرست استفاده می‌کند. هم ترافیک عادی و هم غیرعادی به طبقه‌بندی کننده داده می‌شود. روند در شکل 1 نشان داده‌شده است.



شکل 1. مدل تشخیص و طبقه‌بندی ناهنجاری‌های دولایه.

3.1. مرحله پیش‌پردازش داده

پیش‌پردازش داده‌ها شامل جایگزینی داده‌های نمادین مانند پروتکل و خدمات با مقادیر مجزا/ کامل و تقسیم‌بندی مقادیر به همگن و در حوزه‌ای محدود است. الگوریتم Binning Width برابر استفاده شد و مقادیر اصلی با اعداد باین مربوط به دامنه آن‌ها جایگزین شدند. اطلاعات بیشتر در مقاله قبلی موجود است.

3.2. مرحله انتخاب ویژگی

همان‌طور که در مقاله قبلی ما [4] بیان‌شده است، روش انتخابی فرکانس متوالی (SFFS) استفاده و 26 ویژگی انتخاب شد که مربوط به برای یافتن الگوریتم انتخاب ویژگی با بهترین نتایج بود. ویژگی‌های انتخاب‌شده توسط SFFS بهترین نتایج دقیق را به دست آورد.

3.3. لایه I: تولید ردیاب‌ها و تشخیص ناهنجاری

این لایه GADG (الگوریتم ژنتیک برای تولید ردیاب‌ها) است - همچنین در [4] - برای تولید ردیاب‌ها برای فرآیند تشخیص نفوذ انحرافی استفاده‌شده است. در این فرآیند، آشکارسازهای ناهنجاری با استفاده از GA و کاربرد مفهوم NSA تولید می‌شوند - تولید آشکارسازهایی که با نمایش اتصالات عادی آشنا هستند، قادر به تشخیص بین عادی و غیرطبیعی هستند. ردیاب‌های یا قوانین تولیدشده اساساً مقادیر ویژگی‌های انتخاب‌شده هستند که به‌طور صحیح اتصالات طبیعی را نشان می‌دهند؛ بنابراین، ابتدا جمعیت مورداستفاده برای تولید این آشکارسازها با انتخاب تصادفی از اتصالات معمول در مجموعه داده پرشده است. دو اندازه‌گیری مسافت به‌طور جداگانه اعمال‌شده است —هندسه اقلیدسی و مین کاوسکی- و گروه آشکارساز تولیدشده توسط هر اندازه‌گیری مسافت آزمایش و مقایسه می‌شود.

جدول 1 توزیع پرونده‌های NSL-KDD.

	Total records	Normal	DoS	Probe	U2R	R2L
Train_20%	25192	13449 53.39%	9234 36.65%	2289 9.09%	11 0.04%	209 0.83%
Train_All	125973	67343 53.46%	45927 36.456%	11656 9.25%	52 0.04%	995 0.79%
Test+	22544	9711 43.08%	7458 33.08%	2421 10.74%	200 0.89%	2754 12.22%

در پایان فرآیند تولید آشکارسازها، آشکارسازهای بالغ به سیستم برای شروع فرآیند جداسازی خود از غیر خود آزاد می‌شوند. آشکارسازها از مقادیر برای ویژگی‌های انتخاب‌شده برای نمایش عناصر خودی تشکیل‌شده است. آشکارسازهای تولیدشده از مرحله قبل از طریق داده‌های آزمایش برای شروع فرآیند تشخیص ناهنجاری اجرا می‌شوند. نتایج به‌دست‌آمده از [4] در لایه بعدی - لایه طبقه‌بندی - برای طبقه‌بندی ناهنجاری‌های تشخیص داده‌شده وارد می‌شود، همان‌طور که در زیر با جزئیات توضیح داده‌شده است.

3.4. لایه دوم: استفاده از دسته‌بندی کننده‌ها برای دسته‌بندی حملات

پس از مرحله تشخیص ناهنجاری، اتصالات به‌عنوان عادی یا غیرطبیعی برچسب‌گذاری شده‌اند، اما نوع حمله مشخص نشده است. طبقه‌بندی کننده باید برای برچسب‌گذاری حملات با دسته خاص خود استفاده شود. بسیاری

از طبقه‌بندی کننده‌ها مورد آزمایش و مقایسه قرار گرفتند. این طبقه‌بندی کننده‌ها عبارت‌اند از Bayes Naive، Decisions Trees - NBTree، BFTree، J48، RFT و شبکه‌های عصبی چندلایه Perceptron. در لایه طبقه‌بندی، هم ترافیک عادی و هم غیرعادی به‌صورت جداگانه طبقه‌بندی می‌شوند. برای ترافیک غیرعادی، ناهنجاری‌ها باید به‌عنوان یکی از دسته‌های حمله موجود در مجموعه داده، یا به‌عنوان عادی اگر آن مثبت کاذب باشد، برچسب‌گذاری شوند. برای ترافیک عادی، از طریق طبقه‌بندی انجام می‌شود، به‌طوری‌که اگر یک ناهنجاری به‌عنوان یک منفی نادرست شناسایی شود، به‌عنوان یک حمله به‌درستی با برچسب دسته درست برچسب‌گذاری می‌شود. مدل پیشنهادی به‌عنوان یک سیستم چند عامل در [8] اجرا شد.

4. آزمایش‌ها

این آزمایش با استفاده از مجموعه داده‌های ارزیابی NSL-KDD [21] IDS انجام شد. در تحقیقات پیشین، مجموعه داده KDD Cup 99 [15] بیشترین داده‌های معیار کاربردی برای ارزیابی عملکرد دستگاه‌های تشخیص نفوذ مبتنی بر شبکه بود. مشخص شد که مشکلاتی وجود دارد که الگوریتم یادگیری را منحرف می‌کند و نتایج به دلیل کپی کردن سوابق خود در هر دو مجموعه داده‌های آموزشی و آزمایشی نادرست است. مجموعه داده KDD Cup نیز برای ارزیابی بسیار وسیع است، بنابراین معمولاً بخش‌های کوچکی از داده‌ها برای ارزیابی مورداستفاده قرار می‌گیرند که منجر به نتایج نادرست نیز می‌شود؛ بنابراین، گروه محققین پرونده‌های اضافی را حذف کرده و مجموعه داده‌ها را به‌صورت متناسب برای به کسب تعادل انتخاب کردند و این امر به مجموعه داده NSL-KDD منجر شد. این تحقیق توسط بسیاری از محققین مورداستفاده قرارگرفته است، زیرا تعداد رکوردها برای داده‌های آموزشی و آزمون بسیار کمتر است، بنابراین کل مجموعه‌ها می‌توانند در آزمایش‌ها مورداستفاده قرار گیرند. چهار نوع عمومی حملات در مجموعه داده وجود دارد: رد خدمات (DoS)، کاوشگر، کاربر به ریشه (U2R) و دور به نزدیک (R2L). جدول 1 توزیع سوابق عادی و حملات در مجموعه داده NSL-KDD را نشان می‌دهد.

بعضی از مراحل برای آماده‌سازی فرآیند نیاز به تعدیل تنظیمات خود در عامل اصلی برای کسب بهترین نتایج در عوامل آشکارساز دارد. این مقادیر بهترین نتایج را با ویژگی‌های انتخاب‌شده توسط SFFS در آزمایش قبلی نشان داده‌شده در [5] ارائه داد. در آزمایش، 26 ویژگی توسط SFFS انتخاب شد. برای طبقه‌بندی کننده‌ها، داده‌های

Train_20% برای آموزش استفاده شد، زیرا طبقه‌بندی کننده‌ها نشان داد که نتایج بسیار خوبی بدون نیاز به استفاده از تمام سوابق اطلاعات آموزشی به دست می‌دهد، همان‌طور که در [6،7] ثابت‌شده است. طبقه‌بندی کننده‌های اعمال‌شده در این آزمایش‌ها از طریق ابزارهای Weka استفاده شد [24].

5. نتایج و بحث

دو مجموعه نتیجه از مرحله اول داریم، یکی مجموعه‌ای است که توسط آشکارسازهای تولیدشده با استفاده از اندازه‌گیری فاصله‌ای اقلیدسی و مجموعه‌ای دیگر توسط آشکارسازهای تولیدشده با استفاده از اندازه‌گیری فاصله Minkowski - هم برای مجموعه آموزشی و مجموعه آزمایش به دست می‌آید. فقط نتایج مجموعه آزمایش از طریق طبقه‌بندی کننده‌ها اجرا می‌شود.

برای نتایج اقلیدس، 12889 ناهنجاری شناسایی شد و طبقات واقعی آن‌ها عبارت‌اند از: 1567 اتصالات طبیعی، 6894 اتصالات حمله DoS، 2295 ارتباطات حمله کاوشگر، 159 ارتباطات حمله اتصال U2R و 1974 اتصالات حمله R2L. از سوی دیگر، 9655 مورد طبیعی شناخته شدند و طبقات واقعی آن‌ها عبارت‌اند از: 8144 اتصالات طبیعی، 564 اتصالات حمله DoS، 126 اتصال حمله کاوشگر، 41 اتصال حملهU2R و 780 اتصال حملهR2L . برای نتایج Minkowski، 13239 ناهنجاری شناسایی‌شده و طبقات واقعی آن‌ها عبارت‌اند از: 1718 اتصالات طبیعی، 6939 اتصالات حمله DoS، 2303 ارتباطات حمله کاوشگر، 159 اتصال حمله U2R و 2120 اتصالات حمله R2L. از سوی دیگر، 9305 مورد طبیعی تشخیص داده شد و طبقات واقعی آن‌ها عبارت‌اند از: 7993 اتصالات طبیعی، 519 اتصال حمله DoS، 118 اتصال حمله کاوشگر، 41 اتصال حملهU2R و 634 اتصال حمله R2L.

ازآنجاکه ردیاب‌های Minkowski میزان تشخیص بهتری را ارائه کردند، آزمایش با استفاده از این نتایج تشخیصی ادامه یافت. معیارهای ارزیابی مورداستفاده برای ارزیابی بهتر IDS عبارت‌اند از دقت، فراخوانی و نمره F. دقت بالاتر بدان معنی است که سیستم تنها قادر به تشخیص حملات بود، فراخوانی بیشتر نشان می‌دهد که سیستم قادر به شناسایی تمام حملات بوده و نمره F بالاتر نشان‌دهنده صحت بیشتر تشخیص حملات، بر اساس دقت و مقادیر فراخوانی است. آن‌ها به‌صورت زیر محاسبه می‌شوند.

$$\text{دقت} = \frac{TP}{TP + FP} \quad (1)$$

$$\text{فراخوانی} = \frac{TP}{TP + FN} \quad (2)$$

$$F = 2 * \frac{\text{دقت} * \text{فراخوانی}}{\text{دقت} + \text{فراخوانی}} \quad (3)$$

TP (مثبت واقعی) تعداد حملات درست شناسایی‌شده/ دسته‌بندی‌شده است، FP (مثبت کاذب) تعداد اتصالات عادی است که به‌اشتباه به‌عنوان حملات برچسب‌گذاری شده‌اند و FN(منفی کاذب) تعداد اتصالات نامناسب است که به‌اشتباه به‌عنوان عادی نام‌گذاری شده‌اند.

5.1. نتایج طبقه‌بندی کننده‌ها

طبقه‌بندی کننده‌ها یک‌بار با استفاده از تنها 20 درصد مجموعه آموزشی و بار دیگر با استفاده از تمام مجموعه آموزشی آموزش‌دیده بودند. جدول 2 مقادیر دقت و فراخوانی برای هر طبقه‌بندی کننده را روی ترافیک ناهنجار حاصل از آشکارسازهای Minkowski نشان می‌دهد.

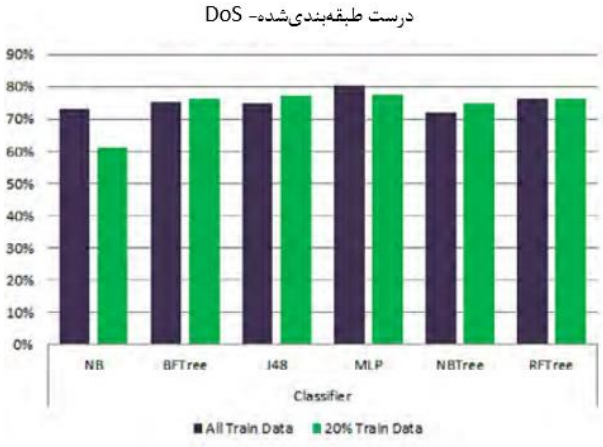
می‌توانیم درک کنیم که مقادیر دقت زیاد هستند که نشان‌دهنده این است که بیشتر حملات شناسایی‌شده، درواقع اتصالات غیرمعمول هستند، درحالی‌که به علت تعداد زیاد حملات شناسایی‌شده به‌عنوان اتصالات معمول، مقادیر یادآوری آن‌چنان زیاد نیستند. شکل 2 اطلاعات مربوط به نتایج طبقه‌بندی ترافیک ناهنجار را برای آشکارسازهای Minkowski برای هر دسته حمله نشان می‌دهد.

همان‌طور که نتایج نشان می‌دهد، DoS با MLP بهتر دسته‌بندی‌شده است. حملات کاوشگر به ترتیب با BFTree با تمام اطلاعات آموزشی و NB با 20٪ از اطلاعات آموزشی بهتر طبقه‌بندی می‌شوند. NB بهترین طبقه‌بندی کننده برای حملات R2L است و برای حملات U2R با استفاده از تمام اطلاعات آموزشی همراه با J48 با استفاده از 20٪ اطلاعات آموزشی است. شکل 3 نتایج طبقه‌بندی ترافیک عادی را نشان می‌دهد که ترافیک طبیعی طبق طبقه‌بندی برای پیدا کردن منفی‌های کاذب و نام‌گذاری آن‌ها با دسته حمله درست آن‌ها طبقه‌بندی می‌شود.

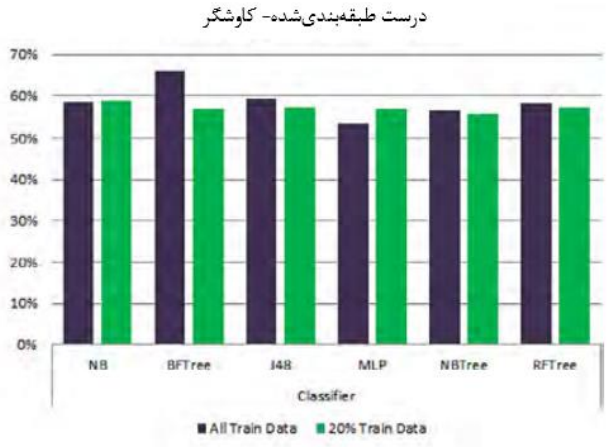
جدول ۲

مقادیر دقت و فراخوانی به‌دست‌آمده از طبقه‌بندی ترافیک ناهنجار معین‌شده توسط ردیاب‌های Minkowski.

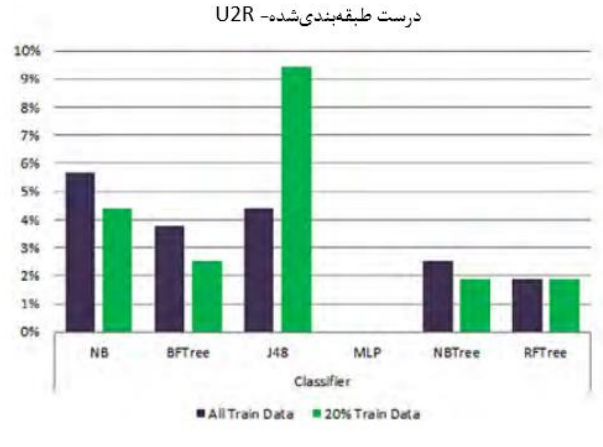
طبقه بندی کننده	TP	FP	FN	دقت	یادآوری	نمره F
Using all of the train data records						
NB	7027	1264	2534	84.75%	73.50%	78.73%
BFTree	6744	121	4454	98.24%	60.23%	74.67%
J48	6580	156	4493	97.68%	59.42%	73.90%
MLP	6842	102	4322	98.53%	61.29%	75.57%
NBTree	6627	105	4309	98.44%	60.60%	75.02%
RFT	6690	113	4663	98.34%	58.93%	73.69%
Using 20% of the train data records						
NB	6271	1297	2677	82.86%	70.08%	75.94%
BFTree	6874	136	3954	98.06%	63.48%	77.07%
J48	6822	105	4351	98.48%	61.06%	75.38%
MLP	6691	123	4260	98.19%	61.10%	75.33%
NBTree	6506	114	4392	98.28%	59.70%	74.28%
RFT	6608	100	4730	98.51%	58.28%	73.24%



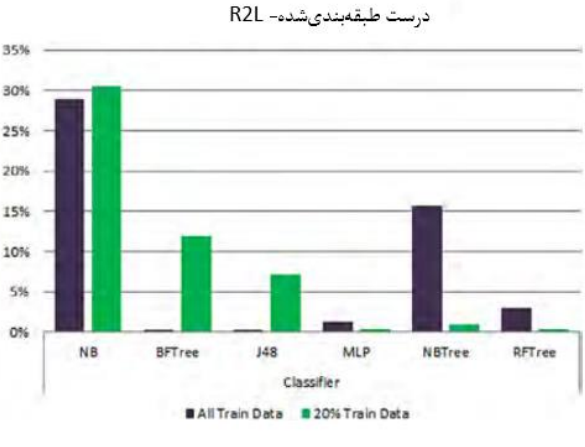
(الف) دسته‌بندی حمله DoS



(ب) دسته‌بندی حمله کاوشگر



(ج) دسته‌بندی حمله U2R



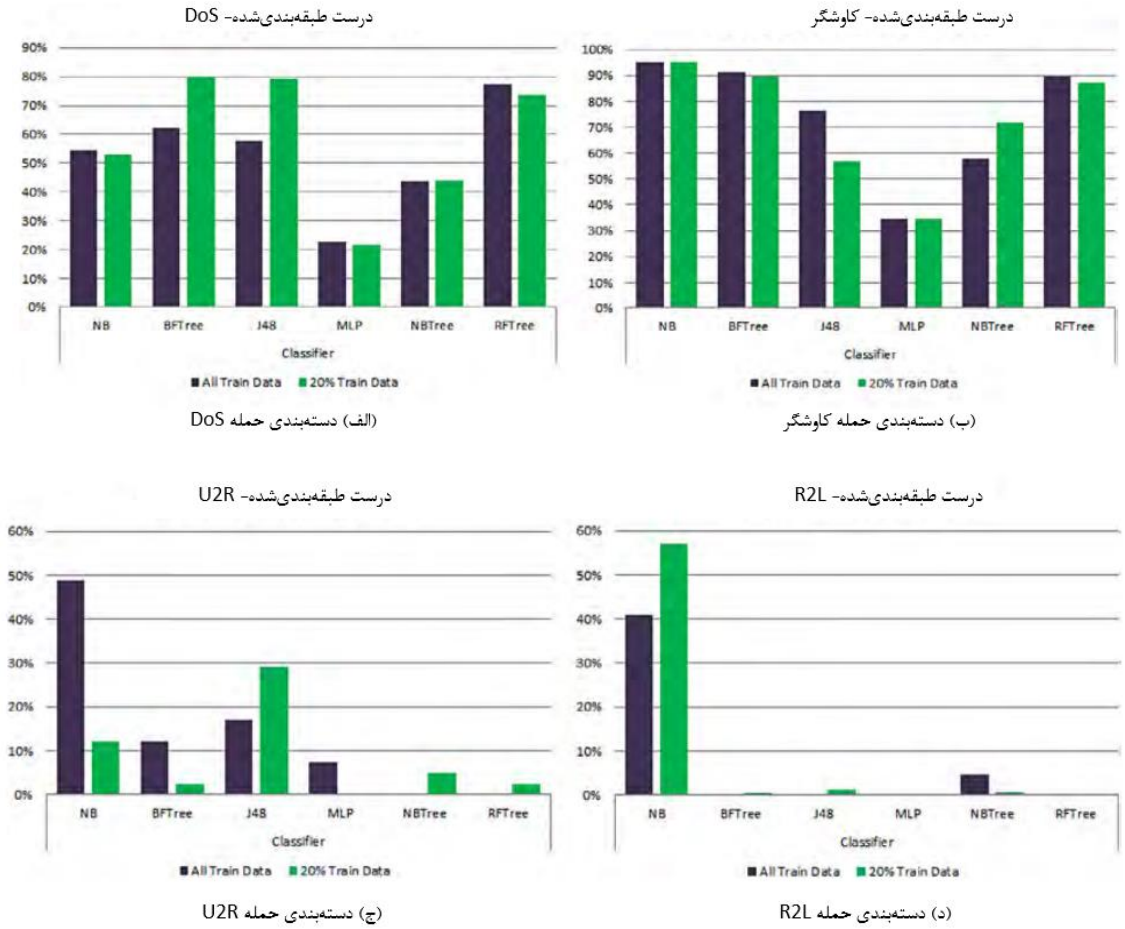
(د) دسته‌بندی حمله R2L

شکل ۲ طبقه‌بندی نتایج در ترافیک غیرعادی

می‌توانیم از طریق نتایج متوجه شویم که برای حملات غیرقانونی که به‌طور عادی شناخته‌شده‌اند، آن‌ها به شرح زیر طبقه‌بندی می‌شوند: DOS ها با استفاده از تمام داده‌های آموزشی با RFTree طبقه‌بندی می‌شوند و J48 و

BFTree با استفاده از 20 درصد اطلاعات آموزشی، با توجه به این‌که توسط BFtree و RFTree، حملات U2R به ترتیب با استفاده از تمام داده‌های آموزشی و J48 با استفاده از 20٪ اطلاعات آموزشی طبقه‌بندی می‌شوند و حملات R2L به‌طور کامل توسط NB طبقه‌بندی می‌شوند.

اضافه کردن حملات به‌طور صحیح از ترافیک شناسایی عادی به TP اصلی شناسایی‌شده در ترافیک غیرعادی طبقه‌بندی‌شده (FN تبدیل به TP)، مقادیر دقت و فراخوانی به شرح زیر است –جدول 3. طبقه‌بندی کننده‌های NBtree و BFTree دارای بالاترین مقادیر دقت هستند، درحالی‌که طبقه‌بندی کننده‌های NB و BFTree دارای بالاترین مقدار یادآوری هستند که بدان معنی است که NB و BFTree قادر به شناسایی حملات بیشتر هستند، اما NBTree و BFTree تعداد مثبت کاذب کمتری دارند و بیشتر آنچه آن‌ها شناسایی کرده‌اند، واقعاً غیرعادی هستند. ازاین‌رو می‌بینیم که بالاترین مقدار F-Score متعلق به طبقه‌بندی کننده NB و سپس طبقه‌بندی کننده BFTree است. این به دلیل توانایی طبقه‌بندی کننده NB برای شناسایی حملات R2L و U2R است که تقریباً توسط طبقه‌بندی‌های دیگر، در هر دو ترافیک غیرطبیعی و معمولی، شناسایی نشده است.



(الف) دسته‌بندی حمله DoS

(ب) دسته‌بندی حمله کاوشگر

(ج) دسته‌بندی حمله U2R

(د) دسته‌بندی حمله R2L

شکل ۳ طبقه‌بندی نتایج در ترافیکی عادی

جدول 3 مقادیر دقت و فراخوانی به‌دست‌آمده از طبقه‌بندی ترافیک غیرطبیعی و نرمال که توسط ردیاب‌های Minkowski شناسایی‌شده‌اند.

Classifier	TP	FP	FN	Precision	Recall	F-Score
Using all of the train data records						
NB	7702	1264	1859	85.90%	80.56%	83.14%
BFTree	7180	121	4018	98.34%	64.12%	77.63%
J48	6976	156	4097	97.81%	63.00%	76.64%
MLP	7004	102	4160	98.56%	62.74%	76.67%
NBTree	6950	105	3986	98.51%	63.55%	77.26%
RFT	7199	113	4154	98.45%	63.41%	77.14%
Using 20% of the train data records						
NB	7025	1297	1923	84.41%	78.51%	81.35%
BFTree	7398	136	3430	98.19%	68.32%	80.58%
J48	7320	105	3853	98.59%	65.52%	78.72%
MLP	6846	123	4105	98.24%	62.51%	76.41%
NBTree	6826	114	4072	98.36%	62.64%	76.53%
RFT	7095	100	4243	98.61%	62.58%	76.57%

طبقه‌بندی کننده NB همچنین قادر به برچسب‌گذاری بیشتر حملات کاوشگر بود که به‌طور غلط به‌عنوان معمولی نسبت به سایر طبقه‌بندی کننده‌ها برچسب‌گذاری می‌شد. بر اساس میزان کاربرد داده‌ها برای آموزش، طبقه‌بندی کننده‌های NB و NBTree نتایج بهتری ارائه دادند، زمانی که تمام مجموعه داده‌های آموزشی مورداستفاده قرار گرفت، درحالی‌که BFTree و J48 هنگامی‌که تنها 20٪ از داده‌های آموزشی مورداستفاده قرار گرفت، نتایج بهتری ارائه دادند. نتایج RFTree و MLP در هر دو مورد نتایج نزدیک به هم داشتند.

داده‌های عادی توسط همه طبقه‌بندی کننده‌ها به‌جز طبقه‌بندی کننده NB شناسایی و دسته‌بندی شدند (تقریباً تمام ترافیک عادی). برای ارتباطات غیرمعمول، برخی از آن‌ها شناسایی شدند و برخی نیز بسته به ارائه آن‌ها در مجموعه داده و وابستگی بین ویژگی‌ها شناسایی نشدند.

شکل ۴. نتایج طبقه‌بندی کلی – ردیاب‌های Minkowski

6. نتیجه‌گیری

در این مقاله، یک سیستم تشخیص نفوذ ترکیبی و سلسله مراتبی ارائه‌شده که مبتنی بر مفاهیم ایمنی است. طبقه‌بندی کننده‌های مختلف برای یافتن بهترین طبقه‌بندی کننده برای کسب اطلاعات بیشتر در مورد حملات شناخته‌شده و پیش‌بینی دسته حملات ناشناخته مورد آزمایش و مقایسه قرار گرفتند. می‌توانیم درک کنیم که به‌طورکلی، درخت‌های تصمیم‌گیری بهترین نتایج را ارائه می‌دهند، اما با توجه به هر دسته، طبقه‌بندی کننده‌ها نتایج مختلفی بر اساس ارائه این دسته‌ها در مجموعه داده‌ها و وابستگی بین ویژگی‌ها دارند. طبقه‌بندی کننده NB دارای بهترین نتایج در مورد حملات کم ارائه‌شده مانند R2L و U2R است. FT نتایج بسیار خوبی داشت، اما مدت‌زمان زیادی برای آموزش ساخت درختان تصادفی برای تصمیم‌گیری طبقه‌بندی نیاز داشت. NBTree و BFTree امتیازات بالاتری نسبت به J48 و RFTree داشتند؛ کاربرد آن‌ها بهتر است، زیرا زمان کمتری برای آموزش را نیاز دارند و در موارد ارائه بالای طبقات، تنها 20 درصد مجموعه آموزشی برای ارائه نتایج بسیار خوب کافی است.MLP بهترین نمرات را در طبقه‌بندی uhnd و DoS برای ارائه بالای آن‌ها در مجموعه آموزشی به دست آورد، اما در موارد حملات U2R و R2L نمی‌توانند آن‌ها را طبقه‌بندی کنند - در بیشتر موارد صفر درصد به‌درستی طبقه‌بندی شدند.

می‌توانیم نتیجه‌گیری کنیم که نیازی به استفاده از طبقه‌بندی کننده‌های پیچیده برای کسب نمرات طبقه‌بندی بالا نیست- NB نرخ‌های تشخیص بالا در موارد دسته‌های حمله کم ارائه‌شده به دست می‌دهد. همچنین، یک طبقه‌بندی کننده تنها برای استفاده و برچسب‌گذاری و پیش‌بینی دسته‌های حملات کافی نیست، طبقه‌بندی کننده‌های چندگانه باید مورداستفاده قرار گیرند تا دقت طبقه‌بندی را افزایش دهند. اگر 20 درصد از اطلاعات آموزشی برای ارائه نمرات بالا کافی است- حتی اگر کمی کمتر از مورد کاربرد تمام اطلاعات آموزشی- سپس زمان کمتر برای آموزش در این مورد بهتر است. همان مجموعه ویژگی‌ها از طریق کل فرایند استفاده‌شده و نتایج رضایت‌بخش را به دست آورده است، بنابراین نیازی به یک مجموعه ویژگی خاص برای هر دسته حمله نیست. شاید برای طبقه‌بندی نوع حمله خاص تحت برچسب بزرگ دسته حمله موردنیاز باشد که جزو کار آینده برای بالا بردن نتایج سیستم خواهد بود. همان‌طور که در شکل 4 نشان داده‌شده است، طبقه‌بندی ترافیک شناسایی‌شده

به‌طور عادی نتایج کلی طبقه‌بندی را افزایش داده است. این مورد می‌تواند برای تحقیقات آینده در نظر گرفته شود تا حملات رفتاری را به‌طور خاص در ترافیک شناسایی‌شده به‌صورت عادی شناسایی کند.

References

[1] U. Aickelin, J. Greensmith, J. Twycross, Immune system approaches to intrusion detection – a review, in: Artificial Immune Systems, Springer, Berlin, Heidelberg, 2004, pp. 316–329.

[2] J.R. Anderson, Knowledge compilation: the general learning mechanism, in: R.S. Michalski, R.S. Michalski, T.M. Mitchell (Eds.), Machine Learning: An Artificial Intelligence Approach 2, Morgan Kaufmann, 1986.

[3] A.S.A. Aziz, A.T. Azar, A.E. Hassanien, S.E.O. Hanafi, Continuous features discretizaion for anomaly intrusion detectors generation, in: WSC17 2012 Online Conference on Soft Computing in Industrial Applications, 2012.

[4] A.S.A. Aziz, A.T. Azar, A.E. Hassanien, S.E.O. Hanafy, Genetic algorithm with different feature selection techniques for anomaly detectors generation, in: 2013 Federated Conference on Computer Science and Information Systems, FedCSIS, IEEE, 2013, pp. 769–774.

[5] A.S.A. Aziz, A.T. Azar, A.E. Hassanien, S.E.O. Hanafy, Genetic algorithm with different feature selection techniques for anomaly detectors generation, in: 2013 Federated Conference on Computer Science and Information Systems, FedCSIS, IEEE, 2013, pp. 769–774.

[6] A.S.A. Aziz, A.E. Hassanien, A.T. Azar, S.E.O. Hanafi, Machine learning techniques for anomalies detection and classification, in: Advances in Security of Information and Communication Networks, Springer, Berlin, Heidelberg, 2013, pp. 219–229.

[7] A.S.A. Aziz, A.E. Hassanien, S.E.O. Hanafy, M.F. Tolba, Multi-layer hybrid machine learning techniques for anomalies detection and classification approach, in: 2013 13th International Conference on Hybrid Intelligent Systems, HIS, IEEE, 2013, pp. 216–221.

[8] A.S.A. Aziz, S.E.O. Hanafi, A.E. Hassanien, Multi-agent artificial immune system for network intrusion detection and classification, in: International Joint Conference SOCO'14–CISIS'14–ICEUTE'14, in: Advances in Intelligent Systems and Computing, vol. 299, Springer International Publishing, 2014, pp. 145–154.

[9] R. Caruana, A. Niculescu-mizil, An empirical comparison of supervised learning algorithms, in: Proceedings of the 23rd International Conference on Machine Learning, ACM, 2006, pp. 161–168.

[10] H. Chauhan, V. Kumar, S. Pundir, E.S. Pilli, A comparative study of classification techniques for intrusion detection, in: 2013 International Symposium on Computational and Business Intelligence, ISCBI, IEEE, 2013, pp. 40–43.

[11] D. Dasgupta, S. Yu, F. Nino, Advances in artificial immune systems: models and applications, Appl. Soft Comput. 11 (2) (2011) 1574–1587.

[12] S. Ganapathy, K. Kulothungan, S. Muthurajkumar, M. Vijayalakshmi, P. Yogesh, A. Kannan, Intelligent feature selection and classification techniques for intrusion detection in networks: a survey, EURASIP J. Wirel. Commun. Netw. 2013 (1) (2013) 1–16.

[13] P. Garcia-Teodora, J. Diaz-Verdejo, G. Macia-Fernandez, E. Vazquez, Anomaly-based network intrusion detection: techniques, systems and challenges, Comput. Secur. 28 (1–2) (2009) 18–28.

[14] M.S. Hoque, Md. Mukit, Md. Bikas, A. Naser, An implementation of intrusion detection system using genetic algorithm, In arXiv preprint arXiv:1204.1336, 2012.

[15] KDD Cup'99 intrusion detection data set, Available on: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html, October 2007.

[16] G. Kim, S. Lee, S. Kim, A novel hybrid intrusion detection method integrating anomaly detection with misuse detection, Expert Syst. Appl. 41 (4) (2014) 1690–1700.

[17] H.J. Liao, K.Y. Tung, C.H. Richard Lin, C.Y. Lin, Intrusion detection system: a comprehensive review, J. Netw. Comput. Appl. 36 (2012) 16–24.

[18] S. Misra, S.C. Misra, I. Woungang, Selected Topics in Communication Networks and Distributed Systems, World Scientific, 2010.
[19] Z. Muda, W. Yassin, M.N. Sulaiman, N.I. Udzir, Intrusion detection based on K-means clustering and Naïve Bayes classification, in: 2011 7th International Conference on Information Technology in Asia, CITA 11, IEEE, 2011, pp. 1–6.
[20] L. Noriega, Multilayer Perceptron Tutorial, School of Computing, Staffordshire University, 2005.
[21] NSL-KDD intrusion detection data set, Available on: http://iscx.ca/NSL-KDD/, March 2009.
[22] S.K. Sharma, P. Pandey, S.K. Tiwari, M.S. Sisodia, An improved network intrusion detection technique based on k-means clustering via Naïve Bayes classification, in: 2012 International Conference on Advances in Engineering, Science and Management, ICAESM, IEEE, 2012, pp. 417–422.
[23] C. So-In, N. Mongkonchai, P. Aimtongkham, N. Wijitsopon, K. Rujirakul, An evaluation of data mining classification models for network intrusion detection, in: 2014 Fourth International Conference on Digital Information and Communication Technology and Its Applications, DICTAP, IEEE, 2014, pp. 90–94.
[24] Weka 3: data mining software in Java, Available on http://www.cs.waikato.ac.nz/~ml/weka/.