Scientific Journal of Electronical & Cyber Defence
Vol. 10, No. 3, Autumn 2022, Serial No. 39

Investigation of a new ensemble method of intrusion detection system on different data sets

M. H. Nataj Solhdar*

* Instructor, Shohdai Huizeh Industrial Campus, Shahid Chamran University, Ahvaz, Iran

(Received: 11/10/2021, Accepted: 18/12/2021)

ABSTRACT

Intrusion detection is a classification problem in which various machine learning (ML) and data mining (DM) techniques are used to classify network data in normal traffic and attack. In addition, the types of network attacks have changed over the years. This paper tries to compare two models of intrusion detection systems, which include adaptive neuro-fuzzy inference systems (ANFIS) and support vector machines (SVM). In addition, it examines and evaluates several instances of data sets related to intrusion detection systems. In the following, a new hybrid method is proposed that uses Particle Swarm Optimization (PSO) to create a classifier combination to provide better accuracy for intrusion detection. Experimental results show that the new method can produce a better performance based on different evaluation criteria. This paper lists the different datasets for evaluating the IDS model and discusses the performance of the proposed hybrid method on the IDS datasets that can be used to efficiently and effectively use the datasets to develop IDS based on ML and DM .

Keywords: Intrusion detection system, adaptive neuro-fuzzy inference system, support vector machines, classifier.

* Corresponding Author Email: N.solhdar@scu.ac.ir

نشریه علمی "پدافند الکترونیکی و سایبری"
سال دهم، شماره ۳، پاییز ۱۴۰۱، ص ۵۷- ۴۳

علمی – پژوهشی

بررسی یک روش ترکیبی جدید سیستم تشخیص نفوذ بر روی مجموعه داده‌های مختلف

محمدحسن نتاج صلحدار[1]

۱- مربی، پردیس صنعتی شهدای هویزه، دانشگاه شهید چمران، اهواز، ایران

(دریافت: ۱۴۰۰/۰۷/۱۹، پذیرش: ۱۴۰۰/۰۹/۲۷)

چکیده

تشخیص نفوذ یک مسئله طبقه‌بندی است که در آن روش‌های مختلف یادگیری ماشین (ML) و داده‌کاوی (DM) برای طبقه‌بندی داده‌های شبکه در ترافیک عادی و حمله استفاده می‌شود. علاوه بر این، انواع حملات شبکه در طول سال‌ها تغییر کرد. در این مقاله سعی شد دو مدل از سیستم‌های تشخیص نفوذ، با هم مقایسه شود، که این مدل‌ها شامل شبکه استنتاج عصبی-فازی سازگار (ANFIS) و ماشین‌های بردار پشتیبان (SVM) می‌باشند. علاوه بر این، چندین نمونه از مجموعه داده‌های مربوط به سیستم‌های تشخیص نفوذ را موردبررسی و ارزیابی قرار می‌دهد. در ادامه، یک روش ترکیبی جدید را بیان می‌کند که از بهینه‌سازی ازدحام ذرات (PSO) به‌منظور ایجاد ترکیب دسته‌بندها برای ایجاد دقت بهتر برای تشخیص نفوذ، استفاده کرده است. نتایج آزمایش نشان می‌دهد که روش جدید می‌تواند کارایی بهتری بر اساس معیارهای مختلف ارزیابی، ارائه کند. این مقاله مجموعه داده‌های مختلف را برای ارزیابی مدل IDS فهرست می‌کند و کارایی روش ترکیبی پیشنهادی بر مجموعه داده‌های IDS را موردبحث قرار می‌دهد که می‌تواند برای استفاده از مجموعه داده‌ها برای توسعه IDS مبتنی بر ML و DM کارآمد و مؤثر بوده و مورداستفاده قرار گیرد.

کلیدواژه‌ها: سیستم تشخیص نفوذ، شبکه عصبی- فازی، ماشین‌های بردار پشتیبان، دسته‌بندی کننده

۱- مقدمه

در دنیای سریع روبه‌رشد امروز، رویکردهای یادگیری ماشین در تعداد زیادی از برنامه‌ها استفاده می‌شود که در آن‌ها برای کشف الگوهای آگاهانه، جالب و مفید از حجم عظیمی از داده‌ها بر اساس نیاز کاربر با کمک تجزیه‌وتحلیل داده‌ها استفاده می‌شود. تشخیص نفوذ از چند دهه پیش به چالش‌برانگیزترین حوزه در زمینه شبکه تبدیل شده است. ایجاد و توسعه سیستم تشخیص نفوذ (IDS) به مقدار زیادی داده نیاز دارد. این حجم زیادی از داده‌ها را که در برابر حملات اقدام می‌کند تجزیه‌وتحلیل می‌کند. نظارت بر فعالیت‌های شبکه و تشخیص حملات و همچنین امنیت سیستم شبکه، اهداف هر نوع IDS است. IDS بر اساس تجزیه‌وتحلیل داده‌ها، روش‌ها یا مدل‌ها و محل قرارگیری آن‌ها به دودسته طبقه‌بندی می‌شود [۱].

روش‌های داده‌کاوی و یادگیری ماشینی، قابلیت یافتن الگوهای ناشناخته جدید، تشخیص نفوذ، کشف الگوهای ناشناخته قبلی رادارند و همچنین سیستم پشتیبانی تصمیم‌گیری برای IDS را به‌خوبی فراهم می‌کنند. به همین دلایل روش‌های داده‌کاوی و یادگیری ماشین در زمینه IDS بسیار مهم هستند [۲]. روش طبقه‌بندی همچنین به دو نوع، فردی و ترکیبی طبقه‌بندی می‌شود. روش طبقه‌بندی فردی، سریع است، همچنین حافظه کمتری برای محاسبه نیاز دارد اما با افزایش الگوهای ناشناخته یا نمونه‌های ناشناخته عملکرد آن کاهش می‌یابد. برعکس، یک روش ترکیبی به زمان و حافظه بیشتری نیاز دارد اما در صورت وجود الگوها یا حملات ناشناخته به‌خوبی عمل می‌کند. برچسب‌گذاری دستی برای هر نمونه نیاز به زمان و هزینه بیشتری در حضور حجم عظیمی از داده‌های ایجادشده از طریق شبکه دارد.

در دهه‌های اخیر، سیستم تشخیص نفوذ مبتنی بر ناهنجاری و تعداد زیادی از مسائل دیگر دسته‌بندی از ایده دسته‌بند ترکیبی، بهره‌مند شده است [۳]. داده‌های جمع‌آوری‌شده به ترتیب به یک مجموعه آموزشی و مجموعه آزمایشی برای آموزش و آزمایش طبقه‌بندی‌کننده تقسیم می‌شوند؛ بنابراین، روش‌های مختلف ML[1] و DM[2] برای توسعه IDS استفاده می‌شود [۴]. مجموعه داده‌های IDS شامل برچسب‌هایی است که از مشاهده الگوهای داده‌های ترافیک شبکه به دست آمده است [۵]. تعداد زیادی از پژوهشگران برای پیدا کردن مجموعه داده‌های جامع و

* رایانامه نویسنده مسئول: N.solhdar@scu.ac.ir

[1] Machine Learning
[2] Data Mining

معتبر جهت آزمون و ارزیابی روش‌های پیشنهادی خودشان چالش‌هایی را در سر راه خود دارند [۶]؛ بنابراین بر اساس فقدان برخی مشخصات آماری مشخص و در دسترس نبودن این مجموعه داده‌ها، هنوز مجموعه داده کاملی به دست نیامده است [۷]. همراه با مجموعه داده، استفاده از روش مناسب برای طبقه‌بندی حملات نیز مهم است. روش‌های متنوعی وجود دارد که با موفقیت برای IDS استفاده‌شده است [۸ و ۹]. بااین‌حال، هر یک از الگوریتم‌های مورداستفاده برای IDS مجموعه داده را به شیوه‌ای متفاوت آموزش و آزمایش می‌کند.

دسته‌بندهای مبتنی بر ترکیب به‌خوبی موردمطالعه قرارگرفته است و برای بهبود دقت وظایف طبقه‌بندی چندگانه استفاده‌شده است. چندین روش ترکیبی شامل میانگین ترکیب‌گر[1]، میانه ترکیب‌گر[2]، ماکزیمم ترکیب‌گر[3]، رأی‌گیری اکثریت[4] و رأی‌گیری اکثریت وزنی (WMV)[5] بیان شده است. در حالی دسته‌بندهای فردی می‌توانند با استفاده هر یک از این روش‌ها ترکیب شوند. WMVها تاکنون به علت سادگی مفهومی، شهودی و اثربخشی آن در عمل به‌عنوان پرطرفدارترین روش در میان روش‌های دیگر به‌حساب می‌آیند [۱۰]. در تحقیق‌های اولیه، نشان داده شده است که روش ترکیبی دارای کارایی بیشتری نسبت به هریک از دسته‌بندهای فردی است. موفقیت یک طبقه‌بند ترکیبی به‌طور قوی بستگی به تنوع در خروجی دسته‌بندهای فردی آن، و همچنین به انتخاب روش برای ترکیب این خروجی‌ها در یک طبقه‌بند فردی دارد [۱۱]. به دلیل آن‌که انتخاب روش ترکیبی مناسب هنوز مشخص نشده است، یک روش ابتکاری برای ترکیب دسته‌بندها، بیان شده است. بهینه‌سازی ازدحام ذرات (PSO) یکی از این روش‌ها است [۱۲]. در این مقاله، دسته‌بندهای فردی، از شبکه عصبی-فازی (ANFIS) و ماشین بردار پشتیبان (SVM) روی مجموعه داده یکسان، در نظر گرفته شده‌اند. کارایی سیستم توسعه‌یافته را می‌توان بر اساس عواملی مانند بهینه‌سازی شاخص‌ها[6]، بهینه‌سازی ویژگی‌ها و تنوع در اندازه مجموعه داده آزمایش و مقایسه کرد. جدا از عملکرد مجموعه داده‌های موجود و روش‌های مورداستفاده برای IDS، انتخاب معیار عملکرد مناسب نیز یکی از عوامل مهمی است که باید موردتوجه قرار گیرد. یکی از متداول‌ترین معیارهای مورداستفاده برای نشان دادن اثربخشی سیستم، «حساسیت» است [۱۳]. در ادامه، کارهای انجام‌شده توسط محققان دیگر در بخش ۲ آماده است، در بخش ۳ پیش‌نیازهای تحقیق آورده شده است که در مورد روش‌های دسته‌بندی و ترکیب توضیحات مختصری داده شد و همچنین در ادامه این بخش به معرفی مجموعه داده پرداخته شده است. در بخش ۴ روش تحقیق آورده شده است که در این بخش الگوریتم پیاده‌سازی و نقاط ضعف و قوت مجموعه داده‌ها توضیح داده شده است و علاوه بر این، روش ارزیابی و نتایج پیاده‌سازی و مقایسه‌ها نیز در همین بخش آورده شده است. در بخش ۵ نیز نتیجه‌گیری کلی از این تحقیق بیان شده است.

۲- کارهای انجام‌شده

اخیراً موج گسترده‌ای از تحقیقات در مورداستفاده از روش‌های ترکیبی برای طراحی سیستم‌های تشخیص نفوذ، ایجاد شده است. در مقاله [۱۴]، ایده استفاده از آشکارسازهای ترکیبی مطرح‌شده است. راهکاری نوین مبتنی بر روش آشکارسازی ترکیبی با یک معماری چهار لایه‌ای پیشنهاد شده است. لایه اول از واحد تحلیلگر جریان داده‌ها و واحد طبقه‌بندی تشکیل شده است که برای طبقه‌بندی نوع سرویس‌های شبکه از ترکیب روش آماری n-گرام و الگوریتم ژنتیک استفاده می‌کند. در لایه تشخیص نفوذ، یک واحد آشکارساز مبتنی بر امضاء و واحدهای آشکارساز مبتنی بر ناهنجاری به شکل ترکیبی پیاده‌سازی شده‌اند که متناسب با برچسب نوع سرویس‌ها فراخوانی می‌شوند. این مقاله مدل طراحی خود را تنها روی مجموعه داده‌های NSL-KDD موردبررسی و آزمایش قرار داده است. عبدالله و همکاران [۱۵] یک IDS با استفاده از ویژگی‌های مبتنی بر IG[7] و الگوریتم‌های یادگیری گروهی ایجاد کردند. آزمایش بر روی مجموعه داده NSL-KDD نشان می‌دهد که بالاترین دقت هنگام استفاده از RF[8] و PART[9] به‌عنوان طبقه‌بندی کننده اصلی تحت قانون احتمال محصول[10] به دست می‌آید. در مطالعه [۱۶]، از مجموعه داده‌های IDS-2018 CSE-CIC، UNSW-NB15، ISCX-2012، NSL-KDD و CIDDS-001 استفاده شد. علاوه بر این، عادی‌سازی حداکثر حداقل (Min-Max normalization) بر روی این مجموعه داده‌ها انجام شد و با الگوریتم‌های ماشین بردار پشتیبان (SVM)، K-نزدیک‌ترین همسایه (KNN)، درخت تصمیم (DT) که از رویکردهای یادگیری ماشین کلاسیک هستند، طبقه‌بندی انجام شد. از نظر عملکرد طبقه‌بندی کننده‌ها، مشاهده شده است که طبقه‌بندی کننده درخت تصمیم نسبت به سایر طبقه‌بندی کننده‌های مورداستفاده موفق‌تر بوده است. هرچند مدل طراحی‌شده دارای دقت خوبی است ولی در شناسایی حملات جدید به‌خوبی عمل نمی‌کند. وانگ و

[1] Mean Combiner
[2] Median Combiner
[3] Max Combiner
[4] Majority Voting
[5] Weighed Majority Voting (Wmv)
[6] Parameter

[7] Information Gain
[8] Random-Forest
[9] Partial Decision List
[10] Product Probability Rule

همکارانش [۱۷] از k نزدیک‌ترین همسایه[1] (K-NN) که روشی مؤثر و ساده برای طبقه‌بندی اشیا بر اساس نزدیک‌ترین نمونه‌های آموزش در فضا است، استفاده کردند. دسته‌بندهای K-NN می‌تواند برای حل مسائل چند کلاسی مورداستفاده قرار گیرد. شاخص k در دسته‌بند K-NN، تعداد همسایه‌ها را در مجموعه مشاهدات آموزش که در اعتبارسنجی یا در مجموعه داده آزمایش، نزدیک‌ترین مقادیر به مشاهدات داده‌شده هستند، نمایش می‌دهد. اختلاف و تفاوت این شاخص‌ها بر دقت هر یک از دسته‌بندهای باینری درون یک خبره تأثیر خواهد گذاشت و پیدا کردن این شاخص یکی از مسائل و مشکلات این نوع مدل‌ها هست. علاوه بر این، سالو و همکاران [۱۸] یک IDS ترکیبی ارائه کردند که از روش‌های انتخاب ویژگی IG و تجزیه‌وتحلیل اجزای اصلی[2] (PCA) استفاده کرده است و همچنین طبقه‌بندی کننده مبتنی بر ماشین بردار پشتیبانی (SVM)، الگوریتم‌های یادگیری مبتنی بر نمونه[3] (IBL) و پرسپترون چندلایه[4] (MLP) را باهم ترکیب می‌کنند. تجزیه‌وتحلیل مقایسه‌ای انجام‌شده بر روی چندین مجموعه داده IDS ثابت کرده است که روش IG-PCA-Ensemble عملکرد بهتری نسبت به اکثر روش‌های موجود دارد. کارایی مدل پیشنهادی تنها بر روی سه مجموعه داده یعنی ISCX 2012، NSL-KDD و Kyoto مورد ارزیابی قرار گرفت. با توجه به داده‌های مقیاس بزرگ تولیدشده از زیرساخت شبکه عظیم، خان و همکاران [۱۹] یک IDS ترکیبی را پیشنهاد کردند که بر اساس شبکه Spark ML و Convolutional-LSTM (Conv-LSTM) برای به‌کارگیری تشخیص ناهنجاری[5] و تشخیص سوءاستفاده[6] به‌صورت جداگانه استفاده‌شده است. ژونگ و همکاران [۲۰] همچنین یک مدل تشخیص ناهنجاری جدید به نام HELAD[7]، که بر اساس الگوریتم آمار افزایشی میراث برای انتخاب ویژگی‌ها و ادغام ارگانیک چندین روش یادگیری عمیق برای طبقه‌بندی است، پیشنهادشده است. سیاریف و همکاران [۲۱] روش‌های دسته‌بندی[8]، تقویتی[9] و پشته‌ای[10] را برای مشکل تشخیص نفوذ به‌منظور افزایش دقت و کاهش نرخ مثبت کاذب[11] استفاده کرد. آن‌ها بر اساس دسته‌بندی‌ها برای این روش‌های ترکیبی، از دسته‌بند بیز ساده، J48 (درخت تصمیم[12])، JRip (قانون القا[13]) و iBK (نزدیک‌ترین همسایه[14]) استفاده کردند.

آن‌ها گزارش دادند که این روش‌ها دقتی بیشتر از ٪۹۹ در تشخیص نفوذهای شناخته‌شده دارند، اما می‌توانند نفوذهای جدیدی را فقط با نرخ دقت حدود ٪۶۰ مشخص کنند. استفاده از روش‌های ترکیبی دسته‌بندی، تقویتی و پشته‌ای نرخ دقت قابل‌توجهی را نشان داده است. بااین‌حال، روش پشته‌ای تنها متدی است که منجر به کاهش قابل‌توجه در نرخ مثبت کاذب ٪ 46/84 دارد، هم‌چنین طولانی‌ترین زمان اجرا را دارد و بنابراین برای مسئله تشخیص نفوذ، در عمل ناکارآمد است. در [۳]، یک IDS جدید مبتنی بر انتخاب ویژگی ترکیبی و مجموعه‌های طبقه‌بندی کننده دو سطح پیشنهادشده است و نتایج تجربی نشان می‌دهد که بهبود قابل‌توجهی در میزان تشخیص در مجموعه داده‌های NSL-KDD و UNSW-NB15 ایجاد می‌کند، اما در حملات جدیدی که در این مجموعه داده‌ها وجود ندارد عملکرد ضعیفی دارد.

بسیاری از روش‌های ترکیبی با استفاده از انتخاب ویژگی و همچنین از روش ترکیبی برای بهبود عملکرد IDS ها تولیدشده است. مالک و همکاران [۲۲] روش ترکیبی بهینه‌سازی ازدحام ذرات (PSO) و جنگل تصادفی[15] (RF) را پیشنهاد کرد. ویژگی‌های مناسب‌تر برای هر کلاس به مدل پیشنهادی کمک می‌کند تا در مقایسه با الگوریتم‌های دیگر دقت بالاتری را در کنار نرخ مثبت کاذب[16] پایین تولید کند. فام و همکاران [۲۳] یک مدل ترکیبی ایجاد کرد که از روش نسبت افزایش به‌عنوان انتخاب ویژگی و بسته‌بندی برای ترکیب طبقه‌بندی کننده‌های پایه درخت استفاده می‌کند. نتایج تجربی نشان می‌دهد که بهترین عملکرد توسط مدل کیسه‌ای که از J48 به‌عنوان طبقه‌بندی پایه استفاده می‌کند ولی تنها بر روی زیرمجموعه ۳۵ ویژگی مجموعه داده NSL-KDD کار می‌کند، تولیدشده است. ماروسی و همکاران [۲۴]، برای ایجاد سیستم تشخیص نفوذ با کارایی بهتر علاوه بر انتخاب ویژگی‌های مؤثرتر در طراحی مدل مدنظر از مدل ترکیبی نیز در طراحی خود استفاده کرده‌اند. آن‌ها مدلی بر اساس ترکیب شبکه‌های عصبی مصنوعی به‌منظور تشخیص نفوذ ارائه داده‌اند، علاوه بر این روشی را برای استخراج ویژگی‌های بهینه، بر روی مجموعه داده KDD CUP ۹۹ بیان می‌کنند. بختوریاو و همکاران [۲۵]، به‌منظور تشخیص نفوذ شبکه عصبی، روش احتمالی را برای طراحی دسته‌بندهای شبکه عصبی پایه به نام مولد ساختارهای شبکه عصبی مبتنی بر احتمال به کار گرفتند. آن‌ها برای طراحی ترکیبی شبکه عصبی، از روشی به نام برنامه‌سازی ژنتیک مبنی بر ENsembling یا (GPEN) استفاده کردند. GPEN، عملگرهای برنامه‌سازی ژنتیک

[1] K-Nearest Neighbors
[2] Principal Component Analysis
[3] Instance-Based Learning
[4] Multi-Layer Perceptron
[5] Anomaly Detection
[6] Misuse Detection
[7] Heterogeneous Ensemble Learning Anomaly Detection Model
[8] Bagging
[9] Boosting
[10] Stacking
[11] False Positive Rate
[12] Decision Tree
[13] Rule Induction
[14] Nearest Neighbor
[15] Random Forest
[16] False Positive Rate

را برای یافتن تابع بهینه برای ترکیب دسته‌بندهای پایه در یک دسته‌بند ترکیبی به کار گرفتند. این روش برای مجموعه داده KDD Cup 1999 باهدف دسته‌بندی نفوذهای ورودی به‌عنوان حمله‌های PROBE و غیر PROBE با استفاده از ۹ تا از ۴۱ ویژگی، اعمال‌شده است.

۳- پیش‌نیاز تحقیق

در این قسمت دسته‌بندهایی که استفاده‌شده و روش ترکیب آن‌ها و همچنین ۱۰ مجموعه داده موردبررسی قرارگرفته‌اند. برای توسعه یک سیستم تشخیص کارآمد برای انواع حملات، معمولاً از SVM طبقه‌بندی استفاده می‌شود. شایان‌ذکر است که SVM عملکرد فوق‌العاده‌ای را در میان ابزارهای موجود ارائه می‌دهد. ماشین بردار پشتیبان به‌طور گسترده برای حل مسئله یادگیری، پیش‌بینی و طبقه‌بندی استفاده می‌شود [۲۶-۲۸]. مدل‌های ANFISبه دلیل عملکرد قابل قبولی که در زمینه ایجاد و آموزش طبقه بند فازی داده دارند، بسیار موردتوجه واقع‌شده‌اند. یک چالش اصلی در طراحی یک سامانه ANFIS رسیدن به یک روش کارآمد، با دقت بالا و قابلیت تفسیر مناسب است که اخیراً در زمینه تشخیص نفوذ هم مورداستفاده قرارگرفته‌اند [۲۹ و ۳۰].

۳-۱- دسته‌بندی کننده عصبی- فازی

شبکه عصبی مصنوعی و منطق فازی، هر دو ابزارهای هوش مصنوعی هستند که می‌توانند برای ساخت یک سیستم هوشمند دیگر، مکمل یکدیگر باشند. شبکه عصبی مصنوعی ساختار محاسباتی سطح پایینی است که به‌خوبی با داده‌های خام اولیه کار می‌کند. در مقابل منطق فازی با استدلال‌های سطح بالایی که با استفاده از دانش یک متخصص در یک حوزه خاص به‌دست‌آمده‌اند، سروکار دارد [۳۱].

شبکه عصبی – فازی می‌تواند به دو صورت ترکیب شبکه عصبی با فازی ممدانی و یا ترکیب شبکه عصبی با فازی سوجینو ایجاد گردد. در سال ۱۹۹۳ ژانگ[1]، برای اولین بار با مدنظر قرار دادن توانایی‌های تئوری فازی که مبتنی بر قواعد منطقی بوده و همچنین روش شبکه عصبی مصنوعی که توانائی استخراج دانش از اطلاعات عددی را دارند، سیستم استنتاج تطبیقی عصبی-فازی را ارائه نمود [۳۲]. سیستم ارائه‌شده توسط ژانگ، انفیس[2] خوانده می‌شود.

در سیستم فازی سوجینو قوانین به‌صورت زیر استنتاج می‌شوند:

IF x_1 is A_1

AND x_2 is A_2

. . . . .

AND x_m is A_m

THEN $y = f(x_1, x_2, \ldots, x_m)$

ورودی و خروجی هر لایه مشخص‌شده و رابطه مرتبط با آن به‌صورت زیر بیان می‌شود [۳۱].

لایه ۱: لایه ۱ لایه ورودی است. گره‌ها در این لایه داده‌ها را برای لایه ۲ آماده می‌کنند. در این لایه هیچ تغییری روی داده‌ها صورت نمی‌گیرد به‌طوری‌که ورودی با خروجی برابر است.

لایه ۲: در این لایه عمل فازی سازی روی داده‌ها انجام می‌شود.

لایه ۳: این لایه، لایه قوانین است. هر گره در این لایه، یک قانون فازی را نشان می‌دهد. هر گره در این لایه، ورودی خود را از خروجی‌های متناظر در لایه قبل می‌گیرد و خروجی آن قدرت آتش[3] هر قانون است.

لایه ۴: لایه ۴ لایه بهنجارسازی[4] است. در این لایه هر گره ورودی خود را از تمام گره‌های لایه قبل می‌گیرد و عدد به‌دست‌آمده برای هر گره در لایه قبل، در این لایه عادی‌سازی[5] می‌شود. خروجی هر گره در این لایه، قدرت قانون عادی‌سازی شده گره متناظر لایه قبل می‌باشد. قدرت آتش بهنجارسازی شده هر قانون، از تقسیم قدرت آتش هر قانون به جمع کل قدرت آتش قانون‌ها به دست می‌آید. قدرت قانون عادی‌سازی شده میزان نفوذ هر قانون در خروجی شبکه را نشان می‌دهد.

لایه ۵: این لایه، لایه غیر فازی سازی[6] نام دارد. هر گره در این لایه، ورودی خود را از گره متناظر در لایه قبل می‌گیرد؛ که در این رابطه، x مقدار ورودی به هر گره، y خروجی گره و k_{ij} ها شاخص‌های مربوط به قانون μ_i می‌باشد. چنانچه انفیس از مرتبه صفر باشد به‌جای x_1 و x_2 صفر قرار داده می‌شود.

لایه ۶: لایه ۶ تنها دارای یک گره می‌باشد که جمع گره‌های غیر فازی شده لایه قبل را محاسبه می‌کند.

در شبکه عصبی – فازی می‌توان با استفاده از دو روش بخش‌بندی شبکه‌ای[7] و خوشه‌بندی کاهشی[8] بدون نیاز به دانش فرد خبره، قوانین فازی را ایجاد کرد. ما از روش خوشه‌بندی کاهشی برای تعیین تعداد قوانین لازم و توابع عضویت استفاده می‌کنیم و سپس از انفیس برای ساخت سیستم تشخیص نفوذ استفاده کرده‌ایم.

[1] Jang
[2] ANFIS
[3] Fire Strength
[4] Normalize
[5] normalization
[6] defuzzification
[7] Grid Partition
[8] Subtractive Clustering

۳-۲- دسته‌بند SVM

ماشین بردار پشتیبان (SVM) روش مؤثری برای حل مسائل دسته‌بندی و رگرسیون است. SVM در اصل پیاده‌سازی اصل مینیمم سازی ریسک ساختاری واپنیک (SRM) است [۳۳] که به داشتن خطای تعمیم کم (ضعیف) معروف است که به‌طور معادل می‌توان گفت که برای مجموعه داده آموزش، بیش برازش زیادی را متحمل نمی‌شود. یک مدل را در معرض بیش برازش یا دارای خطای تعمیم بالا می‌گویند، اگر به‌طور ناچیزی روی نمونه‌هایی که در مجموعه آموزش وجود ندارد، اجرا شود. SVM به‌طور خاص روی مجموعه داده‌هایی که به‌صورت خطی تفکیک‌پذیر هستند.

توابع هسته زیر همراه با SVM مورداستفاده قرارگرفته‌اند [۳۴].

هسته خطی: $K(x_i, x_j) = x_i x_j$

هسته چندجمله‌ای: $K(x_i, x_j) = (y x_i^t x_j + r^d)^2$

هسته RBF: $K(x_i, x_j) = e^{\gamma \|x_i - x_j\|^2}$

هسته حلقوی: $K(x_i, x_j) = \tanh(y x_i^t x_j + r)$

SVM، هنگامی‌که از تابع هسته RBF استفاده شود، بهترین نتایج را برای دسته‌بندی تولید می‌کند [۳۳]. نتایج آزمایش‌ها نشان داده است که عملکرد دسته‌بند SVM با تابع هسته RBF متفاوت با انتخاب تابع RBF است. مقدار انتخاب‌شده برای شاخص RBF توسط بردار RBF با مقدار RBF= 0.2 تعریف‌شده است.

۳-۳- الگوریتم PSO

بهینه‌سازی گروه ذرات یک الگوریتم تکرارشونده مبتنی بر جمعیت است که توسط کندی و ابرهارت [۳۵] ایجاد شده است. الگوریتم با مجموعه‌ای از عوامل، به نام ذرات، در موقعیت‌های تصادفی در فضای مسئله شروع می‌شود. هرکدام از آن‌ها نیز در ابتدا با سرعت تصادفی مقداردهی می‌شوند. یک تابع برازش در محل یک‌ذره تعریف‌شده است. مسئله بهینه‌سازی به‌منظور به دست آوردن بهترین موقعیت حل می‌شود، به عبارتی تابع برازش را به حداقل برساند. در هر تکرار، الگوریتم، برازش هر ذره را ارزیابی، سرعت آن را به‌روزرسانی و موقعیت جدید خود را محاسبه می‌کند. سرعت جدید یک‌ذره، به‌سرعت فعلی آن، فاصله آن از بهترین موقعیت خود تاکنون و فاصله آن از بهترین موقعیت‌های جمعیت بستگی دارد. در مقایسه با الگوریتم‌های ژنتیکی (GA)، در PSO، اپراتورهای ارزیابی مانند تقاطع و جهش[1] جهش[1] وجود ندارد، که این امر باعث سهولت در پیاده‌سازی برای مسائل مختلف شود [۱۲]. توضیحات تکمیلی در ادامه آمده است.

[1] crossover and mutation

۳-۴- مجموعه داده‌ها

در این قسمت، یازده مجموعه داده IDS آنالیز و ارزیابی می‌شود.

DARPA[2]: مجموعه داده، برای آنالیز امنیت شبکه ساخته شد و مشکلات مربوط به تزریق مصنوعی حملات و ترافیک خوش‌خیم را نمایش داد. این مجموعه داده شامل email, browsing, FTP, Talent, IRC و فعالیت‌های SNMP است و حملاتی مثل Dos, Guess password, Buffer overflow, remote FTP, Syn flood, Nmap و Rootkit را شامل می‌شود. این مجموعه داده‌ها، از نظر نوع حمله و زیرساخت شبکه، برای ارزیابی IDS ها بر روی شبکه‌های است [۳۶ و ۳۷].

KDD'99[3]: این مجموعه داده یک نسخه به‌روز شده از DARPA98 با پردازش بخش tcpdump است. شامل حملات مختلفی مانند Neptune-DoS, pod-DoS, Smurf-DoS, and buffer-overflow است [۳۸]. Benign و ترافیک حملات در یک محیط شبیه‌سازی ادغام‌شده‌اند. این مجموعه داده شامل تعداد زیادی از سوابق زائد است و به‌وسیله data corruption ها آسیب‌دیده که منجر به خطا در نتایج آزمایش می‌شود [۳۹]. NSL-KDD با استفاده از KDD و به‌منظور پاسخ به ایرادات KDD ایجاد شد [۴۰]. جدول توزیع حملات در مجموعه داده‌های NSL_KDD در ضمیمه آورده شده است.

DEFCON[4]: مجموعه داده DEFCON-8 در سال ۲۰۰۰ ایجاد شد شامل حملات port scanning و buffer overflow است، درحالی‌که مجموعه داده DEFCON-10 که در سال ۲۰۰۲ ایجاد شد شامل حملات port scan and sweeps, bad packets, administrative privilege, و FTP به‌وسیله پروتکل Talent است. در این مجموعه داده، ترافیک به وجود آمده در «the Capture Flag (CTF)» با ترافیک شبکه واقعی متفاوت است چون شامل ترافیک نفوذی است که با ترافیک معمولی متفاوت است [۴۱].

CAIDA[5]: این سازمان دارای سه مجموعه داده مختلف است، CAIDA OC48، که شامل انواع مختلف داده‌های مشاهده‌شده در پیوند OC48 در سان خوزه، CAIDA DDOS، که شامل ترافیک حمله DDoS یک‌ساعته از فایل‌های ۵ دقیقه‌ای pcap و اینترنت CAIDA است. traces 2016، که آثار ترافیکی غیرفعال از نمایشگر[6] CAIDA Equinix-Chicago در ستون فقرات[7] اینترنت پرسرعت است [۴۲].

[2] Lincoln Laboratory 1998-99
[3] University of California, Irvine 1998-99
[4] The Shmoo Group, 2000-2002
[5] Center of Applied Internet Data Analysis 2002-2016
[6] monitor
[7] backbone

LBNL[1]: مجموعه داده ترافیک شبکه full header است و در یک سایت با اندازه متوسط[2] ثبت‌شده است. این مجموعه داده به‌آسانی می‌تواند هرگونه اطلاعات از یک IP شخصی را شناسایی کند [۴۳].

CDX[3]: این مجموعه داده نشان‌دهنده رقابت‌های جنگی شبکه‌ای است که می‌تواند برای ایجاد مجموعه داده برچسب دار امروزی استفاده شود. شامل ترافیک‌های شبکه‌ای مثل وب، ایمیل، جست‌وجوهای DNS و باقی سرویس‌های موردنیاز است. مهاجمین، برای پیشبرد شناسایی و حمله به‌صورت خودکار از ابزارهای حمله مانند Nessus, Nikto و WebScarab استفاده کردند. این مجموعه داده می‌تواند برای آزمون قوانین هشدار IDS استفاده شود [۴۴].

Kyoto[4]: این مجموعه داده‌ها از طریق honeypot ها ایجادشده است، بنابراین هیچ فرآیندی برای برچسب‌گذاری و شناسایی دستی وجود ندارد، اما به خاطر این‌که فقط حملات به honeypot ها قابل‌مشاهده است دید محدودی از ترافیک شبکه دارد. این مجموعه داده ده ویژگی اضافه مانند شناسایی IDS، تشخیص بدافزار و تشخیص Ashula که از مجموعه داده‌های در دسترس گذشته در آنالیز و ارزیابی NIDS مفید بودند را دارد. ترافیک نرمال در طول حملات مکرراً شبیه‌سازی‌شده و فقط DNS و داده ترافیک mail را تولید می‌کند؛ که در ترافیک شبکه نرمال جهان واقعی منعکس نمی‌شود، پس هیچ false positive وجود ندارد که برای کاهش تعداد هشدارها مهم است [۴۷-۴۵].

Twente[5]: این مجموعه داده شامل سه سرویس ازجمله OpenSSH، Apache web server و Proftp با استفاده از auth/ident روی پورت ۱۱۳ است و داده‌ها را با استفاده از Netflow و از شبکه honeypot گرفته است. تعدادی ترافیک شبکه هم‌زمان مانند auth/ident، ICMP و IRC وجود دارد که کاملاً خوش‌خیم یا بدخیم نیستند. علاوه بر آن، این مجموعه داده برخی ترافیک‌های هشدار ناشناس و نامربوط را شامل می‌شود. این مجموعه داده برچسب‌گذاری شده و واقع‌بینانه‌تر است ولی فقدان تنوع و حجم حملات واضح است [۴۸].

UMASS[6]: مجموعه داده، فایل‌های ردگیری بسته‌های شبکه‌ای هستند و برخی ردگیری‌ها بر روی برنامه‌های بی‌سیم را شامل می‌شود که به‌وسیله یک طرح حمله درخواست دانلود TCP-based تولیدشده است [۴۹]. UMass یک مخزن ردیابی است که توسط دانشگاه ماساچوست آمهرست ارائه شده است[۵۰]. داده‌های این مجموعه داده، مربوط به حمله شبکه با انواع مختلف داده‌ها هستند، این داده‌ها شامل، جریان ترافیک از شبکه TOR، شبیه‌سازی حمله در شبکه اشتراک‌گذاری داده‌های همتا به همتا، شبیه‌سازی حمله محلی سازی غیرفعال با مجموعه داده‌های استخراج واقعیت حاوی داده‌های حسگر (مجاورت، مکان، برچسب‌های مکان و غیره) و داده‌های نظرسنجی (ویژگی‌های شخصی، گروه تحقیق، موقعیت، محله کاشانه و شیوه زندگی) هستند [۵۱].

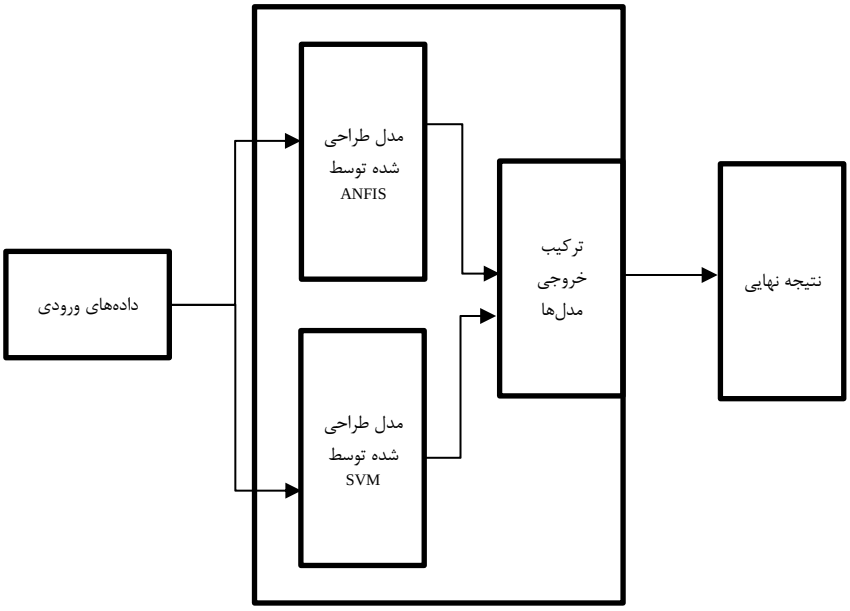
ISCX2012[7]: این مجموعه داده دو پروفایل دارد؛ پروفایل آلفا که طرح‌های متفاوت حمله را اجرا می‌کند و پروفایل بتا که تولیدکننده ترافیک ملایم است و ترافیک شبکه واقعی با اختلال پس‌زمینه ایجاد می‌کند. شامل ترافیک شبکه برای پروتکل‌های HTTP، SMTP، SSH، IMAP، POP3 و FTP با payload packet کامل است. هرچند، پروتکل‌های شبکه جدید را نشان نمی‌دهد، برای این‌که نزدیک به هفتاد درصد از ترافیک‌های شبکه امروزی HTTPS هستند و هیچ ردگیری HTTPS در این مجموعه داده وجود ندارد. به‌علاوه، توزیع حملات شبیه‌سازی‌شده بر اساس ارقام دنیای واقعی نیست [۱۶].

ADFA[8]: این مجموعه داده در هر vector شامل آموزش معمول و داده اعتبارسنجی و ۱۰ حمله است [۵۲]. این مجموعه داده شامل brute force با رمز عبور SSH و FTP، Java based Meterpreter، Add new Superuser, Linux Meterpreter payload و حملات C100Webshel است. مشکلی که این مجموعه داده دارد این است که در این مجموعه داده رفتارهای برخی حملات به‌خوبی از رفتار معمول جدا نشده است [۵۳].

۴- روش تحقیق

هدف این مقاله طراحی یک سیستم تشخیص نفوذ ترکیبی است که دقت تشخیص نفوذ را بهبود بخشد. در شکل (۱) شمای کلی طرح پیشنهادی آورده شده است. همان‌طور که در شکل مشخص است، دسته‌بندی‌ها به‌صورت جداگانه عمل کرده و خروجی خود را به PSO برای ترکیب جواب‌ها می‌فرستند تا جواب نهایی مشخص شود.

1. Lawrence Berkeley National Laboratory and ICSI 2004-2005
2. medium-sized
3. United States Military Academy 2009
4. Kyoto University 2009
5. University of Twente 2009
6. University of Massachusetts 2011
7. University of New Brunswick 2012
8. University of New SouthWales 2013



شکل (۱). شما کلی روش انجام کار

برای تعریف تابع تصمیم نهایی، ابتدا باید نحوه استفاده از وزن‌ها در فرآیند رأی‌گیری را در نظر بگیریم. برای یک مشاهده x، n مقدار خروجی $(y_1, y_2 \ldots, y_n)$ به دست می‌آید که یک مقدار خروجی برای هر متخصص در نظر گرفته می‌شود و در مدل طراحی‌شده، چون هر مدل یک خروجی دارد درنتیجه n=2 خواهد بود. هر مقدار را می‌توان به‌عنوان یک نمونه مثبت یا منفی تعریف کرد، به‌عنوان‌مثال $y_j = \{۱، -۱\}$. که در آن مقدار ۱ مربوط به خروجی متخصص ۱ است و مقدار ۱- نشان‌دهنده خروجی ۰ مدل است. تصمیم نهایی y با ارزیابی معادله (۳) به دست می‌آید.

$$y = sng(\sum_{j=1}^{n} w_j . y_j) \qquad (۳)$$

که در آن موارد تساوی یا sgn(0) ، به‌طور تصادفی مشخص می‌شوند. هر ضریب w_j با خروجی از j امین متخصص y_j ضرب می‌شود و تصمیم نهایی با تعیین علامت مجموع ضرایب وزنی برای هر دوازده متخصص تشکیل می‌شود.

پایه ریاضی الگوریتم ترکیبی به‌صورت زیر است. فرض شده $A \subset R_n$ فضای جستجو و $f: A \rightarrow Y \subseteq R$ تابع هدف مسئله است. همچنین فرض می‌شود که A نیز فضای شدنی مسئله داده شده است. به‌عبارت‌دیگر، محدودیت‌های صریحی برای راه‌حل‌های (جواب) موجود، وجود ندارد؛ بنابراین فضای جستجو به‌صورت مجموعه‌ای از همه موقعیت‌های ذرات N (راه‌حل‌های داوطلب)، به‌صورت $S = \{s_1, s_2, s_3, \ldots, s_N\}$ تعریف می‌شود. هر جواب S_i به‌صورت $s_i= (s_{i1}, s_{i2}, \ldots, s_{in})^T$ در $i=(1,2,\ldots,N)$ تعریف می‌شود که n بعد فضای جستجو است.

اندیس‌ها به‌طور دلخواهی به ذرات اختصاص داده می‌شوند، درحالی‌که تعداد ذرات N یک شاخص تعریف‌شده توسط کاربر الگوریتم است (در واقع به‌عنوان ورودی الگوریتم تعریف می‌شود). تابع هدف $f(s)$ فرض شده است که برای تمام نقاط در A در دسترس است؛ بنابراین هر ذره دارای یک مقدار تابع منحصربه‌فرد، $f_i = f(s_i) \in Y$ است. ذرات که برای حرکت در فضای جستجو در نظر گرفته‌شده‌اند، تکراری هستند. این مورد با به‌روزرسانی موقعیت آن‌ها با استفاده از تغییر موقعیت مناسب، به نام سرعت و به‌صورت $(v_{i1}, v_{i2}, \ldots, v_{in})^T$، در $i=(1,2,\ldots,N)$ انجام‌شده است. سرعت به‌صورت مکرر بروز رسانی می‌شود به‌طوری‌که هر ذره می‌تواند هر ناحیه A را ملاقات کند. اگر t برای شمارش تکرار (یا واحد زمان) باشد، موقعیت فعلی i امین ذره و سرعت آن به ترتیب به‌صورت $s_i(t)$ و $v_i(t)$ مشخص می‌شود.

بهترین موقعیت هر ذره در آرایه‌ای از حافظه ذخیره می‌شود که حاوی بهترین موقعیت‌ها به‌صورت $p_i= (p_{i1}, p_{i2}, \ldots, p_{in})^T \in A$ در $i=(1,2,\ldots,N)$ است؛ بنابراین علاوه بر مجموعه گروه S، مجموعه $P = \{p_1, p_2, \ldots, p_N\}$ برای بهترین موقعیت‌ها، در نظر گرفته می‌شود. این موقعیت‌ها به‌صورت $p_i(t) = \arg\min_t(f_i(t))$ تعریف می‌شوند. یک مکانیسم ارتباطی وجود دارد که اطلاعاتی را از بهترین موقعیتی که توسط تمام ذرات بازدید می‌شود، به اشتراک می‌گذارد. این موقعیت به‌صورت $p_g = \arg\min_t f(p_i(t))$ تعریف می‌شود. معادلات مربوط به بروز رسانی PSO که در این کار استفاده‌شده است، به‌صورت زیر تعریف‌شده است [۵۴]:

$$v_{ij}(t+1)=\omega v_{ij}(t)+\emptyset_p r_p(pij(t)-xij(t))+\emptyset_g r_g(pgj(t)-xij(t)) \qquad (۴)$$

$$s_{ij}(t+1) = s_{ij}(t) + v_{ij}(t+1) \qquad (۵)$$

که i= 1,2,…,N اندیس هر ذره در گروه است؛ j= 1,2,…,N نشان‌دهنده j امین عنصر از i امین ذره s(t) و سرعت vi (t) است؛ rp، rg متغیرهای تصادفی هستند که به‌طور یکنواخت توزیع‌شده‌اند، pi(t) بهترین موقعیت ذره در تکرار قبلی است، p_g (t) نیز بهترین موقعیت در کل گروه برای تکرار قبلی است. عامل‌های ω، $Ø_g$ و $Ø_p$ شاخص‌های رفتاری تعریف‌شده توسط کاربر هستند که به ترتیب وزن یا نسبت سکون (فشردگی)، شتاب ذره و شتاب گروه را نشان می‌دهد.

شبه کد الگوریتم PSO به‌صورت زیر تعریف‌شده است:

الگوریتم PSO

```
procedure PSO
  for particle i ∈ {1, 2, . . ., N} do
    for dimension j ∈ {1, 2, . . ., n} do
      set s_ij ~ U(lowerBoundaryj, upperBoundaryj)
      set d_j ← |upperBoundaryj − lowerBoundaryj|
      set v_ij~U(−d_j, d_j)
      set p_ij ← s_ij
      if f(p_ij) < f(p_gj) then
        set p_gj ← p_ij
  for timestep t ∈ {1, 2, . . ., I_max} do
    for particle i ∈ {1, 2, . . ., N} do
      set r_p ~ U(0, 1)
      set r_g ~ U(0, 1)
      for dimension j ∈ {1, 2, . . ., n} do
        update v_ij, s_ij from (1), (2)
        if f(s_ij) < f(p_ij) then
          set p_ij ← s_ij
          if f(p_ij) < f(p_gj) then
            set p_gj ← p_ij
  print best solution p_gj
```

معیارهای توقف زمانی برآورده می‌شود که تکرار t به حداکثر تعداد مجاز خود یعنی I_{max} برسد. مجموعه‌ای از ذرات s_g (t = I_{max}) با حداقل مقدار تابع تناسب به‌عنوان راه‌حل بهینه اعلام‌شده است. در این مقاله، ذره با بهترین برازش $s_g = (s_{g1}, s_{g2}, \ldots, s_{gn})$ مجموعه بهینه ضرایب وزنی $w = (w_1, w_2, \ldots, w_n)$ را نشان می‌دهد که n نشان‌دهنده تعداد متخصص در گروه است. بنابراین، هر ذره s مجموعه‌ای بالقوه از ضرایب وزنی w را نشان می‌دهد. برای هر مشاهده x در نمونه، معادله (۳) را ارزیابی می‌کنیم تا کلاس پیش‌بینی‌شده با الگوریتم رأی‌گیری y را به دست آوریم. در یک مجموعه آموزشی با اندازه m، تعدادی مشاهدات c را که به‌درستی طبقه‌بندی‌شده‌اند، یعنی y = T. دقت برای مجموعه وزن‌های تولیدشده ACC(w) کسری از مشاهدات طبقه‌بندی‌شده صحیح است، یعنی ACC(w) =c/m، که m تعداد کل مشاهدات از نمونه اعتبارسنجی است. برای دستیابی به عملکرد بهتر طبقه‌بندی‌کننده‌های گروه، باید دقت را به حداکثر برسانیم یا خطا را برای هر ذره در ازدحام به حداقل برسانیم. بنابراین ما عملکرد تابع هزینه را که باید به حداقل برسانیم، به‌صورت زیر تعریف می‌کنیم:

$$ACC(w) = 1 - c/m$$

وزن‌ها برای هر کلاس به‌طور جداگانه تولید می‌شوند. طبقه‌بندی‌کننده گروهی که با وزن‌های PSO ایجادشده است، ساختاری مشابه یک متخصص خواهد داشت که در شکل (۱) نشان داده‌شده است. در نتیجه، ما باید دو مجموعه وزن، یکی برای هر طبقه‌بندی کننده باینری، با PSO تولید کنیم. توجه به این نکته ضروری است که از داده‌های اعتبارسنجی برای تولید وزن استفاده می‌شود. این امر ضروری است زیرا ما نمی‌توانیم دقت ارزیابی هر طبقه‌بندی کننده را با داده‌های آموزشی تصحیح کنیم.

۴-۱- بررسی مجموعه داده‌ها

مجموعه داده‌های تشخیص نفوذ ایجادشده از آثار واقعی ترافیک شبکه در جدول (۱) ارائه شده است. این مجموعه داده‌ها برای ارزیابی عملکرد IDS توسط بسیاری از محققان استفاده شد. در این جدول تعداد ویژگی‌ها و نوع حملات مشخص شده است.

جدول (۱). خلاصه‌ای از مجموعه داده‌ها

نام مجموعه داده	توسعه داده‌شده توسط	ویژگی‌ها	نوع حملات	توضیحات
DARPA	آزمایشگاه MIT لینکلن	41	Dos, R2L, Probe, U2R	این مجموعه داده، نشان‌دهنده ترافیک واقعی شبکه، عدم وجود موارد مثبت کاذب، بی‌نظمی در موارد داده‌های حمله نیست [36, 37].
KDD CUP 99	دانشگاه کالیفرنیا	41	Dos,R2L, Probe, U2R	این مجموعه داده، شامل نمونه‌های اضافی و تکراری داده‌ها است [۳۸].
NSL-KDD	دانشگاه کالیفرنیا	41	Dos,R2L, Probe, U2R	نسخه بهینه‌شده مجموعه داده KDD CUP 99 و شامل تعداد محدودی از انواع حمله است[۴۰].

ادامه جدول (۱). خلاصه‌ای از مجموعه داده‌ها

نام مجموعه داده	توسعه داده‌شده توسط	ویژگی‌ها	نوع حملات	توضیحات
DEFCON	گروه Shmoo	Flag traces	Telnet Protocol Attacks	ویژگی‌ها از طریق مسابقه "Capture the Flag" ثبت می‌شوند [۴۱].
CAIDA	مرکز تجزیه‌وتحلیل داده‌های کاربردی اینترنت	20	DDoS	این مجموعه داده، شامل مواردی است که مخصوص نوع خاصی از حمله یا فعالیت اینترنتی است [۴۲].
LBNL	آزمایشگاه ملی لارنس برکلی	Internet traces	Malicious traces	این مجموعه داده، شامل ۱۰۰ ساعت فعالیت است که آثار سربرگ بسته[1] را برای شناسایی ترافیک مخرب مشخص می‌کند [۴۳].
CDX	آموزشگاه نظامی ایالات‌متحده	5	Buffer Overflow	این مجموعه داده از ابزارهای شبکه Nikto و Nessus برای جذب ترافیک استفاده کرده و برای ارزیابی قوانین هشدار IDS استفاده شد [۴۴].
Kyoto	دانشگاه Kyoto	24	Normal and Attack sessions	این برنامه با استقرار honeypot ها در شبکه توسعه‌یافته است اما هیچ‌گونه جزئیاتی در مورد انواع حمله توصیف نمی‌کند [45-47]
Twente	دانشگاه Twente	IP flows	ترافیک مخرب، ترافیک جانبی، ترافیک ناشناخته و هشدارهای نامربوط	اندازه مجموعه داده کوچک است و دامنه انواع حمله محدود است [۴۸].
ISCX2012	دانشگاه New Brunswick	IP flows	DoS, DDoS, Brute-force, Infiltration	این مجموعه داده شامل سناریوهای شبکه با فعالیت‌های مزاحم و نمونه‌های برچسب داده است [۱۶].
AFDA	دانشگاه South New Wales	System call traces	حملات صفر روز[2]، حمله مخفی‌کاری[3]، حمله C100 Webshell	این مجموعه داده شامل ۱۰ بردار حمله به همراه آثار نمونه‌های دیگر داده است اما حملات محدودی را شامل می‌شود [۵۳].

در نهایت نقاط قوت و ضعف مجموعه داده‌های سیستم‌های تشخیص نفوذ، بر اساس ۱۱ معیار از آخرین چارچوب ارزیابی مجموعه داده، را ارزیابی می‌کنیم [۵۵]. کیفیت مجموعه داده‌های تولیدشده در جدول (۲) نشان داده‌شده است. درمجموع، یازده ویژگی به شرح زیر تعریف می‌شود:

Complete Network Configuration, Complete Traffic, Labeled Dataset, Complete Interaction, Complete Capture, Available Protocols, Attack Diversity, Anonymity, Heterogeneity, Feature set, Metadata.

۴-۲- نتایج تجربی

برای تجزیه‌وتحلیل، از سه معیار ارزیابی بازیابی اطلاعات رایج زیر استفاده شد:

دقت (Pr) یا ارزش قابل پیش‌بینی مثبت، یادآوری (Rc) یا حساسیت F-Measure (F1)

$$\text{Recall (Rc)}=\frac{(TP)}{(TP+FN)} \quad (۳)$$

$$\text{Pr}=\frac{(TP)}{(TP+FP)} \quad (۴)$$

$$\text{F\_measure} =\frac{2}{\frac{1}{Rc}+\frac{1}{Pr}} \quad (۵)$$

تمام پیاده‌سازی‌های این مقاله در کامپیوتری باقابلیت پردازنده 2/53GHz پنج هسته‌ای و چهار گیگابایت حافظه موقت (4G RAM) و در نرم‌افزار متلب نسخه ۷,۱۰,۰ (2010a) پیاده‌سازی شده است. آزمون ارزیابی مجموعه داده، با توجه به آخرین چارچوب ارزیابی مجموعه داده‌های، مقایسه شده است [۱۳]. جدول (۳) و (۴) نتایج عملکرد را با توجه به معیارهای ارزیابی، برای دو الگوریتم یادگیری انتخاب‌شده به نام‌های ANFIS و SVM به‌دست‌آمده بر روی مجموعه داده‌های معرفی‌شده را نشان می‌دهد. یکی از علت‌های متفاوت بودن زمان اجرای هر مجموعه داده می‌تواند این باشد که هر مجموعه نیاز به‌پیش پردازش متفاوتی است. علاوه بر این تعداد و نوع داده‌ها در هر مجموعه متفاوت هستند، لذا این مرحله باعث به وجود آمدن زمان‌های متفاوت در مدل‌های مختلف شده است. تحلیلی که می‌توان در مورد پایین بودن نتایج SVM ارائه داد، این است که چون خروجی این مدل به‌صورت دودویی است یعنی مدل مشخص می‌کند که حمله‌ای صورت گرفته یا نه (با مقدار ۰ یا ۱) بهتر بود از هسته خطی در این مدل استفاده شود و هسته RBF در مدل‌هایی که خواسته شود که مدل طراحی‌شده خروجی را به دسته‌های مختلف تقسیم کند بهتر خواهد بود. یعنی اگر می‌خواستیم حملات مختلف را مشخص کنیم بهتر بود از هسته

[1] Packet Header
[2] Zero-Day
[3] Stealth

RBF استفاده می‌کردیم ولی چون مجموعه داده‌های مختلف داده‌های و حملات یکسانی نداشتند پیاده این روش در این حالت غیرممکن بود.

جدول (۳). نتایج svm

Dataset	Pr	Rc	F1	زمان (s)
DARPA	81/46	94/84	87/64	27/45
NSLKDD	76/57	95/26	84/89	19/16
DEFCON	75/98	96/21	84/9	36/51
CAIDAs	76/89	94/33	84/72	22/73
LBNL	72/93	93/61	81/98	25/26
CDX	69/81	92/24	79/47	33/24
KYOTO	76/66	96/48	85/43	29/84
TWENTE	75/01	94/02	83/52	21/48
ISCX2012	77/27	94/44	84/99	31/34
ADFA2013	75/22	93/71	83/45	23/71

جدول (۴). نتایج انفیس

Dataset	Pr	Rc	F1	زمان (s)
DARPA	79/49	95/34	86/69	28/01
NSLKDD	95/69	97/45	96/56	20/34
DEFCON	80/01	95/46	87/05	35/18
CAIDAs	79/26	95/35	86/56	22/50
LBNL	80/52	96/32	87/71	26/81
CDX	80/96	95/04	87/43	34/12
KYOTO	95/49	97/25	96/36	29/97
TWENTE	95/07	92/03	93/52	21/37
ISCX2012	96/89	92/92	94/86	31/86
ADFA2013	92/54	97/93	87/05	24/03

جدول (۵) شامل نتیجه نهایی ترکیب دو روش انفیس و svm است که همان‌طور که در این جدول مشاهده می‌شود نتایج قابل قبولی از ترکیب دودسته بند به‌دست‌آمده است. در نمودار (۱) نمودار مقایسه‌ای بین روش‌های جداگانه و روش ترکیبی با استفاده از معیار ارزیابی حساسیت (F1) انجام‌گرفته است. و نتایج قابل‌مشاهده است که روش ترکیبی دارای نتایج بهتری است. در نمودار (۲) نیز زمان محاسبه دسته بنده‌ها به‌صورت جداگانه و زمان ترکیب آن‌ها آورده شده است. هرچند زمان محاسبه در این حالت ترکیبی از تک‌تک دسته بنده‌ها بیشتر است ولی با توجه به اینکه دقت تشخیص در بیشتر موارد افزایش یافته است؛ لذا این افزایش ناچیز زمانی را می‌شود چشم‌پوشی کرد. در ادامه در جدول شماره (۶) مدل‌های دیگر که با مجموعه داده‌های متفاوت موردبررسی قرار گرفته‌اند، آورده شده است. در این جدول از معیار دقت استفاده شده است که در بیشتر تحقیقات از این معیار برای ارزیابی استفاده می‌شود. در این مقالات نیز از این معیار هم استفاده شده است. علاوه بر این در بعضی از تحقیقات از انتخاب یا استخراج ویژگی نیز استفاده شده است که در جدول مشخص است. این جدول را می‌توان با نتایج به‌دست‌آمده از روش پیشنهادی در این مقاله در جدول (۵) مورد مقایسه قرار داد.

جدول (۵). نتایج ترکیب با استفاده از PSO

Dataset	Pr	Rc	F1	زمان (S)
DARPA	81/01	97/21	88/37	28/94
NSLKDD	81/96	96/26	88/54	21/40
DEFCON	82/46	96/34	88/86	37/39
CAIDAs	80/26	96/35	87/57	23/45
LBNL	81/52	97/32	88/72	27/68
CDX	96/69	96/45	96/57	35/05
KYOTO	96/49	97/48	96/98	30/15
TWENTE	96/07	96/32	96/19	22/40
ISCX2012	97/89	95/44	96/65	32/75
ADFA2013	93/54	98/93	96/16	24/96

۴-۲- نتایج تجربی

برای تجزیه‌وتحلیل، از سه معیار ارزیابی بازیابی اطلاعات رایج زیر استفاده شد:

دقت (Pr) یا ارزش قابل پیش‌بینی مثبت، یادآوری (Rc) یا حساسیت F-Measure (F1)

$$\text{Recall (Rc)}=\frac{(TP)}{(TP+FN)} \quad (۶)$$

$$\text{Pr}=\frac{(TP)}{(TP+FP)} \quad (۷)$$

$$\text{F\_measure} =\frac{2}{\frac{1}{Rc}+\frac{1}{Pr}} \quad (۸)$$

تمام پیاده‌سازی‌های این مقاله در کامپیوتری باقابلیت پردازنده 2/53GHz پنج هسته‌ای و چهار گیگابایت حافظه موقت (4G RAM) و در نرم‌افزار متلب نسخه ۷,۱۰,۰ (2010a) پیاده‌سازی شده است. آزمون ارزیابی مجموعه داده، با توجه به آخرین چارچوب ارزیابی مجموعه داده‌های، مقایسه شده است [۱۳]. جدول (۳) و (۴) نتایج عملکرد را با توجه به معیارهای ارزیابی، برای دو الگوریتم یادگیری انتخاب‌شده به نام‌های ANFIS و SVM به‌دست‌آمده بر روی مجموعه داده‌های معرفی‌شده را نشان می‌دهد. یکی از علت‌های متفاوت بودن زمان اجرای هر مجموعه داده می‌تواند این باشد که هر مجموعه نیاز به‌پیش پردازش متفاوتی است. علاوه بر این تعداد و نوع داده‌ها در هر مجموعه متفاوت هستند، لذا این مرحله باعث به وجود آمدن زمان‌های متفاوت در مدل‌های مختلف شده است. تحلیلی که می‌توان در مورد پایین بودن نتایج SVM ارائه داد، این است که چون خروجی این مدل به‌صورت دودویی است یعنی مدل مشخص می‌کند که حمله‌ای صورت گرفته یا نه (با مقدار ۰ یا ۱) بهتر بود از هسته خطی در این مدل استفاده شود و هسته RBF در مدل‌هایی که خواسته شود که مدل طراحی‌شده خروجی را به دسته‌های مختلف تقسیم کند بهتر خواهد بود. یعنی اگر می‌خواستیم حملات مختلف را مشخص کنیم بهتر بود از هسته

RBF استفاده می‌کردیم ولی چون مجموعه داده‌های مختلف داده‌های و حملات یکسانی نداشتند پیاده این روش در این حالت غیرممکن بود.

جدول (۳). نتایج svm

Dataset	Pr	Rc	F1	زمان (s)
DARPA	81/46	94/84	87/64	27/45
NSLKDD	76/57	95/26	84/89	19/16
DEFCON	75/98	96/21	84/9	36/51
CAIDAs	76/89	94/33	84/72	22/73
LBNL	72/93	93/61	81/98	25/26
CDX	69/81	92/24	79/47	33/24
KYOTO	76/66	96/48	85/43	29/84
TWENTE	75/01	94/02	83/52	21/48
ISCX2012	77/27	94/44	84/99	31/34
ADFA2013	75/22	93/71	83/45	23/71

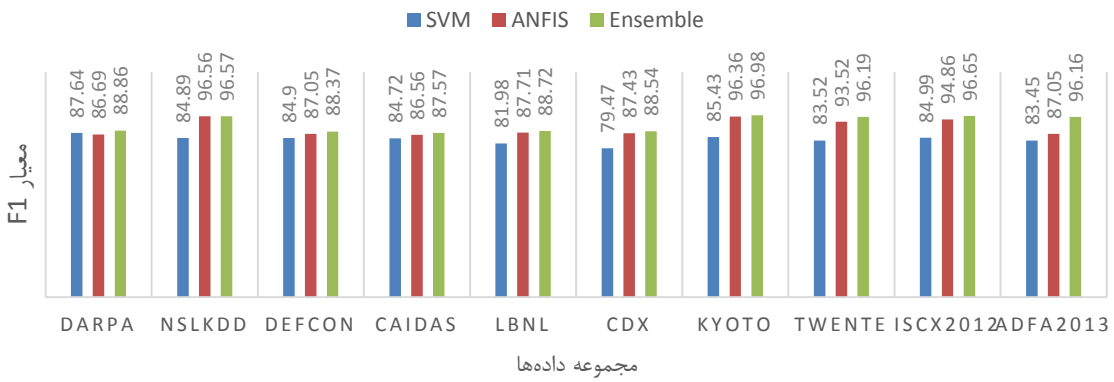
جدول (۴). نتایج انفیس

Dataset	Pr	Rc	F1	زمان (s)
DARPA	79/49	95/34	86/69	28/01
NSLKDD	95/69	97/45	96/56	20/34
DEFCON	80/01	95/46	87/05	35/18
CAIDAs	79/26	95/35	86/56	22/50
LBNL	80/52	96/32	87/71	26/81
CDX	80/96	95/04	87/43	34/12
KYOTO	95/49	97/25	96/36	29/97
TWENTE	95/07	92/03	93/52	21/37
ISCX2012	96/89	92/92	94/86	31/86
ADFA2013	92/54	97/93	87/05	24/03

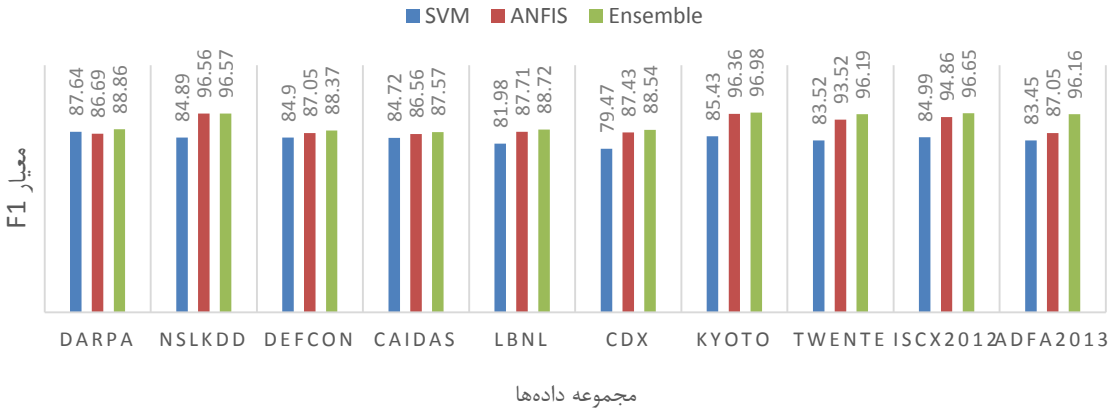
جدول (۵) شامل نتیجه نهایی ترکیب دو روش انفیس و svm است که همان‌طور که در این جدول مشاهده می‌شود نتایج قابل قبولی از ترکیب دودسته بند به‌دست‌آمده است. در نمودار (۱) نمودار مقایسه‌ای بین روش‌های جداگانه و روش ترکیبی با استفاده از معیار ارزیابی حساسیت (F1) انجام‌گرفته است. و نتایج قابل‌مشاهده است که روش ترکیبی دارای نتایج بهتری است. در نمودار (۲) نیز زمان محاسبه دسته بنده‌ها به‌صورت جداگانه و زمان ترکیب آن‌ها آورده شده است. هرچند زمان محاسبه در این حالت ترکیبی از تک‌تک دسته بنده‌ها بیشتر است ولی با توجه به اینکه دقت تشخیص در بیشتر موارد افزایش یافته است؛ لذا این افزایش ناچیز زمانی را می‌شود چشم‌پوشی کرد. در ادامه در جدول شماره (۶) مدل‌های دیگر که با مجموعه داده‌های متفاوت موردبررسی قرار گرفته‌اند، آورده شده است. در این جدول از معیار دقت استفاده شده است که در بیشتر تحقیقات از این معیار برای ارزیابی استفاده می‌شود. در این مقالات نیز از این معیار هم استفاده شده است. علاوه بر این در بعضی از تحقیقات از انتخاب یا استخراج ویژگی نیز استفاده شده است که در جدول مشخص است. این جدول را می‌توان با نتایج به‌دست‌آمده از روش پیشنهادی در این مقاله در جدول (۵) مورد مقایسه قرار داد.

جدول (۵). نتایج ترکیب با استفاده از PSO

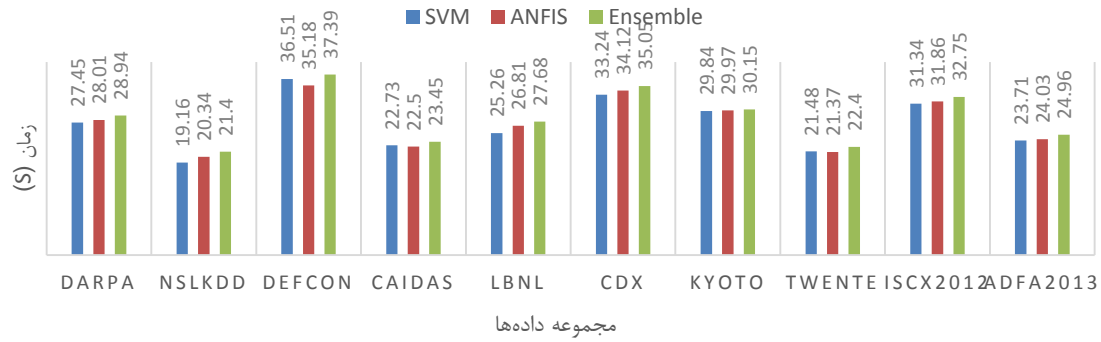
Dataset	Pr	Rc	F1	زمان (S)
DARPA	81/01	97/21	88/37	28/94
NSLKDD	81/96	96/26	88/54	21/40
DEFCON	82/46	96/34	88/86	37/39
CAIDAs	80/26	96/35	87/57	23/45
LBNL	81/52	97/32	88/72	27/68
CDX	96/69	96/45	96/57	35/05
KYOTO	96/49	97/48	96/98	30/15
TWENTE	96/07	96/32	96/19	22/40
ISCX2012	97/89	95/44	96/65	32/75
ADFA2013	93/54	98/93	96/16	24/96



نمودار (۱). نمودار مقایسه‌ای بین روش‌های جداگانه و روش ترکیبی با معیار ارزیابی F1



نمودار (۱). نمودار مقایسه‌ای بین روش‌های جداگانه و روش ترکیبی با معیار ارزیابی F1



نمودار (۲). نمودار مقایسه زمان برحسب ثانیه

جدول (۶). مقایسه چندین روش دیگر بر روی مجموعه داده‌های متفاوت

روش پیاده‌سازی	روش انتخاب یا استخراج ویژگی	تعداد ویژگی‌ها	مجموعه داده	دقت
DMNB [56]	PCA, Random Projection (RP)	All	NSL-KDD	96/50
DBN-SVM [57]	deep belief network (DBN)	All	NSL-KDD	92/84
TUIDS [58]	–	All	NSL-KDD	96/55
PSOM [59]	PCA, Fisher Discriminant Ratio (FDR), Kernel PCA, Isomap	23	NSL-KDD	88/30
EMD [60]	PCA	-	ISCX 2012	90/12
HG-GA-SVM [61]	HG, GA	35	NSL-KDD	97
SVM [62]	-	11	ISCX 2012	97/50
OS-ELM [63]	Filtered, CFS and Consistency subsets evaluation	11	Kyoto	96/37
RFAODE [64]	-	15	Kyoto	90/51
Bagging-REPTree [23]	FVBRM	25	NSL-KDD	83/22
TSE-IDS [65]	Two-stage Ensemble	37	KDD	96
XGBoost-IDS [66]	XGBoost	80	CIC	91/36
SVM Cubic[16]	-	All	ISCX 2012	87/46
SVM Quadratic [16]	-	All	CIDDS	96/6
ZED-IDS [67]	Autoencoder	83	CIC	95/73

۵- نتیجه‌گیری

همان‌طور که در بخش‌های قبل توضیح داده شد، در این تحقیق، ابتدا سیستم‌های تشخیص نفوذ فردی با الگوریتم‌های هوشمند انفیس و ماشین بردار پشتیبان طراحی شدند. این سیستم‌های تشخیص نفوذ را با برخی از مجموعه داده‌های استانداری معروف که نقاط ضعف و قوت آن‌ها را بررسی کردیم مورد ارزیابی قرار دادیم. نتایج به‌دست‌آمده با استفاده از سه معیار ارزیابی دقت، یادآوری و حساسیت بودند که تقریباً نتایج قابل قبولی بودند. در ادامه با استفاده از الگوریتم بهینه‌سازی ازدحام ذرات خروجی دو سیستم طراحی‌شده را با هم ترکیب کرده و یک خروجی به دست آوردیم که نتیجه ترکیب به‌مراتب بهتر از نتیجه فردی سیستم‌های طراحی‌شده بود.

۶- مراجع

[1] S. Akbar, K. N. Rao, & J. Chandulal, "Intrusion detection system methodologies based on data analysis," International Journal of Computer Applications, vol. 5, no. 2, pp. 10-20, 2010.

[2] T. Ahmad & M. N. Aziz, "Data preprocessing and feature selection for machine learning intrusion detection systems," ICIC Express Lett, vol. 13, no. 2, pp. 93-101, 2019.

[3] B. A. Tama, M. Comuzzi, & K.-H. Rhee, "TSE-IDS: A two-stage classifier ensemble for intelligent anomaly-based intrusion detection system," IEEE Access, vol. 7, pp. 94497-94507, 2019.

[4] Z. Chiba, N. Abghour, K. Moussaid, & M. Rida, "Intelligent approach to build a Deep Neural Network based IDS for cloud environment using combination of machine learning algorithms," computers & security, vol. 86, pp. 291-317, 2019.

[5] H. Liu & B. Lang, "Machine learning and deep learning methods for intrusion detection systems: A survey," applied sciences, vol. 9, no. 20, p. 4396, 2019.

[6] R. Koch, M. Golling, & G. D. Rodosek, "Towards comparability of intrusion detection systems: New data sets," in TERENA Networking Conference, vol. 7, 2014.

[7] A. Shiravi, H. Shiravi, M. Tavallaee, & A. A. Ghorbani, "Toward developing a systematic approach to generate benchmark datasets for intrusion detection," computers & security, vol. 31, no. 3, pp. 357-374, 2012.

[8] H. Hindy et al., "A taxonomy and survey of intrusion detection system design techniques, network threats and datasets," 2018.

[9] A. Thakkar & R. Lohiya, "A survey on intrusion detection system: feature selection, model, performance measures, application perspective, challenges, and future research directions," Artificial Intelligence Review, pp. 1-111, 2021.

[10] I. S. Thaseen, C. A. Kumar, & A. Ahmad, "Integrated intrusion detection model using chi-square feature selection and ensemble of classifiers," Arabian Journal for Science and Engineering, vol. 44, no. 4, pp. 3357-3368, 2019.

[11] Y. Shen, K. Zheng, C. Wu, M. Zhang, X. Niu, & Y. Yang, "An ensemble method based on selection using bat algorithm for intrusion detection," The Computer Journal, vol. 61, no. 4, pp. 526-538, 2018.

[12] J. Kennedy, "Swarm intelligence," in Handbook of nature-inspired and innovative computing: Springer, pp. 187-219, 2006.

[13] C. Khammassi & S. Krichen, "A GA-LR wrapper approach for feature selection in network intrusion detection," computers & security, vol. 70, pp. 255-277, 2017.

[14] S. Parsa & s. H. R. Aarabi, "A New Approach to Network Intrusion Detection Based on Hybrid Methods," Scientific Journal of Electronic and Cyber Defense, vol. 5, no. 3, pp. 79-93, 2017. (Persian in)

[15] M. Abdullah, A. Alshannaq, A. Balamash, & S. Almabdy, "Enhanced intrusion detection system using feature selection method and ensemble learning algorithms," International Journal of Computer Science and Information Security (IJCSIS), vol. 16, no. 2, pp. 48-55, 2018.

[16] I. F. Kilincer, F. Ertam, & A. Sengur, "Machine learning methods for cyber security intrusion detection: Datasets and comparative study," Computer Networks, vol. 188, p. 107840, 2021.

[17] W. Wang, X. Zhang, & S. Gombault, "Constructing attribute weights from computer audit data for effective intrusion detection," Journal of Systems and Software, vol. 82, no. 12, pp. 1974-1981, 2009.

[18] F. Salo, A. B. Nassif, & A. Essex, "Dimensionality reduction with IG-PCA and ensemble classifier for network intrusion detection," Computer Networks, vol. 148, pp. 164-175, 2019.

[19] M. A. Khan, M. Karim, & Y .Kim, "A scalable and hybrid intrusion detection system based on the convolutional-LSTM network," Symmetry, vol. 11, no. 4, p. 583, 2019.

[20] Y. Zhong et al., "HELAD: A novel network anomaly detection model based on heterogeneous ensemble learning," Computer Networks, vol. 169, p. 107049, 2020.

[21] I. Syarif, E. Zaluska, A. Prugel-Bennett, & G. Wills, "Application of bagging, boosting and stacking to intrusion detection," in International Workshop on Machine Learning and Data Mining in Pattern Recognition, pp. 593-602, Springer. 2012.

[22] A. J. Malik, W. Shahzad, & F. A. Khan, "Network intrusion detection using hybrid binary PSO and random forests algorithm," Security and Communication Networks, vol. 8, no. 16, pp. 2646-2660, 2015.

[23] N. T. Pham, E. Foo, S. Suriadi, H. Jeffrey, & H. F. M. Lahza, "Improving performance of intrusion detection system using ensemble methods and feature selection," in Proceedings of the Australasian Computer Science Week Multiconference, pp. 1-6, 2018.

[24] A. Maroosi, E. Zabbah, & H. Ataei Khabbaz, "Network Intrusion Detection using a combination of artificial neural networks in a hierarchical manner," Scientific Journal of Electronic and Cyber Defense, vol. 8, no. 1, pp. 89-99, 2020. (in Persian)

[25] V. Bukhtoyarov & V. Zhukov, "Ensemble-Distributed Approach in Classification Problem Solution for Intrusion Detection Systems," Cham, 2014: Springer International Publishing, in Intelligent Data Engineering and Automated Learning – IDEAL 2014, pp. 255-265, 2014.

[26] N. Mohd ,A. Singh, and H. S. Bhadauria, "A Novel SVM Based IDS for Distributed Denial of Sleep Strike in Wireless Sensor Networks," Wireless Personal Communications, vol. 111, no. 3, pp. 1999-2022, 2020.

[27] M. Begli & F. Derakhshan, "A multiagent based framework secured with layered SVM-based IDS for remote healthcare systems," arXiv preprint arXiv:2104.06498, 2021.

[28] H. Zolfi, H. Ghorbani, & M. H. Ahmadzadegan, "Investigation and classification of cyber-crimes through IDS and SVM algorithm," in 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), pp. 180-187, 2019.

[29] M. Masdari & H. Khezri, "A survey and taxonomy of the fuzzy signature-based Intrusion Detection Systems," Applied Soft Computing, pp. 106-301, 2020.

[30] S. Manimurugan, A.-q. Majdi, M. Mohmmed, C. Narmatha, & R. Varatharajan, "Intrusion detection in networks using crow search optimization algorithm with adaptive neuro-fuzzy inference system," Microprocessors and Microsystems, vol. 79, p. 103261, 2020.

[31] M. Negnevitsky, "Artificial intelligence : a guide to intelligent systems / Michael Negnevitsky," (no. Accessed from https://nla.gov.au/nla.cat-vn3803044), New York: Addison-Wesley, 2005.

[32] J.S. Jang, "ANFIS: adaptive-network-based fuzzy inference system," IEEE transactions on systems, man, and cybernetics, vol. 23, no. 3, pp. 665-685, 1993.

[33] F. Kuang, W. Xu, & S. Zhang, "A novel hybrid KPCA and SVM with GA model for intrusion detection," Applied Soft Computing, vol. 18, pp. 178-184, 2014.

[34] S.-J. Horng et al., "A novel intrusion detection system based on hierarchical clustering and support vector machines," Expert Systems with Applications, vol. 38, no. 1, pp. 306-313, 2011.

[35] R. Eberhart & J. Kennedy, "A new optimizer using particle swarm theory," in MHS'95. Proceedings of the Sixth International Symposium on Micro Machine and Human Science, pp. 39-43, 1995, IEEE.

[36] R. K. Vigneswaran, R. Vinayakumar, K. Soman, & P. Poornachandran, "Evaluating shallow and deep neural networks for network intrusion detection systems in cyber security," in 2018 9th International conference on computing, communication and networking technologies (ICCCNT), pp. 1-6, 2018, IEEE.

[37] C. Brown, A. Cowperthwaite, A. Hijazi, & A. Somayaji, "Analysis of the 1999 darpa/lincoln laboratory ids evaluation data with netadhict," in 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications, pp. 1-7, 2009, IEEE.

[38] R. Bala & R. Nagpal, "A review on kdd cup99 and nsl nsl-kdd dataset," International Journal of Advanced Research in Computer Science, vol. 10, no. 2, 2019.

[39] M. Tavallaee, E. Bagheri, W. Lu, & A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications, pp. 1-6, 2009, IEEE.

[40] H. Ji, D. Kim, D. Shin, & D. Shin, "A study on comparison of KDD CUP 99 and NSL-KDD using artificial neural network," in Advances in computer science and ubiquitous computing: Springer, pp. 452-457, 2017.

[41] I. Sharafaldin, A. Gharib, A. H. Lashkari, & A. A. Ghorbani, "Towards a reliable intrusion detection benchmark dataset," Software Networking, vol. 2018, no. 1, pp. 177-200, 2018.

[42] O. Yavanoglu & M. Aydos, "A review on cyber security datasets for machine learning algorithms," in 2017 IEEE international conference on big data (big data), pp. 2186-2193, 2017.

[43] S. Peisert et al., "Lbnl open power data," 2017.

[44] B. Sangster et al., "Toward Instrumenting Network Warfare Competitions to Generate Labeled Datasets," in CSET, 2009.

[45] M. Sato, H. Yamaki, & H. Takakura, "Unknown attacks detection using feature extraction from anomaly-based ids alerts," in 2012 IEEE/IPSJ 12th International Symposium on Applications and the Internet, pp. 273-277, 2012.

[46] R. Chitrakar & C. Huang, "Anomaly based intrusion detection using hybrid learning approach of combining k-medoids clustering and naive Bayes classification," in 2012 8th International Conference on Wireless Communications, Networking and Mobile Computing, pp. 1-5, 2012.

[47] J. Song, H. Takakura, Y. Okabe, M. Eto, D. Inoue, & K. Nakao, "Statistical analysis of honeypot data and building of Kyoto 2006+ dataset for NIDS evaluation," in Proceedings of the First Workshop on Building Analysis Datasets and Gathering Experience Returns for Security, pp. 29-36, 2011.

[48] A. Sperotto, R. Sadre, F. Van Vliet, and A. Pras, "A labeled data set for flow-based intrusion detection," in International Workshop on IP Operations and Management, pp. 39-52, 2009.

[49] "UMASS",http://traces.cs.umass.edu/index.php/Network/Network.

[50] M. Nasr, A. Bahramali, and A. Houmansadr, "Deepcorr: Strong flow correlation attacks on Tor using deep learning," in Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, pp. 1962-1976, 2018.

[51] G. Bissias, B. N. Levine, M. Liberatore, and S. Prusty, "Forensic Identification of Anonymous Sources in OneSwarm," IEEE Transactions on Dependable and Secure Computing, vol. 14, no. 6, pp. 620-632, 2017.

[52] G. Creech and J. Hu, "Generation of a new IDS test dataset: Time to retire the KDD collection," in 2013 IEEE Wireless Communications and Networking Conference (WCNC), pp. 4487-4492, 2013.

[53] T. Mouttaqi, T. Rachidi, and N. Assem, "Re-evaluation of combined Markov-Bayes models for host intrusion detection on the ADFA dataset," in 2017 Intelligent Systems Conference (IntelliSys), pp. 1044-1052, 2017.

[54] Y. Shi and R. Eberhart, "A modified particle swarm optimizer," in 1998 IEEE international conference on evolutionary computation proceedings. IEEE world congress on computational intelligence (Cat. No. 98TH8360), pp. 69-73, 1998.

[55] A. Gharib, I. Sharafaldin, A. H. Lashkari ,and A. A. Ghorbani, "An evaluation framework for intrusion detection dataset," in 2016 International Conference on Information Science and Security (ICISS), pp. 1-6, 2016.

[56] M. Panda, A. Abraham, and M. R. Patra, "Discriminative multinomial naive bayes for network intrusion detection," in 2010 Sixth International Conference on Information Assurance and Security, pp. 5-10, 2010.

[57] M. A. Salama, H. F. Eid, R. A. Ramadan, A. Darwish, and A. E. Hassanien, "Hybrid intelligent intrusion detection scheme," in Soft computing in industrial applications, pp. 293-303, 2011.

[58] P. Gogoi, M. H. Bhuyan, D. Bhattacharyya, and J. K. Kalita, "Packet and flow based network intrusion dataset," in International Conference on Contemporary Computing, pp. 322-334, 2012.

[59] E. De La Hoz, A. Ortiz, J. Ortega, and E. De la Hoz, "Network anomaly classification by support vector classifiers ensemble and non-linear projection techniques," in International Conference on Hybrid Artificial Intelligence Systems, pp. 103-111, 2013.

[60] Z. Tan, A. Jamdagni, X. He, P. Nanda, R. P. Liu, and J. Hu, "Detection of denial-of-service attacks based on computer vision techniques," IEEE transactions on computers, vol. 64, no. 9, pp. 2519-2553, 2014.

[61] M. G. Raman, N. Somu, K. Kirthivasan, R. Liscano, and V. S. Sriram, "An efficient intrusion detection system based on hypergraph-Genetic algorithm for parameter optimization and feature selection in support vector machine," Knowledge-Based Systems, vol. 134, pp. 1-12, 2017.

[62] H. Huang, R. S. Khalid, and H. Yu, "Distributed machine learning on smart-gateway network towards real-time indoor data analytics," in Data Science and Big Data: An Environment of Computational Intelligence, pp. 231-263, 2017.

[63] R. Singh, H. Kumar, and R. Singla, "An intrusion detection system using network traffic profiling and online sequential extreme learning machine," Expert Systems with Applications, vol. 42, no. 22, pp. 8609-8624, 2015.

[64] M .Jabbar and R. Aluvalu, "RFAODE: A novel ensemble intrusion detection system," Procedia computer science, vol. 115, pp. 226-234, 2017.

[65] J. Bao, R. Li, Y. Liu, Y. Liu, and B. Shao, "Ionospheric anomaly detection to support the BDSBAS," IEEE Access, vol. 8, pp. 1691-1704, 2019.

[66] A. Bansal and S. Kaur, "Extreme gradient boosting based tuning for classification in intrusion detection systems," in International conference on advances in computing and data sciences, pp. 372-380, 2018.

[67] M .Catillo, M. Rak, and U. Villano, "Discovery of DoS attacks by the ZED-IDS anomaly detector," Journal of High Speed Networks, vol. 25, no. 4, pp. 349-365, 2019.