Journal of Soft Computing and Information Technology (JSCIT)
Babol Noshirvani University of Technology, Babol, Iran
Journal Homepage: jscit.nit.ac.ir
Volume 9, Number 3, Fall 2020, pp. 43-54
Received: 03/02/2019, Revised: 01/21/2020, Accepted: 03/06/2020

Precision Improvement of Intrusion Detection System using feature reduction based on Fuzzy Rough Set and Ensemble Classifiers

A. Nasabolhosseini[1], J. Hamidzadeh[2*]
1- Faculty of Computer Engineering and Information Technology, Sadjad University of Technology, No. 64 Jalal Al Ahmad St, Mashhad, Iran.
2*- Faculty of Computer Engineering and Information Technology, Sadjad University of Technology, No. 64 Jalal Al Ahmad St, Mashhad, Iran.
[1] a.nasab105@sadjad.ac.ir, [2*] j_hamidzadeh@sadjad.ac.ir

Corresponding author address: J. Hamidzadeh, Faculty of Computer Engineering and Information Technology, Sadjad University of Technology, Mashhad, Iran, Post Code: 91881 – 48848.

Abstract- In today's world, protecting data against intrusion through the Internet or network is necessary, and various tools have been proposed in this field. Intrusion Detection System has the task of identifying and detecting any unauthorized use of data by investigating network traffic. In these systems, many different methods, especially machine learning algorithms, is used. Various approaches have been proposed to improve these algorithms in the intrusion detection process. Some of these approaches include reducing false alarms, reducing dimensionality, reducing samples, ensemble methods, improving training and test dataset, applying multilevel methods, etc. Some of the ensemble methods proposed by researchers do not consider all aspects of the attack. Some other methods use accuracy metric, which in large and unbalanced data, this criterion makes the detection of low-number attacks difficult. One of the challenges in intrusion detection is the low precision of classifiers in identifying the type of network attacks. The purpose of this paper is to propose an intrusion detection system to improve the precision by using fuzzy rough set theory and weighted classifiers ensemble. In our proposed method, after reducing the features by the fuzzy rough set theory, the classifiers ensemble is used to improve the precision of attack detection. The precision of the proposed method in detecting intrusion behavior assaults was 98.93 on average. Also, on average, the detection rate of DoS, probe, R2L, U2R attacks and normal behavior was 96.85, 93.20, 91.31, 100% and 98.14 respectively. The results of the experiments show that the proposed method has more precision than other methods.

Keywords- Intrusion Detection System, Feature Reduction, Ensemble Classifiers, Precision Measure, Fuzzy Rough Set.

مجله علمی پژوهشی رایانش نرم و فناوری اطلاعات
دانشگاه صنعتی نوشیروانی بابل
صفحه مجله: jscit.nit.ac.ir
جلد ۹، شماره ۳، پائیز ۱۳۹۹ ، صفحه ۴۳-۵۴
دریافت: ۱۳۹۷/۱۲/۱۱، بازنگری: ۱۳۹۸/۱۱/۰۱، پذیرش: ۱۳۹۸/۱۲/۱۶

بهبود دقت سامانه تشخیص نفوذ به کمک کاهش‌ویژگی بر اساس مجموعه فازی ناهموار و ترکیب طبقه‌بندها

سیدعادل نسب‌الحسینی[۱]، جواد حمیدزاده*[۲]
۱- دانشکده مهندسی کامپیوتر و فناوری اطلاعات، دانشگاه صنعتی سجاد، مشهد، ایران.
*۲- دانشکده مهندسی کامپیوتر و فناوری اطلاعات، دانشگاه صنعتی سجاد، مشهد، ایران.
[1]a.nasab105@sadjad.ac.ir, [2*]j_hamidzadeh@sadjad.ac.ir

* نشانی نویسنده مسئول: جواد حمیدزاده، مشهد، خیابان جلال‌آل‌احمد۶۴، دانشگاه صنعتی سجاد، دانشکده مهندسی کامپیوتر و فناوری اطلاعات، کدپستی: ۹۱۸۸۱-۴۸۸۴۸

چکیده- در دنیای امروز، محافظت از داده‌ها در مقابل نفوذ از طریق اینترنت یا شبکه، امری ضروری است و ابزارهای مختلفی در این زمینه ارائه شده‌است. سامانه تشخیص نفوذ با بررسی ترافیک شبکه وظیفه شناسایی و تشخیص هرگونه استفاده غیرمجاز از داده‌ها را دارد. در این سامانه‌ها از روش‌های متعددی به ویژه الگوریتم‌های یادگیری ماشین بهره‌گیری می‌شود و رویکردهای مختلفی ازجمله کاهش هشدارهای غلط، کاهش ابعاد، کاهش نمونه‌ها، روش‌های ترکیبی، به‌سازی دادگان آموزشی و آزمون، به‌کارگیری روش‌های چند سطحی و غیره به‌منظور بهبود این الگوریتم‌ها در فرآیند تشخیص نفوذ ارائه‌شده است. برخی از رویکردهای ترکیبی ارائه‌شده توسط محققان، کلیه جنبه‌های حمله را موردنظر قرار نمی‌دهد. بعضی از روش‌ها نیز از معیار صحت استفاده می‌کنند که این معیار در داده‌های حجیم و نامتوازن باعث ضعف در تشخیص حمله‌های با تعداد نمونه‌های بسیار کم می‌گردد. یکی از چالش‌ها در تشخیص نفوذ، دقت پایین طبقه‌بندها در شناسایی نوع حملات شبکه است. هدف از این تحقیق، پیشنهاد یک سامانه برای بهبود دقت در تشخیص نفوذ با استفاده از نظریه مجموعه فازی ناهموار و ترکیب وزن‌دار طبقه‌بندها است. درروش پیشنهادی ما، پس از کاهش ویژگی‌ها توسط نظریه مجموعه فازی ناهموار، از ترکیب طبقه‌بندها برای بهبود دقت در تشخیص حملات استفاده شده است. دقت روش پیشنهادی در شناسایی رفتار حمله به طور میانگین به ۹۸/۹۳ رسید و همچنین به طور میانگین میزان شناسایی رفتارعادی ۹۸/۱۴، حمله‌های منع سرویس ۹۶/۸۵ و حمله‌های پویش ۹۳/۲۰ حمله‌های دسترسی از راه دور ۹۱/۳۱ و حمله‌های کاربر به ریشه ۱۰۰ به دست آمد. نتایج حاصل از انجام آزمایش‌ها نشان دهنده برتری روش پیشنهادی نسبت به سایر روش‌های موجود است.

واژه‌های کلیدی: سامانه تشخیص نفوذ، کاهش ویژگی، ترکیب طبقه‌بندها، معیار دقت، مجموعه فازی ناهموار.

۱- مقدمه

نظر به کاربرد روزافزون شبکه و اینترنت در سراسر جهان میزان آسیب‌پذیری سامانه‌های رایانه‌ای نیز رو به افزایش است. لذا به‌منظور کاهش مخاطرات امنیتی در حوزه فناوری اطلاعات، سامانه‌های تشخیص نفوذ[۱] و جلوگیری از نفوذ[۲] به کمک بشر می‌شتابند. سامانه تشخیص نفوذ یک سامانه دفاعی است که فعالیت‌های مخرب دریک شبکه رایانه‌ای را آشکار می‌کند. در واقع مهم‌ترین مسئله در این سامانه‌ها شناسایی فعالیت‌هایی است که احتمال می‌رود امنیت شبکه را به خطر بیندازد و یا کارهایی که منجر به شروع یک خراب‌کاری در شبکه یا رایانه شود؛ مانند شناسایی اولیه اطلاعات در مرحله جمع‌آوری داده به کمک پویش درگاه‌های[۳] رایانه توسط مهاجم که در نهایت منجر به آسیب رساندن به رایانه یا شبکه می‌شود. یک ویژگی مهم سامانه‌های تشخیص نفوذ توانایی آن‌ها در نمایش فعالیت‌های غیرعادی در شبکه است. به عنوان مثال پس از کشف تلاش کاربران برای ورود به محیط‌های غیرمجاز توسط سامانه تشخیص نفوذ، در اولین فرصت هشدارهای لازم به مدیر سایت[۴]

ارسال خواهد شد. علاوه بر آن یک سامانه تشخیص نفوذ این توانایی را دارد که بتواند حملات و یا نفوذهایی که از داخل و یا خارج از یک سازمان به شبکه آن انجام می‌شود را شناسایی نماید.

سه نوع سامانه تشخیص نفوذ در شبکه‌های رایانه‌ای مورداستفاده قرار می‌گیرد:

۱- سامانه‌های تشخیص نفوذ مبتنی بر میزبان[۵]

این نوع سامانه اطلاعات جمع‌آوری‌شده از یک میزبان شامل ساختار فایل و رفتار برنامه‌های خاص را تحلیل می‌کند [۹, ۱۰].

۲- سامانه‌تشخیص نفوذ مبتنی بر شبکه[۶] (متمرکز)

این سامانه داده‌های ترافیک شبکه را برای تشخیص رفتارهای مشکوک مانند حمله‌های منع سرویس[۷]، پویش درگاه‌ها و یا حتی حمله برای نفوذ به رایانه‌ها را تحلیل می‌کند بدین منظور جهت شناسایی نفوذ آدرس آی‌پی[۸] و سرآیند[۹] لایه انتقال همه بسته‌های داده توسط NIDS کنترل می‌شود [۱۰]. در این سامانه کل سربار تحلیل داده‌ها بر عهده ایستگاه پایه می‌باشد.

۳- سامانه تشخیص نفوذ توزیع‌شده[۱۰] که در آن از ترکیب دونوع قبلی –HIDS و NIDS- استفاده می‌شود و به‌نوعی بار پردازشی بر روی رایانه‌های درون شبکه توزیع می‌شود. این نوع سامانه انرژی زیادی در کل شبکه مصرف می‌کند.

به‌طور کلی سه روش مختلف برای تشخیص حملات در سامانه‌های تشخیص نفوذ وجود دارد:

۱- تشخیص مبتنی بر امضاء[۱۱] (در برخی از مقالات با عنوان تشخیص سوءاستفاده از آن نام‌برده شده است)

در این روش، حمله‌های شناخته‌شده –یعنی حمله‌هایی که تاکنون حداقل یک‌بار انجام‌شده‌اند- به‌راحتی از روی الگوی تعریف‌شده آن‌ها قابل‌شناسایی‌اند اما نقطه ضعف این روش عدم تشخیص حمله‌های ناشناخته یا همان حمله روز صفر[۱۲] است.

۲- تشخیص رفتارغیرعادی[۱۳] (در برخی از مقالات با عنوان تشخیص ناهنجاری از آن نام‌برده شده است)

در این روش الگوی رفتارهای غیرحمله برای سامانه تعریف می‌شود و رفتارهای غیر از آن به‌عنوان حمله شناسایی می‌شوند. نقطه‌ضعف این روش نیز در تولید حد بالایی از هشدارهای اشتباه[۱۴] است.

۳- روش‌های ترکیبی[۱۵] که درواقع از هر دو روش اول و دوم به‌صورت هم‌زمان استفاده می‌کند [۱۱]. درواقع ترکیب دو روش نتیجه بهتری در بردارد اما هزینه محاسباتی زیادی را به سامانه تحمیل می‌کند [۱۰].

با توجه به شرایط مختلف شبکه محلی موردنظر یکی از سه روش بالا مورداستفاده قرار می‌گیرد.

در سال‌های اخیر الگوریتم‌های زیادی مبتنی بر یادگیری ماشین به‌منظور شناسایی حملات استفاده شده است و هر یک از الگوریتم‌ها مدعی هستند که روش آنها نسبت به سایر روش‌ها برتری دارد. اما در دنیای واقعی برنامه‌ها، میزان صحت هر الگوریتم دارای نوسانات و تغییرات است به عنوان مثال در برخی از موارد ممکن است نتایج یک الگوریتم خیلی خوب یا مناسب نباشد و درجایی دیگر و شرایطی دیگر کاملا مناسب است که علت آن مربوط به محدودیت‌های ذاتی الگوریتم‌های یادگیری ماشین است و در واقع هیچ روشی در تمام جنبه‌ها از سایر روش‌ها بهتر نخواهد بود. از این رو به‌منظور به‌دست آوردن نتایج بهتر، از ترکیب چندین روش و الگوریتم، بهره‌گیری می‌شود.

با توجه به حجم بسیار بالا و غیرتکراری جریان داده‌ها در شبکه استفاده از تمامی ویژگی‌های داده باعث می‌شود که فرآیند تشخیص حملات زمان‌بر شده و کارایی سامانه کاهش یابد. روش‌های مختلفی به‌منظور کاهش زمان و حجم پردازش و بهبود کارایی این سامانه‌ها توسط محققان پیشنهادشده است. یکی از روش‌های پیشنهادی کاهش ابعاد بسته‌های اطلاعاتی است. با در نظر گرفتن ابعاد فضای ویژگی[۱۶] در دادگان[۱۷] NSL-KDD که منجر به اشغال منابع زیادی می‌شود در گام اول باید نسبت به کاهش ویژگی‌های موجود اقدام شود [۱۲].

در روش پیشنهادی، با حذف ویژگی‌های غیرضروری به کمک مجموعه فازی ناهموار نسبت به کاهش ابعاد دادگان اقدام نموده و پس از کاهش بار پردازشی، با ترکیب وزن‌دار چندین طبقه‌بند، دقت تشخیص را بهبود دادیم. ساختار ادامه مقاله به شرح ذیل است:

در بخش دوم کارهای مرتبط پیشین بررسی شده است. در بخش سوم روش پیشنهادی و قسمت‌های مختلف الگوریتم‌های آن تشریح شده است. نتایج آزمایش‌ها، تحلیل و پیش‌پردازش دادگان به‌کار رفته در روش پیشنهادی مقاله در بخش چهارم ارائه شده است. نحوه ارزیابی دربخش پنجم توضیح داده شده است و در بخش ششم نتیجه‌گیری و پیشنهادهایی برای کارهای آینده مطرح شده است.

۲- کارهای انجام‌شده

در این روزها بسیاری از محققان برای توسعه سامانه‌های تشخیص نفوذ تلاش می‌کنند. ازاین‌رو الگوریتم‌های فراوانی ازجمله داده‌کاوی، یادگیری ماشین، نظریه اطلاعات، محاسبات نرم، روش‌های آماری و غیره برای بهبود عملکرد IDS ارائه شده است. در اکثر روش‌ها به منظور کاهش زمان و بار محاسباتی، قبل از اجرای الگوریتم اصلی پیش‌پردازشی انجام می‌شود. کاهش ابعاد دادگان یکی از موثرترین روش‌ها به منظور بهبود اجرای الگوریتم‌ها است.

۲-۱- کاهش ویژگی

در مقاله [۱۳]، روشی با عنوان انتخاب نمونه حاشیه ترکیب[۱۸] ارائه شده است. در این مقاله نشان داده شده است که برای استفاده از دادگان بزرگ در الگوریتم‌های یادگیری ماشین، به پیش‌پردازش و حذف نمونه‌های غیرضروری نیاز است. در این مقاله به منظور کاهش بار سیستم از پردازش دادگان، از الگوریتم جنگل تصادفی استفاده شده است. روش پیشنهادی آن‌ها قادر بود تا دادگان بزرگ را با یک زمان پردازش معقول و تاثیر بسیار ناچیز در بازدهی طبقه‌بندی، کوچک‌سازی کند. نویسندگان در مقاله [۱۴]، یک روش انتخاب ویژگی را برای سیستم‌های تشخیص‌نفوذ با استفاده از دادگان NSL-KDD ارائه کردند. در مقاله [۱۵]، دادگان NSL-KDD را برای سیستم تشخیص نفوذ با روش مبتنی بر الگوریتم‌های دسته‌بندی تحلیل نمودند.

در مقاله [۱۶]، روش خوشه‌بندی K-means را که از رویکرد مبتنی بر امضاء تبعیت می‌کرد به‌منظور کاهش نرخ منفی غلط[۱۹]، در سیستم‌های تشخیص‌نفوذ ارائه نمودند.

مقاله [۱۷] تشخیص‌نفوذ از روی شناسایی رفتار غیرعادی را توسعه داده و روش جدیدی جهت محاسبه خارج از محدوده[۲۰] به همین نام (روش شناسایی خارج از محدوده) ارائه نموده است. نویسندگان این مقاله سعی کردند تا دقت مداوم شناسایی حملات کم تکرار را افزایش دهند.

در مقاله [۱۸] روشی را به نام OS-ELM[21] ارائه نمودند و مشکلات امنیتی زیادی ازجمله حجم دادگان ترافیک شبکه، انتخاب ویژگی، صحت پایین تشخیص و نرخ بالای هشدارهای غلط را جهت ارزیابی نتایج مدنظر قراردادند. درمقاله [۱۹] معیارهای فاصله و تشابه را در تشخیص رفتارهای غیرعادی شبکه موردبررسی قراردادند.

در مقاله [۲۰] الگوریتم کاهش ویژگی تعمیم یافته‌ای با استفاده از نظریه مجموعه فازی ناهموار ارائه شد که خصوصیات داده‌ها و نیازهای کاربر در کاربردهای واقعی را به‌صورت هم‌زمان در نظر می‌گرفت. نویسندگان در این مقاله نشان دادند که شاخص تعیین‌کننده کاهش ویژگی باید به هر دو موضوع داده‌ها و خواسته‌های کاربر مرتبط باشد.

در مقاله [۲۱] روشی با عنوان سیستم تشخیص نفوذ شبکه عصبی محرمانه (CNN-IDS)[۲۲] ارائه شد. در ابتدا ویژگی‌های اضافی و بی‌ربط از داده‌های ترافیک شبکه با استفاده از روش‌های کاهش ابعاد مختلف حذف شدند. نویسندگان از روش یادگیری با ناظر استفاده نمودند. آنها به منظور کاهش هزینه محاسبات حالت بردار ترافیک اصلی را به حالت تصویری تبدیل نمودند. آنها از دادگان KDD-CUP99 جهت ارزیابی بازدهی روش پیشنهادی در آزمایش‌های خود استفاده نمودند. نتایج آزمایش‌ها بهبود صحت و نرخ هشدارهای غلط را نسبت به الگوریتم‌های سنتی نشان داد. داده‌های ورودی مناسب برای روش آنها داده‌های دوبعدی بود.

۲-۲- ترکیب طبقه‌بندها

در مقاله [۲۲] یک روش ترکیبی دوسطحی برای تشخیص‌نفوذ ارائه شده است که به‌صورت بالقوه امکان شناسایی حمله‌های شناخته‌شده و ناشناخته را با نرخ پایینی از مثبت‌های غلط[۲۳] دارد. در مقاله [۲۳] یک سیستم تشخیص‌نفوذ چند سطحی برای تشخیص رفتارهای غیرعادی شبکه ارائه شده است. در مقاله [۲۴] الگویی از برنامه‌ریزی عدد صحیح[۲۴] موسوم به (IWIRI)[۲۵] ارائه شد. این روش می‌تواند هنگامی‌که داده‌های جدید اضافه می‌شود بدون نیاز به محاسبه مجدد کل دادگان، کمترین تعداد قوانین ویژگی را برای تصمیم‌گیری پیدا نموده و تجمیع وزن ویژگی‌ها و تناوب اشیا برای جستجوی قوانین بهینه در حالتی که اشیاء اضافه شود را محاسبه کند؛ الگوریتم پیشنهادی این مقاله نیازمند این بود که جدول داده‌ها کامل و بدون کسر مقادیر ویژگی‌های شرط[۲۶] باشد.

در مقاله [۲۵] یک سیستم جدید تشخیص‌نفوذ شبکه ترکیبی چند سطحی ارائه شد که از ترکیب الگوریتم‌های ماشین‌بردارپشتیبان[۲۷] و ماشین‌یادگیری‌بی‌نهایت[۲۸] جهت کاهش نرخ FA و بهبود صحت تشخیص بهره می‌برد.

نویسندگان مقاله به‌منظور ارزیابی میزان کارایی مدل خود از الگوریتم ELM پایه و الگوریتم خوشه‌بندی K-means اصلاح‌شده بر روی دادگان KDD cup 1999 استفاده کردند و نشان دادند که روش پیشنهادی آن‌ها به طرز رضایت‌بخشی بازدهی بالاتری نسبت به الگوریتم‌های SVM و ELM چند سطحی داشته است.

در مقاله [۲۶] روش جدیدی از ترکیب الگوریتم انتخاب ویژگی با استفاده از ماشین بردار پشتیبان چندکلاسه و نزدیک‌ترین‌همسایه K ام ارائه شد نویسندگان مقاله جهت بهبود عملکرد روش‌خود از الگوریتم بهینه‌سازی ازدحام ذرات افزایشی[۲۹] استفاده کردند. هدف آن‌ها بهبود صحت طبقه‌بندی سامانه تشخیص نفوذ بود و برای اجرای آزمایش‌ها از پنج زیرمجموعه تصادفی دادگان KDD Cup99 استفاده کردند. آن‌ها همچنین بر انتخاب ویژگی چند سطحی در بخش پیش‌پردازش دادگان تمرکز نمودند.

در مقاله [۲۷] روشی برای تشخیص نفوذ از ترکیب طبقه‌بندها همراه با الگوریتم خفاش ارائه شد. نویسندگان از زیرمجموعه‌های تصادفی ماشین یادگیری بی‌نهایت به‌عنوان طبقه‌بند پایه استفاده نمودند و به منظور بهبود نتایج از یک روش مبتنی بر الگوریتم خفاش جهت هرس ترکیب استفاده کردند. آن‌ها جهت بهبود طبقه‌بند در الگوریتم خفاش از یک تابع تناسب مبتنی بر صحت و تنوع استفاده کردند و

برای انجام آزمایش‌ها از سه دادگان عمومی KDD99، NSL-KDD و Kyoto استفاده‌کردند. نتایج آن‌ها نشان می‌داد که زیرمجموعه‌های تصادفی، قدرت و صحت شناسایی به‌وسیله الگوریتم ELM ارائه شده را بهبود داده است.

در مقاله [۶] سامانه تشخیص نفوذ شبکه مبتنی بر ترکیب طبقه‌بندها ارائه شد. هدف نویسندگان بهبود صحت طبقه‌بندی بود. آن‌ها نشان دادند که اگر میانگین مقدار بهره اطلاعاتی[۳۰] بین ویژگی‌هایی که در ترکیب قرارگرفته‌اند بین ۰/۰۴۵ تا ۰/۲۵ باشد آنگاه میزان صحت طبقه‌بندی ترکیب حداکثر ۰/۹ خواهد بود. آن‌ها سیستم تشخیص نفوذ شبکه مبتنی بر الگوریتم Adaboost ارائه نمودند و هدف آن‌ها یافتن راهی بود که به کمک آن قبل از پیاده‌سازی روش بتوانند میزان بهبود صحت تشخیص حملات را تخمین بزنند. آن‌ها از دادگان NSL-KDD برای اجرای آزمایش‌های خود استفاده کردند و مرز بین رفتار عادی با حمله Neptune را به کمک ترکیب طبقه بندها تعیین نمودند. روش آن‌ها درواقع جامع نبود و نمی‌توانست تخمینی از سایر حمله‌ها ارائه نماید و معیار موردنظر در این روش نیز صحت تشخیص بود.

به‌تازگی در مقاله [۷] روشی ارائه شد که در آن از الگوریتم‌های شبکه‌های عصبی، درخت تصمیم و رگرسیون محاسباتی جهت تشخیص رفتار غیرعادی بر روی شبکه‌های کامپیوتری استفاده می‌شد. نویسنده مقاله به‌منظور تقویت عملکرد روش، الگوریتم‌ها را با یکدیگر ترکیب نموده و از رویکرد رای اکثریت جهت افزایش صحت تشخیص طبقه‌بندی بر روی مجموعه‌های تصادفی از دادگان KDD Cup99 استفاده نمود؛ اما روش او صرفا توانایی طبقه‌بندی داده‌ها را در ۲ کلاس حمله و عادی داشت.

در مقاله [۲۸] از ترکیب طبقه‌بندها برای تشخیص نفوذ شبکه مبتنی بر رفتار غیرعادی در حالت با ناظر استفاده شد. تمرکز روش نویسندگان بر روی مشکلات ترکیب طبقه‌بندهای یادگیری ماشین در حالت‌های مختلف بود. آن‌ها برای بهبود نتایج از ۵ الگوریتم استفاده کرده و میزان عملکرد طبقه بندها و توانایی یادگیری آن‌ها را روی دادگان NB15 و UNSW مورد تحلیل و بررسی قراردادند. آن‌ها از معیارهای صحت و ROC جهت ارزیابی روش خود استفاده نمودند. آزمایش‌های آن‌ها در نرم‌افزار متلب ۲۰۱۵ اجرا شد و رفتار طبقه‌بندها بیشتر در حوزه شناسایی ناهنجاری در شبکه مورد مقایسه و ارزیابی قرار گرفت. طبق نتایج آنها الگوریتم‌های bagged tree و gentle boost بالاترین و الگوریتم rusboost کمترین نرخ صحت و ROC را به دست آوردند.

در مقاله [۵] یک روش یادگیری ترکیبی تطبیقی ارائه شد و از الگوریتم‌های درخت تصمیم، ماشین بردار پشتیبان، رگرسیون منطقی نزدیک ترین همسایه K ام، جنگل تصادفی و شبکه عصبی عمیق استفاده شد. آنها یک الگوریتم رای‌گیری انطباقی به نام درخت چندگانه ارائه نمودند و به منظور بهبود نتایج شناسایی حملات از روش رای‌گیری استفاده نمودند و دریافتند که کیفیت ویژگی‌های داده عامل مهمی برای تعیین اثر تشخیص است. آنها از دادگان NSL-KDD در آزمایش‌های خود استفاده نمودند و موفق شدند صحت الگوریتم نهایی رای‌گیری را به ۸۵/۲ برسانند.

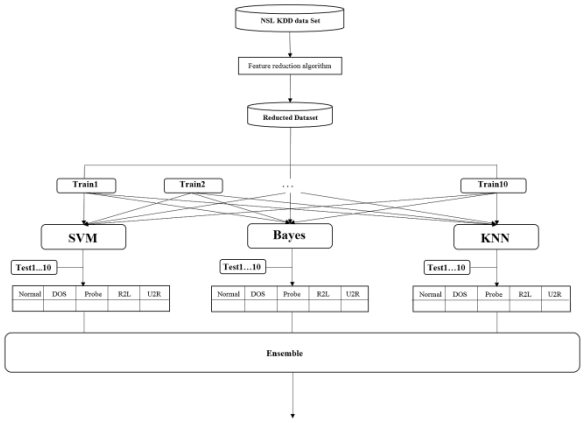
نویسندگان مقاله [۸] یک الگوی تشخیصی برای حملات شناخته-شده و ناشناخته از طریق روشی جدید و غیرپارامتری بیزی ارائه کردند. طرح آنها با عنوان (InBGG-Fs)[۳۱] به سادگی قابل تعمیم به فناوری اینترنت اشیاء و به‌ویژه مناسب جهت برنامه‌های تحت وب شهر هوشمند بود. در روش آنها یادگیری از روی الگوی فعالیت‌های عادی و حمله از طریق استنتاج مبتنی بر الگوریتم بیز بر روی مدل ترکیبی تعمیم‌یافته گاوسی با کران نامحدود انجام می‌شد. در روش آن‌ها به منظور خوشه‌بندی بهتر وزن ویژگی‌ها، پارامترهای مدل و تعداد خوشه‌ها بصورت هم‌زمان سنجیده می‌شد. آنها از انتخاب ویژگی در روش خود استفاده نموده و روش را توسط چند دادگان از جمله KDDCup'99 بررسی کردند. نتایج به دست آمده نشان از کارایی روش در تشخیص حملات مختلف داشت. یکی از معیارهای ارزیابی روش معیار صحت (Accuracy) بود که میزان صحت شناسایی حملات روش آن‌ها ۸۴/۰۶ درصد بود.

۲-۳- جمع‌بندی

در سال‌های اخیر الگوریتم‌های فراوانی مبتنی بر روش‌های تشخیص ناهنجاری و سوءاستفاده به‌منظور شناسایی حملات استفاده‌شده است. هریک از الگوریتم‌ها در شرایط خاصی، خروجی و نتیجه بهتری را نسبت به سایر روش‌ها در تشخیص نفوذ داشته است البته در دنیای واقعی میزان صحت هر الگوریتم دارای نوسانات و تغییراتی است که دلیل آن محدودیت‌های ذاتی الگوریتم‌های یادگیری ماشین است و هیچ روشی در تمامی جنبه‌ها از سایر روش‌ها بهتر عمل نکرده است پس کافیست به‌منظور به دست آوردن نتایج بهتر از ترکیب چندین الگوریتم و روش بهره‌گیری شود تا از برآیند نتایج آنها و همچنین نقاط قوت هر برنامه در شرایط خاص آن استفاده گردد. همچنین با توجه به کارهای انجام‌شده گذشته، استفاده از داده‌ها در آموزش و آزمایش طبقه بندها بدون پیش‌پردازش، نه‌تنها حجم و زمان پردازش را افزایش خواهد داد بلکه ممکن است باعث افت نتیجه خروجی در آن‌ها گردد. لذا با پیش‌پردازش مناسب می‌توان تنها از نمونه‌ها و ویژگی‌های موردنیاز در دادگان استفاده نمود و نتایج بهتر را در زمان کمتری به دست آورد [۲۹].

۳- مدل پیشنهادی

در شکل شماره ۱ طرح کلی الگوریتم پیشنهادی ارائه‌شده است. در اجرای این پروژه ابتدا دادگان ورودی توسط الگوریتم کاهش ویژگی به یک مجموعه داده با صفات کمتر تبدیل شد. سپس دادگان جدید جهت طبقه‌بندی به پنج طبقه‌بند از سه نوع مختلف داده شد. در مدل پیشنهادی از ترکیب پنج طبقه‌بند Bayes، SVM با هسته هرمیت[۳۰] ، SVM(RBF)، 3-NN و 7-NN استفاده شده است. میزان وزن هر الگوریتم بر اساس نتایج شناسایی در مراحل آموزش محاسبه شد. توضیح اینکه در شکل ارائه‌شده به دلیل کمبود فضا فقط سه نوع الگوریتم نمایش داده شده است و امکان نمایش پنج طبقه‌بند وجود نداشت. به منظور تست کامل الگوریتم‌ها توسط دادگان، آموزش طبقه‌بندها به روش 10-fold cross validation انجام شد.



شکل ۱: ساختار کلی الگوریتم پیشنهادی

۳-۱- کاهش ابعاد

پژوهش‌ها در حوزه کاهش ویژگی‌ها نشان داده است که انتخاب مجموعه‌ای کمتر از ویژگی‌های اولیه ضمن کاهش بار پردازشی و افزایش سرعت اجرای برنامه‌ها، سبب بهبود نتایج در الگوریتم‌های یادگیری ماشین می‌شود [۲۱].

نظریه مجموعه ناهموار[۳۲] در سال ۱۹۸۰ توسط آقای پاولاک پیشنهاد شد [۳۱]. این دیدگاه به‌نوعی توسعه مفهوم نظریه مجموعه‌ها برای مطالعه بر روی سامانه‌های هوشمندی است که در آن‌ها عدم قطعیت و ابهام وجود دارد [۳۲]. یکی از مهم‌ترین ویژگی‌های این نظریه یافتن مجموعه کمینه از داده‌ها است که برای طبقه‌بندی مفید است (مانند کاهش ابعاد و تعداد اطلاعات). روش‌های مبتنی بر این نظریه پس از تحلیل اطلاعات پنهان در داده‌ها، اطلاعات غیرمرتبط از مجموعه دادگان را حذف می‌نماید. اطلاعات ورودی نظریه فازی ناهموار به‌صورت جدول‌های ویژگی و مقدار در اختیار است.

اگر جدول T را به‌صورت $T(U,A,C,D)$ در نظر بگیریم به‌گونه‌ای که: U مجموعه اشیا، A ویژگی‌ها، C ویژگی‌های شرطی و D ویژگی‌های تصمیم‌گیری باشند و $C,D \subseteq A$ برای هر مجموعه ویژگی P زیرمجموعه A رابطه تفکیک‌ناپذیری به‌صورت زیر تعریف می‌شود:

$$IND(P) = \{(x,y) \in U \times U : \forall a \in P, a(x) = a(y)\} \quad (۱)$$

حال اگر $P \subseteq C$ و $X \subseteq U$ باشند تقریب بالا و پایین X با توجه به P مساوی است با:

$$\underline{P}X = \{ x \in U : [x]_{IND(P)} \subseteq X \} \quad (۲)$$

$$\overline{P}X = \{ x \in U : [x]_{IND(P)} \cap X \neq \emptyset \} \quad (۳)$$

درجایی که

$$[x]_{IND(P)} = \{ y \in U : a(y) = a(x) , \forall a \in P \} \quad (۴)$$

کلاس هم ارزی x در $IND(P)$ $U \mid$ باشد.

منطقه مثبت P از D مجموعه‌ای از اشیاء مجموعه جهانی U است که می‌توانند به یک کلاس خاص از $U \mid IND(P)$ تعلق داشته و ویژگی‌هایی از P را در خود داشته باشند. مطابق فرمول ذیل به دست می‌آید.

$$POS_P(D) = \cup_{X \in U \mid IND(D)} \underline{P}X \quad (۵)$$

و مقدار وابستگی D روی P به‌صورت زیر محاسبه می‌شود:

$$\gamma_p(D) = \frac{|POS_P(D)|}{|U|} \quad (۶)$$

ویژگی $a \in C$ در مجموعه P غیرضروری گوییم هرگاه

$$\gamma_p(D) = \gamma_{p-a}(D) \quad (۷)$$

در غیر این صورت این ویژگی با توجه به D روی مجموعه P ضروری است؛ و یک مجموعه دلخواه $B \subseteq C$ ضروری است اگر تمام ویژگی‌های آن ضروری باشد [۳۳].

از تعاریف بالا یک مجموعه کمینه از ویژگی‌ها به‌صورت ذیل تعریف می‌شود:

یک مجموعه از ویژگی‌ها $R \subseteq C$ مجموعه کمینه C خواهد بود اگر R مستقل بوده و $POS_R(D) = POS_C(D)$ به‌عبارت‌دیگر، مجموعه کمینه مجموعه‌ای از ویژگی‌هایی است که بخش‌های مختلف ایجادشده توسط C را پوشش دهد.

۳-۲- الگوریتم کاهش ویژگی

فرض کنیم سامانه اطلاعاتی به صورت IS = (U, W, A, V, F) تعریف‌شده است [۳۴]. U و W مجموعه‌های محدود عمومی باشند. A ویژگی‌ها، V کلاس‌ها و F یک تابع از U به مجموعه توانی از W باشد.

گام اول: خواندن ویژگی A از U و W

گام دوم: محاسبه IND(B)

گام سوم: محاسبه IND(B) * (D_k) برای هر $D_k \in U/D$

گام چهارم: محاسبه ماتریس C_{ij} برای پارامترهای تصمیم‌گیری
گام پنجم: تشکیل ویژگی‌های کلیدی با استفاده از هسته
گام ششم: حذف آیتم‌هایی که مقدار C_{ij} آن‌ها مساوی NULL است.
یا K بدون هم‌پوشانی غیر صفر با هسته
گام هفتم: تعیین کردن f_D (IS)
گام هشتم: محاسبه g_D (IS) با استفاده از f_D (IS)
گام نهم: یافتن مجموعه کمینه ویژگی‌ها با استفاده از g > 0.6
گام دهم: تعیین مجموعه کمینه ویژگی‌ها برای حمله نوع i

۳-۳- طبقه‌بندهای مورداستفاده

در روش پیشنهادی ما چندین نوع متفاوت از سه طبقه‌بند بیز، ماشین بردار پشتیبان و نزدیک‌ترین همسایه K ام مورد استفاده قرار گرفتند و نتایج بهتر برای انتخاب بهترین نوع مدنظر قرار گرفت. طبقه‌بند ماشین بردار پشتیبان برای انواع مختلف داده طراحی شده است اما یکی از مشکلات آن در آزمایش‌های انجام شده ما سرعت کم پاسخ‌دهی الگوریتم مذکور بود که وقت زیادی را در آزمایش‌ها می‌گرفت. در اجرای آزمایش‌ها پس از استفاده از چندین الگوریتم ماشین بردار پشتیبان از نوع هسته RBF مانند Fitc-Svm، Svm train و LIBSvm از نوع خاصی از هسته طبقه‌بند ماشین بردار پشتیبان با نام هسته Hermite–Chebyshev جهت افزایش سرعت اجرای الگوریتم طبقه‌بندی استفاده شد [۳۰]. این نوع الگوریتم با توجه به رابطه زیر تعداد نقاط بردار پشتیبان را کاهش داده و نسبت به روش‌های قبلی سریع‌تر عمل می‌کند.

$$k\,(x,z) = \prod_{j=1}^{d} \sum_{i=0}^{n} He_i(x_j) He_i(z_j) \qquad (۸)$$

که در آن $He_n(x)$ چندجمله‌ای متعامد هرمیت[۳۳] است که به روش زیر تعیین می‌شود:

$$He_n(x) = (-1)^n e^{\frac{x^2}{2}} \frac{d^n}{dx^n} e^{-\frac{x^2}{2}}. \qquad (۹)$$

۴-۳- ترکیب طبقه‌بندها

الگوریتم‌های مختلفی در حوزه یادگیری ماشین برای سامانه‌های تشخیص نفوذ ارائه شده‌است. در این پروژه خروجی سامانه شامل ۲ کلاس (رفتار عادی و حمله) یا ۵ کلاس (رفتار عادی، DOS، Probe، U2R و R2L) است. با بررسی کلی می‌توان دریافت که هر الگوریتم در شناسایی برخی از انواع حمله‌ها دقت بیشتر و در برخی دیگر دقت کمتری دارد. یک راهکار برای رسیدن به‌دقت بالاتر به‌کارگیری روش‌های ترکیبی[۳۴] است. روش‌هایی که در آن‌ها k طبقه‌بند یاد گرفته‌شده باهم ترکیب می‌شوند تا الگوی قوی‌تری را ایجاد کنند. درنتیجه دقت مدل ترکیبی از هرکدام از مدل‌های اولیه بیشتر است.

$$f_{com} = Vote(f_1, f_2, \ldots, f_k) \qquad (۱۰)$$

طبقه‌بندها را می‌توان به دو روش ادغام و انتخاب با یکدیگر ترکیب نمود. در حالت ادغام پس از آموزش و انجام آزمون هر یک از طبقه‌بندها، با وزن‌دهی به آن‌ها میزان تأثیر آن طبقه‌بند را در تصمیم‌گیری نهایی مشخص می‌کنیم. در حالت انتخاب از برآیند خروجی یا همان رأی اکثریت چند طبقه‌بند جهت تصمیم‌گیری استفاده می‌کنیم. در روش پیشنهادی این مقاله نخست میزان دقت هریک از طبقه‌بندها را به‌صورت مجزا محاسبه نموده و جهت رأی‌گیری نهایی ترکیب، به هر طبقه‌بند یک وزن اختصاص می‌دهیم بر این اساس ترکیب طبقه‌بندهای مورداستفاده در سامانه گروهی از نوع قابل‌آموزش[۳۵] است [۳۵]. الگوریتم‌های مورد استفاده در روش پیشنهادی شامل SVM، KNN و Bayes هستند. در این مقاله از ترکیب در سطح داده و ترکیب در سطح طبقه‌بندی استفاده‌شده است [۳۵].

۴- دادگان

با توجه به پیشرفت‌های روزافزون فناوری اطلاعات، حجم پردازش و تحلیل داده‌ها افزایش یافته‌است. الگوریتم‌های یادگیری ماشین مانند ماشین‌های بردارپشتیبان، نزدیک‌ترین همسایه K ام[۳۶]، شبکه‌های عصبی مصنوعی و غیره راه‌حل مؤثری برای سازمان‌دهی و استخراج داده‌های مفید از داده‌های موجود فراهم نموده‌اند. روش‌های موجود قادر به کار کردن با حجم وسیع داده‌ها در زمان پردازشی معقول نیستند [۱۳].

در سامانه تشخیص نفوذ دادگان KDD cup 99 به‌عنوان اولین دادگان توسط بسیاری از محققان مورداستفاده قرارگرفت. [۳۶] این دادگان متشکل از ۷ هفته آموزش[۳۷] و دو هفته آزمایش[۳۸] داده‌های ترافیک شبکه به کمک نرم‌افزار Tcpdump data بوده و درمجموع دارای ۷ میلیون رکورد است [۳۷]. اما حجم بسیار بالای این دادگان باعث شد تا به منظور کاهش زمان و بارپردازشی الگوریتم‌ها، دادگانی با حجم کمتر از روی آن تحت عنوان NSL-KDD ایجاد نمایند. در اجرای روش پیشنهادی این مقاله از دادگان NSL-KDD[۳۹] [۳۸] استفاده شد. تعداد نمونه‌های این دادگان ۱۲۵۹۷۳ رکورد است. با توجه به جداول شماره ۱، ۲ و ۳، به دلیل وجود ۴۱ ویژگی و همچنین ۴۰ کلاس مختلف در ابتدا دادگان می‌بایست مورد پیش‌پردازش[۴۰] قرار می‌گرفت. در جداول شماره ۲ و ۳ لیست ویژگی‌ها و کلاس‌های دادگان مورداستفاده نشان داده‌شده است.

۱-۴- پیش‌پردازش

مطابق با جداول شماره ۱ و ۲ تعداد کلاس‌ها در این دادگان ۴۰ عدد است که یک کلاس رفتار عادی یا همان رفتار غیرحمله و ۳۹

کلاس دیگر مربوط به حملات است. در سامانه‌های تشخیص نفوذ حملات به چهار دسته‌بندی تقسیم می‌شوند. این دسته‌بندی در جدول شماره ۲ نمایش داده‌شده است.

جدول۱: لیست کلاس‌ها در دادگان NSL-KDD

ردیف	نام کلاس	تعداد	نوع کلاس
۱	Normal	۱	رفتار عادی
۲	Neptune, warezmaster, snmpgetattack, processtable, guess_passwd, satan, mscan, saint, smurf, apache2, buffer_overflow, back, pod, httptunnel, nmap, ipsweep, snmpguess, udpstorm, mailbomb, portsweep, multihop, sendmail, loadmodule, xterm, worm, teardrop, rootkit, xlock, xsnoop, sqlattack, ftp_write, imap, land, phf, perl, warezclient, named, ps, ftp_write	۳۹	حمله

جدول ۲: لیست دسته‌بندی نوع حملات در دادگان NSL-KDD

کلاس حمله	نوع حمله	تعداد
DoS	Back, Land, Neptune, Pod, Smurf, Teardrop, Apache2, Udpstorm, Processtable, Worm	۱۰
Probe	Satan, Ipsweep, Nmap, Portsweep, Mscan, Saint	۶
R2L	Guess_Password, Ftp_write, Imap, Phf, Multihop, Warezmaster, Warezclient, Spy, Xlock, Xsnoop, Snmpguess, Snmpgetattack, Httptunnel, Sendmail, Named, ftp_write	۱۶
U2R	Buffer_overflow, Loadmodule, Rootkit, Perl, Sqlattack, Xterm, Ps	۷

مطابق با جداول شماره ۱ و ۳ با توجه به تعداد ۴۱ ویژگی به‌منظور پایین‌آوردن بار پردازشی برنامه، ویژگی‌ها را به کمک ترکیب الگوریتم آنتروپی و مجموعه فازی ناهموار کاهش دادیم. برای این منظور دو روش انتخاب ویژگی[۴۱] و استخراج ویژگی[۴۲] وجود دارد. درروش پیشنهادی ما انتخاب ویژگی به کمک مجموعه فازی ناهموار موردتوجه قرار گرفت تا با حذف ویژگی‌هایی که تأثیر چندانی در تعیین کلاس حملات ندارند دادگان مناسب‌تری مورداستفاده قرار-گیرد. از سوی دیگر با تبدیل دادگان به دو نوع ۲ کلاسه -شامل حمله[۴۳] و عدم حمله[۴۴]- و ۵ کلاسه -شامل عدم حمله و ۴ کلاس حمله منع سرویس[۴۵]، حمله پویش[۴۶]، حمله کاربر به ریشه[۴۷] و حمله دسترسی از راه دور[۴۸]- دو دادگان ایجاد نمودیم تا بتوانیم روش پیشنهادی را هم از لحاظ شناسایی و عدم شناسایی نفوذ و هم از لحاظ شناسایی نوع حملات بررسی نماییم.

جدول ۳: لیست ویژگی‌های دادگان NSL-KDD

ردیف	نام ویژگی	نوع / مقادیر ویژگی
۱	duration	real
۲	protocol_type	'tcp','udp', 'icmp'
۳	service	'aol', 'auth', 'bgp', 'courier', 'csnet_ns', 'ctf', 'daytime', 'discard', 'domain', 'domain_u', 'echo', 'eco_i', 'ecr_i', 'efs', 'exec', 'finger', 'ftp', 'ftp_data', 'gopher', 'harvest', 'hostnames', 'http', 'http_2784', 'http_443', 'http_8001', 'imap4', 'IRC', 'iso_tsap', 'klogin', 'kshell', 'ldap', 'link', 'login', 'mtp', 'name', 'netbios_dgm', 'netbios_ns', 'netbios_ssn', 'netstat', 'nnsp', 'nntp', 'ntp_u', 'other', 'pm_dump', 'pop_2', 'pop_3', 'printer', 'private', 'red_i', 'remote_job', 'rje', 'shell', 'smtp', 'sql_net', 'ssh', 'sunrpc', 'supdup', 'systat', 'telnet', 'tftp_u', 'tim_i', 'time', 'urh_i', 'urp_i', 'uucp', 'uucp_path', 'vmnet', 'whois', 'X11', 'Z39_50
۴	flag	'OTH', 'REJ', 'RSTO', 'RSTOS0', 'RSTR', 'S0', 'S1', 'S2', 'S3', 'SF', 'SH
۵	src_bytes	real
۶	dst_bytes	real
۷	land	'0' ,'1'
۸	wrong_fragment	real
۹	urgent	real
۱۰	hot	real
۱۱	num_failed_logins	Real
۱۲	logged_in	'0' ,'1'
۱۳	num_compromised	real
۱۴	root_shell	real
۱۵	su_attempted	real
۱۶	num_root	real
۱۷	num_file_creations	real
۱۸	num_shells	real
۱۹	num_access_files	real
۲۰	num_outbound_cmds	real
۲۱	is_host_login	'0' ,'1'
۲۲	is_guest_login	'0' ,'1'
۲۳	count	real
۲۴	srv_count	real
۲۵	serror_rate	real
۲۶	srv_serror_rate	real
۲۷	rerror_rate	real
۲۸	srv_rerror_rate	real
۲۹	same_srv_rate	real
۳۰	diff_srv_rate	real
۳۱	srv_diff_host_rate	real
۳۲	dst_host_count	real
۳۳	dst_host_srv_count	real
۳۴	dst_host_same_srv_rate	real
۳۵	dst_host_diff_srv_rate	real
۳۶	dst_host_same_src_port_rate	real
۳۷	dst_host_srv_diff_host_rate	real
۳۸	dst_host_serror_rate	real
۳۹	dst_host_srv_serror_rate	real
۴۰	dst_host_rerror_rate	real
۴۱	dst_host_srv_rerror_rate	real

به‌منظور کاهش ویژگی از دو روش آنتروپی[۴۹] و آنتروپی‌فازی استفاده شد -که نتایج مشابهی داشتند- و تعداد ۳۲ ویژگی که در تعیین کلاس رفتار تأثیری نداشتند حذف شدند.

با توجه به حجم بالای دادگان برای اجرای الگوریتم از روش Ivote Bagging [۳۹] دادگان را به قسمت‌های ۱۰۰۰۰ نمونه‌ای تقسیم نموده (آخرین قسمت ۵۹۷۳ رکورد) و به ترتیب به‌عنوان داده‌های ورودی به الگوریتم کاهش ویژگی دادیم. همچنین برای اطمینان از صحت عملکرد پس از اتمام کار بازه‌های بینابین هم به ورودی الگوریتم داده شد مثلا از داده شماره ۳۵۰۰۰ تا ۴۵۰۰۰ و درنهایت با حذف ویژگی‌های بی‌اهمیت از دادگان موجود دادگان جدیدی با تعداد ۷ ویژگی ایجاد شد. در تعداد کل رکوردها تغییری ایجاد نشد و ۱۲۵۹۷۳ رکورد جهت آموزش الگوریتم‌ها مورداستفاده قرار گرفت. پس از اجرای الگوریتم آنتروپی فازی بر روی دادگان NSL-KDD، در حالت ۲ کلاسی ویژگی‌های ۳۳,۳۲,۲۳,۵,۴,۳ و در حالت ۵ کلاسی صفات ۳۵,۳۳,۲۳,۵,۴,۳ به‌عنوان ویژگی‌های تعیین‌کننده کلاس نمونه انتخاب شدند. از تجمیع صفات به دست آمده در دو حالت، دادگانی با ۷ ویژگی از ۴۱ ویژگی موجود به دست آمد که در جدول ۴ ذکر شده است.

جدول ۴: لیست ویژگی‌های انتخاب‌شده توسط‌الگوریتم آنتروپی‌فازی

تعداد کلاس	شماره ویژگی‌ها
دو کلاسی	۳,۴,۵,۲۳,۳۲,۳۳
پنج کلاسی	۳,۴,۵,۲۳,۳۳,۳۵
ویژگی‌های نهایی منتخب	۳,۴,۵,۲۳,۳۲,۳۳,۳۵

پس از آماده سازی دادگان به منظور آموزش و ارزیابی طبقه‌بندهای انتخاب‌شده به روش 10-fold در ۱۰ مرحله مختلف هر بار یک‌دهم دادگان جهت آزمون جدا شد و نه‌دهم دیگر جهت آموزش طبقه‌بندها مورد استفاده قرار گرفت که میانگین نتایج اجرای الگوریتم در جدول شماره ۵ قابل مشاهده است.

جدول ۵: میانگین نتایج اجرای الگوریتم 10-fold برالگوریتم پیشنهادی

رفتار	عادی	DoS	Probe	R2L	U2R
میانگین نتایج روش پیشنهادی	۰/۹۷۹	۰/۹۶۵	۰/۹۲۸	۰/۹۱۰	۰/۵۰۲

۵- نتایج آزمایش‌ها

در این بخش نتایج آزمایش‌های انجام شده در جداول نشان داده شده است. آزمایش‌ها در حالت یادگیری با ناظر در نرم‌افزار متلب ۲۰۱۸ بر روی یک سرور با ۱۶ هسته پردازشگر و مقدار ۱۰۰ گیگابایت رم و همچنین سیستم‌عامل ویندوز سرور ۲۰۱۲ انجام شد؛ که نتایج ارزیابی آن بر اساس میزان دقت، نرخ تشخیص و هشدارهای اشتباه در جداول ارائه‌شده است.

۵-۱- ارزیابی

در جدول شماره ۶ ماتریس درهم‌ریختگی ارائه شده‌است که درآن چهار جزء اصلی تعیین‌کننده جهت ارزیابی معیارهای مختلف، به‌منظور ارزیابی سامانه‌های تشخیص نفوذ نشان داده شده‌اند. در روش پیشنهادی آزمایش‌ها را با سه معیار مختلف مورد بررسی قرار دادیم؛ اما با توجه به اینکه هدف اصلی مقاله بهبود دقت در سامانه‌های تشخیص نفوذ است، معیار دقت[۵۰] بیشتر موردتوجه قرار گرفته است.

جدول ۶: ماتریس درهم‌ریختگی برای سامانه تشخیص نفوذ [۱]

		کلاس‌های تخمینی	
		حمله	عادی
کلاس‌های واقعی	حمله	TP	FN
	عادی	FP	TN

TP: حمله توسط طبقه‌بند به‌درستی شناسایی‌شده است.

FP: رفتار عادی توسط طبقه‌بند به‌اشتباه حمله شناسایی شده‌است.

FN: حمله توسط طبقه‌بند به‌اشتباه رفتار عادی شناسایی شده‌است.

TN: رفتار عادی توسط طبقه‌بند به‌درستی شناسایی شده‌است.

معیار دقت (Precision):

از حاصل تقسیم تشخیص‌های صحیح حمله به کل رفتارهایی که به‌عنوان حمله شناسایی شده‌اند به دست می‌آید.

$$Precision= TP/(TP+FP) \quad (11)$$

معیار نرخ تشخیص (Detection Rate):

از حاصل تقسیم حمله‌های صحیح تشخیص داده‌شده به کل حمله‌ها به دست می‌آید.

$$DR = TP/(TP+FN) \quad (12)$$

معیار نرخ هشدارهای غلط (False Alarm Rate):

از حاصل تقسیم رفتارهای عادی که به اشتباه حمله تشخیص داده‌شده‌اند به کل رفتارهای عادی شبکه به‌دست می‌آید.

$$FAR = FP/(TN+FP) \quad (13)$$

در آزمایش‌های انجام‌شده، مشاهده شد که الگوریتم SVM در بهبود معیار دقت و همچنین کاهش FA نسبت به دو الگوریتم Bayes و KNN بهتر عمل کرده است؛ اما سرعت عملکرد این الگوریتم به‌ویژه در شناسایی نوع حملات نسبت به دو الگوریتم دیگر بسیار کندتر بوده و همچنین در خصوص نرخ تشخیص، طبقه‌بندهای Bayes و KNN نسبت به طبقه‌بند SVM قوی‌تر عمل کردند.

در حالت به‌کارگیری دادگان ۵ کلاسی، شرایط متفاوت است. در جدول شماره ۷ تعداد نمونه‌های موجود از هر یک از کلاس‌ها در حالت ۵ کلاسی نشان داده‌شده است.

جدول ۷: تعداد نمونه‌های موجود از هرکدام از کلاس‌ها در دادگان

کلاس داده	Normal	DOS	Probe	R2L	U2R
تعداد	۶۷۳۴۳	۴۵۹۲۷	۱۱۶۵۶	۹۹۵	۵۲

مطابق با جدول شماره ۷ با توجه به تعداد بسیار کم نمونه‌های دو کلاس R2L و U2R، طبقه‌بندها این دو کلاس را با درصد کمتری شناسایی می‌کردند. در جدول شماره ۹ نتایج آزمایش‌های انجام‌شده بر روی دادگان نشان داده‌شده است.

همان‌گونه که از جدول شماره ۹ قابل استنباط است طبقه‌بند ماشین بردار پشتیبان در حالت ۲ کلاسی نسبت به سایر طبقه‌بندها عملکرد بهتری داشته است و با توجه به وزن‌دهی طبقه‌بندها نتایج طبقه‌بند مذکور در طبقه‌بند ترکیبی هم مشاهده می‌گردد. همچنین با توجه به جدول ۱۰ در حالت ۵ کلاسی طبقه‌بند KNN در معیار دقت نسبت به سایر طبقه‌بندها بهتر عمل نموده است که نتایج آن در طبقه‌بند ترکیبی (روش پیشنهادی) نیز مشاهده می‌گردد. با بررسی نتایج مدل پیشنهادی در نرم‌افزار متلب مشاهده شد که میزان دقت سامانه در حالت دوکلاسی به‌طور میانگین ۹۹/۹۳۶ درصد و در حالت ۵ کلاسی به‌طور میانگین در شناسایی رفتار نرمال ۹۹/۶۷۲ درصد و حمله DOS حدود ۹۹/۳۹۴ درصد و حمله Probe حدود ۹۶/۸۶۷ درصد و حمله‌های R2L و U2R به ترتیب ۸۱/۴۳۷ و ۶۰ درصد بود.

طبق اطلاعات جداول ۷ و۱۰ با توجه به تعداد کم نمونه‌های حمله‌های U2R و R2L نسبت به کل نمونه‌ها، طبقه‌بندها در شناسایی این دو نوع حمله ضعیف عمل‌کردند و می‌توان نتیجه‌گرفت که آموزش طبقه‌بندها برای شناسایی دو حمله مذکور کافی نبوده‌است لذا به منظور بهبود این موضوع مجددا الگوریتم کاهش ویژگی را فقط برای نمونه‌های این دو نوع حمله در دادگان اولیه(شامل ۴۱ ویژگی) به‌صورت مجزا تکرارکردیم که در نتیجه دو ویژگی دیگر نیز به مجموع ویژگی‌های مهم افزوده‌شد و درنهایت یک دادگان با ۹ ویژگی مطابق جدول ۸ ایجاد شد.

جدول ۸: لیست ویژگی‌های انتخاب‌شده توسط الگوریتم آنتروپی فازی برای دو حمله R2L و U2R

تعداد کلاس	شماره ویژگی‌ها
حمله‌های R2L و U2R	۶,۳,۲
ویژگی‌های نهایی منتخب	۳۵,۳۳,۳۲,۲۳,۶,۵,۴,۳,۲

جدول ۹: نتایج میزان دقت، نرخ‌تشخیص و نرخ هشدارهای غلط الگوریتم‌ها پس از کاهش ویژگی با دادگان ۲ کلاسی

الگوریتم‌های طبقه‌بندی	ردیف	معیار ارزیابی		
		Precision	DR	FAR
SVM	1	99.865%	75.85	0.089
	2	99.977	75.163	0.014
	3	99.932	75.849	0.044
	4	99.955	76.424	0.029
	5	99.911	76.725	0.059
	6	99.977	75.844	0.014
	7	99.932	75.869	0.044
	8	99.944	77.01	0.023
	9	99.890	76.853	0.018
	10	99.974	75.680	0.043
Bayes	1	96.34%	99.9%	0.999%
	2	96.86	99.9	1
	3	96.26	99.9	1
	4	96.68	99.9	0.999
	5	96.32	99.9	1
	6	96.29	99.9	1
	7	96.68	99.97	0.003
	8	96.36	99.8	0.999
	9	96.92	99.8	1
	10	95.97	99.48	0.001
KNN	1	99.543%	99.627%	0.404%
	2	99.222	99.812	0.686
	3	99.486	99.691	0.443
	4	99.521	99.555	0.415
	5	99.471	99.658	0.459
	6	99.503	99.657	0.428
	7	99.425	99.576	0.507
	8	99.265	99.554	0.636
	9	99.422	99.608	0.505
	10	99.536	99.673	0.398
ترکیب (روش پیشنهادی)	1	99.865%	75.85	0.089
	2	99.977	75.163	0.014
	3	99.932	75.849	0.044
	4	99.955	76.424	0.029
	5	99.911	76.725	0.059
	6	99.977	75.844	0.014
	7	99.932	75.869	0.044
	8	99.944	77.01	0.023
	9	99.890	76.853	0.018
	10	99.974	75.680	0.043

با مشاهده جدول ۱۰ می‌توان دریافت که شناسایی حملات R2L و U2R که تعداد نمونه‌های آنها در دادگان نسبت به سایر حملات بسیار کم‌تر بوده است، نتایج ضعیف‌تری داشته است. طبقه‌بند KNN نسبت به دو طبقه‌بند دیگر نتایج بهتری داشته است. لذا به منظور بهبود عملکرد این طبقه‌بند در شناسایی دو حمله مذکور -که درنهایت منجر به بهبود نتایج ترکیب خواهد شد- ضمن استفاده از دادگان جدید با ۹ ویژگی تعداد نمونه‌های آموزش و آزمون و همچنین تعداد همسایه‌های (عدد K در الگوریتم KNN) را تغییر دادیم. پس از تکرار آزمایش‌ها با دادگان ۹ ویژگی نتایج بهینه روی الگوریتم KNN با مقادیر مختلف K به دست آمد که پس از اعمال

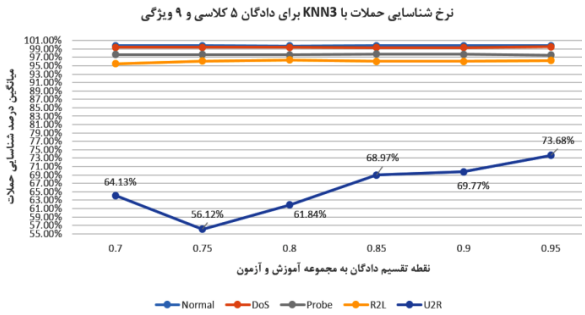
تغییرات بر روی میزان تقسیم داده‌های آموزش و آزمون نتایج آن در جداول ۱۱ و ۱۲ قابل مشاهده است.

جدول ۱۰: نتایج میزان شناسایی کلاس‌های مختلف حمله توسط طبقه‌بندها بر اساس معیار دقت در حالت ۵ کلاسی

Normal	DOS	Probe	R2L	U2R	کلاس / ردیف	طبقه‌بند
86.58	94.95	64.44	50	50	1	SVM
86.81	94.73	65.24	50	50	2	
92.39	94.94	68.23	50	50	3	
86.32	94.78	67.51	50	50	4	
86.74	94.38	67.09	50	50	5	
86.75	94.4	66.69	50	50	6	
88.36	94.81	66.86	50	50	7	
86.27	94.9	67.74	50	50	8	
86.3	94.87	67.55	50	50	9	
86.83	94.76	67.57	50	50	10	
82.43	63.17	64.27	4.57	0.61	1	Bayes
83.92	64.16	63.88	5.48	0.28	2	
82.46	62.83	63.49	5.37	0.46	3	
83.79	64.24	65.81	5.6	0.27	4	
82.64	63.96	64.08	5.84	0.3	5	
83.01	64.02	62.74	5.56	0.26	6	
83.4	64.1	65.14	5.29	0.28	7	
83.15	63.89	65.18	5.48	0.24	8	
83.73	64.34	64.3	5.63	0.37	9	
83.7	63.68	64.13	4.81	0.55	10	
98.62	99.48	97.69	78.94	50	1	KNN
98.82	99.41	96.74	82.89	100	2	
98.59	99.48	96.52	80	50	3	
98.89	98.89	96.58	76.62	50	4	
98.9	99.66	96.96	83.09	100	5	
98.7	99.44	96.64	83.54	50	6	
98.5	99.38	97.05	78.65	50	7	
98.63	99.44	96.46	83.52	50	8	
98.66	99.31	96.64	88.37	50	9	
98.41	99.45	97.39	78.75	50	10	
98.62	99.48	97.69	78.94	50	1	ترکیب (روش پیشنهادی)
98.82	99.41	96.74	82.89	100	2	
98.59	99.48	96.52	80	50	3	
98.89	98.89	96.58	76.62	50	4	
98.9	99.66	96.96	83.09	100	5	
98.7	99.44	96.64	83.54	50	6	
98.5	99.38	97.05	78.65	50	7	
98.63	99.44	96.46	83.52	50	8	
98.66	99.31	96.64	88.37	50	9	
98.41	99.45	97.39	78.75	50	10	

جدول ۱۱: نرخ شناسایی حملات با الگوریتم 3-NN و در حالت تغییر میزان داده‌های آموزش و آزمون

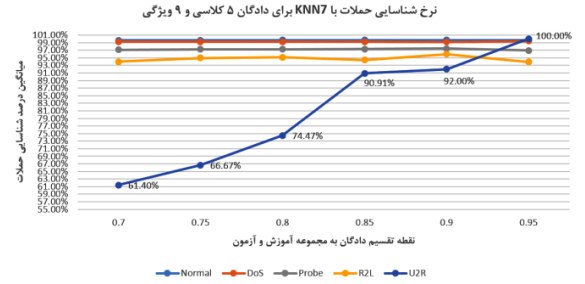
مقدارها به درصد					Class	features	test	train	
Normal	DoS	Probe	R2L	U2R					
99.74	99.35	97.67	95.46	64.13	5	9	0.3	0.7	KNN (K = 3)
99.74	99.41	97.66	96.14	56.12	5	9	0.25	0.75	
99.74	99.37	97.60	96.37	61.84	5	9	0.2	0.8	
99.75	99.35	97.79	96.07	68.97	5	9	0.15	0.85	
99.75	99.33	97.70	96.08	69.77	5	9	0.1	0.9	
99.79	99.52	97.52	96.27	73.68	5	9	0.05	0.95	



شکل ۲: نمودارنرخ شناسایی‌حملات برای ۵کلاس، ۹ویژگی توسط 3-NN در حالات مختلف تعداد داده‌های آموزش و آزمون

جدول ۱۲: نرخ شناسایی حملات با الگوریتم 7-NN و در حالت تغییر میزان داده‌های آموزش و آزمون

مقدارها به درصد					Class	features	test	train	
Normal	DoS	Probe	R2L	U2R					
99.65	99.22	97.15	93.99	61.40	5	9	0.3	0.7	KNN (K = 7)
99.64	99.25	97.26	94.92	66.67	5	9	0.25	0.75	
99.67	99.27	97.25	95.16	74.47	5	9	0.2	0.8	
99.68	99.22	97.30	94.44	90.91	5	9	0.15	0.85	
99.68	99.20	97.42	96.00	92.00	5	9	0.1	0.9	
99.70	99.43	96.95	93.95	100	5	9	0.05	0.95	



شکل۳: نرخ شناسایی‌حملات‌برای ۵کلاس، ۹ویژگی‌توسط 7-NN در حالات مختلف تعداد داده‌های آموزش و آزمون

همان‌گونه که در جدول‌شماره ۱۱ مشاهده می‌شود الگوریتم 3-NN در حالتی که مجموعه آموزش ۹۵ درصد و مجموعه آزمون ۵ درصد از کل داده‌ها باشد در شناسایی رفتار عادی(۹۹/۷۹) و همچنین حملات DoS (۹۹/۵۲) بهترین عملکرد را نشان‌داد. مطابق جدول۱۲ الگوریتم 7-NN نیز با همین درصد از مجموعه آموزش و آزمون نرخ شناسایی حمله U2R را تا صددرصد بهبود داد، همچنین همان‌طور که در شکل‌های شماره ۲ و ۳ مشاهده می‌شود با افزایش میزان داده‌های آموزش، بهبود قابل توجهی در عملکرد طبقه‌بند KNN جهت شناسایی حمله U2R حاصل شد.

در جدول شماره ۱۳ نتیجه مقایسه میزان تشخیص روش پیشنهادی با برخی از سایر روش‌های ارائه‌شده که براساس معیار دقت روی دادگان NSL-KDD آزمایش شده است را مشاهده می‌کنید. نتایج

بدست آمده برتری میزان دقت تشخیص حملات را نسبت به سایر روش‌های ارائه شده بر روی دادگان NSL-KDD نشان می‌دهد.

جدول ۱۳: مقایسه نتایج به‌دست‌آمده از روش پیشنهادی با سایر روش‌های ارائه‌شده براساس معیار دقت (Precision) و دادگان NSL-KDD

شماره مرجع	مولف	نتیجه	روش پیشنهادی
[۲]	(Tama and Rhee 2017)	99.8 (دوکلاسی)	99.93
[۳]	(AMINI, REZAEE et al. 2014)	87.6(Normal) 96.2(DoS) 83.3(Probe) 77.4(R2L) 81.4(U2R)	98.14 96.85 93.20 91.31 100
[۴]	(Dhaliwal, Nahid et al. 2018)	98.41 (دوکلاسی)	99.93
[۵]	(Gao, Shan et al. 2019)	94.93(Normal) 84.37(DoS) 87.11(Probe) 55.27(R2L) 25.00(U2R)	98.14 96.85 93.20 91.31 100
[۶]	(Mkuzangwe and Nelwamondo 2017)	85.17	99.93
[۷]	(Mirza 2018)	97.41	99.93
[۸]	Alhakami, ALharbi et al. 2019)	81.50	99.93

۶- نتیجه‌گیری و کارهای آینده

در این تحقیق یک سامانه تشخیص نفوذ برای بهبود دقت با استفاده از ترکیب وزن‌دار طبقه‌بندها پیشنهاد شد. به منظور ترکیب طبقه‌بندها از روش ادغام استفاده کردیم. نتیجه تصمیم‌گیری بر اساس رأی وزن‌دار طبقه‌بندها تعیین شده است. به‌منظور کاهش بار محاسباتی، قبل از استفاده از دادگان ویژگی‌های آن را به کمک الگوریتم‌های یادگیری ماشین کاهش دادیم. آزمایش‌ها حدود ۱۰ بار تکرار شدند. الگوریتم آنتروپی در مجموعه فازی ناهموار به‌منظور کاهش ویژگی و انتخاب ویژگی‌های مهم به‌کارگیری شد. جهت طبقه‌بندی از سه الگوریتم SVM، Bayes و KNN استفاده شد.

نتایج نشان می‌دهد دقت الگوریتم پیشنهادی در حالت دو کلاسی و در سه کلاس از حالت ۵ کلاسی نسبت به سایر روش‌های ارائه‌شده اخیر بالاتر بوده است و هر الگوریتمی که بتواند نتایج بهتری در شناسایی حملات داشته باشد قابل به‌کارگیری در این روش نیز خواهد بود. برای کارهای آینده، می‌توان بهبود آموزش طبقه‌بندها با استفاده از روش یادگیری عمیق[۵۱] و به‌کارگیری شیوه شناسایی دوسطحی در ترکیب طبقه‌بندها را به منظور بهبود عملکرد روش پیشنهادی بررسی نمود.

مراجع

[1] E. Alpaydin, *Introduction to machine learning*: MIT press, 2009.

[2] B. A. Tama and K.-H. Rhee, "Performance evaluation of intrusion detection system using classifier ensembles," *International Journal of Internet Protocol Technology*, vol. 10, pp. 22-29, 2017.

[3] M. AMINI, N. J. REZAEE, and E. HADAVANDI, "Effective intrusion detection with a neural network ensemble using fuzzy clustering and stacking combination method," *Journal of Computing and Security*, vol. 1, pp. 293-305, 2014.

[4] S. Dhaliwal, A.-A. Nahid, and R. Abbas, "Effective intrusion detection system using XGBoost," *Information*, vol. 9, p. 149, 2018.

[5] X. Gao, C. Shan, C. Hu, Z. Niu, and Z. Liu, "An Adaptive Ensemble Machine Learning Model for Intrusion Detection," *IEEE Access*, vol. 7, pp. 82512-82521, 2019.

[6] N. N. Mkuzangwe and F. Nelwamondo, "Ensemble of classifiers based network intrusion detection system performance bound," in *Systems and Informatics (ICSAI), 2017 4th International Conference on*, 2017, pp. 970-974.

[7] A. H. Mirza, "Computer network intrusion detection using various classifiers and ensemble learning," in *2018 26th Signal Processing and Communications Applications Conference (SIU)*, 2018, pp. 1-4.

[8] W. Alhakami, A. ALharbi, S. Bourouis, R. Alroobaea, and N. Bouguila, "Network Anomaly Intrusion Detection Using a Nonparametric Bayesian Approach and Feature Selection," *IEEE Access*, vol. 7, pp. 52181-52190, 2019.

[9] J. Ryan, M.-J. Lin, and R. Miikkulainen, "Intrusion detection with neural networks," *Advances in neural information processing systems*, pp. 943-949, 1998.

[10] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, "A survey of intrusion detection techniques in cloud," *Journal of Network and Computer Applications*, vol. 36, pp. 42-57, 2013.

[11] O. Depren, M. Topallar, E. Anarim, and M. K. Ciliz, "An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks," *Expert systems with Applications*, vol. 29, pp. 713-722, 2005.

[12] D. M. Farid, L. Zhang, A. Hossain, C. M. Rahman, R. Strachan, G. Sexton, *et al.*, "An adaptive ensemble classifier for mining concept drifting data streams," *Expert Systems with Applications*, vol. 40, pp. 5895-5906, 2013.

[13] M. Saidi, M. E. A. Bechar, N. Settouti, and M. A. Chikh, "Instances selection algorithm by ensemble margin," *Journal of Experimental & Theoretical Artificial Intelligence*, pp. 1-22, 2017.

[14] H.-s. Chae, B.-o. Jo, S.-H. Choi, and T. Park, "Feature Selection for Intrusion Detection using NSL-KDD," *Recent Advances in Computer Science, ISBN*, pp. 978-960, 2015.

[15] L. Dhanabal and D. S. Shantharajah, "A Study on NSL-KDD Dataset for Intrusion Detection System Based on Classification Algorithms," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 4, pp. 446-452, 2015.

[16] S. Duque and M. N. bin Omar, "Using Data Mining Algorithms for Developing a Model for Intrusion Detection System (IDS)," *Procedia Computer Science*, vol. 61, pp. 46-51, 2015.

[17] J. Jabez and B. Muthukumar, "Intrusion Detection System (IDS): Anomaly detection using outlier detection approach," *Procedia Computer Science*, vol. 48, pp. 338-346, 2015.

[18] 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, pp. 8609-8624, 2015.

[19] D. J. Weller-Fahy, B. J. Borghetti, and A. A. Sodemann, "A survey of distance and similarity measures used within network

[29] G. Chandrashekar and F. Sahin, "A survey on feature selection methods," *Computers & Electrical Engineering*, vol. 40, pp. 16-28, 2014.
[30] V. H. Moghaddam and J. Hamidzadeh, "New Hermite orthogonal polynomial kernel and combined kernels in Support Vector Machine classifier," *Pattern Recognition*, vol. 60, pp. 921-935, 2016.
[31] Z. Pawlak, "Rough sets," *International Journal of Parallel Programming*, vol. 11, pp. 341-356, 1982.
[32] W.-Z. Wu, J.-S. Mi, and W.-X. Zhang, "Generalized fuzzy rough sets," *Information sciences*, vol. 151, pp. 263-282, 2003.
[33] F. Fazayeli, L. Wang, and J. Mandziuk, "Feature selection based on the rough set theory and expectation-maximization clustering algorithm," in *International Conference on Rough Sets and Current Trends in Computing*, 2008, pp. 272-282.
[34] S. Muthurajkumar, K. Kulothungan, M. Vijayalakshmi, N. Jaisankar, and A. Kannan, "A rough set based feature selection algorithm for effective intrusion detection in cloud model," in *Proceedings of the international conference on advances in communication, network, and computing*, 2013, pp. 8-13.
[35] L. I. Kuncheva, *Combining pattern classifiers: methods and algorithms*: John Wiley & Sons, 2004.
[36] J. McHugh, "Testing intrusion detection systems: a critique of the 1998 and 1999 darpa intrusion detection system evaluations as performed by lincoln laboratory," *ACM Transactions on Information and System Security (TISSEC)*, vol. 3, pp. 262-294, 2000.
[37] S. Revathi and A. Malathi, "Network Intrusion Detection Based On Fuzzy Logic," *International Journal of Computer Application*, vol. 1, pp. 143-149, 2014.
[38] "NSL-KDD Dataset," U. O. N. Brunswick, Ed., ed.
[39] S. B. Kotsiantis, "Bagging and boosting variants for handling classifications problems: a survey," *The Knowledge Engineering Review*, vol. 29, pp. 78-100, 2014.
intrusion anomaly detection," *IEEE Communications Surveys & Tutorials*, vol. 17, pp. 70-91, 2015.
[20] X. Jia, L. Shang, B. Zhou, and Y. Yao, "Generalized attribute reduct in rough set theory," *Knowledge-Based Systems*, vol. 91, pp. 204-218, 2016.
[21] Y. Xiao, C. Xing, T. Zhang, and Z. Zhao, "An Intrusion Detection Model Based on Feature Reduction and Convolutional Neural Networks," *IEEE Access*, vol. 7, pp. 42210-42219, 2019.
[22] C. Guo, Y. Ping, N. Liu, and S.-S. Luo, "A two-level hybrid approach for intrusion detection," *Neurocomputing*, vol. 214, pp. 391-400, 2016.
[23] S.-Y. Ji, B.-K. Jeong, S. Choi, and D. H. Jeong, "A multi-level intrusion detection method for abnormal network behaviors," *Journal of Network and Computer Applications*, vol. 62, pp. 9-17, 2016.
[24] C.-C. Huang, T.-L. B. Tseng, and C.-Y. Tang, "Feature extraction using rough set theory in service sector application from incremental perspective," *Computers & Industrial Engineering*, vol. 91, pp. 30-41, 2016.
[25] W. L. Al-Yaseen, Z. A. Othman, and M. Z. A. Nazri, "Multi-level hybrid support vector machine and extreme learning machine based on modified K-means for intrusion detection system," *Expert Systems with Applications*, vol. 67, pp. 296-303, 2017.
[26] M. Rajasekaran and A. Ayyasamy, "A Novel Ensemble Approach for Effective Intrusion Detection System," in *Recent Trends and Challenges in Computational Models (ICRTCCM), 2017 Second International Conference on*, 2017, pp. 244-250.
[27] Y. Shen, K. Zheng, C. Wu, M. Zhang, X. Niu, and Y. Yang, "An Ensemble Method based on Selection Using Bat Algorithm for Intrusion Detection," *The Computer Journal*, vol. 61, pp. 526-538, 2017.
[28] V. Timčenko and S. Gajin, "Ensemble classifiers for supervised anomaly based network intrusion detection," in *Intelligent Computer Communication and Processing (ICCP), 2017 13th IEEE International Conference on*, 2017, pp. 13-19.

زیرنویس‌ها:

1 - Intrusion Detection System(IDS)
2 - Intrusion Prevention System(IPS)
3 - Port scaning
4 - Network administrator
5 - Host based IDS(HIDS)
6 - Network based IDS(NIDS)
7 - Denial of Service(DoS)
8 - IP(Internet Protocol)
9 - Header
10 - Distributed Intrusion Detection System(DIDS)
11 - Signature based detection
12 - Zero day attack
13 - Anomaly based detection
14 - False Alarm(FA)
15 - Hybrid metohd
16 - Feature space
17 - Dataset
18 - Ensemble Margin Instance Selection(EMIS)
19 - False negative(FN)
20 - Outlier computation-based
21 - Online sequential extreme learning machine
22 - Convolutional neural network–intrusion detection system
23 - False positive
24 - Integer-programming
25 - Incremental weight incorporated rule identification
26 - Condition attributes
27 - Support vector machine(SVM)
28 - Extreme Learning Machine(ELM)
29 - Incremental Particle Swarm Optimization(IPSO)
30 - Information Gain
31 - Infinite bounded generalized Gaussian mixture with feature selection
32 - Rough Set
33 - Hermite orthogonal polynomials
34 - Ensemble method
35 - Trainable ensembles
36 - K Nearest Neighbor
37 - Training
38 - Testing
39 - https://iscxdownloads.cs.unb.ca/iscxdownloads
40 - Preprocessing
41 - Feature selection
42 - Feature extraction
43 - Attack
44 - Normal
45 - Denial Of Service(DOS)
46 - Probe
47 - User to Root(U2R)
48 - Remote to Local(R2L)
49 - Entropy
50 - Precision
51 - Deep learning