ارائه یک سیستم تشخیص نفوذ جدید مبتنی بر ماشین بردار پشتیبان و بهینه‌سازی کلونی زنبور مصنوعی بهبودیافته

طیبه فیضی[۱]، مربی؛ سیدمحمدحسین معطر[۲]، استادیار

۱- گروه کامپیوتر- واحد نیشابور - دانشگاه آزاد اسلامی - نیشابور - ایران - t.feizi@iau-neyshabur.ac.ir
۲- گروه کامپیوتر - واحد مشهد - دانشگاه آزاد اسلامی - مشهد - ایران - moattar@mshdiau.ac.ir

چکیده: میزان نفوذ در شبکه در حال افزایش است. سیستم تشخیص نفوذ، می‌تواند تا حد زیادی از حملات به شبکه جلوگیری کند. انتخاب ویژگی یک موضوع حیاتی در سیستم‌های تشخیص نفوذ می‌باشد که بر روی صحت و کارایی آن تأثیر بسزایی دارد. در این تحقیق، یک سیستمِ تشخیصِ نفوذ در شبکهِ ترکیبیِ جدید با استفاده از الگوریتم کلونی زنبور مصنوعی بهبودیافته مبتنی بر طبقه‌بند ماشین بردار پشتیبان با روش ارزیابی 10-fold برای انتخاب بهترین ویژگی‌ها پیشنهاد گردیده است. ایده اصلی، از ترکیب معادلات جستجوی بهینه‌سازی ازدحام ذرات و تکاملی تفاضلی در فاز زنبورهای کارگر و ناظر به‌منظور به‌روزرسانی موقعیت زنبورها و به‌کارگیری پرواز لوی در فاز زنبورهای پیشاهنگ، به‌منظور بهبود بهره‌برداری و نرخ همگرایی در الگوریتم کلونی زنبور مصنوعی می‌باشد. روش پیشنهادی مقاومت و پایداری خود را بر روی مجموعه‌داده NSL-KDD نشان داده و به‌طور قابل توجهی توانسته به بهبود عملکرد کلی سیستم تشخیص نفوذ با صحت ۹۸/۹۷ درصد کمک کند.

واژه‌های کلیدی: سیستم تشخیص نفوذ، الگوریتم کلونی زنبور مصنوعی، ماشین بردار پشتیبان، بهینه‌سازی تکاملی، پرواز لوی

A Novel Intrusion Detection System Based on Support Vector Machine and Improved Artificial Bee Colony Optimization

Tayyebe Feizi[1], Instructor; Mohammad Hossein Moattar[2,] Assistant Professor

1- Computer Engineering Department, Neyshabur Branch, Islamic Azad University, Neyshabur, Iran, Email: t.feizi@iau-neyshabur.ac.ir
2- Computer Engineering Department, Mashhad Branch, Islamic Azad University, Mashhad, Iran, Email: moattar@mshdiau.ac.ir

Abstract: Intrusion in the network is increasing. Intrusion detection system can greatly prevent network attacks. Feature selection is a critical issue in intrusion detection systems which have a considerable impact on the accuracy and effectiveness of the system. In this study, a new hybrid network intrusion detection system with improved artificial bee colony algorithm using support vector machine classifier is proposed for feature selection. The main idea is utilizing a combination of search equations of particle swarm optimization and Differential Evolution for updating bee's position of employed and onlooker bees and utilizing levy flight on scout bees phase, to improve exploitation and increase the convergence rate of the standard artificial bee colony algorithm. The robustness and stability of the proposed approach is evaluated on NSL-KDD dataset and showed significant improvement on the overall performance of intrusion detection system with an accuracy of 98.97 percent.

Keywords: Intrusion Detection System, Artificial Bee Colony Algorithm, Support Vector Machine, Evolutionary Optimization, Levy Flight

تاریخ ارسال مقاله: ۱۳۹۶/۶/۱۳
تاریخ اصلاح مقاله: ۱۳۹۶/۱۲/۹
تاریخ پذیرش مقاله: ۱۳۹۷/۲/۱۲
نام نویسنده مسئول: سید محمد حسین معطر
نشانی نویسنده مسئول: گروه کامپیوتر - واحد مشهد - دانشگاه آزاد اسلامی - مشهد - ایران

۱ - مقدمه

استفاده زیاد از اینترنت و سیستم‌های کامپیوتری، مسائل امنیتی متعددی را ایجاد می‌کند. آمارهای CERT بیانگر افزایش نفوذ[۱] در شبکه است. هرگونه نفوذ در جهت آسیب‌زدن به شبکه ممکن است منجر به نقض سیاست‌های امنیتی کامپیوتر همانند محرمانگی[۲]، تمامیت[۳] و دسترسی[۴] به منابع شود. سیستم تشخیص نفوذ[۵] (IDS) از جمله فناوری‌هایی است گاه می‌تواند از بروز حملات به شبکه جلوگیری کند[۱، ۲].

مسئله IDS یک مسئله اصیل پژوهشی در امنیت شبکه می‌باشد. موضوع IDS به دلیل طبیعت غیرخطی نفوذ، رفتار غیرقابل پیش‌بینی ترافیک در شبکه و تعداد زیاد ویژگی در فضای مسئله، جزء مسائل پیچیده می‌باشد[۳، ۴]. کار اصلی IDS طبقه‌بندی فعالیتهای درون شبکه‌ای به دو دسته نرمال و غیرنرمال است به گونه‌ای که از طبقه‌بندی‌های نادرست اجتناب شود[۵]. یک IDS، با حجم بالایی از ترافیک داده‌ها در شبکه مواجه است. این داده‌ها شامل ویژگی‌های بی‌اهمیت و نامرتبط هستند. با انتخاب بهترین ویژگی‌ها می‌توان کل داده‌ها را پوشش داد و الگوی ترافیک شبکه را مشخص نمود[۳].

انتخاب ویژگی، یک موضوع حیاتی و دشوار در IDS است که بر روی دقت و کارایی آن تأثیر می‌گذارد[۸-۶]. از خصوصیات یک IDS مناسب این است که حملات را با دقت بالایی تشخیص دهد در حالیکه IDSهای موجود حجم بالایی از تاییدهای نادرست[۶] (FP) و هشدارهای نادرست[۷] (FN) را متحمل می‌شوند و قادر به اداره ترافیک در حال افزایش نیستند[۹].

نفوذ فعالیتی است که توسط آن محرمانگی، تمامیت و دسترس‌پذیری به منابع دچار اختلال می‌شود. تشخیص نفوذ فرآیندی است که با بررسی رخدادهای شبکه می‌تواند نفوذ را شناسایی کند[۱]. روش‌های تشخیص نفوذ را می‌توان در سه گروه اصلی تشخیص مبتنی بر شناسه[۸] (SD)، تشخیص مبتنی بر بی‌نظمی[۹](AD) و آنالیز پروتکل حالات[۱۰](SPA) طبقه‌بندی کرد[۱، ۱۰]. شناسه، الگوی یک حمله شناخته‌شده می‌باشد که به مجموعه‌ای از قوانین تبدیل شده است. روش SD با ارزیابی حملات بر اساس شناسه و تأثیر آنها در شبکه فعالیت می‌کند. بی‌نظمی، به انحراف در رفتار نرمال یک کاربر گفته می‌شود[۱]. روش AD با توجه به ترافیک غیرعادی موجود و مقایسه ترافیک نرمال و غیرنرمال، تصمیم می‌گیرد که هشدار دهد[۱۰]. در روش SPA، IDS حالات پروتکل را شناسایی و ردگیری می‌کند[۱].

از طرفی رویکردهای تشخیص را می‌توان به پنج زیر گروه تقسیم کرد. در رویکردهای مبتنی بر آمار، از مقادیر میانگین، انحراف معیار و احتمالات استفاده می‌شود. در رویکردهای مبتنی بر الگو، از تطبیق الگو با حملات شناخته‌شده استفاده می‌شود. در رویکردهای مبتنی بر قانون، از قوانین If-Then و If-Then-Else برای ساختن مدل و ایجاد پروفایلی از نفوذهای شناخته‌شده، استفاده می‌شود. در رویکردهای مبتنی بر حالت، از روی رفتارهای موجود در شبکه، یک ماشین حالت متناهی ایجاد شده و از آن به عنوان ابزاری در جهت شناسایی حملات استفاده می‌شود. در رویکردهای مبتنی بر اکتشاف، از مفاهیم بیولوژیکی در طبیعت و هوش‌مصنوعی استفاده می‌شود[۱].

در باقیمانده مقاله، در بخش دوم، کارهای مرتبط با روش پیشنهادی مرور می‌شود. در بخش سوم، ابزارها و روش‌های تحقیق بیان می‌شود. در بخش چهارم، با تمرکز بر روی مسئله انتخاب ویژگی، روش پیشنهادی با دلایل انتخاب هر یک از ابزارها تشریح می‌شود. بخش پنجم حاوی نتایج حاصل از شبیه‌سازی روش پیشنهادی است. بخش ششم نتیجه‌گیری و زمینه‌های پژوهشی آینده را بیان می‌کند.

۲ - کارهای مرتبط

۲-۱- جلوگیری از بهینه محلی

در سال ۲۰۱۳، Wang و همکارانش الگوریتم CABC را برای پیش‌بینی ساختار پروتئین سه‌بعدی ارائه دادند. الگوریتم CABC، جستجوی محلی و سراسری الگوریتم ABC را با جستجوی آشوبناک ترکیب کرد. هدف از این روش جلوگیری از بهینه محلی بود[۱۱].

۲-۲- بهبود جستجوی محلی و نرخ همگرایی

در سال ۲۰۱۳، Bansal و همکارش، جستجوی ممتیک را با الگوریتم ABC ترکیب کردند و روش MeABC را پیشنهاد دادند. در این روش، آن‌ها معادله الگوریتم ABC را به یک معادله جدید الهام‌گرفته از معادله الگوریتم PSO تغییر دادند و در آن از جستجوی محلی (GSS) استفاده کردند. هدف از این روش ایجاد توازن بین اکتشاف[۱۱] و بهره‌برداری[۱۲] در ABC و نهایتاً بهبود جستجوی محلی بود[۱۲].

در سال ۲۰۱۴، Kumar و همکارانش به منظور ایجاد توازن بین اکتشاف و بهره‌برداری، روش‌های MeABC و FPABC را ترکیب کردند و روش MFPABC را ارائه دادند. در این روش، در فاز زنبور کارگر[۱۳] از الگوریتم ABC، در فاز زنبور ناظر[۱۴] از FPABC به‌منظور بهبود جستجوی محلی، در فاز زنبور پیشاهنگ[۱۵] از الگوریتم ABC و برای افزایش نرخ همگرایی از الگوریتم MeABC بعد از فاز زنبور پیشاهنگ استفاده شد. هدف از این روش بهبود جستجوی محلی و افزایش نرخ همگرایی بود[۱۳].

در سال ۲۰۱۴، Shan و همکارانش، الگوریتم ABC ترکیبی مبتنی بر پرواز لوی را پیشنهاد دادند. در این روش از توزیع لوی برای مقداردهی اولیه جمعیت، از ترکیب معادله جهش الگوریتم DE با الگوریتم ABC، برای ایجاد معادله جستجوی زنبورهای کارگر، از ترکیب معادله الگوریتم PSO با الگوریتم ABC برای ایجاد معادله جستجوی زنبورهای ناظر و از مقداردهی اولیه OBL آشوبناک برای ایجاد معادله زنبورهای پیشاهنگ استفاده کردند. هدف از این روش بهبود نرخ همگرایی بود [۱۴].

در سال ۲۰۱۶، Bharti و همکارش، روش CGABC را برای خوشه‌بندی متن، پیشنهاد دادند. در این روش، علاوه بر بهبود معادله جستجوی الگوریتم ABC، از جستجوهای محلی آشوبناک و گرادیان برای بهبود بهره‌برداری الگوریتم ABC استفاده شد. هدف از این روش بهبود کیفیت راه‌حل‌ها و افزایش نرخ همگرایی بود[۱۵].

۲-۳- بهبود نرخ تشخیص نفوذ

در سال ۲۰۱۳، Dastanpour و همکارش به بررسی عملکرد GA با SVM برای انتخاب ویژگی پرداختند و از الگوریتم‌های FFSA وLCFS در تشخیص انواع حملات شبکه استفاده کردند. هدف از این روش بهبود نرخ تشخیص و نرخ تاییدهای نادرست بود[۱۶].

در سال ۲۰۱۶، Hosseini و همکارانش یک IDS مبتنی بر TVCPSO ارائه کردند که به‌طور همزمان برای تنظیم پارامترها و انتخاب ویژگی در طبقه‌بندهای MCLP و SVM به‌کار می‌رفت. هدف از این روش بهبود نرخ تشخیص و کاهش نرخ هشدارهای نادرست بود[۱۷].

در سال ۲۰۱۷، Akashdeep و همکارانش یک IDS جدید ارائه کردند که ابتدا ویژگی‌ها را با دو روش IG و CR به‌طور جداگانه رتبه‌بندی می‌کند سپس با ترکیب رتبه‌ها فیلترینگ انجام می‌دهد. در ادامه ویژگی‌های کاهش‌یافته را به یک شبکه عصبی روبه‌جلو برای آموزش و آزمایش می‌دهد. هدف از این روش بهبود نرخ تشخیص و صحت طبقه‌بند و کاهش نرخ هشدارهای نادرست بود[۱۸].

در سال ۲۰۱۵، Sabry و همکارانش روش ترکیبی جدیدی ارائه دادند که مبتنی بر الگوریتم‌های ID3 و BA به‌منظور انتخاب بهترین ویژگی‌ها در IDS بود که این الگوریتم‌ها به‌ترتیب به‌عنوان طبقه‌بند و روش انتخاب ویژگی به‌کار گرفته شد. هدف از این روش بهبود صحت طبقه‌بند و نرخ تشخیص و کاهش نرخ هشدارهای نادرست بود[۳].

در سال ۲۰۱۷، Wang و همکارانش یک IDS جدید ارائه کردند که مبتنی بر SVM با ویژگی‌های افزوده بود. آن‌ها از تبدیل نسبت‌های تراکم حاشیه لگاریتمی برای تغییر ویژگی‌های اولیه استفاده کردند. با این هدف که ویژگی‌های تغییریافته کیفیت بهتری داشته باشند. آن‌ها بر این عقیده هستند که با نسبت تراکم حاشیه می‌توان قوی‌ترین طبقه‌بندی یکنواخت را انجام داد. هدف از این روش بهبود صحت، سرعت آموزش، نرخ تشخیص و کاهش هشدارهای نادرست بود[۱۹].

در سال ۲۰۱۷، Raman و همکارانش یک IDS با استفاده از هایپرگراف مبتنی بر الگوریتم ژنتیک (HG-GA) ارائه کردند که هدفش بهینه‌سازی پارامترها و انتخاب ویژگی در SVM بود. روش HG-GA از یک تابع هدف وزن‌دهی شده به‌منظور ایجاد توازن بین نرخ تشخیص حداکثری و نرخ هشدارهای نادرست حداقلی استفاده می‌کرد به‌شرط آنکه تعداد ویژگی‌ها بهینه باشد. هدف از این روش بهبود صحت، نرخ تشخیص، نرخ هشدار نادرست و تحلیل زمان اجرا بود[۲۰].

در سال ۲۰۱۷، Bamakan و همکارانش رویکردی مقاوم، خلوت و دقیقی را برای مسئله تشخیص نفوذ چندکلاسی ارائه کردند. مدل پیشنهادی آنها مبتنی بر رگرسیون-طبقه‌بندِ K بردار پشتیبان با تابع زیان Ramp بود که آن را Ramp-KSVCR نامیدند. در این مدل آنها در جهت رفع مشکل توزیع نامتوازن در مجموعه‌داده‌ها، حذف نویز و داده‌های پرت در داده‌های آموزشی و ایجاد مقیاس‌پذیری و کاهش زمان آموزش تلاش کردند. هدف از این روش بهبود صحت طبقه‌بند و نرخ تشخیص و کاهش نرخ هشدارهای نادرست بود[۲۱].

در سال ۲۰۱۷، Raman و همکارانش یک روش جدید مبتنی بر هایپرگراف و شبکه عصبی احتمالی مبتنی بر باقیمانده حسابی پیشنهاد کردند و مدل خود را HG AR-PNN نامیدند. این مدل برای مسئله طبقه‌بندی در IDS به‌کار می‌رفت. آن‌ها از خصوصیت Helly در هایپرگراف، برای تشخیص زیرمجموعه بهینه ویژگی‌ها و از باقیمانده حسابی زیرمجموعه بهینه ویژگی‌ها، برای آموزش PNN استفاده کردند. هدف از این روش بهبود صحت و نرخ تشخیص در قبال حملات با تکرار کمتر بود[۲۲].

۲-۴- بهبود سرعت تشخیص نفوذ

در سال ۲۰۱۴، Mashwani و همکارش، الگوریتم ممتیکِ چندهدفه جدید مبتنی بر رویکرد تجزیه و الگوریتم PSO ارائه کردند و آن را MOEA/D-DE+PSO نامیدند. در این روش، از الگوریتم PSO برای جستجوی محلی و از الگوریتم DE برای جستجوی سراسری استفاده شد. نتایج آزمایشات روش پیشنهادی آنها بسیار امیدوار کننده‌تر از الگوریتم MOEA/D بود. هدف از این روش بهبود نرخ تشخیص و سرعت تشخیص بود[۲۳].

در سال ۲۰۱۴، Zhigang روش ABC-KELM را ارائه کرد که به طور کارا نفوذهای شبکه را تشخیص می‌داد. در این تحقیق برای بهینه‌سازی KELM از الگوریتم ABC استفاده شد. هدف از این روش بهبود صحت و سرعت تشخیص نفوذ بود[۲۴].

در سال ۲۰۱۵، Singh و همکارانش تکنیکی ارائه کردند که مبتنی بر OS-ELM به‌منظور تشخیص نفوذ بود. هدف از این روش بهبود صحت طبقه‌بند، افزایش تاییدهای نادرست و بهبود سرعت تشخیص بود[۲۵].

۲-۵- بهبود صحت طبقه‌بند

در سال ۲۰۱۲، Lin و همکارانش یک الگوریتم هوشمند با امکان انتخاب ویژگی و قوانین تصمیم‌گیری برای سیستم‌های AD پیشنهاد کردند. روش آنها ترکیبی از SVM، DT و SA بود. هدف از این روش بهبود صحت طبقه‌بند بود[۲۶].

در سال ۲۰۱۲، Chung و همکارانش یک IDS ترکیبی جدید ارائه کردند که مبتنی بر IDS-RS به‌منظور انتخاب ویژگی و SSO-WLS

به‌عنوان طبقه‌بند بود. هدف از این روش بهبود صحت طبقه‌بند و جستجوی محلی بود[۲۷].

در سال ۲۰۱۳، Chahkandi و همکارانش به انتخاب ویژگی در IDS به کمک الگوریتم CHABCF پرداختند که در این الگوریتم از تئوری آشوب، الگوریتم ABC و منطق فازی استفاده شد. تئوری آشوب را به‌منظور تولید جمعیت اولیه با تنوع بیشتر به‌کار گرفت و منطق فازی را به‌منظور حذف ابهام ایجاد شده در اثر به‌کارگیری تئوری آشوب استفاده کرد. هدف از این روش بهبود صحت طبقه‌بند بود[۲۸].

در سال ۲۰۱۳، Othman و همکارانش از تکنیک‌های انتخاب ویژگی مبتنی بر Wrapper با استفاده از الگوریتم GDA و طبقه‌بند SVM استفاده کردند. هدف از این روش بهبود صحت طبقه‌بند بود[۲۹].

در سال ۲۰۱۵، Gupta و همکارش یک سیستم IDS مبتنی بر طبقه‌بند SVM و خوشه بندی ارائه دادند. از الگوریتم BC برای خوشه‌بندی و به‌روزرسانی مدل‌ها استفاده شد. هدف از این روش بهبود صحت طبقه‌بند بود[۳۰].

در سال ۲۰۱۵، Amudha و همکارانش روش MABC-EPSO را به‌منظور تشخیص نفوذ ارائه دادند که ترکیبی از الگوریتم‌های MABC و EPSO بود. هدف از این روش بهبود صحت طبقه‌بند است[۶].

در سال ۲۰۱۶، Gurcan و همکارش برای غلبه بر مشکل پیچیدگی محاسبات و تنزل کارایی در اثر تعداد زیاد ویژگی‌ها، از تکنیک Angle Modulation به همراه شش نوع متنوع از الگوریتم ABC که می‌توان به OABC، MABC، GABC، GDABC، CABC، EABC اشاره کرد، استفاده کردند. هدف از این روش بهبود صحت طبقه‌بند بود[۳۱].

در سال ۲۰۱۶، Hosseinzadeh و همکارش برای انتخاب ویژگی در IDS از بهینه‌سازی کلونی مورچه (ACO) استفاده کردند. هدف از این روش بهبود صحت طبقه‌بند و کاهش نرخ هشدارهای نادرست بود [۴].

در سال ۲۰۱۷، Aburomman و همکارش یک طبقه‌بند چندکلاسی جدید با ترکیب SVMهای باینری وزن‌دار در زمینه IDSها ارائه کردند و روش پیشنهادی خود را WOAR-SVM نامیدند. وزن‌ها توسط الگوریتم تکاملی تفاضلی ایجاد می‌شود. روش WOAR-SVM به کمک مجموعه‌ای از وزن‌های فراکتشافی قادر است خطاهای پیش‌بینی را در هر طبقه‌بند باینری جبران کند. در مدل پیشنهادی آنها هر طبقه‌بند باینری می‌تواند مجموعه‌ای منحصر به‌فرد از پارامترها را داشته باشد. هدف از این روش بهبود صحت طبقه‌بند بود[۳۲].

در سال ۲۰۱۷، Ashfaq و همکارانش یک IDS جدید ارائه کردند که در آن از روش یادگیری نیمه‌نظارتی SSL مبتنی بر فازی استفاده می‌شد به‌گونه‌ای که نمونه‌های بدون برچسب به کمک الگوریتم یادگیری تحت‌نظارت برچسب‌دار می‌شوند. آن‌ها یک شبکه عصبی روبه‌جلو SLFN را به‌منظور تولید خروجی بردار عضویت فازی آموزش دادند. طبقه‌بندی نمونه‌های بدون برچسب به کمک مقدار فازی انجام می‌شد. هدف از این روش بهبود صحت طبقه‌بند و کاهش نرخ هشدارهای نادرست بود[۳۳].

در سال ۲۰۱۷، Viegas و همکارانش یک روش تشخیص مبتنی بر بی‌نظمی قابل اعتماد را در محیط دنیای واقعی پیشنهاد کردند. آن‌ها یک روش جدید برای ایجاد پایگاه‌داده‌های نفوذ ارائه کردند. هدف آنها از اینکار به‌روزرسانی و تکثیر راحت پایگاه‌داده‌ها بود. آن‌ها یک روش انتخاب ویژگی چندهدفه ارائه کردند که خصوصیات شبکه دنیای واقعی را در نظر می‌گرفت. هدف از این روش بهبود صحت طبقه‌بند بود[۳۴].

۳ - ابزارها و روش‌ها

۳-۱- الگوریتم کلونی زنبور مصنوعی

در الگوریتم ABC، هر منبع غذا معادل یک راه‌حل در مسئله و مقدار شهد، معادل میزان برازندگی آن راه‌حل است. هر سیکل جستجو شامل سه مرحله می‌باشد. مرحله اول فرستادن زنبورهای کارگر به سوی منابع غذایی و محاسبه مقدار شهد آنها است. مرحله دوم به اشتراک گذاشتن اطلاعات مربوط به شهد منابع غذایی و انتخاب منبع غذا توسط زنبورهای ناظر و محاسبه مقدار شهد منابع است. مرحله سوم تعیین زنبورهای پیشاهنگ و فرستادن آنها به صورت تصادفی به سوی منابع غذایی ممکن می‌باشد. شکل ۱ مراحل اصلی الگوریتم ABC را نشان می‌دهد[۳۵].

1: Initialize Population
2: repeat
3: Place the employed bees on their food sources
4: Place the onlooker bees on the food sources depending on their nectar amounts
5: Send the scouts to the search area for discovering new food sources
6: Memorize the best food source found so far
7: until requirements are met

شکل۱. مراحل اصلی الگوریتم ABC

۳-۱-۱-فاز مقداردهی اولیه جمعیت

در این الگوریتم جمعیتی اولیه از راه‌حل‌های تصادفی به تعداد SN توسط رابطه (۱) تولید می‌شود به‌طوری‌که اندیس‌های $i \in \{1,2,\dots,SN\}$ و $j \in \{1,2,\dots,D\}$ و SN برابر با تعداد منابع غذایی و نیمی از سایز کلونی زنبور (CS) است. پارامتر D برابر با ابعاد مسئله می‌باشد و x_{max}^{j} و x_{min}^{j} حدود بالا و پایین متغیر j هستند. هر راه‌حل x_i، یک بردار D بعدی است. تعداد راه‌حل‌ها (SN) می‌تواند برابر با تعداد زنبورهای کارگر و زنبورهای ناظر باشد. در این فاز سه پارامتر SN، Limit و MCN مقداردهی اولیه می‌شوند و شهد جمعیت اولیه محاسبه می‌شود[۱۵].

x_i (۱)

۳-۱-۲-فاز زنبورهای کارگر

هر زنبور کارگر موقعیت خود را با توجه به اطلاعات محلی و مقدار برازندگی راه‌حل جدید، توسط رابطه (۲) به‌روزرسانی می‌کند به‌طوری که $k \in \{1,2,\dots,SN\}$ و $k \neq$ i و $j \in \{1,2,\dots,D\}$ اندیس‌های تصادفی هستند. φ_{ij} عددی تصادفی در بازه [1,1-] است. تابع φ_{ij} ، به تولید منبع غذایی جدیدِ v_{ij} در اطراف منبع قدیمیِ x_{ij} کمک می‌کند[۱۵].

$v_{}$ (۲)

۳-۱-۳-فاز زنبورهای ناظر

هر زنبور ناظر اطلاعات تمام زنبورهای کارگر را می‌گیرد و بهترین منبع را با توجه به برازندگی آن انتخاب می‌کند. زنبور ناظر منبع غذایی را با توجه به مقدار احتمال منبع انتخاب می‌کند که این احتمال با رابطه (۳) محاسبه می‌شود به‌طوری‌که در آن fit_i برازندگی راه‌حل iام است[۱۵، ۳۵].

$p_{}$ (۳)

۳-۱-۴-فاز زنبورهای پیشاهنگ

پس از مدتی شهد منابع غذایی تمام می‌شود، بنابراین آنها با منابع جدیدی که توسط زنبورهای پیشاهنگ مشخص می‌شود جایگزین می‌شوند. پارامتر Limit بیانگر تعداد سیکل‌هایی است که پس از آن زنبور کارگر منبع غذا را ترک می‌کند. منبع جدید توسط رابطه (۱) تولید می‌شود. ترک منبع باعث جلوگیری از بهینه محلی می‌شود. فاز زنبورهای کارگر، ناظر و پیشاهنگ به تعداد MCN تکرار می‌شود. در پایان بهترین راه‌حل در جمعیت مورد توجه قرار می‌گیرد. شکل ۲، شبه کد مربوط به الگوریتم ABC استاندارد است[۱۵، ۳۵].

1: Initialize the population of solutions x_i by (1), i=1, …, SN
2: Evaluate the population
3: cycle = 1
4: repeat
5: Produce new solutions v_i for the employed bees by using (2) and evaluate them.
6: Apply the greedy selection process for the employed bees
7: Calculate the probability values $Prob_i$ for the solutions x_i by (3)
8: Produce the new solutions v_i for the onlookers by (2) from the solutions x_i selected depending on $Prob_i$ and evaluate them.
9: Apply the greedy selection process for the onlookers
10: Determine the abandoned solution for the scout, if exists, and replace it with a new randomly produced solution x_i by (1)
11: Memorize the best solution achieved so far
12: cycle = cycle + 1
13: until cycle = MCN

شکل۲. شبه کد الگوریتم ABC استاندارد

۳-۲-پرواز لوی

قدم‌زدن تصادفی از طی‌کردن یک سری قدم‌های پیوسته و تصادفی تشکیل می‌شود. طول قدم‌ها می‌تواند ثابت یا متغیر باشد. جهت هر قدم مشابه طول آن می‌تواند متغیری از یک توزیع شناخته‌شده باشد. اگر طول هر قدم از توزیع لوی پیروی کند در اینصورت، قدم‌زدن تصادفی را پرواز لوی می‌نامند[۳۶، ۳۷]. تولید اعداد تصادفی به کمک پرواز لوی شامل دو مرحله می‌باشد: مرحله اول انتخاب جهت تصادفی و مرحله دوم تولید قدم‌هایی که طول آن از توزیع لوی تبعیت کند. توزیع لوی از رابطه (۴) تبعیت می‌کند که در آن β یک اندیس می‌باشد و S طول قدم است.

$L(S) \sim |S|^{-1-\beta}$ 0 (۴)

طول قدم S می‌تواند توسط الگوریتم مانتگنا رابطه (۵) محاسبه شود که در آن u و v دارای توزیع نرمال هستند که توسط روابط (۶) و (۷) محاسبه می‌شوند. طول قدم‌ها می‌تواند مثبت یا منفی باشد بنابراین اندازه قدم با رابطه (۸) محاسبه می‌شود.

$$S = \frac{u}{|v|^{\frac{1}{\beta}}} \quad (۵)$$

$$u \sim N(0,\sigma_u^2),\ v \sim N(0,\sigma_v^2) \quad (۶)$$

$$\sigma_u = \left(\frac{\Gamma(1+\beta)*\sin(\pi\beta/2)}{\Gamma[(1+\beta)/2]*\beta*2^{(\beta-1)/2}}\right)^{1/\beta},\ \sigma_v = 1 \quad (۷)$$

$$step\ size = 0.01 \times S \quad (۸)$$

فاکتور ۰/۰۱ از این واقعیت می‌آید که L/100 باید به اندازه قدم رایج در پیاده‌روی باشد که در آن L مقیاس طول رایج است در غیر این‌صورت، پرواز لوی بیش از حد تهاجمی می‌گردد[۳۸].

۴ - روش پیشنهادی

در روش ارائه‌شده تمرکز بر روی تکنیک انتخاب ویژگی مبتنی بر Wrapper با استفاده از الگوریتم ABC بهبودیافته و طبقه‌بند SVM با روش ارزیابی 10-fold است. هدف انتخاب ویژگی‌هایی است که صحت طبقه‌بند را بهبود بخشد. شکل۳ فلوچارت روش پیشنهادی را نمایش می‌دهد.

۴-۱-پیش‌پردازش

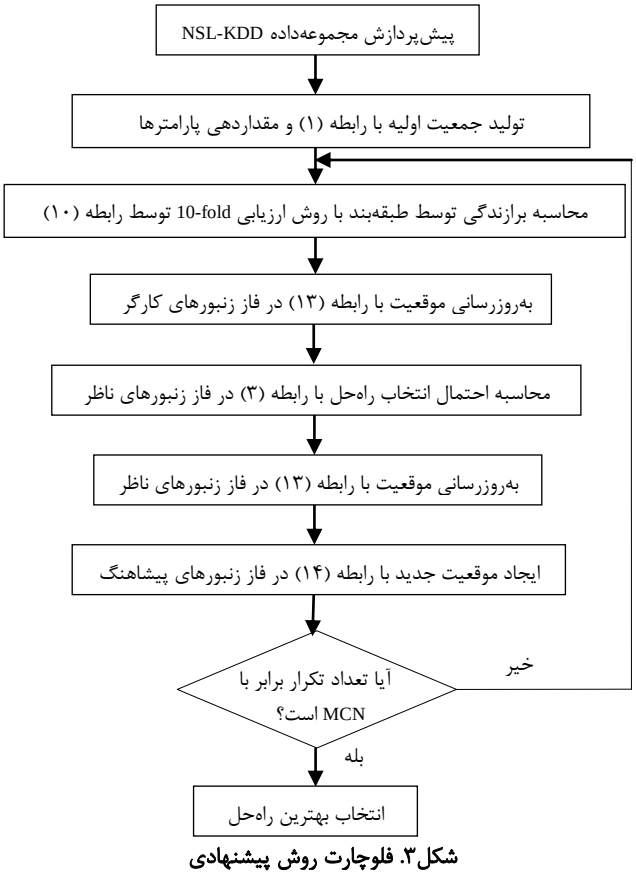
در فاز پیش‌پردازش از نرم‌افزار وکا به‌منظور کاهش ابعاد مسئله استفاده شد. تمام ویژگی‌ها در مجموعه‌داده NSL-KDD دارای اهمیت یکسانی نیستند، بنابراین با حذف ویژگی‌های نامربوط، تکراری و کم‌اهمیت ابعاد مسئله کاهش می‌یابد. بدین ترتیب که در فاز پیش‌پردازش سعی شد ویژگی‌های با اهمیت‌تر را از بین ۴۱ ویژگی استخراج کرد. در نتیجه فضای جستجوی کوچکتری را به‌عنوان ورودی به فرایند مدل پیشنهادی اعمال نمود. فیلترهای Relief و CFS بر روی مجموعه‌داده

NSL-KDD توسط نرم‌افزار وکا اعمال شد و فضای جستجو را کاهش داد. در ادامه بیشتر به آن می‌پردازیم.

۴-۲- تولید جمعیت اولیه و مقداردهی پارامترها

جمعیتی اولیه از راه‌حل‌های تصادفی به تعداد SN توسط رابطه (۱) تولید می‌شود. هر راه‌حل x_i، یک بردار D بعدی است که شامل مولفه‌های v_1، v_2، ... ، v_D می‌باشد که توسط رابطه (۹) نشان داده‌ایم. مقدار پارامتر D و مولفه‌های v_1، v_2، ... ، v_D می‌توانند در بازه اعداد صحیح [۱،۴۱] باشد زیرا در مجموعه‌داده NSL-KDD فقط ۴۱ ویژگی وجود دارد. پس از اعمال فیلتر توسط وکا تعداد ویژگی‌ها کاهش خواهد یافت و به‌همین ترتیب طول بازه نیز کاهش می‌یابد. پارامترهای SN، Limit وMCN در این فاز مقداردهی اولیه می‌شوند. پس از آن مقدار برازندگی جمعیت اولیه با رابطه (۱۰) محاسبه می‌شود.

$$x_i = \{v_1, v_2, v_3 \ldots, v_D\} \quad (۹)$$



شکل۳. فلوچارت روش پیشنهادی

۴-۳- محاسبه برازندگی

در این روش تابع برازندگی معادل با صحت طبقه‌بند SVM با روش ارزیابی 10-fold می‌باشد که مطابق رابطه (۱۰) حاصل می‌شود[۴].

$$Fitness = Accuracy = \frac{TN + TP}{TN + TP + FN + FP} \quad (۱۰)$$

۴-۴-به‌روزرسانی موقعیت

الگوریتم ABC یکی از متدهای معروف برای بهینه‌سازی مسائل پیوسته است. از نظر مفاهیم بهینه‌سازی، به تولید راه‌حل‌های جدید در مناطق ناشناخته، اکتشاف و به ایجاد بهبود در راه‌حل‌های بهینه در مناطق کشف‌شده، بهره‌برداری گویند. الگوریتمی بهینه است که بتواند بین اکتشاف و بهره‌برداری توازن ایجاد کند[۱۳، ۱۴]. الگوریتم ABC از نظر سادگی، انعطاف‌پذیری و مقاومت بر سایر الگوریتم‌ها برتری دارد. بعلاوه این الگوریتم نیاز به تنظیم پارامترهای آموزشی کمتری دارد، بنابراین به آسانی می‌توان آن را با سایر الگوریتم‌ها ترکیب نمود. الگوریتم ABC در فضای جستجو از نظر اکتشاف خوب است اما از نظر بهره‌برداری ضعیف است. در این الگوریتم اکتشاف وظیفه زنبورهای کارگر و ناظر و بهره‌برداری وظیفه زنبورهای پیشاهنگ می‌باشد[۱۵، ۳۵]. از معایب الگوریتم ABC می‌توان به نرخ همگرایی پایین، بهره‌برداری و مقداردهی اولیه ضعیف و تله بهینه محلی اشاره کرد[۱۴]. به‌منظور غلبه بر معایب الگوریتم ABC ، محققان تغییراتی را در روابط (۱) و (۲) ایجاد کردند. در سال ۲۰۱۴، Shan و همکارانش استراتژی جهش "DE/best/1" را با فرایند جستجوی غذا رابطه (۲) در الگوریتم ABC ترکیب کردند و معادله جستجوی جدیدی همانند رابطه (۱۱) را ایجاد کردند که در آن φ_{ij} عددی تصادفی در بازه [-1,1] است.

$$v_i \quad (۱۱)$$

در رابطه (۱۱) بهترین راه‌حل‌ها در جمعیت کنونی، باعث بهبود نرخ همگرایی می‌شود. الگوریتم DE یک الگوریتمِ کارا، قدرتمند، ساده و مبتنی بر جمعیت است. محققان گونه‌های متفاوتی از الگوریتم DE پیشنهاد دادند. یکی از این گونه‌ها که می‌تواند باعث تنوع در جمعیت شود روش "DE/best/1" می‌باشد. در الگوریتم DE، بهترین راه‌حل‌ها در جمعیت کنونی برای بهبود نرخ همگرایی مفید هستند. از طرفی معادله جستجوی غذا رابطه (۲) در الگوریتم ABC، مشابه فرایند جهش در الگوریتم DE می‌باشد[۱۴]. این موارد دلایلی است که آنها استراتژی جهش "DE/best/1" را با فرایند جستجوی غذا رابطه (۲) در الگوریتم ABC ترکیب کردند.

در سال ۲۰۱۶، Bharti و همکارش، اطلاعات بهترین راه‌حل سراسری را در رابطه (۲) مشارکت دادند تا فرایند جستجو به سمت بهترین راه‌حل سراسری حرکت کند. آن‌ها از معادله جستجوی الگوریتم PSO و از مزیت بهترین راه‌حل سراسری در GABC استفاده کردند تا جستجو توسط راه‌حل‌های کاندید هدایت شود. آن‌ها رابطه (۲) را به رابطه (۱۲) تغییر دادند تا بهره‌برداری در این الگوریتم بهبود یابد. به‌طوری‌که Φ_{ij} عددی تصادفی در بازه [-1,1] و ψ_{ij} عددی تصادفی با توزیع یکنواخت در بازه [0,C] می‌باشد و C>0 است.

$$v_i \quad (۱۲)$$

بعلاوه Bharti و همکارش متوجه بودند که رابطه (۲) در الگوریتم استاندارد ABC متأثر از کمیت‌های تصادفی است. موقعیت هر راه‌حل

توسط همسایه تصادفی‌اش به‌روزرسانی می‌شود. اگرچه یک عامل تصادفی، برای اکتشاف خوب است اما برای بهره‌برداری ناکارامد است[۱۴، ۱۵]. این موارد دلایلی است که آنها رابطه (۲) را به رابطه (۱۲) تغییر دادند.

در این کار پژوهشی، تلاش شد که به‌طور همزمان از مزیت بهترین راه‌حل در جمعیت کنونی و اطلاعات بهترین راه‌حل سراسری استفاده شود. به همین منظور روابط (۱۱) و (۱۲) با هم ترکیب شد و رابطه جدید (۱۳) برای جستجو ایجاد گردید. سپس احتمال برازندگی راه‌حل‌ها با رابطه (۳) محاسبه می‌شود.

v_i (۱۳)

انتخاب ویژگی یک مسئله بهینه‌سازی گسسته می‌باشد و الگوریتم ABC یک مسئله بهینه‌سازی پیوسته می‌باشد. سوالی که مطرح می‌شود این است که چطور ما این دو نوع مسئله را به یکدیگر تبدیل کرده‌ایم؟ در فاز شبیه‌سازی برای تبدیل فضای پیوسته به فضای گسسته از تابع round() در متلب استفاده شد. از طرفی برای تبدیل فضای گسسته به فضای پیوسته از توابع rand()، unifrnd() و randn() استفاده شد.

۴-۵-ایجاد موقعیت جدید

برای ایجاد توازن بین اکتشاف و بهره‌برداری، بهتر است که الگوریتم ABC با نوعی جستجوی محلی ترکیب شود. این ترکیب در جهت بهبود بهره‌برداری، افزایش نرخ همگرایی و ایجاد تنوع در جمعیت کمک می‌کند[۶، ۱۲]. بدین منظور در این کار پژوهشی از پرواز لوی در ایجاد موقعیت جدید برای زنبورهای پیشاهنگ استفاده شد.

توزیع لوی از فرمول توانی رابطه (۴) تبعیت می‌کند. طول قدم S توسط رابطه (۵) محاسبه می‌شود. ایجاد موقعیت جدید برای زنبورهای پیشاهنگ توسط رابطه (۱۴) محاسبه می‌شود.

$$x_{i\,j}^{t+1} = x_{i\,j}^{t} + \propto \oplus\, levy(\beta) \quad (۱۴)$$

به‌طوری‌که $i \in \{1,2,\dots,SN\}$ و $j \in \{1,2,\dots,D\}$ اندیس‌های تصادفی هستند. $\propto$ عددی با توزیع یکنواخت در بازه (0,1) می‌باشد. پارامتر t بیانگر تعداد تکرار و عملگر $\oplus$ بیانگر xor است. مقدار $levy(\beta)$ توسط رابطه (۱۵) محاسبه می‌شود[۱۴، ۳۸].

L_i (۱۵)

در ادامه، بهترین راه‌حل در جمعیت کنونی در حافظه ذخیره می‌شود. شرط حلقه بررسی می‌شود و در صورت عدم برقراری شرط، فرایند از فاز زنبورهای کارگر آغاز می‌شود. این فرایند همچنان تکرار می‌شود تا زمانیکه تعداد تکرار برابر با MCN شود. پس از اتمام حلقه تکرار، بهترین راه‌حل سراسری انتخاب می‌شود.

۴-۶-روال الگوریتم روش پیشنهادی

در ابتدا جمعیتی تصادفی با رابطه (۱) ایجاد می‌شود. زنبورهای کارگر، موقعیت هر راه‌حل را با رابطه (۱۳) به‌روزرسانی می‌کنند و برازندگی راه‌حل را با رابطه (۱۰) محاسبه می‌کنند. اگر کیفیت راه‌حل در موقعیت جدید v_{ij} بهتر از موقعیت قبلی x_{ij} شد، موقعیت راه‌حل جدید را در نظر می‌گیرند در غیر این‌صورت، موقعیت قبلی را به خاطر می‌سپارند. این روند برای همه راه‌حل‌ها تکرار می‌شود. سپس احتمال انتخاب راه‌حل توسط رابطه (۳) در فاز زنبورهای ناظر محاسبه می‌شود.

زنبورهای ناظر، مقدار برازندگی که توسط زنبورهای کارگر محاسبه می‌شود را ترجیح می‌دهند. هر چه مقدار برازندگی راه‌حل‌ها بیشتر باشد احتمال انتخاب بیشتر می‌گردد. زنبورهای ناظر پس از انتخاب یک راه‌حل، راه‌حل جدیدی را در مجاورت راه‌حل منتخب با رابطه (۱۳) تولید می‌کنند. سپس برازندگی موقعیت جدید را با موقعیت قبلی مقایسه می‌کند. اگر کیفیت راه‌حل در موقعیت جدید v_{ij} بهتر از موقعیت قبلی x_{ij} شد، موقعیت راه‌حل جدید را در نظر می‌گیرند در غیر این‌صورت، موقعیت قبلی را به خاطر می‌سپارند.

اگر منبعی توسط زنبورهای کارگر تمام شد، یک راه‌حل جدید تصادفی توسط رابطه (۱۴) تولید می‌شود. در هر سیکل، تعدادی زنبور پیشاهنگ که متناظر با پارامتر Limit است، برای اکتشاف راه‌حل جدید به محیط فرستاده می‌شود. در هر تکرار، الگوریتم بهترین راه‌حل جمعیت را به خاطر می‌سپارد و تکرار بعدی را از فاز زنبورهای کارگر شروع می‌کند. فرایند تکرار می‌شود تا زمانیکه تعداد تکرار برابر با MCN شود. شبه کد الگوریتم کلونی زنبور مصنوعی بهبودیافته توسط شکل۴ ارائه شده است. روش پیشنهادی Levy_DE_GABC_SVM نامگذاری شد.

1: Initialize the population of solutions x_i by (1), i=1, …, SN
2: Evaluate the population by (10)
3: cycle = 1
4: repeat
(Exploration phase)
5: Produce new solutions v_i for the employed bees by using (13) and evaluate them by (10)
6: Apply the greedy selection process for the employed bees
7: Calculate the probability values $Prob_i$ for the solutions x_i by (3)
8: Produce the new solutions v_i for the onlookers by (13) from the solutions x_i selected depending on $Prob_i$ and evaluate them by (10)
9: Apply the greedy selection process for the onlookers
(Exploitation phase)
10: Determine the abandoned solution for the scout, if exists, and replace it with a new randomly produced solution x_i by (14)
11: Memorize the best solution achieved so far
12: cycle = cycle + 1
13: until cycle = MCN

شکل۴. شبه کد الگوریتم ABC بهبودیافته

۵ - آزمایشات

در این بخش روال پیاده‌سازی مدل پیشنهادی توضیح داده می‌شود که در آن از معیار ارزیابی صحت طبقه‌بند رابطه (۱۰) استفاده شد. در این بخش مدل پیشنهادی Levy_DE_GABC_SVM، مدل پایه ABC_SVM و مدل SVM شبیه‌سازی شد و نتایج آنها با یکدیگر مقایسه می‌شود. در این تحقیق ملاک ارزیابی، محاسبه میانگین صحت طبقه‌بند و محاسبه میانگین زمان محاسبات است.

۵-۱-مجموعه‌داده NSL-KDD

مجموعه‌داده KDD99 یک مجموعه‌داده استاندارد برای IDS می‌باشد. بیشتر محققین کانون فعالیت خود را بر روی فیلدهای KDD99 متمرکز کرده‌اند و معیارهای آنها در تحقیقاتشان دقت، صحت، نرخ تشخیص و نرخ هشدارهای نادرست بوده است. در این تحقیق از نسخه اصلاح‌شده مجموعه‌داده KDD99 استفاده شده است که مجموعه‌داده NSL-KDD نامیده می‌شود. مجموعه‌داده NSL-KDD شامل دو کلاس اصلی نرمال و حمله است. کلاس حمله خود شامل چهار زیر کلاس DoS، R2L، U2R، Probe می‌باشد. بنابراین مجموعه‌داده NSL-KDD یک مسئله پنج‌کلاسی نیز محسوب می‌شود. مجموعه‌داده NSL-KDD دارای ۴۱ ویژگی می‌باشد[۲۶، ۳۹].

۵-۲-پیش‌پردازش مجموعه‌داده NSL-KDD

در گام اول اسامی ۴۱ ویژگی مجموعه‌داده به برچسب‌هایی با اسامی ساده‌تر تغییر داده شد. در گام دوم به‌منظور استفاده از ماشین بردار پشتیان، مقادیر رشته‌ای فیلدها به مقادیر عددی تبدیل شد. در این تحقیق، طبقه‌بندی هم برای مسئله دوکلاسی و هم برای مسئله پنج‌کلاسی انجام می‌شود. بنابراین در گام سوم فیلد ۴۲ که نوع کلاس را نمایش می‌دهد بسته به نوع مسئله برچسب‌گذاری شد. مجموعه‌داده NSL-KDD شامل ۱۲۵۹۷۳ رکورد و ۴۱ ویژگی می‌باشد. در گام چهارم برای کاهش مقدار حافظه مصرفی و زمان محاسبات، ۱۰ درصد از کل داده‌ها به‌صورت تصادفی انتخاب گردید. توصیفی آماری از مجموعه‌داده در جدول ۱ ارائه شده است.

جدول ۱. توصیفی آماری از مجموعه‌داده در آزمایشات

مجموعه‌داده	NSL-KDD	
	100% NSL-KDD	10% NSL-KDD
تعداد کلاس	یک کلاس نرمال ، چهار کلاس حمله	
تعداد ویژگی	۴۱	۴۱
تعداد نمونه	۱۲۵۹۷۳	۱۲۷۰۴

در گام پنجم ابعاد مسئله کاهش یافت. فیلترهای Relief و CFS، توسط نرم‌افزار وکا بر روی مجموعه‌داده NSL-KDD اعمال شد. با اعمال فیلتر CFS، ویژگی‌هایی که هیچ ارتباطی با هم ندارند حذف می‌شوند. پس از اعمال فیلتر CFS بر روی ویژگی‌های مجموعه‌داده NSL-KDD مطابق جدول ۲، فقط ۷ویژگی در حالت دوکلاسی و ۵ ویژگی در حالت پنج‌کلاسی باقی می‌ماند و بقیه حذف می‌شوند. توصیفی آماری از مجموعه‌داده پس از اعمال فیلتر توسط وکا در جدول ۲ ارائه شد.

جدول۲ . توصیفی آماری از مجموعه‌داده پس از فیلترتوسط وکا

پالایش با وکا	روش CFS		روش Relief	
تعداد کلاس	normal, attack	DoS,R2L,U2R, Probing,normal	normal, attack	DoS,R2L,U2R, Probing,normal
تعداد ویژگی پس از کاهش بعد	۷	۵	۳۰	۳۱
تعداد نمونه پس از پیش‌پردازش	۵۲۸۴	۲۶۷۲	۱۲۴۳۹	۱۲۶۵۸

با اعمال فیلتر Relief توسط وکا، ویژگی‌هایی که نمی‌توانند کلاسهای مختلف را از همدیگر جدا کنند حذف می‌شوند. پس از اعمال فیلتر Relief بر روی ویژگی‌های مجموعه‌داده NSL-KDD مطابق جدول ۲ فقط ۳۰ ویژگی در حالت دوکلاسی و ۳۱ ویژگی در حالت پنج‌کلاسی باقی می‌ماند و بقیه حذف می‌شوند.

پس از اعمال فیلتر، باقیمانده ویژگی‌ها به‌عنوان ورودی به فرایند مدل پیشنهادی اعمال می‌شوند. لیستی از ویژگی‌های باقیمانده پس از اعمال فیلتر در جدول۳ ارائه شده است.

جدول۳ . لیستی از ویژگی‌های باقیمانده پس از اعمال فیلتر

تعداد ویژگی	ویژگی‌های باقیمانده	روش فیلتر
۷	۸، ۱۲، ۲۹، ۳۳، ۳۴، ۳۵، ۳۹	روش CFS دوکلاسی
۵	۸، ۱۲، ۲۹، ۳۳، ۳۹	روش CFS پنج‌کلاسی
۳۰	۱، ۲، ۳، ۴، ۶، ۷، ۸، ۹، ۱۰، ۱۱، ۱۲، ۱۴، ۱۵، ۱۸، ۲۳، ۲۷، ۲۸، ۲۹، ۳۰، ۳۱، ۳۲، ۳۳، ۳۴، ۳۵، ۳۶، ۳۷، ۳۸، ۳۹، ۴۰، ۴۱	روش Relief دوکلاسی
۳۱	۱، ۲، ۳، ۴، ۵، ۷، ۸، ۱۰، ۱۱، ۱۲، ۱۴، ۲۲، ۲۳، ۲۴، ۲۵، ۲۶، ۲۷، ۲۸، ۲۹، ۳۰، ۳۱، ۳۲، ۳۳، ۳۴، ۳۵، ۳۶، ۳۷، ۳۸، ۳۹، ۴۰، ۴۱	روش Relief پنج‌کلاسی

۵-۳-معیار ارزیابی کارایی

کارایی یک IDS با توانایی آن در تولید پیش‌بینی‌های صحیح ارزیابی می‌شود. با مقایسه ماهیت واقعی یک رویداد و پیش‌بینی یک IDS، چهار پیامد TP، FP، FN، TN ممکن است رخ دهد. مدیران امنیتی به‌دنبال کاهش هشدارهای نادرست و افزایش تاییدهای نادرست هستند. در این تحقیق از معیار کارایی صحت طبقه‌بند، رابطه (۱۰) استفاده شد[۱۰].

۵-۴-پیکربندی محیط آزمایش

برای شبیه‌سازی الگوریتم ABC از زبان برنامه‌نویسی MatLab و LibSvm استفاده شد. در شبیه‌سازی، طبقه‌بندی مجموعه‌داده NSL-KDD در دو حالت دوکلاسی و پنج‌کلاسی انجام می‌شود.

نحوه تنظیم پارامترهای مورد استفاده در شبیه‌سازی، بر اساس سایر مقالات، روش GridSearch و نهایتاً مشخصات سخت‌افزاری می‌باشد. مقادیر پارامترهای مورد استفاده در شبیه‌سازی در جدول ۴ ارائه شده است. برخی از پارامترها همانند Φ، ψ و β بر اساس سایر مقالات تنظیم شده است[۱۴، ۱۵، ۳۸]. برای تنظیم سایر پارامترها همانند CS، MCN، Limit و MaxIter از الگوریتم GridSearch استفاده شد. روش GridSearch یک‌بازه‌ای از مقادیر مختلف را برای هر پارامتر لحاظ می‌کند و آزمایشات را با مقادیر بازه تکرار می‌کند تا بهترین تنظیم را برای هر پارامتر بیابد. برای تنظیم پارامتر MaxIter چون با ۴ بار تکرار نتایج مناسبی حاصل شد به همان مقدار اکتفا شد.

برای به‌کارگیری طبقه‌بند SVM بایستی نوع هسته مشخص گردد. در این شبیه‌سازی از دو هسته RBF و Sigmoid با روابط ریاضی (۱۶) و (۱۷) استفاده شد.

در زمان استفاده از هسته‌ها باید پارامترهای آن تنظیم شود. پارامترهای هسته در روابط (۱۶) و (۱۷) gamma ، coef0 و C می‌باشند که آنها از مقادیر استانداردی استفاده کردند که در مقالات دیگر استفاده شده است.

$$\text{RBF kernel} : \exp(-\text{gamma}*|u-v|^2) \quad (16)$$

$$\text{Sigmoid kernel} : \tanh(\text{gamma}*u'*v + \text{coef0}) \quad (17)$$

جدول ۴. پارامترهای مورد استفاده در شبیه‌سازی

عنوان پارامتر	نماد	مقادیر	
		آزمایشات مرحله اول	آزمایشات مرحله دوم
سایز کلونی زنبور	CS	۱۰	۱۰
تعداد منابع غذایی یا تعداد راه‌حل‌ها	NF or NS	۵	۵
تعداد سیکل در ABC	MCN	۲	۲۰
تعداد سیکل‌های منجر شده به ترک منبع غذایی	Limit	۱	۳
عددی در بازه [-1,1]	Φ	تصادفی	تصادفی
عددی با توزیع یکنواخت در	ψ	تصادفی	تصادفی
مقدار β در پرواز لوی	β	۱/۵	۱/۵
نوع هسته در طبقه‌بند	kernel	rbf , sigmoid	rbf
تعداد ویژگی در هر راه‌حل	Dimension	۵ و ۱۰ و ۱۵	۵ و ۱۰ و ۱۵
نوع مسئله ورودی طبقه‌بند	Number of Class	۲ و ۵	۲ و ۵
ماکزیمم تعداد تکرار آزمایشات	MaxIter	۴	۴

این مقادیر از طریق تنظیمات پیش فرض LibSvm قابل دسترسی هستند که gamma = 1/num_features و coef0=0 و C=1 در نظر گرفته شده است.

در روش پیشنهادی ما برای انتخاب ویژگی از دو روش فیلتر و Wrapper استفاده شد. روش‌های پالایش همانند CFS و Relief توسط نرم‌افزار وکا در مرحله پیش‌پردازش انجام شد و هدف از آن کاهش فضای جستجو بود. پس از کاهش فضای جستجو از تکنیک انتخاب ویژگی مبتنی بر Wrapper با استفاده از الگوریتم ABC بهبودیافته و طبقه‌بند SVM استفاده شد.

قابل ذکر است که در کار پژوهشی ما سه مدل SVM، ABC_SVM و Levy_DE_GABC_SVM طی دو مرحله از آزمایشات شبیه‌سازی می‌شود. سپس نتایج آنها به‌طور مجزا نمایش داده شد و در نهایت با نتایج سایر مقالات در شرایط یکسان ارزیابی مطابق جدول ۱۷ مقایسه می‌شود.

در مدل SVM برای انتخاب ویژگی فقط از روش پالایش استفاده شد اما در دو مدل ABC_SVM و Levy_DE_GABC_SVM برای انتخاب بهترین ۵ ویژگی، ۱۰ ویژگی و ۱۵ ویژگی از هر دو روش پالایش و Wrapper کمک گرفته‌ایم.

۵-۴-۱-آزمایشات مرحله اول

آزمایشات مرحله اول به‌طور خاص با مقادیر CS=10، MCN=2، Limit=1 و Maxiter=4 به‌همراه سایر مقادیر جدول ۴ انجام شد.

۵-۴-۱-۱- به‌کارگیری فیلتر Relief

با اعمال فیلتر Relief توسط وکا بر روی مجموعه‌داده NSL-KDD فقط ۳۰ و ۳۱ ویژگی مطابق جدول ۲ انتخاب شد. پس از آن سه مدل Levy_DE_GABC_SVM، ABC_SVM و SVM بر روی ۳۰ویژگی و ۳۱ویژگی اعمال شد که در ادامه به ترتیب خواهیم دید.

در مدل‌های Levy_DE_GABC_SVM و ABC_SVM از هر دو روش پالایش و Wrapper برای انتخاب ویژگی استفاده شد. به‌عبارت دیگر در این دو مدل، پس از اعمال فیلتر Relief توسط وکا، از تکنیک انتخاب ویژگی مبتنی بر Wrapper با استفاده از الگوریتم ABC بهبودیافته و طبقه‌بند SVM استفاده شد. در این مدل‌ها طی دو مرحله آزمایش، میانگین صحت طبقه‌بند و میانگین زمان محاسبات با روش ارزیابی 10-fold محاسبه شد.

اما در مدل SVM فقط از روش پالایش استفاده شد و روش Wrapper نداشته‌ایم. در این مدل نیز میانگین صحت طبقه‌بند و میانگین زمان محاسبات با روش ارزیابی 10-fold محاسبه شد.

۵-۴-۱-۲- نتایج شبیه‌سازی مدل Levy_DE_GABC_SVM

این آزمایشات با هدف انتخاب بهترین ۵ ویژگی، ۱۰ ویژگی و ۱۵ ویژگی از بین ۳۰ و ۳۱ ویژگی توسط مدل پیشنهادی صورت گرفت. این آزمایشات با دو هسته RBF و Sigmoid در دو حالت دوکلاسی و

پنج‌کلاسی انجام شد. روش ارزیابی طبقه‌بند 10-fold می‌باشد. میانگین صحت طبقه‌بند در ۴ بار تکرار به‌روش 10-fold مطابق جدول ۵ ارائه شد. بیشترین میانگین صحت با مقدار ۹۷/۷۳ درصد مربوط به انتخاب بهترین ۱۵ ویژگی با هسته RBF در حالت پنج‌کلاسی و کمترین میانگین صحت با مقدار ۹۴/۲۴ درصد مربوط به انتخاب بهترین ۵ ویژگی با هسته RBF در حالت دوکلاسی می‌باشد.

جدول ۵. تأثیر انتخاب ویژگی بر صحت در مدل پیشنهادی

ارزیابی به‌روش 10-fold با طبقه‌بند SVM				
Evaluator:Relief		Levy_DE_GABC_SVM		
Search:Ranker		تعداد ویژگی		
تعداد کلاس	هسته	۵	۱۰	۱۵
۲	RBF	۹۴/۲۴	۹۷/۴۳	۹۷/۴۱
	Sigmoid	۹۵/۸۸	۹۷/۵۹	۹۷/۶۷
۵	RBF	۹۴/۹۷	۹۷/۱۷	۹۷/۷۳
	Sigmoid	۹۵/۷۱	۹۶/۸۹	۹۷/۲۸

در تمام آزمایشات مدل پیشنهادی، میانگین زمان محاسبات طبقه‌بند در ۴ بار تکرار آزمایشات به‌روش 10-fold مطابق جدول ۶ ارائه شد. بیشترین زمان محاسبات با مقدار ۴۰۵۵/۹۵ ثانیه مربوط به انتخاب بهترین ۱۵ ویژگی با هسته Sigmoid در حالت پنج‌کلاسی و کمترین زمان محاسبات با مقدار ۷۳۴/۷۳ ثانیه مربوط به انتخاب بهترین ۵ ویژگی با هسته Sigmoid در حالت پنج‌کلاسی می‌باشد.

جدول ۶. تأثیر انتخاب ویژگی بر زمان محاسبات در مدل پیشنهادی

میانگین زمان محاسبات (ثانیه)				
ارزیابی به‌روش 10-fold با طبقه‌بند SVM				
Evaluator:Relief		Levy_DE_GABC_SVM		
Search:Ranker		تعداد ویژگی		
تعداد کلاس	هسته	۵	۱۰	۱۵
۲	RBF	۷۴۸/۶۲	۱۳۷۶/۶۱	۲۷۸۰/۴۲
	Sigmoid	۶۴۵/۲۳	۱۳۶۰/۱۷	۲۷۳۷/۳۶
۵	RBF	۱۳۳۳/۱۸	۱۷۸۴/۹۸	۳۳۸۷/۱۷
	Sigmoid	۷۳۴/۷۳	۱۶۵۷/۸۵	۴۰۵۵/۹۵

۵-۴-۱-۳- نتایج شبیه‌سازی مدل ABC_SVM

این آزمایشات با هدف انتخاب بهترین ۵ ویژگی، ۱۰ ویژگی و ۱۵ ویژگی از بین ۳۰ و ۳۱ ویژگی توسط مدل پایه صورت گرفت. این آزمایشات با دو هسته RBF و Sigmoid در دو حالت دوکلاسی و پنج‌کلاسی انجام شد. روش ارزیابی طبقه‌بند 10-fold می‌باشد. میانگین صحت طبقه‌بند در ۴ بار تکرار آزمایشات به‌روش 10-fold مطابق جدول ۷ ارائه شد. بیشترین میانگین صحت با مقدار۹۸/۱۰ درصد مربوط به انتخاب بهترین ۱۰ ویژگی با هسته RBF در حالت پنج‌کلاسی و کمترین، میانگین صحت با مقدار ۹۵/۰۶ درصد مربوط به انتخاب بهترین ۵ ویژگی با هسته Sigmoid در حالت پنج‌کلاسی می‌باشد.

جدول ۷. تأثیر انتخاب ویژگی بر صحت در مدل پایه

ارزیابی به‌روش 10-fold با طبقه‌بند SVM				
Evaluator:Relief		ABC_SVM		
Search:Ranker		تعداد ویژگی		
تعداد کلاس	هسته	۵	۱۰	۱۵
۲	RBF	۹۵/۴۵	۹۷/۴۵	۹۷/۷۲
	Sigmoid	۹۵/۳۰	۹۷/۵۲	۹۷/۰۱
۵	RBF	۹۶/۱۲	۹۸/۱۰	۹۷/۷۹
	Sigmoid	۹۵/۰۶	۹۷/۱۴	۹۷/۴۵

جدول ۸. تأثیر انتخاب ویژگی بر زمان محاسبات در مدل پایه

میانگین زمان محاسبات (ثانیه)				
ارزیابی به‌روش 10-fold با طبقه‌بند SVM				
Evaluator:Relief		ABC_SVM		
Search:Ranker		تعداد ویژگی		
تعداد کلاس	هسته	۵	۱۰	۱۵
۲	RBF	۷۸۷/۹۹	۱۴۳۸/۲۴	۲۴۵۳/۴۴
	Sigmoid	۷۳۴/۵۶	۱۴۶۰/۱۵	۲۱۸۴/۱۸
۵	RBF	۷۸۶/۳۶	۲۰۶۳/۰۹	۳۱۶۷/۲۲
	Sigmoid	۷۰۴/۰۶	۲۳۷۰/۲۸	۲۹۵۵/۹۴

در تمام آزمایشات مدل پایه، میانگین زمان محاسبات طبقه‌بند در ۴ بار تکرار به‌روش 10-fold مطابق جدول ۸ ارائه شد. بیشترین زمان محاسبات با مقدار ۳۱۶۷/۲۲ ثانیه مربوط به انتخاب بهترین ۱۵ویژگی با هسته RBF در حالت پنج‌کلاسی و کمترین زمان محاسبات با مقدار ۷۰۴/۰۶ ثانیه مربوط به انتخاب بهترین ۵ ویژگی با هسته Sigmoid در حالت پنج‌کلاسی می‌باشد.

۵-۴-۱-۴- نتایج شبیه‌سازی مدل SVM بدون استفاده ABC و با فیلتر Relief

این آزمایشات با هدف محاسبه میانگین صحت و میانگین زمان محاسبات طبقه‌بند توسط مدل SVM بر روی ۳۰ و ۳۱ ویژگی صورت گرفت. این آزمایشات با دو هسته RBF و Sigmoid در دو حالت دوکلاسی و پنج‌کلاسی انجام شد. روش ارزیابی طبقه‌بند 10-fold می‌باشد.

میانگین صحت طبقه‌بند مطابق جدول ۹ ارائه شد. بیشترین میانگین صحت با مقدار ۹۴/۴۲ درصد مربوط به هسته Sigmoid در حالت دوکلاسی و کمترین میانگین صحت با مقدار ۹۲/۰۴ درصد مربوط به هسته Sigmoid در حالت پنج‌کلاسی می‌باشد.

جدول ۹. نتایج صحت در مدل SVM بدون ABC و با فیلتر Relief

ارزیابی به‌روش 10-fold با طبقه‌بند SVM

Evaluator:Relief, Search:Ranker			
SVM	هسته	تعداد ویژگی	تعداد کلاس
۹۴/۳۷	RBF	۳۰	۲
۹۴/۴۲	Sigmoid		
۹۲/۰۶	RBF	۳۱	۵
۹۲/۰۴	Sigmoid		

در تمام آزمایشات مدل SVM ، میانگین زمان محاسبات طبقه‌بند در ۴ بار تکرار آزمایشات به‌روش 10-fold مطابق جدول ۱۰ ارائه شد. بیشترین زمان محاسبات با مقدار ۳۳۱/۷۲ ثانیه مربوط به هسته Sigmoid در حالت پنج‌کلاسی و کمترین زمان محاسبات با مقدار ۲۱۹/۰۷ ثانیه مربوط به هسته RBF در حالت دوکلاسی می‌باشد.

جدول ۱۰. زمان محاسبات در مدل SVM بدون ABC و با فیلتر Relief

میانگین زمان محاسبات (ثانیه)			
ارزیابی به‌روش 10-fold با طبقه‌بند SVM			
Evaluator:Relief, Search:Ranker			
SVM	هسته	تعداد ویژگی	تعداد کلاس
۲۱۹/۰۷	RBF	۳۰	۲
۲۲۱/۴۲	Sigmoid		
۳۲۹/۹۱	RBF	۳۱	۵
۳۳۱/۷۲	Sigmoid		

۵-۴-۱-۵- به‌کارگیری فیلتر CFS

با اعمال فیلتر CFS توسط وکا بر روی مجموعه‌داده NSL-KDD فقط ۵ و ۷ ویژگی مطابق جدول ۲ انتخاب شد. بنابراین فقط می‌توان مدل SVM را بر روی ۵ ویژگی و ۷ ویژگی اعمال کرد. در مدل SVM فقط از روش فیلتر استفاده شده و روش Wrapper نداشته‌ایم. در این مدل نیز میانگین صحت طبقه‌بند و میانگین زمان محاسبات با روش ارزیابی 10-fold محاسبه گردید.

۵-۴-۱-۶- نتایج شبیه‌سازی مدل SVM بدون استفاده ABC و با فیلتر CFS

این آزمایشات با هدف محاسبه میانگین صحت و میانگین زمان محاسبات طبقه‌بند توسط مدل SVM بر روی ۵ و ۷ ویژگی صورت گرفت. این آزمایشات با دو هسته RBF و Sigmoid در دو حالت دوکلاسی و پنج‌کلاسی انجام شد. روش ارزیابی طبقه‌بند 10-fold می‌باشد. میانگین صحت طبقه‌بند در ۴ بار تکرار آزمایشات مطابق جدول ۱۱ ارائه شد. بیشترین میانگین صحت با مقدار ۸۳/۶۴ درصد مربوط به هسته Sigmoid در حالت دوکلاسی و کمترین میانگین صحت با مقدار ۷۳/۰۷ درصد مربوط به هسته RBF در حالت پنج‌کلاسی می‌باشد.

جدول ۱۱. تأثیر انتخاب ویژگی بر صحت طبقه‌بند در مدل SVM بدون ABC و با فیلتر CFS

ارزیابی به‌روش 10-fold با طبقه‌بند SVM			
Evaluator: CFS , Search:GreedyStepwise			
SVM	هسته	تعداد ویژگی	تعداد کلاس
۸۳/۶۳	RBF	۷	۲
۸۳/۶۴	Sigmoid		
۷۳/۰۷	RBF	۵	۵
۷۳/۱۸	Sigmoid		

در تمام آزمایشات مدل SVM ، میانگین زمان محاسبات طبقه‌بند در ۴ بار تکرار مطابق جدول ۱۲ ارائه شد. بیشترین زمان محاسبات با مقدار ۵/۸۱ ثانیه مربوط به هسته Sigmoid در حالت دوکلاسی و کمترین زمان محاسبات با مقدار ۲/۴۲ ثانیه مربوط به هسته RBF و Sigmoid در حالت پنج‌کلاسی می‌باشد.

جدول ۱۲. تأثیر انتخاب ویژگی بر زمان محاسبات طبقه‌بند در مدل SVM بدون ABC و با فیلتر CFS

میانگین زمان محاسبات (ثانیه)			
ارزیابی به‌روش 10-fold با طبقه‌بند SVM			
Evaluator: CFS , Search:GreedyStepwise			
SVM	هسته	تعداد ویژگی	تعداد کلاس
۵/۷۹	RBF	۷	۲
۵/۸۱	Sigmoid		
۲/۴۲	RBF	۵	۵
۲/۴۲	Sigmoid		

۵-۴-۲-آزمایشات مرحله دوم

آزمایشات مرحله دوم به‌طور خاص با مقادیر CS=10، MCN=20، Limit=3 و Maxiter=4 به‌همراه سایر مقادیر جدول ۴ انجام شد. افزایش مقادیر پارامترها در مدل پیشنهادی و مدل پایه تأثیر به‌سزایی در افزایش میانگین صحت و میانگین زمان محاسبات داشته است. در آزمایشات مرحله دوم فقط دو مدل Levy_DE_GABC_SVM، ABC_SVM بر روی خروجی حاصل از فیلتر Relief یعنی ۳۰ ویژگی و ۳۱ ویژگی اعمال شد که در ادامه به‌ترتیب خواهیم دید.

۵-۴-۲-۱- نتایج مدل Levy_DE_GABC_SVM با تنظیم پارامترها

این آزمایشات با هدف انتخاب بهترین ۵ ویژگی، ۱۰ ویژگی و ۱۵ ویژگی از بین ۳۰ و ۳۱ ویژگی توسط مدل پیشنهادی تکرار شد. این آزمایشات فقط با هسته RBF در دو حالت دوکلاسی و پنج‌کلاسی انجام شد. روش ارزیابی طبقه‌بند 10-fold می‌باشد. میانگین صحت طبقه‌بند در ۴ بار تکرار آزمایشات به‌روش 10-fold مطابق جدول ۱۳ ارائه شد. در مدل پیشنهادی در انتخاب بهترین ۱۵ویژگی با هسته RBF در حالت پنج‌کلاسی میانگین صحت به مقدار ۹۸/۹۷ درصد افزایش یافته است.

جدول ۱۳. تأثیر انتخاب ویژگی بر صحت مدل پیشنهادی با تنظیم پارامترها

ارزیابی به‌روش 10-fold با طبقه‌بند SVM

Evaluator:Relief		Levy_DE_GABC_SVM		
Search:Ranker		تعداد ویژگی		
تعداد کلاس	هسته	۵	۱۰	۱۵
۲	RBF	۹۸/۰۳	۹۸/۰۸	۹۸/۱۱
۵	RBF	۹۸/۳۴	۹۸/۸۶	۹۸/۹۷

در تمام آزمایشات مدل پیشنهادی، میانگین زمان محاسبات طبقه‌بند در ۴ بار تکرار به‌روش 10-fold مطابق جدول ۱۴ ارائه شد. در مدل پیشنهادی در انتخاب بهترین ۱۵ویژگی با هسته RBF در حالت پنج‌کلاسی میانگین زمان محاسبات به مقدار ۲۲۴۹۳/۷۷ ثانیه افزایش یافته است.

جدول ۱۴. تأثیر انتخاب ویژگی بر زمان محاسبات مدل پیشنهادی با تنظیم پارامترها

میانگین زمان محاسبات (ثانیه)				
ارزیابی به‌روش 10-fold با طبقه‌بند SVM				
Evaluator:ReliefF		Levy_DE_GABC_SVM		
Search:Ranker		تعداد ویژگی		
تعداد کلاس	هسته	۵	۱۰	۱۵
۲	RBF	۴۳۵۰/۵۰	۱۰۷۱۵/۲۶	۱۳۸۵۶/۳۹
۵	RBF	۷۰۶۳/۷۹	۱۲۵۲۰/۲۰	۲۲۴۹۳/۷۷

۵-۴-۲-۲- نتایج مدل ABC_SVM با تنظیم پارامترها

این آزمایشات با هدف انتخاب بهترین ۵ ویژگی، ۱۰ ویژگی و ۱۵ ویژگی از بین ۳۰ و ۳۱ ویژگی توسط مدل پایه تکرار شد. این آزمایشات فقط با هسته RBF در دو حالت دوکلاسی و پنج‌کلاسی انجام شد. روش ارزیابی طبقه‌بند 10-fold می‌باشد. میانگین صحت طبقه‌بند در ۴ بار تکرار آزمایشات به‌روش 10-fold مطابق جدول ۱۵ ارائه شد. در مدل پایه در انتخاب بهترین ۱۵ ویژگی با هسته RBF در حالت پنج‌کلاسی میانگین صحت به مقدار ۹۸/۳۷ درصد افزایش یافته است.

جدول ۱۵. تأثیر انتخاب ویژگی بر صحت طبقه‌بند در مدل پایه با تنظیم پارامترها

ارزیابی به‌روش 10-fold با طبقه‌بند SVM				
Evaluator:ReliefF		ABC_SVM		
Search:Ranker		تعداد ویژگی		
تعداد کلاس	هسته	۵	۱۰	۱۵
۲	RBF	۹۷/۸۵	۹۸/۰۶	۹۸/۰۸
۵	RBF	۹۷/۶۸	۹۸/۲۶	۹۸/۳۷

در تمام آزمایشات مدل پایه، میانگین زمان محاسبات طبقه‌بند در ۴ بار تکرار آزمایشات به‌روش 10-fold مطابق جدول ۱۶ ارائه شد. در مدل پایه در انتخاب بهترین ۱۵ویژگی با هسته RBF در حالت پنج‌کلاسی میانگین زمان محاسبات به مقدار ۲۱۸۸۸/۵۵ ثانیه افزایش یافته است.

جدول ۱۶. تأثیر انتخاب ویژگی بر زمان محاسبات طبقه‌بند در مدل پایه با تنظیم پارامترها

میانگین زمان محاسبات (ثانیه)				
ارزیابی به‌روش 10-fold با طبقه‌بند SVM				
Evaluator:ReliefF		ABC_SVM		
Search:Ranker		تعداد ویژگی		
تعداد کلاس	هسته	۵	۱۰	۱۵
۲	RBF	۵۲۸۷/۸۳	۹۱۹۹/۹۴	۱۸۰۴۵/۶۹
۵	RBF	۸۲۳۷/۹۵	۱۴۱۵۵/۵۸	۲۱۸۸۸/۵۵

نتایج آزمایشات نشان داد که با افزایش مقادیر پارامترهای MCN و Limit، میانگین صحت طبقه‌بند در مدل پیشنهادی بیشتر از مدل پایه و در مدل پایه بیشتر از مدل SVM می‌باشد. با این افزایش، میانگین صحت طبقه‌بند در مدل پیشنهادی به ۹۸/۹۷ درصد افزایش یافت. محققان بر این نظر هستند که با افزایش چشمگیر مقادیر MCN، Limit، SN و MaxIter میانگین صحت طبقه‌بند در روش پیشنهادی غالباً بهتر از روش پایه خواهد شد و امید آن می‌رود به ۱۰۰ درصد همگرا شود. تمامی آزمایشات بیانگر کارایی مدل پیشنهادی در مقایسه با کارهای پژوهشی گذشته است.

۵-۴-۳- تنظیم پارامترها با الگوریتم تاگوچی

آزمایشات برای مدل پیشنهادی Levy_DE_GABC_SVM با تنظیم پارامترها به‌روش تاگوچی تکرار شد. در این آزمایشات برخی از پارامترها همانند Φ، ψ و β مطابق جدول ۴ و بر اساس سایر مقالات مقداردهی شد[۱۴،۱۵،۳۸]. اما برای تنظیم سایر پارامترها همانند CS، MCN، Limit، Dimension از الگوریتم تاگوچی استفاده شد. این آزمایشات با هسته RBF و بر روی مجموعه‌داده چندکلاسی انجام شد. در طراحی آزمایشات تاگوچی تمام آزمایشات انجام نمی‌گیرد و بلکه تنها با انجام بخشی از آن‌ها می‌توان به بهترین سطح از هر فاکتور دست یافت. نتایج به‌دست آمده از هر آزمایش در روش تاگوچی به نرخ سیگنال به نویز[۱۶] تبدیل می‌گردد. در این نرخ، مقدار مطلوب (میانگین) به عنوان سیگنال و مقدار نامطلوب (انحراف معیار)، نویز نامیده می‌شود. هدف در این آزمایشات یافتن سطوحی است که نرخ سیگنال به نویز را حداکثر نماید. در این آزمایشات، برای هر یک از پارامترها پنج سطح مطابق جدول ۱۷ لحاظ شده است.

تمام این آزمایشات بر روی مدل پیشنهادی انجام شد و مقدار تابع هدف که همان مقدار صحت طبقه‌بند می‌باشد مشخص گردید. مقادیر تابع هدف در ۲۵ آزمایش در جدول ۱۸ نشان داده شد.

جدول۱۷. سطوح فاکتورهای الگوریتم تاگوچی بر روی مدل پیشنهادی

پارامترها	سطح ۱	سطح ۲	سطح ۳	سطح ۴	سطح ۵
CS	۱۰	۲۰	۳۰	۴۰	۵۰
MCN	۱۰	۲۰	۳۰	۴۰	۵۰
Limit	۱	۲	۳	۴	۵
Dimension	۵	۱۰	۱۵	۲۰	۲۵

جدول ۱۸. مقادیر تابع هدف (صحت) در ۲۵ آزمایش مختلف

ردیف	بعد	کران	MCN	CS	صحت
۱	۵	۱	۱۰	۱۰	۹۸/۴۳
۲	۱۰	۲	۲۰	۱۰	۹۸/۸۰
۳	۱۵	۳	۳۰	۱۰	۹۹/۲۹
۴	۲۰	۴	۴۰	۱۰	۹۹/۰۰
۵	۲۵	۵	۵۰	۱۰	۹۹/۱۱
۶	۱۵	۲	۱۰	۲۰	۹۹/۰۰
۷	۲۰	۳	۲۰	۲۰	۹۸/۸۵
۸	۲۵	۴	۳۰	۲۰	۹۹/۳۲
۹	۵	۵	۴۰	۲۰	۹۸/۹۰
۱۰	۱۰	۱	۵۰	۲۰	۹۹/۱۷
۱۱	۲۵	۳	۱۰	۳۰	۹۸/۵۲
۱۲	۵	۴	۲۰	۳۰	۹۸/۸۸
۱۳	۱۰	۵	۳۰	۳۰	۹۹/۰۰
۱۴	۱۵	۱	۴۰	۳۰	۹۹/۲۷
۱۵	۲۰	۲	۵۰	۳۰	۹۹/۳۱
۱۶	۱۰	۴	۱۰	۴۰	۹۸/۸۰
۱۷	۱۵	۵	۲۰	۴۰	۹۹/۲۷
۱۸	۲۰	۱	۳۰	۴۰	۹۹/۴۱
۱۹	۲۵	۲	۴۰	۴۰	۹۹/۳۸
۲۰	۵	۳	۵۰	۴۰	۹۸/۹۰
۲۱	۲۰	۵	۱۰	۵۰	۹۹/۳۰
۲۲	۲۵	۱	۲۰	۵۰	۹۸/۰۴
۲۳	۵	۲	۳۰	۵۰	۹۸/۹۷
۲۴	۱۰	۳	۴۰	۵۰	۹۹/۲۵
۲۵	۱۵	۴	۵۰	۵۰	۹۹/۴۱

همانطور که ملاحظه می‌گردد حداکثر مقدار صحت در ۲۵ آزمایش مختلف ۹۹/۴۱ درصد می‌باشد، که این مقدار در آزمایش ۲۵ نیز حاصل شده است. روش پیشنهادی با تنظیم پارامترها به‌روش جستجوی مشبک، دارای مقدار صحت ۹۸/۹۷ بوده است که با جستجوی تاگوچی این نتایج بهبود یافته است. واضح است که اگر تنظیم پارامترها دقیقتر صورت گیرد به‌طور منطقی نتایج بهتری خواهیم داشت.

۵-۴-۴-آزمون ویلکاکسون

آزمون آماری مورد استفاده برای تأیید نتایج، آزمون ناپارامتری رتبه‌بندی علامت‌دار ویلکاکسون[۱۷] بوده است. آزمون مذکور برای بررسی تفاوت معنادار بین روش پیشنهادی و روش پایه و همچنین این دو روش بدون تنظیم پارامترها انجام شده است. در هر یک از موارد تفاوت معناداری به‌ازای هر دو هسته RBF و Sigmoid بررسی شده است. این موارد به ترتیب در جداول ۱۳، ۱۵، ۵ و ۷ گزارش شده است.

در این آزمون فرضیه‌های H0 و H1 به‌صورت زیر تعریف شده‌اند:

H0: تفاوت معناداری بین دو روش وجود ندارد

H1: تفاوت معناداری بین دو روش وجود دارد.

از آنجا که طول دنباله مقادیر حاصل از هر آزمایش ۶ است و به‌بیان دیگر نمونه‌های ورودی آزمون دارای طول ۶ هستند، به‌ازای سطح معناداری ۰/۰۵ مقدار بحرانی ویلکاکسون برابر ۱ است. از این‌رو هرگاه خروجی آزمون از ۱ کمتر یا مساوی باشد، شرط H0 رد می‌شود که حاکی از تفاوت معنادار دو روش است. مقدار خروجی آزمون مذکور به‌ازای هر جفت روش مورد مقایسه مطابق جدول ۱۹ است.

جدول ۱۹: خروجی آزمون رتبه‌بندی علامت‌دار ویلکاکسون برای هر دو جفت روش (مقدار کمتر از ۱ به‌معنای معنادار بودن تفاوت به‌ازای سطح معناداری ۰/۰۵ است)

	روش پایه بدون تنظیم پارامترها و هسته RBF	روش پایه بدون تنظیم پارامترها و هسته Sigmoid	روش پایه با تنظیم پارامترها و هسته RBF	روش پیشنهادی بدون تنظیم پارامترها و هسته RBF	روش پیشنهادی بدون تنظیم پارامترها و هسته Sigmoid
روش پیشنهادی با تنظیم پارامترها و هسته RBF	۰	۰	۰	۰	۰

همانطور که در جدول فوق مشخص است، خروجی آزمون برای همه حالات مقدار صفر است که حاکی از تفاوت معنادار روش پیشنهادی و روش‌های دیگر است. مقدار حاصل به این معناست که سایر روش‌ها در هیچ آزمایشی بهتر از روش پیشنهادی عمل نکرده‌اند و این به‌معنای برتری قابل ملاحظه روش پیشنهادی است.

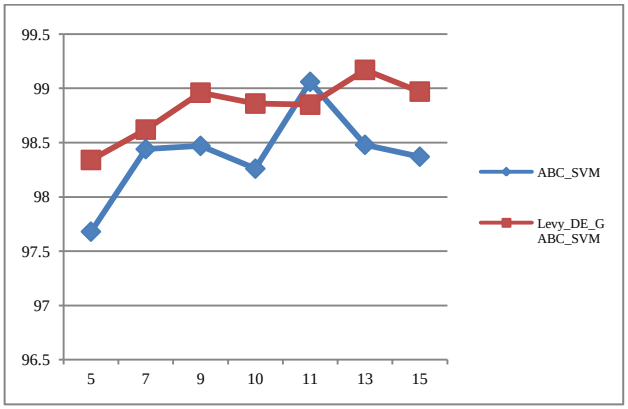
۵-۴-۵- بررسی به‌ازای تعداد ویژگیهای انتخابی

آزمایشات دیگری با هدف انتخاب بهترین ۵ ویژگی، ۷ ویژگی، ۹ ویژگی، ۱۰ ویژگی، ۱۱ ویژگی، ۱۳ ویژگی و ۱۵ ویژگی از بین ۳۱ ویژگی توسط مدل پیشنهادی و مدل پایه تکرار شد. دراین آزمایشات دو مدل Levy_DE_GABC_SVM، ABC_SVM بر روی خروجی حاصل از فیلتر Relief یعنی ۳۱ویژگی اعمال شد که در ادامه خواهیم دید. در این آزمایشات هسته RBF و حالت مسئله پنج‌کلاسی لحاظ شد. روش ارزیابی طبقه‌بند 10-fold می‌باشد. میانگین صحت طبقه‌بند در ۴ بار تکرار آزمایشات به‌روش 10-fold مطابق جدول ۲۰ و شکل ۵ ارائه شده است.

با استفاده از آزمون رتبه‌بندی علامت‌دار ویلکاکسون و با توجه به توضیحاتی که در بخش ۵-۴-۴ گفته شد، با توجه به طول نمونه‌های برابر با ۷ و سطح معناداری ۰/۰۵ و اینکه با این تنظیمات مقدار بحرانی ویلکاکسون ۲ خواهد بود، باز هم تفاوت معناداری بین روش پیشنهادی در سطر دوم و روش پایه وجود دارد (خروجی آزمون مذکور در این حالت ۲ است که کمتر مساوی مقدار بحرانی ویلکاکسون است و بنابراین فرضیه H0 رد می‌شود).

جدول ۲۰. مقایسه تأثیر تعداد ویژگی بر صحت طبقه‌بند در مدل پایه و مدل پیشنهادی با تنظیم پارامترها

ارزیابی به‌روش 10-fold با طبقه‌بند SVM							
	تعداد ویژگی						
	۵	۷	۹	۱۰	۱۱	۱۳	۱۵
ABC_SVM	۹۷/۶۸	۹۸/۴۴	۹۸/۴۷	۹۸/۲۶	۹۹/۰۶	۹۸/۴۸	۹۸/۳۷
Levy_DE_GABC_SVM	۹۸/۳۴	۹۸/۶۲	۹۸/۹۶	۹۸/۸۶	۹۸/۸۵	۹۹/۱۷	۹۸/۹۷



شکل۵. مقایسه تأثیر تعداد ویژگی بر صحت طبقه‌بند در مدل پایه و مدل پیشنهادی با تنظیم پارامترها به‌روش جستجوی مشبک

همانطور که در شکل ۵ ملاحظه می‌شود، در اغلب موارد صحت طبقه‌بند در مدل پیشنهادی از مدل پایه بیشتر است و صحت مدل پیشنهادی با انتخاب بهترین ۱۳ ویژگی با هسته RBF در حالت پنج‌کلاسی به مقدار ۹۹/۱۷ درصد افزایش یافته است.

۵-۴-۶- مقایسه با کارهای پیشین

در ادامه، نرخ صحت در مدل پیشنهادی، مدل پایه و مدل SVM با نرخ صحت روش‌های طبقه‌بندی که برگرفته از سایر مقالات است مقایسه شد.

در صورتی می‌توان نتایج مقالات را با یکدیگر مقایسه کرد که شرایط ارزیابی برابری داشته باشیم. شرایط یکسان ارزیابی شامل یکسانی در مجموعه‌داده و روش ارزیابی طبقه‌بند می‌باشد. در این مقاله از مجموعه‌داده استاندارد NSL-KDD و از روش ارزیابی استاندارد 10-fold استفاده شده است. جهت انجام مقایسات مقالاتی که شرایط ارزیابی برابری با کار پژوهشی ما داشت بررسی شد و عیناً نتایج آن مقالات به‌همراه نتایج مدل پیشنهادی، مدل پایه و مدل SVM در جدول ۲۱ درج گردیده است.

جدول ۲۱. مقایسه نرخ صحت در روش‌های طبقه‌بندی پیشین

روش انتخاب ویژگی	میانگین صحت	روش‌های طبقه‌بندی
تمام ویژگی‌ها	۹۹/۱۱	C4.5 [6]
GA	۹۸/۶۹	
Best-first	۹۸/۸۴	
CFS	۹۹/۴۱	
تمام ویژگی‌ها	۹۹/۵۳	BayesNet [6]
GA	۹۹/۵۲	
Best-first	۹۸/۹۱	
CFS	۹۸/۹۲	
ABC_SVM [6]	۹۲/۷۶	ABC باینری
PSO_SVM [6]	۸۳/۸۸	
GA_SVM [6]	۸۰/۷۳	
تمام ویژگی‌ها	۹۸/۲۴	KNN [6]
FFS	۹۸/۱۱	
SSO [6]	۹۲/۷۰	SSO
RSDT [6]	۹۷/۸۸	Rough set
FC_ANN [6]	۹۶/۷۱	تمام ویژگی‌ها
تمام ویژگی‌ها	۸۸/۵۹	MABC_EPSO [6]
SFSM	۹۹/۳۲	
RFSM	۹۹/۸۲	
کاهش ویژگی	۹۷/۸۴	TVCPSO_SVM [17]
کاهش ویژگی	۹۶/۸۸	TVCPSO_ MCLP [17]
ویژگی‌های افزوده	۹۹/۳۱	LMDRT_SVM[19]
ویژگی‌های افزوده	۹۹/۲۸	LMDRT_SVM2[19]
کاهش ویژگی	۹۴/۸۹	ANN_binary_class [25]
کاهش ویژگی	۹۴/۰۴	ANN_multi_class [25]
کاهش ویژگی	۹۴/۳۱	AdaBoost_binary_class[25]
کاهش ویژگی	۸۰/۵۵	AdaBoost_multi_class [25]
کاهش ویژگی	۸۷/۲۹	NaiveBayes_binary_class [25]
کاهش ویژگی	۸۲/۴۷	NaiveBayes_multi_class [25]
کاهش ویژگی	۹۵/۴۵	ELM_binary_class[25]
کاهش ویژگی	۹۲/۹۴	ELM_multi_class [25]
کاهش ویژگی	۹۸/۶۶	OS_ELM_binary_clas [25]
کاهش ویژگی	۹۷/۶۷	OS_ELM_multi_class [25]
SVM_SA	۹۹/۹۶	DT_SVM_SA[26]
تمام ویژگی‌ها	۹۹/۰۳	SVM[26]
تمام ویژگی‌ها	۹۸/۸۵	DT[26]
SSO	۹۳/۳۰	Hybrid SSO[27]
Relief	۹۴/۴۲	Proposed SVM_binary class
CFS	۸۳/۶۴	Proposed SVM_binary class
Relief و ABC استاندارد	۹۸/۳۷	Proposed ABC_SVM_multi_class
Relief و ABC بهبودیافته	۹۸/۹۷	Proposed Levy_DE_GABC_SVM_multi_class

۶ - نتیجه‌گیری و کارهای آینده

در این تحقیق، یک سیستمِ تشخیصِ نفوذ در شبکهِ ترکیبیِ جدید با استفاده از الگوریتم ABC بهبودیافته مبتنی بر طبقه‌بند SVM با روش ارزیابی 10-fold برای انتخاب بهترین ویژگی‌ها پیشنهاد گردید. روش پیشنهادی از ترکیب معادلات جستجوی PSO و DE در فاز زنبورهای کارگر و ناظر به‌منظور به‌روزرسانی موقعیت زنبورها و به‌کارگیری پرواز

لوی در فاز زنبورهای پیشاهنگ به‌منظور بهبود بهره‌برداری و نرخ همگرایی در الگوریتم استاندارد ABC می‌باشد.

در مرحله پیش‌پردازش با اعمال فیلترهای Relief و CFS توسط نرم‌افزار وکا بر روی مجموعه‌داده NSL-KDD فضای جستجو کاهش یافت. سپس توسط مدل‌های پیشنهادی، پایه و SVM میانگین صحت طبقه‌بند و میانگین زمان محاسبات برای انتخاب بهترین ۵ ویژگی، ۱۰ ویژگی و ۱۵ ویژگی در دو حالت دوکلاسی و پنج‌کلاسی با هسته‌های RBF و Sigmoid محاسبه شد.

آزمایشات نشان می‌دهد که میانگین صحت طبقه‌بند در انتخاب بهترین ۱۰ ویژگی و بهترین ۱۵ ویژگی بیشتر از میانگین صحت طبقه‌بند در انتخاب بهترین ۵ ویژگی است. آزمایشات نشان می‌دهد که میانگین صحت طبقه‌بند در روش‌های Wrapper همانند مدل‌های پیشنهادی و پایه بهتر از میانگین صحت طبقه‌بند در مدل SVM است. در مقابل زمان محاسبات در روش Wrapper خیلی بیشتر از زمان محاسبات در مدل SVM است. در آزمایشات مرحله دوم میانگین صحت طبقه‌بند در روش پیشنهادی در میانگین ۴ بار اجرا به ۹۹ درصد همگرا شد. محققان بر این نظر هستند که با افزایش چشمگیر مقادیر MCN, Limit, SN و MaxIter میانگین صحت طبقه‌بند در مدل پیشنهادی غالباً بهتر از مدل پایه خواهد شد و امید آن می‌رود به ۱۰۰ درصد همگرا شود.

در پیشنهاد کارهای آینده می‌توان گفت که اهمیت مقداردهی اولیه جمعیت در الگوریتم‌های مبتنی بر جمعیت از آن جهت است که می‌تواند بر روی نرخ همگرایی و کیفیت راه‌حل نهایی اثر بگذارد. در این مرحله به منظور افزایش تنوع در جمعیت، می‌توان از توزیع لوی بهره برد. بعلاوه برای افزایش نرخ همگرایی می‌توان پرواز لوی را به‌طور مستقل بعد از فاز زنبورهای پیشاهنگ بر روی بهترین راه‌حل سراسری به‌کار برد. حتی می‌توان برای به‌کارگیری از مزایای پیشنهادات مذکور، موارد را به‌طور همزمان به‌کار برد. همچنین می‌توان در فاز زنبورهای کارگر یا ناظر یا هر دو فقط از معادله جستجوی PSO یا معادله جستجوی DE استفاده نمود و هر کدام را به‌طور جداگانه آزمایش کرد. ضمناً می‌توان معادله جستجو را در فاز زنبورهای کارگر و ناظر متفاوت در نظر گرفت و بالاخره می‌توان تمام موارد را با هم به‌کار برد و از مزایای آنها استفاده نمود.

مراجع

[1] H. J. Liao, C. H. R. Lin, Y. C. Lin and K. Y. Tung, "Intrusion detection system: a comprehensive review," Journal of Network and Computer Applications, vol. 36, no. 1, pp. 16-24, 2013.

[۲] رحیم به جانی، محمد کلانتری و امیر مسعود افتخاری مقدم، «ارائه چهارچوبی مبتنی بر نظریه بازی‌ها برای جلب مشارکت گره‌ها در فرآیند شناسایی گره‌های مخرب در شبکه‌های حسگر بی‌سیم»، مجله مهندسی برق دانشگاه تبریز، مقالات آماده انتشار، ۱۳۹۶.

[3] A. Eesa, Z. Orman and A. Brifcani, "A new feature selection model based on ID3 and bees algorithm for intrusion detection system," Turkish Journal of Electrical Engineering and Computer Sciences, vol. 23, pp. 615-622, 2015.

[4] A .M. Hosseinzadeh and P. Kabiri, "Feature selection for intrusion detection system using ant colony optimization," International Journal of Network Security, vol. 18, no. 3, pp. 420-432, 2016.

[5] L. Mohammadpour, M. Hussain, A. Aryanfar, V. Maleki Raee and F. Sattar, "Evaluating performance of intrusion detection system using support vector machines: review," International Journal of Security and Its Applications, vol. 9, no. 9, pp. 225-234, 2015.

[6] P. Amudha, S. Karthik and S. Sivakumari, "A hybrid swarm intelligence algorithm for intrusion detection using significant features," The Scientific World Journal, vol. 2015, pp. 1-16, 2015.

[7] P. Amudha, S. Karthik and S. Sivakumari, "An experimental analysis of hybrid classification approach for intrusion detection," Indian Journal of Science and Technology, vol. 9, no. 13, 2016.

[8] O. Alomari and Z. A. Othman, "Bees algorithm for feature selection in network anomaly detection," Journal of Applied Sciences Research, vol. 8, no. 3, pp. 1748-1756, 2012.

[9] M. Aldwairi, Y. Khamayseh and M. Al-Masri, "Application of artificial bee colony for intrusion detection systems," Security and Communication Networks Security, vol. 8 no. 16, pp. 2730-2740, 2015.

[10] S. X. Wu and W. Banzhaf, "The use of computational intelligence in intrusion detection systems: A review," Applied Soft Computing, vol. 10, pp.1–35, 2010.

[11] Y. Wang, G. D. Guo and L .F. Chen, "Chaotic artificial bee colony algorithm: A new approach to the problem of minimization of energy of the 3D protein structure," Molecular Biology, vol. 47, no. 6, pp. 894–900, 2013.

[12] J. C. Bansal, H. Sharma, K. V. Arya and A. Nagar, "Memetic search in artificial bee colony algorithm," Soft Computing, vol. 17, no. 10, pp. 1-18, 2013.

[13] V. K. Sharma, R. Kumari and S. Kumar, "Memetic search in artificial bee colony algorithm with fitness based position update," IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014), Jaipur, India, 25 September 2014.

[14] H. Shan, T. Yasuda and K. Ohkura, "A levy flight based hybrid artificial bee colony algorithm for solving numerical optimization problems," IEEE Congress on Evolutionary Computation (CEC), Beijing, China, 22 September 2014.

[15] K. K. Bharti and P. K. Singh, "Chaotic gradient artificial bee colony for text clustering," Soft Comput, vol. 20, pp. 1113–1126, 2016.

[16] A. Dastanpour and R. A. R Mahmood, "Feature selection based on genetic algorithm and support vector machine for intrusion detection system," in Proc of 2nd International Conference on Informatics Engineering & Information Science (ICIEIS2013), pp. 169-181, 2013.

[17] S. M. H. Bamakan, H. Wang, T. Yingjie and Y. Shi, "An effective intrusion detection framework based on MCLP/SVM optimized by time-varying chaos particle swarm optimization," Neuro Computing, vol. 199, pp. 90–102, 2016.

[18] Akashdeep, I. Manzoor and N. Kumar, "A feature reduced intrusion detection system using ANN classifier," Expert Systems with Applications, vol. 88, pp. 249–257, 2017.

[19] H. Wang, J. Gu and S. Wang, "An effective intrusion detection framework based on SVM with feature augmentation," Knowledge-Based Systems, vol. 136, pp. 130–139, 2017.

[20] M. R. G. Raman, N. Somu, K. Kirthivasan, R. Liscano and V. S. 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.

[21] S. M. H. Bamakan, H. Wang and Y. Shi, "Ramp loss K-Support Vector Classification-Regression; a robust and sparse multi-class approach to the intrusion detection problem," Knowledge-Based Systems, vol. 126, pp. 113–126, 2017.

[22] M. R. G. Raman, N. Somu, K. Kirthivasan and V. S. S. Sriram, "A hypergraph and arithmetic residue-based probabilistic neural network for classification in intrusion detection systems," Neural Networks, vol. 92, pp. 89–97, 2017.

[23] W. K. Mashwani and A. Salhi, "Multiobjective memetic algorithm based on decomposition," Applied Soft Computing, vol. 21, pp.221–243, 2014.

[24] Z. Zhang, "Efficient computer intrusion detection method based on artificial bee colony optimized kernel extreme learning machine,"

Telkomnika Indonesian Journal of Electrical Engineering, vol. 12, no. 3, pp. 1954 -1959, 2014.
[25] R. Singh, H. Kumar and R. K. Singl, "An intrusion detection system using network traffic profiling and online sequential extreme learning machine," Expert Systems With Applications, vol. 42, pp. 8609–8624, 2015.
[26] S. W. Lin, K. C. Ying, C. Y. Lee and Z. J. Lee, "An intelligent algorithm with feature selection and decision rules applied to anomaly intrusion detection," Applied Soft Computing, vol. 12, pp. 3285–3290, 2012.
[27] Y. Chung and N. Wahid, "Hybrid network intrusion detection system using simplified swarm optimization (SSO)," Applied Soft Computing, vol. 12, pp. 3014–3022, 2012.
[28] V.Chahkandi, M. Yaghoobi and G. Veisi, "Feature selection with chaotic hybrid artificial bee colony algorithm based on fuzzy (CHABCF)," Journal of Soft Computing and Applications, vol. 2013, no. 1, pp. 1-8, 2013.
[29] Z. A. Othman, L. M. Theng, S. Zainudin and H. M. Sarim, "Great deluge algorithm feature selection for network intrusion detection," Journal of Applied Science and Agriculture, vol. 8, no. 4, pp. 322-330, 2013.
[30] M. Gupta and S. K. Shrivastava, "Intrusion detection system based on svm and bee colony," International Journal of Computer Applications, vol. 111, no. 10, pp. 0975 – 8887, 2015.
[31] Y. Gurcan and A. DoLan, "Angle modulated artificial bee colony algorithms for feature selection," Applied Computational Intelligence and Soft Computing, vol. 7, pp. 1-6, 2016.
[32] A. A. Aburomman and M. I. Reaz, "A novel weighted support vector machines multiclass classifier based on differential evolution for intrusion detection systems," Information Sciences, vol. 414, pp. 225–246, 2017.
[33] R. A. R. Ashfaq, X. Z. Wang, J. Z. Huang, H. Abbas and Y. L. He, "Fuzziness based semi-supervised learning approach for intrusion detection system," Information Sciences, vol. 378, pp. 484–497, 2017.
[34] E. K. Viegas, A. O. Santin and L. S. Oliveira, "Toward a reliable anomaly-based intrusion detection in real-world environments," Computer Networks, vol. 127, pp. 200–216, 2017.
[35] D. Karaboga and B. Akay, "A comparative study of artificial Bee Colony algorithm," Applied Mathematics and Computation, vol. 214, pp. 108–132, 2009.
[36] J. P. Nolan, *Stable Distributions, Models for Heavy Tailed Data*, Math/Stat Department American University, 2015.
[۳۷] زینب صادقی چوینلی و سید محمد حسین معطر، «زمان‌بندی سیستم‌های تولید کارگاهی انعطاف‌پذیر با استفاده از الگوریتم جستجوی فاخته بهبودیافته با خوشه‌بندی مارکوف و پرواز لوی»، مجله مهندسی برق دانشگاه تبریز، دوره ۴۶، شماره ۴، صفحه ۱۸۵-۱۹۳، زمستان ۱۳۹۵.
[38] R. Jensi and J. G. Wiselin, "An enhanced particle swarm optimization with levy flight for global optimization," Applied Soft Computing, vol. 43, pp. 248–261, 2016.
[39] L. Dhanabal and S. P. 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, no. 6, 2015.

زیرنویس‌ها

[1] Intrusion
[2] Confidentiality
[3] Integrity
[4] Availability
[5] Intrusion Detection Systems
[6] False Positive
[7] False Negative
[8] Signature-based Detection (SD-IDS)
[9] Anomaly-based Detection (AD-IDS)
[10] Stateful Protocol Analysis (SPA-IDS)
[11] Exploration
[12] Exploitation
[13] Employed Bee
[14] Onlooker Bee
[15] Scout Bee
[16] Signal-To-Noise
[17] Wilcoxon Signed Rank Test