Semnan University

Journal of Modeling in Engineering

Journal homepage: https://modelling.semnan.ac.ir/

ISSN: 2783-2538

Research Article

An Intrusion Detection System Based on Deep Learning and Metaheuristic Algorithm for IOT

Bahman Sanjabi[a], Mahmood Ahmadi[b,*]

[a] *Master's degree in Computer Architecture Engineering, Department of Computer Engineering and Information Technology, Razi University, Iran*
[b] *Associate Professor, Department of Computer Engineering and Information Technology, Razi University, Iran*

PAPER INFO

Paper history:

Received: 29 April 2023
Revised: 25 May 2023
Accepted: 13 September 2023

Keywords:
Deep learning;
Inrusion detection systems;
Internet of things;
Meta-heuristic algorithms;
Geray wolf optimizer.

ABSTRACT

oday, due to the considerable benefits of the Internet of Things (IoT) in various fields such as smart homes, industry, cars, agriculture, etc., its application is very widespread. Due to this, the security of these networks is receiving more and more attention. One of the methods of providing security in networks as well as IoT network is intrusion detection systems. Traditional intrusion detection systems are not very efficient for use in the Internet of Things, so the use of new methods is required. One of these methods is intrusion detection systems based on machine learning and deep learning that have been considered in this area. They are trained in machine learning and deep neural network learning to detect attack patterns. There are important parameters for setting up a machine learning network, and choosing the right value for these parameters has a great impact on system accuracy. In this paper, a method is presented that uses meta-heuristic algorithms such as genetic algorithm, particle swarm optimization, artificial bee colony and gray wolf to find the optimal hyperparameters for the deep learning network and the intrusion detection system is created based on these hyperparameters. This method was implemented using the Tensorflow and keras libraries and tested on the KDDCup99, UNSW-NB15 and Bot-IoT datasets. The results showed that the proposed method can detect attacks with a high accuracy of 99%.

DOI: https://doi.org/10.22075/jme.2023.30503.2443

*** Corresponding author.**
E-mail address: m.ahmadi@razi.ac.ir

How to cite this article:
Ahmadi, M., & Sanjabi, B. (2024). An Intrusion detection system based on deep learning and metaheuristic algorithm for IOT. Journal of Modeling in Engineering, 22(76), 69-83. doi: 10.22075/jme.2023.30503.2443

مقاله پژوهشی

سیستم تشخیص نفوذ مبتنی بر یادگیری عمیق و الگوریتم‌های فرا ابتکاری برای اینترنت اشیاء

بهمن سنجابی[۱]، محمود احمدی[۲،*]

اطلاعات مقاله

دریافت مقاله: ۱۴۰۲/۰۲/۰۹
بازنگری مقاله: ۱۴۰۲/۰۳/۰۴
پذیرش مقاله: ۱۴۰۲/۰۶/۲۲

واژگان کلیدی:
یادگیری عمیق،
سیستم تشخیص نفوذ،
بهینه‌سازی ازدحام ذرات،
گرگ خاکستری،
کلونی زنبور عسل مصنوعی،
الگوریتم ژنتیک.

چکیده

امروزه به خاطر فواید قابل ملاحظه‌ی اینترنت اشیاء (IoT) در حوزه‌های مختلف از قبیل خانه‌های هوشمند، صنایع، خودروها، کشاورزی و ... کاربرد آن بسیار گسترش یافته است. با توجه به این مطلب، امنیت این شبکه‌ها روز به روز مورد توجه بیشتری قرار می‌گیرد. یکی از روش‌های تأمین امنیت در شبکه‌ها و همینطور شبکه‌ی اینترنت اشیاء، سیستم‌های تشخیص نفوذ می‌باشد. سیستم‌های تشخیص نفوذ سنتی کارایی مناسبی برای استفاده در شبکه‌ی اینترنت اشیاء ندارند، لذا استفاده از روش‌های جدید مورد نیاز است. یکی از این روش‌ها، سیستم‌های تشخیص نفوذ مبتنی بر یادگیری ماشین و یادگیری عمیق هستند که در این حوزه مورد توجه قرار گرفته‌اند. در یادگیری ماشین و یادگیری عمیق، شبکه‌ی عصبی برای تشخیص الگوهای حمله آموزش داده می‌شوند. پارامترهای مهمی برای تنظیم شبکه‌ی یادگیری ماشین وجود دارند که انتخاب مقدار مناسب برای این پارامترها تأثیر فراوانی در دقت سیستم دارد. در این پژوهش، روشی ارائه شده است که با استفاده از الگوریتم‌های فراابتکاری نظیر الگوریتم ژنتیک، بهینه‌سازی ازدحام ذرات، کلونی زنبور عسل مصنوعی و گرگ خاکستری، ابرپارامترهای بهینه برای شبکه‌ی یادگیری عمیق را یافته و سیستم تشخیص نفوذی براساس این ابرپارامترها ایجاد می‌شود تا تشخیص نفوذ در شبکه‌ی اینترنت اشیاء انجام گردد. این روش با استفاده از کتابخانه‌های Tensorflow و keras پیاده‌سازی شده و روی مجموعه داده‌های KDDCup99 ، UNSW-NB15 و Bot-IoT آزمایش شده است. نتایج نشان داده است که روش پیشنهادی با دقت بالای ۹۹.۶٪ می‌تواند حملات را تشخیص دهد.

DOI: https://doi.org/10.22075/jme.2023.30503.2443

۱-مقدمه

در سال‌های اخیر، با توسعه سریع فناوری‌های پردازش ابری و هوش مصنوعی، اینترنت اشیاء نیز به شدت توسعه یافته است. ابزارهای هوشمند گوناگون از طریق ارتباطات می‌توانند مقدار زیادی داده و اطلاعات دریافت کنند. اینترنت اشیاء و ابزارهای هوشمند تسهیلات و کاربردهای زیادی برای مردم به ارمغان آورده‌اند که باعث محبوبیت هرچه بیشتر این تکنولوژی شده است. اما استفاده از فناوری‌های نوین خطراتی در رابطه با حریم خصوصی و امنیت با خود دارند. با توجه به اینکه تجهیزات اینترنت اشیاء داده‌های شخصی زیادی از کاربر جمع‌آوری و ذخیره می‌کنند، این شبکه‌ها به اهداف مهمی برای حملات گوناگون تبدیل شده‌اند. در این حالت حفظ حریم خصوصی و امنیت داده‌ها بسیار مهم است.

برای حفاظت از شبکه‌های اینترنت اشیاء یک سیستم دفاعی در این شبکه‌ها باید وجود داشته باشد. سیستم تشخیص

* پست الکترونیک نویسنده مسئول: m.ahmadi@razi.ac.ir
۱-دانش آموخته کارشناسی ارشد مهندسی معماری کامپیوتر، گروه مهندسی کامپیوتر و فناوری اطلاعات، دانشگاه رازی، ایران
۲- دانشیار گروه مهندسی کامپیوتر و فناوری اطلاعات، دانشگاه رازی، ایران

استناد به این مقاله:
احمدی، محمود، و سنجابی، بهمن. (۱۴۰۳). سیستم تشخیص نفوذ مبتنی بر یادگیری عمیق و الگوریتم‌های فرا ابتکاری برای اینترنت اشیاء. مدل سازی در مهندسی، ۲۲(۷۶)، ۸۳-۶۹. doi: 10.22075/jme.2023.30503.2443

نفوذ این هدف را برآورده می‌نمایند. تشخیص نفوذگران به شبکه یکی از مراحل مهم در تأمین امنیت در شبکه‌های اینترنت اشیاء به شمار می‌آید. سیستم‌های تشخیص نفوذ یکی از چندین روش برای مدیریت مسائل امنیتی می‌باشند. لایه شبکه تنها به عنوان زیرساختی برای ارتباط ابزارهای مختلف اینترنت اشیاء کاربرد ندارد، بلکه فرصتی برای ایجاد مکانیزم دفاعی مبتنی بر شبکه ایجاد می‌نماید. سیستم تشخیص نفوذ در این لایه قرار می‌گیرد [۱].

روش‌های یادگیری ماشین و یادگیری عمیق عملکرد موفقیت‌آمیزی در یافتن حملات در شبکه‌ها، خصوصاً شبکه‌ی اینترنت اشیاء از خود نشان داده‌اند. این روش‌ها می‌توانند رفتار ناهنجار و مخرب در محیط شبکه‌ی اینترنت اشیاء را به شکل سریع و با محاسبات کم یاد بگیرند و رفتار درست را از رفتار نادرست به خوبی تشخیص دهند. از این رو الگوریتم‌های مبتنی بر یادگیری ماشین و یادگیری عمیق پروتکل‌های امنیتی قوی و محکمی برای ایمن کردن شبکه و تجهیزات اینترنت اشیاء مهیا می‌کنند [۲-۳]. با افزایش حملات و روش‌های جدید به کار برده شده توسط مهاجمین، بهبود در کارایی و تطابق پذیری سیستم‌های تشخیص نفوذ امری ضروری است[۴].

استفاده از روش‌های برجسته و کارآمد در حل مسائل امنیتی مانند شبکه‌های عصبی، هوش مصنوعی و یادگیری ماشین روز به روز بیشتر می‌گردد. دستیابی به راهکار بهینه‌تر در کارایی، دقت، سرعت و مصرف انرژی یکی از چالش‌های مهم این حوزه به حساب می‌آید؛ بنابراین استفاده از ترکیبی از این روش‌ها برای رسیدن به یک سیستم تشخیص نفوذ قوی در شبکه‌های اینترنت اشیاء در این پژوهش مورد استفاده قرار گرفت. چارچوب ایجاد شده در این پژوهش توانایی بررسی تأثیر کارایی ترکیب الگوریتم‌های فراابتکاری با روش یادگیری عمیق را در حوزه تشخیص نفوذ شبکه‌های اینترنت اشیاء نشان داده و نتایج مفیدی برای پژوهش‌های بعدی در این حوزه فراهم می‌آورد. الگوریتم‌های فرا ابتکاری زیادی در زمینه بهینه‌سازی وجود دارند که برخی از آن‌ها از زندگی موجودات زنده الهام گرفته شده اند و برخی از رفتارهای مواد شیمیایی و قوانین فیزیک و گروهی دیگر ابتکاری و جدید می‌باشند. عملکرد هر الگوریتم در مقابل مسئله‌ی مورد استفاده متفاوت است و به سادگی نمی‌توان الگوریتم مناسب برای هر مسئله را مشخص نمود [۵]. الگوریتم ژنتیک به عنوان پایه و اساس الگوریتم‌های فراابتکاری، الگوریتم بهینه‌سازی ازدحام ذرات که یکی از شناخته شده ترین الگوریتم‌های ازدحامی است، همچنین الگوریتم کلونی زنبور مصنوعی که در برخی مسائل گسسته به خوبی نتیجه می‌دهد و الگوریتم گرگ خاکستری یکی از جدیدترین الگوریتم‌های شناخته شده فراابتکاری است برای این پژوهش انتخاب شده‌اند. هدف از این پژوهش ارائه و پیاده‌سازی یک سیستم تشخیص نفوذ برای شبکه‌های اینترنت اشیاء با استفاده از شبکه‌ی باور عمیق و الگوریتم‌های فراابتکاری مانند الگوریتم گرگ خاکستری، بهینه‌سازی ازدحام ذرات، کلونی زنبور مصنوعی، ژنتیک می‌باشد، به طوری که با ترکیب بهینه‌ای از شبکه‌ی یادگیری باور عمیق با دقت بالای ۹۹٪ حملات را تشخیص دهد.

در ادامه مقاله بدین شرح سازمانده شده است. در بخش ۲ کارهای مرتبط ارائه میشد. بخش ۳، مفاهیم شبکه باور عمیق و الگوریتم های فراابتکاری بیان میشود. در بخش ۴ راهکار پیشنهادی معرفی میگردد. بخش ۵ نتایج ارزیابی بدست امده بحث میشود. بخش ۶ نتیجه گیری بیان می گردد.

۲- کارهای مرتبط

در این بخش کارهای انجام شده در حوزه تشخیص نفوذ سیستم های اینترنت اشیا ارائه میگردد.

احمدی طاهری در [۶] به ارائه روشی مبتنی بر یادگیری عمیق برای تشخیص نفوذ در شبکه پرداخته است. در این پژوهش با استفاده ساختار شبکه عصبی کانولوشن یک معماری برای تشخیص نفوذ به شبکه طراحی شده است. برای استفاده از این ساختار، داده‌ها را به شکل رکوردهای تصویری تبدیل نموده و به عنوان ورودی به سیستم وارد شد. نتایج نشان دادند که استفاده از این روش در استخراج خودکار ویژگی‌ها بسیار خوب عمل می‌کند [۶].

در مقاله [۷]، سیستمی تحت عنوان INTI برای تشخیص حملات سیاه‌چاله بر روی اینترنت اشیاء ۶ LoWPAN ارائه شده است، که حملات روی مسیریابی را تشخیص می‌دهد. همچنین این سیستم اثرات نامطلوب بر روی کارائی سیستم تشخیص نفوذ مانند خطای منفی و مثبت یا مصرف زیاد انرژی را کاهش می‌دهد. این روش ترکیبی از استراتژی‌های مراقبت، اعتبار و اطمینان را برای تشخیص مهاجم به کار می‌برد. نتایج نشان دادند که کارایی این سیستم در نرخ تشخیص حمله، تعداد خطاهای مثبت و

منفی به شکل مناسب عمل می‌کند.

رویکردی دیگر به تشخیص نفوذ با استفاده از بررسی بسته‌های مبادله شده بین دستگاه‌های فیزیکی درون شبکه می‌پردازد. این روش برای یافتن حمله از نوع (botnet شبکه‌ی رباتی) در اینترنت اشیاء طراحی شده است که در آن ترافیک عبوری از مسیریاب‌ها آنالیز و بررسی می‌گردند. در این روش که به شکل متمرکز عمل تشخیص نفوذ را انجام می‌دهد از یک دروازه استفاده می‌شود و ترافیک عبوری از طریق این دروازه تجزیه و تحلیل شده و در صورت تشخیص نفوذ هشداری به مدیر ارسال می‌گردد. این روش خطای مثبت و نرخ تشخیص خوبی در کنار مصرف انرژی کمتری ارائه می‌کند [۸].

یک سیستم تشخیص نفوذ برای شبکه‌های حسگر بی‌سیم که با استفاده از مشخصه ترافیک و رفتار غیرعادی حملات را شناسایی می‌کرد توسط Amaral و همکارانش ارائه شد. در این روش تعدادی گره به عنوان مراقب در شبکه پخش می‌شوند که بر همسایه‌ها نظارت می‌کنند. هر کدام از این گره‌ها بسته‌های ارسالی همسایه‌های خود را با قوانین مشخص شده مطابقت داده و در صورت تشخیص نفوذ به سیستم مدیریت رویداد مرکزی اطلاع می‌دهند. مجموعه قوانین هر کدام از گره‌های مراقب متفاوت بوده و در محدوده آن گره همسایه‌ها توسط آن قوانین نظارت می‌شوند [۹].

در پژوهشی که در مقاله [۱۰] در خصوص تشخیص ناهنجاری در اینترنت اشیاء انجام شد، از ترکیب دو روش خوشه‌بندی وزندار معکوس و درخت تصمیم استفاده گردید. با استفاده از روش خوشه‌بندی وزندار معکوس داده‌ها براساس تشابه گروه‌بندی می‌گردند سپس با استفاده از درخت تصمیم دسته‌بندی روی آنها صورت می‌گیرد. این روش با استفاده از MATLAB شبیه‌سازی و مورد ارزیابی قرار گرفت که نتایج آن میزان تشخیص ناهنجاری بسیار خوبی را نشان داد.

برای تشخیص نفوذ در شبکه‌های اینترنت اشیاء راهکاری در مقاله [۱۱] ارائه گردید که مبتنی بر ماژول دسته‌بندی دوسطحی و کاهش ابعاد دولایه‌ای می‌باشد. این چارچوب برای یافتن حملات U2R و R2L ارائه شد. در اینجا از الگوریتم دسته‌بندی Naïve Bayes برای عامل‌های سیستم تشخیص نفوذ که در کل شبکه توزیع شده‌اند استفاده شد. این عامل‌ها ترافیک یا فعالیت مخرب در گره‌های شبکه را تشخیص می‌دهند. این روش خطای منفی به مقدار ۵.۵٪ کاهش داد.

درمقاله [۱۲] سیستم تشخیص نفوذی ارائه شده است که از الگوریتم یادگیری ماشین برای تشخیص ناهنجاری‌های امنیتی در شبکه‌های اینترنت اشیاء استفاده می‌کند. این روش تشخیص برای پروتکل‌های ارتباطی مختلف شبکه که در اینترنت اشیاء استفاده می‌شوند، قابل کاربرد می‌باشد. از دیگر قابلیت‌های این سیستم مقیاس‌پذیری آن است که می‌توان برای شبکه‌های کوچک تا بزرگ استفاده نمود. در این روش از یادگیری عمیق مبتنی بر شبکه‌ی باور عمیق[2] با دو لایه مخفی استفاده شده است. نتایج شبیه‌سازی و آنالیز آن به خوبی قابلیت شناسایی حملات سیاه‌چاله، عدم دسترسی توزیع‌شده، کرم‌چاله و فرصت طلبی را نشان داد.

یکی دیگر از روش‌های ترکیبی برای بهبود سیستم تشخیص نفوذ در شبکه‌های اینترنت اشیاء در مقاله [۱۳] ارائه شده است. در این روش که با استفاده از الگوریتم ژنتیک توسعه یافته و شبکه باور عمیق DBN صورت گرفت. در این روش با استفاده از الگوریتم ژنتیک ابتدا پارامترهای شبکه بهینه‌سازی شده و سپس یادگیری شبکه‌ی DBN صورت می‌گیرد و در نهایت شبکه‌ی DBN به تشخیص نفوذ با تحلیل داده‌ها می‌پردازد. استفاده از الگوریتم ژنتیک موجب بهینه شدن ساختار شبکه شده و تشخیص مناسب حملات می‌گردد. نتایج نشان دادند که این روش تا حد خوبی تشخیص حملات را نسبت به روش‌های دیگر انجام می‌دهد.

الگوریتم بهینه‌سازی ازدحام ذرات[3] (PSO) یکی از الگوریتم‌های ابتکاری جستجوی بهینه می‌باشد که ایده‌ی آن از همکاری و ازدحام در جمعیت‌های بیولوژیکی گرفته شده است. این الگوریتم که مشابه الگوریتم ژنتیک براساس روش جستجوی بهینه و اشتراک گذاری اطلاعات در جمعیت و با استفاده از ترکیب قوانین جبر و احتمال عمل می‌کند. در این روش ابتدا ذرات در مکان‌های تصادفی تولید شده و سپس با سرعت متغیر به سمت بهینه حرکت می‌کنند [۱۴].

در مقاله [۱۵] دو الگوریتم به شکل گسسته روی ۸ مسئله مختلف اجرا شدند. دو معیار مورد بررسی کیفیت پاسخ بهینه و میزان محاسبات برای رسیدن به پاسخ بهینه

[2] Deep Belief network
[3] Particle swarm optimization

(کارایی محاسباتی) در نظر گرفته شد. نتایج آن حاکی از آن است که هر دو الگوریتم پاسخ بهینه خیلی خوبی به دست می‌آورند اما کارایی محاسباتی الگوریتم PSO نسبت به الگوریتم ژنتیک بهتر می‌باشد [۱۵].

در مقاله‌ای دیگر از الگوریتم یادگیری عمیق برای تشخیص حملات بات نت استفاده شده است. این روش با استفاده از تکنیک نمونه‌برداری کمینه ترکیبی برای دستیابی به تعادل در دسته‌ها و سپس جهت اجرای دسته‌بندی بر روی ترافیک شبکه‌ی متعادل شده از شبکه‌ی عصبی بازگشتی عمیق بهره می‌برد. این روش روی مجموعه داده‌های Bot-IoT اجرا شد و نتایج حاصل از اجرا دقت بالای ۹۹ درصد را نشان داد [۱۶].

جدول ۱. مقایسه روش‌های انجام شده

حوزه پژوهش	روش کار	مجموعه داده‌های استفاده شده	معایب	دقت تشخیص
شبکه	شبکه عصبی کانولوشن [۶]	NSL-KDD	مجموعه داده قدیمی	٪ ۹۷
اینترنت اشیاء	خوشه بندی و درخت تصمیم [۱۰]	Intel Dataset	استفاده از مجموعه داده‌ای که زیاد رایج نیست	٪ ۹۷
	کاهش ویژگی ها و مدل بیز ساده [۱۱]	NSL-KDD	مجموعه داده قدیمی	٪ ۸۶
	شبکه باور عمیق [۱۳]	NSL-KDD	مجموعه داده قدیمی	٪ ۹۸
	شبکه عصبی کانولوشن روی حملات Botnet [۱۷]	Bot-IoT	نتایج فقط برای حملات Botnet	٪ ۹۹
	شبکه عصبی بازگشتی عمیق [۱۶]	Bot-IoT	نتایج فقط برای حملات Botnet	٪ ۹۹

در مقاله [۱۷]، روشی برای تشخیص نفوذ در شبکه‌ی اینترنت اشیاء به نام BotIDS ارائه کردند. در این روش یک گره که نظارت و تشخیص نفوذ را بر روی تمامی گره‌های شبکه انجام می‌دهد، به شبکه افزوده شده است. این سیستم تشخیص نفوذ در سه فاز عمل می‌کند، ابتدا در فازهای اول و دوم پیش‌پردازش مجموعه داده را انجام داده و مدل را ایجاد می‌کند سپس در فاز سوم مدل را با پیش‌بینی داده‌های تست ارزیابی می‌نماید. ایجاد مدل با استفاده از ترکیب شبکه‌ی عصبی چرخشی و شبکه‌ی عصبی بازگشتی انجام می‌گیرد. نتایج اجرای این روش روی مجموعه داده Bot-IoT به دقت بالای ۹۹ درصد دست یافت [۱۷].

در انتها باید گفت با توجه به کارهای انجام شده در این زمینه معمولاً از مجموعه داده‌های قدیمی استفاده می‌شود(جدول ۱) که با نیاز واقعی فاصله فراوانی دارند یا برخی کارها بر روی نوع خاصی از حملات تمرکز نموده‌اند که در شبکه‌های اینترنت اشیاء حملات مختلفی قابلیت وقوع دارند، لذا کار برای یافتن راه حل بهینه‌تر که با محدودیت‌های شبکه‌های اینترنت اشیاء سازگار باشد ادامه دارد. در این راستا روشی ارائه داده شده است که به شکلی انعطاف پذیر ساختار شبکه‌ی باور عمیق را سازماندهی نماید به گونه ای که دقت تشخیص نفوذ بالاتر و نرخ خطای مثبت کمی را داشته باشد.

۳- مفهوم شبکه‌ی باور عمیق و الگوریتم‌های فراابتکاری

در این بخش مفهوم شبکه ی باور عمیق و الگوریتم های فرابتکاری به طورمختصر بیان میگردد.

۳-۱- شبکه‌ی باور عمیق

شبکه‌های یادگیری عمیق شبکه‌ی عصبی مصنوعی هستند که از چندین لایه از نرون‌ها تشکیل می‌شوند، لایه نخست لایه‌ی ورودی در نظر گرفته می‌شود و لایه‌ی آخر به عنوان لایه‌ی خروجی در نظر گرفته می‌شود. در بین این دو لایه چند لایه از نرون‌های قرار می‌گیرد که به آنها لایه‌های مخفی گفته می‌شود. ماشین‌های بولتزمن محدودشده[۴] (RBM) مدل‌های مولد عمیقی هستند که برای انجام یادگیری کم عمق توزیع احتمال در مجموعه‌ی داده‌ها توسعه یافته است. ماشین‌های بولتزمن شامل دو لایه می‌باشند: لایه‌ی پنهان و لایه‌ی قابل مشاهده که هیچ اتصالی بین دو گره در یک لایه وجود ندارد.

[4] Restricted Boltzmann Machine

این ماشین‌ها به شکل مدل‌های بدون جهت ایجاد می‌گردند که ویژگی‌ها را از داده‌های ورودی یاد می‌گیرند و سپس ویژگی‌های لایه‌ی قبلی به عنوان متغیرهای نهفته برای لایه‌ی بعدی در نظر گرفته می‌شود.

شبکه‌ی باور عمیق یک مدل مولد عمیقی است که با روی هم قرار دادن ماشین‌های بولتزمن ایجاد می‌شود. مدل شبکه‌ی باور عمیق به شکل بدون ناظر و به صورت سلسله مراتبی آموزش می‌بینند. در واقع لایه‌های شبکه‌ی باور عمیق به صورت لایه‌های ماشین بولتزمن آموزش می‌بینند و برای فاز پیش-تعلیم به شکل پشته روی هم قرار می‌گیرند. به تدریج پس از فاز پیش-تعلیم، شبکه‌ی باور عمیق به شکل شبکه‌ی فیدفوروارد تبدیل شده و وزن‌های آن به روش همگرایی مقابله‌ای تنظیم می‌شود. در فاز پیش-تعلیم، ویژگی‌ها با استفاده از رویکرد لایه‌ایی حریصانه آموزش داده می‌شوند. برای تنظیم بهینه از لایه softmax که ویژگی‌ها را براساس نمونه‌های برچسب‌دار تنظیم می‌شوند، استفاده می‌شود [۳].

۳-۲-الگوریتم‌های فراابتکاری

الگوریتم ژنتیک یک الگوریتم تکاملی برای بهینه‌سازی محاسبات پیچیده مهندسی براساس روش‌های زیست‌شناسی وراثت و جهش است که جان هنری هولند و شاگردانش در دانشگاه میشیگان ارائه کردند. همه الگوریتم‌های ژنتیک شامل مؤلفه‌های کروموزوم، جمعیت اولیه، ارزیابی برازندگی، انتخاب، تقاطع، جهش و خاتمه هستند.

روش کار الگوریتم ژنتیک به صورت خلاصه بدین صورت می‌باشد که در مرحله اول، یک جمعیت اولیه به صورت تصادفی تولید می‌شود. هرکدام از افراد برای صلاحیت برازندگی در مرحله بعدی حساب می‌شوند. بهترین افراد در مرحله انتخاب، انتخاب می‌شوند. افراد با برازندگی بیشتر، احتمال بالاتری برای زادوولد دارند. زادوولد با ترکیب این افراد انتخاب شده، در مرحله تقاطع انجام می‌شود. در مرحله جهش، تغییرات تصادفی بر روی برخی از افراد انجام می‌شود. هدف از عملگر جهش این است که از همگرا شدن الگوریتم به کمینه محلی جلوگیری و جواب‌های با امکان جدید در جمعیت وارد کند. الگوریتم تا پیدا کردن کمینه تابع برازندگی، یا ارضاء ضابطه توقف ادامه پیدا می‌کند. معمولاً بیشترین ضابطه توقف مورد استفاده در این الگوریتم، رسیدن تعداد تولید نسل به بیشینه مقدار لحاظ شده است [۲۱].

بهینه‌سازی ازدحام ذرات یک الگوریتم فرا ابتکاری است که ایده اصلی آن توسط یک روان‌شناس اجتماعی و یک مهندس برق به نام ابرهارت شکل گرفت. در PSO تعدادی از ذرات وجود دارند که در فضای جستجوی تابعی که قصد بهینه کردن آن را داریم پخش شده‌اند. هر ذره تابع مطلوبیت را در موقعیت کنونی خود محاسبه می‌کند. پس از آن با مقایسه اطلاعات محل فعلی‌اش و بهترین محلی که تاکنون در آن قرار گرفته است و همچنین اطلاعات مربوط به بهترین ذرات در جمع، جهتی را برای حرکت انتخاب می‌کند. به این صورت تمامی ذرات جهت حرکت را انتخاب کرده و پس از انجام حرکت، یک مرحله از الگوریتم به پایان می‌رسد [۲۲]. این روند تا زمانی که جواب مورد نظر بدست آید، ادامه می‌یابد.

الگوریتم بهینه‌سازی فراابتکاری زنبورعسل مصنوعی براساس هوش جمعی، با الگوگیری از نتایج مطالعه‌ای بر روی رفتار هوشمند کلونی‌های زنبورعسل در غذایابی توسعه داده یافت. چهار فاز اصلی در اجرای الگوریتم ABC به ترتیب ۱- مقداردهی اولیه، ۲- غذایابی توسط زنبورهای کارگر، ۳- جستجوی محلی توسط زنبورهای تماشاگر، ۴- غذایابی تصادفی توسط زنبورهای پیشاهنگ می‌باشد.

از روش شکار توسط گرگ‌های خاکستری، روشی برای یافتن جواب بهینه در مسائل الهام گرفته شد. به طور خلاصه در الگوریتم GWO، فرایند جستجو با ایجاد یک جمعیت تصادفی از گرگ‌های خاکستری (راه‌حل‌های کاندید) شروع می‌شود. در طول دوره تکرار، گرگ‌های آلفا، بتا و دلتا موقعیت احتمالی شکار را برآورد می‌کنند. گرگ‌های خاکستری عمدتاً با توجه به موقعیت آلفا، بتا و دلتا به فرایند جستجو می‌پردازند. آن ها برای جستجوی شکار از یکدیگر فاصله گرفته و برای حمله به آن به یکدیگر نزدیک شده و همکاری می‌کنند [۲۴].

پیچیدگی زمانی الگوریتم ژنتیک به شدت وابسته به تعداد جمعیت و تعداد نسل‌های مورد استفاده است. در صورت استفاده از n بعد در فضای جستجو، پیچیدگی زمانی الگوریتم ژنتیک $O(n * k * g)$ خواهد بود که در آن k تعداد جمعیت و g تعداد نسل‌های مورد استفاده در الگوریتم است. پیچیدگی زمانی الگوریتم ازدحام ذرات به شدت وابسته به تعداد ذرات و تعداد بعد در فضای جستجو است. در صورت استفاده از n بعد در فضای جستجو، پیچیدگی

زمانی الگوریتم ازدحام ذرات $O(n * p * i)$ خواهد بود که در آن p تعداد ذرات و i تعداد تکرارهای مورد استفاده در الگوریتم است.

پیچیدگی زمانی الگوریتم کلونی زنبور عسل به شدت وابسته به تعداد کلون‌ها، تعداد عامل‌ها در هر کلون و تعداد نسل‌های مورد استفاده است. در صورت استفاده از n بعد در فضای جستجو، پیچیدگی زمانی الگوریتم کلونی زنبور عسل $O(n^2*m*\log(n))$ خواهد بود که در آن n تعداد عامل‌ها (مورچه ها) در هر کلون و m تعداد لبه های مورد استفاده در الگوریتم است [۲۳].

پیچیدگی زمانی الگوریتم گرگ خاکستری به شدت وابسته به تعداد گرگ‌ها و اندازه جمعیت مورد استفاده است. پیچیدگی زمانی الگوریتم گرگ خاکستری $O(n*m*maxiter)$ خواهد بود که در آن n اندزه جمعیت و m تعداد گرگها و حداکثر تعداد تکرارهای مورد استفاده در الگوریتم است [۲۴].

همچنین در مورد پیچیدگی الگوریتم های یادگیری ماشین هر چه تعداد لایه‌ها کمتر باشد، زمان آموزش کاهش می‌یابد. علاوه بر آن هر چه شبکه مختصرتر باشد، پیچیدگی آن نیز کمتر است .طبق فرمول های (۱) و (۲)

$$f = 0.99 \times p + 0.01 \times l \qquad (۱)$$

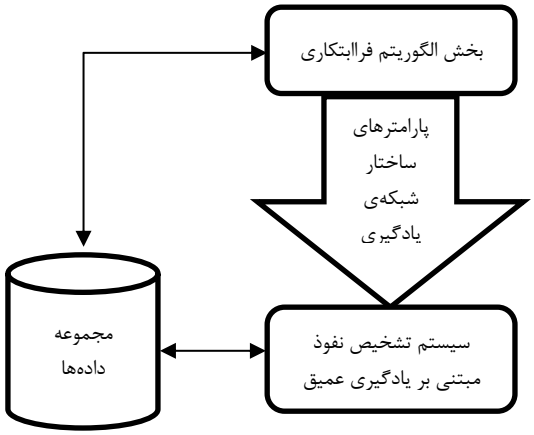
$$p = \frac{N_{correct}}{N_{all}} \qquad (۲)$$

Ncorrect تعداد تشخیص صحیح، Nall تعداد کل نمونه های داده وp طبق فرمول به عنوان نرخ تشخیص صحیح به دست می‌آید. l نسبت معکوس با تعداد لایه‌های مخفی دارد و به شکل عددی بین صفر تا یک می‌باشد، هر چقدر تعداد لایه‌های مخفی بیشتر باشد این مقدار به صفر نزدیک تر است.برای سایر روش ها این مقدار محاسبه گردیده که رقم بالاتری دارد.

۴-راهکار پیشنهادی

در این پژوهش به نحوه طراحی سیستم تشخیص نفوذ پرداخته شد. این سیستم شامل دو بخش اصلی است، بخش ابتدایی که با استفاده از الگوریتم فرا ابتکاری و مجموعه داده‌ها، راه‌حل مناسبی برای مقادیر پارامترهای شبکه‌ی یادگیری عمیق می‌یابد. بخش دوم سیستم تشخیص نفوذ مبتنی بر یادگیری عمیق است که با استفاده از داده‌های بخش اول شبکه‌ی یادگیری عمیق را تشکیل داده و سیستم تشخیص نفوذ را برای بررسی داده‌ها مهیا می‌کند. برای بالابردن دقت سیستم تشخیص نفوذ استفاده از رویکرد الگوریتم‌های فراابتکاری انتخاب گردید (شکل ۱). سپس با استفاده از ابزار تنسورفلو که مبتنی بر زبان پایتون می‌باشد، طرح پیشنهادی پیاده‌سازی شد و روی مجموعه داده‌های KDDCUP99 و UNSW-NB15 و Bot-IoT اجرا گردید.

در این پژوهش چهار الگوریتم ژنتیک، بهینه‌سازی ازدحام ذرات، زنبور عسل مصنوعی، بهینه‌سازی گرگ خاکستری استفاده شد که نتایج حاصل از هر چهار الگوریتم نزدیک به هم هستند. بنابراین در این رابطه می‌توان گفت سیستم تشخیص نفوذی مبتنی بر یادگیری عمیق هر اندازه که برای یک مجموعه داده یا یک شبکه‌ی خاص به خوبی تنظیم گردد اما با بروزرسانی شبکه یا انتقال به شبکه‌ی دیگر کارایی اولیه خود را از دست بدهد، اما با استفاده از الگوریتم‌های فرا ابتکاری برای تنظیم شبکه‌ی یادگیری عمیق به شکل پویا و براساس داده‌های بروز، این مشکل برطرف می‌گردد که در مقالات گذشته کمتر مورد توجه قرار گرفته است.



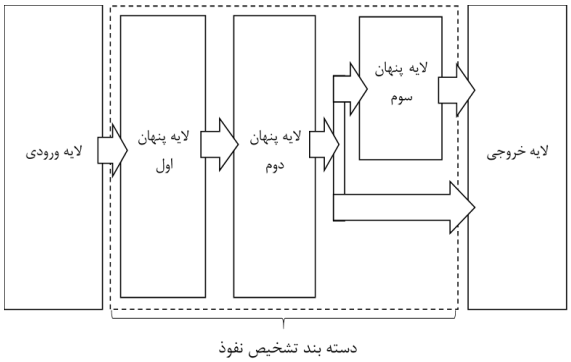
شکل ۱. ساختار کلی روش پیشنهادی شامل دو بخش اصلی است که ابتدا بخش الگوریتم فرا ابتکاری عمل کرده و نتیجه‌ی آن انتخاب پارامترهای تعیین کننده در سیستم تشخیص نفوذ مبتنی بر یادگیری عمیق است.

۴-۱- بخش الگوریتم فراابتکاری

الگوریتم‌های فراابتکاری (تکاملی) که مبتنی بر جمعیت اولیه هستند و به تدریج و مرور زمان به سمت حالت بهینه حرکت می‌کنند. این روش‌ها شامل چند جزء اصلی هستند که در برخی الگوریتم‌ها همه یا تعدادی از این اجزاء با الهام از زندگی موجودات زنده، قوانین فیزیکی یا شیمیایی و ... به

سمت یافتن حالت بهتر حرکت می‌کنند. از اجزاء اصلی می‌توان به عملیاتی چون انتخاب، ترکیب، جهش، تابع برازش و ... اشاره نمود.

ساختار کلی الگوریتم فراابتکاری مطابق شکل (۱) می‌باشد. در ساختار استفاده شده ابتدا براساس مسئله جمعیت اولیه‌ی مناسب به تعداد مشخص شده در پارامترهای الگوریتم ایجاد می‌گردد. برای هر نمونه از جمعیت تابع برازشی اجرا می‌گردد که نشان دهنده بهینگی جواب می‌باشد. این تابع برازش می‌تواند براساس دقت سیستم یادگیری عمیق یا برحسب میزان خطای سیستم باشد که در زمان اجرا توسط کاربر قابل تغییر است. پس از برازش جمعیت اولیه نمونه‌ها براساس این مقدار رتبه‌بندی می‌شوند تا در ادامه براساس الگوریتم پیاده‌سازی شده عملیاتی از قبیل ترکیب جمعیت‌ها، جهش نمونه‌ها، حرکت به سمت بهینه‌های محلی و ... روی آنها صورت پذیرد. پس از تولید نمونه‌های جدید از نمونه‌های قبلی تابع برازش روی نمونه‌های جدید انجام گرفته و در صورت بهتر شدن نمونه‌های جدید جایگزین نمونه‌های قبلی می‌شوند، بدین ترتیب تعداد نمونه‌ها در هر دور ثابت می‌باشند و به سمت بهترشدن حرکت می‌نمایند. پس از اتمام هر دور از الگوریتم فراابتکاری اگر شرایط خاتمه الگوریتم فرارسیده باشد الگوریتم متوقف شده و بهترین جواب به دست آمده برای بخش دوم که سیستم تشخیص نفوذ مبتنی بر یادگیری عمیق است ارسال می‌گردد.



شکل ۲. ساختار سیستم تشخیص نفوذ مبتنی بر شبکه باور عمیق یکی از مشکلاتی که ممکن است در روش‌های یادگیری ماشین خصوصاً شبکه‌های یادگیری عمیق باعث اثرات منفی گردد، مسئله‌ی بیش برازش است که در جهت رفع این مشکل از لایه‌های حذف تصادفی در بین لایه‌ها استفاده شده است.

۴-۲-بخش شبکه‌ی یادگیری عمیق

پس از تکمیل مرحله‌ی قبل نمونه‌ی بهینه‌ای که ساختار شبکه‌ی یادگیری عمیق را ایجاد می‌کند به دست می‌آید. حال با توجه به این نمونه شبکه‌ای از لایه‌های مختلف مطابق شکل (۲) ایجاد می‌گردد که تعداد لایه‌های آن و تعداد نرون‌های هر لایه براساس نمونه تعیین می‌شود.

الگوریتم ۱. شبه‌کد روش پیشنهادی

f_i : the best of this generation
f_{best} : the global best
PART ONE: Methaheuristic Algorithm
1: Initialization
2: Calculate the fitness of initial population
$f = 0.99 \times p + 0.01 \times l$
3: for I from 1 to 50
4: Do one generation of Metaheuristic Algorithm
5: Calculate fitness value
6: if $f_i > f_{best}$
7: $f_{best} \leftarrow f_i$
8: end if
9: end for
PART TWO: Deep Belief Network
10: extract L and N from f_{best}
11: for I from 1 to L
12: training the I^{th} RBM
13: end for
14: fine-tune the RBM and Back Propagation
15: Test IDS-DBN with test set

شبه کد روش پیشنهادی در الگوریتم شماره ۱ قابل رؤیت می‌باشد. همانطور که قبلاً بیان شد روش پیشنهادی از دو قسمت تشکیل شده است. قسمت اول الگوریتم فراابتکاری است که به تعداد مشخصی تکرار می‌شود تا به نتیجه‌ی بهینه دست یابد. سپس در قسمت دوم که بخش شبکه‌ی باور عمیق است در دو مرحله ایجاد می‌گردد. در مرحله نخست هر لایه‌ی RBM به شکل جدا آموزش داده می‌شود و پس از آموزش هر لایه، لایه‌ی بعدی مانند پشته بر روی آن قرار می‌گیرد. در مرحله دوم لایه‌ی آخر به عنوان شبکه عصبی پس انتشار تنظیم می‌شود و به اصلاح شبکه‌ی یادگیری می‌پردازد تا میزان خطا به کمترین مقدار برسد.

۵-۱- ارزیابی و نتایج

در این بخش نتایج بدست آمده بررسی و ارزیابی میشود.

۵-۱-پارامترهای شبیه سازی

مجموعه داده KDDCUP99 در سال ۱۹۹۹ توسط Stolfo و همکارانش براساس داده‌های ثبت شده در پروژه ارزیابی سیستم تشخیص نفوذ به نام DARPA'98 ساخته شد و پس از آن به عنوان مجموعه داده‌ی ارزیابی روش‌های تشخیص نفوذ، بالاترین کاربرد را داشته است. این مجموعه داده شامل حدود ۴۹۰ هزار رکورد می‌باشد که هر نمونه‌ی آن دارای ۴۱ ویژگی و یک برچسب است که برچسب نرمال بودن یا نوع حمله را نشان می‌دهد. به علت وجود مشکلاتی

همچون ناهمواری توزیع حملات در مجموعه‌های KDDCUP99، تحقیقاتی در خصوص تغییرات و متناسب سازی انجام صورت گرفته است؛ مانند مقاله Portnoy و همکارانش در سال ۲۰۰۱ که مجموعه آموزشی را به ده زیرمجموعه شامل ۴۹۴ هزار نمونه تقسیم نمودند و از میان آن‌ها بهترین زیرمجموعه را با نام KDD99_10Percent به عنوان مجموعه‌ی آموزش و از داده‌های آزمایشی نیز مجموعه‌ای با نام Corrected شامل ۳۱۱ هزار نمونه را ارائه نمودند [۱۸]. اغلب تحقیقاتی که در حوزه‌ی تشخیص نفوذ انجام شده به جای مجموعه‌ی اصلی KDDCUP99 از این دو مجموعه آموزشی و آزمایشی استفاده کرده‌اند. در این پژوهش ابتدا دقت کل و سپس معیارهای ضروری برای هر گروه از حملات مورد ارزیابی قرار گرفت. جزئیات گروه‌های حملات مربوط به داده‌های آموزش و آزمایش این مجموعه داده در جدول ۲ آمده است.

جدول ۲. تعداد داده‌های درون مجموعه داده KDDCUP99 به تفکیک گروه حملات

نام گروه حملات	تعداد در مجموعه آموزشی	تعداد در مجموعه آزمایشی	جمع کل	درصد از کل
Normal	۹۷۲۷۸	۶۰۵۹۱	۱۵۷۸۶۹	%۱۹/۶
DoS	۳۹۱۴۵۸	۲۲۹۸۵۳	۶۲۱۳۱۱	%۷۷/۲
U2R	۵۲	۲۲۸	۲۸۰	%۰/۰۴
R2L	۱۱۲۶	۱۶۱۸۹	۱۷۳۱۵	%۲/۱۶
Probe	۴۱۰۷	۴۱۶۶	۸۲۷۳	%۱

در مجموعه داده UNSW-NB15 با ابزار IXIA PerfectStorm ترافیک شبه واقعی عادی و غیرعادی شبیه‌سازی شده است. در ساختاری که برای ایجاد مجموعه داده UNSW-NB15 استفاده شده علاوه بر ابزار IXIA PerfectStorm از ابزار Tcpdump برای استخراج بسته‌ها از واسط شبکه نیز استفاده شده است [۱۹].

در جدول ۳، خصوصیات مجموعه داده UNSW-NB15 به صورت آماری ارائه شده است که نشان دهنده مدت زمان شبیه‌سازی، تعداد جریان‌های منبع، تعداد بسته‌های مبدأ، تعداد بسته‌های مقصد، انواع پروتکل، تعداد بسته‌های ارسالی عادی و مخرب و تعداد آدرس‌های IP مبدأ/مقصد است.

جدول ۳. آمار و خصوصیات داده‌های درون مجموعه داده UNSW-NB15 [۱۹]

ویژگی‌های آماری		۱۶ ساعت	۱۵ ساعت
تعداد جریان‌ها		۹۸۷۶۲۷	۹۷۶۸۸۲
بایت منبع		۴۸۶۰۱۶۸۸۶۶	۵۹۴۰۵۲۳۷۲۸
بایت مقصد		۴۴۷۴۳۵۶۰۹۴۳	۴۴۳۰۳۱۹۵۵۰۹
بسته‌های منبع		۴۱۱۶۸۴۲۵	۴۱۱۲۹۸۱۰
بسته‌های مقصد		۵۳۴۰۲۹۱۵	۵۲۵۸۵۴۶۲
نوع پروتکل	TCP	۷۷۱۴۸۸	۷۲۰۶۶۵
	UDP	۳۰۱۵۲۸	۶۸۸۶۱۶
	ICMP	۱۵۰	۳۷۴
	Others	۱۵۰	۳۷۴
برچسب	عادی	۱۰۶۴۹۸۷	۱۱۵۳۷۷۴
	حمله	۲۲۲۱۵	۲۹۹۰۶۸
منحصر به فرد	IP مبدأ	۴۰	۴۱
	IP مقصد	۴۴	۴۵

پارامترهای عمومی مورد استفاده در الگوریتم‌های فراابتکاری در جدول شماره ۴ ذکر شده است.

تعداد نورونها در لایه ورودی برابر با تعداد ویژگی های مجموعه داده میباشد و تعداد نورونها در لایه خروجی برابر با تعداد کلاسهای حملات در مجموعه داده میباشد. برای لایه های پنهان که بین لایه ورودی و خروجی قرار دارند، تعداد نورونها از راه حل بدست امده از فاز اول استفاده میگردد. تعداد نورونها هر لایه طبق رابطه زیر محاسبه میگردد.

$$N_i = 8 + \left[\frac{n_i}{64} \times 56\right] \qquad (۳)$$

دراینجا n_i عددی است که از راه حل بدست امده از الگوریتم فراابتکاری برای راه حل iام مشخص شده است. چون تعداد نورون ها از ۶ بیت بدست میاید پس این عداد بین صفر تا ۶۴ میباشد. طبق تجربیات بدست امده تعداد نورون خیلی کم سبب کاهش دقت و کارایی شبکه یادگیری عمیق میگردد. بنابراین برای رفع این مشکل با یتفاده از فرمول فوق تضمین میشود که اعداد زیر ۸ برای تعداد نورون در نظر گرفته نشود و حد بالای نورون ۶۴ در نظر گرفته شود.

جدول ۴. پارامترهای مورد استفاده در الگوریتم‌های فراابتکاری

ردیف	پارامتر	مقدار
۱	جمعیت اولیه	۲۰
۲	تعداد تکرار	۵۰
۳	تعداد بیت هر جمعیت	۲۰
۴	تعداد لایه های پنهان	۳
۵	تعداد نرونهای لایه پنهان	۶۴>تعداد نورون>۸

هر نمونه‌ی جمعیت یا کروموزوم در این الگوریتم‌ها شامل ۲۰ بیت می‌باشد که به چهار قسمت تقسیم می‌گردد. قسمت اول تعداد لایه‌های شبکه‌ی یادگیری عمیق را مشخص می‌کند که بین ۲ یا ۳ لایه متغیر است. قسمت دوم و سوم و چهارم تعداد نرون‌های هر لایه را مشخص می‌کنند.

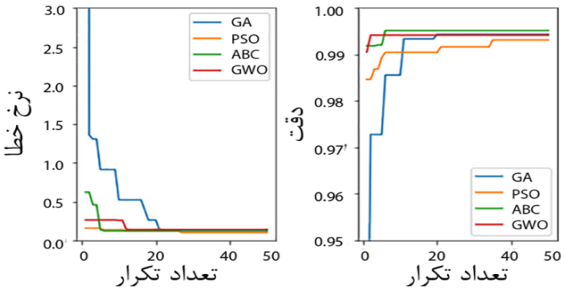
پیاده‌سازی روی یک سیستم رایانه‌ای شخصی با پردازنده i7-7700 اینتل و رم ۸ گیگابایت اجرا شد. برای پیاده‌سازی از زبان پایتون استفاده شده است. تمامی شبکه‌های باور عمیق با استفاده از کتابخانه keras پیاده‌سازی گردید [۲۰]. کتابخانه keras از کتابخانه قوی TensorFlow بهره می‌برد [۲۱]. برای پردازش و استانداردسازی داده‌های مورد استفاده از کتابخانه‌های pandas و numpy استفاده شد. برای ارزیابی و محاسبه معیارهای مورد نظر از کتابخانه scikit-learn که در حوزه یادگیری ماشین بسیار قوی عمل می‌کند استفاده شد [۲۲].

در این مقاله داده ها به سه مجموعه تقسیم شده است. ٪۷۰ داده برای اموزش، ٪۲۰ برای تست و ٪۱۰ برای اعتبار سنجی استفاده شده است.

۵-۲-ارزیابی دقت

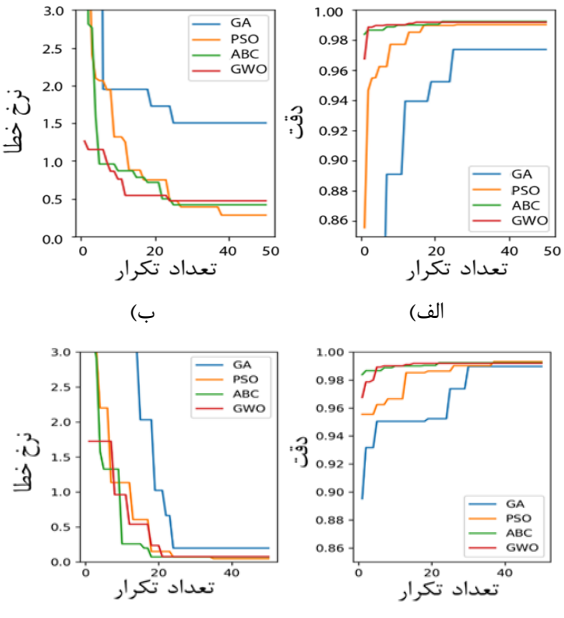
دو معیار بسیار مهم در طراحی شبکه‌ی یادگیری عمیق در مقالات مورد استفاده قرار می‌گیرد. این دو معیار عبارتند از دقت و از دست دادن (مقدار خطا) که در شکل (۳) نتایج به دست آمده برای الگوریتم‌های فراابتکاری «الگوریتم ژنتیک»، «بهینه‌سازی ازدحام ذرات»، «زنبور عسل مصنوعی» و «بهینه‌سازی گرگ خاکستری» به نمایش درآمده است.

با توجه به نتایج روی مجموعه داده‌های KDDCup می‌توان نتیجه گرفت که الگوریتم زنبور عسل مصنوعی در به دست آوردن دقت عملکرد بهتری دارد اما در مبحث میزان خطا هرچند PSO، GA و ABC به ترتیب نتایج بهتری به دست می‌آورند اما نتایج همه‌ی آنها پس از ۵۰ بار تکرار نزدیک به هم می‌باشد. در زمینه‌ی میزان خطا الگوریتم‌های ABC و PSO بسیار به هم نزدیکند به سرعت به مقدار بهینه می‌رسند و پس از آن دو الگوریتم GWO سریعتر به نتایج بهینه می‌رسد و در انتها الگوریتم ژنتیک با تأخیر به مقادیر بهینه دست می‌یابد.



الف) ب)

شکل -۳. میزان معیار به دست آمده از اجرای الگوریتم‌های ژنتیک، ازدحام ذرات، زنبورعسل مصنوعی و گرگ خاکستری الف) دقت ب) از دست دادن (خطای تشخیص) برای مجموعه داده‌های KDDCup



الف) ب) ج) د)

شکل ۴. میزان معیار به دست آمده از اجرای الگوریتم‌های ژنتیک، ازدحام ذرات، زنبورعسل مصنوعی و گرگ خاکستری الف) دقت ب) از دست دادن (خطای تشخیص) برای مجموعه داده‌های UNSW-NB15 ج) دقت د) خطای تشخیص برای مجموعه داده‌های Bot-IoT

همانطور که در نتایج مربوط به نمودارهای فوق قابل مشاهده است در به دست آوردن دقت الگوریتم‌های زنبورعسل مصنوعی و گرگ خاکستری و پس از آن ازدحام

ذرات به دقت بالاتری دست پیدا کردند، در حوزه میزان خطا الگوریتم‌های ازدحام ذرات، زنبورعسل مصنوعی و گرگ خاکستری به ترتیب میزان خطای کمتری به دست آورده‌اند و پس از آن الگوریتم ژنتیک با اختلاف میزان خطای بیشتری را به دست آورده است.

از نتایج روی مجموعه داده‌ها مشخص است که کارکرد الگوریتم‌ها در هر دو مجموعه داده‌ها با اختلاف جزئی مشابه هم عمل می‌کنند.

در حوزه‌ی دقت الگوریتم‌های ABC و GWO سریعتر به مقدار بهینه و بالای ٪۹۹ دست پیدا می‌کنند و پس از آن دو الگوریتم‌های PSO و GA به دقت بالای ٪۹۹ می‌رسند. نکته‌ی حائز اهمیتی که در الگوریتم بهینه‌سازی گرگ خاکستری وجود دارد آن است که از همان مراحل اولیه دقت بالایی به دست می‌آورد که به دلیل پراکندگی نمونه‌های جمعیت و سپس هدایت جمعیت به سمت سه نمونه‌ی برتر در حل این نوع مسائل می‌باشد.

جدول۵. مقدار میانگین بازخوانی برای الگوریتم‌های فراابتکاری پیاده‌سازی شده

نام الگوریتم		مقدار میانگین بازخوانی		
		KDDCup	UNSW-NB15	Bot-IoT
فراابتکاری	ژنتیک	٪ ۹۹/۴	٪ ۹۸/۷	٪ ۹۹/۱
	بهینه‌سازی ازدحام ذرات	٪ ۹۹/۳	٪ ۹۹/۱	٪ ۹۹/۳
	زنبور عسل مصنوعی	٪ ۹۹/۵	٪ ۹۹/۱	٪ ۹۹/۴
	بهینه‌سازی گرگ خاکستری	٪ ۹۹/۴	٪ ۹۹/۳	٪ ۹۹/۶
یادگیری عمیق بدون الگوریتم فراابتکاری		٪ ۹۲/۱	٪ ۹۰/۳	٪ ۹۱/۵

همه‌ی الگوریتم‌های فراابتکاری استفاده شده پس از تعداد مشخصی تکرار به مقداری بالای ٪۹۹ در میزان تشخیص صحیح حملات دست می‌یابند. در صورتی که اگر شبکه‌ی یادگیری عمیق بدون بهینه‌سازی الگوریتم فراابتکاری استفاده شود در حالت میانگین به مقداری حدود ٪۹۲ دست پیدا می‌کند.

جدول ۶. مقدار میانگین بازخوانی برای گروه حملات مختلف در مجموعه داده

گروه حملات	مقدار میانگین بازخوانی			
	ژنتیک	بهینه‌سازی ازدحام ذرات	زنبور عسل مصنوعی	بهینه‌سازی گرگ خاکستری
DoS	٪ ۹۹/۲	٪ ۹۹/۰۲	٪ ۹۹/۴۲	٪ ۹۹/۲۵
R2L	٪ ۸۵/۱۱	٪ ۸۴/۳۶	٪ ۸۷	٪ ۹۰/۱۴
U2R	٪ ۷۲/۴۱	٪ ۷۴/۹۶	٪ ۷۴/۱۲	٪ ۷۳
Probe	٪ ۷۹/۳	٪ ۷۳/۲۲	٪ ۸۷/۴	٪ ۸۷/۱
میانگین کل	٪ ۹۹/۱	٪ ۹۸/۹	٪ ۹۹/۲	٪ ۹۹/۲

در گروه حملاتی که در مجموعه داده‌های مورد استفاده قرار دارد و نتایج مقدار بازخوانی در گروه حملات ممانعت از خدمات (DoS) بهترین نتیجه بدست می‌آید. در این گروه حملات همه‌ی الگوریتم‌ها نتایج مشابهی به دست آورده‌اند. در زمینه کشف حملات ارتباط راه‌دور به وسیله محلی الگوریتم گرگ خاکستری، در گروه حملات دسترسی به هسته الگوریتم بهینه‌سازی ازدحام ذرات، در گروه حملات کاوش الگوریتم ژنتیک نتایج بهتری به‌دست آورده‌اند. در جدول F1-Score مقدار این معیار برای الگوریتم‌های GA، PSO، ABC و GWO آمده است.

جدول ۷. مقدار میانگین F1-Score برای الگوریتم‌های فراابتکاری پیاده‌سازی شده

نام الگوریتم		مقدار میانگین F1-Score		
		KDDCup	UNSW-NB15	Bot-IoT
فراابتکاری	شبکه‌ی باور عمیق - ژنتیک	٪ ۹۸/۳	٪ ۹۷/۵	٪ ۹۸/۸
	شبکه‌ی باور عمیق - بهینه‌سازی ازدحام ذرات	٪ ۹۸/۴	٪ ۹۸/۱	٪ ۹۹/۱
	شبکه‌ی باور عمیق - زنبور عسل مصنوعی	٪ ۹۹/۲	٪ ۹۸	٪ ۹۹/۴
	شبکه‌ی باور عمیق - بهینه‌سازی گرگ خاکستری	٪ ۹۹	٪ ۹۸/۸	٪ ۹۹/۶
شبکه‌ی باور عمیق بدون الگوریتم فراابتکاری		٪ ۹۳/۷	٪ ۹۰/۱	٪ ۹۲/۸

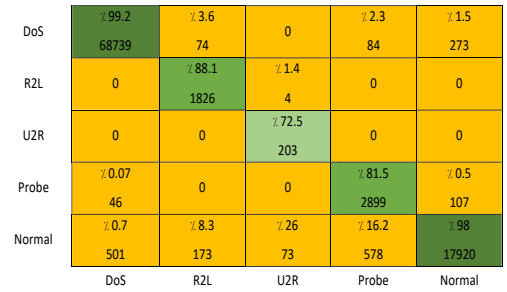
با توجه به نتایج به دست آمده تمامی الگوریتم‌های فراابتکاری مقدار F1-Score را برای مجموعه داده‌های KDDCup و Bot-IoT بالای ۹۸٪ و برای مجموعه داده‌های UNSW-NB15 بالای ۹۷٪ به دست آورده‌اند، این در حالی است که یادگیری عمیق به تنهایی به حداکثر مقدار ۹۳/۷٪ می‌رسد.

جدول ۸. مقدار میانگین F1-Score برای گروه حملات مختلف در مجموعه داده

گروه حملات	مقدار میانگین F1-Score			
	ژنتیک	بهینه‌سازی ازدحام ذرات	زنبور عسل مصنوعی	بهینه‌سازی گرگ خاکستری
DoS	٪ ۹۹/۳	٪ ۹۹/۰۵	٪ ۹۹/۴۲	٪ ۹۹/۴
R2L	٪ ۸۶/۰۲	٪ ۸۴/۷۹	٪ ۸۷/۵۴	٪ ۹۱/۸۵
U2R	٪ ۷۱/۷۲	٪ ۷۵/۶۱	٪ ۷۵/۶۷	٪ ۷۳/۷۷
Probe	٪ ۸۴/۹۳	٪ ۷۵/۴۳	٪ ۸۵/۷۹	٪ ۸۷/۲۶
میانگین	٪ ۹۹/۱	٪ ۹۸/۹	٪ ۹۹/۳	٪ ۹۹/۳

در گروه‌های حملات موجود در مجموعه داده که مورد بررسی قرار گرفته است، نتایج فوق برای هر الگوریتم فراابتکاری به دست آمده که میزان تشخیص هر چهار الگوریتم در مورد گروه حملات ممانعت از خدمات نزدیک به هم و بالای ٪۹۹ می‌باشد. در حوزه حملات دسترسی راه‌دور به وسیله محلی الگوریتم بهینه‌سازی گرگ خاکستری با ٪۹۱ بهترین عملکرد را دارد، در مورد حملات دسترسی به هسته الگوریتم‌های بهینه‌سازی ازدحام ذرات و زنبور عسل مصنوعی با ٪۷۵ نتیجه بهتری به دست آورده‌اند و در حملات کاوش الگوریتم ژنتیک با ٪۸۵ بیشترین مقدار F1-Score را به خود اختصاص داده است.

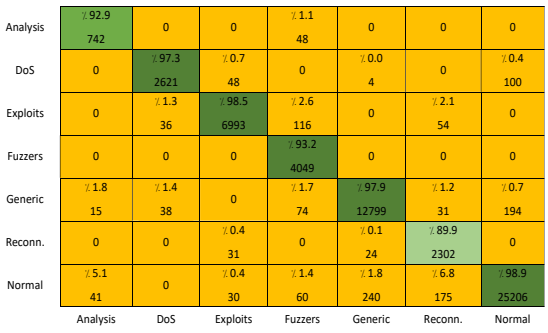
در شکل (۵) ماتریس درهم ریختگی مربوط به مجموعه داده‌های KDDCup مشاهده می‌شود. در این مجموعه داده بیشترین آمار مربوط به حملات DoS و ترافیک عادی می‌باشد. عملکرد سیستم تشخیص نفوذ در تشخیص ترافیک عادی و حملات DoS بسیار خوب می‌باشد. اما حملات نوع U2R که از لحاظ آماری کمترین مقدار حمله در مجموعه داده‌ها است میزان تشخیص ٪ ۷۲/۵ را نشان می‌دهد. دلیل آن هم تعداد بسیار کم این تعداد حمله در مجموعه‌ی داده می‌باشد که شبکه‌ی یادگیری عمیق به دلیل کم بودن آمار این نوع حمله الگوی مناسب آن را نمی‌تواند به خوبی تشخیص دهد. بنابراین دچار مقداری خطا در تشخیص آن می‌گردد.



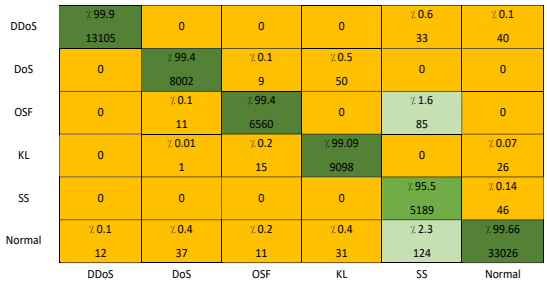
شکل ۵. ماتریس درهم ریختگی برای مجموعه داده KDDCup

در شکل (۶) ماتریس درهم ریختگی برای مجموعه داده‌ی UNSW-NB15 مشاهده می‌شود. در این نمودار مشخص است که میزان دقت تشخیص در یافتن حملات DoS، Exploits و Generic دارای دقت بسیار خوبی بوده و همچنین ترافیک عادی سیستم را نیز با دقت بالا تشخیص می‌دهد. بنابراین می‌توان گفت تشخیص ترافیک عادی از حمله در حد بالایی است و این امر سبب می‌شود سیستم تشخیص نفوذ در شبکه عملکرد عادی شبکه را دچار اختلال جدی نخواهد کرد.

در شکل (۷) ماتریس در هم ریختگی برای مجموعه داده‌های Bot-IoT ارائه شده است. این مجموعه داده که مربوط به اینترنت اشیاء می‌باشد و بیشتر حملات این نوع شبکه‌ها را در خود دارد برای بررسی کارایی سیستم ما بسیار حائز اهمیت است. آنچه مشاهده می‌شود این است که دقت در تشخیص حملات در انواع حمله‌ی موجود در مجموعه داده در حد خیلی خوبی می‌باشد. این سیستم تشخیص نفوذ می‌تواند با کمترین اختلال در کنار شبکه‌ی اینترنت اشیاء قرار گرفته و امنیت را تا حد بسیار خوبی برای شبکه تأمین نماید.



شکل ۶. ماتریس درهم ریختگی برای مجموعه داده UNSW-NB15



شکل ۷. ماتریس درهم ریختگی برای مجموعه داده Bot-IoT

۵-۳- مقایسه با سایر روش ها

نتایج نهایی در زمینه نرخ تشخیص (دقت) که در مقالات و منابع ذکر شده در جدول زیر آمده است.

جدول۹. مقایسه نتایج روش پیشنهادی با کارهای مرتبط

حوزه پژوهش	روش کار	مجموعه داده‌های استفاده شده	دقت تشخیص
شبکه	شبکه عصبی کانولوشن [۶]	NSL-KDD	٪ ۹۷
اینترنت اشیاء	خوشه بندی و درخت تصمیم [۱۰]	Intel Dataset	٪ ۹۷
	کاهش ویژگی ها و مدل بیز ساده [۱۱]	NSL-KDD	٪ ۸۶
	شبکه باور عمیق [۱۳]	NSL-KDD	٪ ۹۸
	شبکه عصبی کانولوشن روی حملات Botnet [۱۷]	Bot-IoT	٪ ۹۹/۴
	شبکه عصبی بازگشتی عمیق [۱۶]	Bot-IoT	٪ ۹۹/۵
	روش پیشنهادی	KDDCup	٪ ۹۹/۴
		UNSW-NB15	٪ ۹۹/۲
		Bot-IoT	٪ ۹۹/۶

طبق اطلاعات این جدول، روش پیشنهادی، در میزان دقت تشخیص حملات نسبت به کارهای ذکر شده بهتر بوده و با کسب٪۹۹/۶ دقت عملکرد قابل قبولی ارائه نموده است. دلیل این امر نیز استفاده از الگوریتم‌های فرا ابتکاری در انتخاب پارامترهای شبکه‌ی یادگیری عمیق بوده است. همانطور که در مورد پیاده‌سازی توضیح داده شد در روش پیشنهادی براساس مجموعه داده کوچکی و با استفاده از الگوریتم‌های فراابتکاری ابرپارامترهای مناسبی به دست می‌آید که ساختار شبکه‌ی باور عمیق با توجه به این ابرپارامترها ایجاد می‌گردد، بنابراین سیستم تشخیص نفوذی که به وجود می‌آید با مجموعه داده‌ها متناسب بوده و کارایی بهتری به ارمغان می‌آورد.

۶- نتیجه‌گیری

یکی از مسائل و چالش‌های حوزه یادگیری ماشین و شبکه‌ی یادگیری عمیق آن است که ابرپارامترهای مناسب براساس مسئله چگونه انتخاب شود. این مسئله توسط الگوریتم‌های فرا ابتکاری قابل حل بوده و می‌توان آن را به شکل مسئله‌ی بهینه‌سازی در نظر گرفت. در این پژوهش به مسئله سیستم‌های تشخیص نفوذ در اینترنت اشیاء پرداخته شد. در این راستا با استفاده از یادگیری عمیق که در حوزه دسته‌بندی و تشخیص الگو یکی از قوی‌ترین و جدیدترین روش‌های این حوزه می‌باشد استفاده گردید. نتایج به دست آمده نشان داد که استفاده از الگوریتم فراابتکاری در یافتن ساختار بهینه برای سیستم تشخیص نفوذ مبتنی بر یادگیری عمیق سبب شد که بیش از ۶٪ دقت تشخیص حملات بهبود یابد. در این پژوهش چهار الگوریتم ژنتیک، بهینه‌سازی ازدحام ذرات، زنبور عسل مصنوعی، بهینه‌سازی گرگ خاکستری استفاده شد که نتایج حاصل از هر چهار الگوریتم نزدیک به هم هستند. بنابراین در این رابطه می‌توان گفت سیستم تشخیص نفوذی مبتنی بر یادگیری عمیق هر اندازه که برای یک مجموعه داده یا یک شبکه‌ی خاص به خوبی تنظیم گردد اما با بروزرسانی شبکه یا انتقال به شبکه‌ی دیگر کارایی اولیه خود را از دست بدهد، اما با استفاده از الگوریتم‌های فرا ابتکاری برای تنظیم شبکه‌ی یادگیری عمیق به شکل پویا و براساس داده‌های بروز، این مشکل برطرف می‌گردد. پیشنهاد می‌گردد که محققین در آینده در شبکه‌های خاص مانند شبکه‌های خودرویی یا شبکه‌های پرنده‌های بدون سرنشین از سیستم پیشنهادی برای تشخیص نفوذ استفاده کنند. علاوه بر این، می‌توان از الگوریتم‌های فراابتکاری جدیدتر که در حوزه مسائل گسسته عملکرد مناسبی دارند نیز جهت بهبود ابرپارامترها استفاده کرد و به نتایج متفاوتی دست یافت.

مراجع

[1] Haddad Pajouh Hamed, Javidan Reza, Khayami Raouf, Dehghantanha Ali, and Raymond Choo Kim-Kwang. "A Two-layer dimension reduction and two-tier classification model for anomaly-based intrusion detection in IoT backbone networks". IEEE Transactions on Emerging Topics in Computing 7, no. 2 (2016): 314-323.

[2] Asharf, Javed, Nour Moustafa, Hasnat Khurshid, Essam Debie, Waqas Haider, and Abdul Wahab, "A review of intrusion detection systems using machine and deep learning in internet of things: challenges, solutions and future directions". Electronics, 9, no.7 (2020):1-45.

[3] Ankit Thakkar and Ritika Lohiya, "A review on machine learning and deep learning perspectives of IDS for IoT: recent updates, security issues, and challenges". Archives of Computational Methods in Engineering 28, no.4 (2020) 3211-3243.

[4] Chen Yuanfang, Zhang Yan, Maharjan Sabita, Alam Muhammad, and Wu Ting. "Deep learning for secure mobile edge computing". IEEE Network 43, no. 4 (2019): 36-41.

[5] Abdel-Basset Mohamed, Abdel-Fatah Laila, and Sangaiah Arun Kumar , "Metaheuristic algorithms: A comprehensive review". In Computational Intelligence for Multimedia Big Data on the Cloud with Engineering Applications, Academic press (2018):185-231.

[۶] احمدی طاهری، محمدحسن. ارائه روشی مبتنی بر یادگیری عمیق برای تشخیص نفوذ شبکه های کامپیوتری. پایان نامه. مؤسسه آموزش عالی سینا. ۱۳۹۶.

[7] Cervantes Christian, Poplade Diego, Nogueira Michele, and Santos Aldri. "Detection of sinkhole attacks for supporting secure routing on 6LoWPAN for Internet of Things". In: 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM), IEEE,(1015):606-611.

[8] Eung Jun Cho, Jin Ho Kim and Choong Seon Hong. "Attack model and detection scheme for botnet on 6LoWPAN". In: Asia-Pacific network operations and management symposium, Springer(2009):515–518.

[9] João P. Amaral, Luís M. Oliveira, Joel J. P. C. Rodrigues, Guangjie Han, and Lei Shu, "Policy and network-based intrusion detection system for IPv6-enabled wireless sensor networks". In: 2014 IEEE International Conference on Communications (ICC), IEEE (2014):1796 – 1801.

[10] A. Alghuried, "A Model for anomalies detection in Internet of Things (IoT) using inverse weight clustering and decision tree". Masters dissertation, Technological University Dublin (2017).

[11] Atefinia Ramin, and Ahmadi Mahmood, "Network intrusion detection using multi-architectural modular deep neural network". Journal of Supercomputing 71, no. 4 (2021): 3571–3593.

[12] Chawla Shiven, "Deep learning-based intrusion detection system for Internet of Things (Doctoral dissertation) (2017).

[13] Zhang Ying, Li Peisong, and Wang Xinheng, "Intrusion detection for IoT-based on improved genetic algorithm and deep belief network". IEEE Access, 7, 31711-31722, 2019.

[14] Kennedy James, and Eberhart Russell, "Particle swarm optimization". In Proceedings of ICNN'95-International Conference on Neural Networks 4, no.2, (1995):1942-1948.

[15] Hassan Rania, Cohanim Babak, de Weck Olivier and Venter Gerhard. "A comparison of particle swarm optimization and the genetic algorithm". In 46th AIAA/ASME/ASCE/AHS/ASC Structures, Structural Dynamics and Materials conference (2005): 1897-1903 .

[16] Popoola, Segun I., Bamidele Adebisi, Ruth Ande, Mohammad Hammoudeh, Kelvin Anoh, and Aderemi A. Atayero, "SMOTE-DRNN: A deep learning algorithm for botnet detection in the Internet-of-Things networks". Sensors 21, no .9, (2021): 2851-2861.

[17] Idrissi Idriss, Boukabous Mohammed, Azizi Mostafa, Moussaoui Omar, and El Fadili Hakim, "Toward a deep learning-based intrusion detection system for IoT against botnet attacks". IAES International Journal of Artificial Intelligence 10, no.1, (2021): 110-122.

[18] Leonid Portnoy, Eleazar Eskin, and Salvatore J. Stolfo, "Intrusion detection with unlabeled data using clustering", Proceedings of ACM CSS Workshop on Data Mining Applied to Security, (2001):123-132.

[19] Moustafa Noor, and Slay Jill, "UNSW-NB15: A comprehensive dataset for network intrusion detection systems (UNSW-NB15 network data set)". 2015 Military Communications and Information Systems Conference (MilCIS) (2015):1-6.

[20] Chollet François, “keras,” https://github.com/fchollet/keras, 2021.

[21] Abadi Martín, Agarwal Ashish, Barham Paul, Brevdo Eugene, Chen Zhifeng, and Citro Craig, “Tensorflow: large-scale machine learning on heterogeneous distributed systems”. OSDI'16: Proceedings of the 12th USENIX conference on Operating Systems Design and Implementation, (2016): 265–283.

[22] Pedregosa Fabian, Varoquaux Gaël, Gramfort Alexandre, Michel Vincent, and Thirion Bertrand, “Scikit-learn: machine learning in Python”. Journal of Machine Learning Research 12, no. 3, (2011): 2825-2830.

[23] Attiratanasunthron Nattapat, Fakcharoenphol Jittat, “A running time analysis of an Ant Colony Optimization algorithm for shortest paths in directed acyclic graphs”, Information Processing Letters 105, no. 3, (2008): 88-92.

[24] Yan Fu, Xu Jianzhong, Yun Kumchol, “Dynamically dimensioned search grey wolf optimizer based on positional interaction information”, Computational Methods for Modeling, Simulating, and Optimizing Complex Systems 2019, (2019):1-37.