JOURNAL OF SOUTHERN COMMUNICATION ENGINEERING
ISLAMIC AZAD UNIVERSITY BUSHEHR BRANCH
E-ISSN: 2980-9231
https://jce.bushehr.iau.ir
https://doi.org/10.30495/jce.2023.1992146.1215

Vol. 14/ No. 53/Autumn 2024

Research Article

A Distributed Denial-of-Service (DDoS) Attack Detection Approach in Fog Layer Based on Distributed Blockchain Database and Machine Learning

Mohsen Eghbali, PhD Student [1] | Mohammad Reza Mollhoseini Ardakani, Assistant Professor[2*]

[1]Department of Computer Engineering, Maybod Branch, Islamic Azad University, Maybod, Iran, m.eghbali@maybofiau.ac.ir

[2]Department of Computer Engineering, Maybod Branch, Islamic Azad University, Maybod, Iran, mr.mollahoseini@iau.ac.ir

Correspondence
Mohammadreza Mollahoseini Ardakani, Associate Professor, Department of Computer Engineering, Maybod Branch, Islamic Azad University, Maybod, Iran,
mr.mollahoseini@iau.ac.ir

Received: 24 July 2023
Revised: 27 August 2023
Accepted: 13 September 2023

Abstract

DDoS attacks make network services unavailable to users by sending fake traffic by botnets. One of the methods to deal with DDoS attacks is to use machine learning, but these methods face challenges such as high volume of IoT traffic and data imbalance. This paper introduces a distributed intrusion detection system in the fog layer that detects network attack traffic in a decentralized manner. In this method, each fog node acts as an intrusion detection system, and by exchanging blacklists through the blockchain, they increase the secrecy of detecting attacks. Fog nodes identify the main features of network traffic using the Coati optimization algorithm and use these features to train a multilayer neural network in intrusion detection. The selection of features reduces traffic and increases the accuracy and speed of attack detection. Based on game theory, the GAN method is used to balance network traffic. Tests performed in the MATLAB and on the NSL-KDD show that the proposed system has accuracy, sensitivity, and precision of 98.67%, 98.52%, and 98.34%, respectively. This method is more accurate in identifying network attacks than feature selection methods such as WOA, GWO, and HHO and more accurate than LSTM and CNN.

Keywords: The intrusion detection system, Fog layer, Machine learning, GAN neural network, Feature selection, Coati Optimization Algorithm (COA).

Highlights

- Network traffic balancing in fog layer with game theory based on GAN network.
- Presenting a binary version of the Kuati optimization algorithm presented in 2023 for feature selection.
- Maintaining the confidentiality of the proposed intrusion detection system with blockchain and exchanging the blacklist with blockchain between fog nodes.
- Providing a distributed intrusion detection system in the fog layer to detect attacks on IoT.

Citation: M. Eghbali, and M.R. Mollhoseini Ardakani "A Distributed Denial-of-Service (DDoS) Attack Detection Approach in Fog Layer Based on Distributed Blockchain Database and Machine Learning," *Journal of Southern Communication Engineering*, vol. 14, no. 53, pp. 67–90, 2024, doi:10.30495/jce.2023.1992146.1215, [in Persian].

مقاله پژوهشی

یک رویکرد تشخیص حملات توزیع شده در لایه مه و بر اساس پایگاه داده توزیع شده بلاک چین و یادگیری ماشین

محسن اقبالی[۱] | محمّدرضا ملاحسینی اردکانی*[۲]

[۱] دانشجوی دکتری مهندسی کامپیوتر، گروه مهندسی کامپیوتر، واحد میبد، دانشگاه آزاد اسلامی، میبد، ایران، m.eghbali@maybodiau.ac.ir

[۲] استادیار گروه مهندسی کامپیوتر، واحد میبد، دانشگاه آزاد اسلامی، میبد، ایران، mr.mollahoseini@iau.ac.ir

نویسنده مسئول

* محمّدرضا ملاحسینی اردکانی، استادیار گروه کامپیوتر، واحد میبد، دانشگاه آزاد اسلامی، میبد، ایران، mr.mollahoseini@iau.ac.ir

چکیده:

حملات DDoS با ارسال حجم زیادی از ترافیک کاذب توسط باتنت‌ها، سرویس‌های شبکه را از دسترس کاربران خارج می‌کنند. یکی از روش‌های مقابله با حملات DDoS، استفاده از یادگیری ماشین است، اما این روش‌ها با چالش‌هایی مانند حجم بالای ترافیک IoT و عدم توازن در داده‌ها مواجه‌اند. این مقاله سیستم تشخیص نفوذ توزیع‌شده‌ای در لایه مه معرفی می‌کند که به‌صورت غیرمتمرکز ترافیک حملات شبکه را شناسایی می‌کند. در این روش، هر گره مه به عنوان سیستم تشخیص نفوذ عمل کرده و با تبادل لیست سیاه‌ها از طریق بلاکچین، محرمانگی شناسایی حملات را افزایش می‌دهند. گره های مه ویژگی‌های اصلی ترافیک شبکه را با استفاده از الگوریتم بهینه‌سازی کوآتی(Coati) شناسایی کرده و از این ویژگی‌ها برای آموزش شبکه عصبی چندلایه ا در تشخیص نفوذ استفاده می‌کنند. انتخاب ویژگی‌ها ترافیک را کاهش داده و دقت و سرعت شناسایی حملات را افزایش می‌دهد. برای تعادل ترافیک شبکه، از روش GAN بر اساس نظریه بازی‌ها استفاده می‌شود. آزمایش‌ها در محیط نرم‌افزاری متلب و روی NSL-KDD نشان می‌دهد که سیستم پیشنهادی دارای دقت، حساسیت و صحتی به ترتیب ۹۸.۶۷٪، ۹۸.۵۲٪ و ۹۸.۳۴٪ است. این روش در شناسایی حملات شبکه دقیق‌تر از روش‌های انتخاب ویژگی مانند WOA، GWO و HHO و نیز دقیق‌تر از LSTM و CNN است.

کلید واژه‌ها: سیستم تشخیص نفوذ، لایه مه، یادگیری ماشین، شبکه عصبی GAN، انتخاب ویژگی، الگوریتم بهینه‌سازی کوآتی.

تاریخ دریافت:۲ مرداد ۱۴۰۲
تاریخ بازنگری: ۵ شهریور۱۴۰۲
تاریخ پذیرش: ۲۲ شهریور۱۴۰۲

https://doi.org/10.30495/jce.2023.1992146.1215

۱-مقدمه

با توسعه سریع فناوری اینترنت اشیاء[1] زمینه های بیشتری مانند خانه های هوشمند، شهرهای هوشمند، حمل و نقل هوشمند، مدیریت لجستیک هوشمند و غیره در این صنعت بیشتر و بیشتر شده است. پیش بینی می شود که در سال ۲۰۳۰ تعداد دستگاه های IoT مورد استفاده در سراسر جهان نزدیک به ۱۲۵ میلیارد دستگاه خواهد بود[۱]. با این حال، هنوز در برخی از زمینه‌های مرتبط با اینترنت اشیاء از جمله امنیت، حریم خصوصی، مدیریت هویت و غیره مسائلی وجود دارد [۲]. در میان مسائل امنیتی، حملات انکار سرویس توزیع شده[2] یک تهدید جدی است. از آنجایی که اکثر دستگاه‌های اینترنت اشیاء با منابع محدود حافظه و محاسبات محدود هستند، حفاظت امنیتی در این دستگاه ها وجود ندارد. مهاجمان از آسیب‌پذیری‌های موجود

[1] Internet of Things (IoT)
[2] Distributed Denial of Service (DDoS)

در دستگاه‌های IoT سوءاستفاده می‌کنند و آنها را به عنوان بخشی از بات‌نت‌ها[1] برای راه‌اندازی حملات DDoS کنترل می‌کنند [۳]. به عنوان مثال، در سال ۲۰۱۶، یک حمله DDoS معروف به DynDNS، ارائه‌دهنده یک سیستم نام دامنه پویا ، بسیاری از سرویس‌های وب از جمله Github و Twitter را مجبور به توقف کرد. علاوه بر این، نه تنها قربانیان قادر به ارائه خدمات نبودند، بلکه صاحبان دستگاه‌های اینترنت اشیا نیز پول زیادی را برای پهنای باند و توان مصرفی خرج کردند [۴]. هدف حملات DDoS مصرف پهنای باند یا منابع و جلوگیری از دسترسی کاربران قانونی به خدمات است [۵]. محققان مختلف درباره حملات DDoS در سه لایه معماری اینترنت اشیاء بحث کردند. برای لایه ادراک، حملات پارازیت[2]، کشتن دستورات و حملات همگام‌سازی[3] برای جلوگیری از خواندن داده‌ها از RFID وجود دارد [۶]. در لایه شبکه، حملات لایه با هدف از بین بردن منابع قربانی با روش‌های مختلف، مانند حملات سیل، حملات سیل مبتنی بر بازتاب، حملات سیلابی بهره برداری از پروتکل و حملات سیل مبتنی بر تقویت انجام می‌شود [۷]. حملات DDoS در سطح برنامه پیچیده‌تر از حملات لایه شبکه و ادراک در نظر گرفته می‌شوند و شناسایی آنها توسط فیلترها دشوارتر است. برنامه‌های کاربردی با پتانسیل حمله شامل DNS، پروتکل انتقال ابرمتن (HTTP)، پروتکل صدا از طریق اینترنت (VoIP) و غیره می باشند [۸].

برای شناسایی و کاهش حملات DDoS در اینترنت اشیا، راه حل های مختلفی پیشنهاد شده است. یکی از روشهای تشخیص حملات DDoS بکارگیری سیستم‌های تشخیص نفوذ[4] به شبکه است. سیستم‌های تشخیص نفوذ با تجزیه و تحلیل ترافیک شبکه ترافیک حمله را از ترافیک عادی طبقه‌بندی و تفکیک می‌کنند و هشدار لازم را برای دیوار آتش ارسال می‌کنند تا ترافیک شبکه کنترل کنند. سیستم‌های تشخیص نفوذ بر پایه یادگیری ماشین و یادگیری بر خلاف روشهای لیست سیاه و اکتشافی توانایی تشخیص حملات جدید را دارند و می‌توانند حملات روز صفر[5] با حملات جدید را تشخیص دهند [۹]. از جمله سیستم‌های تشخیص نفوذ بر پایه یادگیری ماشین و یادگیری عمیق می‌توان به روشهای مانند درخت تصمیم‌گیری [۱۰]، شبکه عصبی بازگشتی [۱۱]، ماشین بردار پشتیبان [۱۲] و شبکه عصبی کانولوشن [۱۳] اشاره نمود. سیستم تشخیص نفوذ برای اینترنت اشیاء باید توانایی تجزیه و تحلیل حجم زیادی از ترافیک شبکه را داشته باشد و از طرفی به صورت توزیع شده پیاده‌سازی می‌شود تا بتواند حجم بالایی از ترافیک شبکه را مورد تجزیه و تحلیل قرار دهد و در زمان واقعی حملات را تشخیص دهد. برای بهبود عملکرد سیستم‌های تشخیص نفوذ به شبکه از روشهای انتخاب ویژگی در کنار روشهای یادگیری ماشین استفاده می‌شود تا ویژگی‌های مهم برای یادگیری ماشین و تشخیص نفوذ کشف شود [۱۴].

مجموعه داده‌های مورد استفاده برای آموزش مدل‌های یادگیری ماشین می‌توانند دارای تعداد زیادی ویژگی باشند. اگرچه برخی از این ویژگی‌ها تأثیر زیادی بر نتیجه طبقه‌بندی دارند، برخی از ویژگی‌ها ممکن است تأثیر کمی یا بدون تأثیر بر نتیجه طبقه‌بندی داشته باشند. استفاده از ویژگی‌هایی که تاثیر کمی بر طبقه بندی دارند می‌تواند زمان و هزینه‌های فرآیند را افزایش دهد. هدف کاهش ویژگی‌هایی است که تأثیر کمی در طبقه بندی دارند و استفاده از ویژگی‌های بسیار مؤثر را فراهم می‌کند.

روش‌های فیلتر[6][۱۵]، تعبیه شده[7][۱۶] و بسته بندی[8][۱۷] به عنوان روش‌های انتخاب ویژگی استفاده شده است. روش فیلتر عمدتاً بر ویژگی‌های ذاتی ویژگی‌ها تمرکز دارد، در حالی که روش بسته‌بندی بر سودمندی ویژگی‌ها بر اساس عملکرد طبقه‌بندی کننده تمرکز دارد. روش تعبیه شده سعی می‌کند از ویژگی های هر دو روش فیلتر و پوشش برای بهینه سازی عملکرد یک الگوریتم یا مدل یادگیری استفاده کند [۱۸]. در بیشتر سیستم‌های تشخیص نفوذ از الگوریتم‌های انتخاب ویژگی بر پایه الگوریتم‌های فراابتکاری نظیر الگوریتم بهینه‌سازی وال [۱۹]، الگوریتم بهینه‌سازی گرگ خاکستری [۲۰] و الگوریتم بهینه‌سازی شاهین هریس [۲۱] استفاده می‌شود تا ترافیک شبکه دچار کاهش ابعاد شود و سیستم تشخیص نفوذ با سرعت و دقت بیشتری حملات را تشخیص دهد.

---

[1] Botnet
[2] Jamming
[3] De-synchronising attacks
[4] Intrusion detection systems
[5] Zero day attacks
[6] Filter mode
[7] Embedded method
[8] Wrapper method

در روش پیشنهادی برای تشخیص حملات به شبکه از یک سیستم تشخیص نفوذ توزیع شده در لایه مه اینترنت اشیاء استفاده می‌شود. در روش پیشنهادی از معماری توزیع شده گره‌های مه برای ارایه یک سیستم تشخیص نفوذ استفاده می‌شود. در روش پیشنهادی برای حل مشکل عدم تعادل در کلاس‌های اکثریت و اقلیت ترافیک و مجموعه داده شبکه از روش متعادل‌سازی شبکه عصبی متخاصم[1][۲۲] بر پایه تئوری بازی و یادگیری عمیق استفاده می‌شود. متعادل‌سازی مجموعه داده دقت مدل‌ها را برای تشخیص دقیق حملات افزایش می‌دهد. در مرحله دوم ترافیک شبکه در لایه مه با انتخاب ویژگی دچار کاهش ابعاد می‌شود. برای کاهش ابعاد ترافیک شبکه در لایه مه از الگوریتم بهینه‌سازی کوآتی[2] [۲۳] که سال ۲۰۲۳ ارایه شده است استفاده می‌شود. در مرحله دوم ویژگی‌های مهم و انتخاب شده به عنوان شبکه عصبی چند لایه انتخاب شده تا ترافیک شبکه به دسته عادی و حمله طبقه‌بندی شود. روش پیشنهادی هر گره مه یک لیست سیاه از آدرس گره‌های حمله کننده دارد و این لیست را با بلاک‌چین[3] [۲۴] با سایر گره‌های مه به اشتراک می‌گذارد. نقش بلاک چین، عدم دستکاری لیست‌های سیاه مبادله شده در لایه مه است تا امنیت تبادل پیام‌ها در لایه مه افزایش داده شود. هدف از روش پیشنهادی ارایه یک سیستم تشخیص نفوذ توزیع شده در لایه مه است که حجم زیاد ترافیک شبکه را با تقسیم کاری مورد تحلیل قرار داده و حملات DDoS را شناسایی نماید. هدف دیگر ارایه یک سیستم تشخیص نفوذ با تلفیق هوش گروهی و یادگیری ماشین است تا ترافیک شبکه را با دقت بیشتری تحلیل نماید. هدف دیگر روش پیشنهادی افزایش محرمانگی پیامهای مبادله شده بین سیستم‌های تشخیص نفوذ با بلاک چین است. سهم نویسندگان در این مقاله شامل موارد ذیل است:

- متعادلسازی ترافیک شبکه در لایه مه با تئوری بازی مبتنی بر شبکه GAN
- ارایه یک نسخه باینری از الگوریتم بهینه‌سازی کوآتی که در سال ۲۰۲۳ ارایه شده برای انتخاب ویژگی
- حفظ محرمانگی سیستم تشخیص نفوذ پیشنهادی با بلاک چین و مبادله لیست سیاه با بلاک چین بین گره‌های مه
- ارایه یک سیستم تشخیص نفوذ توزیع شده در لایه مه برای تشخیص حملات به IoT

مزیت روش پیشنهادی نسبت به سایر سیستم‌های تشخیص نفوذ آن است که در لایه مه پیاده‌سازی می‌شود و دارای یک معماری توزیع شده است. معماری توزیع شده بر خلاف معماری متمرکز باعث می‌شود تا به جای یک سیستم تشخیص نفوذ همزمان چند سیستم تشخیص نفوذ وجود داشته باشد و حجم بالایی از ترافیک شبکه مورد تحلیل قرار گرفته شود. یک مزیت دیگر روش پیشنهادی آن است به دلیل معماری غیرمتمرکز آن اگر یک سیستم تشخیص نفوذ در لایه مه مورد حمله DDoS قرار گرفته شود آنگاه سایر گره‌های مه یا سایر سیستم‌های تشخیص نفوذ می‌توانند حملات را تشخیص دهند. مزیت مهم دیگر سیستم تشخیص نفوذ پیشنهادی آن است ترافیک آموزشی را با روشهای جدید مانند تئوری بازی متعادل‌سازی می‌کند و این موضوع باعث افزایش دقت مدل پیشنهادی می‌شود. یک مزیت دیگر روش پیشنهادی آن است که ویژگی‌های مهم ترافیک شبکه را با هوش گروهی مبتنی بر رفتار کوآتی‌ها که در سال ۲۰۲۳ ارایه شده است، انتخاب نموده و ترافیک شبکه را بر اساس این ویژگی‌های مهم کاهش ابعاد می‌دهد. کاهش دادن ابعاد ترافیک در لایه مه باعث می‌شود تا سرعت یادگیری افزایش داده شود و سیستم تشخیص نفوذ با سرعت بیشتر حملات را تشخیص دهد. یک مزیت مهم روش پیشنهادی آن است که جلوی حملات در لایه مه گرفته می‌شود تا حملات به لایه ابر وارد نشوند. روش پیشنهادی دارای محدودیت‌هایی است از جمله آفلاین بودن ترافیک شبکه. یک چالش دیگر روشهای انتخاب ویژگی با هوش گروهی و الگوریتم‌های فراابتکاری، عدم قطعیت بالای آنها در یافتن جواب بهینه در هر آزمایش است. این مقاله در پنج بخش تهیه و تدوین شده است. در بخش دو، ادبیات موضوعی و کارهای مرتبط در زمینه تشخیص حملات به شبکه ارایه شده است. در بخش سه، سیستم تشخیص نفوذ پیشنهادی بر پایه تئوری بازی و شبکه عصبی GAN و الگوریتم بهینه‌سازی کوآتی و بلاک چین ارایه می‌شود. در بخش چهار، روش پیشنهادی پیاده‌سازی و تحلیل می‌شود و در ادامه در بخش ۵ نتایج تحقیق و یافته‌های تحقیق ارایه می‌گردد.

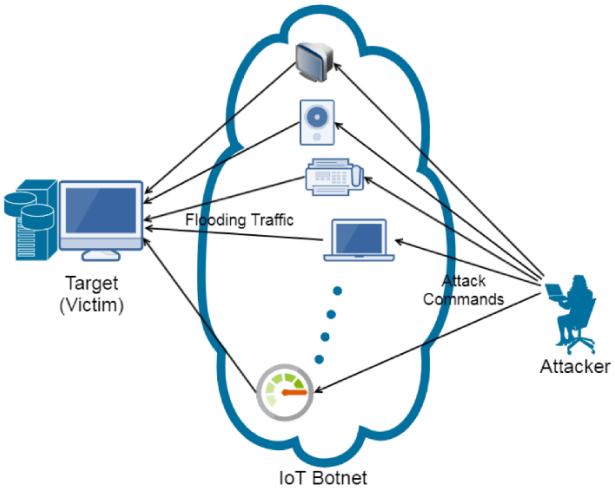
[1] Adversarial neural network
[2] Coati Optimization Algorithm (COA)
[3] Blockchain

۲-کارهای مرتبط

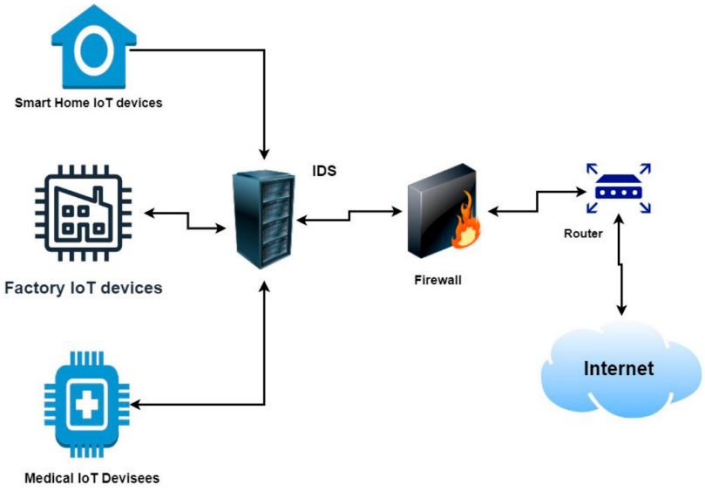
در دنیای پر سرعت امروز، که در آن تعداد دستگاه‌های متصل به اینترنت در حال افزایش است و برنامه‌های کاربردی آنلاین با سرعتی سریع در حال رشد هستند، امنیت اطلاعات در حال تبدیل شدن به یک ضرورت مطلق است. از زمان شروع شبکه جهانی وب، ۱.۲ میلیارد وب سایت توسعه یافته است و تعداد زیادی از برنامه های کاربردی آنلاین با خدمات وب مختلف مانند تجارت الکترونیک، بانکداری آنلاین، خرید آنلاین، آموزش آنلاین، مراقبت های بهداشتی الکترونیک و سیستم‌های کنترل صنعتی برای زیرساخت های حیاتی و غیره ادغام شده اند. امروزه مهاجمان سایبری برای انجام حملات موفقیت آمیز به کسب و کارها و دولت ها بسیار ماهر و مجهز هستند. جرایم سایبری امروزه تجارت بزرگی است و حجم اطلاعات دزدیده شده بسیار زیاد است. دسته های مختلفی از بدافزارها وجود دارد. این یک خطر بزرگ برای دولت ها، مشاغل و مصرف کنندگان در سراسر جهان است. لازم نیست برای یادآوری حمله گسترده به بانکی در بنگلادش که در آن ۸۱ میلیون دلار به سرقت رفت، به گذشته برگردیم. این یک یادآوری دائمی است از اینکه این حملات چقدر می‌توانند موثر باشند. از رایانه‌های خود بانک برای انتقال مبالغ هنگفتی استفاده می‌شد. آمارها نشان می‌دهد که ۲۰ درصد از کسب و کارهای آسیب دیده در دسته مشاغل کوچک، ۳۳ درصد در گروه متوسط و ۴۱ درصد در دسته مشاغل بزرگ قرار می‌گیرند. هر چه تهدید گسترده‌تر باشد، آگاهی از مسائل و حفاظت از اطلاعات مهم اهمیت بیشتری پیدا می کند. هشتاد و دو درصد از سازمان‌ها در معرض حداقل یک یا چند حمله قرار گرفته اند که در آن داده ها به سرقت رفته و برای فلج کردن خدمات قربانی استفاده می‌شود. سازمان‌هایی که تحت تأثیر حملات DDoS قرار گرفتند، کاهش ۲۶ درصدی در عملکرد سرویس‌های خود و ۴۱ درصد از قطع شدن سرویس‌های آسیب‌دیده را گزارش کردند [۲۵]. در یک حمله DDoS، دستگاه‌های متعددی به یک سرور یا شبکه حمله می‌کنند. هدف این حمله بارگذاری بیش از حد یک سرور یا شبکه هدفمند با درخواست های تقلبی متعدد است تا با ترافیک معمولی آن تداخل ایجاد کند. این امر منابع شبکه را تحت‌الشعاع قرار می دهد و در نتیجه ترافیک قانونی با اختلالات سرویس مواجه می‌شود. این حملات با شبکه‌های دستگاه‌های متصل به اینترنت از جمله رایانه‌های شخصی و سایر دستگاه‌ها که به نرم‌افزارهای مخرب آلوده شده‌اند که مستعد دستکاری از راه دور هستند، اجرا می‌شوند. این دستگاه‌ها به عنوان ربات شناخته می‌شوند. حملات DDoS به این دلیل مؤثر هستند که از بات‌نت‌ها یا گروه‌هایی از رایانه‌های در معرض خطر به‌عنوان منبع اصلی حمله خود استفاده می‌کنند. هنگامی که یک بات نت ایجاد شد، مهاجم می تواند با ارسال دستورات از راه دور به هر ربات، حمله را هدایت کند. هر یک از ربات‌های بات‌نت در حالی که توسط بات‌نت مورد هدف قرار می‌گیرد، درخواست‌هایی را به IP سرور قربانی ارسال می‌کند، که ممکن است شبکه را تحت تأثیر قرار دهد و ترافیک قانونی را مختل کند. هر ربات یک دستگاه اینترنتی واقعی است که تمایز بین حملات و ترافیک قانونی را به چالش می‌کشد. همان‌طور که قبلا مشخص شد، مهاجمان DDoS حملات خود را از طریق یک بات نت آغاز می کنند. بنابراین، معماری یک حمله DDoS شامل یک مهاجم، یک بات نت و شبکه یا سرور هدف خواهد بود. در شکل ۱، مکانیزم حملات DDoS به شبکه نمایش داده شده است[۲۶].

در این شکل مشاهده می‌شود اشیاء هوشمند مانند دوربین هوشمند به بدافزار آلوده شده و نقش حمله کننده به شبکه را برعهده دارد. برای تشخیص حملات به شبکه و شناسایی حملات در سرویس خدمات، سیستم تشخیص نفوذ و دیوار آتش نقش حیاتی دارند. مطابق شکل۲، یک سیستم تشخیص نفوذ ترافیک شبکه را تحلیل نموده و حملات را برای دیوار آتش ارسال نموده تا آنها را مسدود نماید[۲۷].

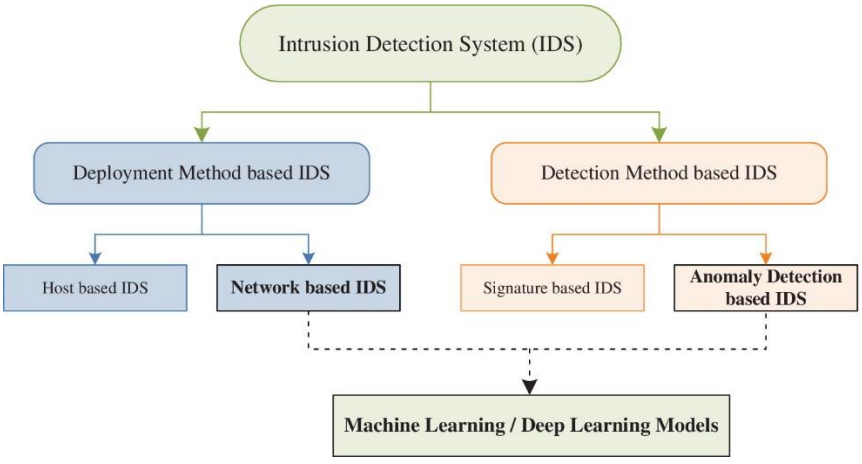
سیستم‌های تشخیص نفوذ به شبکه بر اساس عملکردی که دارند به چند گروه مطابق شکل ۳، طبقه‌بندی می‌شوند [۲۸].



شکل ۱: مکانیزم حملات DDoS در اینترنت اشیاء[۲۶]
Figure 1. Mechanism of DDoS attacks in Internet of Things [26]



شکل ۲: عملکرد سیستم تشخیص نفوذ و دیوار آتش[۲۷]
Figure 2. Performance of intrusion detection system and firewall [27]



شکل۳ : دسته بندی سیستم های تشخیص نفوذ[۲۸]
Figure 3. Classification of intrusion detection systems [28]

سیستم تشخیص نفوذ به چند رویکرد طبقه بندی می‌شود. روش اول یک رویکرد مبتنی بر امضا[1] است که داده‌های سیستم فعلی را با امضای مستند حمله نفوذی که در پایگاه داده سیستم تشخیص نفوذ ذخیره شده است مقایسه می‌کند. وقتی سیستم تشخیص نفوذ یک تطابق را تشخیص می‌دهد، آن را به عنوان نفوذ طبقه بندی می‌کند. این روش امکان تشخیص سریع و دقیق را فراهم می‌کند. پایگاه داده امضا باید به طور منظم نگهداری شود که این یک اشکال است. همچنین، دستگاه ممکن است قبل از وصله حمله نفوذ بعدی هک شود. علاوه بر این، دارای معایب دیگری مانند بارگذاری بیش از حد شبکه، قیمت تطبیق امضای بالا و تعداد بالای هشدارهای اشتباه است. سیستم تشخیص نفوذ بر پایه امضاء، که حملاتی را که چندین بسته را در بر می‌گیرند، تجزیه و تحلیل می‌کند، با استفاده از بسته های شبکه و امضاهای تطبیق در مقابل یک پایگاه داده امضا، شناسایی دشوار است. با پیچیدگی بدافزارهای مدرن، استخراج امضا مورد نیاز خواهد بود. روش دوم مبتنی بر ناهنجاری یا مبتنی بر رفتار[2] است که در آن سیستم تشخیص نفوذ هنگامی که دستگاه رفتار غیرعادی نشان می‌دهد، نفوذ را تشخیص می‌دهد. با استفاده از این ابزار می توان تهدیدات شناخته شده و ناشناخته را شناسایی کرد. با این حال، این تکنیک دارای دقت ضعیف و نرخ بالای هشدارهای کاذب به عنوان معایب است [۲۹]. از سوی دیگر، یک رویکرد ترکیبی، رویکردهای مبتنی بر امضا و ناهنجاری را با هم ترکیب می‌کند. این سیستم حملات شناسایی شده را با استفاده از رویکرد مبتنی بر امضا و حملات ناشناخته را با استفاده از رویکرد مبتنی بر ناهنجاری شناسایی می کند. کنار هم قرار دادن این دو روش می‌تواند منجر به تشخیص دقیق تر شود، اما آنها پتانسیل ناکارآمدی و افزایش هزینه های محاسباتی را دارند. این رویکرد به رفع محدودیت‌های یک فرآیند واحد کمک می‌کند، بنابراین قابلیت اطمینان کلی سیستم اینترنت اشیاء را بهبود می‌بخشد. عیب آشکار این است که کل سیستم تشخیص نفوذ می‌تواند از نظر اندازه و پیچیدگی رشد کند. این امر عملکرد سیستم را پیچیده‌تر می‌کند و به منابع بیشتری نیاز دارد. روش تشخیص نفوذ می‌تواند منابع و زمان زیادی را مصرف کند، به خصوص اگر پروتکل های زیادی در چارچوب اینترنت اشیا وجود داشته باشد[۳۰و۲۹].

در ادامه تعدادی از کارهای مرتبط در تشخیص حملات و بخصوص حملات DDoS مرور و بررسی می‌شود و از طرفی سیستم‌های تشخیص نفوذ در این حوزه با روش‌های یادگیری ماشین مرور می‌شود.

در [۳۱]، سال ۲۰۲۳، یک سیستم تشخیص نفوذ شبکه برای حملات DDoS با استفاده از رمزگذارهای خودکار عمیق ارایه دادند. در این مقاله، ما یک معماری سیستم تشخیص نفوذ شبکه بر اساس یک رمزگذار خودکار عمیق آموزش‌دیده بر روی داده‌های جریان شبکه پیشنهاد شده است، که این مزیت را دارد که نیازی به دانش قبلی از توپولوژی شبکه یا معماری زیربنایی آن نیست. نتایج تجربی نشان می‌دهد که مدل پیشنهادی می‌تواند ناهنجاری‌های ناشی از حملات انکار سرویس توزیع‌شده، ارائه نرخ تشخیص بالا و آلارم‌های کاذب کم شناسایی کند.

در [۳۲]، سال ۲۰۲۳، پیاده‌سازی مدل تشخیص نفوذ برای حملات DDoS در شبکه‌های اینترنت اشیاء را ارایه دادند. این مقاله انواع مختلفی از طبقه‌بندی‌کننده‌ها را معرفی می‌کند که برای تشکیل سیستم‌های تشخیص نفوذ سبک وزن مناسب برای محافظت در برابر حملات انکار خدمات توزیع شده در شبکه‌های IoT استفاده می‌شوند. مجموعه داده های مورد استفاده برای آزمایش ها و تحقیقات BOT-IoT و مجموعه داده شبکه TON-IoT توسط دانشگاه New South Wales سیدنی استرالیا است.

در [۳۳]، سال ۲۰۲۳، یک سیستم تشخیص نفوذ DDoS بر اساس روش ترکیبی CNN و LSTM ارایه دادند. در این مطالعه، یک روش طبقه‌بندی یادگیری عمیق جدید با ترکیب دو الگوریتم یادگیری عمیق رایج، شبکه‌های عصبی کانولوشنو حافظه کوتاه‌مدت بلند مدت پیشنهاد شده است. برای آزمایش مدل از مجموعه داده NSL-KDD استفاده شده است. این معماری متشکل از هفت لایه برای دستیابی به عملکرد بالاتر در مقایسه با CNN و LSTM سنتی است. مدل پیشنهادی بالاترین دقت ۹۹/۲۰ درصد را در مقایسه با کار قبلی به دست آورد.

در [۳۴]، سال ۲۰۲۳، یک سیستم تشخیص نفوذ شبکه کارآمد برای شبکه های توزیع شده با استفاده از تکنیک یادگیری ماشین ارایه دادند. در این مطالعه، تکنیک طبقه‌بندی مبتنی بر الگوریتم جنگل تصادفی برای انتخاب ویژگی استفاده شده است. برای ذخیره تعداد زیادی از حملات محتاطانه، از سیستم فایل Hadoop و معماری Apache Spark برای افزایش سرعت پردازش

[1] Signature base
[2] Anomaly based or behavior based

داده‌ها، به عنوان راه حل پیشنهادی استفاده می‌شود. این روش با استفاده از مجموعه داده معیار NSL-KDD برای یافتن دقت و بسیاری از پارامترهای دیگر ارزیابی شده است. نتایج تجربی نشان داد روش آنها از تکنیک‌های یادگیری ماشین، درخت تصمیم، جنگل تصادفی و تحلیل مؤلفه اصلی، شبکه بیزین[1]، ماشین بردار پشتیبان و رگرسیون لجستیک[2] دقت بیشتری در تشخیص حملات دارد.

در [۳۵]، سال ۲۰۲۳، یک مدل مبتنی بر هسته RBF-SVM[3] برای تشخیص حملات DDoS ارایه دادند. راه‌حل پیشنهادی از تکنیک جستجوی پارامتر جامع اعتبارسنجی متقابل جستجوی شبکه و هسته تابع پایه شعاعی از الگوریتم ماشین بردار پشتیبان استفاده می‌کند. طرح پیشنهادی آنها در شبکه دارای میانگین خطای مطلق ۰/۰۰۶ است و نسبت به نسخه استاندارد ماشین بردار پشتیبان دقت بیشتری دارد.

در [۳۶]، سال ۲۰۲۳، یک سیستم تشخیص نفوذ شبکه تطبیقی جدید برای اینترنت اشیاء ارایه دادند. روش آنها ترکیبی از روشهای Fast R-CNN وگرادیان برای تشخیص حملات است. مدل پیشنهادی آنها در تشخیص "حملات سایبری" به دقت بالای دارد و از شبکه عصبی کانولوشن دقت بیشتری ارایه می‌دهد.

در [۳۷]، سال ۲۰۲۳، تشخیص حملات به شبکه با استفاده از سیستم تشخیص نفوذ بهبودیافته با هوش گروهی را ارایه دادند. این مطالعه یک سیستم تشخیص نفوذ موثر با بهینه‌ساز گرگ خاکستری و ماشین تقویت گرادیان LightGBM را پیشنهاد دادند. مجموعه داده InSDN برای آموزش و آزمایش سیستم پیشنهادی، که به عنوان یک مجموعه داده معیار جدید در نظر گرفته می‌شود، استفاده شده است. ارزیابی سیستم پیشنهادی نشان داد که روش پیشنهادی به دقتی بیش از ۹۸٪ دست یافته است.

در [۳۸]، سال ۲۰۲۳، یک روش بهینه‌سازی پارامترهای شبکه BPN با استفاده از الگوریتم بهینه‌سازی ذرات برای تشخیص نفوذ در محیط ابری را ارایه دادند. آنها مجموعه داده KDD cup 99 را برای تشخیص حملات مورد استفاده قرار دادند. برای افزایش بهینه‌سازی شبکه عصبی، از بهینه‌سازی ازدحام ذرات استفاده کردند و در نتیجه تشخیص دقیق را افزایش دادند و دقت روش آنها به حدود ۹۶/۵٪ رسیده است.

در [۳۹]، سال ۲۰۲۳، چارچوبی جدید برای تشخیص حملات DDoS با استفاده از تکنیک‌های ترکیبی و مبتنی بر شبکه عصبی LSTM ارایه دادند. در این کار تحقیقاتی، روش‌های تشخیص حمله DDoS مبتنی بر استخراج ویژگی‌های شبکه باور عمیق و مدل حافظه کوتاه‌مدت ترکیبی بر پایه LSTM در مجموعه داده NSL-KDD پیشنهاد دادند. در روش هیبریدی LSTM، تکنیک بهینه سازی ازدحام ذرات که برای بهینه سازی وزن شبکه عصبی LSTM ترکیب شده است، خطای پیش بینی را کاهش می‌دهد. این روش شبکه باور عمیق برای استخراج ویژگی های بسته های IP استفاده می‌شود و حملات DDoS را بر اساس مدل PSO-LSTM شناسایی می‌کند. علاوه بر این، ترافیک عادی شبکه را به دقت پیش‌بینی می‌کند و ناهنجاری‌های ناشی از حملات DDoS را تشخیص می‌دهد. معماری PSO-LSTM پیشنهادی از تکنیک‌های طبقه‌بندی شامل ماشین بردار پشتیبانی استاندارد و LSTM از نظر عملکرد تشخیص حمله دقت بیشتری دارد.

در [۴۰]، سال ۲۰۲۳، یک روش تشخیص نفوذ برای شناسایی حملات انکار سرویس با استفاده از کدهای خروجی تصحیح خطا و استنتاج عصبی فازی تطبیقی ارایه دادند. روش پیشنهادی فرآیند تشخیص نفوذ را در سه مرحله به نام‌های پیش پردازش، استخراج ویژگی و طبقه‌بندی انجام می‌دهد. در ابتدا تجزیه و تحلیل اجزای اصلی برای استخراج ویژگی ها استفاده می‌شود، در ادامه سیستم استنتاج عصبی فازی تطبیقی برای طبقه بندی استفاده می‌شود. در این مدل طبقه بندی، از الگوریتم بهینه سازی ازدحام ذرات برای بهینه سازی ساختار شبکه عصبی فازی استفاده شده است. عملکرد روش پیشنهادی با استفاده از پایگاه داده NSLKDD ارزیابی شده است. نتایج نشان می‌دهد که روش پیشنهادی می‌تواند انواع حملات DoS را با دقت بالا تشخیص دهد و عملکرد بهتری از شبکه‌های عصبی مشابه دارد.

در [۴۸]، سال ۲۰۲۳، یک روش انتخاب ویژگی ترکیبی برای تشخیص نفوذ شبکه مبتنی بر شبکه عصبی مصنوعی چند لایه در مجموعه داده UNSW-NB15 ارایه دادند. آنها از ترکیبی از دو روش فیلتر، به ترتیب به دست آوردن اطلاعات (IG) و جنگل

---

[1] Bayesian network

[2] Logistic regression

[3] Radial Basis Function-Support Vector Machine

تصادفی (RF) برای کاهش فضای جستجوی زیرمجموعه ویژگی‌ها استفاده کردند. در مرحله دوم رویکرد آنها، از یک روش پوشش مبتنی بر یادگیری ماشین استفاده کردند که حذف ویژگی بازگشتی (RFE) را برای کاهش بیشتر ابعاد ویژگی و در عین حال در نظر گرفتن ارتباط ویژگی‌های مشابه فراهم می‌کند. نتایج نشان می‌دهد که روش آنها فضای ویژگی را از ۴۲ به ۲۳ کاهش می‌دهد و دقت شبکه عصبی با انتخاب ویژگی از ۸۲/۲۵٪ به ۸۴/۲۴٪ بهبود یافته است.

در [۴۹]، سال ۲۰۲۳، یک مدل کارآمد تشخیص نفوذ شبکه برای امنیت اینترنت اشیاء با استفاده از طبقه‌بندی کننده K-NN ارایه دادند. در این پژوهش از تجزیه و تحلیل مؤلفه اصلی، آزمون آماری تک متغیره، و الگوریتم ژنتیک برای انتخاب ویژگی به طور جداگانه برای بهبود کیفیت داده‌ها و انتخاب ویژگی استفاده می‌شود. ارزیابی روش آنها بر روی مجموعه داده Bot-IoT انجام می‌شود. آزمایشات نشان داد با اعمال انتخاب ویژگی، زمان آموزش از ۵۱۱۸۲/۲۲ ثانیه به زیر یک دقیقه کاهش داده می‌شود.

در [۵۰]، سال ۲۰۲۳، یک سیستم تشخیص نفوذ برای شناسایی حملات وب بر اساس مجموعه‌ای از تکنیک‌های انتخاب ویژگی فیلتر ارایه دادند. پژوهش آنها مجموعه‌ای از تکنیک‌های انتخاب ویژگی فیلتر را پیشنهاد می‌کند تا با انتخاب یک چهارم از ویژگی‌های رتبه‌بندی‌شده، یک زیرمجموعه ویژگی قابل‌توجه برای تشخیص حمله به دست آید. آزمایشات نشان داد روش آنها با ۲۴ ویژگی انتخاب شده و درخت تصمیم‌گیری دارای بهترین نتایج برای تشخیص نفوذ است.

در [۵۱]، سال ۲۰۲۳، یک روش انتخاب ویژگی جدید مبتنی بر بهبود الگوریتم بهینه‌سازی کرکس آفریقایی برای تشخیص حمله DDoS ارایه شده است. در این مطالعه، یک الگوریتم بهینه‌سازی کرکس آفریقایی بهبود یافته بر اساس معادلات سینوس و کسینوس برای انتخاب ویژگی‌های مؤثر حملات DDoS پیشنهاد شده‌است. برای انتخاب زیرمجموعه بهینه ویژگی‌ها، نزدیکترین همسایه به عنوان طبقه بندی کننده در روش استفاده می‌شود. عملکرد روش پیشنهادی در دو مجموعه داده CIC-DDOS2019 و NSL-KDD برای تشخیص حمله DDoS با برخی از پیشرفته‌ترین فناوری‌های اخیر مقایسه می‌شود. نتایج آزمایش نشان می‌دهد که روش پیشنهادی آنها نسبت به الگوریتم‌های فراابتکاری رایج در تشخیص و انتخاب ویژگی برای شناسایی حملات دقیق‌تر است.

در [۵۲]، سال ۲۰۲۳، یک تکنیک انتخاب ویژگی پویا برای تشخیص حمله DDoS ارایه شده است. در این پژوهش، به منظور انتخاب ویژگی‌های مؤثر، یک تکنیک انتخاب ویژگی ترکیبی مبتنی بر رأی‌گیری پیشنهاد شده است. روش ترکیبی نه تنها ابعاد ویژگی ها را کاهش می‌دهد و افزونگی را از بین آنها حذف می‌کند، بلکه بهترین ویژگی‌های مرتبط را برای طبقه‌بندی ارائه می‌دهد. آزمایشات نشان داد پرسپترون[1] چند لایه با الگوریتم ژنتیک (MLP-GA) به عنوان یک طبقه‌بندی کننده، با ارائه دقت ۹۸٪/۸، نرخ مثبت کاذب ۰/۶٪ و قابلیت تشخیص زودهنگام، از طبقه‌بندی‌کننده‌های معمولی بهتر عمل می‌کند.

در [۵۳]، سال ۲۰۲۲، یک روش تشخیص حمله DDoS در رایانش ابری بر اساس انتخاب ویژگی گروه و یادگیری عمیق را ارایه دادند. در این پژوهش، یک حالت یادگیری عمیق ترکیبی مبتنی بر ترکیب شبکه عصبی کانولوشن با حافظه بلند مدت به دلیل استحکام و کارایی آن در تشخیص ترافیک عادی و حمله استفاده شده است. آنها برای تشخیص حملات از مجموعه داده CICIDS 2017 استفاده نمودند. نتایج نشان داد روش آنها از شبکه عصبی CNN و LSTM دقت بیشتری در تشخیص حملات دارند.

در [۵۴]، سال ۲۰۲۲، یک روش جدید برای تشخیص نفوذ با شناسایی نقاط پرت چند متغیره و انتخاب ویژگی ReliefF ارایه دادند. در روش آنها ابتدا، رویکرد انتخاب ویژگی ReliefF برای شناسایی بهترین ویژگی‌هایی که عملکرد طبقه‌بندی را در سطح بالایی حفظ می‌کنند، به کار گرفته شده است و ۲۰ ویژگی تعیین شده است. سپس، برای یافتن نقاط پرت در مجموعه داده، از رویکردهای فاصله و کای اسکوئر Mahalanobis استفاده شده است. پس از آن، روش‌های مختلف یادگیری ماشین برای مجموعه داده اعمال شده و نتایج با هم مقایسه شده‌اند. دقت بالای این روش در مجموعه داده NSL-KDD مزیت آن است اما ایراد آن عدم معماری توزیع شده برای تشخیص حملات است که سیستم تشخیص نفوذ آنها را در مواجه با حجم زیادی از ترافیک کند خواهد کرد.

[1] perceptron

در [۵۵]، سال ۲۰۲۱، ترکیب انتخاب ویژگی مبتنی بر PCA با طبقه‌بندی درخت تصادفی برای تشخیص نفوذ در شبکه اینترنت اشیاء را ارایه دادند. نتایج تجربی روی مجموعه داده‌های ترافیک شبکه‌های IoT نشان می‌دهد که سیستم تشخیص نفوذ پیشنهادی با استفاده از طبقه‌بندی درخت تصادفی بهترین عملکرد را از نظر دقت و مصرف انرژی به دست می‌آورد. در جدول۱، روش، مزایا و معایب هر یک از سیستمهای تشخیص نفوذ با هم مقایسه شده است.

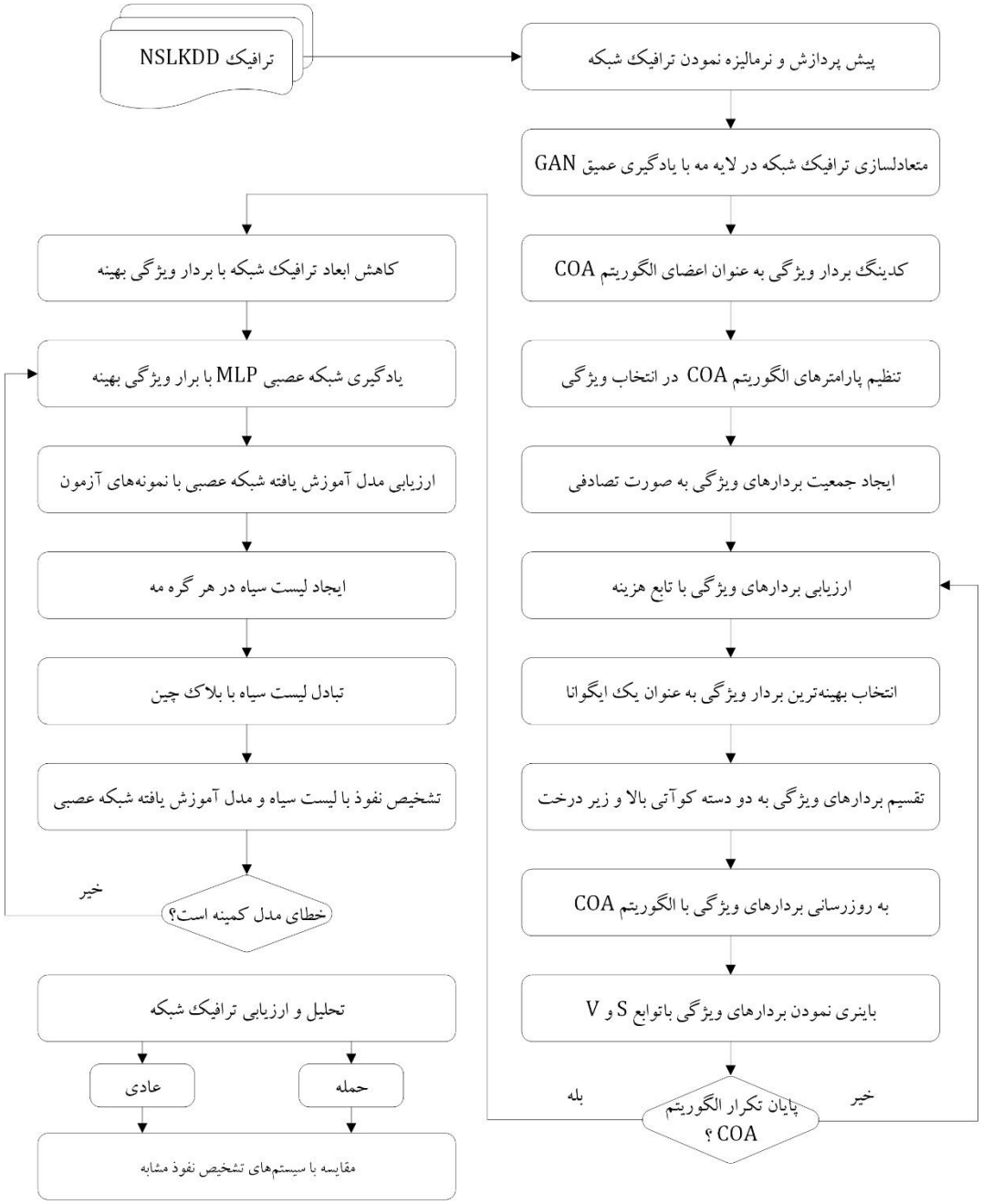
جدول ۱: خلاصه مطالعات مرور شده در زمینه تشخیص حملات به شبکه

Table 1: Summary of reviewed studies in the field of network attack detection

پژوهش	روش	مزیت	عیب
در [۳۱]، سال ۲۰۲۳	تشخیص نفوذ شبکه برای حملات DDoS با استفاده از رمزگذارهای خودکار عمیق	نرخ تشخیص بالا و آلارم‌های کاذب کم	عدم بکارگیری انتخاب ویژگی و عدم متعادلسازی مجموعه داده
در [۳۲]، سال ۲۰۲۳	انواع مختلفی از طبقه‌بندی‌کننده‌ها برای تشخیص حملات	بکارگیری دو مجموعه داده	عدم معماری توزیع شده برای تشخیص حملات در زمان واقعی
در [۳۴]، سال ۲۰۲۳	الگوریتم جنگل تصادفی برای انتخاب ویژگی	دقت بیشتر از شبکه بیزین، ماشین بردار پشتیبان و رگرسیون لجستیک	عدم متعادلسازی مجموعه داده و معماری متمرکز سیستم تشخیص نفوذ
در [۳۵]، سال ۲۰۲۳	مدل مبتنی بر هسته RBF-SVM برای تشخیص حملات	دقت بیشتر از الگوریتم ماشین بردار	نیاز به داده‌های آموزشی زیادی دارد.
در [۳۶]، سال ۲۰۲۳	روشهای Fast R-CNN وگرادیان برای تشخیص حملات	دقت بیشتر از شبکه عصبی کانولوشن	پیچیدگی بالا
در [۳۷]، سال ۲۰۲۳	بهینه‌ساز گرگ خاکستری و ماشین تقویت گرادیانLightGBM	دقتی بیش از ۹۸٪	مقایسه‌های ضعیف و عدم متعادلسازی مجموعه داده
در [۳۸]، سال ۲۰۲۳	شبکه عصبی BPN با استفاده از الگوریتم بهینه‌سازی ذرات	دقت روش آنها ۹۶/۵٪ است.	بکارگیری مجموعه داده قدیمی
در [۳۹]، سال ۲۰۲۳	برای بهینه سازی وزن شبکه عصبی LSTM با الگوریتم PSO	دقت بیشتر از LSTM	فقط ویژگی‌های مرتبط با IP بررسی شده است.
در [۴۰]، سال ۲۰۲۳	استنتاج عصبی فازی تطبیقی در تشخیص حملات	عملکرد بهتری از شبکه‌های عصبی مشابه دارد.	قطعیت آنها بالا نیست.
در [۴۸]، سال ۲۰۲۳	تشخیص نفوذ شبکه مبتنی بر شبکه عصبی مصنوعی چند لایه و انتخاب ویژگی با جنگل تصادفی و روش IG	کاهش ابعادترافیک شبکه از۴۱ویژگی به۲۳ ویژگی	دقت متوسط
در [۴۹]، سال ۲۰۲۳	طبقه‌بندی کننده K-NN	کاهش زمان آموزش	روش نزدیکترین همسایه هوشمندی بالایی ندارد.
در [۵۰]، سال ۲۰۲۳	تکنیک‌های انتخاب ویژگی فیلتر	توانایی تشخیص حملات وب در شبکه	دقت متوسط و عدم متعادلسازی مجموعه داده
در [۵۱]، سال ۲۰۲۳	الگوریتم بهینه‌سازی کرکس آفریقایی بهبود یافته در تشخیص حملات	تحلیل روی دو مجموعه داده	پیچیدگی زیاد الگوریتم کرکس و عدم متعادلسازی مجموعه داده
در [۵۲]، سال ۲۰۲۳	تکنیک انتخاب ویژگی پویا برای تشخیص حمله	دقت ۹۸/۸٪	ترکیب الگوریتم ژنتیک و شبکه عصبی زمان آموزش را افزایش می‌دهد.
در [۵۳]، سال ۲۰۲۲	ترکیب شبکه عصبی CNN و LSTM در تشخیص حملات در لایه ابر	دقت بیشتر از شبکه عصبی CNN و LSTM	پیچیدگی محاسباتی زیاد
در [۵۴]، سال ۲۰۲۲	شناسایی نقاط پرت چند متغیره و انتخاب ویژگی ReliefF در تشخیص حملات	شناسایی حملات پیچیده	عدم معماری توزیع شده و عدم متعادلسازی مجموعه داده
در [۵۵]، سال ۲۰۲۱	انتخاب ویژگی مبتنی بر PCA و درخت تصادفی	دقت بیشتر از درخت تصادفی	عدم تشخیص ویژگی‌های موثر در حملات

۳-روش پیشنهادی

در روش پیشنهادی یک سیستم تشخیص نفوذ در لایه مه ارایه می‌شود که چارچوب آن در شکل ۴، نمایش داده شده است. با توجه به چارچوب ارایه شده، در ابتدا ترافیک شبکه به عنوان ورودی لایه مه در نظر گرفته می‌شود و سپس در ادامه ترافیک شبکه با روش یادگیری عمیق GAN متعادلسازی می‌شود. در مرحله بعدی از نسخه باینری الگوریتم کوآتی برای انتخاب ویژگی در لایه مه استفاده می‌شود و ویژگی‌های مهم به عنوان ورودی شبکه عصبی چند لایه در نظر گرفته می‌شود. شبکه عصبی مصنوعی نقش طبقه‌بندی ترافیک شبکه به دو دسته حمله و عادی را بر عهده دارد و سپس هر گره مه لیست سیاه خود را به روزرسانی می‌کند. در ادامه لیست سیاه بین گره‌های مه با بلاک چین مبادله می‌شود تا هکر نتواند لیستهای سیاه را دستکاری نماید. در نهایت مئل آموزش یافته با استفاده از داده‌های آزمون مورد ارزیابی قرار گرفته می‌شود و از نظر شاخص دقت و حساسیت با روشهای مشابه مورد مقایسه قرار گرفته می‌شود.



شکل۴: چارچوب سیستم تشخیص نفوذ پیشنهادی

Figure 4. The framework of the proposed intrusion detection system

۳-۱-پیش پردازش ترافیک

ترافیک شبکه دارای مجموعه‌ای از ویژگی‌ها است که مقدار آن‌ها می‌تواند دارای دامنه متفاوتی باشد. برای آنکه دقت مدلهای یادگیری ماشین افزایش داده شود بهتر است که دامنه و کران پایین و بالای همه ویژگی‌های مجمعه داده در بازه [a,b] نرمال شود و برای این منظور از رابطه ۱، استفاده می‌شود و اگر بازه نرمالسازی بین صفر و یک باشد از رابطه۲، استفاده می‌شود:

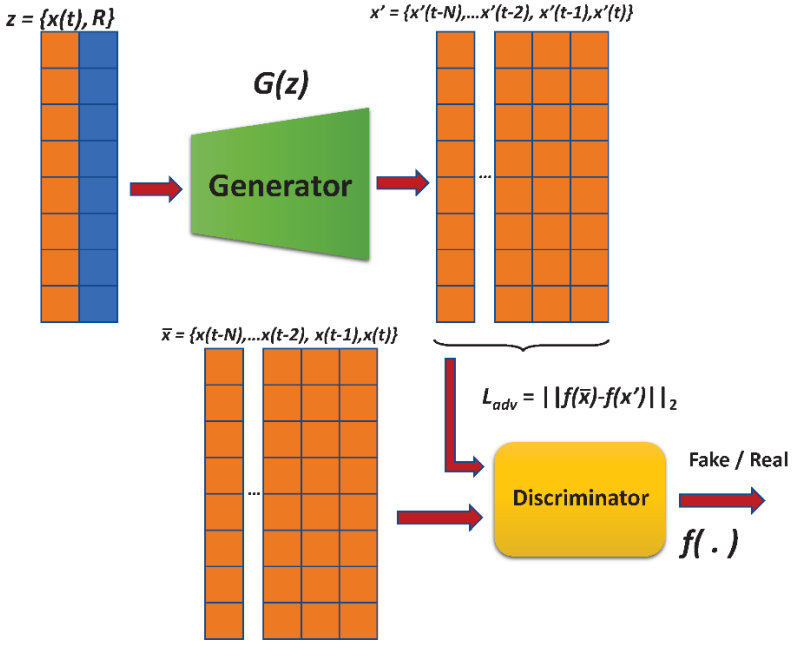
$$X_n = a + \frac{(Max(X) - X)(b-a)}{Max(X) - Min(X)} \quad (۱)$$

$$X_n = \frac{(Max(X) - X)}{Max(X) - Min(X)} \quad (۲)$$

در این رابطه‌ها، Max و Min به ترتیب بیشترین و کمترین مقدار ویژگی X است و X_n مقدار نرمال شده ویژگی X است.

۳-۲-متعادلسازی ترافیک با شبکه GAN

شبکه‌های متخاصم مولد (GAN) نشان‌دهنده یک پیشرفت اخیر در یادگیری ماشین هستند و یک کلاس قدرتمند از شبکه‌های عصبی هستند که در یادگیری بدون نظارت مورد استفاده قرار می‌گیرند. آنها مدل‌های مولد هستند به این معنا که نمونه‌های داده جدیدی ایجاد می‌کنند که شبیه داده‌های آموزشی اصلی است. داده‌های جدید بر اساس یادگیری الگوهای موجود در داده‌های اصلی ایجاد می‌شوند. کاربردهای متعددی از GAN ها در امنیت شبکه وجود دارد. شبکه GAN یک شبکه عصبی بر اساس تئوری بازی است که مانند شکل۵، دارای دو بخش مولد و متمایزگر است. بخش مولد بر اساس اطلاعات و داده‌های نویز و تصادفی و تاثیر آنها روی داده‌های واقعی تلاش می‌کند تا داده‌های مصنوعی و جعلی را ایجاد کند و اگر متمایزگر فریب بخورد و داده‌های جعلی را به عنوان داده واقعی در نظر بگیرد آنگاه مولد برنده می‌شود. اگر متمایز فریب نخورد و داده مصنوعی و جعلی را تشخیص دهد آنگاه متمایزگر برنده شده است. به عبارتی بین متمایزگر و مولد یک بازی Min-Max برقرار است.



شکل ۵: ساختار شبکه عصبی GAN در تولید نمونه های مصنوعی و جعلی[۴۱]

Figure 5. The structure of GAN neural network in generating artificial and fake samples [41]

در این شکل، نمونه‌های واقعی با x و نمونه‌های جعلی با x' نمایش داده می‌شود و بردار نویز نیز با z در نظر گرفته می‌شود. تابع هدف در شبکه عصبی GAN به صورت معادله ۳، تعریف می‌شود[۴۲]،

$$\min_G \max_D V(G,D) = \mathbb{E}_{s\sim p(s)}[\log D(s)] + \mathbb{E}_{z\sim p(z)}[\log(1-D(G(z)))] \quad (۳)$$

p(s) پراکندگی داده‌های واقعی است و g(z) تولید نمونه‌های نویز را بر عهده دارد و z مقادیر تصادفی برای ایجاد نمونه‌های جعلی است. در این معادله، D(s) احتمال یک نمونه برای قرار گیری در کلاس نمونه‌های واقعی است.

۳-۳- انتخاب ویژگی با الگوریتم بهینه سازی کوآتی

مسئله انتخاب ویژگی یک مسئله باینری و گسسته است زیرا بردارهای ویژگی دارای مقادیر ۰ یا ۱ می‌باشند که به ترتیب عدم انتخاب ویژگی و انتخاب ویژگی را نشان می‌دهد. چون مجموعه داده بکار رفته NSL-KDD است و این مجموعه داده دارای ۴۱ ویژگی است لذا هر بردار ویژگی دارای ۴۱ عنصر است که مقادیر آنها باینری و گسسته است از این نظر باید برای انتخاب ویژگی یک الگوریتم بهینه‌سازی گسسته و باینری را استفاده نمود. در روش پیشنهادی برای باینری نمودن راه‌حلها یا بردارهای ویژگی در الگوریتم بهینه‌سازی کوآتی از توابع تبدیل نظیر S و V استفاده می‌شود. نقش توابع تبدیل، تبدیل فضای پیوسته به گسسته و باینری است.

الگوریتم بهینه‌سازی کوآتی بر اساس رفتار نوعی راکون به نام کوآتی الگوبرداری شده است. در این الگوریتم رفتار شکار کردن ایگوانا توسط کوآتی و فرار از چنگال پلنگ برای مدل‌سازی آنها در نظر گرفته می‌شود. در این الگوریتم کوآتی‌ها به دو دسته تقسیم می‌شوند و دسته اول بالای درخت رفته و ایگوانا را می‌ترسانند و ایگوانا به زمین می‌افند و دسته دوم از فرصت استفاده می‌کند و تلاش می‌کنند تا ایگوانا را شکار کنند. در ادامه کوآتی‌ها می‌توانند از موقعیت خطرناک که می‌تواند آنها را به عنوان طعمه یک پلنگ قرار دهد نیز فرار کنند. در این الگوریتم هر راه‌حل مسئله یک کوآتی است و بهینه‌ترین راه‌حلی که پیدا شده است نیز یک ایگوانا است. در ابتدا راه‌حلهای تصادفی و جمعیت اولیه بردارهای ویژگی یا کوآتی‌ها در ماتریس X قرار داده می‌شود و X_i یک راه‌حل نظیر راه‌حل i ام است. در رابطه۴، جمعیت اولیه بردارهای ویژگی در ماتریس X قرار داده شده است و در اینجا N راه‌حل وجود دارد و هر بردار ویژگی m مولفه دارد[۲۳]،

$$X=\begin{bmatrix} X_1 \\ \vdots \\ X_i \\ \vdots \\ X_N \end{bmatrix}_{N\times m}=\begin{bmatrix} x_{1,1} & \cdots & x_{1,j} & \cdots & x_{1,m} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ x_{i,1} & \cdots & x_{i,j} & \cdots & x_{i,m} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ x_{N,1} & \cdots & x_{N,j} & \cdots & x_{N,m} \end{bmatrix}_{N\times m} \quad (۴)$$

هر بردار ویژگی یا یک کوآتی نیاز به ارزیابی دارد و برای ارزیابی از تابع هدف انتخاب ویژگی در رابطه۵، استفاده می‌شود،

$$F\left(X_i\right)=\alpha.E+\beta\frac{\|X_i\|}{m} \quad (۵)$$

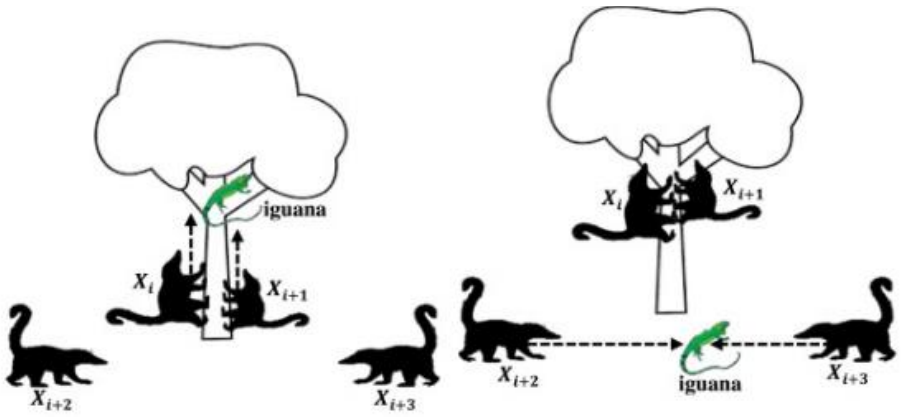
در تابع هدف پیشنهادی، E خطای تشخیص DDOS است و $\|X_i\|$ تعداد ویژگی‌های انتخاب شده توسط بردار ویژگی X_i است. Alpha و Beta به ترتیب دو عدد تصادفی بین صفر و یک است که مجموع آنها یک است. بردارهای ویژگی با تابع هدف ارزیابی می‌شوند و مقدار ارزیابی آنها در رابطه ۶، نمایش داده شده است. هر بردار ویژگی که تابع هدف را کمینه‌تر نماید، شایستگی بیشتری برای انتخاب ویژگی دارد[۲۳]،

$$F=\begin{bmatrix} F_1 \\ \vdots \\ F_i \\ \vdots \\ F_N \end{bmatrix}_{N\times 1}=\begin{bmatrix} F(X_1) \\ \vdots \\ F(X_i) \\ \vdots \\ F(X_N) \end{bmatrix}_{N\times 1} \quad (۶)$$

در فاز بهره‌برداری الگوریتم کوآتی، نصف جمعیت بردارهای ویژگی یا کوآتی‌ها از درخت بالا می‌روند تا ایگوانا از بالای درخت سقوط کند و در ادامه نصف دیگر جمعیت آن را تعقیب می‌کند تا آن را شکار نماید که در شکل ۶، نمایش داده شده است. در معادلات ۷، ۸ ، ۹ و ۱۰ رفتار تعقیب روی درخت و زمین ایگوانا توسط کوآتی را نمایش می‌دهد [۲۳]،

$$X_i^{P1}: x_{i,j}^{P1}=x_{i,j}+r\cdot\left(Iguana_{\ j}-I.x_{i,j}\right), i=1,2,..,\left\lfloor\frac{N}{2}\right\rfloor andj=1,2,..,m \quad (۷)$$

$$\text{Iguana}^{G}:\ \text{Iguana}_j^{G}=lb_j+r\cdot\left(ub_j-lb_j\right),\ j=1,2,..,m \quad (۸)$$



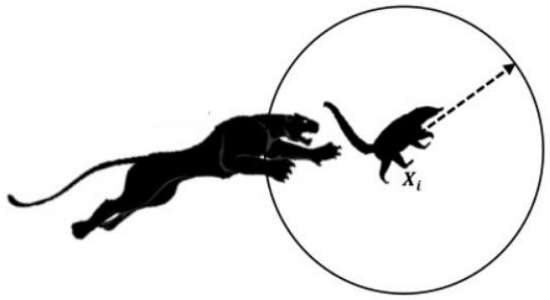
شکل ۶: سقوط و تعقیب ایگوانا توسط جمعیت الگوریتم بهینه سازی کوآتی[۲۳]

Figure 6. Falling and chasing iguana by the population of the Koati optimization algorithm [23]

$$X_i^{P1}: x_{i,j}^{P_1} = \begin{cases} x_{i,j} + r \cdot \left(\text{Iguana}_j^G - I \cdot x_{i,j} \right), F_{\text{Iguana}^G} < F_i \\ x_{i,j} + r \cdot \left(x_{i,j} - \text{Iguana}_j^G \right), else \end{cases} \quad (۹)$$
$$for\ i = \left\lfloor \frac{N}{2} \right\rfloor + 1, \left\lfloor \frac{N}{2} \right\rfloor + 2, .., N\ and\ j = 1, 2, .., m$$

$$X_i = \begin{cases} X_i^{P_1}, & F_i^{P_1} < F_i, \\ X_i, & else. \end{cases} \quad (۱۰)$$

X_i^{Pi} موقعیت جدید یک بردار ویژگی تحت تاثیر تعقیب است و F_i^{Pi} مقدار تابع هدف به ازای راه‌حل X_i^{Pi} است و r یک عدد تصادفی در بازه ۰ تا ۱۰ است. $Iguana_j^G$ نشان دهنده بعد j موقعیت جواب بهینه یا موقعیت ایگوانا است. مقدار ارزیابی یک ایگوانا با F_{Iguana}^G در نظر گرفته می‌شود. I یک عدد تصادفی و برابر ۱ یا ۲ است که ضریب تاثیر تعقیب و فرار است. فرآیند فرار کوآتی‌ها از شکارچیان مرحله بهره برداری یا جستجوی محلی است و در شکل ۷، نمایش داده شده است. در این حالت کوآتی از شکارچی فرار کرده و به یک موقعیت جدید رفته و برای مدلسازی این رفتار از معادلات ۱۱، ۱۲ و ۱۳ استفاده می‌شود [۲۳]،



شکل۷ : فرار کواتی‌ها از موقعیت خطر[۲۳]
Figure 7. The escape of Kuwaitis from a dangerous situation [23]

$$lb_j^{local} = \frac{lb_j}{t}, ub_j^{local} = \frac{ub_j}{t}, where\ t = 1, 2, .., T. \quad (۱۱)$$

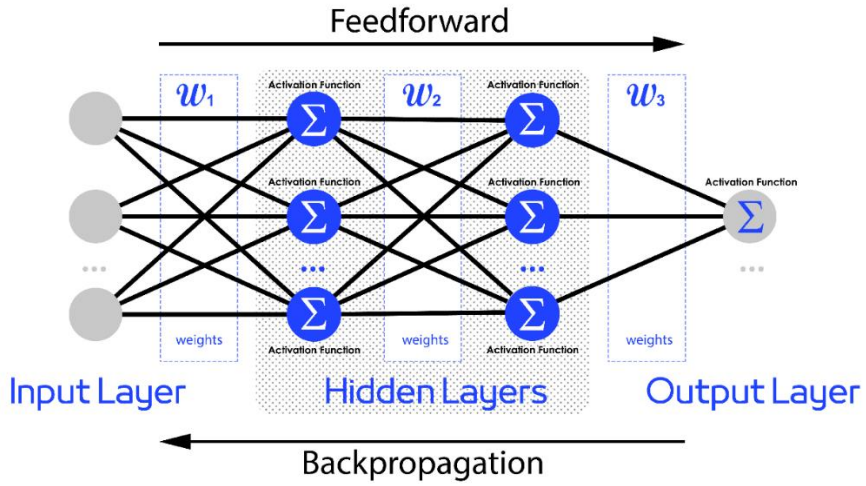
$$X_i^{P2}: x_{i,j}^{P2} = x_{i,j} + (1-2r) \cdot \left(lb_j^{local} + r \cdot \left(ub_j^{local} - lb_j^{local} \right) \right) i = 1, .., N,\ j = 1, .., m. \quad (۱۲)$$

$$X_i = \begin{cases} X_i^{P2}, & F_i^{P2} < F_i \\ X_i, & else \end{cases} \quad (۱۳)$$

X_i^{P2} موقعیت جدید یک بردار ویژگی در جستجوی محلی است. lb_j^{local} و ub_j^{local} به ترتیب محدوده بالا و پایین ابعاد بردارهای ویژگی است که به ترتیب یک و صفر است. t شمارنده تکرار الگوریتم و T حداکثر تعداد تکرار الگوریتم بهینه‌سازی کوآتی است. انتخاب ویژگی توسط روشهای فراابتکاری فقط در فاز انتخاب ویژگی دارای مقداری سربار زمانی است اما این سربار در مقابل کاهش ابعاد ترافیک بسیار ناچیز است. زمان اجرای الگوریتم‌های فراابتکاری برای انتخاب ویژگی در حد چند ثانیه است و انتخاب ویژگی فقط یک بار زمان آموزش شبکه عصبی اجراء می‌شود و با کشف بردار ویژگی بهینه دیگر فاز انتخاب ویژگی متوقف شده است. به عبارت ساده‌تر با انتخاب ویژگی بردار ویژگی در اوایل فرآیند اجرای سیستم تشخیص نفوذ، ویژگی‌های مهم کشف می‌شوند و در ادامه کار سیستم تشخیص نفوذ این بردار ویژگی بهینه باعث می‌شود تا یادگیری و طبقه‌بندی روی همه ویژگی‌ها انجام نشود و فقط روی ویژگی‌های انتخاب شده انجام شود و در این مرحله و داده‌های آزمون زمان طبقه‌بندی و تشخیص نفوذ به دلیل کاهش ابعاد ترافیک شبکه کاهش خواهد یافت. به عبارت دیگر انتخاب ویژگی مقداری سربار زمانی برای اموزش روی داده‌های آموزشی تحمیل می‌کند اما در زمان طبقه‌بندی داده‌ها و ترافیک آزمون این زمان جبران شده و باعث افزایش سرعت طبقه‌بندی ترافیک می‌شود.

۳-۴- طبقه بندی با شبکه عصبی چند لایه

در یک شبکه عصبی زمانی که وزن لایه‌های پنهان کاملاً به هم متصل می‌شوند، شبکه عصبی چند لایه نامیده می‌شود. در شبکه عصبی چند لایه هر نورون شبکه یک تابع فعال سازی دارد. تحت الگوریتم‌های پیشخور دسته‌بندی می‌شوند که در آن داده‌ها از ورودی، از طریق لایه‌های پنهان به خروجی در یک جهت جریان می‌یابند. اگر الگوریتم فقط مجموع وزنی هر نورون را محاسبه کند و به لایه بعدی منتقل شود، نمی‌تواند وزن های مورد استفاده برای به حداقل رساندن تابع هزینه را یاد بگیرد. تا زمانی که الگوریتم تکرار نشود، هیچ یادگیری موثری وجود ندارد. برای انجام این کار، ما باید از BP به عنوان یک الگوریتم یادگیری استفاده کنیم، که به شبکه عصبی چند لایه اجازه می دهد تا وزن شبکه را به طور مکرر با استفاده از گرادیان نزول تنظیم کند تا عملکرد هزینه را تا حد امکان پایین بیاورد. به طور خلاصه، شبکه عصبی چند لایه دارای چندین لایه پنهان است و پیشخور به جریان داده شبکه عصبی چند لایه در یک جهت از ورودی به خروجی اشاره دارد. شبکه عصبی چند لایه به یک شبکه عصبی با نورون های کاملاً متصل و استفاده از نوعی تابع فعال سازی اشاره دارد. در شکل۸، ساختار یک شبکه عصب چند لایه که در لایه مه و گره‌های مه نقش طبقه‌بندی کردن ترافیک شبکه را بر عهده دارد نمایش داده شده است.

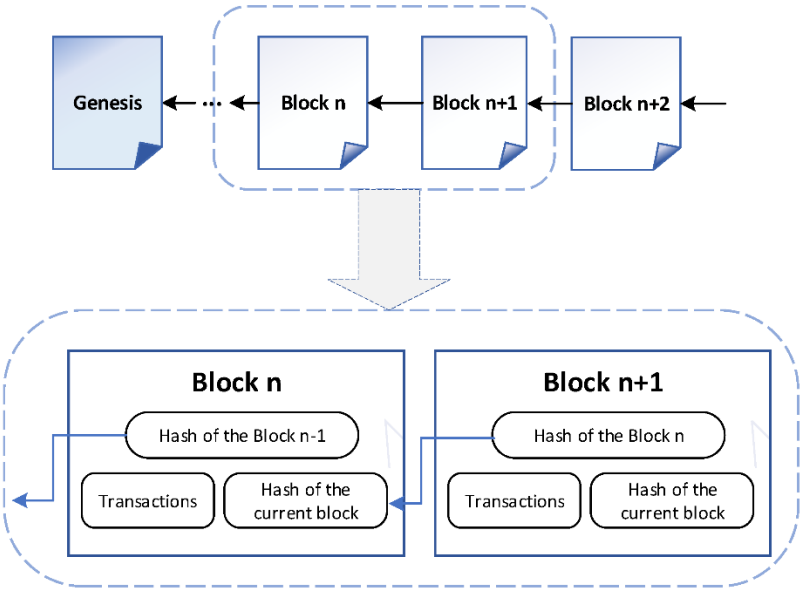


شکل ۸: ساختار شبکه عصبی چند لایه[۴۳]
Figure 8. Multilayer neural network structure [43]

۳-۵-تبادل لیست سیاه با بلاک چین

در روش پیشنهادی هر گره مه با یادگیری ماشین و هوش گروهی، ترافیک حمله را تشخیص داده و آدرس این ترافیک‌ها را در یک لیست سیاه قرار داده و با سایر گره‌های مه به اشتراک می‌گذارد. بلاک چین را می‌توان به عنوان یک شبکه همتا به همتای توزیع شده از بلوک‌ها تعریف کرد. هر بلوک با استفاده از هش رمزنگاری به بلوک قبلی پیوند داده می‌شود. فناوری بلاک چین در زمینه‌های مختلفی مانند مراقبت های بهداشتی، آموزشی، انرژی و غیره به کار گرفته شده است. سه نوع دفتر کل بلاک چین وجود دارد که در حال حاضر مورد استفاده قرار می‌گیرند و عبارتند از عمومی، کنسرسیوم و خصوصی است. بلاک چین های عمومی (مانند اتریوم) برای هر کسی که به اینترنت دسترسی دارد در دسترس است و هر کسی می تواند بلاک چین را بخواند و دفتر کل بلاک چین را حفظ کند، یعنی مکانیزم عضویت در آن وجود ندارد. بلاک چین های کنسرسیوم (مانند Hyperledger Fabric) توسط یک نهاد تاسیس شده نگهداری می‌شود که به دیگران دسترسی می‌دهد و یک کنسرسیوم از پیش تعریف شده از همتایان دارد که زنجیره را حفظ می‌کنند. بلاک چین‌های خصوصی توسط یک نهاد نگهداری می‌شوند که دسترسی به دیگران را فراهم می‌کند و هیچ فرآیند توافقی وجود ندارد. ابتدایی‌ترین تعریف بلاک چین این است که زنجیره‌ای از بلوک است که هر بلوک به کمک یک رابطه ریاضی به بلوک قبل از خود متصل می شود [۴۴]. بلوک به خودی خود محفظه ای از داده است. شکل۹، ساختار تولید زنجیره بلوک را نشان می‌دهد. فرض اصلی زیربنای بلاک چین این است که هر بلوک حاوی یک هش

خودشناس منحصر به فرد است که یکپارچگی زنجیره را تضمین می کند. هش[1] نمایه بلوک، داده‌ها(در اینجا لیست سیاه شامل IP گره‌های حمله کننده)، مهر زمانی و البته هش هش بلوک قبلی، این هش خودشناس را تشکیل می‌دهد. همچنین حاوی رکوردی از تراکنش‌ها به نام دفتر کل است که در زمان تولید بلاک چین انجام شده است. همانطور که هر بلوک به بلوک قبل از خود ارجاع می‌دهد، سابقه ای از تمام تراکنش هایی که قبل از تولید بلوک فعلی انجام شده است وجود دارد [۴۵]. در روش پیشنهادی هر گره مه یک عضو قرارداد بلاک چین است و لیست سیاه خود را به عنوان داده‌ها در یک بلاک قرار داده و آن را برای همه گره‌های مه ارسال می‌کند. گره‌های مه اگر هویت ارسال کننده را تایید کنند آنگاه اطلاعات لیست سیاه گره مه را با اطلاعات لیست سیاه خود ترکیب و تلفیق می‌کند.



شکل ۹: ساختار بلاک چین[۴۵]
Figure 9. Blockchain structure [45]

گره‌های که در بازه‌های زمانی مشخص می‌توانند لیست سیاه خود را با هم مبادله کنند یا می‌توان یک رویکرد مبتنی بر آستانه در نظر گرفت و به عنوان مثال اگر هر لیست سیاه ۵٪ دچار تغییر شود آنگاه گره مه می‌تواند درخواست اشتراک گذاری لیست سیاه را با بلاک چین نماید. در روش پیشنهادی از رویکرد اول استفاده شده است و گره‌ها بعد ۱۰ دقیقه لیست سیاه خود را مبادله می‌کنند. کاهش زمان مورد نظر باعث افزایش سربار ارسال و دریافت پیامها در لایه مه می‌شود. گره‌های مه برای انتقال و اشتراک گذاری لیست سیاه خود در بلاک چین از فرآیند و مراحل ذیل استفاده می‌کنند:

- در ابتدا گره مه لیست سیاه خود را در قسمت داده یک بلاک قرار می‌دهد.
- گره مورد نظر بلاک را برای سایر گره‌های مه ارسال می‌کند.
- گره‌های مه، اعتبار گره ارسال کننده را بررسی می‌کنند و اگر همه روی اعتبار گره مه اجماع داشتند آنگاه لیست سیاه را به زنجیره بلاک چین اضافه می‌کنند.
- یک نسخه از زنجیره بلاک چین برای همه گره‌ها ارسال می‌شود که شامل لیست سیاه اشتراکی است.

۴-نتایج تجربی

در این بخش سیستم تشخیص نفوذ پیشنهادی برای تشخیص حملاتDDoS پیاده‌سازی و مورد تحلیل قرار گرفته می‌شود. در اینجا، از نرم‌افزار متلب برای پیاده‌سازی هوش گروهی و شبکه عصبی مصنوعی استفاده می‌شود.

[1] Hash

۴-۱-پارامترهای پیاده سازی

اندازه جمعیت بردارهای ویژگی یا جمعیت الگوریتم کوآتی برابر ۲۰ و تعداد تکرار آن برابر ۵۰ است و هر آزمایش ۳۰ مرتبه تکرار و میانگین خروجی آنها محاسبه می‌شود. محدوده نرمالسازی در این مقاله بازه ۰ و ۱ است و از طرفی هم مقدار ضرایب Alpha و Beta در تابع هدف تصادفی و بین صفر و یک انتخاب می‌شود. سایر پارمترهای الگوریتم بهینه‌سازی کوآتی مانند مقادیر [۲۳]، تعیین می‌شود. شبکه عصبی مصنوعی نیز دارای دو لایه و در هر لایه به تعداد ویژگی‌های اولیه مجموعه داده NSL-KDD نورون مصنوعی در نظر گرفته می‌شود.

۴-۲-مجموعه داده

مجموعه داده NSL-KDD در این پژوهش برای پیاده‌سازی و ارزیابی روش پیشنهادی استفاده می‌شود. این مجموعه داده تعدادی زیادی حمله و از جمله حمله DDoS را پوشش می‌دهد. مجموعه داده NSL-KDD یک نسخه تصفیه شده از KDD'99 قبلی خود است، یک معیار شناخته شده در تحقیق در مورد تکنیک های تشخیص نفوذ است. این مجموعه داده برچسب‌گذاری شده به فایل‌های آموزشی و آزمایشی تقسیم می‌شود و می‌توان آن را از پایگاه داده آنلاین [۴۵] دانلود کرد.

علاوه بر ترافیک عادی، ۲۳ نوع حمله مستند شده (به عنوان مثال، نپتون، ipsweep، portsweep) وجود دارد که به چهار دسته اصلی انکار سرویس، کاوشگر، کاربر به ریشه و از راه دور به کاربر طبقه‌بندی می‌شوند. مقوله DDoS به حملاتی اشاره دارد که منابع موجود سرور را مصرف می‌کنند و سیستم مورد حمله را برای انجام درخواست‌های کاربر قانونی مشکل می‌سازد. یک حمله کاوشگر معمولاً قبل از حمله دسترسی انجام می شود و شامل جمع آوری اطلاعات در مورد قربانی، معمولاً با اسکن آدرس های IP و پورت‌ها است. حمله کاربر به ریشه تلاش می‌کند تا در سیستمی که مهاجم قبلاً دسترسی کاربر را دارد، دسترسی ریشه غیرمجاز به دست آورد. در یک مورد از راه دور به کاربر، یک اتصال غیرمجاز از یک سیستم راه دور تحت کنترل مهاجم برای به دست آوردن دسترسی محلی انجام می‌شود. برای هر رکورد ترافیک شبکه، ۴۱ نوع ویژگی وجود دارد که به عنوان انواع حمله یا عادی طبقه بندی می شوند. ۹ عدد از آنها مقادیر گسسته و ۳۲ مقدار باقی مانده پیوسته هستند. داده‌های گسسته از مقادیری استفاده می‌کنند که فقط می‌توانند مقادیر خاصی داشته باشند و قابل تقسیم نیستند. داده‌های پیوسته از مقادیری استفاده می‌کنند که می‌توانند هر مقدار عددی را به خود بگیرند و می توانند به بخش های کوچکتر تقسیم شوند. این ویژگی ها را می‌توان به چهار دسته پایه، محتوا، ترافیک مرتبط با زمان و ترافیک مبتنی بر میزبان طبقه بندی کرد [۴۵].

۴-۳-متریکهای ارزیابی

برای ارزیابی سیستم تشخیص نفوذ پیشنهادی از شاخص‌های ارزیابی مانند دقت۱، حساسیت۲ و صحت۳ مطابق معادله ۱۴، ۱۵، ۱۶ فرموله شده است.

$$Accuracy = ACC = \frac{TP + TN}{TP + TN + FP + FN} \times 100\% \quad (۱۴)$$

$$Sensitivity = Recall = DR = \frac{TP}{TP + FN} \times 100\% \quad (۱۵)$$

$$Precision = P = \frac{TP}{TP + FP} \times 100\% \quad (۱۶)$$

پارامترهای TP، TN، FP و FN به شکل تعریف می‌شود:

- نمونه‌های صحیح مثبت(TP): ترافیک وارد شده به لایه مه از نوع DDoS است و سیستم تشخیص نفوذ پیشنهادی آن را در دسته حملات DDoS قرار داده است.
- نمونه‌های غلط مثبت(FP): ترافیک وارد شده به لایه مه از نوع DDoS نبوده و سیستم تشخیص نفوذ پیشنهادی آن را در دسته حملات DDoS قرار داده است.

[1] Accuracy
[2] Sensitivity
[3] Precision

- نمونه‌های صحیح منفی(TN): ترافیک وارد شده به لایه مه از نوع DDoS نبوده و سیستم تشخیص نفوذ پیشنهادی آن را در دسته حملات DDoS قرار نداده است.
- نمونه‌های غلط منفی(FN): ترافیک وارد شده به لایه مه از نوع DDoS است و سیستم تشخیص نفوذ پیشنهادی آن را در دسته حملات DDoS قرار نداده است.

۴-۳-ارزیابی روش پیشنهادی

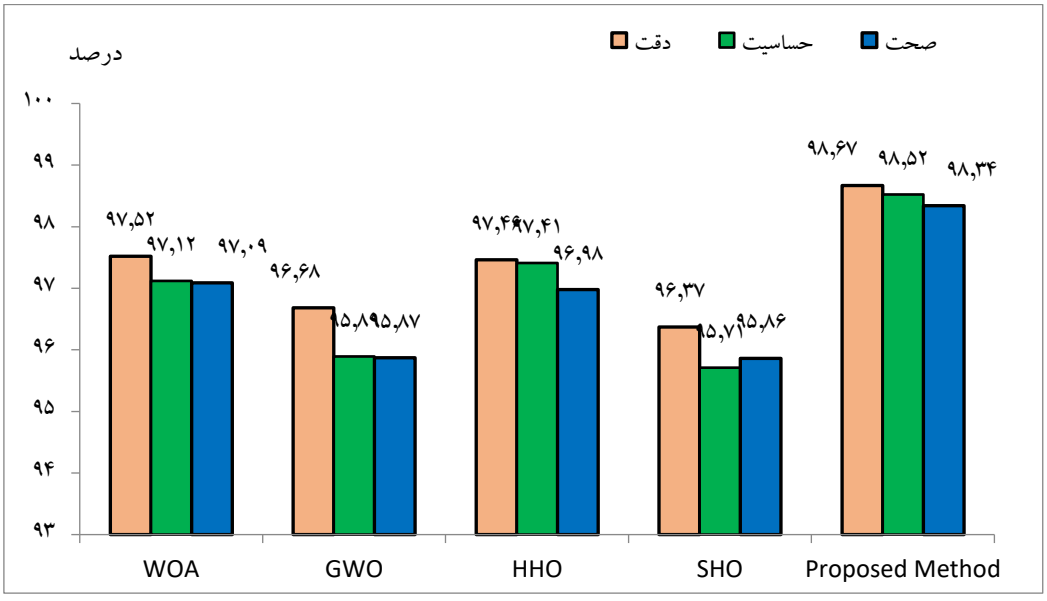
برای ارزیابی سیستم تشخیص نفوذ پیشنهادی سه حالت در نظر گرفته شده است. در حالت اول فقط از شبکه عصبی MLP در لایه مه استفاده می‌شود و در حالت دوم از شبکه عصبی MLP و الگوریتم انتخاب ویژگی COA استفاده می‌شود. در حالت سوم از الگوریتم یادگیری عمیق GAN در ترکیب با شبکه عصبی، هوش گروهی COA استفاده شده است. شاخص دقت، حساسیت و صحت روش پیشنهادی با روشهای مورد نظر در جدول۲، ارایه شده است.

جدول ۲: شاخص دقت، حساسیت و صحت در تشخیص حملات به شبکه

Table 2. Index of accuracy, sensitivity and accuracy in detecting network attacks

حالت	دقت	حساسیت	صحت
MLP	۸۹/۶۵	۸۸/۳۴	**۸۷/۶۴**
COA+MLP	۹۲/۶۳	۹۱/۵۸	**۹۱/۸۲**
GAN+COA+MLP(GCM) or Proposed Method	۹۸/۶۷	۹۸/۵۲	**۹۸/۳۴**

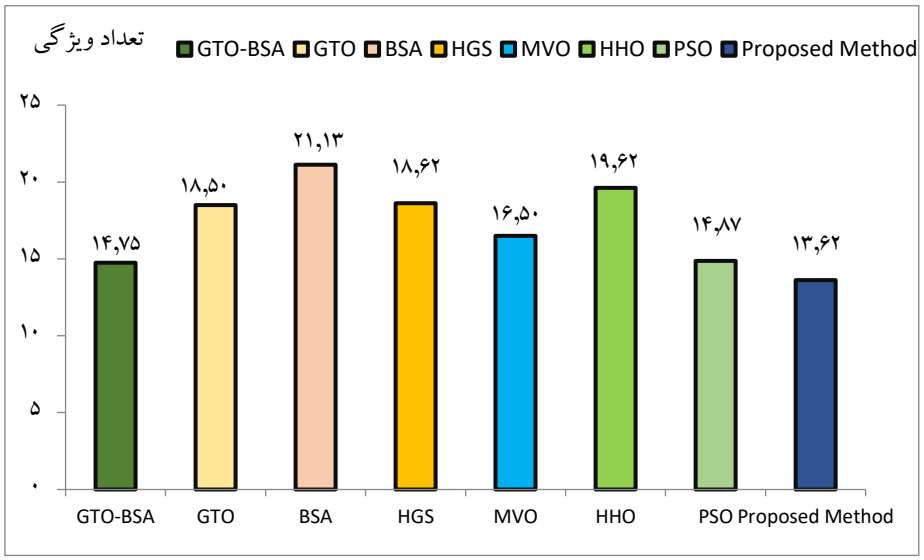
آزمایشات انجام شده نشان می‌دهد بدون متعادلسازی مجموعه داده و بدون انتخاب ویژگی، دقت، حساسیت و صحت روش پیشنهادی برای تشخیص نفوذ به ترتیب برابر ۸۹/۶۵٪، ۸۸/۳۴٪ و ۸۷/۶۴٪ است. اگر از ترکیب الگوریتم بهینه‌سازی کوآتی و شبکه عصبی مصنوعی بدون متعادلسازی مجموعه داده استفاده شود آنگاه دقت، حساسیت و صحت روش پیشنهادی برای تشخیص نفوذ به ترتیب برابر ۹۲/۶۳٪، ۹۱/۵۸٪ و ۹۱/۸۲٪ می‌شود. در صورتی که از متعادلسازی مجموعه داده با یادگیری عمیق شبکه GAN استفاده شود و انتخاب ویژگی نیز با الگوریتم بهینه‌سازی کوآتی در کنار شبکه عصبی مصنوعی چند لایه در لایه مه انجام شود آنگاه دقت، حساسیت و صحت روش پیشنهادی به ترتیب برابر ۹۸/۶۷٪، ۹۸/۲٪ و ۹۸/۳۴٪ است. یک فاز مهم روش پیشنهادی انتخاب ویژگی با روشهای هوش گروهی است و در اینجا روش پیشنهادی در تشخیص نفوذ با الگوریتم بهینه‌سازی وال یا WOA، الگوریتم گرگ بهینه‌سازی خاکستری یا GWO، الگوریتم بهینه‌سازی شاهین یا HHO و الگوریتم بهینه‌سازی کفتار یا SHO مقایسه می‌شود که نتایج آن در شاخص دقت، حساسیت و صحت در شکل۱۰، نمایش داده شده است.



شکل ۱۰: مقایسه دقت، حساسیت و صحت تشخیص حملات با روشهای هوش گروهی

Figure 10. Comparing the accuracy, sensitivity and accuracy of attack detection with group intelligence methods

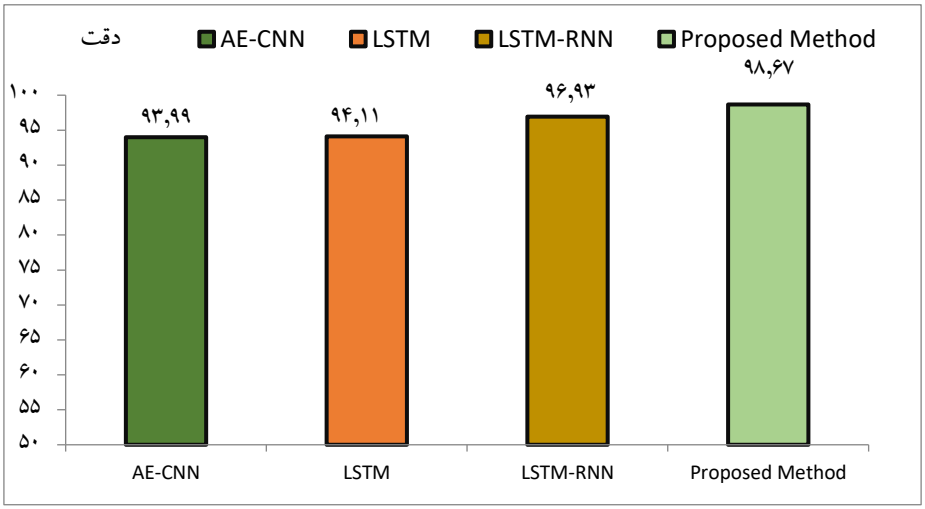
آزمایشات و مقایسه‌های انجام شده در متلب نشان می‌دهد روش پیشنهادی حداقل از الگوریتم بهینه‌سازی وال یا WOA، الگوریتم گرگ بهینه‌سازی خاکستری یا GWO، الگوریتم بهینه‌سازی شاهین یا HHO و الگوریتم بهینه‌سازی کفتار یا SHO دارای دقت، حساسیت و صحت بیشتری در تشخیص نفوذ است. دلیل دقت بیشتر روش پیشنهادی نسبت به الگوریتم‌های فرابتکاری مشابه آن است که روش پیشنهادی بین جستجوی بهره‌برداری و بهره‌وری نوعی تعادل برقرار کرده و فضای ویژگی را بهتر برای یافتن ویژگی‌های بهینه مورد جستجو قرار می‌دهد. روش پیشنهادی را می‌توان در تعداد ویژگی انتخاب شده با الگوریتم‌های مشابه نیز مقایسه نمود و در اینجا نتایج آزمایشات با مطالعه[۴۶] مقایسه و در شکل۱۱، نمایش داده می‌شود.



شکل ۱۱: مقایسه و متوسط تعداد ویژگی انتخاب شده از ترافیک شبکه

Figure 11. Comparison and average number of features selected from network traffic

تعداد ویژگی‌های انتخاب شده برای تشخیص حملات در روشهای GTO-BSA، GTO، BSA، HGS، MVO، HHO، PSO به ترتیب برابر ۱۴/۷۵، ۱۸/۵، ۲۱/۱۳، ۱۸/۶۲، ۱۶/۵۰، ۱۹/۶۲، ۱۴/۸۷ است و این در حالی است که تعداد متوسط تعداد ویژگی در آزمایشات در روش پیشنهادی برابر ۱۳/۶۲ است که نسبت به ۴۱ ویژگی در حدود ۶۶/۷۸٪ فضای ویژگی را کاهش ابعاد داده است. روش پیشنهادی در شاخص دقت برای تشخیص حملات با مطالعه [۴۷]، مطابق شکل ۱۲، مقایسه شده است.



شکل ۱۲: مقایسه شاخص دقت روش پیشنهادی با چند روش یادگیری عمیق

Figure 12. Comparing the accuracy index of the proposed method with several deep learning methods

ارزیابی‌ها نشان می‌دهد دقت روش پیشنهادی از روشهای AE-CNN، LSTM، LSTM-RNN بیشتر است. دقت، روشهای یادگیری عمیق AE-CNN، LSTM، LSTM-RNN برای تشخیص حملات به ترتیب برابر۹۳/۹۹٪، ۹۴/۱۱٪، ۹۶/۹۳٪ است و از دقت روش پیشنهادی مقادیر کمتری نشان می‌دهد. دقت روش پیشنهادی در تشخیص حملات از روشهای یادگیری عمیق بیشتر است که دلیل آن متعادلسازی مجموعه داده و انتخاب ویژگی هوشمندانه است. روش پیشنهادی به دلیل استفاده از بلاک چین، توانایی بالایی در احراز هویت دارد و پیامهای رد و بدل شده لیست سیاه آن نیز دارای امنیت بالایی است.

۵-نتیجه گیری

در سال‌های اخیر، اینترنت اشیا به عنوان یکی از خلاقانه‌ترین فناوری‌ها در محاسبات ارزیابی شده است، زیرا پتانسیل تغییر هر حوزه از زندگی انسان را دارد. با توجه به گزارشات تا سال ۲۰۲۰ تا ۲۰۲۵، پیش بینی می‌شود که تعداد دستگاه های هوشمند متصل به اینترنت به ۵۰ میلیارد و ۷۵ میلیارد برسد و آن را به یکی از سریع ترین ها تبدیل کند. زمینه‌هایی در تاریخ محاسبات هدف اینترنت اشیاء اتصال دستگاه‌ها و برقراری ارتباط ماشین به ماشین است، در نتیجه به دستگاه‌ها اجازه می‌دهد تا اطلاعات را بدون دخالت انسان مبادله کنند. اینترنت اشیا طیف وسیعی از کاربردها مانند خانه های هوشمند، شهرهای هوشمند، اندازه گیری هوشمند، کشاورزی، شبکه های هوشمند، مراقبت های بهداشتی هوشمند و غیره را پوشش می دهد. با توجه به پیشرفت-های روزافزون در فناوری اطلاعات و ارتباطات و مسائل مربوط به امنیت سایبری جهانی، نگرانی های امنیتی و حفظ حریم خصوصی به طور کلی به عنوان یک چالش اصلی استقرار اینترنت اشیا شناخته شده است. استقرار گسترده دستگاه‌های اینترنت اشیاء در یک محیط باز، شبکه‌ها را در معرض حملات سایبری و تهدیدات امنیتی مختلف قرار داده است.

حملات سایبری متعددی مانند پخش مجدد، کرم چاله، انکار سرویس ،کانال جانبی و غیره، همچنان یک تهدید برای اینترنت اشیاء هستند. از این رو، توسعه یک معیار امنیتی موثر که بتواند به طور مداوم و فوری حملاتی مانند حملات DoS در شبکه‌های IoT را یاد بگیرد و شناسایی کند، مهم است.سیستم های تشخیص نفوذ مبتنی بر امضا و مبتنی بر ناهنجاری به عنوان راه حل‌های امنیتی برای کاهش حملات و نفوذ به شبکه اینترنت اشیاء عمل می‌کنند. در این پژوهش یک سیستم تشخیص نفوذ کارآمد در لایه مه ارایه شده است و سیستم تشخیص نفوذ به صورت توزیع شده مستقر است و از این جهت حجم زیادی از ترافیک شبکه در زمان کم ارزیابی و تحلیل می‌شود. در روش پیشنهادی هر گره مه نقش یک سیستم تشخیص نفوذ را بر عهده دارد و از طرفی در لایه مه با یادگیری عمیق GAN ترافیک شبکه متعادل و با الگوریتم فراابتکاری COA که سال ۲۰۲۳ ارایه شده است ویژگی‌های مهم ترافیک شبکه در گره‌های مه تشخیص داده می‌شود. در روش پیشنهادی گره‌های مه با استفاده از بلاک چین لیست سیاه خود را با هم به اشتراک می‌گذارند تا محرمانگی سیستم تشخیص نفوذ توزیع شده افزایش یابد. آزمایشات در مجموعه داده NSL-KDD نشان داد روش پیشنهادی در تشخیص حملات از روشهای انتخاب ویژگی نظیر WOA، GWO، SHOو HHO دقت بیشتری دارد و از طرفی نسبت به روشهای یادگیری نظیر LSTM و CNN توانایی و دقت بیشتری در تشخیص حملات دارد. مزیت روش پیشنهادی در انتخاب ویژگی‌های دقیق و کاهش ابعاد بیشتر ترافیک شبکه نسبت به روشهای فراابتکاری مشابه است از طرفی دقت بیشتر نسبت به چند روش یادگیری عمیق مزیت اصلی روش پیشنهادی است. حفظ محرمانگی و ارسال ایمن پیامها و لیست سیاه بین گره‌های مه با بلاک چین از مزایای دیگر روش پیشنهادی است. در پژوهش آتی از شبکه عصبی ترکیبی CNN و LSTM به ترتیب برای استخراج ویژگی و طبقه‌بندی ترافیک شبکه استفاده می‌شود و از طرفی یک سیستم تشخیص نفوذ دو سطحی در لایه مه و ابر ارایه می‌شود. در این مطالعه پارامترهای شبکه عصبی مصنوعی با آزمون و خطا تعیین شد اما با بهینه‌سازی آنها می‌توان عملکر این شبکه را بهبود داد. یکی دیگر از پژوهش‌های آتی ما بهینه‌سازی پارامترهای شبکه LSTM با روشهای فراابتکاری جدید است تا پارامترهای انتخاب شود که شبکه LSTM دارای خطای کمتری در تشخیص حملات شود. در پژوهش آتی همچین زمانبندی وظایف در لایه مه و ابر برای تشخیص حملات نیز پیشنهادی می‌شود. یک رویکرد زمان‌بندی گردش کار موثر ابری در زمان تشخیص نفوذ با روشهای نظیر الگوریتم ذرات و زمان‌بندی کار برای محاسبات چند ابری با توجه به محدودیت‌های امنیتی و قابلیت اطمینان برای کاربردهای تشخیص نفوذ می‌تواند از پیشنهادات آتی ما باشد.

مراجع

[1] Z. Shah, I. Ullah, , H. Li, A. Levula and K. Khurshid, "Blockchain based solutions to mitigate distributed denial of service (DDoS) attacks in the Internet of Things (IoT): A survey," *Sensors*, vol. 22, no. 3, 2022, doi: 10.3390/s22031094.

[2] B. Kaur, S. Dadkhah, F. Shoeleh, E. C. P. Neto, P. Xiong, S. Iqbal and A. A. Ghorbani, "Internet of things (IoT) security dataset evolution: Challenges and future directions," *Internet of Things*, vol. 22, p. 100780, 2023, doi: 10.1016/j.iot.2023.100780.

[3] N. Elsayed, Z. ElSayed and M. Bayoumi, "IoT Botnet Detection Using an Economic Deep Learning Model," *arXiv preprint arXiv:2302.02013, IEEE World AI IoT Congress (AIIoT)*, 2023, doi: 10.48550/arXiv.2302.02013.

[4] P. Pan, X. Ma, Y. Fu and F. Chen, "Automating Group Management of Large-Scale IoT Botnets for Antitracking. Security and Communication Networks," *Security and Communication Networks*, vol. 2022, Article ID: 4196945, doi: 10.1155/2022/4196945.

[5] P. Kumari and A. K. Jain, "A comprehensive study of DDoS attacks over IoT network and their countermeasures," *Computers & Security*, vol. 127, p. 103096, 2023, doi: 10.1016/j.cose.2023.103096.

[6] S. A. Khanday, H. Fatima and N. Rakesh, "Implementation of intrusion detection model for DDoS attacks in Lightweight IoT Networks," *Expert Systems with Applications*, vol. 215, p. 119330, 2023, doi: 10.3390/app13179937.

[7] F. T. Zahra, Y. S. Bostanci and M. Soyturk, "Real-Time Jamming Detection in Wireless IoT Networks," in *IEEE Access*, vol. 11, pp. 70425-70442, 2023, doi: 10.1109/ACCESS.2023.3293404.

[8] S. Kumar, A. Guerrero and C. Navarro, "Cyber Security Flood Attacks and Risk Assessment for Internet of Things (IoT) Distributed Systems," *IEEE World AI IoT Congress (AIIoT)*, Seattle, WA, USA, 2023, pp. 0392-0397, doi: 10.1109/AIIoT58121.2023.10174553.

[9] M. Mahmood and Q. Shafi, "A Smart IDS in IoT System to Detect Zero-Day Intrusions Using Automated Signature Update," *Research Square*, 2023, doi: 10.21203/rs.3.rs-3014508/v1.

[10] M. Douiba, S. Benkirane, A. Guezzaz and M. Azrour, "An improved anomaly detection model for IoT security using decision tree and gradient boosting," *The Journal of Supercomputing*, vol. 79, no. 3, pp. 3392-3411, 2023, doi: 10.1007/s11227-022-04783-y.

[11] A. Belhadi, Y. Djenouri, D. Djenouri , G. Srivastava and J. C. W Lin, "Group intrusion detection in the Internet of Things using a hybrid recurrent neural network," *Cluster Computing*, vol. 26, no. 2, pp. 1147-1158, 2023, doi: 10.1007/s10586-022-03779-w.

[12] G. O. Anyanwu, C. I. Nwakanma, J. M. Lee and D. S. Kim, "RBF-SVM kernel-based model for detecting DDoS attacks in SDN integrated vehicular network," *Ad Hoc Networks*, vol. 140, p. 103026, 2023, doi: 10.1016/j.adhoc.2022.103026.

[13] I. Priyadarshini, P. Mohanty, A. Alkhayyat, R. Sharma and S. Kumar, " SDN and application layer DDoS attacks detection in IoT devices by attention-based Bi-LSTM-CNN," *Transactions on Emerging Telecommunications Technologies*, p. e4758, 2023, doi: 10.1002/ett.4758.

[14] S. S. S. Othman, C. F. M. Foozy and S. N. B. Mustafa, "Feature Selection of Distributed Denial of Service (DDos) IoT Bot Attack Detection Using Machine Learning Techniques," *Journal of Soft Computing and Data Mining*, vol. 4 , no. 1, pp. 63-71, 2023, doi: 10.30880/jscdm.2023.04.01.006.

[15] R. Alkanhel, E. S. M. El-kenawy, A. A. Abdelhamid, A. Ibrahim, M. A. Alohali, M. Abotaleb and D. S. Khafaga, "Network Intrusion Detection Based on Feature Selection and Hybrid Metaheuristic Optimization," *Computers, Materials & Continua*, vol. 74, no. 2, pp. 2677-2693, 2023, doi: 10.32604/cmc.2023.033273.

[16] B. Bencsik, I. Reményi, M. Szemenyei and J. Botzheim, "Designing an embedded feature selection algorithm for a drowsiness detector model based on electroencephalogram data," *Sensors*, vol. 23, no. 4, 2023, doi: 10.3390/s23041874.

[17] M. Shafiq, Z. Tian, A. K. Bashir, X. Du and M. Guizani, "IoT malicious traffic identification using wrapper-based feature selection mechanisms," *Computers & Security* , vol. 94 , p. 101863, 2020, doi: 10.1016/j.cose.2020.101863.

[18] R. Yadav, I. Sreedevi and D. Gupta, "Augmentation in performance and security of WSNs for IoT applications using feature selection and classification techniques," *Alexandria Engineering Journal*, vol. 65, pp. 461-473, 2023, doi: 10.1016/j.aej.2022.10.033.

[19] M. S. Aliabadi, and A. Jalalian, "Detection of attacks in the Internet of Things with the feature selection approach based on the whale optimization algorithm and learning by majority voting," *Research Square* , 2023, doi: 10.21203/rs.3.rs-2424464/v2.

[20] R. Alkanhel, , E. S. M. El-kenawy, A. A. Abdelhamid, A. Ibrahim, M. A. Alohali, M. Abotaleb and D. S. Khafaga, "Network Intrusion Detection Based on Feature Selection and Hybrid Metaheuristic Optimization," *Computers, Materials & Continua*, vol. 74, no. 2, pp. 2677-2693, 2023, doi: 10.32604/cmc.2023.033273.

[21] I. Katib, and M. Ragab, "Blockchain-Assisted Hybrid Harris Hawks Optimization Based Deep DDoS Attack Detection in the IoT Environment," *Mathematics*, vol. 11, no. 8, pp. 1-16 , 2023 , doi: 10.3390/math11081887.

[22] T. K. Boppana and P. Bagade, "GAN-AE: An unsupervised intrusion detection system for MQTT networks," *Engineering Applications of Artificial Intelligence*, vol. 119, 2023, doi: 10.1016/j.engappai.2022.105805.

[23] M. Dehghani, Z. Montazeri, E. Trojovská and P. Trojovský, "Coati Optimization Algorithm: A new bio-inspired metaheuristic algorithm for solving optimization problems," *Knowledge-Based Systems*, vol. 259, p. 110011, 2023 , doi: 10.1016/j.knosys.2022.110011.

[24] M. R. Alam, S. I. Khan, S. B. Z Chowa, A. H Chowdhury, S. R. Kabir and M. J. Sadeq, "Use of Blockchain to Prevent Distributed Denial-of-Service (DDoS) Attack: A Systematic Literature Review," *Advances in Distributed Computing and Machine Learning*, vol. 660, pp. 39-47, 2023, doi: 10.1007/978-981-99-1203-2_4.

[25] Y. Zhang, Y. Liu, X. Guo, Z. Liu, X. Zhang and K. Liang, "A BiLSTM-Based DDoS Attack Detection Method for Edge Computing," *Energies*, vol. 15, no. 21, 2022, doi: 10.3390/en15217882.

[26] S. H. Lee, Y. L. Shiue, C. H. Cheng, Y. H. Li and Y. F. Huang, "Detection and Prevention of DDoS Attacks on the IoT," *Applied Sciences*, vol. 12, no. 23, 2022, doi: 10.3390/app122312407.

[27] S. Alosaimi and S. M. Almutairi, "An Intrusion Detection System Using BoT-IoT," *Applied Sciences*, vol. 13, no. 9, 2023, doi: 10.3390/app13095427.

[28] Z. Ahmad, A. Shahid Khan, C. Wai Shiang, J. Abdullah and F. Ahmad, "Network intrusion detection system: A systematic study of machine learning and deep learning approaches," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 1, p. e4150, 2021, doi: 10.1002/ett.4150.

[29] H. A. Hassan, E. E. Hemdan, W. El-Shafai, M. Shokair and F. E. A. El-Samie, "Intrusion Detection Systems for the Internet of Thing: A Survey Study," *Wireless Personal Communications*, vol. 128, no. 4, pp. 2753-2778, doi: 10.1007/s11277-022-10069-6.

[30] R. Malik, Y. Singh, Z. A Sheikh, P. Anand, P. K, Singh and T. C. Workneh, "An improved deep belief network ids on iot-based network for traffic systems," *Journal of Advanced Transportation*, vol. 2022, Article ID: 7892130, 2022, doi: 10.1155/2022/7892130.

[31] I. Ortega-Fernandez, M. Sestelo, J. C. Burguillo and C. Pinon-Blanco, "Network intrusion detection system

for DDoS attacks in ICS using deep autoencoders," *Wireless Networks*, pp. 1-17, 2023, doi: 10.1007/s11276-022-03214-3.

[32] S. A. Khanday, H. Fatima and N. Rakesh, "Implementation of intrusion detection model for DDoS attacks in Lightweight IoT Networks," *Expert Systems with Applications*, vol. 215, Article ID: 119330, 2023, doi: 10.3390/app13179937.

[33] A. S. A. Issa and Z. Albayrak, "Ddos attack intrusion detection system based on hybridization of cnn and lstm. Acta Polytechnica Hungarica," *Acta Polytechnica Hungarica*, vol. 20 , no. 3, pp. 1-19, 2023, doi: 10.12700/APH.20.3.2023.3.6.

[34] A. Maryposonia, "An Efficient Network Intrusion Detection System for Distributed Networks using Machine Learning Technique," in *IEEE International Conference on Trends in Electronics and Informatics (ICOEI)*, 2023, pp. 1258-1263, doi: 10.1109/ICOEI56765.2023.10126055.

[35] G. O. Anyanwu, C. I. Nwakanma, J. M.Lee and D. S. Kim, "RBF-SVM kernel-based model for detecting DDoS attacks in SDN integrated vehicular network," *Ad Hoc Networks*, vol. 140, p. 103026, 2023, doi: 10.1016/j.adhoc.2022.103026.

[36] P. Aravamudhan, "A novel adaptive network intrusion detection system for internet of things," *Plos one*, vol. 18, no. 4 , p. e0283725, 2023, doi: 10.1371/journal.pone.0283725.

[37] A. Almazyad, L. Halman and A. Alsaeed, "Probe Attack Detection Using an Improved Intrusion Detection System," *Computers, Materials & Continua*, vol. 74, no. 3, pp. 4769-4784, 2023, doi: 10.32604/cmc.2023.033382.

[38] G. Nagarajan and P. J. Sajith, "Optimization of BPN parameters using PSO for intrusion detection in cloud environment," *Soft Computing*, pp. 1-12, doi: 10.1007/s00500-023-08737-1.

[39] A. Thangasamy, B. Sundan and L. Govindaraj, "A Novel Framework for DDoS Attacks Detection Using Hybrid LSTM Techniques," *Computer Systems Science & Engineering*, vol. 45, no. 3, pp. 1-15, doi: 10.32604/csse.2023.032078.

[40] Z. Majidian, S. TaghipourEivazi, B. Arasteh and S. Babai, "An intrusion detection method to detect denial of service attacks using error-correcting output codes and adaptive neuro-fuzzy inference," *Computers and Electrical Engineering*, vol. 106, p. 108600, 2023, doi: 10.1016/j.compeleceng.2023.108600

[41] P. Radoglou Grammatikis, P. Sarigiannidis, G. Efstathopoulos and E. Panaousis, "ARIES: A novel multivariate intrusion detection system for smart grid," *Sensors*, vol. 20, no. 18, pp. 1-20, 2020, doi: 10.3390/s20185305.

[42] W. Xu, J. Jang-Jaccard, T. Liu, F. Sabrina and J. Kwak, "Improved Bidirectional GAN-Based Approach for Network Intrusion Detection Using One-Class Classifier," *Computers*, vol. 11, no. 6, May 2022, doi: 10.3390/computers11060085.

[43] S. Alzughaibi and S. El Khediri, "A Cloud Intrusion Detection Systems Based on DNN Using Backpropagation and PSO on the CSE-CIC-IDS2018 Dataset," *Applied Sciences*, vol. 13, no. 4, Feb. 2023, doi: 10.3390/app13042276.

[44] R. K. Gupta, V. Chawla, R. K. Pateriya, P. K. Shukla, S. Mahfoudh, and S. B. H. Shah, "Improving collaborative intrusion detection system using blockchain and pluggable authentication modules for sustainable Smart City," *Sustainability*, vol. 15, no. 3, 2023, doi: 10.3390/su15032133.

[45] "NSL-KDD Dataset", *Available online: https://www.unb.ca/cic/datasets/nsl.html* , accessed on 27 December 2022.

[46] S. S. Kareem, R. R. Mostafa, F. A. Hashim and H. M. El-Bakry, "An effective feature selection model using hybrid metaheuristic algorithms for iot intrusion detection," *Sensors*, vol. 22, no. 4, pp. 1-22, Feb. 2022, 1396, doi: 10.3390/s22041396.

[47] R. Yao, N. Wang, Z. Liu, , P. Chen, and X. Sheng, "Intrusion detection system in the advanced metering infrastructure: a cross-layer feature-fusion CNN-LSTM-based approach," *Sensors*, vol. 21, no. 2, 2021, doi: 10.3390/s21020626.

[48] Y. Yin, J. Jang-Jaccard, W. Xu, A. Singh, J. Zhu, F. Sabrina and J. Kwak, "IGRF-RFE: a hybrid feature selection method for MLP-based network intrusion detection on UNSW-NB15 dataset," *Journal of Big Data*, vol. 10, no. 1, pp. 1-26, 2023, doi: 10.48550/arXiv.2203.16365.

[49] M. Mohy-eddine, A. Guezzaz, S. Benkirane and M. Azrour, "An efficient network intrusion detection model for IoT security using K-NN classifier and feature selection," *Multimedia Tools and Applications*, vol. 82, no. 15, pp. 23615–23633 , 2023, doi: 10.1007/s11042-023-14795-2.

[50] D. Kshirsagar and S. Kumar, "Towards an intrusion detection system for detecting web attacks based on an ensemble of filter feature selection techniques," *Cyber-Physical Systems*, vol. 9, no. 3, pp. 244-259, Jan. 2022, doi: 10.1080/23335777.2021.2023651.

[51] Z. Sharifian, B. Barekatain, A. A. Quintana, Z. Beheshti and F. Safi-Esfahani, "Sin-Cos-bIAVOA: A new feature selection method based on improved African vulture optimization algorithm and a novel transfer function to DDoS attack detection," *Expert Systems with Applications*, vol. 228, p. 120404, October 2023, doi: 10.1016/j.eswa.2023.120404.

[52] U. S. Chanu, K. J. Singh and Y. J. Chanu, "A dynamic feature selection technique to detect DDoS attack," *Journal of Information Security and Applications*, vol. 74, p. 103445, May 2023, doi: 10.1016/j.jisa.2023.103445.

[53] Y. Sanjalawe, and T. Althobaiti, "DDoS Attack Detection in Cloud Computing Based on Ensemble Feature Selection and Deep Learning", *Computers, Materials & Continua*, vol. 75, no. 2, pp. 3571-3588, 31 March 2023, doi: 10.32604/cmc.2023.037386.

[54] B. Uzun and S. Ballı, "A novel method for intrusion detection in computer networks by identifying multivariate outliers and ReliefF feature selection," *Neural Computing and Applications*, vol. 34, no. 20, pp. 17647-17662, June 2022, doi: 10.1007/s00521-022-07402-2.

[55] N. Alsharif, "Ensembling PCA-based Feature Selection with Random Tree Classifier for Intrusion Detection on IoT Network," in *International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)*, Semarang, Indonesia, 2021, pp. 317-321, doi: 10.23919/EECSI53397.2021.9624298.