JOURNAL OF SOUTHERN COMMUNICATION ENGINEERING
ISLAMIC AZAD UNIVERSITY BUSHEHR BRANCH

E-ISSN: 2980-9231
https://sanad.iau.ir/journal/jce

https://doi.org/10.30495/jce.2023.1998267.1233

Vol. 14/ No. 55/2025

Research Article

Detection of DDoS Attacks in SDN Switches with Deep Learning and Swarm Intelligence Approach

Mohsen Eghbali[1] | Mohammad Reza Mollakhalili Meybodi[2*]

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

[2]Department of Computer Engineering, Maybod Branch, Islamic Azad University, Maybod, Iran.
mollakhalili@maybodiau.ac.ir

Correspondence
Mohammad Reza Mollakhalili Meybodi, Associate Professor of Computer Engineering, Maybod Branch, Islamic Azad University, Maybod, Iran.
mollakhalili@maybodiau.ac.ir

Main Subjects:
Internet of things

Paper History:
Received: 16 October 2023
Revised: 2 December 2023
Accepted: 17 December 2023

Abstract

This paper introduces an efficient intrusion detection system for the Internet of Things, addressing the challenge of malware-infected IoT nodes acting as botnet attackers, along with issues in existing intrusion detection systems such as feature selection, data imbalance, and centralization. The proposed system leverages the distributed architecture of SDN. The method begins by balancing the dataset using the SMOTE technique. Essential features are then selected using the African Vulture Optimization Algorithm. Subsequently, an LSTM deep learning model is trained within the SDN controller. SDN switches utilize this trained model for attack detection. To enhance attack mitigation, attacking node addresses are shared among SDN switches, ensuring consistent recognition and enabling effective Distributed Denial-of-Service (DDoS) attack prevention across the network. Experimental results obtained in MATLAB, using the NSL-KDD dataset, demonstrate the proposed method's effectiveness, achieving an accuracy of 99.34%, a sensitivity of 99.16%, and a precision of 98.93% in attack detection. The proposed method outperforms feature selection methods based on WOA, HHO, and AO algorithms, and deep learning methods like LSTM, RNN, and CNN, particularly in detecting DDoS attacks.

Keywords: Internet of Things, Intrusion detection system, DDoS attacks, SDN network, Deep learning.

Highlights

- Development of a distributed intrusion detection system based on SDN architecture.
- Dataset balancing using SMOTE method in SDN controller.
- Introduction of a feature selection and binary version of the AVOA for attack detection.
- Integration of swarm intelligence and LSTM deep learning in SDN network to detect IoT attacks.

Citation: M. Eghbali, and M.R. Mollakhalili Meybodi, "Detection of DDoS Attacks in SDN Switches with Deep Learning and Swarm Intelligence Approach," *Journal of Southern Communication Engineering*, vol. 14, no. 55, pp. 94–120, 2025, doi:10.30495/jce.2023.1998267.1233 [in Persian].

1. Introduction

The Internet of Things (IoT) has undergone remarkable advancements, becoming a cornerstone of modern technology. Smart devices are now ubiquitous, seamlessly integrated into everyday life, offering unprecedented convenience and efficiency. The proliferation of IoT devices has revolutionized various sectors, including smart homes, healthcare, transportation, and energy management, by enabling automation, enhancing productivity, and optimizing resource utilization [1]. However, this rapid expansion has also introduced significant challenges, particularly in the realms of security and privacy.

One of the most pressing concerns is the vulnerability of IoT devices to cyberattacks. These devices, often designed with limited computational resources and security measures, are prime targets for malicious actors. Among the most prevalent and damaging attacks are Distributed Denial of Service (DDoS) attacks. In such attacks, a multitude of compromised IoT devices, infected with malware, are harnessed to overwhelm a target network with excessive traffic, rendering it inaccessible to legitimate users [2]. The consequences of these attacks can be severe, disrupting critical services and causing substantial financial and reputational damage.

The rise in DDoS attacks has been fueled by the increasing number of IoT devices connected to the internet. These devices, equipped with sensors and remote communication capabilities, have become integral components of the IoT ecosystem. However, their widespread adoption has also expanded the attack surface, making them attractive targets for cybercriminals. The situation is exacerbated by the fact that many IoT devices are deployed with default configurations and lack robust security mechanisms, making them easy prey for malware such as the Mirai botnet, which has been responsible for some of the largest DDoS attacks in recent history [3].

To combat these threats, researchers have developed various intrusion detection techniques. Traditional methods include signature-based detection, which relies on a database of known attack patterns, and anomaly-based detection, which identifies deviations from normal network behavior [4]. While these approaches have proven effective to some extent, they are not without limitations. Signature-based methods struggle to detect novel attacks, while anomaly-based techniques can generate high false-positive rates. Moreover, the centralized nature of many intrusion detection systems poses scalability challenges, particularly in the context of IoT networks, which generate vast amounts of data.

In recent years, machine learning and deep learning have emerged as powerful tools for enhancing intrusion detection capabilities. These techniques can analyze complex, high-dimensional data and identify subtle patterns indicative of malicious activity [5]. Deep learning, in particular, has shown great promise due to its ability to model non-linear relationships and capture intricate features in network traffic. However, the effectiveness of these methods depends on the quality and balance of the training data. Imbalanced datasets, where one class of data is underrepresented, can lead to biased models with poor detection performance [6].

To address these challenges, this paper proposes a distributed intrusion detection system within a Software-Defined Networking (SDN) framework. SDN offers a centralized control plane that can dynamically manage network resources and traffic flows, providing a flexible and scalable platform for implementing security measures [7]. The proposed system leverages several advanced techniques to enhance detection accuracy and efficiency:

1. Data Balancing: The Synthetic Minority Over-sampling Technique (SMOTE) is used to balance the dataset, ensuring that the model is trained on a representative sample of both normal and attack traffic [8]. This step is crucial for improving the model's ability to detect rare but critical attack events.
2. Feature Selection: The African Vulture Optimization Algorithm (AVOA) is employed for feature selection. This metaheuristic algorithm, inspired by the foraging behavior of vultures, excels at navigating complex, high-dimensional search spaces to identify the most relevant features for intrusion detection [9]. By reducing the dimensionality of the data, AVOA enhances the efficiency of the detection process and improves the model's performance.
3. Deep Learning: The system incorporates Long Short-Term Memory (LSTM) networks, a type of recurrent neural network known for its ability to capture temporal dependencies in sequential data. LSTM is particularly well-suited for analyzing network traffic, which often exhibits time-based patterns. The trained LSTM model, along with the optimized feature set, is deployed across the SDN switches, enabling distributed detection of DDoS attacks in real-time.

The primary contribution of this research is the development of an efficient, distributed intrusion detection system tailored for IoT networks. By integrating data balancing, intelligent feature selection, and deep learning within an SDN architecture, the proposed system addresses key challenges in IoT security, such as data imbalance, scalability, and detection accuracy. The system's distributed nature ensures that it can handle the high volume of traffic generated by IoT devices, while its advanced algorithms enable precise and timely detection of DDoS attacks.

In summary, this paper presents a comprehensive solution to the growing threat of DDoS attacks in IoT networks. By leveraging the strengths of SDN, machine learning, and deep learning, the proposed system offers a robust and scalable approach to enhancing the security of IoT ecosystems [10]. The findings of this research have significant

implications for the development of future intrusion detection systems, paving the way for more secure and resilient IoT infrastructures.

2. Innovation and contributions

The proposed method for detecting network attacks employs a distributed architecture within SDN switches. This method consists of the following steps:

1. Data Balancing with SMOTE: The SDN controller receives network traffic and balances the dataset using the Synthetic Minority Over-sampling Technique (SMOTE). This technique generates synthetic samples for minority classes (e.g., attack traffic), addressing data imbalance and preventing overfitting.
2. Feature Selection with AVOA: The controller utilizes the African Vulture Optimization Algorithm (AVOA) to select the most important features from the network traffic. AVOA excels in identifying optimal features due to its ability to perform both global and local searches simultaneously. Each feature vector is treated as a vulture, and the optimal feature vectors are selected using objective functions.
3. Training the LSTM Deep Learning Model: The controller employs an LSTM (Long Short-Term Memory) neural network to classify network traffic. LSTM is particularly effective for analyzing time-series data and avoids issues such as the vanishing gradient problem. The trained LSTM model, along with the optimal feature vector, is distributed to the SDN switches.
4. Intrusion Detection in SDN Switches: Each SDN switch analyzes network traffic using the optimal feature vector and the LSTM model to detect attacks. The switches can also share information about malicious IP addresses of attacking nodes and block malicious traffic.
5. Information Sharing Among Switches: SDN switches share information about malicious IP addresses among themselves, enabling more effective identification and mitigation of DDoS attacks.

Key Innovations of This Paper:

- Data Balancing: The use of SMOTE resolves data imbalance issues, improving model accuracy and robustness.
- Intelligent Feature Selection: The African Vulture Optimization Algorithm (AVOA) accurately selects important features, reducing data dimensionality and enhancing detection efficiency.
- Use of LSTM: The LSTM neural network is highly effective for detecting DDoS attacks due to its ability to process time-series data and capture temporal dependencies.
- Distributed Architecture: Distributing the intrusion detection process across SDN switches increases system speed, scalability, and efficiency.

This method integrates advanced techniques such as SMOTE, AVOA, and LSTM to create an efficient and accurate intrusion detection system for SDN networks.

3. Materials and Methods

In the proposed method, the SDN controller utilizes the optimal feature vector calculated by the African Vulture Optimization Algorithm (AVOA) as the input for the LSTM classifier. The LSTM neural network, a deep learning model, incorporates input, forget, and output gates, making it highly efficient for classifying network traffic. This network models hidden states and cell states using specific equations, enabling it to analyze time-series data and retain critical information in its memory. These characteristics make LSTM particularly effective for detecting network attacks.

One of the key advantages of the LSTM network is its ability to avoid issues such as vanishing gradients or exploding gradients, which are common in traditional recurrent neural networks (RNNs). Additionally, LSTM can process longer sequences of data, overcoming the limitations imposed by activation functions. By leveraging the AVOA algorithm to select important features, the accuracy and effectiveness of LSTM in detecting attacks are significantly improved.

The proposed process involves the following steps:

1. Data Balancing: Network traffic enters the SDN controller and is balanced using the SMOTE method.
2. Feature Selection: The AVOA algorithm is applied to select the optimal features, and the feature vectors are updated.
3. Model Deployment: The trained LSTM model, along with the optimal feature vector, is distributed to the SDN switches.
4. Attack Detection: The switches use the LSTM model to detect DDoS attacks and block malicious IP addresses.

This method achieves high accuracy in attack detection by intelligently combining feature selection and deep learning.

4. Results and Discussion

The proposed intrusion detection system is implemented in an SDN architecture using Matlab and evaluated against similar methods. It utilizes 70% of the data for training and 30% for testing, with data normalized between 0 and 1. The system employs the AVOA for feature selection and LSTM for classification, achieving high

accuracy, sensitivity, and precision. The NSL-KDD dataset, which includes four main attack types, is used for evaluation. However, the dataset is highly imbalanced, with normal traffic dominating. To address this, the SMOTE method is applied to balance the data by generating synthetic samples for minority classes.
Experimental results show that without balancing, the system achieves 96.68% accuracy, 95.52% sensitivity, and 95.44% precision. With SMOTE balancing, these metrics improve to 99.34%, 99.16%, and 98.93%, respectively. The system outperforms other feature selection algorithms like WOA, HHO, and GEO due to the superior intelligence and hierarchical mechanism of AVOA. Additionally, it surpasses deep learning methods such as CNN and CNN+LSTM, as well as hybrid swarm intelligence algorithms like Black Widow and Honey Bee and Grey Wolf Optimizer, in terms of accuracy. However, it slightly lags behind the majority voting-based method.
In conclusion, the proposed method combines SMOTE, AVOA, and LSTM to create an efficient and accurate intrusion detection system. Data balancing and intelligent feature selection significantly enhance its performance, making it highly effective in detecting DDoS and other cyberattacks. This approach demonstrates the importance of addressing data imbalance and leveraging advanced optimization and deep learning techniques for robust network security.

5. Conclusion

The Internet of Things connects smart devices to generate and collect vast amounts of data, but it faces significant challenges from cyberattacks that disrupt services. To address this, the proposed method introduces an efficient intrusion detection system within a distributed SDN architecture. This system leverages the SMOTE algorithm to balance imbalanced datasets like NSL-KDD and uses the AVOA for feature selection to reduce network traffic dimensionality. The selected features are then used to train a LSTM neural network, enabling accurate attack detection. Evaluations show that the proposed method outperforms deep learning models like CNN and RNN, as well as feature selection algorithms such as WOA, HHO, and GWO, in terms of accuracy.
A key strength of the proposed method lies in its use of swarm intelligence, which enables parallel searching for optimal feature vectors. Parameters like population size and iteration count are carefully tuned to balance accuracy and computational efficiency. Future work could explore integrating majority voting mechanisms for attack detection in SDN switches and employing advanced neural networks like GRU and CNN to further enhance detection capabilities. This approach demonstrates the importance of combining data balancing, intelligent feature selection, and distributed architectures for robust IoT security.

6. Acknowledgement

The authors express their gratitude to the esteemed reviewers and all those who assisted in the execution of this research.

References

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

[2] H. Kareemullah, D. Najumnissa, M. M. Shajahan, M. Abhineshjayram, V. Mohan and S. A. Sheerin, "Robotic Arm controlled using IoT application," *Computers and Electrical Engineering*., vol. 105, p. 108539, Jun. 2023, doi: 10.1016/j.compeleceng.2022.108539.

[3] O. E. Tayfour, A. Mubarakali, A. E. Tayfour, M. N. Marsono, E. Hassan and A. M. Abdelrahman, "Adapting deep learning-LSTM method using optimized dataset in SDN controller for secure IoT," *Soft Computing*., pp. 1-9, Mar. 2023, doi: 10.1007/s00500-023-08348-w.

[4] K. P. Reddy, K. R. Raju, K. C. Mouli and M. Praveen, "An intelligent network intrusion detection system for anomaly analyzer using machine learning for software defined networks," *In AIP Conference Proceedings*, vol. 2548, no. 1, July 2023, doi: 10.1063/5.0118479.

[5] R. J. Gohari, L. Aliahmadipour and M. K. Rafsanjani, "Deep learning-based intrusion detection systems: A comprehensive survey of four main fields of cyber security," *Journal of Mahani Mathematical Research Center*, vol. 12, no. 2, pp. 289-324, May. 2023, doi: 10.22103/jmmr.2022.19961.1305.

[6] A. Javadpour, P. Pinto, F. Ja'fari and W. Zhang, "DMAIDPS: a distributed multi-agent intrusion detection and prevention system for cloud IoT environments," *Cluster Computing*, vol. 26, no. 1, pp. 367-384, May. 2022, doi: 10.1007/s10586-022-03621-3.

[7] S. Javanmardi, M. Shojafar, R. Mohammadi, M. Alazab and A. M. Caruso, "An SDN perspective IoT-Fog security: A survey," *Computer Networks*, vol. 229, p. 109732, June. 2023, doi: 10.1016/j.comnet.2023.109732.

[8] O. Habibi, M. Chemmakha, and M. Lazaar, "Imbalanced tabular data modelization using CTGAN and machine learning to improve IoT Botnet attacks detection," *Engineering Applications of Artificial Intelligence*, vol. 118, p. 105669, Feb. 2023, doi: 10.1016/j.engappai.2022.105669.

[9] B. Abdollahzadeh, F. S. Gharehchopogh and S. Mirjalili, "African vultures optimization algorithm: A new nature-inspired metaheuristic algorithm for global optimization problems," *Computers & Industrial Engineering*, vol. 158, p. 107408, 2021, doi: 10.1016/j.cie.2021.107408.

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

Declaration of Competing Interest: Authors do not have a conflict of interest. The content of the paper is approved by the authors.

Author Contributions: All authors reviewed the manuscript.

E-ISSN: 2980-9231
https://sanad.iau.ir/journal/jce

مهندسی مخابرات جنوب
دانشگاه آزاد اسلامی واحد بوشهر

https://doi.org/10.30495/jce.2023.1998267.1233

مقاله پژوهشی

شناسایی حملات DDoS در سوئیچ‌های SDN با رویکرد یادگیری عمیق و هوش گروهی

محسن اقبالی[1] | محمّدرضا ملاخلیلی میبدی*[2]

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

[2]گروه مهندسی کامپیوتر، واحد میبد، دانشگاه آزاد اسلامی، میبد، ایران.
mollakhalili@maybodiau.ac.ir

نویسنده مسئول:
*محمّدرضا ملاخلیلی میبدی، استادیار گروه مهندسی کامپیوتر، واحد میبد، دانشگاه آزاد اسلامی، میبد، ایران.
mollakhalili@maybodiau.ac.ir

موضوع اصلی:
اینترنت اشیا

تاریخچه مقاله:
تاریخ دریافت: ۲۴ مهر ۱۴۰۲
تاریخ بازنگری: ۱۱ آذر ۱۴۰۲
تاریخ پذیرش: ۲۶ آذر ۱۴۰۲

چکیده:

در این مقاله، یک سیستم کارآمد تشخیص نفوذ برای اینترنت اشیا (IoT) ارائه شده است که به چالش گره‌های IoT آلوده به بدافزارهای مختلف و تبدیل شدن هر دستگاه هوشمند به گره حمله‌کننده باتنت می‌پردازد. همچنین، مسائل موجود در سیستم‌های تشخیص نفوذ فعلی، مانند انتخاب ویژگی‌های هوشمند، عدم تعادل مجموعه داده‌های آموزشی و تمرکزگرایی را نیز مد نظر قرار می‌دهد. سیستم پیشنهادی از معماری توزیع‌شده شبکه‌های نرم‌افزارمحور (SDN) بهره می‌برد. روش پیشنهادی با متعادل‌سازی مجموعه داده‌ها با استفاده از تکنیک SMOTE آغاز می‌شود. سپس، ویژگی‌های اساسی با استفاده از الگوریتم بهینه‌سازی کرکس آفریقایی انتخاب می‌شوند. در مرحله بعد، یک مدل یادگیری عمیق LSTM در کنترلر SDN آموزش داده می‌شود. سوئیچ‌های SDN از این مدل آموزش‌دیده برای تشخیص حملات استفاده می‌کنند. برای بهبود مقابله با حملات، آدرس‌های گره‌های حمله‌کننده بین سوئیچ‌های SDN به اشتراک گذاشته می‌شوند، که تشخیص سازگار را تضمین کرده و امکان جلوگیری موثر از حملات منع سرویس توزیع‌شده (DDoS) را در سراسر شبکه فراهم می‌کند. نتایج تجربی به دست آمده در MATLAB، با استفاده از مجموعه داده NSL-KDD، اثربخشی روش پیشنهادی را نشان می‌دهد و دقت ۹۹.۳۴٪، حساسیت ۹۹.۱۶٪ و دقت ۹۸.۹۳٪ را در تشخیص حملات به دست می‌آورد. روش پیشنهادی عملکرد بهتری نسبت به روش‌های انتخاب ویژگی مبتنی بر الگوریتم‌های WOA، HHO و AO، و روش‌های یادگیری عمیق مانند LSTM، RNN و CNN، به ویژه در تشخیص حملات DDoS، دارد.

کلید واژه‌ها: اینترنت اشیاء، سیستم تشخیص نفوذ، حملات DDoS، شبکه SDN، یادگیری عمیق.

تازه های تحقیق:

- ارایه یک سیستم تشخیص نفوذ توزیع شده در بستر معماریSDN
- متعادل‌سازی مجموعه داده با استفاده از روش SMOTE در کنترلر کننده‌SDN
- ارایه یک نسخه انتخاب ویژگی و باینری از الگوریتم کرکس آفریقایی در تشخیص حملات
- تلفیق هوش گروهی و یادگیری عمیق LSTM در شبکه SDN برای تشخیص حملات در اینترنت اشیاء

۱-مقدمه

فناوری اینترنت اشیاء[1] به حدی پیشرفت کرده است که بسیاری از افراد در زندگی روزمره به شکلی از دستگاه‌های هوشمند استفاده می‌کنند و یا با آن‌ها تعامل دارند. از مزایای اینترنت اشیاء می‌توان به خودکارسازی، بهبود بهره‌وری و استفاده مؤثر از منابع و موارد دیگر اشاره کرد [۱]. تعداد دستگاه‌های فیزیکی با قابلیت ارتباط از راه دور و حسگر متصل به اینترنت در چند سال گذشته افزایش‌یافته است. الگوی رشد اتصال به اینترنت دستگاه IoT نقطه اوج پیشرفت تحقیقات در ارتباطات بی‌سیم، محاسبات ابری و تجزیه‌وتحلیل داده‌ها در سال‌های اخیر و همچنین تعداد برنامه‌هایی است که اینترنت اشیاء ارائه می‌دهد، ازجمله خانه‌های هوشمند، مراقبت‌های بهداشتی هوشمند، سامانه‌های حمل‌ونقل هوشمند، شبکه هوشمند و بسیاری دیگر [۲]. بااین‌وجود، امنیت و حریم خصوصی ارائه‌شده توسط اینترنت اشیاء همچنان یک نگرانی است، زیرا این دستگاه‌ها بیشتر در معرض حملات امنیتی و آسیب‌پذیری هستند و دشمنان دائماً به دنبال راه‌های جدیدی برای به خطر انداختن دستگاه‌های ناامن و آسیب‌پذیر بازشده عمومی هستند. علاوه بر این، دستگاه‌های اینترنت اشیاء از طریق اینترنت به سرویس‌های ابری متصل می‌شوند تا به‌روزرسانی‌ها را ارسال کنند و پیشنهادها یا توصیه‌هایی را برای انجام اقدامات هوشمندانه از طرف کاربران دستگاه اینترنت اشیا دریافت کنند، بنابراین، وجود دستگاه‌های اینترنت اشیا پیچیدگی بیشتری به مدیریت و نگهداری شبکه‌ها می‌افزاید و باعث ایجاد نسل جدیدی از شبکه‌های هوشمند شده است [۱ و ۲].

اخیراً خطر حملات سایبری به دلیل آسیب‌پذیری‌هایی در برخی دستگاه‌های متصل به اینترنت که اغلب آن‌ها را به اهداف آسانی تبدیل می‌کند، افزایش‌یافته است. امروزه حملات زیادی علیه اینترنت اشیاء انجام می‌شود که نمونه آن حملات رد سرویس خدمات توزیع‌شده[2] است. در این حملات تعدادی زیادی گره در اینترنت اشیاء به بدافزار[3] آلوده می‌شود و هرکدام از آن‌ها تبدیل به یک بات نت[4] می‌شود. حجم حملات به شبکه اینترنت اشیاء در سال‌های اخیر افزایش‌یافته است و این حملات کاربران و سرویس‌های شبکه را تهدید می‌کنند [۳]. حملات انکار سرویس یکی از محبوب‌ترین و تهدیدکننده‌ترین حملات به امنیت شبکه است. این تهدید در نقض در دسترس بودن سرویس‌های شبکه با ممانعت از دسترسی کاربران مجاز به خدمات هدف نشان داده می‌شود. برخلاف حملات DoS که از یک منبع راه‌اندازی می‌شوند، حملات DDoS به شیوه‌ای توزیع‌شده از چندین منبع راه‌اندازی می‌شوند. مهاجمان یک حمله DDoS را انجام می‌دهند تا هدف را با سیل بی‌امان ترافیک مغلوب کنند که منجر به مصرف توان محاسباتی و همچنین ظرفیت شبکه پیوندهای شبکه می‌شود. اولین حمله DDoS در اوت ۱۹۹۹ در شبکه کامپیوتری دانشگاه مینه‌سوتا انجام شد. مهاجم توانست کامپیوترهای شبکه را برای حدود دو روز خاموش کند. در فوریه ۲۰۰۰، وب‌سایت‌های معروفی مانند eBay، Yahoo، Buy و Amazon موردحمله DDoS قرار گرفتند. پس‌ازآن، حملات DDoS ازنظر فرکانس به رشد خود ادامه دادند و امروزه از دستگاه‌های IoT استفاده می‌کنند و روش‌های پیچیده جدیدی را برای فراگیرشدن اتخاذ می‌کنند [۴].

طبق گزارش‌های سازمان‌های امنیت شبکه در سال ۲۰۲۲، حملات DDoS به‌طورکلی نسبت به سال قبل افزایش‌یافته است. حملات لایه برنامه نظیر HTTP DDoS و Ransom DDoS در سال ۲۰۲۲ نسبت به سال قبل به ترتیب ۱۱۱ درصد و ۶۷ درصد افزایش‌یافته است. حملات لایه شبکه در سال ۲۰۲۲ نسبت به سال قبل ۹۷ درصد و در سه‌ماهه سوم نسبت به یک چهارم مشابه سال قبل ۲۴ درصد افزایش‌یافته است [۵]. از زمان ظهور حملات DDoS، جامعه تحقیقاتی با این تهدید از طریق چندین تکنیک شناسایی، ازجمله: طرح ردیابی، سیستم خودکار فیلتر ترافیک، تشخیص مبتنی بر امضاء[5] و تشخیص مبتنی بر ناهنجاری[6] با این تهدید مقابله کرده‌اند [۶].

---

[1] Internet of Things (IoT)
[2] Distributed denial-of-service (DDoS)
[3] Malware
[4] Botnet
[1] Signature-based detection
[6] Anomaly-based detection

طرح ردیابی متکی بر یافتن مکان‌های منابع حمله است، درحالی‌که یک سیستم فیلتر ترافیک، مستقل از فیلتر ترافیک برای جداسازی ترافیکی استفاده می‌کند که مبدأ یا مقصد شبکه نیست. طرح تشخیص مبتنی بر امضا، پایگاه داده خود را از تهدیدات مخرب شناخته‌شده ایجاد می‌کند و ترافیک جدید را با آن پایگاه داده مقایسه می‌کند تا فعالیت‌های مخرب را شناسایی کند، درحالی‌که طرح تشخیص مبتنی بر ناهنجاری، رفتار شبکه را برای تشخیص فعالیت‌های مخرب از ترافیک عادی بر اساس یک آموزش نظارت می‌کند. در بیشتر مطالعات از روش‌های یادگیری ماشین[۱] و یادگیری عمیق[۲] برای توسعه سیستم‌های تشخیص نفوذ بر اساس ناهنجاری ترافیک شبکه استفاده می‌شود [۳].

یادگیری ماشین و یادگیری عمیق می‌تواند برای تشخیص نفوذ در ترافیک شبکه به‌عنوان یکی از مؤثرترین تکنیک‌های تشخیص استفاده شود. به‌طور خاص، یادگیری عمیق در سال‌های اخیر عملکرد بسیار خوبی در تشخیص حملات از خود نشان داده است. ازآنجایی‌که داده‌های واقعی غیرخطی، پیچیده و بسیار ابعادی هستند، ساخت مدل‌های یادگیری عمیق چندین نورون پنهان دارد و هر نورون یک تابع غیرخطی دارد. ساختار پیچیده مدل‌های یادگیری عمیق باعث می‌شود آن‌ها را در درک بهتر داده‌های پیچیده و غیرخطی در حوزه هدف بهتر کنند [۷]. یکی از چالش‌های مهم سامانه‌های تشخیص نفوذ به شبکه ساختار متمرکز سیستم تشخیص نفوذ است و اگر سیستم تشخیص نفوذ متمرکز ارائه شود چالش‌هایی برای آن وجود دارد که مهم‌ترین آن‌ها زمان زیاد برای تشخیص حملات در حجم بالایی از ترافیک است. عدم تمرکز در سیستم‌های تشخیص نفوذ باعث تقسیم‌کاری و بهبود زمان تشخیص حملات می‌شود. عدم تمرکز در سیستم‌های تشخیص نفوذ باعث می‌شود اگر یک سیستم تشخیص نفوذ مورد حمله واقع شود آنگاه سایر سیستم‌های تشخیص نفوذ می‌توانند حملات را تشخیص دهند[۸].

قابلیت مدیریت منابع شبکه متمرکز از مزایای شبکه‌های نرم‌افزار محور[۳] است که می‌توان از این معماری توزیع‌شده برای تشخیص حملات استفاده نمود. منابع شبکه را می‌توان به کمک این فناوری مدیریت کرد و ترافیک شبکه را می‌توان با استفاده از کنترلر شبکه‌های نرم‌افزار محور برای بهبود امنیت کنترل کرد [۹]. امروزه، شبکه‌های نرم‌افزار محور به‌خوبی برای پردازش نه‌تنها ترافیک شبکه پروتکل قدیمی بلکه دستگاه‌های اینترنت اشیاء که ترافیک شبکه را با پروتکل OpenFlow و برنامه‌های کنترل‌کننده شبکه‌های نرم‌افزار محور سفارشی‌شده تولید می‌کنند، مجهز است. اگرچه شبکه‌های نرم‌افزار محور می‌تواند برای مدیریت مسیریابی، مدیریت منابع، نظارت و مدیریت ترافیک، تشخیص امنیت و کاهش در محیط‌های اینترنت اشیاء استفاده شود، شبکه‌های نرم‌افزار محور نیز به دلیل وجود دستگاه‌های اینترنت اشیاء مستعد حملات جدید نظیر بات نت‌ها است. به‌عنوان‌مثال، دستگاه‌های اینترنت اشیاء پیکربندی‌شده پیش‌فرض با استفاده از بدافزار بات نت میرا[۴] در معرض خطر قرار می‌گیرند و ارتباطات فرمان و کنترل را با سرور مهاجم راه دور برای تبدیل‌شدن به بخشی از ارتش ربات آغاز می‌کنند. این ربات‌ها در معرض خطر را می‌توان برای ایجاد ترافیک شبکه مخرب و سیل کنترل‌کننده شبکه‌های نرم‌افزار محور استفاده کرد. منابع کنترل‌کننده یا اشباع منابع شبکه می‌تواند منجر به خاموش شدن کل شبکه با حملات انکار سرویس توزیع‌شده یا DDoS شود [۱۰]. احتمالات متعدد دیگری برای حمله وجود دارد، مسمومیت توپولوژی[۵] [۱۱]، به خطر انداختن کنترلر یا سوئیچ‌ها با آسیب‌پذیری‌های شناخته‌شده [۱۲]، یا حملات روز صفر[۶] [۱۳] ازجمله آن‌ها است. هدف از سیستم تشخیص نفوذ کارآمد، تشخیص با نرخ خطای اندک و زمان کم برای تشخیص حملات است اما برای تشخیص حملات DDoS در اینترنت اشیاء چالش‌های وجود دارد که ازجمله آن‌ها می‌توان به موارد ذیل اشاره نمود:

- سیستم‌های تشخیص نفوذ اگر روی مجموعه داده نامتعادل آموزش داده شوند دارای دقت اندکی خواهند بود و ازاین‌جهت بهتر است که کلاس‌های اقلیت در مجموعه داده با روش‌های متعادل‌سازی افزایش داده شوند.
- معماری متمرکز برای تشخیص حملات توانایی تحلیل حجم ترافیک اینترنت اشیاء را ندارد و ازاین‌جهت بهتر است برای شبکه اینترنت اشیاء معماری‌های توزیع‌شده تشخیص نفوذ توسعه داده شود.

---

[1] Machine learning
[2] Deep learning
[3] Software-defined networking (SDN)
[4] Mirai
[5] Topology poisoning
[6] Zero-day attacks

- حجم و تعداد ویژگی‌های ترافیک شبکه اینترنت اشیاء قابل‌توجه است و در این میان فقط برخی از ویژگی‌های ترافیک شبکه اهمیت بیشتری دارند؛ لذا توسعه سیستم‌های تشخیص نفوذ با انتخاب ویژگی هوشمندانه دارای اهمیت بالایی است.

برای رفع چالش‌های فوق در این مقاله یک سیستم تشخیص نفوذ توزیع‌شده در بستر معماری شبکه‌های نرم‌افزار محور ارائه می‌شود. در مرحله اول ترافیک شبکه در کنترلر شبکه نرم‌افزار محور با روش SMOTE[1] متعادل‌سازی می‌شود [۱۴]. در مرحله دوم از الگوریتم بهینه‌سازی کرکس آفریقایی[2] که اخیراً ارائه‌شده است برای انتخاب ویژگی استفاده می‌شود [۱۵]. مزیت این الگوریتم هوش گروهی دقت بالا و مدل‌سازی پیچیده برای یافتن جواب‌های بهینه در فضاهای چندبعدی و پیچیده است. در مرحله سوم کنترل‌کننده بر اساس یادگیری عمیق LSTM یک مدل طبقه‌بندی ایجاد می‌کند و این مدل آموزش‌یافته به همراه بردار ویژگی بهینه را برای سوئیچ‌های شبکه نرم‌افزار محور ارسال می‌کند تا ترافیک حملات DDoS را شناسایی نمایند. هدف اصلی این مقاله ارائه یک سیستم تشخیص نفوذ کارآمد در بستر معماری شبکه نرم‌افزار محور و تشخیص دقیق و سریع حملات به اینترنت اشیاء است. سهم نویسندگان از این تحقیق شامل موارد ذیل است:

- ارائه یک سیستم تشخیص نفوذ توزیع‌شده در بستر معماری SDN
- متعادل‌سازی مجموعه داده با استفاده از روش SMOTE در کنترلر کننده SDN
- ارائه یک نسخه انتخاب ویژگی و باینری از الگوریتم کرکس آفریقایی در تشخیص حملات
- تلفیق هوش گروهی و یادگیری عمیق LSTM در شبکه SDN برای تشخیص حملات در اینترنت اشیاء

این مقاله در چند بخش تهیه و نگارش شده است. در بخش II کارهای مرتبط در زمینه‌ی تشخیص حملات DDoS مرور شده است. در بخش III، سیستم تشخیص نفوذ پیشنهادی در معماری SDN با الگوریتم بهینه‌سازی کرکس آفریقایی و یادگیری عمیق LSTM توسعه داده‌شده است. در بخش IV، روش پیشنهادی پیاده‌سازی و تحلیل می‌شود و با روش‌های مشابه مقایسه می‌شود. در بخش آخر یا V نتایج تحقیق و یافته‌های تحقیق به همراه پیشنهادهای آتی ارائه می‌گردد.

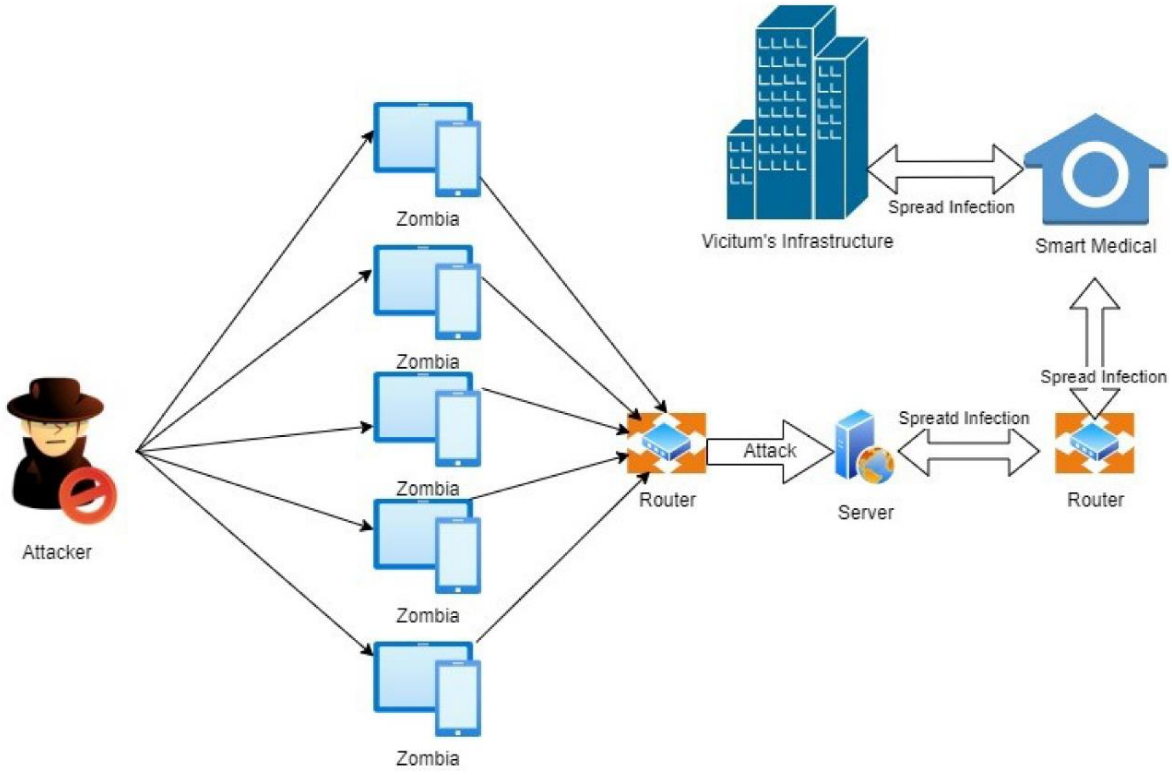
۲-کارهای مرتبط

یک حمله انکار سرویس یک دستگاه یا شبکه را بیش‌ازحد بارگذاری می‌کند و آن را غیرقابل دسترسی می‌کند. مهاجمان این کار را با ارسال ترافیکی بیشتر از میزان توانایی هدف انجام می‌دهند که باعث شکست آن و ناتوانی در ارائه خدمات به کاربران عادی خود می‌شود. یک شبکه به‌هم‌پیوسته و توزیع‌شده از ماشین‌ها باعث حمله DDoS می‌شود که می‌تواند شامل اینترنت اشیاء باشد و می‌تواند تحت تأثیر بدافزارهایی باشد که از راه دور کنترل می‌شوند. یک بات نت می‌تواند مستقیماً به هر ربات حمله کند و دستورالعمل‌ها را از راه دور ارسال کند. در یک بات نت، شبکه آسیب‌دیده یا سرور، هر ربات درخواستی را به یک آدرس IP مشخص ارسال می‌کند و باعث ایجاد یک DoS به ترافیک عادی می‌شود. جدا کردن ترافیک عادی از ترافیک مهاجم چالش‌برانگیز است. نمونه‌های رایج حملات DDOS عبارت‌اند از سیل UDP، سیلاب SYN و تقویت DNS است. امروزه حملات DDoS بسیار کوتاه اتفاق می‌افتد. گزارش‌های نشان می‌دهد که میانگین مدت حمله DDoS در سال ۲۰۲۲ بین ۵ تا ۱۰ ثانیه و ظرفیت آن‌ها در بیشتر موارد ۵ گیگا بیت در ثانیه در ۲۴ ساعت است [۱۶].

با رشد سریع اینترنت اشیاء، بات نت می‌تواند به‌راحتی مقیاس‌های گسترده‌تری از حملات را با استفاده از دستگاه‌های اینترنت اشیاء انجام دهد. ربات مخرب دستگاهی است که آلوده‌شده است و آن دستگاه می‌تواند یک دستگاه اینترنت اشیاء باشد. ربات‌های آلوده گاهی به هم متصل می‌شوند و بات نت‌هایی را تشکیل می‌دهند. سپس این بات نت‌ها فعالیت‌هایی مانند حملات DDoS را انجام می‌دهند. حمله DDoS شکلی از حمله است که در آن ترافیک مخرب هدف یا زیرساخت مرتبط را بارگذاری می‌کند. این امر با استقرار ربات‌ها، شبکه‌ای از رایانه‌های آلوده به بدافزار و سایر دستگاه‌های معروف به زامبی‌ها[3] به دست می‌آید که مهاجم ممکن است از راه دور آن‌ها را مدیریت کند، همان‌طور که در شکل ۱، نشان داده‌شده است [۱۷].

---

[1] Synthetic Minority Over-sampling Technique (SMOTE)
[2] African Vultures Optimization Algorithm (AVOA)
[3] Zombies

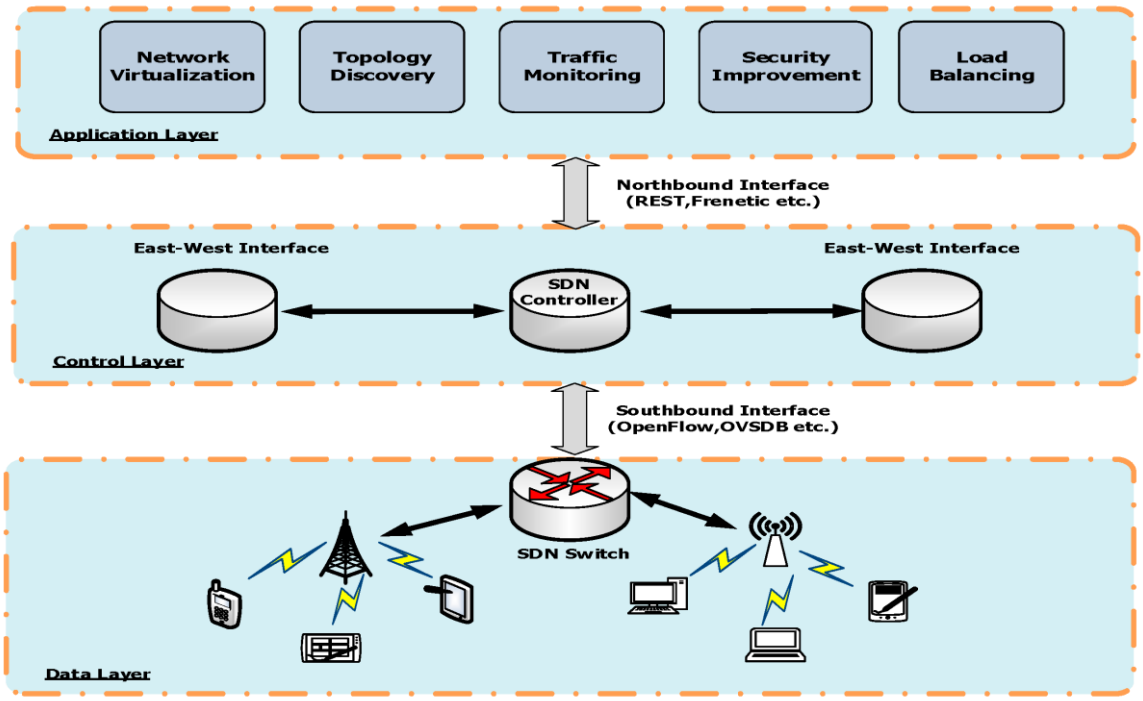


شکل ۱: مکانیزم وقوع حملات DDoS علیه سرویس‌های شبکه[۱۷]

Figure 1. The mechanism of DDoS attacks against network services [17]

حملات رد سرویس خدمات توزیع‌شده به طور قابل‌توجهی پهنای باند و اتصال را محدود می‌کند و باعث ازکارافتادن تمام خدمات شبکه می‌شود. اکوسیستم‌های ابری بیشترین ضرر را به دلیل انکار خدمات و تخریب متحمل می‌شوند. هدف اصلی آسیب رساندن به دسترسی به منابع برای کاربران قانونی است. شناسایی ترافیک حمله در یک حمله DDoS به دلیل شباهت آن به ترافیک عادی دشوار است، زیرا آن‌ها مانند بسته‌های شبکه معمولی رفتار می‌کنند [۱۷]. یک معماری کاربردی برای ارائه سیستم‌های تشخیص نفوذ، معماری SDN است. مزیت حالت توزیع‌شده این معماری، در صورتی که سیستم تشخیص نفوذ در آن مستقر شود از نوع توزیع‌شده خواهد بود. SDN فناوری جدیدی است که مدیریت شبکه را با ساختار پویا و قابل‌برنامه‌ریزی خود تسهیل می‌کند. در SDN صفحات کنترل و داده از یکدیگر تقسیم می‌شوند و مدیریت شبکه توسط یک کنترل‌کننده مرکزی انجام می‌شود و بنابراین کنترل‌کننده‌ای که می‌تواند کل شبکه را از یک نقطه مدیریت کند، می‌تواند به‌سرعت سیاست‌های مختلف شبکه را در کل شبکه اعمال کند. شکل ۲، ساختار لایه‌ای محیط SDN را نشان می‌دهد.

با این‌حال، این رویکرد جدید در حال ظهور علاوه بر مزایایی که ارائه می‌دهد، مشکلات امنیتی را نیز به همراه دارد. علاوه بر حملاتی که در ساختارهای شبکه سنتی با آن مواجه می‌شوند، SDN نیز در معرض حملات خاص خود قرار دارد. شاید خطرناک‌ترین این حملات، حملات به کنترلر باشد، زیرا مهاجمی که کنترلر را تصاحب می‌کند، می‌تواند توانایی مدیریت یا اختلال در تمام ترافیک شبکه را داشته باشد. حملات DDoS که در آن کاربران از دسترسی به خدمات شبکه محروم می‌شوند، در رأس حملات به کنترل‌کننده قرار دارند. در ادامه این بخش تعدادی از کارهای مرتبط در زمینه‌ی تشخیص نفوذ در اینترنت اشیاء و با رویکرد شبکه SDN مرور می‌شود.



شکل ۲: معماری SDN و لایه‌های آن[۱۸]
Figure 2. SDN architecture and its layers [18]

در [۱۹] یک رویکرد پیش‌بینی و تشخیص حملات DDoS در محاسبات لبه با یادگیری عمیق در شبکه SDN را پیشنهاد دادند. آن‌ها یک چارچوب جدید به نام CoWatch برای پیش‌بینی و تشخیص مشترک حملات DDoS در سناریوهای محاسبات لبه پیشنهاد دادند. آن‌ها مدل LSTM را برای طراحی الگوریتمی برای پیش‌بینی مشترک و تشخیص حملات DDoS بررسی و ایجاد کردند. نتایج آزمایش بر روی تعدادی از مجموعه داده‌ها عملکرد امیدوارکننده CoWatch را در اثربخشی و کارایی نشان می‌دهد. در [۲۰] چارچوب امن SDN-IoT برای تشخیص حملات DDoS با استفاده از یادگیری عمیق را پیشنهاد دادند. چارچوب پیشنهادی از مجموعه داده CICDDoS2019 برای شناسایی حملات بازتابی و حملات بهره‌برداری در TCP، UDP و ICMP آزمایش می‌شود. نتایج تجربی نشان می‌دهد که چارچوب پیشنهادی می‌تواند به‌طور مؤثر حملات DDoS را شناسایی و کاهش دهد درحالی‌که از منابع CPU به‌طور مؤثر و در زمان کوتاه‌تری در مقایسه با رویکردهای موجود استفاده می‌کند. در [۲۱] برای تشخیص حملات DDoS یک روش یادگیری گروهی در جریان داده برای دستگاه‌های سنجش هوشمند IoT ارائه دادند. روش آن‌ها می‌توانند مجموعه داده‌های غیر سلسله‌مراتبی و نامتعادل مشابه حملات Mirai را مدیریت و شناسایی کنند. در [۲۲] تشخیص حملات DDoS ناشناخته در شبکه‌های اینترنت اشیاء با استفاده از یک مدل یادگیری ترکیبی را پیشنهاد دادند. آن‌ها یک رویکرد جدید را پیشنهاد دادند که یک مدل شبکه عصبی کانولوشنال مرتب‌سازی نرم را با ضریب پرت محلی و تشخیص ناهنجاری مبتنی بر جداسازی با استفاده از مدل‌های گروه‌های نزدیک‌ترین همسایه که از روش‌های یادگیری نظارت‌شده و بدون نظارت استفاده می‌کنند، ترکیب می‌کند. ارزیابی‌ها نشان داد دقت روش آن‌ها در تشخیص حملات می‌تواند تا ۹۸/۹۴ درصد افزایش یابد و حملات ناشناخته را تشخیص دهد. در [۲۳] یک شبکه عصبی همبستگی برای تشخیص حمله DDoS در سیستم اینترنت اشیاء ارائه دادند. آن‌ها به‌طور گسترده معماری‌های پیشنهادی را با ارزیابی پنج مدل شبکه عصبی مختلف که بر روی مجموعه داده‌ای که از یک سیستم اینترنت اشیاء دارای ۴۰۶۰ گره در دنیای واقعی آموزش دادند. آزمایش‌ها نشان دادند حافظه کوتاه‌مدت و یک مدل مبتنی بر ترانسفورماتور، در ارتباط با معماری‌هایی که از اطلاعات همبستگی گره‌های اینترنت اشیا استفاده می‌کنند، عملکرد بالاتری نسبت به مدل‌های دیگر ارائه می‌کنند. در [۲۴] تشخیص مبتنی بر تغییرات آنتروپی در حملات DDoS بررسی‌شده است. هدف آن‌ها دستیابی به شناسایی حملات DDoS با روش تشخیص مبتنی بر قانون با استفاده از معیارهای

تئوری اطلاعات است. تغییر در آنتروپی ویژگی‌های ترافیک فراتر از یک آستانه، نشانگر تغییر در تراکم ترافیک به یک شبکه است. در این مقاله، ما یک تحلیل عملکرد از پارامترهای مختلف مرتبط با تشخیص حملات DDoS مبتنی بر تغییرات آنتروپی ارائه می‌شود. در [۲۵] یک رویکرد طبقه‌بندی تعبیه‌شده برای تشخیص حملات DDoS مبتنی بر ترافیک اینترنت اشیاء ارائه‌شده است. عملکرد مدل آن‌ها با اجرای چهار سناریو مختلف مبتنی بر ترافیک اینترنت اشیاء ارزیابی می‌شود. در این پژوهش مجموعه داده Bot-IoT در دسترس عموم برای طراحی و اعتبارسنجی رویکرد طبقه‌بندی چند کلاسه پیشنهادی استفاده می‌شود. نتایج نشان می‌دهد که رویکرد پیشنهادی ۸۴/۴ درصد نرخ کاهش ویژگی و تقریباً ۵/۱۹ درصد دقت طبقه‌بندی بالاتر از رویکردهای موجود ارائه می‌کند. در [۲۶] یک روش انتخاب ویژگی برای تشخیص حمله رد سرویس خدمات توزیع‌شده با استفاده از تکنیک‌های یادگیری ماشین ارائه دادند. در این پژوهش ویژگی‌های مهم دو مجموعه داده NF_ToN_IoT و NF_BoT_IoT با دو روش انتخاب ویژگی Information Gain و Gain Ratio انتخاب می‌شوند و با استفاده از الگوریتم Ranker رتبه‌بندی می‌شوند. سپس این مجموعه داده‌ها با استفاده از چهار الگوریتم مختلف مانند شبکه باور[1]، نزدیک‌ترین همسایه، جدول تصمیم‌گیری و جنگل تصادفی آزمایش می‌شوند. آزمایش‌ها نشان داد بهترین طبقه‌بندی کلی شبکه بیزین با دقت ۹۷/۵۰۶ درصد و ۹۰/۶۷ درصد برای هر دو مجموعه داده NF_ToN_IoT و NF_BoT_IoT است. در[۲۷] یک روش شناسایی حملات DDoS در دستگاه‌های IoT توسط Bi-LSTM-CNN ارائه دادند. این مقاله یک حافظه کوتاه‌مدت دوسویه مبتنی بر توجه ترکیبی با شبکه‌های عصبی کانولوشن برای شناسایی حملات DDoS در لایه برنامه و SDN پیشنهاد می‌کند. آن‌ها چندین مدل یادگیری ماشین دیگر مانند رگرسیون لجستیک[2]، درخت‌های تصمیم[3]، جنگل‌ها تصادفی[4]، ماشین‌های بردار پشتیبان[5]، نزدیک‌ترین همسایگان[6]، تقویت گرادیان شدید[7]، شبکه‌های عصبی مصنوعی[8]، CNN، LSTM، CNN-LSTM را برای ارزیابی عملکرد مدل پیشنهادی خود به کار گرفتند. تجزیه‌وتحلیل تجربی روی مجموعه داده‌های چندگانه نشان می‌دهد که مدل پیشنهادی طبقه‌بندی را به‌طور مؤثر با دقت ۹۹/۷۴ درصد انجام می‌دهد.

۳-روش پیشنهادی

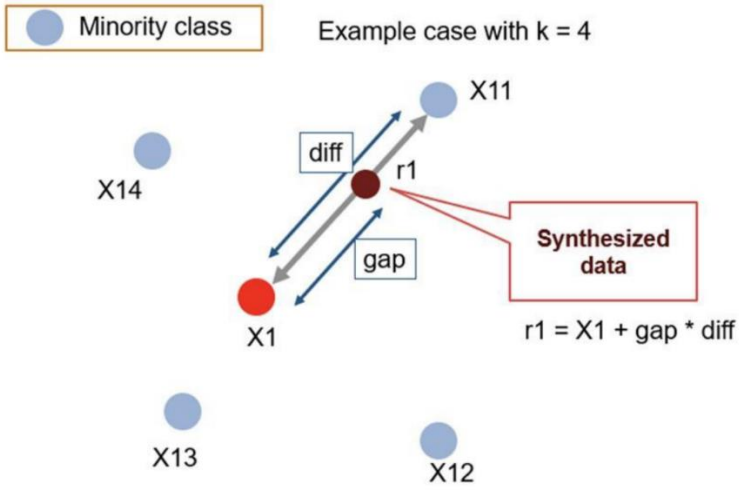
روش پیشنهادی برای تشخیص حملات به شبکه از معماری توزیع‌شده در سوئیچ‌های SDN استفاده می‌شود و روش پیشنهادی دارای اجزای ذیل است:

- کنترل‌کننده در ابتدا ترافیک شبکه را دریافت نموده و با روش SMOTE آن را متعادل‌سازی می‌کند.
- کنترل‌کننده با استفاده از الگوریتم بهینه‌سازی کرکس آفریقایی می‌تواند ویژگی‌های مهم ترافیک شبکه را تشخیص دهد و آن را برای کاهش ابعاد ترافیک شبکه استفاده نماید.
- کنترل‌کننده می‌تواند روش یادگیری عمیق مانند LSTM را آموزش دهد و این مدل آموزش‌یافته را برای سوئیچ-های SDN ارسال کند.
- کنترلر کننده بردار ویژگی بهینه و مدل آموزش‌یافته LSTM را برای سوئیچ‌های SDN ارسال می‌کند و هر سوئیچ می‌تواند بر اساس الگوی بردار ویژگی و مدل آموزش‌یافته LSTM اقدام به تشخیص نفوذ نماید.
- سوئیچ‌های SDN می‌توانند IP های مخرب گره‌های حمله‌کننده را باهم به اشتراک بگذارند.

یک بخش مهم روش پیشنهادی متعادل‌سازی مجموعه داده تشخیص نفوذ است تا مدل‌سازی و دقت یادگیری افزایش داده شود. در روش پیشنهادی برای افزایش تعداد نمونه‌های اقلیت در مجموعه داده از روش SMOTE استفاده می‌شود تا تعداد نمونه‌های حمله که کمتر از تعداد نمونه‌های عادی است افزایش یابد. SMOTE نمونه‌های مصنوعی را برای کلاس اقلیت ایجاد می‌کند تا

[1] Bayesian Network
[2] Logistic regression
[3] Decision trees
[4] Random forest
[5] Support vector machines
[6] Nearest neighbors
[7] Extreme Gradient Boosting
[8] Artificial Neural Networks

مجموعه داده را متعادل کند. این رویکرد می‌تواند مشکل اضافه برازش را به دلیل نمونه‌گیری بیش‌ازحد تصادفی حل کند. ابتدا، SMOTE نمونه‌های داده مصنوعی را با استفاده از روش k-نزدیک‌ترین همسایه ایجاد می‌کند. با انتخاب تصادفی داده‌ها از کلاس اقلیت شروع می‌شود و الگوریتم k نزدیک‌ترین همسایه‌ها را برای داده‌ها تنظیم می‌کند. سپس داده‌های ترکیبی بین داده‌های تصادفی و داده‌های k نزدیک‌ترین همسایگان به‌طور تصادفی انتخاب می‌شوند. شکل ۳، روش کار SMOTE را نشان می‌دهد.



شکل ۳: روش تولید نمونه‌های مصنوعی با SMOTE [۲۸]
Figure 3. The method of producing synthetic samples with SMOTE [28]

بعد از متعادل‌سازی مجموعه داده در کنترل‌کننده با روش SMOTE، در مرحله فاز انتخاب ویژگی با الگوریتم بهینه‌سازی کرکس آفریقایی انجام می‌شود. در این مرحله هر بردار ویژگی یک عضو الگوریتم بهینه‌سازی کرکس آفریقایی است و توسط این الگوریتم بهینه‌ترین بردار ویژگی کشف می‌شود. دلایل استفاده از الگوریتم بهینه‌سازی کرکس آفریقایی در انتخاب ویژگی به شرح ذیل است:

- الگوریتم بهینه‌سازی کرکس آفریقایی در ژورنال Elsevier چاپ‌شده و یک مقاله معتبر در زمینه‌ی هوش گروهی است. این الگوریتم اخیراً ارائه شده است و با توجه به آزمایش‌های نویسندگان، الگوریتم آن‌ها از الگوریتم‌های فرا ابتکاری مطرح نظیر ژنتیک و الگوریتم ذرات دارای خطای کمتری در یافتن جواب بهینه است.
- الگوریتم بهینه‌سازی کرکس آفریقایی دارای مدل‌سازی قوی است و جستجوی سراسری و محلی را هم‌زمان انجام می‌دهد. پیروی راه‌حل‌های مسئله از چند راه‌حل بهینه دریافتن جواب بهینه، باعث شده نوعی سلسله مراتب رهبری دریافتن جواب بهینه در این الگوریتم وجود داشته باشد و از این جهت الگوریتم بسیار رفتار هوشمندانه‌ای دارد.
- اگر یکی از راه‌حل‌ها در نزدیکی بهینه محلی باشد توسط دو راه‌حل شایسته با احتمال زیاد از بهینه محلی دور می‌شود و احتمال همگرایی الگوریتم به بهینه‌های محلی کم است.
- به دلیل مدل‌سازی قابل‌توجه و دقیق الگوریتم بهینه‌سازی کرکس آفریقایی، این الگوریتم برای حل مسائلی با ابعاد بالا مانند انتخاب ویژگی بسیار کارآمد است.

در روش پیشنهادی هر بردار ویژگی یک سطر ماتریس جمعیت الگوریتم کرکس یا AVOA و مطابق رابطه ۱، است.

$$P = \begin{bmatrix} p_{1,1} & \cdots & \cdots & p_{1,j} & p_{1,d-1} & p_{1,d} \\ p_{2,1} & \cdots & \cdots & p_{2,j} & p_{2,d-1} & p_{2,d} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ p_{n-1,1} & \cdots & \cdots & \cdots & p_{n-1,d-1} & p_{n-1,d} \\ p_{n,1} & \cdots & \cdots & p_{n,j} & p_{n,d-1} & p_{n,d} \end{bmatrix} \quad (۱)$$

در این ماتریس جمعیت، هر ستون یک ویژگی مرتبط با تشخیص نفوذ است و در اینجا d ابعاد مسئله یا تعداد ویژگی‌های مجموعه داده است. اگر از مجموعه داده NSL-KDD استفاده شود مقدار d برابر با ۴۱ است. در این رابطه، n تعداد بردارهای ویژگی است. در این ماتریس $p_{i,j}$ نشان‌دهنده بردار ویژگی i و j بردار ویژگی i است. هر بردار ویژگی برای ارزیابی نیاز به یک روش طبقه‌بندی دارد تا مشخص کند بردار ویژگی تا چه اندازه خطا در تشخیص نفوذ دارد. در روش پیشنهادی می‌توان از روش‌های مبتنی بر درخت تصمیم‌گیری برای ارزیابی بردار ویژگی استفاده نمود. باید توجه شود که طبقه‌بندی‌کننده نهایی در این مقاله، روش LSTM است؛ اما در فاز ارزیابی بردارهای ویژگی از درخت تصمیم‌گیری استفاده می‌شود.

هر بردار برای ارزیابی از تابع هدف رابطه ۲، استفاده می‌کند.

$$F(P_i) = \alpha.\mathrm{E} + \beta.\frac{\|P_i\|}{\|d\|} \quad (۲)$$

در تابع هدف E خطای تشخیص حملات به شبکه توسط بردار ویژگی P_i با استفاده از درخت تصمیم‌گیری است و $\|P_i\|$ تعداد ویژگی انتخاب‌شده توسط بردار ویژگی P_iاست. در این رابطه، α و β به ترتیب ضرایب خطای تشخیص نفوذ و کاهش ابعاد مسئله است. در ساخت درخت تصمیم‌گیری با الگوریتم C5.0 نرخ بهره اطلاعات را به‌عنوان استاندارد برای تعیین بهترین متغیر گروه بندی و نقطه تقسیم‌بندی می‌گیرد و اندازه سود و هزینه به دست آوردن اطلاعات را در نظر می‌گیرد. هر چه نرخ به دست آوردن اطلاعات متغیرها بیشتر باشد، بهتر است از آن‌ها به‌عنوان متغیرهای گروه‌بندی استفاده شود. متفاوت از الگوریتمC5.0 ، درخت CARTضریب جینی را به‌عنوان ویژگی تقسیم انتخاب می‌کند و ویژگی را با بزرگ‌ترین ضریب جینی برای تقسیم انتخاب می‌کند. در روش پیشنهادی از درخت تصمیم‌گیری با الگوریتم C5.0 برای ارزیابی بردارهای ویژگی استفاده می‌شود زیرا نرخ بهره اطلاعات در آن بکار رفته که درواقع اهمیت ویژگی‌ها را در خود نهفته دارد. بردارهای ویژگی که این تابع را بیشتر کمینه نمایند به‌عنوان بردار ویژگی بهینه در نظر گرفته می‌شوند. هر کرکس برای انتخاب یک سردسته و حرکت به سمت آن از احتمال رابطه ۳، استفاده می‌کند.

$$p_i = \frac{F_i}{\sum_{i=1}^{n} F_i} \quad (۳)$$

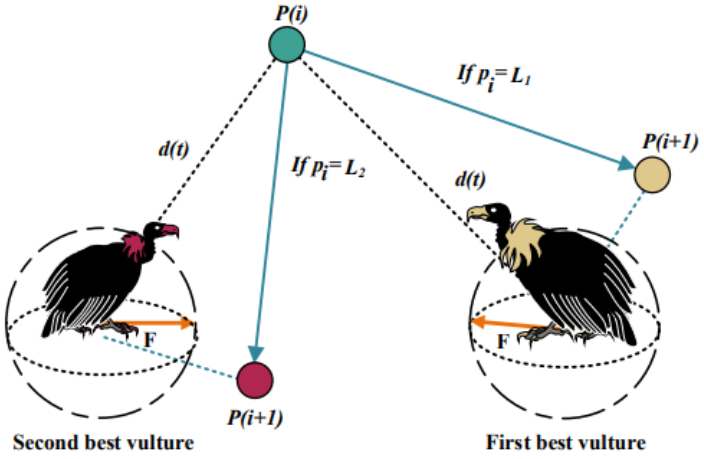
در اینجا F_i شایستگی یک بردار ویژگی یا کرکس معادل آن است و P_i نیز احتمال حرکت یک کرکس به سمت یکی از دو کرکس بهینه است. در شکل ۴ حرکت یک کرکس و انتخاب یکسر دسته و پرواز به سمت آن را نشان می‌دهد.

کرکس‌ها در حین پرواز و جستجو پیرامون دو جواب بهینه می‌توانند گرسنه شوند و برای غذا با سایر کرکس‌ها مبارزه کنند. برای مدل‌سازی رفتار گرسنگی و حمله از رابطه ۴ و ۵ استفاده می‌شود.

$$t = h \times (\sin^{w}\left(\frac{\pi}{2} \times \frac{iter}{Maxlter}\right) + \cos\left(\frac{\pi}{2} \times \frac{iter}{Maxlter} - 1\right)) \quad (۴)$$

$$F = (2 \times rand + 1) \times z \times \left(1 - \frac{iter}{Maxlter}\right) + t \quad (۵)$$

در رابطه ۴ و ۵، iter شمارنده تکرار الگوریتم و Maxlter حداکثر شماره تکرار الگوریتم است. z یک عدد تصادفی یکنواخت در بازه [۱+،۱-] است. h یک عدد تصادفی در بازه [۲+،۲-] است. w یک ضریب وزنی بین ۱ تا ۲ برای تأثیر افزایش میزان گرسنگی و حمله کرکس‌ها است. می‌توان فرض کرد که دو بردار ویژگی در تشخیص نفوذ به ترتیب با $BestVulture_1$ و $BestVulture_2$ نشان داده می‌شود. بر اساس مقدار F می‌توان استراتژی حمله به سمت غذا را تشخیص داد. اگر $|F| > 1$ باشد یک کرکس فقط در آسمان می‌چرخد و سیر است و به دنبال غذا نیست. اگر $|F| \leq 1$ باشد کرکس گرسنه است و دارای رفتاری تهاجمی برای حمله به سمت طعمه است.



شکل ۴: پرواز یک کرکس به سمت یکی از دو کرکس بهینه جمعیت به‌صورت تصادفی
Figure 4. Flight of a vulture towards one of the two optimal population vultures randomly

اگر $|F| > 1$ باشد کرکس‌ها جستجوی اکتشافی را انجام می‌دهند. در این حالت یک عدد تصادفی بین صفر و یک برای یک کرکس در نظر گرفته می‌شود و اگر کوچک‌تر از P_i باشد از رابطه ۶ و ۷ و اگر بیشتر از p1 باشد از رابطه ۸، استفاده می‌شود.

$$P(i+1) = R(i) - D(i) \times F \quad (۶)$$

$$D(i) = |X \times R(i) - P(i)| \quad (۷)$$

در اینجا P(i) موقعیت یک بردار ویژگی و P(i+1) موقعیت جدید همان بردار ویژگی یا کرکس است. X یک ضریب تصادفی بین صفر و دو برای حمله است. R(i) یکی از بردارهای ویژگی $BestVulture_1$ و $BestVulture_2$ است که تصادفی در نظر گرفته می‌شود.

$$P(i+1) = R(i) - F + rand((ub - lb)) \quad (۸)$$

در رابطه ۸، ub و lb به ترتیب محدوده بالا و پایین یک راه‌حل است. اگر $|F| \leq 1$ باشد در این حالت دو وضعیت پیش خواهد آمد در حالت اول اگر $|F| \geq 0/5$ باشد و عدد تصادفی کمتر از p2 باشد از رابطه ۹ برای به‌روزرسانی بردارهای ویژگی استفاده می‌شود و اگر بیشتر از مقدار p2 باشد از رابطه ۹، استفاده می‌شود.

$$P(i+1) = D(i) \times (F + rand) - d(t) \quad (۹)$$

$$d(t) = R(i) - (P(i)) \quad (۱۰)$$

در رابطه ۹ و ۱۰، d(t) فاصله یک بردار ویژگی یا یک کرکس از یکی از دو بردار ویژگی بهینه $BestVulture_1$ یا $BestVulture_2$ است. اگر $|F| \geq 0/5$باشد و عدد تصادفی ایجادشده برای هر کرکس و بردار ویژگی بیشتر از p2 باشد برای به‌روزرسانی بردارهای ویژگی یا راه‌حل‌های مسئله از رابطه ۱۱، ۱۲ و ۱۳ استفاده می‌شود.

$$S_1 = R(i) - (\frac{rand \times P(i)}{2\pi}) \times \cos(P(i)) \quad (۱۱)$$

$$S_2 = R(i) - (\frac{rand \times P(i)}{2\pi}) \times \sin(P(i)) \quad (۱۲)$$

$$P(i+1) = R(i) - (\frac{S_1 + S_2}{2}) \quad (۱۳)$$

اگر مقدار $|F| < 0/5$ باشد و از طرفی عدد تصادفی تولیدشده برای هر بردار ویژگی کمتر از پارامتر p3 باشد برای به‌روزرسانی بردارهای ویژگی از رابطه ۱۴، ۱۵ و ۱۶ استفاده می‌شود.

$$A_1 = BestVulture_1(i) - (\frac{BestVulture_1 \times P(i)}{BestVulture_1 \times P(i)^2}) \times F \quad (۱۴)$$

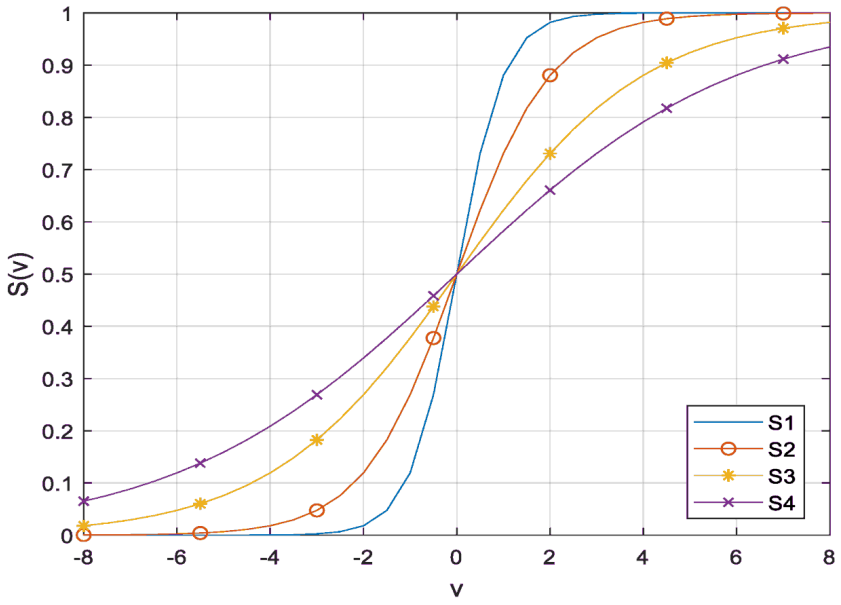
$$A_2 = BestVulture_2(i) - (\frac{BestVulture_2 \times P(i)}{BestVulture_2 \times P(i)^2}) \times F \quad (۱۵)$$

$$P(i+1) = \frac{(A_1 + A_2)}{2} \quad (۱۶)$$

اگر مقدار $|F| < 0/5$ باشد و عدد تصادفی تولیدشده برای هر بردار ویژگی بیشتر از p3 باشد برای به‌روزرسانی هر یک از بردارهای ویژگی از رابطه ۱۷ استفاده می‌شود.

$$p(i+1) = R(i) - |d(t) \times F \times Levy(d)| \quad (۱۷)$$

در اینجا Levy(d) یک تابع پروازی در d بعد است و |d(t)| قدر مطلق فاصله یک راه‌حل از یکی از راه‌حل‌ها بهینه مسئله است. بردارهای ویژگی که توسط الگوریتم AVOA محاسبه می‌شوند نیاز به باینری کردن دارند لذا برای باینری نمودن آن‌ها از توابع نگاشت S و V استفاده می‌شود که نمونه آن‌ها در شکل۵ و ۶ نمایش داده‌شده است. در ابتدا می‌توان بردارهای ویژگی را توسط روابط ۱۸، ۱۹، ۲۰ و ۲۱ با استفاده از توابع S نرمالیزه نمود و یا توسط روابط ۲۲، ۲۳، ۲۴ و ۲۵ با تابع V بردارهای ویژگی رابین صفر و یک نرمالیزه نمود. بعد از نرمال‌سازی بردارهای ویژگی توسط روابط ۲۶ و ۲۷ می‌توان بردارهای ویژگی را با آستانه مرتبط با تابع S و V به مقادیر صفر یا یک نگاشت داد و آن را باینری نمود. در این رابطه‌ها $V_{l,d}$به نشان‌دهنده مؤلفه d بردار ویژگی l است. مقادیر r_1 تا r_5 نیز اعداد تصادفی بین صفر و یک است [۲۹].



شکل ۵: تابع تبدیل S برای باینری کردن بردارهای ویژگی به‌روزرسانی شده توسط الگوریتم AVOA [۲۹]

Figure 5. S transform function to binarize feature vectors updated by AVOA algorithm [29]

$$S1(v_{l,d}(t+1)) = \frac{\pi_\eta}{1+\exp(-2v_{l,d}(t+1))} \quad (۱۸)$$

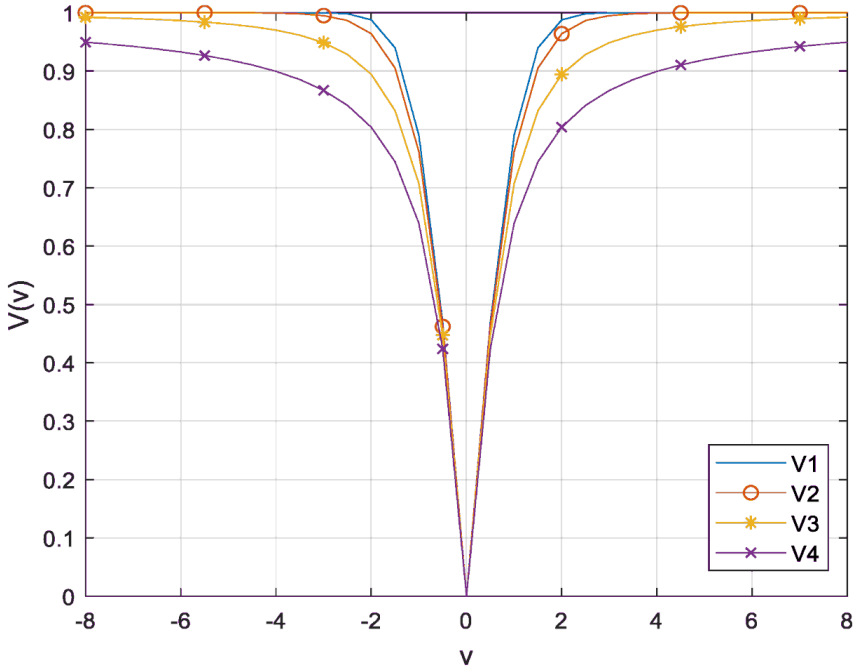
$$S2(v_{l,d}(t+1)) = \frac{1}{1+\exp(-v_{l,d}(t+1))} \quad (۱۹)$$

$$S3(v_{l,d}(t+1)) = \frac{1}{1+\exp(-v_{l,d}(t+1)/2)} \quad (۲۰)$$

$$S3(v_{l,d}(t+1)) = \frac{1}{1+\exp(-v_{l,A}(t+1)/3)} \quad (۲۱)$$

$$V1(v_{l,A}(t+1)) = \left| erf\left(\frac{\sqrt{\pi}}{2} v_{l,d}(t+1)\right) \right| \quad (۲۲)$$

$$V2(v_{l,d}(t+1)) = \left| \tanh(v_{l,d}(t+1)) \right| \quad (۲۳)$$



شکل ۶: تابع تبدیل V برای باینری کردن بردارهای ویژگی به‌روزرسانی شده توسط الگوریتم AVOA [۲۹]

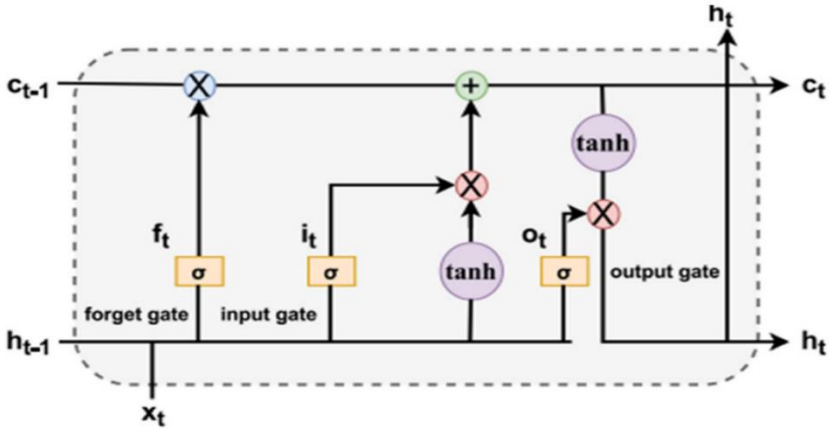
Figure 6. V transform function to binarize feature vectors updated by AVOA algorithm [29]

$$V3(v_{l,A}(t+1)) = \left| \frac{v_{l,A}(t+1)}{\sqrt{1+(v_{l,A}(t+1)^2}} \right| \quad (۲۴)$$

$$V4(v_{l,A}(t+1)) = \left| \frac{2}{\pi} \arctan\left(\frac{\pi}{2} v_{l,A}(t+1)\right) \right| \quad (۲۵)$$

$$x_{l,d}(t+1) = \begin{cases} 1, & if \quad S(v_{l,A}(t+1)) > r_4 \\ 0, otherwise \end{cases} \quad (۲۶)$$

$$x_{l,d}(t+1) = \begin{cases} 1 - x_{l,d}(t), & if \quad V(v_{l,A}(t+1)) \geq r_5 \\ x_{l,d}(t) \quad , otherwise \end{cases} \quad (۲۷)$$



شکل ۷: ساختار شبکه عصبی LSTM

Figure 7. LSTM neural network structure

در روش پیشنهادی کنترلر SDN ، بردار ویژگی بهینه‌ای که توسط الگوریتم AVOA محاسبه می‌شود نوع ورودی طبقه‌بندی کننده LSTM را تعیین می‌کند. شبکه عصبی LSTM یک روش یادگیری عمیق است که مطابق شکل ۷، دارای گیت‌های فراموشی، خروجی و ورودی است و یک ابزار کارآمد برای طبقه‌بندی ترافیک شبکه است. در معادلات ۲۸، ۲۹، ۳۰، ۳۱ و ۳۲، مدل‌سازی شبکه عصبی یادگیری عمیق LSTM را نشان داده است [۳۰].

$$i_t = \sigma(W_{xi}x_t + W_{hi}x_{t-1} + W_{ci}c_{t-1} + b_i) \quad (۲۸)$$

$$f_t = \sigma(W_{xf}x_t + W_{hf}h_{t-1} + W_{cf}c_{t-1} + b_f) \quad (۲۹)$$

$$o_t = \sigma(W_{xo}x_t + W_{ho}h_{t-1} + W_{co}c_t + b_o) \quad (۳۰)$$

$$c_t = f_t c_{t-1} + i_t \tanh(W_{xc}x_t + W_{hc}h_{t-1} + b_c) \quad (۳۱)$$

$$h_t = o_t + \tanh(c_t) \quad (۳۲)$$

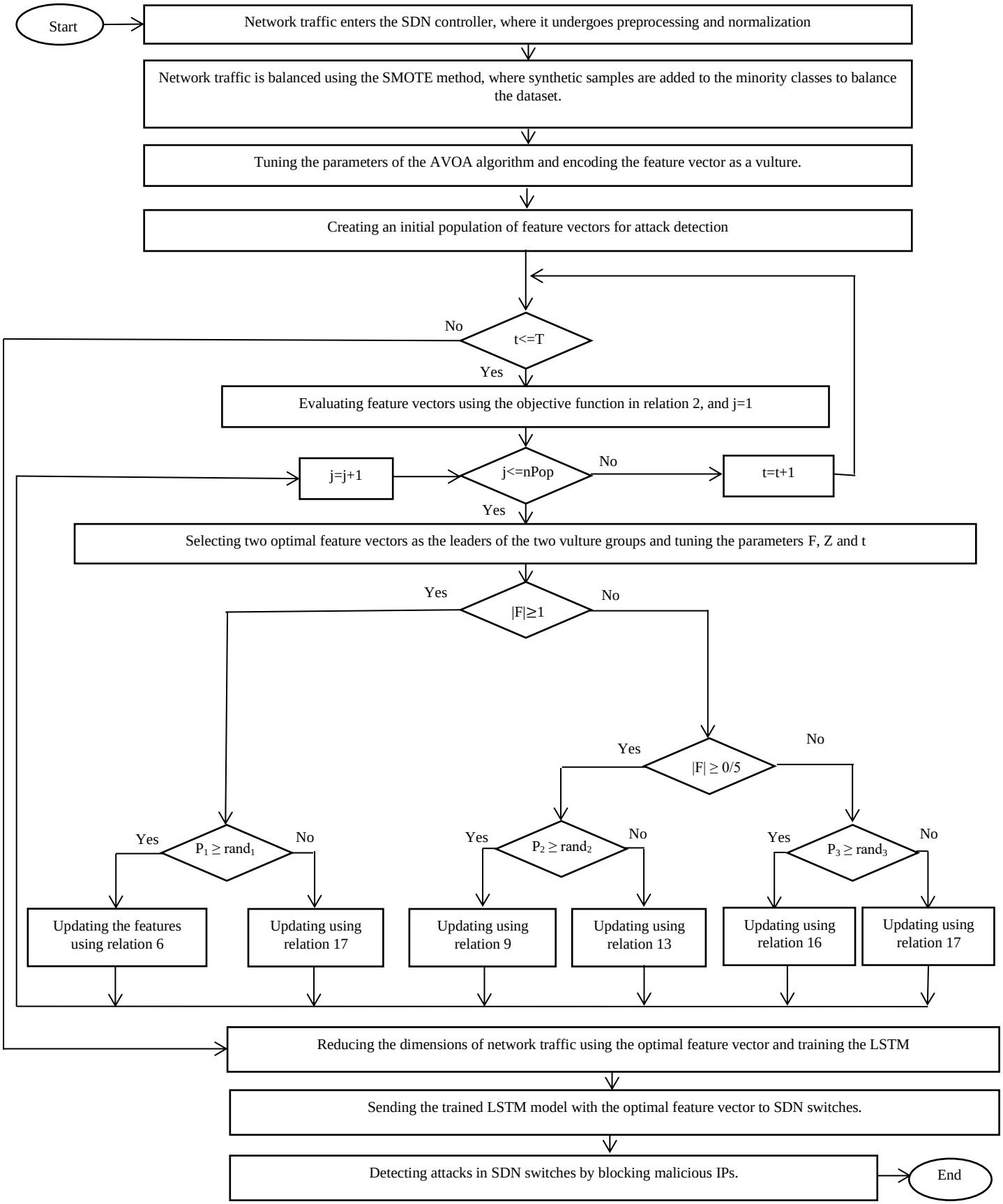
که در آن، ft، ot و ct به ترتیب ورودی، فراموشی، خروجی و فعال‌سازی دروازه سلولی در هر زمان t هستند. در این معادلات، σ تابع سیگموئید لجستیک و W_x ماتریس‌های وزن شبکه عصبی است و b_x بایاس‌های شبکه است. h_{t-1} حالت پنهان در مرحله زمانی $t-1$ است و c_{t-1} وضعیت سلول در زمان $t-1$ است. در اینجا شبکه LSTM نقش طبقه‌بندی کننده ترافیک شبکه را بر عهده دارد و مدل آموزش‌یافته از طریق کنترل‌کننده برای سوئیچ‌های شبکه ارسال می‌شود. شبکه عصبی LSTM یک روش قدرتمند برای تجزیه‌وتحلیل سری‌های زمانی و جریان‌های داده‌ای است. در این شبکه برخی از اطلاعات به گیت فراموشی سپرده می‌شوند و برخی دیگر نگهداری می‌شوند. مزیت این شبکه آن است که قبل و بعد یک جریان داده‌ای تا حدودی به خاطر سپرده می‌شود. دلیل استفاده از شبکه عصبی LSTM در بخش طبقه‌بندی روش پیشنهادی آن است که این روش در بسیاری از پژوهش‌ها برای تحلیل ترافیک شبکه استفاده‌شده و نتایج ارزشمندی به دست آورده است.

شبکه عصبی از نوع LSTM مشکل محو شوندگی تدریجی و انفجار گرادیان را ندارد برخلاف شبکه‌های بازگشتی و کانولوشن، آموزش آن پیچیده نیست. در شبکه‌های عصبی بازگشتی اگر از tanh یا relu به‌عنوان یک تابع فعال‌سازی استفاده شود، نمی‌تواند دنباله‌های بسیار طولانی را پردازش کند؛ اما شبکه عصبی LSTM این چالش را ندارد. فیلتر کردن ترافیک ورودی آن با الگوریتم بهینه‌سازی کرکس در فاز انتخاب ویژگی نیز توان این شبکه را برای یادگیری روی ویژگی‌های اصلی افزایش می‌دهد و توانایی تشخیص آن را در تشخیص حملات افزایش می‌دهد.

در شکل ۸، فلوچارت روش پیشنهادی برای تشخیص حملات در سوئیچ‌های SDN نمایش داده‌شده است و دارای مراحل ذیل است:

- ترافیک شبکه وارد کنترلر SDN می‌شود تا برای ایجاد مدل طبقه‌بندی از آن استفاده شود.
- ترافیک شبکه در کنترلر با روش SMOTE متعادل‌سازی می‌شود و سپس حجم نمونه‌های اقلیت افزوده می‌شود تا مجموعه داده متعادل‌سازی شود.
- الگوریتم AVOA[1] برای انتخاب ویژگی در کنترلر استفاده می‌شود و در اینجا هر بردار ویژگی یک کرکس است که توسط معادلات الگوریتم AVOA مورد به‌روزرسانی قرارگرفته می‌شوند.
- بردارهای ویژگی در هر تکرار با تابع هدف ارزیابی می‌شوند تا درنهایت بهینه‌ترین بردارهای ویژگی انتخاب شود و دو بردار ویژگی بهینه اول به‌عنوان سردسته کرکس‌ها انتخاب می‌شود.
- در روش پیشنهادی در هر تکرار بردارهای ویژگی با توابع نظیر S و V باینری می‌شوند تا درنهایت بردارهای ویژگی مجدد حالت صفر و یک خود را به دست آورند.
- کنترلر کننده SDN بر اساس بردار ویژگی شبکه عصبی LSTM را آموزش داده و یک مدل طبقه‌بندی را ایجاد می‌کند.

[1] African Vultures Optimiztion Algorithm



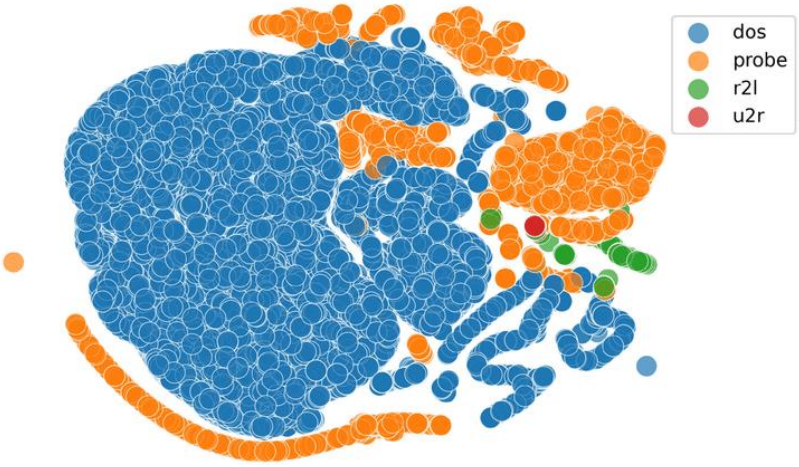
شکل ۸: فلوچارت روش پیشنهادی در تشخیص حملات به شبکه

Figure 8. Flowchart of the proposed method in detecting network attacks

- کنترلر کننده SDN بردار ویژگی بهینه و مدل یادگیری LSTM را برای سوئیچ‌های SDN ارسال کرده و هر سوئیچ SDN در ابتدا توسط بردار ویژگی بهینه، ترافیک شبکه را کاهش ابعاد داده و سپس در ادامه با مدل طبقه‌بندی LSTM ترافیک شبکه را به دودسته حمله و عادی طبقه‌بندی می‌کند.
- سوئیچ‌های SDN، IP گره‌های حمله‌کننده در حملات DDoS را باهم به اشتراک می‌گذارند و از آن‌ها برای بلاک کردن ترافیک حملات استفاده می‌کنند.

۴-نتایج تجربی

در این بخش سیستم تشخیص نفوذ پیشنهادی در معماری SDN در محیط Matlab پیاده‌سازی می‌شود و سپس در ادامه با آزمایش‌هایی روش پیشنهادی در تشخیص حملات با روش‌های مشابه مقایسه می‌شود. در روش پیشنهادی ۷۰ درصد از ترافیک شبکه آموزشی است و ۳۰ درصد دیگر برای ارزیابی به‌عنوان داده‌های آزمون و اعتبارسنجی استفاده می‌شود. در روش پیشنهادی محدوده نرمال‌سازی بین ۰ و ۱ است و نوع تابع فعالیت نیز در هر آزمایش تصادفی انتخاب می‌شود. درروش پیشنهادی تعداد بردارهای ویژگی برابر ۱۵ و تعداد تکرار الگوریتم AVOA برابر ۵۰ است و هر آزمایش ۳۵ مرتبه تکرار شده است. مقدار پارامترهای p1، p2 و p3 در الگوریتم AVOA به ترتیب برابر ۰/۶، ۰/۴ و ۰/۶ تنظیم می‌شود. مجموعه داده NSL-KDD یک مجموعه داده جهانی در زمینه تشخیص حملات به شبکه است و مطابق شکل ۹، این مجموعه داده دارای عدم تعادل در چهار حمله مختلف است [۳۲].



شکل ۹: عدم تعادل در مجموعه داده NSL-KDD
Figure 9. Imbalance in the NSL-KDD dataset

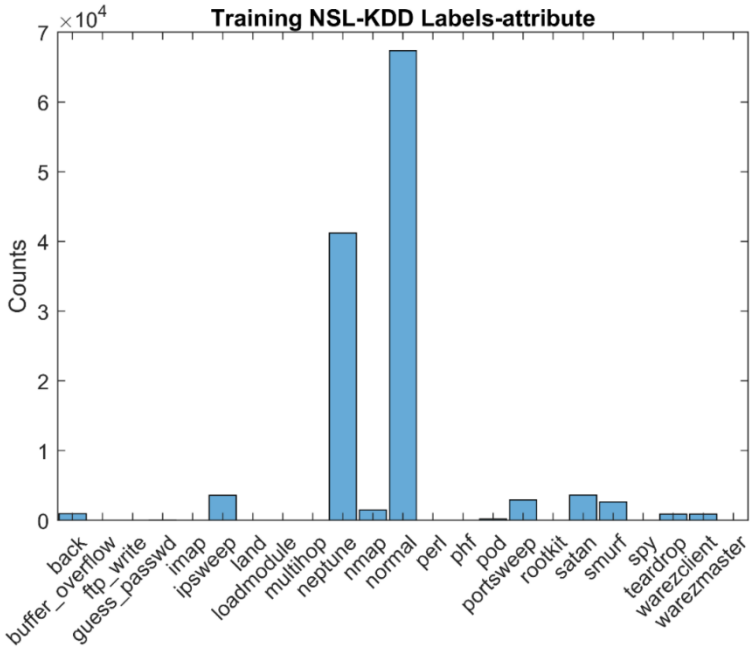
در این مجموعه داده برای هر ورودی یا نمونه، از ۴۱ ویژگی مختلف ارائه‌شده که هر یک از آن‌ها ممکن است به نوع حمله رکورد یا نوع عادی آن اختصاص داده شود. مقادیر مشخصه می‌توانند اسمی، باینری یا عددی باشند. بااین‌حال، برخلاف KDD CUP 99، مجموعه آموزشی مجموعه داده NSL-KDD حاوی هیچ ورودی تکراری نیست؛ بنابراین، طبقه‌بندی نسبت به رکوردهای متداول‌تر تعصب ندارند؛ بنابراین، در NSL-KDD، تکنیک‌هایی با نرخ تشخیص بهتر رکوردهای مکرر در مجموعه‌های آزمایشی بر عملکرد یادگیرندگان تأثیر نمی‌گذارند. از ۴۱ ویژگی موجود در این مجموعه داده، سه ویژگی نوع اسمی، Protocol_type، Service و Flag وجود دارد. درحالی‌که سایر ویژگی‌ها همه از نوع عددی هستند. حملات انکار سرویس (DoS)، حملات از راه دور به سیستم محلی (R2L)، حمله کاربر به ریشه (U2R) و حملات کاوشگر چهار دسته اصلی حملات سایبری در این مجموعه هستند. در جدول ۱، ایست ویژگی‌های بکار رفته در مجموعه داده NSL-KDD به نمایش گذاشته شده است [۳۴].

مجموعه داده NSL-KDD یک مجموعه داده به‌شدت نامتعادل است؛ زیرا مطابق شکل ۱۰، حملات مختلف دارای نمونه‌هایی به‌اندازه یکسان نیست [۳۴].

جدول ۱: ویژگی‌های بکار رفته در مجموعه داده NSL-KDD

Table 1. Features used in the NSL-KDD dataset

Feature type	Features
Numerical	Duration, src_bytes, dst_bytes, land, wrong_fragment, urgent, hot, num_failed_logins, logged_in, num_compromised, root_shell, su_attempted, num_root, num_file_creations, num_shells, num_access_files, num_outbound_cmds, is_host_login, is_guest_login, count, srv_count, serror_rate, srv_serror_rate, rerror_rate, srv_rerror_rate, same_srv_rate, diff_srv_rate, srv_diff_host_rate, dst_host_count, dst_host_srv_count, dst_host_same_srv_rate, dst_host_diff_srv_rate, dst_host_same_src_port_rate, dst_host_srv_diff_host_rate, dst_host_serror_rate, dst_host_srv_serror_rate, dst_host_rerror_rate and dst_host_srv_rerror_rate.
Non-numerical	"Protocol_type", "Service", and "Flag".



شکل ۱۰: عدم تعادل در مجموعه داده NSL-KDD

Figure 10. Imbalance in the NSL-KDD dataset

در این مجموعه داده ترافیک عادی بیشترین سهم از ترافیک را دارد و از طرفی حمله‌ای نظیر neptune دارای بیشترین سهم در بین انواع حملات است و از طرفی حمله‌ای نظیر Perl دارای تعداد نمونه‌های اندک است. برای رفع این چالش و افزایش تعداد نمونه‌ای انواع حملات ازجمله DDoS می‌توان با روش تولید داده مصنوعی SMOTE تعدادی نمونه مصنوعی ایجاد نمود و به مجموعه داده اضافه نمود. در روش پیشنهادی مجموع حملاتی نظیر DDoS به تعداد ترافیک عادی با روش SMOTE تولید و به مجموعه داده اضافه می‌شود. در روش پیشنهادی تعداد نمونه‌های عادی برابر ۶۵۰۰۰ و تعداد نمونه‌های حمله نیز به ۶۵۰۰۰ افزایش داده می‌شود تا مجموعه داده متعادل شود.

یکی از مهم‌ترین روش‌های به دست آوردن تخمین خطای مدل از طریق داده‌های تست، روش اعتبارسنجی متقابل هست که یکی از روش‌های آن، "K-fold cross validation" است. در این روش به‌صورت تصادفی داده‌ها را به K بخش به‌طور یکسان تقسیم می‌شوند به‌طوری‌که در هر مجموعه تقریباً nk مشاهده برای k=1,…,K قرار بگیرد. در آزمایش‌ها انجام‌شده مقدار k برابر ۱۰ تنظیم‌شده است. برای ارزیابی سیستم تشخیص نفوذ پیشنهادی به‌عنوان یک روش طبقه‌بندی ترافیک شبکه از متریک‌های مانند دقت[1]، حساسیت[2] و صحت[3] مطابق رابطه‌های ۳۳، ۳۴، ۳۵ فرموله شده است.

$$Accuracy = ACC = \frac{TP + TN}{TP + TN + FP + FN} \times 100\% \quad (۳۳)$$

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

$$Sensitivity = \text{Re}call = DR = \frac{TP}{TP + FN} \times 100\% \quad (۳۴)$$

$$\text{Pr}ecision = P = \frac{TP}{TP + FP} \times 100\% \quad (۳۵)$$

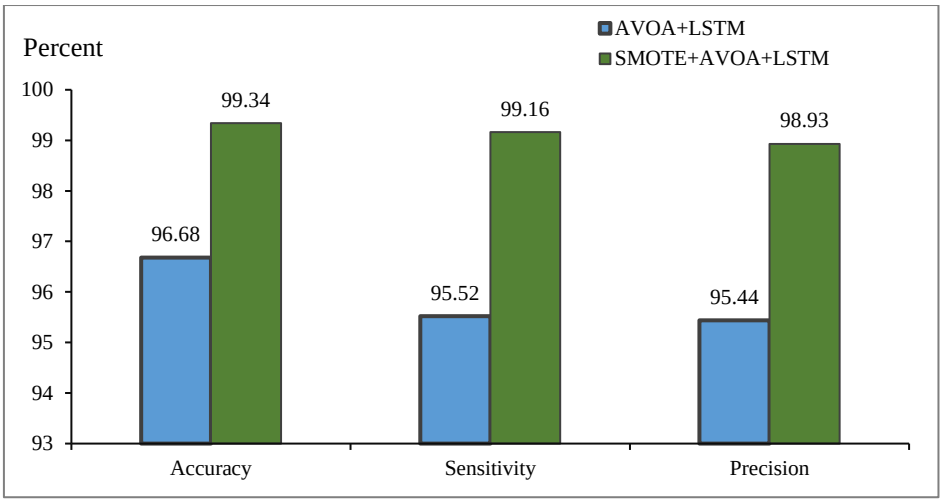
پارامترهای TP، TN، FP و FN به شکل تعریف می‌شود:

- نمونه‌های صحیح مثبت (TP): ترافیک واردشده به سوئیچ SDN از نوع حمله بوده و روش پیشنهادی به‌درستی این ترافیک را در کلاس حمله قرار داده است.
- نمونه‌های غلط مثبت (FP): ترافیک واردشده به سوئیچ SDN از نوع عادی بوده و روش پیشنهادی به‌اشتباه این ترافیک را در کلاس حمله قرار داده است.
- نمونه‌های صحیح منفی (TN): ترافیک واردشده به سوئیچ SDN از نوع عادی بوده و روش پیشنهادی به‌درستی این ترافیک را در کلاس عادی قرار داده است.
- نمونه‌های غلط منفی (FN): ترافیک واردشده به سوئیچ SDN از نوع حمله بوده و روش پیشنهادی به‌اشتباه این ترافیک را در کلاس عادی قرار داده است.

آزمایش‌ها انجام‌شده نشان می‌دهد روش پیشنهادی بدون متعادل‌سازی مجموعه داده دارای دقت، حساسیت و صحتی برابر ۹۶/۶۸ درصد و ۹۵/۵۲ درصد و ۹۵/۴۴ درصد است و این در حالی است که اگر متعادل‌سازی مجموعه داده با روش SMOTE انجام شود آنگاه دقت، حساسیت و صحتی برابر ۹۹/۳۴ درصد، ۹۹/۱۶ درصد و ۹۸/۹۳ درصد است. برای اجرای هر روش دو حالت مستقل ذیل در نظر گرفته‌شده تا اطمینان حاصل شود که آزمایش‌ها مستقل است:

- در ابتدا مجموعه داده نامتعادل به‌عنوان ورودی روش پیشنهادی در نظر گرفته‌شده است و آزمایش‌ها چند بار تکرار شده است و متوسط شاخص‌ها مانند دقت، حساسیت و صحت محاسبه‌شده است.
- در مرحله دوم در آزمایش‌هایی مستقل، مجموعه داده در ابتدا به کمک روش SMOTE متعادل‌سازی شده است.

در نمودار شکل ۱۱، شاخص‌های دقت، حساسیت و صحت روش پیشنهادی در دو حالت باهم مقایسه شده است.

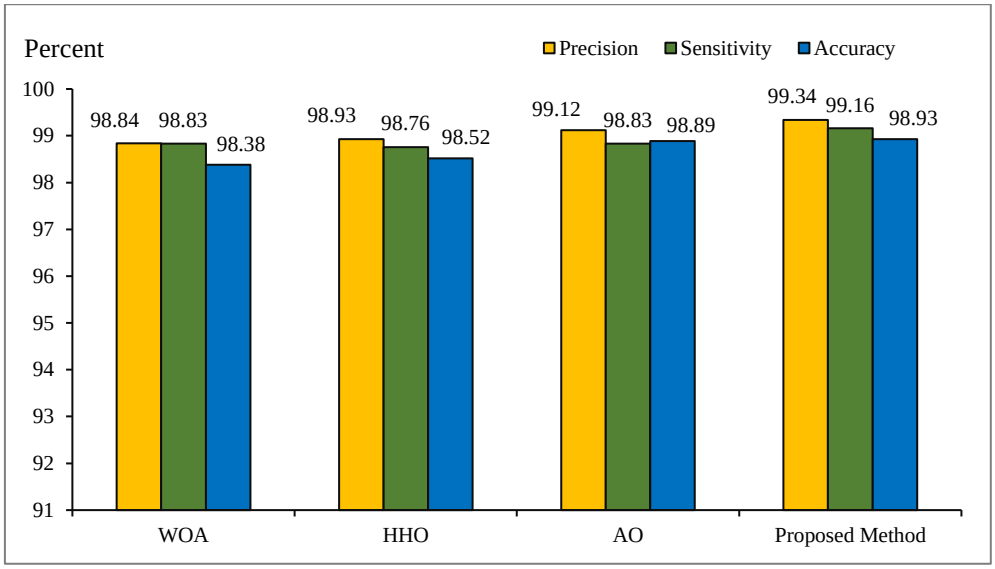


شکل ۱۱: نقش متعادل‌سازی مجموعه داده در افزایش دقت، حساسیت و صحت مدل پیشنهادی

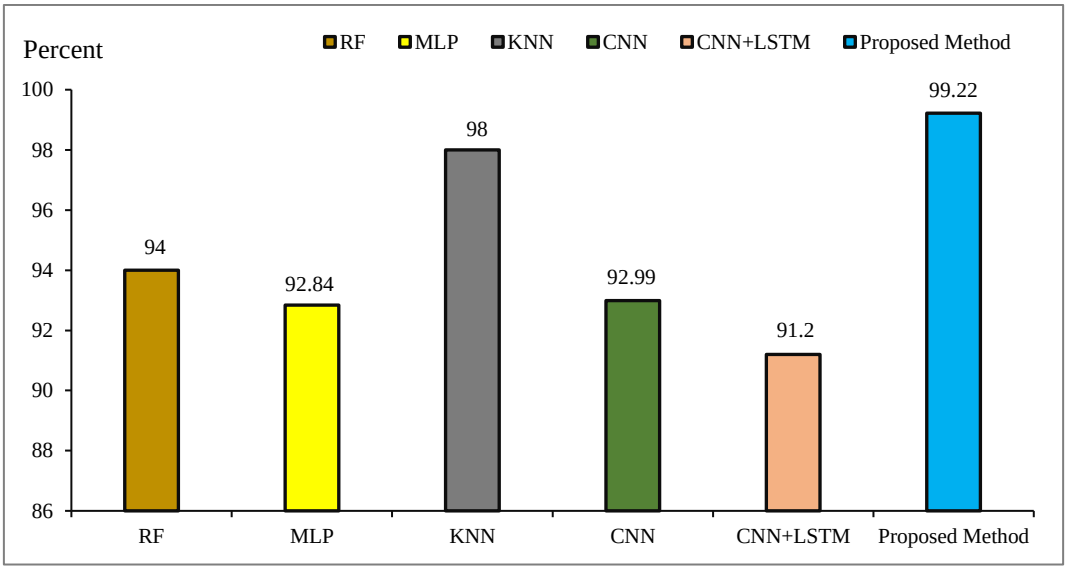
Figure 11. The role of data set balancing in increasing the accuracy, sensitivity and accuracy of the proposed model

آزمایش‌ها نشان می‌دهد که اگر از متعادل‌سازی در روش پیشنهادی استفاده شود آنگاه شاخص دقت، حساسیت و صحت روش پیشنهادی به ترتیب ۳/۶۴ درصد و ۲/۶۶ درصد و ۳/۴۹ درصد در تشخیص حملات بهبود خواهد داشت. انتخاب ویژگی نقش مهمی در دقت روش پیشنهادی دارد و در نمودار شکل ۱۲، شاخص دقت، حساسیت و صحت روش پیشنهادی با الگوریتم‌های

انتخاب ویژگی ازجمله الگوریتم بهینه‌سازی وال[1](WOA)، الگوریتم بهینه‌سازی شاهین[2](HHO)، الگوریتم بهینه‌سازی عقاب طلایی[3] (GEO) مقایسه شده است. در این مقایسه‌ها تلاش شده است تا هرکدام از الگوریتم‌های مورد مقایسه جایگزین روش انتخاب ویژگی در ترکیب SMOTE و LSTM شود تا تأثیر آن در تشخیص حملات ارزیابی شود.



شکل ۱۲: مقایسه دقت، حساسیت و صحت تشخیص حملات با روش‌های انتخاب ویژگی
Figure 12. Comparison of accuracy, sensitivity and accuracy of attack detection with feature selection methods

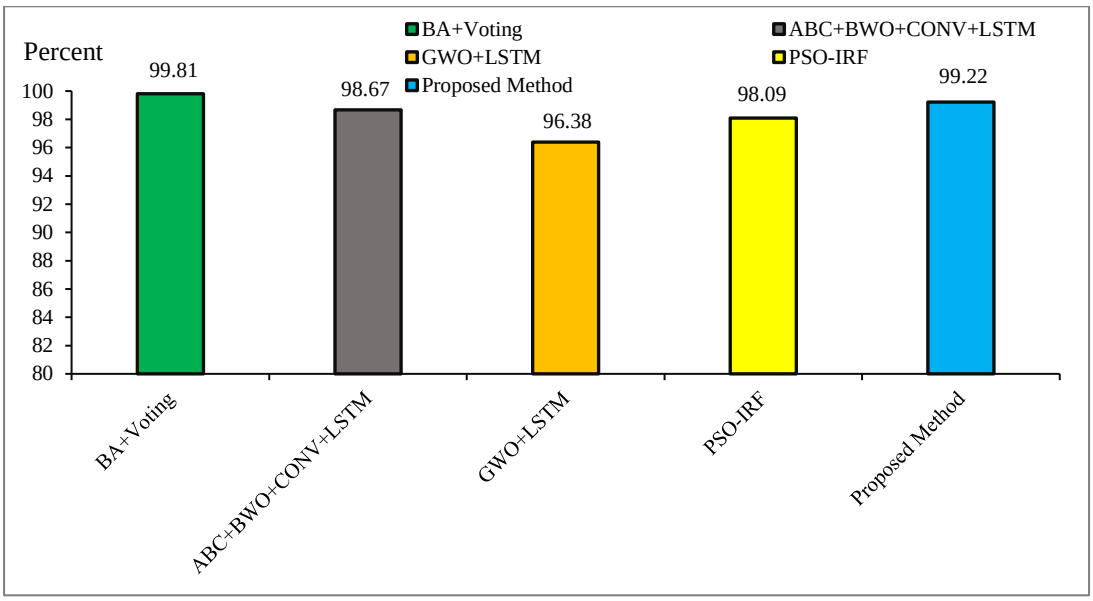


شکل ۱۳: مقایسه دقت تشخیص حملات با روش‌های یادگیری
Figure 13. Comparison of attack detection accuracy with learning methods

تجزیه‌وتحلیل آزمایش‌ها نشان می‌دهد که در بین روش‌های موردنظر الگوریتم AVOA یا روش پیشنهادی در ترکیب با یادگیری عمیق LSTM دارای دقت، حساسیت و صحت بیشتری نسبت به سایر روش‌های فرا ابتکاری در انتخاب ویژگی است. یکی از دلایل دقت بیشتر روش پیشنهادی در تشخیص حملات نسبت به این روش‌ها آن است که مکانیزم جستجوی AVOA نسبت به سایر الگوریتم‌ها هوشمندی بیشتری دارد و از طرفی الگوریتم AVOA دارای یک نوع سلسله‌مراتب رهبری و هدایت جمعیت

[1] Whale Optimization Algorithm (WOA)
[2] Haris Hawks Optimization Algorithm (HHO)
[3] Golden Eagle Optimizer Optimization Algorithm (GEO)

توسط دو جواب بهینه است که در سایر الگوریتم این مکانیزم وجود ندارد. در نمودار شکل ۱۳، روش پیشنهادی در شاخص دقت با چند روش یادگیری ماشین و یادگیری عمیق مقایسه شده است[۳۲].



شکل ۱۴: مقایسه دقت روش پیشنهادی با روش‌های هوش گروهی ترکیب‌شده با یادگیری ماشین و یادگیری عمیق

Figure 14. Comparing the accuracy of the proposed method with group intelligence methods combined with machine learning and deep learning

در این نمودار مشاهده می‌شود روش پیشنهادی از روش‌های یادگیری عمیق نظیر CNN و CNN+LSTM دارای دقت بیشتری در تشخیص حملات است. یکی از دلایل این موضوع آن است که روش پیشنهادی دارای فاز انتخاب ویژگی هوشمندانه با الگوریتم AVOA است و از طرفی داده‌ها در مجموعه داده در روش پیشنهادی با SMOTE متعادل‌سازی می‌شود. در پژوهش [۳۳] که در سال ۲۰۲۳ ارائه شده است برای تشخیص حملات از چند روش انتخاب ویژگی مانند الگوریتم خفاش با مکانیزم رأی‌گیری[۱]، الگوریتم ترکیبی بیوه سیاه و زنبورعسل[۲]، الگوریتم گرگ خاکستری[۳] و الگوریتم ذرات[۴] استفاده‌شده است و روش پیشنهادی مطابق نمودار شکل ۱۴، با این روش‌ها در شاخص دقت مقایسه شده است. آزمایش‌ها نشان می‌دهد دقت روش پیشنهادی از روش‌های تشخیص نفوذ بر پایه الگوریتم ترکیبی بیوه سیاه و زنبورعسل، الگوریتم گرگ خاکستری و الگوریتم ذرات دقت بیشتری دارد و فقط نسبت به سیستم تشخیص نفوذ بر پایه یادگیری با رأی‌گیری اکثریت دارای دقت کمتری است.

۵-نتیجه‌گیری

اینترنت اشیاء شبکه‌ای از دستگاه‌های هوشمند به‌هم‌پیوسته است که در تولید و جمع‌آوری حجم عظیمی از داده‌ها کمک می‌کند. دستگاه‌های اینترنت اشیاء در حال حاضر در هر زمینه‌ای از زندگی روزمره ما استفاده می‌شوند. یکی از چالش‌های مهم اینترنت اشیاء حملات به شبکه و زیرساخت‌های آن است. شناسایی حملات سایبری ازاین‌جهت مهم است که باعث آسیب و متوقف شدن سرویس‌های کاربردی در اینترنت اشیاء می‌شود. سیستم‌های تشخیص نفوذ یک روش کارآمد برای تشخیص حملات و مقابله با انواع حملات سایبری هستند. یکی از چالش‌های سیستم‌های تشخیص نفوذ عدم تطبیق آن‌ها با معماری اینترنت اشیاء است. در روش پیشنهادی یک سیستم تشخیص نفوذ کارآمد در بستر معماری توزیع‌شده شبکه نرم‌افزار محور ارائه‌شده است. مزیت سیستم تشخیص نفوذ پیشنهادی آن است که به‌صورت توزیع‌شده در سوئیچ‌های شبکه نرم‌افزار محور مستقر است.

[1] BA+Voting
[2] ABC+BWO+CONV+LSTM
[3] GWO+LSTM
[4] PSO-IRF

استقرار سیستم تشخیص نفوذ در شبکه نرم‌افزار محور باعث می‌شود ترافیک در حین مبادله در سیستم سوئیچینگ نیز تحلیل و ارزیابی شود. روش پیشنهادی برای رفع چالش عدم تعادل در مجموعه داده آموزشی NSL-KDD از الگوریتم SMOTE استفاده می‌کند و برای کاهش ابعاد ترافیک شبکه در کنترلر کننده شبکه نرم‌افزار محور از الگوریتم بهینه‌سازی کرکس آفریقایی استفاده می‌کند. در روش پیشنهادی ویژگی‌های مهم ترافیک شبکه برای آموزش شبکه عصبی حافظه‌ی کوتاه‌مدت طولانی در شبکه نرم‌افزار محور استفاده می‌شود. ارزیابی‌ها نشان می‌دهد روش پیشنهادی به دلیل انتخاب ویژگی مؤثر و متعادل‌سازی مجموعه داده از روش‌های یادگیری عمیق نظیر شبکه عصبی حافظه‌ی کوتاه‌مدت طولانی، شبکه عصبی بازگشتی و شبکه عصبی کانولوشن دقت بیشتری در تشخیص حملات دارد و نسبت به روش‌های انتخاب ویژگی نظیر الگوریتم بهینه‌سازی وال، الگوریتم بهینه‌سازی شاهین هریس، الگوریتم بهینه‌سازی عقاب طلایی، الگوریتم بهینه‌سازی ذرات، الگوریتم بهینه‌سازی گرگ خاکستری، الگوریتم بهینه‌سازی کلونی زنبورعسل دارای دقت بیشتری در تشخیص حملات است.

یکی از عوامل مهم و تأثیرگذار در افزایش کارایی روش پیشنهادی در تشخیص حملات به شبکه استفاده از هوش گروهی است. هوش گروهی به دلیل آنکه اعضای آن جستجوی موازی را باهم هم انجام می‌دهند شانس زیادی برای یافتن بردارهای ویژگی بهینه دارد. برای آنکه الگوریتم هوش گروهی توانایی بهتری برای جستجو داشته باشد، اندازه جمعیت، تعداد تکرار آن و مقادیر پارامترها بسیار تأثیرگذار است. به‌طورکلی با افزایش اندازه جمعیت و تعداد تکرار الگوریتم بهینه‌سازی کرکس آفریقایی احتمال یافتن جواب بهینه افزایش خواهد داشت. با افزایش اندازه جمعیت، فضای مسئله بیشتر مورد جستجو قرارگرفته می‌شود و با افزایش تکرار نیز شانس همگرایی به جواب‌های بهینه افزایش خواهد یافت. افزایش اندازه جمعیت و تعداد تکرار از یک آستانه باعث افزایش قابل‌توجه در دقت نمی‌شود و فقط زمان اجرای آزمایش‌ها را افزایش می‌دهد؛ لذا در آزمایش‌ها اندازه جمعیت و تکرار الگوریتم منطقی و مانند اکثر پژوهش‌ها در نظر گرفته‌شده است. پارامترهای الگوریتم بهینه‌سازی کرکس نیز بر اساس مقاله مرتبط با این الگوریتم تنظیم‌شده است. از پیشنهادهای آتی ما به‌کارگیری مکانیزم رأی‌گیری اکثریت در تشخیص حملات در سوئیچ‌های شبکه نرم‌افزار محور و همچنین به‌کارگیری شبکه عصبی واحد بازگشتی گیتی و شبکه عصبی کانولوشن برای تشخیص حملات است.

مراجع

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

[2] H. Kareemullah, D. Najumnissa, M. M. Shajahan, M. Abhineshjayram, V. Mohan and S. A. Sheerin, "Robotic Arm controlled using IoT application," *Computers and Electrical Engineering*., vol. 105, p. 108539, Jun. 2023, doi: 10.1016/j.compeleceng.2022.108539.

[3] O. E. Tayfour, A. Mubarakali, A. E. Tayfour, M. N. Marsono, E. Hassan and A. M. Abdelrahman, "Adapting deep learning-LSTM method using optimized dataset in SDN controller for secure IoT," *Soft Computing*., pp. 1-9, Mar. 2023, doi: 10.1007/s00500-023-08348-w.

[4] A. Bashaiwth, H. Binsalleeh and B. AsSadhan, "An Explanation of the LSTM Model Used for DDoS Attacks Classification," *Applied Sciences*, vol. 13, no. 15, pp. 1-30, Jul. 2023, doi: 10.3390/app13158820.

[5] DDoS Attacks History. Radware. Available online: https://www.radware.com/security/ddos-knowledge-center/ddos-chronicles/ddos-attacks-history, accessed on 17 July 2023.

[6] K. P. Reddy, K. R. Raju, K. C. Mouli and M. Praveen, "An intelligent network intrusion detection system for anomaly analyzer using machine learning for software defined networks," *In AIP Conference Proceedings*, vol. 2548, no. 1, July 2023, doi: 10.1063/5.0118479.

[7] R. J. Gohari, L. Aliahmadipour and M. K. Rafsanjani, "Deep learning-based intrusion detection systems: A comprehensive survey of four main fields of cyber security," *Journal of Mahani Mathematical Research Center*, vol. 12, no. 2, pp. 289-324, May. 2023, doi: 10.22103/jmmr.2022.19961.1305.

[8] A. Javadpour, P. Pinto, F. Ja'fari and W. Zhang, "DMAIDPS: a distributed multi-agent intrusion detection and prevention system for cloud IoT environments," *Cluster Computing*, vol. 26, no. 1, pp. 367-384, May. 2022, doi: 10.1007/s10586-022-03621-3.

[9] S. Javanmardi, M. Shojafar, R. Mohammadi, M. Alazab and A. M. Caruso, "An SDN perspective IoT-Fog security: A survey," *Computer Networks*, vol. 229, p. 109732, June. 2023, doi: 10.1016/j.comnet.2023.109732.

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

[11] Y. Gao and M. Xu, "Defense against software-defined network topology poisoning attacks," *Tsinghua Science and Technology*, vol. 28, no. 1, pp. 39-46, February 2023, doi: 10.26599/TST.2021.9010077.

[12] C. Singh and A. K. Jain, "Detection and Mitigation of DDoS Attacks on SDN Controller in IoT Network using Gini Impurity," *Computer Security and Reliability*, pp. 1-27, May 2023, doi: 10.21203/rs.3.rs-2991752/v1.

[13] D. Jin, S. Chen, H. He, X. Jiang, S. Cheng and J. Yang, "Federated Incremental Learning based Evolvable Intrusion Detection System for Zero-Day Attacks," *IEEE Network*, vol. 37, no. 1, pp. 125-132, April 2023, doi: 10.1109/MNET.018.2200349.

[14] O. Habibi, M. Chemmakha, and M. Lazaar, "Imbalanced tabular data modelization using CTGAN and machine learning to improve IoT Botnet attacks detection," *Engineering Applications of Artificial Intelligence*, vol. 118, p. 105669, Feb. 2023, doi: 10.1016/j.engappai.2022.105669.

[15] B. Abdollahzadeh, F. S. Gharehchopogh and S. Mirjalili, "African vultures optimization algorithm: A new nature-inspired metaheuristic algorithm for global optimization problems," *Computers & Industrial Engineering*, vol. 158, p. 107408, 2021, doi: 10.1016/j.cie.2021.107408.

[16] R. M. A. Haseeb-ur-rehman, A. H. M. Aman, M. K. Hasan, K. A. Z. Ariffin, A. Namoun, A. Tufail and K. H. Kim, "High-Speed Network DDoS Attack Detection: A Survey," *Sensors*, vol. 23, no. 6850, Aug. 2023, doi: 10.3390/s23156850.

[17] S. Ullah, Z. Mahmood, N. Ali, T. Ahmad and A. Buriro, "Machine Learning-Based Dynamic Attribute Selection Technique for DDoS Attack Classification in IoT Networks," *Computers*, vol. 12, no. 115, May 2023, doi: 10.3390/computers12060115.

[18] Ö. Tonkal, H. Polat, E. Başaran, Z. Cömert and R. Kocaoğlu, "Machine learning approach equipped with neighbourhood component analysis for DDoS attack detection in software-defined networking," *Electronics*, vol. 10, no. 11, p. 1227, 2021, doi: 10.3390/electronics10111227.

[19] H. Zhou, Y. Zheng, X. Jia and J. Shu, "Collaborative prediction and detection of DDoS attacks in edge computing: A deep learning-based approach with distributed SDN," *Computer Networks*, vol. 225, p. 109642, April 2023, doi: 10.1016/j.comnet.2023.109642.

[20] M. Cherian and S. L. Varma, "Secure SDN–IoT Framework for DDoS Attack Detection Using Deep Learning and Counter Based Approach," *Journal of Network and Systems Management*, vol. 31, no. 54, 2023, doi: 10.1007/s10922-023-09749-w.

[21] T. M. Ghazal, N. A. Al-Dmour, R. A. Said, A. Omidvar, U. Y. Khan, T. R. Soomro, H. M. Alzoubi, M. Alshurideh, T. M. Abdellatif, A. Moubayed and L. Ali, "DDoS Intrusion Detection with Ensemble Stream Mining for IoT Smart Sensing Devices," *In The Effect of Information Technology on Business and Marketing Intelligence Systems*, pp. 1987-2012, 2023, doi: 10.1007/978-3-031-12382-5_109.

[22] X. H. Nguyen and K. H. Le, "Robust detection of unknown DoS/DDoS attacks in IoT networks using a hybrid learning model," *Internet of Things*, vol. 23, p. 100851, 2023, doi: 10.1016/j.iot.2023.100851.

[23] A. Hekmati, N. Jethwa, E. Grippo and B. Krishnamachari, "Correlation-Aware Neural Networks for DDoS Attack Detection In IoT Systems," *Computer Science*, Feb. 2023, doi: 10.48550/arXiv.2302.07982.

[24] N. Pandey and P. K. Mishra, "Performance analysis of entropy variation-based detection of DDoS attacks in IoT," *Internet of Things*, vol. 23, p. 100812, October. 2023, doi: 10.1016/j.iot.2023.100812.

[25] P. Shukla, C. R. Krishna and N. V. Patil, "EIoT-DDoS: embedded classification approach for IoT traffic-based DDoS attacks," *Cluster Computing*, pp. 1-20, 2023, doi: 10.1007/s10586-023-04027-5.

[26] 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.

[27] 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*, vol. 34, no. 4, pp. 1-14, Feb.2023, doi: 10.1002/ett.4758.

[28] J. N. Lee and J. Y. Lee, "An Efficient SMOTE-Based Deep Learning Model for Voice Pathology Detection," *Applied Sciences*, vol. 13, no. 3571, Feb. 2023, doi: 10.3390/app13063571.

[29] J. Too, A. R. Abdullah and N. Mohd Saad, "Binary competitive swarm optimizer approaches for feature selection," *Computation*, vol. 7, no. 31, 2019, doi: 10.3390/computation7020031.

[30] R. Elsayed, R. Hamada, M. Hammoudeh, M. Abdalla and S. A. Elsaid, "A Hierarchical Deep Learning-Based Intrusion Detection Architecture for Clustered Internet of Things," *Journal of Sensor and Actuator Networks*, vol. 12, no. 3, December 2022, doi: 10.3390/jsan12010003.

[31] G. Dlamini and M. Fahim, "DGM: a data generative model to improve minority class presence in anomaly detection domain," *Neural Computing and Applications*, vol. 33, no. 33, pp. 13635-13646, 2021, doi: 10.1007/s00521-021-05993-w.

[32] K. O. Adefemi Alimi, K. Ouahada, A. M. Abu-Mahfouz, S. Rimer and O. A. Alimi, "Refined LSTM based intrusion detection for denial-of-service attack in Internet of Things," *Journal of sensor and actuator networks*, vol. 11, no. 32, July 2022, doi: 10.3390/jsan11030032.

[33] M. Bakro, R. R. Kumar, A. A. Alabrah, Z. Ashraf, S. K. Bisoy, N. Parveen, S. Khawatmi and A. Abdelsalam, "Efficient Intrusion Detection System in the Cloud Using Fusion Feature Selection Approaches and an Ensemble Classifier," *Electronics*, vol. 12, no. 11, May 2023, doi: 10.3390/electronics12112427.

[34] M. H. Alwan, Y. I. Hammadi, O. A. Mahmood, A. Muthanna and A. Koucheryavy, "High Density Sensor Networks Intrusion Detection System for Anomaly Intruders Using the Slime Mould Algorithm," *Electronics*, vol. 11, no. 20, October 2022, doi: 10.3390/electronics11203332.