



Research Article

Denial-of-Service Attack Detection over IPv6 Network Based on KNN Algorithm

Yasser Alharbi,¹ Ali Alferaidi,¹ Kusum Yadav,¹ Gaurav Dhiman ,² and Sandeep Kautish ³

¹College of Computer Science and Engineering, University of Ha'il, Ha'il, Saudi Arabia

²Department of Computer Science, Government Bikram College of Commerce, -147001, Patiala, Punjab, India

³LBEF Campus, Kathmandu, Nepal

Correspondence should be addressed to Sandeep Kautish; dr.skautish@gmail.com

Received 19 October 2021; Revised 29 November 2021; Accepted 8 December 2021; Published 24 December 2021

Academic Editor: Junjuan Xia

Copyright © 2021 Yasser Alharbi et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

With the rapid increase and complexity of IPv6 network traffic, the traditional intrusion detection system Snort detects DoS attacks based on specific rules, which reduces the detection performance of IDS. To solve the DoS intrusion detection problem in the IPv6 network environment, the lightweight KNN optimization algorithm in machine learning is adopted. First, the double dimensionality reduction of features is achieved through the information gain rate, and discrete features with more subfeatures are selected and aggregated to further dimensionality reduction and feature dimension of the actual operation. Secondly, the information gain rate is used as the weight to optimize the sample Euclidean distance measurement. Based on the proposed measure of the reverse distance influence, the classification decision algorithm of the KNN algorithm is optimized to make the detection technology better. The effect is further improved. The experimental results show that the traditional TAD-KNN algorithm based on average distance and the GR-KNN algorithm that only optimizes the distance definition, the GR-AD-KNN algorithm can not only improve the overall detection performance in the detection of IPv6 network traffic characteristics but also for small groups of samples. As a result, classification has better detection results.

1. Introduction

With the rapid development of computer networks, traditional IPv4 network addresses have gradually been exhausted. To alleviate this problem, the birth of NAT technology has delayed the exhaustion of IPv4 addresses but still has not fundamentally solved the problem of insufficient addresses. Next, the generation of the Internet network protocol IPv6 [1–3] has radically solved this problem, significantly increasing the number of IP addresses that can be used and providing many IP addresses for networks such as the Internet of Things, as shown in Figure 1.

The difference between IPv6 and IPv4 is not only in the number of available addresses. There are significant differences, and the IP datagram headers of the two protocol versions are also different. At the same time, protocols such as ARP have been cancelled in the IPv6 network and replaced by the NDP protocol. Therefore, to a certain

extent, the two versions are still differences in the IP protocol. In terms of security, with the rapid development of IPv6 technology, there are more and more DoS attacks related to it, and the emergence of IPv6 does not wholly eliminate DoS attacks [4–6].

For DoS attacks in the network, the network intrusion detection system (IDS) can detect such hidden network security risks [7]. IDS can find the changes in the data transmitted on the web to find the abnormal situation in the network in time. However, currently in the network, the amount and type of traffic are increasing rapidly. Therefore, IDS based on specific rules may have poor adaptability and more extended rule matching time when detecting DoS attacks in IPv6 networks [8].

Aiming at DoS attacks in IPv6 networks, this paper studies intrusion detection technology and realizes the function of DoS intrusion detection based on IPv6 networks [9]. The specific contributions are as follows:

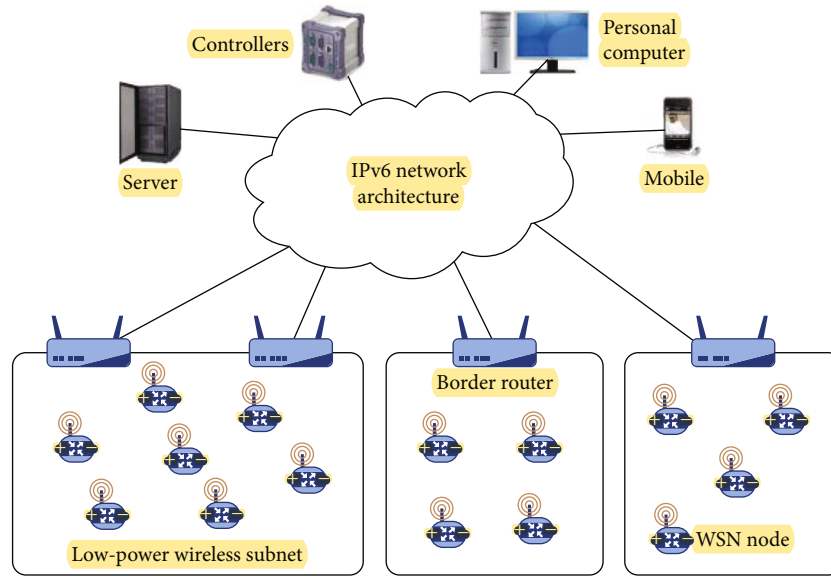


FIGURE 1: IPv6 network architecture.

- (1) Due to the rapid increase of IPv6 traffic, this paper reduces the dimensionality of network traffic characteristics to improve the detection efficiency based on the information gain rate. As a result, it achieves the effect of “dual dimensionality reduction” for discrete features [10, 11]. Furthermore, once the realization of feature selection, discrete type features are partially aggregated, which can further reduce the feature dimension in actual calculations and improve the detection efficiency of DoS attacks in IPv6 networks
- (2) Use the information gain rate as the weight of the feature, and use the idea of offset increment average distance to optimize the decision-making method of the KNN algorithm to improve the stability of the KNN algorithm. For example, the GR-AD-KNN (Information Gain Ratio Average Distance KNN) algorithm is used for IPv6 DoS intrusion detection, which optimizes detection performance and reduces the negative impact of “small group classification disadvantages”

2. DoS Attack on IPv6

With the rapid development of the network scale, the number of devices connected to the Internet has skyrocketed, and the original IPv4 network addresses have gradually dried up [12]. Therefore, the birth of the IPv6 network has solved the problem of insufficient addresses [13], and it is also for the Internet of Things. Moreover, it has laid the foundation for developing other industries that require many network addresses. In recent years, the scale of IPv6 networks has continued to expand [14]. The original purpose was to solve the problem of insufficient addresses. Therefore, IPv6 networks have not fundamentally prevented network attacks from occurring. For

example, in IPv6 networks, DoS attacks are still a relatively common network intrusion attack [15–17].

Traditional network intrusion detection the software Snort can detect DoS attacks. The detection rules in the literature [18] can be supplemented with honeypot technology logs. However, using many specific rules to detect DoS attacks in network traffic will reduce Snort and execution efficiency of intrusion detection software. To solve the problem of feature selection, literature [19] proposed a feature selection framework, using support vector machine (SVM) and particle swarm optimization (PSO), determined the best detection feature, and realized the effect of DoS attack detection on IPv6 networks. In the new IPv6 environment, network traffic is increasing rapidly, and DoS attacks have not disappeared. The amount of IPv6 network traffic is more significant than traditional IPv4, and it is necessary to detect DoS attacks. The time and amount of calculation will also increase. Therefore, detecting DoS attacks in the IPv6 network should pay attention to the detection performance. It is necessary to select essential features to reduce the feature dimension in the detection process as much as possible. Features can be used for attack detection, but the impact of different features in the actual detection process is also high or low. This article should use machine learning methods to detect DoS attacks on IPv6 networks and use a double dimensionality reduction method. Features are selected, and discrete types of subfeatures are filtered and aggregated. At the same time, the weight of different features is reflected through the information gain rate, which is used in DoS attack detection to improve the adaptability and detection efficiency of the detection system [20, 21].

3. Information Gain

The information gain rate originated from c4.5 algorithms is used in the decision tree splitting process [4]. The decision tree algorithm uses the id3 algorithm based on information

gain, but this will make it easier to choose attributes with more values [5]. Therefore, in some cases, it is not appropriate to use information gain as a reference indicator for feature weights. In a decision tree, in general, the attribute with the more significant information gain rate is closer to the root node, and the impact of such characteristics in the classification process is also more critical [22, 23]. Therefore, this paper uses the information gain rate as an essential evaluation index for feature “dual dimensionality reduction” and uses the information gain rate as the weight to improve the distance to improve the effectiveness of the classification algorithm. The information gain rate is based on the original information gain.

4. KNN Algorithm

The KNN algorithm is one of the commonly used algorithms in machine learning. This algorithm has the characteristics of lightweight classification. SVM algorithm and random forest algorithm need to be trained based on samples first. In the network intrusion detection system to detect DoS attacks, this often requires high timeliness. The KNN algorithm with fast response capability does not need to train the classifier before use, so that this algorithm can be better used for DoS intrusion detection. The implementation process of the traditional KNN algorithm is as follows: First, calculate the distance between the point to be measured and all known types of sample points; second, sort according to the space; finally, based on the nearest k sample points, count the number of sample points in each category, and select one. The class with the most significant number is used as the classification result of the topics to be tested. However, for small group sample points, the classification decision-making disadvantages may occur due to the change of k value during the classification process. At the same time, the traditional KNN algorithm has the same number of reasons for the problem of bias in classification decisions [6].

On the other hand, the use of ordinary Euclidean distance to measure the distance between two points cannot reflect the importance of different features to a certain extent. In literature [10], the analytic hierarchy process is used to assign the feature weights, but the analytical hierarchy process may be subject to a certain degree of subjectivity. Literature [11], based on the information gain rate, gives weighting the Euclidean distance feature in the KNN algorithm thought. Therefore, in this research, this paper improves the deficiencies of the KNN algorithm so that the improved algorithm can be better used for DoS intrusion detection in IPv6 networks.

5. Intrusion Detection Algorithm

5.1. Feature Selection and Dimensionality Reduction. Based on IPv6 network traffic, traffic characteristics can be extracted from it and used to describe changes in network traffic. Network traffic characteristics can be divided into discrete features and continuous features according to types. Among them, discrete features can be divided into discrete digital features and type discrete features. However, if only

the original features are selected for feature selection, this is still far from enough. The number of feature dimensions involved in the calculation may also show explosive growth in the actual calculation process. In the execution process of the classification algorithm, the types of discrete features are all. Therefore, it needs to be converted into 0-1 features, which will cause the overall number of dimensions of features to grow rapidly, which will affect the performance of classification and detection to a certain extent. As mentioned before, the traffic in IPv6 networks is growing rapidly, and it should be as accurate as possible to the final. As a result, the actual number of features involved in the calculation is reduced. Therefore, based on IPv6 network traffic characteristics, it is necessary to reduce the original first-level features and reduce the dimensionality of the second-level “type sub-features” in the type discrete features and thus improve the execution efficiency of later classification.

In this paper, the information gain rate is used as the evaluation index of feature importance. Based on the information gain rate, the function of “double dimension reduction” is realized for the feature. For discrete digital features, the information gain rate of the feature can be directly calculated. However, in the continuous type, in calculating the information gain rate of the feature, it is necessary to discredit the continuous feature first and then calculate the information gain rate of the feature [5]. The following process is the discretization method of the continuous feature.

5.2. GR-AD-KNN Algorithm. In-network DoS intrusion attacks, because some attacks occur less frequently, fewer data can be used for training or detection. On the other hand, to improve the performance of IPv6 network traffic DoS intrusion detection, when detecting, a lightweight classification algorithm should be selected to reduce the time and space costs caused by training. Therefore, a lightweight KNN algorithm that does not need to be trained in advance meets the above requirements.

The traditional KNN algorithm has the problem of “small group classification disadvantage.” When the k value is not selected correctly, the algorithm has high sensitivity and poor stability, leading to misjudgments when classifying data of small group types. Therefore, this shortcoming needs to be optimized if you use the KNN algorithm for DoS intrusion detection in an IPv6 network. The original KNN algorithm used the core evaluation indicators to classify samples based on quantity. Although this has a faster detection speed, it brings the problem of “small group classification disadvantage.” In the original KNN algorithm classification process, the classification algorithm believes that all sample points have the same value among the most recent k sample points. Therefore, a large sample size group will negatively impact a small sample size group during classification decision-making. In fact, in the classification process, points with different distances from the sample to be tested should have different values in decision-making. Therefore, this article adopts. The idea of offsetting the average length of the increment optimizes the algorithm of the KNN decision-making part.

On the other hand, in the traditional KNN algorithm, Euclidean distance is usually used as an index to measure the distance between two points. Using the idea of the literature, the information gain rate is used to optimize the Euclidean distance calculation of the algorithm ways to improve the influence of essential features and their subfeatures in classification decision-making.

In brief, under the condition that the distance between the point to be measured and the sample point increases at an equal length, the change in the increment of the reverse influence is no longer a similar increase; the farther the distance from the point to be measured is caused by the distance interval, the more significant the growth of the reverse influence. Therefore, the farther the distance of the sample point is, the greater the increased speed of the reverse influence. This requires the overall consistency of the “behavior” of the sample points involved in the classification decision-making process, because issues with a longer distance will have a more “serious” reverse influence on the classification of this category due to a more significant negative impact. Compared with the traditional ordinary average distance algorithm, the above decision method adds each type of sample point and set the idea of “holistic decision-making.” Researchers are proposing various protocol schemes [24–28] to maintain integrity, confidentiality, and security of the information shared among users and servers.

6. Experiments and Results

The experimental data set selected for DoS intrusion detection in the IPv6 network is derived from the 10% test set, a training set of the KDDCUP99 [29] data set; the normal type samples and the attack type samples related to DoS attacks are selected. The data specified in this data set features can be divided into TCP basic features, TCP content features, and time-based and host-based network traffic features; therefore, this paper uses this data set to test the algorithm’s performance. In addition, through analysis, the number of discrete features in the data set is 9; the number of continuous features is 32. Because the number of samples of some types of attacks in the network is small, in the experiment process, this paper retains all small sample groups; based on the approximate percentage, the approximate ratio is fine-tuned; from different numbers of samples are randomly selected from the large sample group as the data set for this experiment. To verify the classification effect of the algorithm, during the formation of the test set, the sample types that did not exist in the original training set were deleted.

The experiment is mainly divided into two parts. The first part is to realize the double dimensionality reduction of features and calculate the information gain rate of the first-level and second-level features. When calculating the information gain rate of the first-level feature to achieve the dimensionality reduction function, this paper adopts the continuous type. The average value of each feature and discrete feature is used as the filtering threshold. In the secondary non-0-1 discrete subfeature dimensionality reduction and threshold calculation process, only features with

many subfeatures are subjected to dimensionality reduction and aggregation operations. For example, in the above data concentrated, features Service and Flag belong to the category of discrete features, and their subfeatures are both 70 and 11, respectively. Therefore, only Service and Flag are considered.

The dimensionality reduction process of Flag’s subfeatures; and the feature Protocol type only has three subfeatures, so it does not need to participate in the second dimensionality reduction process. The second part of the experiment is to evaluate the performance of the GR-AD-KNN algorithm. In the classification algorithm, in terms of experimental control settings, this article will only compare the GR-KNN algorithm with the weighted optimization of the Euclidean distance and the GR-AD-KNN algorithm. Ten experiments are performed, respectively, and the average F1-Score of the ten experiments is recorded for judgment of the optimization of the algorithm. In terms of the selection of k value, six sets of horizontal control experiments are set up. Finally, to test the overall improvement effect of selecting sample points on the overall improvement of the experimental classification results by comparing the traditional TAD-KNN based on average distance decision-making.

The classification capabilities of the Traditional Average Distance-KNN algorithm and the GR-AD-KNN algorithm are used to count the detection results of attack types with weak detection capabilities to evaluate the improvement and stability of the classification performance of the algorithm. In terms of evaluation indicators, we use the F1-Score indicator to measure the detection performance of the algorithm comprehensively. Among them, the calculation method of the F1-Score indicator is as follows:

$$F1 - score = \frac{Precision * Recall}{Precision + Recall} \quad (1)$$

The experiment designed in Section 1 first preprocessed the experimental data set, thereby transforming 41-dimensional traffic features into 122-dimensional features. By implementing one-level dimensionality reduction, the dimensionality of the features is reduced to 106. Then, we reduce the dimensionality of the subfeatures of Service and Flag. Next, we set the size of the parameter bound_number in the secondary dimensionality reduction process to 5. Finally, the dimension of the feature that participates in the classification calculation can be determined to 36. Information obtained by analysis, the gain rate can be used as the weight of different features. Based on Algorithm 1, the secondary dimensionality reduction of Service and Flag features will generate other aggregated subfeatures of their respective categories, namely, subfeatures service_others and subfeature flag_others. These two features are in Europe. The calculated weight in the distance is obtained by calculating the average value of the information gain rate of the subfeatures whose class is not selected and the information gain rate is nonzero.

This paper conducts a control experiment on the GR-KNN algorithm and the GR-AD-KNN algorithm. It sets up

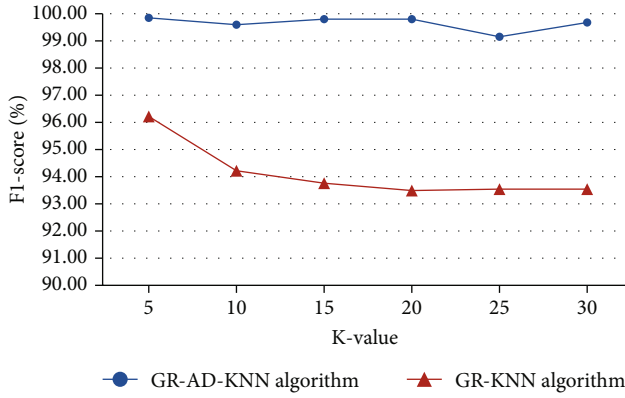


FIGURE 2: GR-KNN algorithm and GR-AD-KNN algorithm detection.

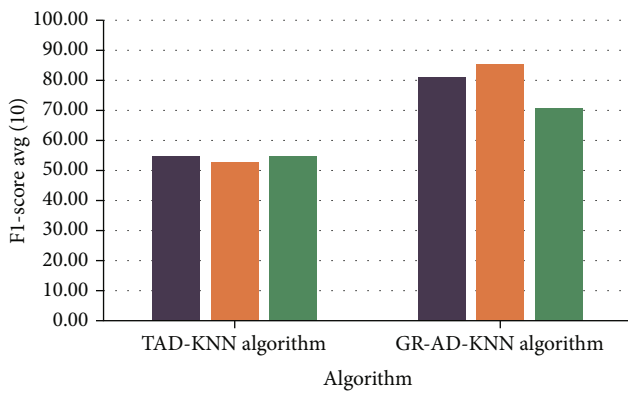


FIGURE 3: Ten average F1-Score detection results of Teardrop attack.

six horizontal control experiments with k , respectively [6, 8, 15, 28, 30, 31], and records the experimental results. At the same time, before the algorithm performance comparison experiment starts, the data in the two data sets are normalized, respectively. The specific experimental comparison results are shown in Figure 2.

It can be seen from Figure 2 that the experimental classification results of the GR-AD-KNN algorithm are better. At the same time, the GR-AD-KNN algorithm is less sensitive to the value of k , thereby reducing the algorithm's strictness of selecting the value of k and reducing the factor the negative impact of excessive sensitivity caused by model parameter adjustment. On the other hand, this paper compares the detection performance of the traditional TAD-KNN algorithm based on the average Euclidean distance and the GR-AD-KNN algorithm. For example, when k is 5, we conducted three rounds of experiments independently, and each round of experiments included ten detection experiments. Finally, the average value of 10 detection results of F1-Score with Teardrop's attack type in each game was counted, as shown in Figure 3.

Through experiments, it can be found that when comparing the performance of the two algorithms to detect the Teardrop attack type, the GR-AD-KNN algorithm has a better detection effect for the Teardrop attack type, which can show that the optimized algorithm can improve the original

detection ability. Therefore, the optimized KNN algorithm for DoS intrusion detection in the IPv6 network has better classification results and detection performance.

7. Conclusion

This article uses the IPv6 network DoS intrusion attack technology as the research background and the information gain rate. To evaluate the quality of network features, the double dimensionality reduction method is used to achieve the effect of feature dimensionality reduction and improve the classification execution efficiency of the later classification algorithm. In terms of classification algorithms, this article will improve the KNN algorithm GR-AD-KNN. The algorithm is used in the field of DoS attack detection. Based on the weight provided by the information gain rate, making different characteristics have different degrees of influence is realized. Based on the idea of the offset increment average distance, the point to be measured is improved. It is recognized that the effect of different long and short distance sample points on decision-making is different, and the algorithm's stability is improved. The problem of "small group classification disadvantages" is alleviated. Therefore, the above research has a better effect on realizing DoS intrusion detection in IPv6 network strong theoretical significance.

Data Availability

The data used to support the findings of this study are available from the author upon request (kusumasyadav0@gmail.com).

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

- [1] A. Altaher, S. Ramadass, and A. Ali, "A dual stack IPv4/IPv6 testbed for malware detection in IPv6 networks," in *2011 IEEE International Conference on Control System, Computing and Engineering*, pp. 168–170, Penang, Malaysia, 2011.
- [2] D. Gu, Y. Xue, D. Wang, Z. Luo, and B. Yan, "Improving IPv6 transition management with IPv6 network virtualization," in *2017 9th International Conference on Advanced Infocomm Technology (ICAIT)*, pp. 95–104, Chengdu, 2017.
- [3] S. Praptodiyono, R. K. Murugesan, R. Budiarto, and S. Ramadass, "Handling transmission error for IPv6 packets over high speed networks," *First International Conference on Distributed Framework and Applications*, vol. 2008, pp. 159–163, 2008.
- [4] R. Kumar and G. Dhiman, "A comparative study of fuzzy optimization through fuzzy number," *International Journal of Modern Research*, vol. 1, 2021.
- [5] I. Chatterjee, "Artificial intelligence and patentability: review and discussions," *International Journal of Modern Research*, vol. 1, pp. 15–21, 2021.

- [6] P. K. Vaishnav, S. Sharma, and P. Sharma, "Analytical review analysis for screening COVID-19," *International Journal of Modern Research*, vol. 1, pp. 22–29, 2021.
- [7] C. -W. Tseng, L. -F. Wu, S. -C. Hsu, and S. -W. Yu, "IPv6 DoS attacks detection using machine learning enhanced IDS in SDN/NFV environment," in *2020 21st Asia-Pacific Network Operations and Management Symposium (APNOMS)*, pp. 263–266, Daegu, Korea (South), 2020.
- [8] A. K. Al-Ani, M. Anbar, A. Al-Ani, and D. R. Ibrahim, "Match-prevention technique against denial-of-service attack on address resolution and duplicate address detection processes in IPv6 link-local network," *IEEE Access*, vol. 8, pp. 27122–27138, 2020.
- [9] J. N. Goel and B. M. Mehtre, "Dynamic IPv6 activation based defense for IPv6 router advertisement flooding (DoS) attack," *IEEE International Conference on Computational Intelligence and Computing Research*, vol. 2014, pp. 1–5, 2014.
- [10] G. Dhiman and V. Kumar, "Spotted hyena optimizer: a novel bio-inspired based metaheuristic technique for engineering applications," *Advances in Engineering Software*, vol. 114, pp. 48–70, 2017.
- [11] G. Dhiman and V. Kumar, "Emperor penguin optimizer: a bio-inspired algorithm for engineering problems," *Knowledge-Based Systems*, vol. 159, pp. 20–50, 2018.
- [12] N. R. Samineni, F. A. Barbhuiya, and S. Nandi, "Stealth and semi-stealth MITM attacks, detection and defense in IPv4 networks," in *2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing*, pp. 364–367, Solan, India, 2012.
- [13] R. K. Murugesan, S. Ramadass, and R. Budiarto, "Increased performance of IPv6 packet transmission over ethernet," in *2009 2nd IEEE International Conference on Computer Science and Information Technology*, pp. 171–175, Beijing, China, 2009.
- [14] R. K. Murugesan and S. Ramadass, "IPv6 address distribution: an alternative approach," in *2010 3rd IEEE International Conference on Broadband Network and Multimedia Technology (IC-BNMT)*, pp. 252–257, Beijing, China, 2010.
- [15] M. Huang, J. Liu, and Y. Zhou, "An improved SEND protocol against DoS attacks in mobile IPv6 environment," *IEEE International Conference on Network Infrastructure and Digital Content*, vol. 2009, pp. 232–235, 2009.
- [16] L. He and K. He, "Efficient memory-bounded optimal detection for GSM-MIMO systems," *IEEE Transactions on Communications*, vol. 69, no. 1, pp. 101–112, 2021.
- [17] L. He and K. He, "Learning-based signal detection for MIMO systems with unknown noise statistics," *IEEE Transactions on Communications*, vol. 69, no. 5, pp. 3025–3038, 2021.
- [18] K. Kishimoto, K. Ohira, Y. Yamaguchi, H. Yamaki, and H. Takakura, "An adaptive honeypot system to capture IPv6 address scans," *International Conference on Cyber Security*, vol. 2012, pp. 165–172, 2012.
- [19] M. Yang and T. Li, "A RDO-PSO algorithm for anycast routing with multi-QoS constraints," in *2009 4th International Conference on Computer Science & Education*, pp. 376–379, Nanning, 2009.
- [20] L. Chen, "Intelligent ubiquitous computing for future UAV-enabled MEC network systems," *Cluster Computing*, 2021.
- [21] L. Chen, "A fog assisted intelligent framework based on cyber physical system for safe evacuation in panic situations," *Computer Communications*, vol. 178, no. 1, pp. 297–306, 2021.
- [22] W. Zhou, "PSO based offloading strategy for cache-enabled mobile edge computing UAV networks," *Cluster Computing*, vol. 2021, no. 24, 2021.
- [23] S. Tang and L. Chen, "Computational intelligence and deep learning for next-generation edge-enabled industrial IoT," *IEEE Trans Network Science and Engineering*, vol. 8, no. 1, pp. 114–125, 2021.
- [24] S. Du and J. Li, "Parallel processing of improved KNN text classification algorithm based on Hadoop," in *2019 7th international conference on information, Communication and Networks (ICICN)*, pp. 167–170, Macao, Macao, 2019.
- [25] H. Song, E. Zhu, and L. Ma, "Design of embedded real-time target tracking system based on KNN algorithm," in *2020 IEEE 9th Joint International Information Technology and Artificial Intelligence Conference (ITAIC)*, pp. 443–446, Chongqing, China, 2020.
- [26] A. A. Bahashwan, M. Anbar, I. H. Hasbullah, Z. R. Alashhab, and A. Bin-Salem, "Flow-based approach to detect abnormal behavior in neighbor discovery protocol (NDP)," *IEEE Access*, vol. 9, pp. 45512–45526, 2021.
- [27] M. A. Lawal, R. A. Shaikh, and S. R. Hassan, "A DDoS attack mitigation framework for IoT networks using fog computing," *Procedia Computer Science*, vol. 182, pp. 13–20, 2021.
- [28] P. Kushwaha, H. Buckchash, and B. Raman, "Anomaly based intrusion detection using filter based feature selection on KDD-CUP 99," in *TENCON 2017 - 2017 IEEE Region 10 Conference*, pp. 839–844, 2017.
- [29] V. Aliksieiev and B. Andrii, "Information analysis and knowledge gain within graph data model," in *2019 IEEE 14th International Conference on Computer Sciences and Information Technologies (CSIT)*, pp. 268–271, 2019.
- [30] H. Sukarman, F. Y. Rizkiyana, and M. F. A. F. Apriyanto, "The design of information system and technology strategy for improving performance of healthcare service with EA3 framework: (case study: summit)," in *2020 International Conference on Information Management and Technology (ICIMTech)*, pp. 788–793, Bandung, Indonesia, 2020.
- [31] M. Soni, G. Dhiman, B. S. Rajput, R. Patel, and N. K. Tejra, "Energy-effective and secure data transfer scheme for mobile nodes in smart city applications," *Wireless Personal Communications*, 2021.