The Asian Journal of Professional and Business Studies, Volume 1, Issue 2 (Dec) 2020, pp. 7-12
https://journal.uptm.edu.my/index.php/ajpbs
e-ISSN 2716-666X, ISSN 2462-1072

Packet Threshold Algorithm Coupled With Machine Learning For DDos Classification Attacks

Mohd Azahari Mohd Yusof[1*], Nor Hafiza Abd Samad[2], Rukhiyah Adnan[3]
[1,2,3]Kolej Universiti Poly-Tech MARA
56100 Kuala Lumpur, Malaysia
Corresponding Author*azahari@kuptm.edu.my

Received	Revised	Accepted	Published
31 Octoberl 2026	20 November 2026	30 November 2026	31 Dec 2026

ABSTRACT

Distributed denial-of-service (DDoS) attacks remain among the most pervasive and disruptive threats to Internet-based services, enabling adversaries to overwhelm organizational servers and render them inaccessible to legitimate users on a global scale. These attacks can be launched remotely and often involve multiple vectors simultaneously, including Slowloris, UDP flood, Smurf, HTTP flood, TCP SYN flood, and ping of death. In response to this challenge, this study proposes a novel detection approach termed the packet threshold algorithm (PTA), integrated with machine learning techniques to effectively distinguish between legitimate traffic and DDoS attacks. Specifically, four classifiers— K-nearest neighbour (KNN), Naïve Bayes, logistic regression, and support vector machine (SVM)—are combined with PTA to enhance detection performance while minimising false positives. The experimental results demonstrate that the PTA-KNN hybrid model outperforms the other configurations, achieving a detection accuracy of 99.83% with a notably low false-positive rate of 0.02%. These findings highlight the effectiveness of PTA-based hybrid models, particularly PTA-KNN, in improving the reliability and accuracy of DDoS attack detection systems.

Keywords: DDoS attack, False positive rate, Detection accuracy, Machine learning

How to Cite:
Moho Yusof, M. A., Abd Samad, N. H. ., & Adnan, R. . (2020). Packet Threshold Algorithm Coupled With Machine Learning For DDOS Classification Attacks. *The Asian Journal of Professional & Business Studies*, *1*(2), 7–12. https://doi.org/10.61688/ajpbs.v1i2.50

1. INTRODUCTION

Currently, computer networks are essential and widely used by users worldwide. They provide many functions to network users, including information exchange, even when they are in different places. Computer networks are formed by combining several devices to form several types of networks, such as local area networks, metropolitan area networks, wide area networks, and wireless networks (Caulfield and Fielder 2015). However, computer networks are often interrupted by several network attacks, including Distributed Denial of Service (DDoS) attacks.

DDoS attacks prevent users from accessing network systems, even if they are legitimate users (Azahari Mohd Yusof, Hani Mohd Ali, & Yusof Darus, 2018). Usually, attackers use botnets to launch DDoS attacks, in which the botnet helps the DDoS attack proceed more smoothly. There are three categories of DDoS attacks based on (Gadelrab, Elsheikh et al. 2018), the first category is protocol attack, followed by application layer attack, and the third category is volume-based attack. TCP SYN floods, Smurf, and Ping of Death are three types of DDoS attacks in the category of protocol attacks. An attacker launches a TCP SYN flood by sending a large number of SYN requests to the target server simultaneously to keep the target server inoperable (Kolahi, Alghalbi et al. 2014). Attackers build Smurf attacks by sending large amounts of ICMP packets to all broadcast addresses of a target server, where the target server fails to respond to all requests (Sandeep and Rajneet 2014). The Ping of Death occurs when an attacker attempts to override a target server by sending more than 65,535 bytes of ICMP packets (Gunasekhar, Rao, Saikiran, & Lakshmi, 2014). Two examples of DDoS attacks in the application layer attack category are the zero-day attack and Slowloris, where the zero-day attack was created by the attacker to avoid software developers fixing the defects that have been detected in the software that has been developed (Singh, Joshi et al. 2017). Slowloris is a tool used by attackers to disable a target server through a single computer by sending multiple HTTP partial requests consistently (Calvert & Khoshgoftaar, 2019). Another two DDoS attacks, ICMP flood and UDP flood, have been considered as volume-based attacks. Attackers can turn off a target server by generating an ICMP flood, where they send large amounts of ICMP packets to that target server (Alqahtani, Balushi et al. 2014). In addition, attackers can also send multiple UDP packets to generate a UDP flood to disrupt target server stability (Badis, Doyen, & Khatoun, 2014).

We present a technique for detecting normal and DDoS packets, including Smurf, UDP flood, Ping of Death, and TCP SYN flood attacks, using our proposed algorithm called the Packet Threshold Algorithm (PTA). Although several types of DDoS attacks can be generated by attackers from anywhere in the world, our study focuses on the four types of DDoS attacks mentioned for a few specific reasons. According to Arora and Dalal (2019), these four types of DDoS attacks are the most popular types of attacks launched by attackers at any given time because DDoS has a very simple concept: generating a large amount of traffic to the target server. When a DDoS attack is successful, it is extremely difficult to stop, unless the attacker becomes too tired to continue the attack on the target server. Most importantly, PTA is combined with four machine learning models–KNN, Naïve Bayes, logistic regression, and SVM–to compare them in terms of detection accuracy and false positive rate.

This paper is organised into five main sections. Section 2 presents some strengths and weaknesses found in previous studies. These are related to DDoS attack detection techniques. The methodology and evaluation in Section 3 are designed to describe several phases of our study, including the measurement parameters used to obtain the results. The results and discussion are presented in Section 4, and the conclusion is presented in Section 5.

2. LITERATURE REVIEW

DDoS attacks are intended to disable the target server so that it is not accessible to anyone at that time. Therefore, most organisations need to have specific techniques to address DDoS issues in their computer network environments. Several solutions have been developed by previous researchers. It includes the least squares support vector machine designed by Sahi et al. (2017), where the technique has loaded a function named CS_DDoS. It is a classifier that determines whether incoming packets are normal or DDoS packets. The classifier contains two important stages: the detection stage and the prevention stage. The detection stage determines whether the packet present in the cloud is a normal packet or a TCP

SYN flood. Meanwhile, the prevention stage will act to records and blacklists the source IP if the incoming packet is detected as a DDoS attack.

Density-based spatial clustering and application with noise technique was formed by (Al-Mamory & Algelal, 2017), which is based on the concept of entropy. They used the DARPA dataset to perform experimental activities to verify the accuracy of their techniques. They compared the technique with other techniques, such as k-means, FCM, and GKFCM, to verify the strength of their technique in terms of detection accuracy and false positive rate. In addition, an artificial neural network technique was designed by (Peraković, Periša et al. 2016) to determine whether incoming packets are DDoS or non-network attacks. They conducted a simulation to verify the technique in terms of detection accuracy. All packets that were classified as DDoS attacks were migrated into a new dataset. They began the simulation using the MATLAB tool by applying several network packets from four different datasets. Another technique is the hop-count filter proposed by (Li, Yang et al. 2015), which is useful for detecting clean packets or DDoS attacks. The technique is loaded with the packet threshold algorithm, in which if the incoming packet exceeds the specified packet threshold, the packet is known as a DDoS attack.

Unfortunately, all the techniques mentioned above have two unresolved problems: the false positive rate and detection accuracy. The high false positive rate of existing techniques can be attributed to the fact that they are unable to differentiate between clean packets and DDoS traffic effectively. In addition, some techniques can achieve a high detection rate (for specific network traffic); however, they have a 0.9% false positive rate, which is considered high. Moreover, some techniques mistakenly detect two different types of DDoS attacks; for example, UDP packets are detected as TCP packets because of flow inequality. This renders the technique ineffective in detecting different types of DDoS attacks based on attack behaviour. As a major conclusion, the problem of a high false positive rate will have a severe impact on the detection accuracy of a technique developed. In addition, some of these techniques can only detect DDoS attacks in general, without focusing on specific types of DDoS attacks, such as TCP SYN floods, Smurf, and Ping of Death. The detection of a specific type of DDoS attack is important because it can be easily launched to disrupt server activity using different packet types, such as UDP, ICMP, or TCP.

3. METHODOLOGY

To support this study, we need to consider four important phases, as shown in Figure 1. Each of these phases must be completed to produce a successful study based on the objectives set out in Section 1.

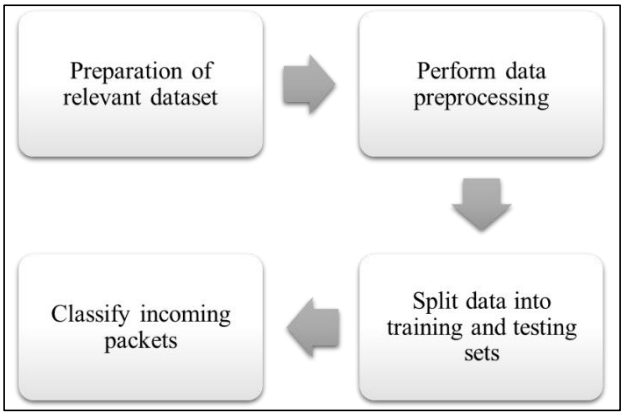

Figure 1. Research Methodology

The first phase of our study was the preparation of relevant datasets containing several incoming packets that had been captured; these are open source datasets, as presented in Table 1. Although several open datasets are available, the datasets we used are particularly suitable for our study because the recorded incoming packets consist of normal and DDoS packets. Moreover, we focused on five types of packets: normal, Smurf, UDP flood, Ping of Death, and TCP SYN flood packets.

Table 1. Sample of DDoS Dataset

Source Address	Destination Address	Packet Type	Packet Size	…	Packet Class
192.168.10.87	192.168.10.78	ICMP	65,535		Ping of Death
192.168.10.97	192.168.10.124	UDP	1,192		UDP flood
192.168.10.124	192.168.10.97	ICMP	1,540		Smurf
192.168.10.54	192.168.10.87	TCP	55		Normal
192.168.10.78	192.168.10.65	TCP	77		TCP SYN flood

In the second phase, data preprocessing is performed, which involves two important steps: data cleaning and data reduction. We used the data cleaning method to ensure that the data stored in the dataset was accurate and consistent without any error. Subsequently, we implemented a data reduction method in which we selected important data in our study to ensure that the simulation ran smoothly. Both of these methods are important to our study because the originally obtained data were inconsistent, incomplete, and noisy.

After completing the data preprocessing activities, we split the data into training and testing sets. We provided 80% of the data for the training set and the remaining 20% for the testing set. There are 240,000 samples in the dataset used in our study. This means that there were 192,000 samples in the training set and 48,000 samples in the testing set.

The final phase to complete this study is to classify incoming packets, whether they are normal or DDoS packets. We propose a technique called the Packet Threshold Algorithm (PTA), which is combined with four machine learning techniques: Naive Bayes (NB), K-nearest neighbour (KNN), logistic regression (LR), and support vector machine (SVM), as shown in Figure 2. The PTA determines the type of packet class that will be sent to the server, including normal packets, ping of death, UDP flood, Smurf, and TCP SYN flood. Normal packets are detected if the packet type is TCP, ICMP, or ICMP sent to the server, not exceeding 60 packets per second. The PTA detects a ping of death if the ICMP packet received by the server exceeds 65,535 bytes per second. Smurf can be detected by the PTA if the ICMP packet received by the server exceeds 60 and is less than 65,535 bytes per second. Additionally, a UDP flood is detected by the PTA if the UDP packet size received by the server exceeds 60 packets per second.

We apply two performance metrics to our proposed technique: detection accuracy and false positive rate. The detection accuracy is used to determine the correct number of detected packets. The false positive rate is used to determine the number of normal packets that are inaccurately detected as DDoS packets or DDoS packets that are inaccurately detected as DDoS packets.

```
if[(ps < 60) & (pt == 'tcp') | (pt == 'udp') | (pt == 'icmp')]:
    print(ddos_df.iloc[[0], [-1]])
    print('Action: pass packets')

if[(ps >= 60) & (pt == 'tcp')]:
    print(ddos_df.iloc[[159], [-1]])
    print('Action: drop packets')

if[(ps >= 60) & (pt == 'udp')]:
    print(ddos_df.iloc[[2], [-1]])
    print('Action: drop packets')

if[(ps >= 65535) & (pt == 'icmp')]:
    print(ddos_df.iloc[[25], [-1]])
    print('Action: drop packets')

if[(ps >= 60) & (ps < 65535) & (pt == 'icmp')]:
    print(ddos_df.iloc[[17], [-1]])
    print('Action: drop packets')
```

Figure 2. Packet Threshold Algorithm (PTA)

4. FINDINGS AND DISCUSSION

Referring to Table 2, it shows the results obtained in our study. PTA-KNN achieved 9 detection accuracy of 99.83 %, which is the highest percentage among the four techniques considered, with only a 0.02% false-positive rate. A total of 47,920 packets were successfully detected, including 42,914 normal packets, 133 Ping of Death, 393 Smurf, 88 TCP SYN flood, and 4,392 UDP flood packets. The second-best technique is PTA-SVM, which achieved 9 detection accuracy of 99.63% with a 0.02% false-positive rate. This technique successfully detected 47,821 packets, including 42,916 normal packets, 133 Ping of Death, 298 Smurf, 85 TCP SYN flood, and 4,389 UDP flood packets. Next, the third useful technique is PTA-LR, which it has successfully detected 42,916 normal packets, 133 Ping of Death, 220 Smurf, 84 TCP SYN flood and 4,249 UDP flood as the packet itself. Hereby, the technique has achieved 99.17% detection accuracy with 0.26% false positive rate. Meanwhile, PTA-NB achieved a detection accuracy of 98.68% with a 1.08% false-positive rate. This technique successfully detected 47,367 packets, including 42,643 normal packets, 133 Ping of Death, 299 Smurf, 83 TCP SYN flood, and 4,209 UDP flood packets.

Table 2: Performance Comparison of PTA Coupled With Four Machine Learning

Technique	Detection Accuracy	False Positive Rate	Packet Class				
			Normal	Ping Of Death	SMURF	TCP SYN FLOOD	UDP FLOOD
PTA-SVM	99.63%	0.02%	42,916	133	298	85	4,389
PTA-NB	98.68%	1.08%	42,643	133	299	83	4,209
PTA-LR	99.17%	0.26%	42,916	133	220	84	4,249
PTA-KNN	99.83%	0.02%	42,914	133	393	88	4,392

5. CONCLUSION

We designed the PTA technique to detect five types of incoming packets based on the specified packet threshold and packet type. Most importantly, the technique has been combined into four machine learning techniques, they are KNN, Naïve Bayes, Logistic Regression and SVM. The technique was tested to determine the percentage of detection accuracy and false positive rate, and it was found that the PTA-KNN technique is the best among the other three techniques.

6. ACKNOWLEDGEMENT

The authors affirm that this study was conducted independently without financial support, external funding, or institutional sponsorship. No grants or monetary assistance were received for the completion of the research or preparation of this manuscript. In addition, artificial intelligence tools were utilized solely to enhance language clarity and improve grammatical accuracy, without influencing the conceptual development or interpretation of the study.

REFERENCES

Al-mamory, S. O., & Algelal, Z. M. (2017). A modified DBSCAN clustering algorithm for proactive detection of DDoS attacks. *2017 Annual Conference on New Trends in Information & Communications Technology Applications (NTICT)*.

Alqahtani, S. M., Balushi, M. A., & John, R. (2014). An intelligent intrusion detection system for cloud computing (SIDSCC). *2014 International Conference on Computational Science and Computational Intelligence.*

Arora, S., & Dalal, S. (2019). DDoS attacks simulation in cloud computing environment. *International Journal of Innovative Technology and Exploring Engineering (IJITEE), 9*(1), 414–417.

Azahari Mohd Yusof, M., Hani Mohd Ali, F., & Yusof Darus, M. (2018). Detection and defense algorithms of different types of DDoS attacks. *International Journal of Engineering and Technology, 9*(5), 410–444. https://doi.org/10.7763/ijet.2017.v9.1008

Badis, H., Doyen, G., & Khatoun, R. (2014). Understanding botclouds from a system perspective: A principal component analysis. *2014 IEEE Network Operations and Management Symposium (NOMS)*.

Calvert, C., & Khoshgoftaar, T. M. (2019). Impact of class distribution on the detection of slow HTTP DoS attacks using big data. *Journal of Big Data, 6*, 1–18.

Caulfield, T., & Fielder, A. (2015). Optimising time allocation for network defence. *Journal of Cybersecurity, 1*(1), 37–51.

Gadelrab, M., Elsheikh, M., Ghoneim, M., & Rashwan, M. (2018). BotCap: Machine learning approach for botnet detection based on statistical features. *International Journal of Communication Networks and Information Security, 10*, 563–579.

Gunasekhar, T., Rao, K. T., Saikiran, P., & Lakshmi, P. (2014). A survey on denial of service attacks. *International Journal of Computer Science and Information Technologies*.

Kolahi, S. S., Alghalbi, A. A., Alotaibi, A. F., Ahmed, S. S., & Lad, D. (2014). Performance comparison of defense mechanisms against TCP SYN flood DDoS attack. *International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*.

Li, C., Yang, J., Wang, Z., Li, F., & Yang, Y. (2015). A lightweight DDoS flooding attack detection algorithm based on synchronous long flows. *2015 IEEE Global Communications Conference (GLOBECOM)*.

Peraković, D., Periša, M., Cvitić, I., & Husnjak, S. (2016). Artificial neuron network implementation in detection and classification of DDoS traffic. *2016 24th Telecommunications Forum (TELFOR)*.

Sahi, A., Lai, D., Li, Y., & Diykh, M. (2017). An efficient DDoS TCP flood attack detection and prevention system in a cloud environment. *IEEE Access, 5*, 6036–6048.

Sandeep, & Rajneet. (2014). A study of DoS & DDoS – Smurf attack and preventive measures. *International Journal of Computer Science and Information Technology Research*.

Singh, U., Joshi, C., & Singh, S. (2017). ZDAR system: Defending against the unknown. *International Journal of Computer Science and Mobile Computing, 5*(12), 143–149.