ICAR '21

INTERNATIONAL CONFERENCE
OF CROSS-DISCIPLINARY
ACADEMIC RESEARCH 2021

Organizer :

KUPTM
KOLEJ UNIVERSITI POLY-TECH MARA KUALA LUMPUR
DKU033(W)

Co-organizer :

Institute for Management and Business Research (IMBRe)
Universiti Utara Malaysia

UNIVERSITI SAINS MALAYSIA

UNIVERSITY OF MALAYA

UniKL
UNIVERSITI KUALA LUMPUR

icar2021.kuptm.edu.my

e ISBN 978-967-26577-0-5

e-ISBN 978-967-26577-0-5

PACKET THRESHOLD ALGORITHM (PTA) COUPLED WITH MACHINE LEARNING FOR DDOS ATTACK DETECTION

*Mohd Azahari Mohd Yusof[1]
azhari@kuptm.edu.my
Nor Hafiza Abd Samad[2]
hafiza@kuptm.edu.my
Nor Shamshillah Kamarzaman[3]
shilla@kuptm.edu.my
Nurshafinas Roslan[4]
shafinas@gapps.kptm.edu.my
Rukhiyah Adnan[5]
rukhiyah@kuptm.edu.my

*Corresponding author

Faculty of Computing & Multimedia,
Kolej Universiti Poly-Tech MARA Kuala Lumpur, Malaysia[1,2,3,4,5]

ABSTRACT

Today, the Internet world is burdened with various threats, where is generated by attackers all over the world. One of the Internet threats is DDoS attacks. DDoS attacks can deny access made by anyone, including authorised users, to a system. There are several types of DDoS attacks that an attacker can generate. They include UDP flood, HTTP flood, Slowloris, TCP SYN flood and ICMP flood. This paper is prepared to propose a technique to detect packets, whether normal packets or DDoS attacks. This technique is called Packet Threshold Algorithm (PTA), where it is combined with several machine learning techniques for packet classification. The PTA is coupled with Support Vector Machine (PTA-SVM), K-Nearest Neighbor (PTA-KNN), Logistic Regression (PTA-LR) and Naïve Bayes (PTA-NB). The combination of these techniques is able to distinguish five packets that have been generated. They are normal packet, Ping of Death, TCP SYN flood, Smurf and UDP flood. All techniques were tested to look at detection accuracy and false-positive rate. Hence, the best technique is based on the highest percentage of detection accuracy with a low false-positive rate. Thus, our study found that PTA-KNN is the best technique based on the achievement of 99.83% detection accuracy with a 0.02% false-positive rate compared to the achievement of the other three techniques.

Keywords: Packet Threshold Algorithm, Machine Learning, Detection Accuracy, False Positive Rate.