SPECTRAL ANALYSIS OF DDOS PRE-ATTACK WITH FOURIER TRANSFORM

By

Sachlany Kasman

21951016

MASTER'S DEGREE

in

MASTER OF INFORMATION TECHNOLOGY

FACULTY OF ENGINEERING AND INFORMATION TECHNOLOGY

SWISS GERMAN UNIVERSITY
The Prominence Tower
Jalan Jalur Sutera Barat No. 15, Alam Sutera
Tangerang, Banten 15143 - Indonesia

February 2021

SPECTRAL ANALYSIS OF DDOS PRE-ATTACK WITH FOURIER TRANSFORM

By

Sachlany Kasman

21951016

MASTER'S DEGREE

in

MASTER OF INFORMATION TECHNOLOGY

FACULTY OF ENGINEERING AND INFORMATION TECHNOLOGY

SWISS GERMAN UNIVERSITY
The Prominence Tower
Jalan Jalur Sutera Barat No. 15, Alam Sutera
Tangerang, Banten 15143 - Indonesia

January 2021

STATEMENT BY THE AUTHOR

I hereby declare that this submission is my own work and to the best of my knowledge, it contains no material previously published or written by another person, nor materials which to a substantial extent has been accepted for the award of any other degree or diploma at any educational institution, except where due acknowledgment is made in the thesis.

Sachlany Kasman

Student Date

Approved by:

Dr. Ir. Lukas, MAI, CISA, IPM

Thesis Advisor Date

Dr. Charles Lim, BSc., MSc.

Thesis Co-Advisor Date

Maulahikmah Galium, S.Kom, M.Sc, PhD

Dean of Faculty of Engineering and Information Technology Date

ABSTRACT

SPECTRAL ANALYSIS OF DDOS PRE-ATTACK WITH FOURIER TRANSFORM

By

Sachlany Kasman
Dr. Ir. Lukas, MAI, CISA, IPM , Advisor
Dr. Charles Lim, BSc., MSc. , Co-Advisor

SWISS GERMAN UNIVERSITY

Analyzing Distributed Denial of Service (DDoS) pre-attack and anomaly detection in Machine Learning (ML) has profoundly popular in academic research, intrusion prevention system, and DDoS detection. ML algorithms, computer vision, and digital signaling processing in the cybersecurity field have improved significantly. As a result, specific technique and method for detecting and analyzing attack have introduced. For this reason, we propose a technique of digital signaling processing and ML for detecting attack of DDoS. Further, leveraging Fourier Transform in ML computation effort reduces computational cost and complexity for deploying effective and efficient DDoS Defense. Spectral analysis is a method to discretely quantify spectrum and frequencies for extracting attack features from the data-set. This research proposes a technique and methodology that leverages filtering, convolution, spectral analysis with Fourier Transform that distinguish multi-classes attack into the taxonomy of NSL-KDD data-set. Our research achieves 98-99% accuracy compared to previous work. Further, the techniques help security researchers and analysts reduce ever-evolved adversaries' threats to develop an effective defensive strategy towards future attacks.

Keywords: Fast Fourier Transform, Discrete Fourier Transform, FFT, DFT, Spectrogram, Spectral Analysis, Digital Signaling Process, Convolution.

DEDICATION

I would like to thank God, my wife, daughter and son for letting me conducting this research.

ACKNOWLEDGEMENT

First and foremost, I would like to express my sincere gratitude to Dr. Ir. Lukas, MAI, CISA, IPM and Dr. Charles Lim, BSc., MSc. as my thesis advisor for continuous support of my Master's of Information Technology study and research, for their patient, motivation, enthusiasm, and immense of knowledge. Their guidance helped me all the time of research and writing of the thesis. I could not having a better advisor and co-advisor as well as mentor for my Master's study.

Beside my advisor and co-advisor, I would like to thank the rest of my thesis committee for their encouragement, insightful comments, and challenging questions.

I also thank to MIT Batch-25 fellow students in Swiss German University MIT that were tirelessly available for discussion, sharing thoughts, experiences, and even spent time together during the COVID-19 pandemic.

Last but not the least, I would like to thank my beloved family; my wife Maria Ulfa, my daughter Chinta Kurnia Putri, my son Azreel Mugaddim Jorell for supporting me throughout my life and study.

Table of Contents

List of Figures

List of Tables