

**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

SWISS GERMAN UNIVERSITY

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

Sachlany Kasman

ABSTRACT

SPECTRAL ANALYSIS OF DDOS PRE-ATTACK WITH FOURIER TRANSFORM

By

Sachlany Kasman

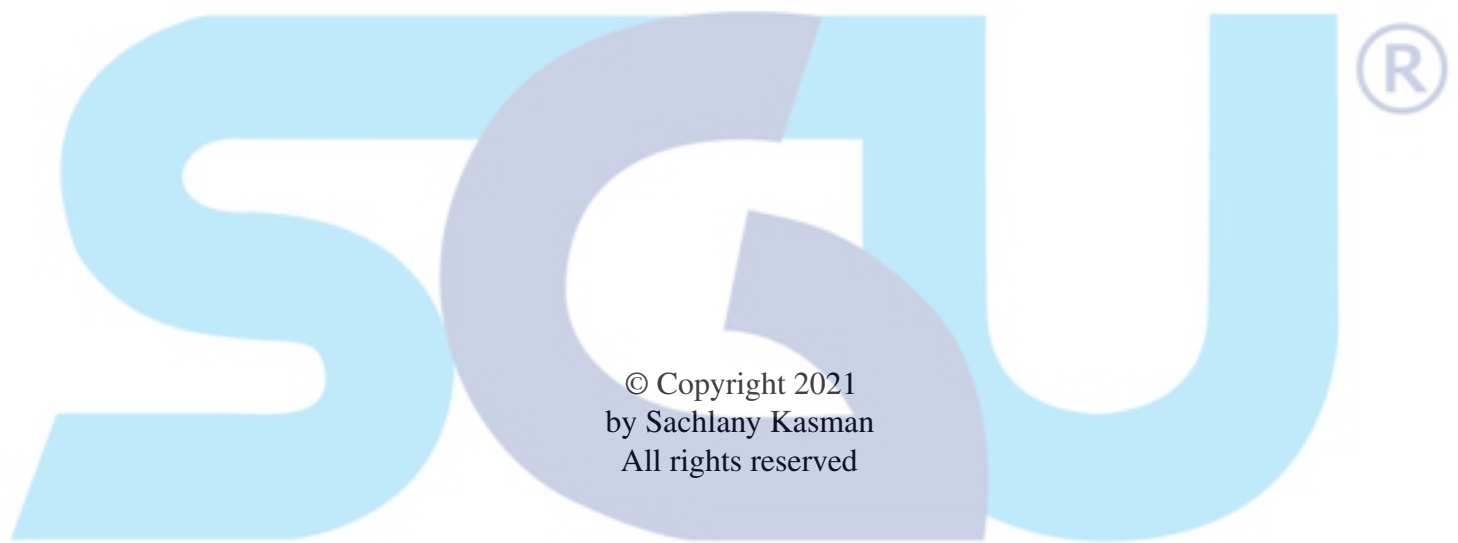
Dr. Ir. Lukas, MAI, CISA, IPM , Advisor

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.



SWISS GERMAN UNIVERSITY

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.



SWISS GERMAN UNIVERSITY

Table of Contents

	Page
STATEMENT BY THE AUTHOR	1
ABSTRACT	2
DEDICATION	4
ACKNOWLEDGEMENT	5
TABLE OF CONTENTS	8
LIST OF FIGURES	9
LIST OF TABLES	10
1. INTRODUCTION	11
1.1 Background	11
1.2 Problem Statement	12
1.3 Research Objective	14
1.4 Research Question	15
1.5 Scope and Limitation	16
1.6 Significance of Study	16
1.7 Thesis Structure	17
2. LITERATURE REVIEW	18
2.1 Network Anomaly	18
2.2 DDoS Attacks	18
2.3 Challenges in DDoS Attack Detection	19
2.4 Digital Signal Processing	19

2.5	Fast Fourier Transform (FFT)	20
2.6	Definition of the Fourier Transform	21
2.7	Discrete Fourier Transform	22
2.8	Related Works	23
3.	RESEARCH METHODS	28
3.1	Research Framework	28
3.1.1	Data Processing and Analysis	29
3.2	Algorithm of Framework	30
3.3	Data Pre-processing	30
3.3.1	NSL-KDD Data Set	31
3.3.2	Label Encoding	31
3.3.3	One-Hot-Encoding to Categorical Features	31
3.3.4	Split Train Test-set	32
3.3.5	Split data-frame into X and Y	33
3.3.6	Feature Selection	33
3.4	Frequency-Domain Analysis	34
3.4.1	Discrete Fourier Transform (DFT)	35
3.4.2	Fast Fourier Transform (FFT)	36
3.5	Signal Analysis	37
3.5.1	Low Pass Filter	37
3.5.2	Spectral Analysis	38
3.6	Performance Evaluation and Validation	39
4.	RESULTS AND DISCUSSIONS	41
4.1	Experiment setup	41
4.1.1	Hardware setup	41
4.1.2	Software Setup	41
4.2	Dataset Input	42
4.3	Data Pre-processing	42
4.4	Exploratory Data Analysis	43
4.4.1	Analysis and Validation	43
4.4.2	Attack Signal Extraction	43

4.4.3	Spectral Analysis	44
4.4.4	Low Pass Filtering	46
4.4.5	Spectral Experiment Results	47
4.4.6	Performance Result Comparison	48
5.	CONCLUSIONS AND RECOMMENDATIONS	51
5.1	Conclusions	51
5.2	Recommendations	51
5.3	Future Works	51
	REFERENCES	59
	GLOSSARY	60



SWISS GERMAN UNIVERSITY

List of Figures

1.1	Significant DDoS Attack size reported for Service Providers	13
1.2	Motivation behind DDoS Attacks	14
2.1	Cisco Annual Internet Report, 2018-2023	20
2.2	Confusion Matrix for performance measurement	23
2.3	Confusion Matrix	23
3.1	Research Framework	28
3.2	Convolution Neural Network - CNN	40
4.1	Confusion Matrix DoS, Probe, R2L, and U2R	45
4.2	Train Data Spectrum	45
4.3	Test Test Spectrum	46
4.4	Original Signal	46
4.5	Train Data Spectrum	47
4.6	Test Test Spectrum Plot	47
4.7	Original FFT Signal Analysis	48
4.8	Filtered FFT Signal Analysis	48
4.9	Train Image Data	49
4.10	Test Image Data	50

List of Tables

2.1	Related Works	26
2.2	Data-set related works	27
3.1	Train and test data shapes	31
3.2	Train and test data shapes	31
4.1	Hardware Configuration	41
4.2	Software Configuration	42
4.3	Train and test shapes	42
4.4	Performance analysis and validation	44
4.5	Recursion Feature Elimination (RFE) best features	49

SWISS GERMAN UNIVERSITY