

CONTENTS

	PAGE
ENGLISH ABSTRACT	i
THAI ABSTRACT	ii
ACKNOWLEDGEMENTS	iii
CONTENTS	iv
LIST OF TABLES	vi
LIST OF FIGURES	viii
LIST OF ABBREVIATIONS	ix
 CHAPTER	
1. INTRODUCTION	1
1.1 Motivation	
1.2 Objective and Research Scope	1
1.3 General Approach	2
1.4 Research Contribution	2
1.5 Report Overview	2
 2. LITERATURE SURVEY AND BACKGROUND STUDY	3
2.1 Literature Survey	3
2.1.1 IDS for Offline Data	3
2.1.2 IDS for Online Data	8
2.2 Background Study	15
2.2.1 Artificial Intelligence	15
2.2.2 Machine Learning	15
2.2.3 Fuzzy Logic	16
2.2.4 Fuzzy Rule	17
2.2.5 Genetic Algorithm (GA)	17
2.2.6 KDD99 Dataset	19
 3. RESEARCH METHODOLOGY	22
3.1 Preprocessing Phase	23
3.2 Training Phase	24
3.2.1 Fuzzy Logic Algorithm	24
3.2.2 Genetic Algorithm	25
3.2.3 String Encoding	26
3.2.4 Fuzzy Genetic Algorithm	26
3.3 Detecting Phase	28
3.3.1 Data Normalization	28
3.3.2 Data Classification	28
3.3.3 Evaluation Criteria	28
3.4 Simulation Tools	29
 4. EXPERIMENTAL RESULTS AND DISCUSSION	30
4.1 Offline Detection	30
4.1.1 Fuzzy GA with KDD99 Dataset	30
4.1.1.1 One-Rule	31
4.1.1.2 Two-Rule	33

CONTENTS (Cont.)	PAGE
4.1.2 Fuzzy GA with Real-time Dataset	34
4.1.2.1 One-Rule	34
4.1.2.2 Two-Rule	35
4.1.3 Fuzzy GA with Unknown Detection	36
4.1.4 Intrusion Detection with Various Approaches	37
4.2 Online Detection	40
4.2.1 Experimental Setting	40
4.2.2 Experimental Result	40
5. CONCLUSION	41
REFERENCES	42
CURRICULUM VITAE	45

LIST OF TABLES

TABLE	PAGE
2.1 Distribution of different classes in training and testing datasets	5
2.2 Detection rate with different numbers of KDD99 features	5
2.3 Data record taken for training and testing in	6
2.4 Summary of offline IDS	7
2.5 Real-time detection rate of RT-UNNID using SOM ART-1 and ART-2	8
2.6 Attack name (left) and feature name in proposed approach (right)	9
2.7 Threshold for attacking graphlets	11
2.8 Feature list of real-time network IDS for large-scale attacks based on incremental mining approach	12
2.9 Features in online dataset	13
2.10 Attack names in the dataset	14
2.11 Features used in NIDSs	14
2.12 Summary of online IDS	15
2.13 Number of each attack in 10% version file of KDD99 dataset	19
2.14 Forty one features of KDD99 dataset	20
3.1 Twelve essential features in pre-processed data	23
3.2 Attack type and simulation tools	29
4.1 Number of records of each attack in KDD99 dataset (A-full version and B-10% version containing approximately 5,000,000 records and 200,000 records respectively)	30
4.2 Experimental result from Fuzzy Genetic Algorithm with KDD99 dataset	31
4.3 Detection rule of KDD99 dataset obtained from training process	31
4.4-1 Experimental results of Fuzzy Genetic Algorithm with KDD99 dataset	32
4.4-2 Experimental results comparing different numbers of features used for Back attack and Pod attack	32

LIST OF TABLES (Cont.)

TABLE	PAGE
4.5 Experimental results of Fuzzy Genetic Algorithm with KDD99 dataset	33
4.6 DoS rule with KDD99 dataset obtained from Dos training process	33
4.7 Probe rule with KDD99 dataset obtained from Probe training process	34
4.8 Experimental results of Fuzzy Genetic Algorithm with real-time dataset	34
4.9 Detection rule of real-time dataset obtained from training process	34
4.10 Experimental results of Fuzzy Genetic Algorithm with real-time dataset	35
4.11 Detection rate of real-time dataset from using two rules of Fuzzy Genetic Algorithm	36
4.12 Probe rule of real-time dataset from training process	36
4.13 DoS rule of real-time dataset from training process	36
4.14 Seven test cases with unknown data types	37
4.15 Experimental results with unknown attack type with real-time dataset	38
4.16 Number of KDD99 data records in training dataset and testing dataset	38
4.17 Results from various detection algorithms	39
4.18 Experimental result from CPE network environment	40

LIST OF FIGURES

FIGURE	PAGE
1.1 Network environments and intrusion detection system	1
2.1 Optimizing fuzzy K-means for network anomaly framework	4
2.2 Block diagram of proposed IDS from using K-means, fuzzy neural network and SVM algorithm	6
2.3 RT-UNNID systems	8
2.4 DoS attack graphlets	10
2.5 CPU initialized for LD ² (left) and snort (right)	10
2.6 Memory usage for LD ² (left) and snort (right)	10
2.7 Architecture of NIDS	11
2.8 Network topology for simulation	12
2.9 Similarity degradation during flooding for DoS.Win32.IIS	12
2.10 Boolean logic and fuzzy logic	16
2.11 Trapezoidal membership function	17
2.12 Fuzzy rule	17
2.13 Example of chromosome	17
2.14 Genetic algorithm crossover multi values	18
3.1 Real-time detection model	22
3.2 Trapezoidal fuzzy set {a=2, b=3, c=4, d=5}	24
3.3 Fuzzy encoding for each feature {a=2, b=3, c=4, d=5}	26
3.4 Encoding string	26
3.5 Fuzzy genetic algorithm pseudo code	27
4.1 Real-time network environments	40

LIST OF ABBREVIATIONS

AI	Artificial Intelligent
ANN	Artificial Neural Network
ART	Adaptive Resonance Theory
DoS	Denial of Service
DR	Detection Rate
FA	False Alarm
HIDS	Host-Based Intrusion Detection System
IDPS	Intrusion Detection and Prevention System
IDS	Intrusion Detection System
KDD99	International Conference on Knowledge Discovery and Data Mining 1999
LD2	Lightweight Detection System
MAWI	Measurement and Analysis on WIDE Internet
METROSEC	Metrology for Security and Quality of Service
MOGFIDS	Multi-Objective Genetic Fuzzy Intrusion Detection System
N/A	Not Available
NIDS	Network-Based Intrusion Detection System
Probe	Port Scan
PSO	Particle Swarm Optimization
R2L	Remote to Local Attack
RT-UNNID	Real-Time Unsupervised Neural-Net-Based Intrusion Detector
SOM	Self Organizing Maps
SVM	Support Vector Machine
TN	True Negative Rate
U2R	User to Root

LIST OF ABBREVIATIONS (Cont.)

UI	User Interface
UNN-Engine	Unsupervised Neural-Net-Based Engine
WIDE	Widely Integrated Distributed Environment
UDP	User Datagram Protocol
TCP	Transmission Control Protocol
ICMP	Internet Control Message Protocol
ARP	Address Resolution Protocol
IP	Internet Protocol