



Cairo University

# COMPROMISED NODE DETECTION USING HIERARCHICAL FUZZY LOGIC AND FEATURE REDUCTION

By

Ahmed Shawki Bayoumi Abu Daia

A Thesis Submitted to the  
Faculty of Engineering at Cairo University  
In Partial Fulfillment of the  
Requirements for the Degree of  
MASTER OF SCIENCE  
In  
Computer Engineering

FACULTY OF ENGINEERING  
CAIRO UNIVERSITY  
GIZA, EGYPT  
2017



COMPROMISED NODE DETECTION USING  
HIERARCHICAL FUZZY LOGIC AND FEATURE  
REDUCTION

By  
Ahmed Shawki Bayoumi Abu Daia

A Thesis Submitted to the  
Faculty of Engineering at Cairo University  
In Partial Fulfillment of the  
Requirements for the Degree of  
MASTER OF SCIENCE  
In  
Computer Engineering

Under the Supervision of

Prof. Dr. Magda B. Fayek

Professor  
Computer Engineering Department  
Faculty of Engineering, Cairo University

Dr. Rabie A. Ramadan

Doctor  
Computer Engineering Department  
Faculty of Engineering, Cairo University

FACULTY OF ENGINEERING  
CAIRO UNIVERSITY  
GIZA, EGYPT  
2017



# COMPROMISED NODE DETECTION USING HIERARCHICAL FUZZY LOGIC AND FEATURE REDUCTION

By  
Ahmed Shawki Bayoumi Abu Daia

A Thesis Submitted to the  
Faculty of Engineering at Cairo University  
In Partial Fulfillment of the  
Requirements for the Degree of  
MASTER OF SCIENCE  
In  
Computer Engineering

Approved by the  
Examining Committee

---

Prof. Dr. Magda B. Fayek, Thesis Main Advisor  
Computer Department, Faculty of Engineering at Cairo University

---

Prof. Dr. Ihab E. Talkhan, Internal Examiner  
Computer Department, Faculty of Engineering at Cairo University

---

Prof. Dr. Mohamed Z. Abd El Megeed, External Examiner  
Computer Department, Faculty of Engineering at Al Azhar University

FACULTY OF ENGINEERING  
CAIRO UNIVERSITY  
GIZA, EGYPT  
2017



**Engineer's Name:** Ahmed Shawki Bayoumi Abu Daia  
**Date of Birth:** 10/03/1983  
**Nationality:** Egyptian  
**E-mail:** Ahmed.Shawky@outlook.com  
**Phone:** 01118114070  
**Address:** 32 Mahmoud Ateeq St. Al-Margoushy,  
Shoubra El Khiema, Cairo, Egypt  
**Registration Date:** 01 / 10 / 2011  
**Awarding Date:** / / 2017  
**Degree:** Master of Science  
**Department:** Computer Engineering



**Supervisors:**

Prof. Dr. Magda B. Fayek  
Dr. Rabie A. Ramadan

**Examiners:**

Prof. Magda B. Fayek (Thesis main advisor)  
Prof. Ihab E. Talkhan (Internal examiner)  
Prof. Mohamed Z. Abd El Megeed (External examiner)  
(Professor at Computer Engineering Department, Faculty  
of Engineering at Al Azhar University)

**Title of Thesis:**

## COMPROMISED NODE DETECTION USING HIERARCHICAL FUZZY LOGIC AND FEATURE REDUCTION

**Key Words:**

Wireless Attacks; Network Attacks; Hierarchal Fuzzy Logic; FURIA Fuzzy Logic;  
Particle Swarm Optimization (PSO); Machine Learning

**Summary:**

This research proposes a hierarchal fuzzy logic system used for detecting the compromised or attacked nodes in wireless networks. The proposed system is composed of three hierarchal layers and each layer composed of concrete components built using the Fuzzy Unordered Rule Induction Algorithm (FURIA) fuzzy logic. The Particle Swarm Optimization (PSO) technique is used at the data preprocessing phase to reduce the significant features number. We used NSL-KDD dataset for the training and evaluation phases, and the WEKA is the environment used for experiments.





## **Acknowledgments**

In the name of Allah, the Lord of the worlds, the Most Merciful, the Most Gracious, all praise be to Allah, and prayers and peace be upon His servant and messenger Mohamed. First and foremost, I must acknowledge my endless thanks to Allah, the Ever-Magnificent; the Ever-Glorious; the Ever-Thankful, for His assistance and bless. I am sure that this work would have never become truth, without His guidance.

There are some people without whom this thesis might not have been written, and to whom I am greatly indebted. I owe a profound obligation of appreciation to my university for giving me the opportunity to complete this work. I am grateful to people, who worked with me from the beginning till the completion of this research particularly my supervisor Dr. Rabie Ramadan, who has always been honorable and munificent during all phases and difficulties of the research, and I highly appreciate the efforts and endless support by Dr. Magda Fayek. Last but not least, deepest thanks to all people who encourage me and took part in making this thesis real.



## **Dedication**

I dedicate this thesis to the sake of Allah my Creator and my Master; messenger Mohammed (peace be upon him); the soul of my father who continued to learn, grow and develop me and who has been a source of encouragement and inspiration to me throughout my life; my mother may Allah protect and save her; my dearest wife, Tayseer, for her endless support and motivation, constant encouragement, limitless giving and great sacrifice, helping me accomplish my degree; and my beloved daughters: Rital, and Loujin, whom I can't stop loving them. To all my beloved family, the symbol of love and giving; my friends who encourage and support me; and All the people in my life who touch my heart.



# Table of Contents

<b>ACKNOWLEDGMENTS .....</b>	<b>I</b>
<b>DEDICATION .....</b>	<b>II</b>
<b>TABLE OF CONTENTS.....</b>	<b>III</b>
<b>LIST OF TABLES .....</b>	<b>V</b>
<b>LIST OF FIGURES .....</b>	<b>VI</b>
<b>NOMENCLATURE .....</b>	<b>VIII</b>
<b>ABSTRACT .....</b>	<b>X</b>
<b>CHAPTER 1 : INTRODUCTION .....</b>	<b>1</b>
1.1.PROBLEM STATEMENT .....	1
1.2.NETWORK SECURITY SERVICES .....	1
1.3.WSN POSSIBLE ATTACKS .....	2
1.4.ATTACK CATEGORIZATION FEATURES .....	10
1.5.ORGANIZATION OF THE THESIS .....	16
<b>CHAPTER 2 LITERATURE REVIEW .....</b>	<b>17</b>
2.1.TRUST AND TRUST METHODOLOGIES .....	17
2.2.COMPROMISED NODE MITIGATION TECHNIQUES .....	19
2.3.ATTACK AVOIDANCE TECHNIQUES .....	26
<b>CHAPTER 3 : PROPOSED SOLUTION .....</b>	<b>27</b>
3.1.INTRODUCTION .....	27
3.2.PROPOSED SOLUTION ARCHITECTURE .....	27
3.2.1.First Layer Components .....	27
3.2.2.Second Layer Components .....	28
3.2.3.Third Layer Components .....	29
3.3.DATA PREPROCESSING .....	31
3.3.1.Feature minimization using PSO .....	31
3.3.2.Testing and training data preparation .....	32
3.4.FURIA ALGORITHM .....	32
<b>CHAPTER 4 : DATASET .....</b>	<b>35</b>
4.1.INTRODUCTION .....	35
4.2.DATASET STATISTICS .....	36
4.2.1.NSL KDD Test+ .....	36

4.2.2.NSL KDD Test-21 .....	38
4.2.3.NSL KDDTrain+_20Percent .....	39
<b>CHAPTER 5 : EXPERIMENTAL RESULTS AND ANALYSIS .....</b>	<b>41</b>
5.1.PERFORMANCE EVALUATION CRITERIA .....	41
5.2.PSO FEATURE SELECTION EXPERIMENT RESULTS .....	44
5.3.FURIA EXPERIMENT RESULTS .....	53
5.3.1.Layer 1 (Attack Existence Detection) Results .....	54
5.3.2.Layer 2 (Detecting Attack Category) Results .....	55
5.3.3.Layer 3 (Detecting Attack Name) Results .....	58
5.3.3.1.DoS Attacks Results .....	58
5.3.3.2.Probes Attacks Results .....	64
5.3.3.3.R2L Attack Results .....	66
5.3.3.4.U2R Attack Results .....	74
5.4.COMPARATIVE STUDY .....	77
<b>CHAPTER 6 : DISCUSSION AND CONCLUSIONS.....</b>	<b>81</b>
<b>APPENDIX A: WEKA RAW RESULT DATA .....</b>	<b>82</b>
<b>REFERENCES .....</b>	<b>126</b>

## List of Tables

Table 1.1: Detecting features of different attacks .....	10
Table 1.2: Detected attacks by certain feature.....	14
Table 2.1: ISA possible encryption levels .....	23
Table 2.2: Mitigation techniques pros and cons .....	24
Table 4.1: NSL-KDD coloring scheme and meaning .....	36
Table 4.2: Categories statistics in NSL-KDD Test+ file.....	36
Table 4.3: Attacks statistics in NSL-KDD Test+ file.....	36
Table 4.4: Categories statistics in NSL-KDD Test-21 file.....	38
Table 4.5: Attacks statistics in NSL-KDD Test-21 file.....	38
Table 4.6: Categories statistics in NSL-KDD Train +_20Percent file .....	39
Table 4.7: Attacks statistics in NSL-KDD Train +_20Percent file .....	40
Table 3.1: Selected Feature sets based on PSO suggestions .....	52
Table 5.1: Comparative Study of Classification Techniques .....	78
Table 5.2: Comparing FURIA and LSSVM-IDS with different parameters.....	79
Table 5.3: Comparing FURIA and LSSVM-IDS with other systems .....	80