COMPARATIVE STUDY BETWEEN FUZZY C-MEANS ALGORITHM AND ARTIFICIAL IMMUNE NETWORK ALGORITHM IN INTRUSION DETECTION SYSTEM

AHMED A. A. ABUNADA

A Project report submitted in partial fulfillment of the requirements for the award of the degree of Master of Science Computer (Information Security)

Faculty of Computing
Universiti Teknologi Malaysia

JANUARY 2013
I dedicate this project to my respected and beloved my mother ‘Ibtesam Saed Al-khateb’ and My father ‘Abdurabou Ahmed Abunada’, thank you for the moral and financial support you have given me throughout my academic life.

To my respected supervisor, Dr. Anazida Zainal

To my beloved country, Palestine, Gaza

To all my brothers and sisters

To all my friends
ACKNOWLEDGEMENT

First and foremost, all praise and thanks are due to Allah, and peace and blessings be upon his Messenger, Mohammed (Peace Be Upon Him). Next, I wish to express my sincere appreciation to my main supervisor, Dr. Mrs. Anazida Zainal, for encouragement, guidance, critics, and friendship.
Intrusion Detection Systems (IDS) is special software developed in order to protect the system against security threats and malware. IDS provides second line of defense after rule based firewall. Unfortunately IDS with supervised learning approach heavily rely on labeled training data and generally it fails to detect novel attacks and produces high false alarm. Besides, data labeling is expensive and time consuming. However, a systematic method which offers the capability to alleviate this problem is through the use of unsupervised approaches, which is the basis for this research. In addition to that, to investigate this phenomenon, a comparison between two clustering algorithms based on an anomaly detection system IDS is proposed. Related literature has given a direction towards comparing two clustering algorithm which are Artificial Immune Network (AIN) and Fuzzy c-means (FCM). The performance of those two clustering algorithm were measured based on false positive rate, false negative rate, hit rate and detection. This study has evaluated and analyzed AIN and FCM clustering algorithms. The finding shows that AIN gives higher overall accuracy and hit rate. It also gives lower false alarms on both datasets used in the study. Consistent good performances of AIN in clustering network traffic data into respective classes has made AIN a promising clustering technique to be used in detection novel attack traffic in IDS.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>CHAPTER</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>DECLAREATION</td>
<td>ii</td>
</tr>
<tr>
<td></td>
<td>DEDICATION</td>
<td>iii</td>
</tr>
<tr>
<td></td>
<td>ACKNOWLEDGMENT</td>
<td>iv</td>
</tr>
<tr>
<td></td>
<td>ABSTRACT</td>
<td>v</td>
</tr>
<tr>
<td></td>
<td>ABSTRAK</td>
<td>vi</td>
</tr>
<tr>
<td></td>
<td>TABLE OF CONTENTS</td>
<td>vii</td>
</tr>
<tr>
<td></td>
<td>LIST OF TABLES</td>
<td>xi</td>
</tr>
<tr>
<td></td>
<td>LIST OF FIGURES</td>
<td>xiii</td>
</tr>
<tr>
<td></td>
<td>LIST OF ABBREVIATION</td>
<td>xvi</td>
</tr>
</tbody>
</table>

## INTRODUCTION 1

1.1 Introduction 1  
1.2 Problem Background 3  
1.3 Problem Statement 5  
1.4 Purpose of study 5  
1.5 Objective of study 5  
1.6 Scope of study 6  
1.7 Significant of Study 6  
1.8 Organization of Report 7

## LITERATURE REVIEW 8

2.1 Introduction 8  
2.2 Intrusion Detection System 8  
    2.2.1 Host-based Intrusion Detection System 12
2.2.2 Network-based Intrusion Detection System 13
2.2.3 Types of attack 13
2.2.4 Misuse Intrusion Detection System 14
   2.2.4.1 Snort 15
2.2.5 Anomaly Intrusion Detection 16
   2.2.5.1 Architecture of Network-based Anomaly 17
detection
   2.2.5.2 Components of Anomaly Detection 18
   2.2.5.3 Techniques used to develop
       Anomaly Detection 19

2.3 K-Means Clustering 24
   2.3.1 K-Means clustering in Intrusion Detection 24

2.4 Self-Organizing Maps 25
   2.4.1 Self-Organizing algorithm 27
   2.4.2 Goodness of SOM Network Architecture 28

2.5 Fundamentals of Human Immune System 29

2.6 Artificial Immune System 32
   2.6.1 Clonal Selection 33
   2.6.2 Negative Selection 35
   2.6.3 Immune Network Theory 36
       2.6.3.1 Algorithm of Immune Network 38

2.7 Fuzzy C-means Clustering 42
   2.7.1 Adaptive Neuro-fuzzy Inference System 45

2.8 Related work 46

2.9 Summary 51

3 RESEARCH METHODOLOGY 52
3.1 Introduction 52
3.2 Research Framework 52
3.3 Research Design 55
   3.3.1 Phase 1: Dataset Preparation 55
   3.3.2 Phase 2: Developing Artificial Immune
       Network using Matlab 56
   3.3.3 Phase 3 Developing Fuzzy c-means algorithm 56
## 3.3.4 Phase 4 Evaluation and interpretation for Fuzzy c-means and Artificial Immune Network algorithms

56

3.4 KDD CUP 99 Dataset

58

3.4.1 Data Samples Preparation

62

3.5 Summary

65

### 4 IMPLEMENTATION AND TESTING FUZZYC-MEANS

66

4.1 Introduction

66

4.2 Experimental Setup

66

4.3 Implementation of Fuzzy c-means

67

4.4 Results of Fuzzy c-means (FCM)

67

4.4.1 Fuzzy c-means Using Data Test 1

69

4.4.2 Fuzzy c-means Using Data Test 2

77

4.5 Discussion and Overall Results

82

4.6 Summary

83

### 5 IMPLEMENTATION AND TESTING ARTIFICIAL IMMUNE NETWORK

84

5.1 Introduction

84

5.2 Experimental Setup

85

5.3 Implementation of artificial Immune Network

85

5.4 Results of Artificial Immune Network

87

5.4.1 Artificial Immune Network Using Data Test 1

87

5.4.2 Artificial Immune Network Using Data Test 2

92

5.5 Discussion and Overall Results

97

5.6 Comparison between FCM and AIN

98

5.7 Summary

103

### 6 CONCLUSION AND FUTURE WORK

104

6.1 Introduction

104

6.2 Project Achievements and Challenges

104

6.3 Future Work

105
6.4 Summary 106

REFERENCE 107

APPENDIX A 110
# LIST OF TABLES

<table>
<thead>
<tr>
<th>TABLE NO.</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Examples on supervised algorithms</td>
<td>20</td>
</tr>
<tr>
<td>2.2</td>
<td>Related studies</td>
<td>47</td>
</tr>
<tr>
<td>3.1</td>
<td>Formula used to calculate the performance</td>
<td>57</td>
</tr>
<tr>
<td>3.2</td>
<td>Variables for IDS data set</td>
<td>59</td>
</tr>
<tr>
<td>3.3</td>
<td>Best selected significant features obtained by clustering algorithms in two different samples of data.</td>
<td>61</td>
</tr>
<tr>
<td>3.4</td>
<td>The explanation of most 6 significant features</td>
<td>62</td>
</tr>
<tr>
<td>3.5</td>
<td>The distribution of the Normal and others attacks in the data sample</td>
<td>63</td>
</tr>
<tr>
<td>3.6</td>
<td>The contain of sample Test1</td>
<td>63</td>
</tr>
<tr>
<td>3.7</td>
<td>The contain of sample Test2</td>
<td>64</td>
</tr>
<tr>
<td>4.1</td>
<td>Parameters used for FCM</td>
<td>67</td>
</tr>
<tr>
<td>4.2</td>
<td>Distribution of Data in Test 1 and test 2 sets.</td>
<td>68</td>
</tr>
<tr>
<td>4.3</td>
<td>Best few selected membership values for Normal cluster</td>
<td>70</td>
</tr>
<tr>
<td>4.4</td>
<td>Accuracy of detection result using Test1-FCM</td>
<td>71</td>
</tr>
<tr>
<td>4.5</td>
<td>Confusion matrix for Test 1 datasets</td>
<td>72</td>
</tr>
<tr>
<td>4.6</td>
<td>Accuracy of detection result using Test2-FCM</td>
<td>77</td>
</tr>
<tr>
<td>4.7</td>
<td>Confusion matrix for Test 2 datasets</td>
<td>78</td>
</tr>
<tr>
<td>5.1</td>
<td>Best few selected Threshold</td>
<td>85</td>
</tr>
<tr>
<td>5.2</td>
<td>Distribution of Data in Test 1 and Test 2 sets.</td>
<td>87</td>
</tr>
<tr>
<td>5.3</td>
<td>Accuracy of detection result</td>
<td>87</td>
</tr>
<tr>
<td>5.4</td>
<td>Confusion matrix for Test 1 datasets using AIN</td>
<td>88</td>
</tr>
<tr>
<td>5.5</td>
<td>Accuracy of detection result using Test2</td>
<td>93</td>
</tr>
<tr>
<td>Section</td>
<td>Title</td>
<td>Page</td>
</tr>
<tr>
<td>---------</td>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>5.6</td>
<td>Confusion matrix for Test 2 datasets</td>
<td>93</td>
</tr>
<tr>
<td>5.7(a)</td>
<td>Comparison result between FCM and AIN using Test 1</td>
<td>99</td>
</tr>
<tr>
<td>5.7(b)</td>
<td>Comparison result between FCM and AIN using Test 2</td>
<td>100</td>
</tr>
<tr>
<td>5.8(a)</td>
<td>Comparison of overall performance measures for FCM and AIN using dataset Test 1</td>
<td>101</td>
</tr>
<tr>
<td>5.8(b)</td>
<td>Comparison of overall performance measures for FCM and AIN using dataset Test 2</td>
<td>102</td>
</tr>
<tr>
<td>FIGURE NO.</td>
<td>TITLE</td>
<td>PAGE</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>2.1</td>
<td>Four possible outcomes of detection</td>
<td>9</td>
</tr>
<tr>
<td>2.2(a)</td>
<td>Classifier of false positive and negative rate</td>
<td>10</td>
</tr>
<tr>
<td>2.2(b)</td>
<td>Classifier of false positive and negative rate</td>
<td>11</td>
</tr>
<tr>
<td>2.2</td>
<td>A basic ROC graph</td>
<td>12</td>
</tr>
<tr>
<td>2.3</td>
<td>IDS taxonomy</td>
<td>17</td>
</tr>
<tr>
<td>2.4</td>
<td>Generic ANIDS functional architecture</td>
<td>24</td>
</tr>
<tr>
<td>2.5</td>
<td>K-means algorithm</td>
<td>28</td>
</tr>
<tr>
<td>2.6</td>
<td>SOM algorithm</td>
<td>29</td>
</tr>
<tr>
<td>2.7</td>
<td>SOM Network Architecture</td>
<td>31</td>
</tr>
<tr>
<td>2.8</td>
<td>The structure of immune system</td>
<td>31</td>
</tr>
<tr>
<td>2.9</td>
<td>B-cell and T-cell receptor for pattern recognition</td>
<td>34</td>
</tr>
<tr>
<td>2.10</td>
<td>Clonal Selection process</td>
<td>36</td>
</tr>
<tr>
<td>2.11</td>
<td>Immune Network theory</td>
<td>37</td>
</tr>
<tr>
<td>2.12</td>
<td>View on Idiotypic Immune Network</td>
<td>38</td>
</tr>
<tr>
<td>2.13</td>
<td>Algorithm of Immune Network</td>
<td>39</td>
</tr>
<tr>
<td>2.14(a)</td>
<td>Dataset with three clusters</td>
<td>43</td>
</tr>
<tr>
<td>2.14(b)</td>
<td>Corresponding network structure</td>
<td>54</td>
</tr>
<tr>
<td>2.15</td>
<td>Pseudo-code of Fuzzy c-Means</td>
<td>64</td>
</tr>
<tr>
<td>3.1</td>
<td>Research Framework</td>
<td>65</td>
</tr>
<tr>
<td>3.2</td>
<td>percentage of Sample Test 1</td>
<td>68</td>
</tr>
<tr>
<td>3.3</td>
<td>percentage of Sample Test 2</td>
<td>69</td>
</tr>
<tr>
<td>4.1</td>
<td>Disabused of Test 1 in percentage (%)</td>
<td>70</td>
</tr>
<tr>
<td>4.2</td>
<td>Membership of each data in Test 1</td>
<td>71</td>
</tr>
<tr>
<td>4.3</td>
<td>Three memberships for the detection accuracy</td>
<td>73</td>
</tr>
</tbody>
</table>
4.4 Normal detection Accuracy using Test1-FCM 74
4.5 Detection Accuracy of Probe Traffic using Test1-FCM 75
4.6 Detection Accuracy of DoS Traffic using Test1-FCM 75
4.7 Detection Accuracy of U2R Traffic using Test1-FCM 75
4.8 Detection Accuracy of R2L Traffic using Test1-FCM 76
4.9 Overall Accuracy using Test1-FCM 77
4.10 Detection Accuracy of Normal Traffic using Test2-FCM 79
4.11 Detection Accuracy of Probe Traffic using Test2-FCM 80
4.12 Detection Accuracy of DoS Traffic using Test2-FCM 80
4.13 Detection Accuracy of U2R Traffic using Test2-FCM 81
4.14 Detection Accuracy of R2L Traffic using Test2-FCM 81
4.15 Overall Accuracy using Test2-FCM 82
4.16 Result comparison between Test1 And Test 2 83
5.1 Trade-off between the final number of output cells(N) and the suppression threshold $S \sigma$ 86
5.2 Classification Accuracy for Normal data using Test1-AIN 89
5.3 Detection accuracy of Probe Traffic using Test1-AIN 90
5.4 Detection accuracy of DoS Traffic using Test1-AIN 90
5.5 Detection accuracy of U2R Traffic using Test1-AIN 91
5.6 Detection Accuracy of R2L Traffic using Test1-AIN 91
5.7 Overall Accuracy using Data Test1-AIN 92
5.8 Detection Accuracy of Normal Traffic using Test2-AIN 94
5.9 Detection Accuracy of Probe traffic using Test2-AIN 95
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.10</td>
<td>Detection Accuracy of DoS Traffic using Test2-AIN</td>
<td>95</td>
</tr>
<tr>
<td>5.11</td>
<td>Detection Accuracy of U2R Traffic using Test2-AIN</td>
<td>96</td>
</tr>
<tr>
<td>5.12</td>
<td>Detection accuracy of R2L Traffic using Test2-AIN</td>
<td>96</td>
</tr>
<tr>
<td>5.13</td>
<td>Overall Accuracy using Test2-AIN</td>
<td>97</td>
</tr>
<tr>
<td>5.14</td>
<td>Result comparison between Test1 And Test 2</td>
<td>89</td>
</tr>
</tbody>
</table>
## LIST OF ABBREVIATION

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDS</td>
<td>Intrusion detection system</td>
</tr>
<tr>
<td>AIN</td>
<td>Artificial Immune network</td>
</tr>
<tr>
<td>FCM</td>
<td>Fuzzy c-means</td>
</tr>
<tr>
<td>FP</td>
<td>False positive</td>
</tr>
<tr>
<td>FN</td>
<td>False Negative</td>
</tr>
<tr>
<td>HIDS</td>
<td>Host-based Intrusion detection system</td>
</tr>
<tr>
<td>NIDS</td>
<td>Network-based Intrusion detection system</td>
</tr>
<tr>
<td>ROC</td>
<td>Receiver Operating Characteristics</td>
</tr>
<tr>
<td>DoS</td>
<td>Denial of Service Attack</td>
</tr>
<tr>
<td>U2R</td>
<td>User to Root Attack</td>
</tr>
<tr>
<td>R2L</td>
<td>Remote to Local Attack</td>
</tr>
<tr>
<td>SOM</td>
<td>Self-Organizing Maps</td>
</tr>
<tr>
<td>aiNet</td>
<td>Artificial Immune Network</td>
</tr>
</tbody>
</table>
CHAPTER 1

INTRODUCTION

1.1 Introduction

Because of the growing utilization of computer networks in lots of facets of our existence, the amount of weaknesses is also growing leading to the network assets not available and split up the machine discretion, integrity and availability. Makes use of pose a significant security threat for that stability and also the security of knowledge within the network atmosphere. According to Qasem (2010), network invasion attack involves an array of activities. It offers trying to destabilize the network, attaining unauthorized use of files with rights, or mishandling and misusing of software.

Intrusion Detection Systems (IDS’s) are security tools, like other measures for example anti-virus programs, firewalls, and access control schemes, usually are meant to strengthen the safety of knowledge and communication systems (Garcia-Teodoro et al., 2009). An Intrusion Detection System is a vital element of the computer and knowledge security framework between normal activities from the system and actions that may be considered intrusive.

The objective of IDS would be to identify unauthorized use or accessibility computer or network in the outdoors atmosphere by individuals who do not possess the authority or access privileges to such systems. The primary purpose of Intrusion
Detection would be to develop a system that may instantly scan the network activity and identify such invasion attacks (Qasem, 2010). An IDS can be used to identify several kinds of malicious actions that may compromise the safety and trust of the computer or network. Including network attacks against vulnerable services, data driven attacks on programs, host based attacks for example privilege escalation, unauthorized logins and access to sensitive files, and malware.

There are two main intrusion detection approaches, misuse intrusion detection system and anomaly intrusion detection system exist. The Misuse intrusion detection is based on attack signatures, the detailed description of the sequence of actions performed by the attacker. This approach provides the platform which allows the detection of intrusions perfectly matching the signatures. On the other hand, the misuse detection recognizes known attack patterns and uses well-defined patterns of the attack.

The anomaly detection concentrates on the unusual activities of designs and uses the standard behavior designs to recognize an intrusion. Many researchers mentioned that the anomaly intrusion detection can solve the issues that misuse detection cannot solve. Garcia-Teodoro et al., (2009) highlighted that the primary advantage of anomaly detection approach is its ability to identify or detect previously unknown intrusions. Panda and Patra (2005), mentioned that, it's a must have way of discovering makes use of once the training information is unlabeled too for discovering unknown kinds of makes use of. They further stated that, the technique that satisfies this require is the anomaly detection and without supervision approach.

Meanwhile, IDS’s can also be categorized according to the host system into two types:

1. Host-based IDS (HIDS)
2. Network-based IDS (NIDS)
The host-based IDS operates at the host level and monitors a single host machine using the audit trails of the host operating system, whereas network-based IDS operates at the network level and monitors any number of hosts on the network.

1.2 Problem Background

By dealing with very large number of data over networks, it is difficult to classify them manually to detect possible intrusions. Labeled data could be acquired by simulating intrusions, but this really is restricted to the group of known attacks and can neglect to address new kinds of attacks that could occur later on. Consequently of the limited ability in discovering unknown attacks, the recognition product is not efficient in acquiring the network data (Qasem, 2010). Therefore, a procedure for discovering makes use of once the information is unlabeled is required, in addition to discovering new and unknown kinds of attacks.

Anomaly detection algorithms hold the advantage that they may identify new types of intrusions as diversions from normal usage, Leon et al., (2004). Going by this problem and given some normal data to train from, and given a totally new bit of test data, invasion recognition formula is always to decide if test data take part in “normal” order to be able to detect an anomalous behavior. Referring to this issue as supervised anomaly detection because the models are produced only using the normal behavior across the network. In comparison, without supervision anomaly detection attempts to recognize anomalous behavior without needing any understanding regarding the training data. However, both kinds of anomaly detection schemes are stricken by maximum false alarms.

Qasem (2010) maintains that, in many conditions, labeled information is unavailable and the time is right consuming and incredibly costly to label the information by hand. Meanwhile, there's always an engaged alternation in normal traffic designs as well as constantly emerging of novel attacks each one of these
problems result in the supervised approach not practical solution for IDS. To resolve these complaints, scientists proceed to focus on without supervision approach, for example clustering because this without supervision approach doesn't rely on the labeled data and it doesn't consume us just as much time as supervised needs. Without a doubt, clustering will work for new novel attacks. Various without supervision techniques happen to be suggested however the recognition rate of IDS is quite insufficient compared to supervised approaches.

Bace and Mell (2001) suggest that, to manage to identify novel attacks, anomaly-based Intrusion detection systems was recommended. The job starting with modeling a range of normal or valid behavior, especially when the observed behavior diverges from this model, then an anomaly is elevated. However, anomaly-based IDSs are more likely to false positives that may be triggered by novel, but non-malicious traffic, as it is difficult to make a model connected wonderful possible normal traffic. These false positives generally are a considerable hindrance to effective operators monitoring the NIDS, consequently of occasions wasted in considering them. Single Percent false positive rate might trigger huge amounts of bogus alerts particularly when run on the large volumes of traffic common in current systems. This, according to Axelsson (2000), is known as the base rate fallacy. Nonetheless, anomaly-based approach has remained an active part of research interest and is the main focus of this research also.

Artificial immune system technique was introduced in late 90’s and it received a lot of attention from researchers. The ability of immune system to protect human body were adopted many algorithms such as Negative selection, Clonal selection and immune network. Applications Artificial Immune system include that of computer and internet security, network intrusion detection and computer viruses.

Immune network which is a clustering technique was founded by Jerne’s idio typic network theory (Jerne1974), which suggests that the immune systems looks after a network of interconnected B-cells. In artificial immune network (AIN) models, a B-cell population includes two sub-populations: the very first population
as well as the cloned population. The very first set is created in the subset of raw training data to create the B-cell network.

1.3 Problem Statement

Supervised techniques do suffer low detection accuracy and high false alarm especially when dealing with novel attacks. Besides, labeling network traffic instances is expensive and time consuming. Furthermore, a supervised technique can be obsolete, especially when network traffic is dynamic. It warrants an updating of reference model. Therefore, clustering often seen to be a better solution as it can deal with changes.

1.4 Purpose of Study

In this research the performance of Fuzzy c-means algorithm (FCM) as well as Artificial Immune Network algorithm (AIN) will be compared in terms of detection accuracy, false alarms and hit rate. At the end of this comparison, an analysis of their performances will be discussed and the algorithm that shows better performance will be highlighted and recommended.

1.5 Objectives of Study

This research has the following objectives:

i. To study and investigate performance of Fuzzy c-Means algorithm in IDS.

ii. To study and investigate performance of Immune Network algorithm in IDS.
iii. To compare the performance of Fuzzy c-Means algorithm and Immune network algorithm in IDS.

1.6 Scope of Study

The scope of project is listed below:

i. Two clustering technique (Fuzzy c-means) and (Artificial Immune network) will be used in this study.

ii. The data used in this study is from KDD Cup 1999 Intrusion Detection dataset.

iii. The study intends to use two datasets which will comprise of 5,092 and 6,890 samples in order to retain actual distribution of KDD Cup 1999 data.

iv. Matlab will be used to code Fuzzy c-means (FCM), and Artificial Immune Network (AIN) algorithms.

v. The classification will be based on five classes which are Normal, Probe, DoS,U2R and R2L. as in works of (Abraham and Grosan, 2006, Zainal et al., 2009), (Dutta, 2009)

vi. Performance will be evaluated based on detection accuracy, False positive rate, False negative rate and Hit rate.

1.7 Significant of Study

This study evaluates the performance of two algorithms: Artificial Immune Network clustering and Fuzzy c-means algorithm for the network-based IDS in terms of detection accuracy, and false alarms by studying each one and investigate them to show which one is more suitable to be used in IDS.
1.8 Organization of Report

The thesis consists of 6 chapters. Chapter one describes the introduction, background of the study, research objectives and questions, the scope of the study and its primary objectives. The second chapter reviews available and related literature on Intrusion detection Systems, Artificial Immune Network, supervised and without supervision, Fuzzy c-means and clustering approaches. Chapter three describes the study methodology along with the appropriate framework for the study. The 4th chapter provides the results and analysis of the findings of the first algorithm which is Fuzzy c-means (FCM). The 5th chapter provides the results and analysis of the findings of the second algorithm which is Artificial Immune Network (AIN) and the evaluation with Fuzzy c-means based on the detection Accuracy, False alarms and the Hit rate. Lastly, chapter 6 covers the conclusion and the future works.
REFERENCES


