UNIVERSITY OF BAHRAIN

College of Information Technology



Fuzzy Logic and Goal Programming for Distributed Denial of Service Attacks in Wireless Sensor Networks

A Thesis Submitted in Partial Fulfillment of the Requirements for the Master Degree in Information Technology

Submitted by

Rola Yusuf Mohammed AlOmari

20033002

Supervised by

Dr. Salman Ahmed Khan

Assistant Professor

University of Bahrain

Kingdom of Bahrain

June, 2014

DECLARATION

I declare that this work is the result of my own investigation and that it has not already been accepted in substance for any degree, nor is it being currently submitted for any degree.

Signed : ..... Date : 23-6-2014.
Rola AlOmari(candidate)

The Thesis defense committee considers the Thesis titled :

"FUZZY LOGIC AND GOAL PROGRAMMING FOR DISTRIBUTED DENIAL OF SERVICE ATTACKS IN WIRELESS SENSOR NETWORKS"

Submitted by Rola Yousif AlOmari to the College of Information Technology satisfactory and acceptable for the Master of Science degree in Information Technology.

Thesis Defense Committee :

Dr. Salman A. Khan
Supervisor

College of Information Technology
University of Bahrain

Dr. Malick M. Ndiaye
External Examiner

Department of Industrial Engineering
American University of Sharjah

Dr. Ali A. Khan
Internal Examiner

College of Information Technology
University of Bahrain

Dedicated to my beloved family

Acknowledgements

All praise to Allah Almighty, and peace and blessings on his last messenger. I would like to express my thanks and appreciation to my supervisor Dr. Salman Khan, who has been a tremendous mentor for me. His encouragement, precious guidance, and support in academics as well as in life have been priceless.

My deepest gratitude to my family for their love and support through my life. Words cannot express how grateful I am to every member of my family. A special thanks to my parents, for their prayers, love, and care. Their prayer for me was what sustained me thus far.

At the end, I would like to show my gratitude to all my friends for their support and continuous willingness to help. They were always there cheering me up and stood by me through the good times and bad.

Abstract

Wireless sensor networks (WSNs) have emerged as an important technology for monitoring of critical situations that require real-time sensing and data acquisition for decision-making purposes. Security of wireless sensor networks is a contemporary challenging issue. A significant number of various types of malicious attacks have been identified against the security of WSNs in recent times. Due to the unreliable environments in which WSNs operate, the threat of distributed attacks against sensory resources such as power consumption, communication, and computation capabilities cannot be neglected. In the case of distributed denial of service attacks (DDoS) in WSNs, the consumption of the node's energy resources is the most targeted vulnerability because of the resource-limited nature and short-lived batteries of the sensor nodes. Therefore, detection mechanisms for DDoS in WSNs require a solution that is fully distributed and inexpensive in terms of communication and energy requirements. Due to the conflicting nature of the two important parameters that affect the performance of any DDoS attack detection scheme in WSN, namely, attack detection rate and node energy decay rate, achieving the optimized values of specific parameters of the detection scheme is becoming a very challenging task. In other words, the task is to establish a reasonable trade-off between the two parameters. In this thesis, the above task can be viewed as a multi-criteria decision-making (MCDM) problem. Both fuzzy logic and goal programming (GP) based approaches are proposed in the context of DDoS attacks in WSNs. The proposed approaches are modelled and formulated as multi-criteria decision-making problem, while considering attack detection rate and energy decay rate as the two decision criteria. Beside GP approach, Dubois and Prade's (D&P), Werners, and Unified And-Or (UAO) fuzzy operators are used to develop a mechanism to achieve the best trade-off between the two aforementioned conflicting criteria. All mentioned schemes have been evaluated empirically with respect to their operator related parameters. The empirical analysis proves the effectiveness of the proposed approaches. Results suggest that (D&P) operator produced the best results among all operators when focussing on the effect of the operator related parameter on the overall membership. Whereas, when focussing on the effect of membership values of the attack detection and energy decay rates on the overall membership, (D&P) operator produced the worst results. A comparative analysis of the proposed approaches revealed that Werners and UAO operators performed best in large size networks and GP was a better choice for small size networks.

Contents

Acknowledgements ii

List of Tables ix

List of Figures ix

1 Introduction 1
- 1.1 Wireless Sensor Networks . . . 2
- 1.2 Motivation . . . 5
- 1.3 Objectives . . . 7
- 1.4 Methodology . . . 7
- 1.5 Contributions . . . 8
- 1.6 Thesis Outline . . . 9

2 Background and Literature Review 11
- 2.1 Attack Patterns in Wireless Sensor Networks . . . 11
- 2.2 Attack Detection in Wireless Sensor Networks . . . 16
- 2.3 Multi-criteria Decision-making . . . 20
- 2.4 Fuzzy Logic and Goal programming for the Multi-criteria Decision-making Problem . . . 22
  - 2.4.1 Fuzzy Logic . . . 22
  - 2.4.2 Goal Programming . . . 24
- 2.5 Conclusions . . . 25

3 Multi-criteria Decision-making for Distributed Denial of Service Attacks in Wireless Sensor Networks 27
- 3.1 Background . . . 27
  - 3.1.1 The Problem's Application Domain . . . 28
  - 3.1.2 Formal Definition of the Problem . . . 30
- 3.2 Multi-criteria Decision-making Approach to the Problem . . . 31
- 3.3 Test Cases and Input Data . . . 37
- 3.4 Conclusions . . . 39

4 Application of Dubois & Prade's Operator to DDoS Attack Detection in WSNs 40
- 4.1 Introduction . . . 40

4.2 Application of the Dubois and Prade's operator to the problem . . . 41
4.3 Results and Discussion . . . 43
4.3.1 Effect of number of GN nodes on the best value for α for different values of γ . . . 45
4.3.2 Effect of value of γ on the best trade-off between ADR and EDR . . . 46
4.3.3 Effect of γ on memberships of ADR, EDR, and overall membership for different number of GN nodes . . . 49
4.3.4 Effect of value of γ on the Ratio of mGN and GN nodes . . . 51
4.4 Conclusions . . . 52

5 Application of Werners Operator to DDoS Attack Detection in WSNs 53
5.1 Introduction . . . 53
5.2 Application of the Werners operator to the problem . . . 54
5.3 Results and Discussion . . . 56
5.3.1 Effect of number of GN nodes on the best value for α for different values of β . . . 58
5.3.2 Effect of value of β on the best trade-off between ADR and EDR . . . 60
5.3.3 Effect of β on memberships of ADR, EDR, and overall membership for different number of GN nodes . . . 61
5.3.4 Effect of value of β on the Ratio of mGN and GN nodes . . . 62
5.4 Conclusions . . . 64

6 Application of Unified AND-OR Operator to DDoS Attack Detection in WSNs 65
6.1 Introduction . . . 65
6.2 Application of the Unified And-Or operator to the problem . . . 67
6.3 Results and Discussion . . . 67
6.3.1 Effect of number of GN nodes on the best value of α for different values of ν . . . 69
6.3.2 Effect of value of ν on the best trade-off between ADR and EDR . . . 71
6.3.3 Effect of ν on memberships of ADR, EDR, and overall membership for different number of GN nodes . . . 72
6.3.4 Effect of value of ν on the Ratio of mGN and GN nodes . . . 74
6.4 Conclusions . . . 75

7 Application of Goal Programming Approach for DDoS Attack Detection in WSNs 76
7.1 Application of Goal Programming to The Problem . . . 76
7.2 Results and Discussion . . . 77
7.3 Conclusions . . . 81

8 Comparisons of Approaches 82

8.1 Comparison of Fuzzy Logic Operators 82
8.1.1 Effect of value of operator related parameter on the overall membership 83
8.1.2 Effect of memberships of ADR and EDR on the overall membership 85
8.2 Comparison between Fuzzy Logic and Goal Programming 87
8.3 Conclusions 90

9 Conclusions **92**
9.1 Summary 92
9.2 Future Work 94

Appendix A - Nomenclature **102**

Appendix B - Derived Publications **104**

List of Tables

1.1 Technical Specifications of Mica2 sensor node. 3
1.2 Technical Specifications of Rene sensor node. 3

3.1 Values of α, mGN, EDR, and ADR for the test case with 128 GN nodes. The corresponding membership values of EDR and ADR are also listed. 37
3.2 Values of α, mGN, EDR, and ADR for the test case with 256 GN nodes. The corresponding membership values of EDR and ADR are also listed. 38
3.3 Values of α, mGN, EDR, and ADR for the test case with 512 GN nodes. The corresponding membership values of EDR and ADR are also listed. 38
3.4 Values of α, mGN, EDR, and ADR for the test case with 1024 GN nodes. The corresponding membership values of EDR and ADR are also listed. 38
3.5 Values of α, mGN, EDR, and ADR for the test case with 2048 GN nodes. The corresponding membership values of EDR and ADR are also listed. 39

4.1 Overall membership using D&P operator for different values of γ versus values of α, with GN =128. Best membership values are in boldface. . . 44
4.2 Overall membership using D&P operator for different values of γ versus values of α, with GN =256. Best membership values are in boldface. . . 44
4.3 Overall membership using D&P operator for different values of γ versus values of α, with GN =512. Best membership values are in boldface. . . 44
4.4 Overall membership using D&P operator for different values of γ versus values of α, with GN =1024. Best membership values are in boldface. . 45
4.5 Overall membership using D&P operator for different values of γ versus values of α, with GN =2048. Best membership values are in boldface. . 45
4.6 Values of γ and the ratio of mGN and GN nodes for N= 128 to 2048 GN nodes. 51

5.1 Overall membership using Werners operator for different values of β versus values of α, with GN =128. Best membership values are in boldface. 56
5.2 Overall membership using Werners operator for different values of β versus values of α, with GN =256. Best membership values are in boldface. 57
5.3 Overall membership using Werners operator for different values of β versus values of α, with GN =512. Best membership values are in boldface. 57
5.4 Overall membership using Werners operator for different values of β versus values of α, with GN =1024. Best membership values are in boldface. 57

5.5 Overall membership using Werners operator for different values of β versus values of α, with GN =2048. Best membership values are in boldface. 58
5.6 Values of β and the ratio of mGN and GN nodes for N= 128 to 2048 GN nodes. 64

6.1 Overall membership using UAO operator for different values of ν versus values of α, with GN =128. Best membership values are in boldface. . . 67
6.2 Overall membership using UAO operator for different values of ν versus values of α, with GN =256. Best membership values are in boldface. . . 68
6.3 Overall membership using UAO operator for different values of ν versus values of α, with GN =512. Best membership values are in boldface. . . 68
6.4 Overall membership using UAO operator for different values of ν versus values of α, with GN =1024. Best membership values are in boldface. . 68
6.5 Overall membership using UAO operator for different values of ν versus values of α, with GN =2048. Best membership values are in boldface. . 69
6.6 Values of ν and the ratio of mGN and GN nodes for N= 128 to 2048 GN nodes 74

7.1 Deviations for EDR, ADR, and Overall for GN=128. Lowest overall deviation is in boldface. 77
7.2 Deviations for EDR, ADR, and Overall for GN=256. Lowest overall deviation is in boldface. 78
7.3 Deviations for EDR, ADR, and Overall for GN=512. Lowest overall deviation is in boldface. 78
7.4 Deviations for EDR, ADR, and Overall for GN=1024. Lowest overall deviation is in boldface. 79
7.5 Deviations for EDR, ADR, and Overall for GN=2048. Lowest overall deviation is in boldface. 79

8.1 Comparison of D&P, Werners, and UAO for the Overall Membership 83
8.2 Comparison of the effect of memberships of EDR and ADR on the overall membership (the objective) for D&P, Werners and UAO. . . 85
8.3 Comparison of the effect of regression coefficients of deviations of EDR and ADR on the overall deviation for GP. 87
8.4 Percentage difference between the regression coefficients of MemADR and MemEDR for using D&P operator. 89
8.5 Percentage difference between the regression coefficients of MemADR and MemEDR using Werners operator. 89
8.6 Percentage difference between the regression coefficients of MemADR and MemEDR using UAO operator. 89
8.7 Percentage difference between the regression coefficients of deviation of ADR and deviation of EDR using goal programming. 90
8.8 Average Percentage difference for D&P, Werners, UAO, and goal programming. 90

List of Figures

3.1 Membership functions for (a) Attack Detection Rate and (b) Energy Decay Rate. 34
3.2 Flowchart of fuzzy logic for the MCDM problem. 35
3.3 Flowchart of Goal programming for the MCDM problem. 36

4.1 Effect of γ on D&P function. 42
4.2 Progression of α vs GN nodes for (a) $\gamma = 0.1$ (b) $\gamma = 0.2$ (c) $\gamma = 0.3$ (d) $\gamma = 0.4$ (e) $\gamma = 0.5$ (f) $\gamma = 0.6$ (g) $\gamma = 0.7$ (h) $\gamma = 0.8$ (i) $\gamma = 0.9$ (j) $\gamma = 1.0$. 47
4.3 Effect of value of γ on α for (a) GN = 128 (b) GN = 256 (c) GN = 512 (d) GN = 1024 (e) GN = 2048. 48
4.4 Effect of γ on MemADR, MemEDR, and OM for (a) GN = 128 (b) GN = 256 (c) GN = 512 (d) GN = 1024 (e) GN = 2048. 50

5.1 Effect of β on Werners function. 55
5.2 Progression of α vs GN nodes for (a) $\beta = 0.1$ (b) $\beta = 0.2$ (c) $\beta = 0.3$ (d) $\beta = 0.4$ (e) $\beta = 0.5$ (f) $\beta = 0.6$ (g) $\beta = 0.7$ (h) $\beta = 0.8$ (i) $\beta = 0.9$ (j) $\beta = 1.0$. 59
5.3 Effect of value of β on α for (a) GN = 128 (b) GN = 256 (c) GN = 512 (d) GN = 1024 (e) GN = 2048 61
5.4 Effect of β on MemADR, MemEDR, and OM for (a) GN = 128 (b) GN = 256 (c) GN = 512 (d) GN = 1024 (e) GN = 2048. 63

6.1 Effect of ν on UAO function. 66
6.2 Progression of α vs GN nodes for (a) $\nu = 0.1$ (b) $\nu = 0.2$ (c) $\nu = 0.3$ (d) $\nu = 0.4$ (e) $\nu = 0.5$ (f) $\nu = 0.6$ (g) $\nu = 0.7$ (h) $\nu = 0.8$ (i) $\nu = 0.9$ (j) $\nu = 1.0$ 70
6.3 Effect of value of ν on α for (a) GN = 128 (b) GN = 256 (c) GN = 512 (d) GN = 1024 (e) GN = 2048 72
6.4 Effect of ν on MemADR, MemEDR, and OM for (a) GN = 128 (b) GN = 256 (c) GN = 512 (d) GN = 1024 (e) GN = 2048 73

7.1 Plots depicting the effect of variation of α on the Deviation of Attack Detection Rate, Deviation of Energy Decay Rate, and the Overall Deviation for (a) GN = 128 (b) GN = 256 (c) GN = 512 (d) GN = 1024 (e) GN = 2048. 80

Chapter 1

Introduction

In today's era, smart environments have brought revolution to all aspects of our life. We can see their applications to utilities, industries, home, shipping, entertainment, crisis management, homeland defense, smart spaces, and transportation systems automation, among many others. A smart environment principally depends on sensory data from the real world [43]. This data is obtained from multiple sensors of different modalities in distributed locations [43]. In order to achieve this, sensors, which are inexpensive and low power tiny devices are connected in a specific manner, thus forming sensor networks.

Sensor networks consist of a set of connected sensor nodes. Each sensor node is equipped with one or more sensors, communication subsystems, storage and processing resources, and in some cases, actuators [46]. Sensors in a node monitor and observe various phenomena such as thermal, optical, acoustic, seismic, and acceleration events, while the processing and other components analyze the raw data and formulate answers for specific user requests. Recent advances in technology have facilitated improvements in the design and implementation of new generations of sensor network nodes, packaged in very small and inexpensive form, and capable of sophisticated computation and wireless communication abilities. Seaphan *et al.* [46] suggest that these new classes of sensor networks, commonly referred to as wireless sensor networks (WSN), show enormous potential with applications ranging in areas that have already been mentioned, to domains still beyond imagination.

1.1 Wireless Sensor Networks

Unlike the fixed wireless networks, WSNs are on-the-fly networks which are mainly characterized by the absence of a centralized coordination or fixed infrastructure. As a result, wireless sensor networks are rapidly and widely deployed in rough environments where sensor nodes generally self-configure, and form a routing topology to facilitate communication of sensed data to the base station, or to other sensor nodes such as battlefields and bushes [57]. A major benefit of the sensors in WSN is that they perform in-network processing to reduce large streams of raw data into useful aggregated information [56]. Certainly, this information is very crucial and enormous resource for monitoring and collecting data about traffic, detection of critical actions in their operational environments, assessing and evaluating the information, formulating meaningful user displays, and performing decision-making and alarm functions [43].

Wireless sensors have a number of characteristics that make them ideal for logistics usage. For instance, the wireless communication capacities, autonomous power and small size allow connection sensors to the internet to be maintained for long periods.

One of the possible uses of WSNs is in cargo shipboard, logistics and transport companies, where there is a need to monitor the transportation conditions of goods such as the temperature, location and tracking a package from origin to destination. WSNs can be also used for military applications to alert military command and control units of the occurrence of events of interest in hostile regions [65]. Moreover, WSNs can be used in medical applications such as the design of a body network. According to Wood *et al.* [70] and Bri *et al.* [9], a body network is composed of tiny portable devices equipped with a variety of sensors (such as heart-rate, temperature sensor), and performs biophysical monitoring, patient identification, location detection, and other desired tasks. Due to a wide range of applications being designed today based on WSNs, it is not unreasonable to expect that in the next ten to fifteen years, the world will be covered with WSNs and access to them via the internet will be easily possible [65].

According to a survey which was done by Yick *et al.* [77], there are two kinds of sensor nodes used in a WSN. One is the normal sensor node deployed to sense the phenomena and the other is the gateway node that interfaces the sensor network to the external world. Base station is operating as the centralized station that collects and aggregates the sensory data received from other sensor nodes. Tables

TABLE 1.1: Technical Specifications of Mica2 sensor node.

Parameter	Specification
Sensor Node Name	Mica2
Program+Data Memory	4 KB RAM
External Memory	128 KB flash
Programming	TinyOS, SOS and MantisOS
Microcontroller	ATMEGA 128L
Transceiver	Chipcon 868/916 MHz

TABLE 1.2: Technical Specifications of Rene sensor node.

Parameter	Specification
Sensor Node Name	Rene
Program+Data Memory	512 bytes RAM
External Memory	8 KB flash
Programming	TinyOS
Microcontroller	ATMEL8535
Transceiver	916 MHz

1.1 and 1.2 illustrate some technical specification of two commercial sensor nodes Mica2 and Rene respectively [77].

Sensor nodes are generally static post-deployment within their environment. For data delivery in this network, WSNs follow one of the following three common applications [67]:

- *One to many*: When a single base station broadcasts or multicasts a message (possibly a query) to several or all of sensor nodes in the network.
- *Many to one*: When a number of sensor nodes transfer their individual sensory data and readings to either the base station or another sensor node, called the data aggregation node, responsible for collecting sensory readings.
- *Peer communication*: When sensor nodes exchange messages with other nodes at the same level of communication hierarchy, for purposes of co-ordination and control message exchange.

Network topology defines many details which are important to understand the way that a network behaves. The topology may describe the positions of nodes in the network, the direction of data movement inside the network, and the arrangement of nodes based on their positions. The root topology is the one applied in sensor networks, with the base station operating as the root, or in other words, the central entity for control, coordination, and delivery operations of the network. The base station is connected to either a single (or, more commonly, multiple) node(s) in the level below. Several intermediary sensor nodes can also participate in the routing process by aggregating localized sensory data, for delivery to the base station. The purpose of having such intermediary aggregation nodes is to reduce the effects of routing on the overall energy consumption rates of the network. As a consequence, longevity in the lifetime of the sensor network is attained [64].

Because of the critical nature of the applications that employ WSNs, any malicious attack can compromise the network, resulting in a huge damage to the entire network. Therefore, security of WSNs, by itself is a critical issue due to many constraints like limited energy, computational power, and low memory [35]. Researchers working in this area have proposed a number of techniques to secure a network. The most common forms of attacks on modern day computing systems and networks are not directly applicable on WSN environments [3]. The primary reasons for this lack of applicability are manifold. First and the foremost is the resource constrained nature of sensor nodes. This is augmented by the lack of a single entry point to the network. Furthermore, non-triviality in targeting specific 'critical' sensor nodes as well as their inaccessibility are also contributing factors [3].

The above discussion signifies the fact that the detection of attacks in WSNs is crucial and must be done after having a clear understanding of attack classes and nature by studying the definitions of attack models for such networks. Attacks can be countered by attack detection, attack mitigation, and attack prevention. The detection of an attack is the first step in attack defense that needs to be taken, before any attack mitigation techniques are actually applied. Similarly, attack prevention, although non-trivial in nature, is another approach towards protection of the network from malicious attacks.

Security in Wireless Sensor Networks

As discussed earlier in this section, the nature of the applications that employ WSNs are significantly sensitive. Therefore, any malicious attack on such networks

can critically compromise and harm the network, resulting in a huge damage to the entire network.

According to [65], if adversaries exist, they can perpetrate a wide variety of attacks on a WSN including black hole, Sybil, replays, wormhole, and denial of service attacks. According to the reviewed literature, sensor network attacks can be classified in three basic categories: identity, routing, and network intrusion attacks [3]. Different attack types are classified within these three categories. These include active attacks [35], passive attacks [35], flood attacks [33, 32], black hole attacks [35], Sybil attacks [54], information alteration [58], Worm holes [63], looping [63], Node replication [55], and Denial of Service (DoS) attacks [3]. Denial of Service (DoS) attack can cause serious damage in the resource constrained WSNs. The reason is that an adversary overwhelms the sensor nodes by flooding a series of fake packets to the victim node. When more than one adversary broadcast the fake traffic to the same victim node, the attack is referred to as Distributed Denial of service (DDoS) attack [3].

In the next Chapter, an elaborated discussion of the classifications of different attacks threatening WSNs will be given.

1.2 Motivation

There are two sensitive parameters that affect the performance of a WSN when it comes to DDoS attacks. These are detection of an attack on the network, as well as conservation of energy of a sensor node. Both parameters are equally important in their own respect and require optimization. However, the two parameters are conflicting in nature. This means that if one tries to optimize or improve one parameter, it degrades the quality of the other. In this situation, none of the two parameters can be completely optimized alone, and a solution that provides the best balance between the two parameters is desired. This makes the attack detection a daunting and challenging task. The above problem can be viewed as a multi-criteria decision-making (MCDM) problem. The MCDM is employed in situations requiring decisions to be made in presence of multiple, usually conflicting, criteria [45]. The objective of MCDM is to make decisions about selecting the best alternative from a finite set of available alternatives. More specifically, an MCDM method uses numeric techniques to help decision-makers choose among a discrete set of alternative decisions [69].

A number of approaches exist to deal with the MCDM problem. Two efficient and frequently used approaches are based on fuzzy logic [78] and goal programming (GP) [11, 28].

Fuzzy logic has been successfully applied to MCDM problems in various disciplines. In dealing with MCDM problems, fuzzy aggregation operators play a pivotal role. A number of fuzzy aggregation operators have been proposed over the years, which can be classified as s-norms and t-norms. As will be discussed later in Chapter 2, t-norm operators are of much interest for decision-makers due to their capability of decision-making considering all criteria simultaneously in the decision-making process.

Various t-norm operators, such as Dubois & Prade (D&P) [17, 18], Werners [72, 73], and Unified And-Or (UAO) [37, 38, 39], have demonstrated some unique features than other fuzzy operators. As will be discussed in Chapter 2, this uniqueness is due to a parameter, which has a simpler construction than many other fuzzy aggregation operators. This particular aspect of the aforementioned three operators makes them attractive candidates for MCDM problems. For the three operators, it is relatively much easier to find a fairly suitable value for the operator related parameter that would result in best trade-off solutions. The attractiveness is further amplified by the fact that these three fuzzy functions have already been applied successfully to a number of MCDM problems [8, 12, 23, 39, 40, 41, 48, 53, 60, 61, 68, 75, 79]. In addition to fuzzy logic, GP is another popular and powerful MCDM technique. Due to its simplicity and elegance, the technique has also been applied to a variety of MCDM problems in different domains [1, 14, 44, 30, 80].

The above issues provide a strong motivation to apply and analyze the performance of D&P, Werners, and UAO fuzzy functions, as well as the GP approach to the MCDM problem considered in this thesis. This problem is concerned with finding the best trade-off of attack detection rate (ADR) and energy decay rate (EDR) for DDoS attacks in WSNs. The application of fuzzy logic and GP approaches to a high performance network, such as a WSN, is not an easy task due to the resource demanding nature of such a network, the high expenses for building the network, and impracticality of unaltered deployment on these resource constrained networks.

1.3 Objectives

The primary objectives of this thesis are as follows:

1. To address the multi-criteria nature of the attack detection in DDoS attacks in WSNs by extending the work undertaken in [38, 7] while considering ADR and EDR as the decision criteria.
2. To show that fuzzy logic and GP are suitable and effective approaches to deal with the MCDM problem considered in this thesis.
3. To apply and analyze the performance of Werners operator for the problem considered in this thesis.
4. To apply and analyze the performance of UAO operator for the problem considered in this thesis.
5. To propose an MCDM approach based on D&P operator for the problem considered in this thesis, and analyze the performance of the proposed approach.
6. To propose an MCDM approach based on GP for the problem considered in this thesis, and analyze the performance of the proposed approach.
7. To perform a comparative analysis of the proposed approaches and to find out which approach performs the best.

1.4 Methodology

The MCDM schemes proposed in this thesis are first presented and discussed. Since some of the fuzzy operators presented in Chapters 4, 5 and 6 have been used in previously published work, well-known benchmark cases that exist in [7] and [38] has been used to quantify performance of the proposed algorithms.

In this thesis, the work is based on an empirical study where experiments are done to get the results. Firstly, data is collected at network of nodes, each time with different number of ordinary nodes and base station nodes. Secondly, the analysis is done using Excel to calculate and investigate some important values. To have a comprehensive analysis, samples of the two conflicting parameters are selected for different number of nodes in order to test the effect on the results.

For each scheme proposed in the thesis, values for the best overall membership are obtained to find the best trade-off between the two decision criteria, i.e., the attack detection and energy decay or consumption rates.

Lastly, the data analysis is done by analyzing the results based on fuzzy logic and GP procedures which are the focus of the proposed study.

The performances of the various schemes or procedures proposed are empirically compared.

1.5 Contributions

The key contributions of the thesis are:

1. An approach based on fuzzy logic proposed in [38, 7] is revisited and is extended by performing an in-depth analysis of two fuzzy operators, namely, Werners and UAO. This in-depth analysis includes:
   a. Sensitivity analysis of the Werners operator and the associated operator related parameter β. This is an extension of the work undertaken in [7] which did not perform the sensitivity analysis of the operator.

   b. Sensitivity analysis of the UAO operator and the associated operator related parameter ν. This is an extension of the work undertaken in [38] which did not perform the sensitivity analysis of the operator.

2. An approach based on D&P fuzzy aggregation operator is developed, and sensitivity analysis of the operator and the associated operator related parameter γ is done. This is the first such attempt with regard to the application of the operator to the problem considered in this thesis.

3. An approach based on GP is developed and analyzed for the problem being considered. This is the first such attempt with regard to the application to the problem considered in this thesis.

4. The proposed approaches are mutually compared to find out which approach was most effective in dealing with the MCDM problem considered in this thesis.

1.6 Thesis Outline

This thesis is divided into four parts of nine chapters. The first part is Chapter 1, 2, and 3 which are the background, literature review, and problem domain. The second part is Chapters 4, 5, 6, and 7 which generally present the novel application and analysis of fuzzy logic operators and GP to the problem in hand. More specifically, Chapters 4, 5, and 6 discuss the fuzzy logic approach for the problem in hand in the context of D&P, Werners, and UAO operators. Chapter 7 deals with the application of GP to the considered problem.

The third part is Chapter 8 which presents and describes the mutual comparisons of all the proposed schemes in the second part. Finally, the research conclusion and future work are given in Chapter 9. Following is more detailed explanations for each chapter describing the chapter's main points and contributions.

Chapter 1 gives the initial background on the topic which is the motivation for the work. More elaborated discussions about WSNs including the definition, topology, applications and security are given in this chapter. It also explains the methodology used in the thesis. Moreover, the thesis motivation, objectives, and contributions are also addressed in that chapter. Chapter 2 discusses the different attack models in WSN. The chapter also provides a detailed overview about the DDoS attacks in the internet and in WSNs. This is followed by a review of the literature about the schemes used to detect DDoS attack in WSN. Furthermore, MCDM concept is first introduced. A discussion on the techniques used to solve MCDM problems for DDoS attacks in WSNs is given. The concepts of fuzzy logic and GP are given. A discussion of all related work in this area is summarized.

In Chapter 3, a detailed definition and formulation of the problem considered in this thesis is given. First, the background of the problem domain which is the DDoS attack in WSNs is given. This is followed by an elaborated discussion about basic concepts and important issues related to the DDoS attack detection scheme based on the distributed pattern recognition model for WSNs. The approach of MCDM to the problem is explained. Finally, the data for the five test cases used for evaluation is provided and discussed.

Chapter 4 discusses the proposal and application of D&P operator for DDoS attack detection in WSNs. Followed by a detailed discussion of the process, an empirical analysis is performed to evaluate the effectiveness of the proposed approach. This mainly includes the sensitivity analysis of the D&P operator.

Chapter 5 provides a brief overview of the Werners fuzzy logic operator and how the operator has been applied to the problem considered in this thesis. The chapter focusses on the same decision criteria that were considered in Chapter 4 namely the attack detection rate and energy decay rate. Further, sensitivity analysis of the Werners operator is performed to evaluate the effectiveness of the proposed approach. This is followed by a detailed discussion of the empirical results.

Chapter 6 describes the application of the UAO operator to the DDoS attack detection in WSNs. After providing an overview of the UAO fuzzy logic operator, the chapter also discusses the effectiveness of the UAO operator and its applicability to the problem. An empirical analysis is performed followed by a detailed discussion of the analyzed results using some examples and tests.

Chapter 7 provides the formulation and development of the GP based approach with attack detection and energy decay rates as the two decision criteria. An empirical analysis is also performed to evaluate and prove the effectiveness of the proposed approach. Finally, the chapter gives a detailed discussion of the analyzed results.

Chapter 8 presents mutual comparisons of all the schemes proposed in Chapters 4 to 7. The first aim is to evaluate and compare the performance of the three fuzzy logic operators presented in the thesis. The second aim is to give an elaborated discussion of the best fuzzy logic operator among all the proposed operators. Another aim is to compare the fuzzy logic approach and GP. Finally, the chapter also determines which of the proposed approaches perform the best when applied to the problem.

Finally, Chapter 9 summarizes the presented work, highlights the main achievements, and provides a basis for future work.

Chapter 2

Background and Literature Review

Chapter 1 highlighted the wide applicability of WSNs for number of critical-mission technologies. To achieve goals of critical-mission applications that deploy WSN technology, a set of sensors are used. Sensor nodes in WSNs are capable of aggregating and processing information for two levels of communications. Communications can be locally (in-network) and wirelessly with other elements (outside-the-network) to deliver the information. A sensor node is a simple device, and cannot perform extensive calculation or store significant amount of data. Therefore, those nodes are connected to the active user through internet. Because of the two levels of communications in the WSN, both the in-network and outside-the-network communications have to be protected and secured.

Threats to the security of WSNs can result in a huge damage to very critical systems such as the environment and human life. WSNs are susceptible to many forms of attacks. Those attacks will be discussed in details in Section 2.1. Furthermore, WSNs require a solution that is fully distributed and inexpensive in terms of communication method, energy consumption, and memory requirements.

2.1 Attack Patterns in Wireless Sensor Networks

In contrast to resource-rich networks such as the internet, a WSN is less stable, more resource constrained, subjected to open wireless communication, and directly threatened by physical risks of different issues during deployment and operation. These factors increase the susceptibility of WSNs to different types of attacks. In

the following discussion, various attack models in WSN are discussed. The first class of attacks is referred to as active while the second one is passive attacks. According to [36], active attacks occur when the attacker causes a physical damage to the network such as destruction of resources or fake in-site deployment. On the other hand, passive attacks are considered to be more dangerous than the active attacks because the network would be unable to recognize its adversary or attacker. For these attacks, the attacker eavesdrops at the WSN communications in order to collect network's sensitive information and find points of weaknesses of the network. Afterwards, the attacker exploits this information to launch active attacks in the suitable time [36]. In addition, Karlof *et al.* [32] introduced flood attacks in WSNs. The main purpose of this attack is to destroy network resources by broadcasting excessive messages called the "Hello" messages in the whole network. The attacker pretends that the sender of the packet is a neighbor of a sink node. Therefore, when the sender node wants to send any sensory data to a sink node, it forwards it to attacker's node. As a result, any information is forwarded towards the base station and those packets can be easily accessible to the attacker. Another type of attack is the black hole attack where attacker eavesdrops on the path of requested packets from its neighbors. Then some fake information is sent back as a reply about the shortest path towards a sink node. So, each node in its surrounding sets the attacker as a next node for data forwarding toward sink. Any node which intends to send data to a base station will forward it towards attacker. This provides the attacker with an opportunity to analyze these packets and extract important information [36]. A worm hole attack occurs when the whole traffic of the network is tunnelled in a particular direction at a distant place, which causes prevention of data receiving in other parts of the network. As a result, significant information which should be delivered to the base station in a specific time is sent towards the worm hole which will confiscate the base station from receiving it [63].

Another attack is Sybil attack, which was first introduced by the authors of [54], where the attack occurs when malicious devices illegitimately take on multiple identities of legitimate sensor nodes in the network. Sybil attack was discussed later in [36], and suggested that the main purposes of this attack were to increase the resource utilization and decrease data integrity. Using the same concept, node replication attack can be launched by adding a new sensor node in the network, which is using the identification (ID) of a legitimate user. This attacker node replication can cause a big destruction in network. Once the replicated node is able to access the network then there is a possibility that the attacker may get the position of a strategic node (the base station)[55].

Sensor nodes always communicate with the base station and transfer sensed information to it. Nevertheless, there are still chances of spoofing data by the attacker in the middle of communication. Information alteration is the class of attack where an attacker pretends to be one of the neighbors of the victim sensor node to gain the access to the sensory information being transmitted between the sensor node and the base station [58]. According to [63], looping attack occurs when few nodes in the network take part in circulating the sensory data in a particular region. This attack stops data from being sent to its particular destination node and keeps revolving in the same region.

Finally, DoS mainly aims to waste the available resources of the network. In this attack, the attacker (malicious node) sends extra packets in the network without any need and keeps the route as well as the base station busy. This prevents the authentic user from sending data, accessing resources, and getting services. A special scenario of DoS is the DDoS attack in WSNs. Since the thesis is concerned with the DDoS attacks in WSNs, the purpose of this chapter is to provide a primer on DDoS attacks and a review of related literature.

Distributed Denial of Service Attacks

There are a number of important factors that increase the vulnerability of WSNs to DoS attacks. These factors mainly encompass the communication bandwidth, limited energy, and memory requirements. Therefore, the WSN limited resource can be easily exhausted by a DoS attack. The main objective of a DoS attack is to waste the available resources of the network. In this attack, an adversary (attacker node) sends extra packets (replayed packets or fake traffic) in the network in order to keep the route as well as the base station busy. This results in authentic users being unable to send data, access resources, and get services. Thus, as reported by Baig [3], a DoS attack is launched to prevent the legitimate users of the network from fully utilizing the network resources to get a particular service.

As mentioned earlier, a special case and a more perilous form of DoS attack against a WSN is to overwhelm nodes by flooding packets from distributed adversaries. This would create enormous amount of fake traffic on the attacked network and cause a DDoS attack. The aim of DDoS attack is to quickly exhaust the limited energy, communication bandwidth, memory, and Central Processing Unit (CPU) of resource-limited sensor nodes. Since the application area of this thesis is focussed on DDoS in WSN, the following sections provide a general overview of DDoS attack in the internet and in WSNs.

Distributed Denial of Service Attack in the Internet

As previously mentioned in this chapter, the objective of DDoS attack in the resource-rich networks such as the internet is to overwhelm the target server with an immense volume of traffic in a way that prevents the legitimate internet user from accessing the attacked server to use the service. When the internet was first designed, the main purpose was to deliver packets from sender to the receiver. In fact, any damage (hardware or software) to one of the two parties (sender or receiver) can result in subsequent damage to the other party. The internet design raises several security issues concerning opportunities for DDoS attacks. According to Reiher and Mirkovic [49], DDoS attacks pose an immense threat to the internet. Research in this field has grown rapidly and is becoming more complex. One reason is that attackers constantly modify their attacking mechanisms to bypass the security systems which were built by the internet designers. However, at the same time researchers in turn modify their approaches to handle the newly evolving attacks [49].

Being innovative in an unproductive way, hackers relentlessly keep on conceiving new approaches to launch DDoS attacks in the internet. Following are some internet-oriented DDoS attacking approaches reported in literature [24]:

- DDoS attackers target the whole network physically by destroying the network devices (hardware machines) in the victim network. As a result, the victim will be prevented from performing its operations.
- DDoS attackers target specific network resource by sending a stream of packets to the victim and keep it busy or break the link down in order to make the service unavailable.
- DDoS attackers send distorted packets to confuse to victim's functionality in a way that force the victim to freeze or shutdown.
- DDoS attackers overload the internet infrastructure rather than targeting specific victims.

For the aforementioned approaches, DDoS hackers use several techniques to perform the attack. Generally the attack is launched based on the flooding mechanism which simply exploits the large bandwidth of the intermediate network and at the same time the limited amount of processing in the victim resources.

Packets are sent with spoofed return addresses to random ports on the victim host [76]. The attacked victims are then exploited for participation in the attack process, and under the control of the main attacker, these victims can send hoax packets in their turn.

Distributed Denial of Service Attack in Wireless Sensor Network

The authors in [21] and [25] have stated that DDoS attack in WSNs do not exploit any particular vulnerability in the network design infrastructure. Instead, the attacker takes advantage of the asymmetry property between the bandwidth of intermediate pathways and the processor in the end networks. Reiher and Mirkovic [49] found that, in the network design stage, the desire for large throughput and high performance led to basic changes in the network design. Because of the need of large throughput, the design of network is done so that high bandwidth pathways are in the intermediate network, while the end networks invested in only as much bandwidth and processing capabilities as they thought they might need. Thus, malicious attackers can misuse the abundant resources of the unwitting intermediate network for broadcasting and delivery of stream of numerous messages to a less resource-limited victim [10].

Baig [3] described the behavior of DDoS attack in WSN in details. In the process, the adversary exploits a group of hosts, the zombies, to perform the attack by simultaneously sending useless packets towards the victim, leading to a flood of requests at the victim's end. As a result, the intensity of the traffic becomes high enough to incapacitate either the victim, or its network from further operations. Baig also stated that DDoS attack process consists of two stages, namely, zombie initiation, and attack launch [3].

Chaba *et al.* [34] reported DDoS attacks in Mobile Adhoc Networks (MANETs). These attacks can be classified into resource and bandwidth depletion attacks. In resource depletion, the attack is designed to tie up the resources of a victim system by exploiting the Transmission Control Protocol (TCP) and sending willfully incorrect semantic Internet Protocol (IP) packets to crash the victim system. The bandwidth depletion DDoS attack follows the same concept of the DDoS attack in WSN, where the attacker sends unwanted traffic to flood the network [34].

When an adversary decides to launch a DDoS in a particular WSN, the need for learning about vulnerable nodes in the network or part of another networks arises. Through the zombie initiation phase of the attack, the adversary compromises the vulnerable nodes, and installs attacker source code or script on them.

In other words, this phase can be referred to as the attack deployment where an attacker installs a DDoS attack tools in one or more vulnerable hosts. According to Baig [3], the attacker script which was installed in the nodes during the first stage, will instruct the zombies later in the attack launch stage to generate packets with randomly selected source addresses and send these packets to the victim nodes. Mostly, the main aim of a DDoS attack in WSN is to overwhelm a sensor node with large inflow of requests leads to exhausting the limited energy of that node. Therefore, DDoS in WSN is also referred to as the distributed node exhaustion attack [3].

Security is an important parameter that needs to be considered when transmitting sensitive information in WSNs. Indeed, detection of DDoS attacks is not an easy task because of the distributed nature of such attacks. Further, the performance of any detection scheme is affected by several parameters related to the scheme itself as well as some network parameters that need to be defined in the first stage of network initialization.

2.2 Attack Detection in Wireless Sensor Networks

Traditional security procedures that are used to protect the wired networks cannot be applied easily to secure the WSNs. The first reason is short lifetime of sensor devices. This is due to the fact that sensors are limited in their energy, computation (processing), memory, and communication capabilities. The second reason is the physical nature of the sensor devices which make them highly vulnerable to physical attacks. Unfortunately, almost all WSNs are threatened by all the attacks previously discussed in Section 2.1 [56]. In fact, the detection of attacks in WSNs is crucial and must be done after having a clear understanding of attacks classification and nature by learning the definitions of attack models for such networks. Fundamentally, attacks can be countered by attack detection, attack mitigation, and attack prevention [3]. Baig [3] further outlined the DDoS attack detection in WSN problem using a three-tier approach, consisting of attack prevention, followed by attack detection, and lastly attacker identification and post-attack mitigation.

It is particularly important for researchers in the discipline of WSN to understand how a clan of adversaries cooperate with each other and attack the system. The

use of the already performed DDoS attacks specification as a reference by itself is not a sufficient approach. Attackers frequently find new models of the same attack and target different vulnerabilities in the network ports, pathways, and devices.

Related Work

This section presents the work of prominent researchers in the field of WSNs, highlighting the strengths of their detection techniques as well as the deficiencies. There are many proposed methods in the literature that aim at devising mechanisms to detect a DDoS attack. However, most of these solutions are meant for the wired internet, and there is little research effort on mechanisms against DDoS attacks in WSN. Following is a summary of the attack detection techniques proposed for wireless sensor networks in the literature.

Singh *et al.* [59] reported that the detection mechanisms against DDoS attacks in the wireless networks can be classified into two major categories; local and global. The local defense mechanisms are implemented inside the wireless network, whereas the global mechanisms require a cooperation of several internet subnets, which typically cross company boundaries. The focus of this section will be the local mechanisms which are implemented inside a local network.

Tan and Seah [66] compared the statistical filtering approach in wired and wireless networks and discussed the application of this approach to dropping attack traffic packets in one of the most popular types of WSNs, the MANETs. A framework for statistical filtering in MANETs to combat DDoS attacks was proposed. The filter is equipped with more processing and storage capabilities and can work like other legitimate nodes to forward the packets to neighbors. For this approach, the hierarchical based filtering structure has been utilized in which nodes are grouped into a cluster. A cluster node or the base station sensor node is responsible for monitoring and controlling the routing and filtering within its cluster. Depending on the cluster-based method to apply the statistical filtering in the network can decrease the time needed to deliver the messages between the nodes and as a result increase the DDoS attack detection rate. Whereas, the routing protocol for this cluster-based is a real challenge.

Lee *et al.* [42] realized that it is important to detect DDoS attacks in their early stage in order to prevent generation of massive traffic which exhausts the network bandwidth, energy, and other system resources. The proposed approach focused on traffic matrix to detect DDoS attacks quickly and accurately. One advantage of this approach is in terms of increasing the detection accuracy and speed.

However, several limitations must be considered, for instance, difficulty in finding out the correct values of the traffic matrix parameters. Moreover, the procedures used to find the traffic matrix parameters created computational overheads which exhaust the memory and computing processors in the nodes when DDoS attacks did not occur. Previously mentioned limitations fostered the authors to propose an enhanced DDoS attacks detection approach. The authors proposed a modified approach based on genetic algorithms optimization technique [27] to optimize the parameters of the traffic matrix in order to maximize the detection rates. In addition, the study has provided some insights to improve the traffic matrix building operation by reforming the hash function to decrease hash collisions and replacing the time based window size with a packet based window size to reduce the computational overheads.

The flow monitoring table is another detection technique against DDoS attack proposed by Venkataramani and Arunmozhi [2]. This flow monitoring table contains information about each flow of data received at each node in the network including the value of data sending rate. This rate is calculated for each flow at the intermediate nodes. With each flow in the network, the flow monitoring table is constantly updated and sent to the destination. During the flow, the sender will be alerted if any traffic congestion occurred at the destination. As a result, the sender will reduce its sending rate. If the channel becomes congested continuously, the destination using the updated flow monitoring table can find which sender nodes do not reduce their sending rate. Then the destination checks current sending rate with the previous sending rate of a flow. If both rates are the same, the corresponding sender of the flow is considered as an attacker. Once the DDoS attackers are found, all packets from those nodes will be discarded. An advantage of this scheme is the improvement of performance of Adhoc network, bandwidth, and packet delivery rate. On the other hand, one limitation of the scheme is the time needed to calculate the data sending rate and updating the table at each flow, which will increase the delay rate at the network, possibly resulting in dropping of legitimate users' packets.

Juneja *et al.* [31] presented a prevention mechanism against DDoS attack that concurrently performs and applies stateless and stateful signature analysis. In their proposed scheme, pre-authentication filters are applied before actual verification of unoriginal messages in order to prevent fake messages from being spread across the entire network. This saves the network from attacks without wasting much energy, thus resulting in increasing the lifetime of network and trustable communication. Moreover, the approach helps in tracing the original source of

attack without applying any specific trace-back technique and resources for implementation. Thus, attack traffic gradually gets blocked at source and network continues with normal operations.

Islam *et al.* [29] observed that since the major task of any defense system is to detect these attacks accurately and quickly to avoid unrecoverable loss, most of the research in this regard has been focused on the detection techniques without exploiting spatial placement of detection system in a network. Therefore, their work focussed on the optimized placement of detection nodes in a network for distributed detection of DDoS attacks and used two heuristic algorithms. The authors examined the placement problem of finding a minimum cardinality set of nodes to detect DDoS attacks such that no attack traffic can reach the target without being monitored by these sensors. The placement problem is first formulated as set packing and then as set covering. Results of their study revealed that not only they minimized the number of these node required, but also they reduced the cost, processing overheads, and delays in identifying an attack.

Sathiyabama and Moorthy [52] proposed a defensive technique for DDoS attack in Wireless Local Area Network (WLAN). The approach is based on the authentication technique which includes an Authentication Server (AS), a Wireless Station (WS) and an Access Point (AP). The authentication server holds both regular and attacker database. The attacker database can be constructed from the outcome of fuzzy decision-making. Before granting any session in the WS, AS checks the occurrence of WS in the attacker database. If it is found to be an attacker, AS denies the session key for the WS by isolating the WS from further communications. In order to prevent the authentication request flooding attacks, traffic pattern filtering rule is implemented. Based on the simulation results, the proposed technique is an efficient defensive mechanism against DDoS attack.

Ku *et al.* [74] designed a scheme for DDoS attack detection based on selecting a node called protection node in the network. For the purpose of selection of the protection node, the authors implemented a hierarchical network architecture in which the nodes are divided into multiple levels based on their importance. Once a DDoS attack has been detected, the suspected traffic will be forwarded to the protection node. The victim will function as usual and it is expected that the attacker will stop the meaningless efforts after a certain length of attacking time.

Baig [4] studied the effect of malicious nodes on the limited energy resources during a DDoS attack in WSN. The study aimed at maximizing the lifetime of the nodes in the WSN by quick detection of the DDoS attack. A classic fault-tolerant,

distributed, pattern recognition scheme for DDoS attacks in cluster-based WSNs, called the Graph Neuron (GN), was proposed. The scheme assumed that timely detection of DDoS attacks can be achieved by facilitating distributed detection of patterns of traffic flow in the network toward a set of potential target nodes, by a set of collaborating attack-detector nodes. Additionally, a trade-off equation is defined for computing the optimal cluster sizes based on several network parameters and node loss ratio. Subsequently, a detailed simulation analysis was done to test the effectiveness and performance of the proposed scheme. The study provided some insights into the proposed scheme to show that it performed well even with suboptimal numbers of clusters for certain network scenarios. This pattern-based scheme is also referred to as the fault-tolerant scheme [6]. The scheme has a limitation that it lacks a trade-off mechanism between improved performance of the detection scheme (higher detection rates) and corresponding increase in the use of the energy resources of the sensor nodes participating in the detection process. Due to this deficiency, the scheme yielded poor results in terms of either energy decay or the attack detection rates. The reason for this deficiency is related to application aspect value (discussed in Chapter 3) which was not optimized based on the two criteria of the scheme, energy decay and attack detection rates.

Therefore, the work done in this thesis is basically motivated by this problem. In other words, the aim is to find a fair balance between the two parameters by performing a fuzzy-based decision-making approach that will provide the optimal value for the attack detection scheme, based on the experimental results obtained under varying network conditions. For this reason, the proposed work was further improved by Khan and Baig [7, 38] by considering the DDoS attack as an MCDM problem. Fuzzy logic was employed in order to find the best balance between the ADR and EDR. In other words, achieving a reasonable trade-off between attack detection and node energy utilization.

2.3 Multi-criteria Decision-making

Many real-world problems deal with multiple conflicting criteria that need to be evaluated in making decisions. These problems are referred to as MCDM problems. A common example is the cost or price which is usually conflicting with the measure of the quality criteria. In making decision in a multiple criteria system, the need of being comfortable with the consequences of such decisions is significantly important.

Hence, modelling such problems well and considering multiple criteria explicitly leads to more informed and better decisions. A more formal definition of an MCDM method states that it is "a method that uses numeric techniques to help decision-makers choose among a discrete set of alternative decisions. This is achieved on the basis of the impact of the alternatives on certain criteria and thereby on the overall utility of the decision-maker(s)" [69]. A variety of approaches were implemented to solve MCDM problems, such as interactive programming [81], GP [11, 28], and fuzzy set theory [78] among many others. The most difficult part of the task to compare decision methods and choose the best one is that a paradox is reached, i.e., what approach should be used to choose the best decision-making method. MCDM problems have received significant attention in order to find efficient approaches to solve them.

MCDM is employed in situations requiring decisions to be made in presence of multiple, usually conflicting, criteria [45]. The objective of MCDM is to make decisions about selecting the best alternative from a finite set of available alternatives [69].

Due to the involvement of multiple criteria, a number of issues are associated with MCDM. In majority of cases, the data associated with criteria are non-commensurate. Non-Commensurate variables, are quantities with different units that cannot be compared by a common standard. Therefore, normalization is applied to these quantities in order to make them share a common standard of measurement. Subsequently, the multiple criteria are normalized between the maximum and the minimum extremes in order to map them to [0,1] range. Furthermore, another issue is the preference of criteria over one another may be desired by the decision-maker [37]. For the normal case of solving MCDM problem, all objectives or criteria are considered as having an equal level of importance. For certain special cases, the decision-maker assigns preference to one objective over the others based on the design requirement or the problem's needs. Decision-maker's preferences force the solution of the MCDM to bias towards one objective and are incorporated into the MCDM search process to focus on regions of greater interest [37].

A number of approaches exist to deal with the above two issues. Two efficient and frequently used approaches are based on fuzzy logic [78] and GP [11, 28]. Therefore, the motivation also arises to utilize fuzzy logic and GP to address the MCDM problem for the DDoS attack detection in WSN. Since fuzzy logic and GP are the focus areas of this thesis, a detailed overview of both is given in the next section.

2.4 Fuzzy Logic and Goal programming for the Multi-criteria Decision-making Problem

In this section, an overview of the fuzzy logic approach with emphasis on various t-norm operators is provided. This is followed by outlining various applications of the three fuzzy operators employed to solve the MCDM problem proposed in this thesis. Finally, the concept of GP approach and its application to the same problem are also discussed.

2.4.1 Fuzzy Logic

Fuzzy logic [78] is a mathematical discipline that expresses human reasoning in precise mathematical notation. Fuzzy logic is also known for providing a convenient tool for interfacing linguistic variables with numerical data and for expressing user's preference in a gradual and qualitative way [19]. Therefore, fuzzy logic can efficiently be used to solve the MCDM problem presented in this thesis. As mentioned earlier, fuzzy logic is an efficient approach that can be used to solve such problems in order to find the best values of the detection scheme parameters, so as to ascertain a reasonable trade-off between attack detection and node energy utilization. There are several operators for fuzzy union and fuzzy intersection. For fuzzy union, the operators are known as s-norm operators while fuzzy intersection operators are known as t-norm. Generally s-norm is implemented using "max" and t-norm as "min" function. However, formulation of MCDM functions neither desire pure "ANDing" of t-norm nor the pure "ORing" of s-norm [37].

The reason for this is that in the decision-making process, the pure-ANDing implemented with "min" function considers the effect of the objective with the lowest membership only, completely ignoring the effect of all membership values associated with the other objectives. On the other hand, pure-ORing utilizing the "max" function considers the effect of the highest membership, and ignores the effect of small membership values in the decision-making process.

For many practical applications, t-norms play an important role in fuzzy logic when dealing with situations that require consideration of all criteria involved in the decision-making process. A t-norm utilized in frameworks where multi-valued logic is used. For instance, fuzzy logic is a framework where multiple values are need to be considered in the decision simultaneously. Since MCDM problems require simultaneous consideration of all criteria under investigation,

the "AND" operator in a fuzzy rule plays a crucial role in defining that rule. Consequently, a need arises to develop t-norm operators that would effectively handle the multi-criteria nature of the problem by efficiently incorporating the characteristics of different objectives (through their membership functions) into one fuzzy rule. A number of t-norm operators have been proposed in literature, including Dombi's operator [15, 16], Hamacher's operator [26], Frank's operator [22], Weber's operators [71], Schweizer's operators [62], Mizumoto's operators [51, 50], D&P operator [17, 18], Werners operator [72, 73], and UAO operator [39]. These operators are mathematically represented in the following Eqs. (2.1) to (2.10)

$$\textbf{Dombi}: \quad D(\mu_A, \mu_B) = \frac{1}{1 + \left(\left(\frac{1}{\mu_A} - 1 \right)^{\beta} + \left(\frac{1}{\mu_B} - 1 \right)^{\beta} \right)^{\frac{1}{\beta}}}, \qquad \beta > 0 \qquad (2.1)$$

$$\textbf{Hamacher}: \quad H(\mu_A, \mu_B) = \frac{\mu_A \mu_B}{\beta + (1-\beta)(\mu_A + \mu_B - \mu_A \mu_B)}, \qquad \beta \geq 0 \qquad (2.2)$$

$$\textbf{Frank}: \quad F(\mu_A, \mu_B) = \log_{\beta} \left(1 + \frac{(\beta^{\mu_A} - 1)(\beta^{\mu_B} - 1)}{\beta - 1} \right), \qquad \beta > 0, \beta \neq 1 \qquad (2.3)$$

$$\textbf{Weber 1}: W_1(\mu_A, \mu_B) = max \left\{ 0, \left(\frac{\mu_A + \mu_B - 1 + \beta \mu_A \mu_B}{1 + \beta} \right) \right\}, \quad \beta > -1 \qquad (2.4)$$

$$\textbf{Weber 2}: W_2(\mu_A, \mu_B) = max\{0, (1+\beta)\mu_A + (1+\beta)\mu_B - \beta\mu_A\mu_B - (1+\beta)\}, \quad \beta > -1 \qquad (2.5)$$

$$\textbf{Schw 1}: S_1(\mu_A, \mu_B) = \sqrt[\beta]{max \left\{ 0, (\mu_A^{\beta} + \mu_B^{\beta} - 1) \right\}}, \qquad \beta > 0 \qquad (2.6)$$

Schw 2 :$S_2(\mu_A, \mu_B) = 1 - \sqrt[\beta]{(1-\mu_A)^\beta + (1-\mu_B)^\beta - (1-\mu_A)^\beta(1-\mu_B)^\beta}$, $\beta > 0$ (2.7)

Dubois and Prade : $DP(\mu_A, \mu_B) = \frac{\mu_A \mu_B}{max\{\mu_A, \mu_B, \gamma\}}$, $0 \leq \gamma \leq 1$ (2.8)

Werners : $W(\mu_A, \mu_B) = \beta \times \min\{\mu_A, \mu_B\} + (1-\beta) \times \frac{1}{2}(\mu_A + \mu_B)$, $0 \leq \beta \leq 1$ (2.9)

Unified AndOr : $U(\mu_A, \mu_B) = \frac{\mu_A \mu_B + \nu \max(\mu_A, \mu_B)}{\nu + \max(\mu_A, \mu_B)}$, $0 \leq \nu \leq 1$ (2.10)

In the above functions, μ_A and μ_B represent the membership functions for two criteria (for the MCDM problem), namely, A and B, respectively. Furthermore, in the above equations there are associated parameters (e.g. β in Eqs. (2.1) - (2.7), and γ, β, and ν in Eqs. (2.8) - (2.10) respectively) for each equation. These parameters are referred to as operator related parameters that control the behavior of each t-norm function. It can be observed from the structure of the equations that the limits of each parameter are different.

2.4.2 Goal Programming

GP is one of the first techniques exclusively developed for multi-criteria decision-making [47]. The method was designed for linear models and has an effective role in industrial optimization problems [13]. GP is an approach that can be used to solve MCDM problems which are of conflicting nature. GP can handle relatively large numbers of variables, constraints, and objectives. GP is an attractive alternative to fuzzy logic, since the former does not have any 'operator related parameters'. GP has also been applied to a huge number of MCDM problems in different domains [1, 14, 44, 30, 80]. In GP, targets (goals) that need to be achieved, are assigned by the decision-maker. Values associated with these goals are then incorporated into the decision-making problem as additional constraints [13].

The decision-maker specifies aspiration levels (i.e. the ideal values of the objectives), T_i $(i = 1, ..., K)$, for the objective functions, and absolute deviations from these aspiration levels are minimized to the best possible extent [47]. For a minimization problem, goals are of the form $f_i(\mathbf{x}) \leq T_i$. The objective is to minimize the sum of the absolute values of the differences between target values and actually achieved values [13]. $f_i(\mathbf{x})$ represents actually achieved values.

Design constraints may be used in GP. Two Types of constraints are defined in Eq. (2.11), g_m and h_m, representing inequality constraints (may take the form $\leq$ or $\geq$) and equality constraints respectively. For the problem considered in this thesis, no design constraints are defined.

The simplest form of GP is formulated as follows in Eq. (2.11) [20]:

$$\text{Minimize} \sum_{i=1}^{K} |f_i(\mathbf{x}) - T_i| \tag{2.11}$$

$$\begin{aligned} &\text{subject to } \mathbf{x} \in S \\ &g_m(\mathbf{x}) \leq 0, \quad m = 1, \cdots, n \\ &\mathrm{h}_m(\mathbf{x})=0, \quad m = n+1, \cdots, n+n_h \end{aligned}$$

2.5 Conclusions

Securing WSNs require a solution that is fully distributed and inexpensive in terms of communication, energy, and memory requirements. It is particularly important for researchers to understand how cooperating adversaries might attack the system. Adversaries can severely limit the value of a WSN through DDoS attacks. This is done by broadcasting lager amount of hoax packets in the network to prevent the legitimate users of the network from getting the service. Hence, security is one of the most important features when deployment in WSNs is considered. DDoS attacks are a complex and serious problem, and as a result, several approaches have been proposed to counter them. This chapter has presented several approaches for security, firstly, the DDoS attack and its effects. Secondly, the chapter introduced the DDoS in its relation to the internet and in the WSNs. This was followed by a discussion of the various methods available in the literature to detect DDoS in wireless networks and sensor networks.

A number of concluding remarks could be made. For example, through the surveyed literature about DDoS detection schemes, it was apparent that there is no absolute powerful scheme for detection. However, the main focus was to review the available schemes and present some of their merits and limitations. Through the summary of those schemes, the chapter showed the strengths and weaknesses of such methodologies. Furthermore, the chapter demonstrated the initial motivations towards proposing the schemes used in this thesis. Also, it showed what have been accomplished so far in the domain.

The next chapter discusses the formulation of the problem considered in this thesis and then the application of fuzzy logic and GP to this problem.

Chapter 3

Multi-criteria Decision-making for Distributed Denial of Service Attacks in Wireless Sensor Networks

This chapter provides a detailed definition and formulation of the problem considered in this thesis. In Section 3.1, the background of the problem domain which is the DDoS attack in WSNs is given. This is followed by an elaborated discussion about basic concepts and important issues related to the DDoS attack detection scheme based on the distributed pattern recognition model for WSNs. After this, the approach of MCDM to the problem is explained. Finally, the data for the five test cases used for evaluation is provided and discussed.

3.1 Background

The DDoS attack aims to prevent the service of a network from being available to its legitimate users. The main purpose of the DDoS attack is achieved by generating a large amount of fake traffic (hoax packets) and then sending those packets to one or more victim nodes in the target network simultaneously. This leads to consuming the bandwidth and energy of the network. In the case of DDoS in wireless sensor networks, the node's energy resources is the most targeted vulnerability because of the resource-limited nature and short-lives batteries of the sensor nodes.

Based on what was discussed in Chapter 1, due to the critical nature of the applications that employ WSNs, any malicious attack can critically compromise the network, resulting in a huge damage to the entire network. Therefore, detection mechanisms for DDoS in WSNs require a solution that is fully distributed and inexpensive in terms of communication and energy requirements. As mentioned in Chapter 2, the work in this thesis is motivated by the work done in [7] and [38]. Hence, for the purpose of this chapter, the original model [3] of the application domain which is the DDoS attack detection based on the distributed pattern recognition model for WSNs, is presented in the next subsection.

3.1.1 The Problem's Application Domain

This section discusses the relevant concepts in connection with the DDoS attack detection scheme based on the distributed pattern recognition model for wireless sensor networks proposed in [3].

The author of [3] suggests that DDoS attack in WSN can be launched by adversary nodes (outside the network) or by exploiting vulnerable nodes inside the network (victims). Detection mechanisms that have been deployed for detecting the other types of attack are non-applicable in WSNs. This is due to the nature of the WSNs and the distributed model of the attack itself. Hence, for distributed attack detection, a distributed accurate mechanism is needed to efficiently detect the malicious nodes and ignore the fake traffic. Unlike the centralized detection procedures where a single base station is responsible for all activities related to the detection process in the entire network, the distributed schemes decrease the delays of communications between nodes and eliminate single point of failure vulnerability, which will result in a more effective detection scheme.

Baig [3] modelled a class of attack called the DDoS attack in WSNs, and proposed a pattern-based scheme to detect such attacks applicable for scenarios. Therein, the adversary class consists of malicious nodes injected in the network for a huge traffic generation, directed from distributed ends, towards a target node set. Furthermore, it was also assumed that a single victim node may be targeted with overwhelming number of incoming requests from multiple ends of the network. According to the attack modelled by Baig [3], attacker nodes can either be compromised nodes operating in the network (victims), or a laptop-class adversary. Basically, the attack detection scheme proposed in [3] and [6] operates in five phases, namely, Initialization, Observation, Communication, Verdict, and Pattern Update.

The distributed pattern recognition algorithm (Graph Neuron (GN))

Baig [3] modelled the attack detection scheme based on three tiers (layers) of operations. The first tier consists of a base station node which is responsible for monitoring and collecting data resulting from the communications between nodes and has the final decision in the network. The second tier consists of a set of sensor nodes imposed with an additional task on them. Since these nodes follow the characteristics of the distributed pattern recognition algorithm, namely, the Graph Neuron, the nodes are referred to as Graph Neuron or GN nodes. During the initialization phase, sensor nodes are selected by the base station to operate as Graph Neuron (GN) nodes to observe network traffic flow, and generate traffic observation patterns for each target node as a part of the detection scheme [3]. The observed traffic flow in the network is compared by the GN nodes with the predefined thresholds of maximum number of traffic packets, receivable by each of the victim nodes of the network during some defined time intervals. The GN nodes further collaborate with peer GN nodes, to reconstruct an entire pattern of traffic flow observation, to confirm that an attack is in progress.

The third tier of the scheme consists of a set of localized decision-making nodes called master Graph Neuron (mGN) nodes, where the mGN nodes belong to the set of GN nodes. The mGN nodes are selected to serve as the decision-making nodes of the scheme based on mSelect algorithm proposed in [3]. The mGN nodes are responsible for taking a localized decision on whether an attack is in progress or not. Finally, mGN nodes reconstruct a pattern of observed network traffic flow from the GN nodes of their respective jurisdictions, and communicate with the base station in the first layer. Therefore, the final decision as to whether an attack is taking place or not lies with the base station.

Baig [3] also formulated a trade-off equation Eq. (3.1). In order to achieve reasonable attack detection rates at the cost of minimal energy resource usage, the trade-off equation calculated the time interval a node waits to repeat the pattern recognition detection scheme. This time interval is referred to as the optimal length of a time epoch [3]. The equation provides a trade-off between frequent attack detection, and the lifetimes of the attack detector nodes. The factor α, defined as the application aspect value, is inversely proportional to the value of optimal length of time epoch, and is normalized between [0.0 - 1.0]. The system parameter, α, defines the significance of the accuracy in attack detection over the

energy decay rates or vice versa of the GN/mGN nodes.

$$\Delta_{opt} = \sqrt{\frac{2.(n-m).[E_{elec} + \frac{E_{DA}}{2} + \epsilon_{fs}.d_{mn}^2] + \epsilon_{mp}.d_{mb}^4}{\alpha.TI_e}} \tag{3.1}$$

where,
Δ_{opt} = Optimal length of time epoch.
α = application aspect value {0.0 - 1.0}.
N = Number of sensor nodes.
n = Number of GN nodes.
m = Number of mGN nodes.
TI_e = Expected Traffic Intensity (nJ/bit).
d_{mn} = Average distance from detector node to mGN node (experimental).
d_{mb} = Average distance from mGN node to base station (experimental).
E_{DA} = Data aggregation energy = 5 nJ/bit/signal.
E_{elec} = Hardware energy = 50 nJ/bit.
ϵ_{fs}=10 pJ/bit/m^2.
ϵ_{mp}=0.0013 pJ/bit/m^2.

An appropriate value of α plays a significant role in the modelling of aforementioned detection scheme. The value of α is selected at network initialization time, and it affects the total number of mGN nodes selected by the detection algorithm [3]. As part of the formerly published work in [3] and [6], the detection scheme was modelled based on a fixed value of 0.5 for α. However, scheme yielded poor results with this value in terms of either energy decay or the attack detection rates because of the reason that the value of α was not optimized based on the two criteria of the scheme.

3.1.2 Formal Definition of the Problem

The work done in this thesis is motivated by the problem with the GN detection scheme mentioned earlier in Section 3.1. The detection scheme was modelled based on using a fixed value for α, which is 0.5. This results in producing poor results in terms of either energy decay or the attack detection rates. The aforementioned problem is considered as a MCDM problem in this thesis. The aim is to find a fair balance between the two parameters by performing a fuzzy-logic and GP based decision-making approaches. This will provide the optimal value

of α for the attack detection scheme, based on the experimental results obtained under varying network conditions. The optimal value of α is primarily affected by the type of the application that employs WSNs. For instance, certain applications of WSNs require the scheme to converge less frequently so as to reduce the overhead, thus increasing the lifetimes of the network, but at the cost of lower attack detection rates. In this case, smaller values of α help reducing the overall energy consumption rates incurred by the attack detection scheme. On the other hand, other applications require the scheme to converge more frequently to increase the attack detection rates, at the cost of more resource usage. In such scenarios, higher values of α, close to unity are considered.

In brief, in order to achieve the ideal level of the DDoS attack detection scheme, the detection rate should be near to perfection and ought to perform 100%. The cost of achieving such high detection rates is compensated from the sensor nodes lifetime. Such high detection rates would have a big effect on the energy utilization of the sensor nodes participating in the attack detection process, since the extensive processing may lead to a premature exhaustion of the limited energy supply of these sensors. In other words, the ADR and the EDR are *conflicting* in nature; improving one factor will negatively affect the other. It is, therefore, necessary to find the ideal balance between these two factors, and compute the most optimal ratio of the two, to achieve a reasonably high detection rate without imposing high energy demands on the limited sensory resources [7, 38].

3.2 Multi-criteria Decision-making Approach to the Problem

Due to the conflicting nature of the two important parameters that affect the performance of any DDoS attack detection scheme in WSN, namely, ADR and EDR, achieving the optimized values of specific parameters of the detection scheme is becoming a very challenging issue. In other words, the task is to establish a reasonable trade-off between the two parameters. This issue can be resolved by viewing the problem as a MCDM problem (refer to the discussion about MCDM in Section 3.2).

For the purpose of the problem considered in this thesis, two linguistic variables were defined as "Attack Detection Rate" (ADR) and "Energy Decay Rate" (EDR), with the corresponding membership functions being denoted as MemADR and

MemEDR respectively. The first criterion is the ADR which is defined as the ratio of the total number of attack packets classified correctly, over the total number of attack packets [3]. The node EDR is considered as the second criterion of the function and is defined as the amount of energy utilized by a node for attack detection. The interest is in the term "low" within a set for the energy decay rate, and the term "high" for the attack detection rate. The objective is to find the optimal value of the parameter α that will yield a system with the best trade-off between these two criteria. For this purpose, the following fuzzy rule is defined:

Rule: **IF** a solution X has *high attack detection rate*
AND *low energy decay rate* **THEN** it is a
good solution.

In the above rule, X refers to the solution that has resulted due to a certain value of α. The word "low energy decay rates" is the fuzzy subset of solutions of low energy decay rates, whereas "high attack detection rate" represents the fuzzy subset of solutions of high attack detection rate. As mentioned earlier in Section 2.4, each fuzzy subset is defined by a membership function μ. The membership function returns a value in the range [0,1] which expresses the degree of satisfaction with the particular objective criterion.

As mentioned in Section 2.4, there is an associated constant (e.g. β in Eqs. (2.1) - (2.7), and γ, β, and ν in Eqs. (2.8) - (2.10) respectively) for each equation. This constant is referred to as operator related parameter that controls the behavior of the function. It can be observed from the structure of these equations that many of them may not be a suitable choice in the context of the application domain. It is due to their complex structure, and more importantly, due to their unbounded operator related parameters which have an open-ended range.

A careful observation of these functions reveals that the functions of D&P, Werners, and UAO are different than the other functions mentioned. This difference is due to the fact that the underlying operator related parameter (mentioned as β in Eqs. (2.1) - (2.7)) is open-ended; there is no upper limit to the value of β which makes it almost impossible to choose the most appropriate value of β that would result in the best balance between the two decision-making criteria. This particular aspect of the functions in Eqs. (2.1) - (2.7) make them rather unattractive for MCDM problems. In contrast, the D&P, Werners, and UAO operators (mathematically represented by Eqs. (2.8) - (2.10)) also have an operator related

parameter, but this variable is bounded by upper and lower limits. Therefore, it is relatively much easier to find a fairly suitable value for the operator related parameter that would result in best trade-off solutions. This particular strength of the D&P, Werners, and UAO functions make them attractive candidates for the MCDM problem considered in this thesis. The attractiveness is further amplified by the fact that these three fuzzy functions have already been applied successfully to a number of MCDM problems [8, 12, 23, 39, 40, 41, 48, 53, 60, 61, 68, 75, 79].

From the aforementioned discussion, the use of fuzzy logic, and more specifically, of D&P, Werners, and UAO operators, can be appreciated to solve the MCDM problem of DDoS attack detection in WSNs. However, despite the fact that these operators have an edge over the other operators due to a bounded range of operator related parameters, these operators still need analysis in order to find the most suitable value of the operator related parameter. In this thesis, analysis will be done in order to investigate the effect of changing the values the different parameters related to the operators such as (γ in D&P, β in Werners, and ν in UAO).

However, before the operators can be applied to the problem being considered, the membership functions for the two criteria, need to be defined. These membership functions are found as discussed below.

Membership Function For Attack Detection Rate

To develop the membership function for the ADR, denoted by MemADR, two extreme values are determined. The minimum value, denoted as "MinADR" , is taken to be zero. The maximum value, "MaxADR", is taken to be the highest value possible (e.g. 100%) which corresponds to a value of 1. Figure 3.1 (a) provides the pictorial representation of the corresponding membership function. Since the two extreme values were already in the [0,1] range, there was no need for normalization (refer to Section 3.2).

Membership Function for Energy Decay Rate

Similar to the membership function for the ADR, to find the membership function for EDR, MemEDR, two extreme values are determined. The minimum and maximum values are respectively taken to be the lowest and highest values found in all the generated solutions. Thus, the minimum value (lower bound), "MinEDR", was found to be 230.0 μJ/sec. The maximum value,"MaxEDR", was to 12102.3 μJ/sec. Subsequently, the EDR is normalized between MinEDR and MaxEDR in

order to map it to [0,1] range, so as to make it commensurable with ADR. Figure 3.1 (b) illustrates the corresponding membership function.

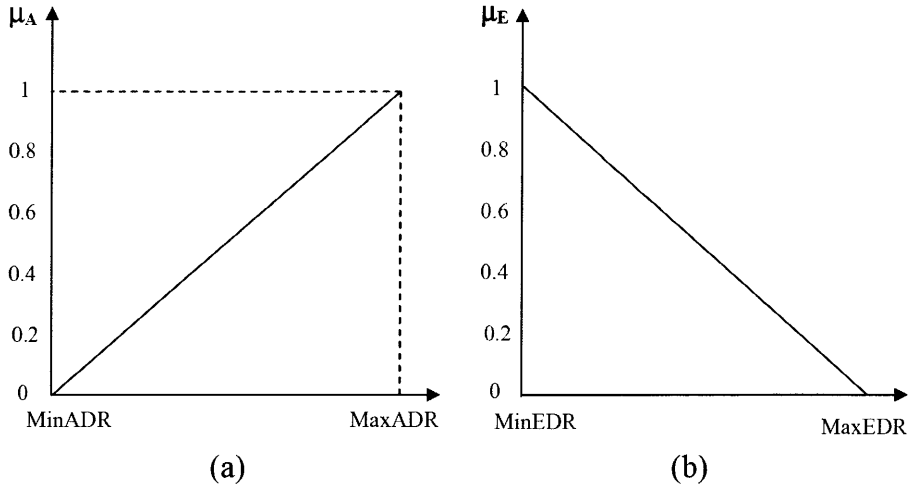


FIGURE 3.1: Membership functions for (a) Attack Detection Rate and (b) Energy Decay Rate.

Formulation of the Multi-criteria Decision-making Problem

The formulation of fuzzy logic and GP for the MCDM problem considered in this thesis and introduced in Section 3.2 is represented in Figures 3.2 and 3.3, respectively.

Figure 3.2 illustrates the flowchart of the problem when applying fuzzy logic to solve it. As was mentioned in Section 3.2, normalization of the both decision criteria (ADR and EDR) need to be done. Normalization is done by finding the membership functions for the two criteria. As was discussed earlier in this section, the membership of ADR is denoted by MemADR and the membership of EDR is denoted by MemEDR. Both ADR and EDR normalized between the minimum and maximum values which were mentioned previously (MinADR, MaxADR, MinEDR, and MaxEDR).

After normalizing the two criteria by calculating the membership functions, the overall membership is calculated. Overall membership is found by applying one of the three fuzzy operators (mathematically represented by Eqs. (2.8) - (2.10)). For the same number of GN nodes and the same value of the operator related parameter, this process is repeated ten times. For each iteration, α value is changed from [0.1-1.0]. The highest overall membership value is the best.

Figure 3.3 illustrates the flowchart of the problem when applying GP to solve it. As was mentioned in Section refsec:mcdm, normalization of the both decision criteria (ADR and EDR) need to be done. Deviations of the normalized criteria are then found. After finding the two deviations (DevADR and DevEDR), the overall deviation is calculated by adding the two deviations. For the same number of GN nodes, the process is repeated ten times. For each iteration, α value is changed from [0.1-1.0]. The lowest overall deviation value is the best.

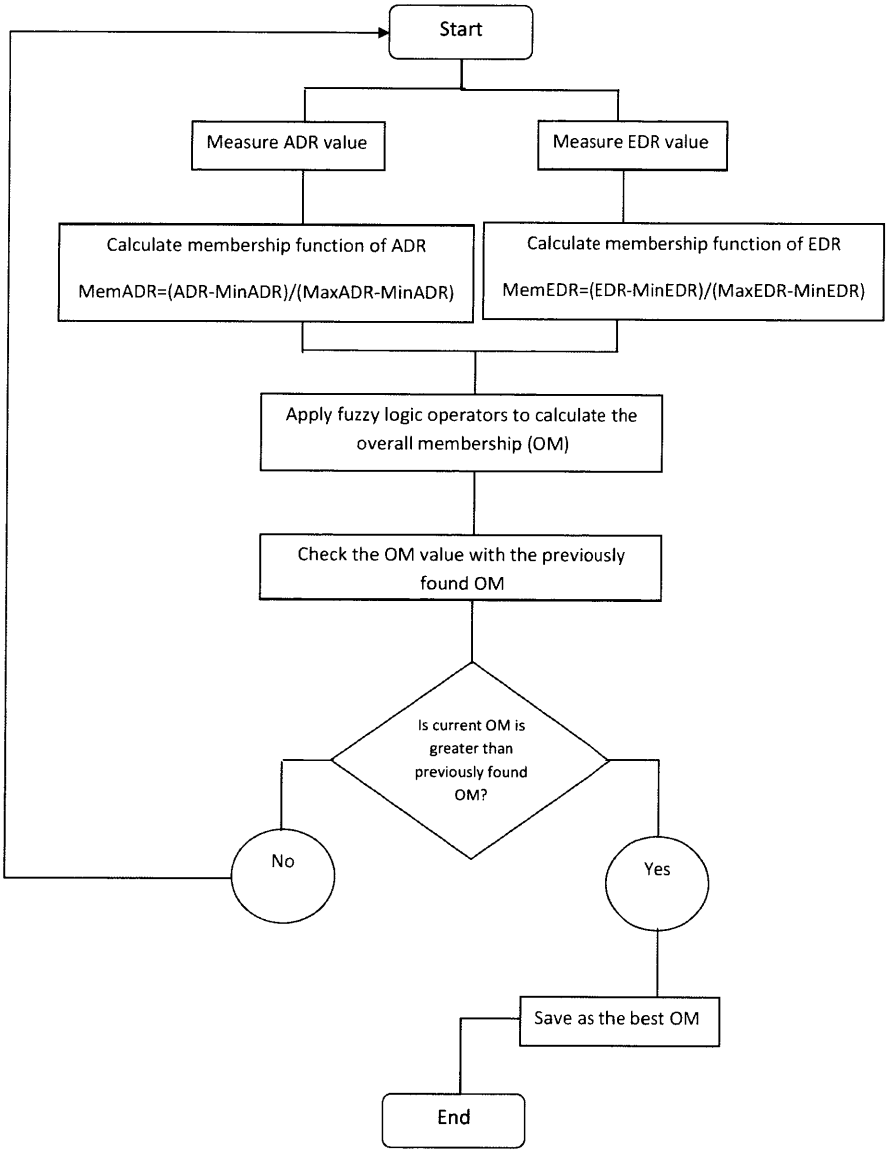


FIGURE 3.2: Flowchart of fuzzy logic for the MCDM problem.

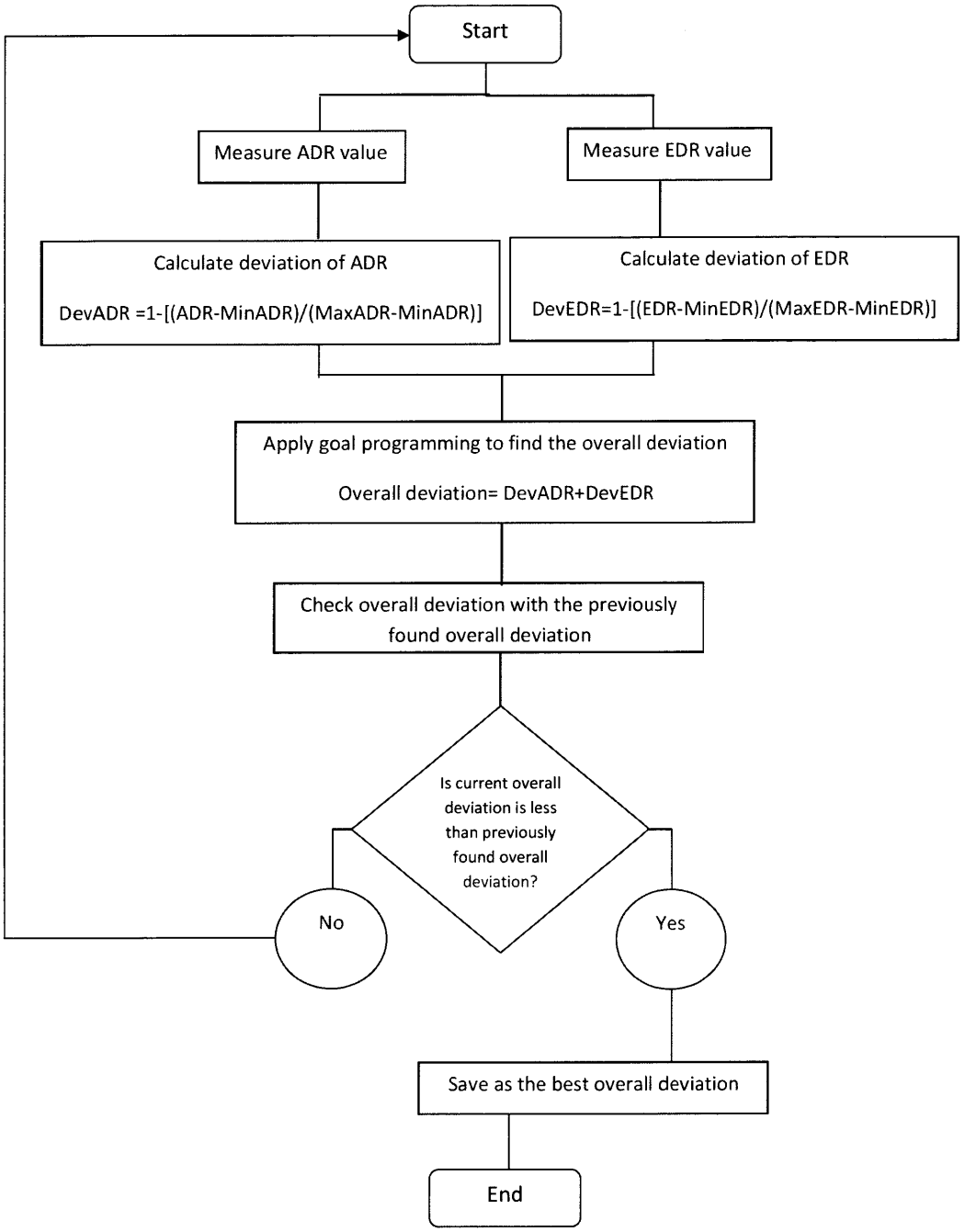


FIGURE 3.3: Flowchart of Goal programming for the MCDM problem.

3.3 Test Cases and Input Data

For the problem considered in this thesis, the input data for the assessment of the proposed approach was taken from the relevant literature [3, 5, 7, 38], which consisted of five different test scenarios having 128, 256, 512, 1024, and 2048 GN nodes. Tables 3.1 to 3.5 provide the necessary details about this input data. Different values of application aspect α, ranging from 0.1 to 1.0, were used as given in column 1 of the tables, and corresponding values of mGN, EDR, and ADR are listed in columns 2, 3, and 4 respectively. Since the decision variables are EDR and ADR, the membership values of these two variables, computed using the membership functions as discussed in Section 2.4, are listed in the last two columns of these tables.

Four sets of experiments were performed, where the effect of variation in operator related parameters, on different factors associated with the DDoS MCDM problem was studied. Recall from Section 2.4, the operator related parameter value lies between 0 and 1. Therefore, the operator related parameter was varied from 0 to 1, with a step size of 0.1. In the first experiment, the effect of number of GN nodes on the best value of α for different values of the operator related parameter was studied. The second experiment focused on the effect of variation in the operator related parameter on the best trade-off between ADR and EDR. In the third experiment, the focus is on evaluating the effect of variation in the value of the operator related parameter on the memberships of EDR and ADR, as well as on the overall membership. Finally, the fourth experiment assessed the effect of value of the operator related parameter on the ratio of mGN and GN nodes.

TABLE 3.1: Values of α, mGN, EDR, and ADR for the test case with 128 GN nodes. The corresponding membership values of EDR and ADR are also listed.

α	mGN	EDR	ADR	MemEDR	MemADR
0.1	2	284.8	0.099	0.996	0.099
0.2	2	296.6	0.100	0.995	0.100
0.3	2	283.6	0.120	0.996	0.120
0.4	2	265.8	0.120	0.997	0.120
0.5	4	464.4	0.130	0.981	0.130
0.6	4	422.8	0.160	0.982	0.160
0.7	4	430.0	0.180	0.984	0.180
0.8	6	615.6	0.190	0.968	0.190
0.9	17	1739.1	0.290	0.875	0.290
1.0	46	4807.0	0.400	0.622	0.400

TABLE 3.2: Values of α, mGN, EDR, and ADR for the test case with 256 GN nodes. The corresponding membership values of EDR and ADR are also listed.

α	mGN	EDR	ADR	MemEDR	MemADR
0.1	2	302.2	0.310	0.994	0.310
0.2	2	259.8	0.360	0.998	0.360
0.3	2	234.2	0.410	1.000	0.410
0.4	3	295.2	0.420	0.995	0.420
0.5	4	331.2	0.440	0.992	0.440
0.6	4	240.0	0.440	1.000	0.440
0.7	6	339.6	0.500	0.991	0.500
0.8	9	469.8	0.560	0.980	0.560
0.9	18	802.8	0.640	0.953	0.640
1.0	69	2711.7	0.710	0.795	0.710

TABLE 3.3: Values of α, mGN, EDR, and ADR for the test case with 512 GN nodes. The corresponding membership values of EDR and ADR are also listed.

α	mGN	EDR	ADR	MemEDR	MemADR
0.1	2	362.0	0.460	0.989	0.460
0.2	2	291.6	0.480	0.995	0.480
0.3	2	248.2	0.490	0.999	0.490
0.4	2	230.0	0.500	1.000	0.500
0.5	4	346.8	0.520	0.991	0.520
0.6	5	361.5	0.540	0.979	0.540
0.7	7	466.9	0.550	0.980	0.550
0.8	10	584.0	0.590	0.971	0.590
0.9	19	1007.0	0.660	0.936	0.660
1.0	91	4377.1	0.760	0.657	0.760

TABLE 3.4: Values of α, mGN, EDR, and ADR for the test case with 1024 GN nodes. The corresponding membership values of EDR and ADR are also listed.

α	mGN	EDR	ADR	MemEDR	MemADR
0.1	2	543.2	0.600	0.974	0.600
0.2	2	461.8	0.670	0.981	0.670
0.3	2	407.4	0.700	0.985	0.700
0.4	2	374.2	0.700	0.988	0.700
0.5	3	490.5	0.710	0.978	0.710
0.6	4	486.8	0.740	0.979	0.740
0.7	6	646.8	0.770	0.966	0.770
0.8	9	919.8	0.790	0.943	0.790
0.9	21	2018.1	0.860	0.852	0.860
1.0	102	8323.2	0.910	0.331	0.910

TABLE 3.5: Values of α, mGN, EDR, and ADR for the test case with 2048 GN nodes. The corresponding membership values of EDR and ADR are also listed.

α	mGN	EDR	ADR	MemEDR	MemADR
0.1	2	714.0	0.85	0.960	0.850
0.2	2	587.8	0.86	0.970	0.860
0.3	2	556.0	0.88	0.973	0.880
0.4	2	489.0	0.88	0.979	0.880
0.5	4	856.8	0.89	0.948	0.890
0.6	4	629.6	0.89	0.967	0.890
0.7	6	820.8	0.91	0.951	0.910
0.8	11	1359.6	0.92	0.907	0.920
0.9	32	3673.6	0.94	0.716	0.940
1.0	113	12102.3	0.96	0.019	0.960

3.4 Conclusions

This chapter provided the background and preliminaries of MCDM with the specific context of DDoS in WSNs. A formal definition of the problem was provided, along with a discussion of various MCDM approaches to the problem considered in this thesis. The chapter also provided the test cases and input data which will be used for empirical analysis and evaluation of the proposed schemes as discussed in the later chapter.

The next chapter is focussed on the application of fuzzy logic aggregation operator, namely, Dubois and Prade's operator to DDoS attack detection in WSNs.

Chapter 4

Application of Dubois & Prade's Operator to DDoS Attack Detection in WSNs

This chapter proposes the application of D&P operator for DDoS Attack Detection in WSNs. A detailed discussion of the process is provided. Following this an empirical analysis is performed to evaluate the effectiveness of the proposed approach.

4.1 Introduction

As discussed in Chapter 2, D&P operator [17] [18] has been applied to a variety of problems [23][12][79], and is mathematically represented in Eq. (4.1) as:

$$f(\mu_A, \mu_B) = \frac{\mu_A \mu_B}{max\{\mu_A, \mu_B, \gamma\}}, \quad 0 \leq \gamma \leq 1 \tag{4.1}$$

where μ_A and μ_B represent the membership values for the two criteria A and B, respectively, and $f(\mu_A, \mu_B)$ represents the value of the overall objective function. γ is a variable referred to as operator related parameter, and is used to control the behavior of the function [17][18]. In the context of the MCDM problem considered herein, μ_A and μ_B represent the membership functions for the two criteria, namely, A and B, respectively. The values of membership functions are always in the zero-one range ($0 \leq \mu_A \leq 1$ and $0 \leq \mu_B \leq 1$).

As mentioned in Chapter 3, for the purpose of the problem considered in this thesis, two linguistic variables were ADR and EDR, with the corresponding membership functions denoted as MemADR and MemEDR respectively. The value of γ varies between 0 and 1. For a value of 0, the result of Eq. (4.1) is found by multiplying the two membership values for ADR and EDR. Then dividing the result of multiplication by the maximum value between the two aforementioned memberships. While a value of 1 shows the pure multiplication function between the memberships of ADR and EDR. This behavior is due the fact that for γ= 1, the denominator of the function Eq. (4.1) will always be 1 regardless of the values of memberships of ADR and EDR.

Figure 4.1 depicts instances of the D&P aggregation operator with different values of γ. The figure illustrates the behavior of the operator when having membership functions in the range 0 to 1 and at the same time changing the value of γ. In Figure 4.1 the three dimensions represent the values of three memberships (μ_A, μ_B, and overall). The color clarifies the range of values of the overall membership. As the overall membership value gets higher, the color changes (red color represents the highest range of the overall membership values). As illustrated in Figures 4.1 (b) to (d), different values of γ for D&P gives almost the same behavior. High values of the overall membership function were measured in Figures 4.1 (b) to (d). Whereas, in Figures 4.1 (e) and (f), lower values of the overall membership function were archived.

4.2 Application of the Dubois and Prade's operator to the problem

As discussed in Section 2.4, t-norms play an important role in fuzzy logic. Since many MCDM problems require simultaneous optimization of multiple and conflicting objectives, the AND operator in a fuzzy rule plays a crucial role in defining that rule. Consequently, a need arises to develop t-norm operators that would effectively handle problems of such nature by efficiently incorporating the characteristics of different criteria (through their membership functions) into a single fuzzy rule. Section 2.4 introduced a number of t-norm operators proposed in the literature. These t-norms are also referred to as "soft AND" functions. The D&P operator is specifically chosen because of its soft AND capability and due to the simple design (refer to the discussion about fuzzy logic in Section 2.4), so as to

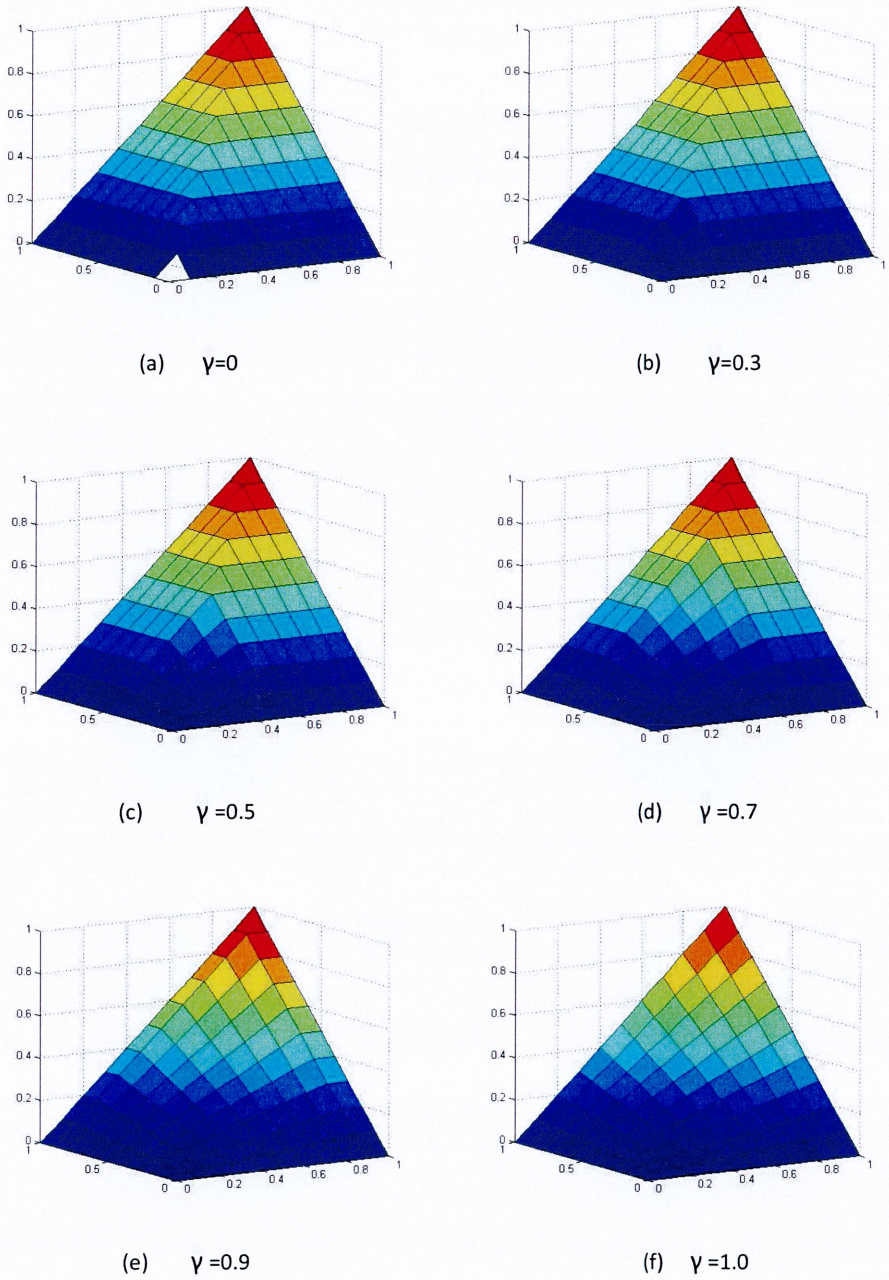


FIGURE 4.1: Effect of γ on D&P function.

be applied to the MCDM problem of selecting the best solution from the set of available alternatives for the DDoS attack detection problem.

The main purpose of attack detection is met in its entirety if the attack detection rate is close to 100%. To achieve this high rate, the two criteria of the attack detection and energy decay rates should be balanced so as to achieve the most optimal ratio of the two, and D&P fuzzy operator seems to be a suitable choice.

The following section analyzes the performance of the proposed approach while considering the effect of the two design criteria.

4.3 Results and Discussion

The applicability and effectiveness of the D&P operator to the MCDM problem under consideration was analyzed through several experiments. As mentioned in Chapter 3, the input data for the assessment and the necessary problem specific details were taken from the relevant literature [3, 5, 7, 38], and are presented in Section 3.3 as described in Tables (3.1) to (3.5). The membership values of attack detection rate, energy decay rate, and operator related parameter, γ, are used to calculate the overall membership by applying the definition of D&P operator. The results is provided in Tables 4.1 to 4.5. Different values of the application aspect ratio α, ranging from 0.1 to 1.0, were used as given in column 1 of the tables, and corresponding values of the overall membership for each value of γ ranging from 0.1 to 1.0 are listed in columns 2 to 11, respectively. The best membership values for each value of γ are denoted in boldface. For instance, the best overall membership for γ=0.1 was found to be 0.4000 at α=0.1 (see Table 4.1).

Following four experiments were performed, where the effect of variation in the D&P operator related parameter, γ, on different factors associated with the DDoS MCDM problem was studied. Recall from Section 4.2, that the value of γ lies between 0 and 1. Therefore, γ was varied from 0 to 1, with a step size of 0.1. In the first experiment, the effect of number of GN nodes on the best value of α for different values of γ was studied. The second experiment focused on the effect of variation in γ on the best trade-off between ADR and EDR. In the third experiment, the effect of variation in the value of γ on the memberships of EDR and ADR, as well as on the overall membership, was evaluated. Finally in the fourth experiment, the effect of value of γ on the ratio of mGN and GN nodes was assessed. Details of these experiments are provided in the following discussion.

TABLE 4.1: Overall membership using D&P operator for different values of γ versus values of α, with GN =128. Best membership values are in boldface.

α	OM (γ=0.1)	OM (γ=0.2)	OM (γ=0.3)	OM (γ=0.4)	OM (γ=0.5)	OM (γ=0.6)	OM (γ=0.7)	OM (γ=0.8)	OM (γ=0.9)	OM (γ=1.0)
0.1	0.0990	0.0990	0.0990	0.0990	0.0990	0.0990	0.0990	0.0990	0.0990	0.0986
0.2	0.1000	0.1000	0.1000	0.1000	0.1000	0.1000	0.1000	0.1000	0.1000	0.0994
0.3	0.1200	0.1200	0.1200	0.1200	0.1200	0.1200	0.1200	0.1200	0.1200	0.1195
0.4	0.1200	0.1200	0.1200	0.1200	0.1200	0.1200	0.1200	0.1200	0.1200	0.1196
0.5	0.1300	0.1300	0.1300	0.1300	0.1300	0.1300	0.1300	0.1300	0.1300	0.1275
0.6	0.1600	0.1600	0.1600	0.1600	0.1600	0.1600	0.1600	0.1600	0.1600	0.1572
0.7	0.1800	0.1800	0.1800	0.1800	0.1800	0.1800	0.1800	0.1800	0.1800	0.1770
0.8	0.1900	0.1900	0.1900	0.1900	0.1900	0.1900	0.1900	0.1900	0.1900	0.1839
0.9	0.2900	0.2900	0.2900	0.2900	0.2900	0.2900	0.2900	0.2900	**0.2820**	**0.2538**
1.0	**0.4000**	**0.4000**	**0.4000**	**0.4000**	**0.4000**	**0.4000**	**0.3553**	**0.3109**	0.2764	0.2487

TABLE 4.2: Overall membership using D&P operator for different values of γ versus values of α, with GN =256. Best membership values are in boldface.

α	OM (γ=0.1)	OM (γ=0.2)	OM (γ=0.3)	OM (γ=0.4)	OM (γ=0.5)	OM (γ=0.6)	OM (γ=0.7)	OM (γ=0.8)	OM (γ=0.9)	OM (γ=1.0)
0.1	0.3100	0.3100	0.3100	0.3100	0.3100	0.3100	0.3100	0.3100	0.3100	0.3082
0.2	0.3600	0.3600	0.3600	0.3600	0.3600	0.3600	0.3600	0.3600	0.3600	0.3591
0.3	0.4100	0.4100	0.4100	0.4100	0.4100	0.4100	0.4100	0.4100	0.4100	0.4099
0.4	0.4200	0.4200	0.4200	0.4200	0.4200	0.4200	0.4200	0.4200	0.4200	0.4177
0.5	0.4400	0.4400	0.4400	0.4400	0.4400	0.4400	0.4400	0.4400	0.4400	0.4363
0.6	0.4400	0.4400	0.4400	0.4400	0.4400	0.4400	0.4400	0.4400	0.4400	0.4396
0.7	0.5000	0.5000	0.5000	0.5000	0.5000	0.5000	0.5000	0.5000	0.5000	0.4955
0.8	0.5600	0.5600	0.5600	0.5600	0.5600	0.5600	0.5600	0.5600	0.5600	0.5489
0.9	0.6400	0.6400	0.6400	0.6400	0.6400	0.6400	0.6400	0.6400	**0.6400**	**0.6097**
1.0	**0.7100**	**0.7100**	**0.7100**	**0.7100**	**0.7100**	**0.7100**	**0.7100**	**0.7055**	0.6271	0.5644

TABLE 4.3: Overall membership using D&P operator for different values of γ versus values of α, with GN =512. Best membership values are in boldface.

α	OM (γ=0.1)	OM (γ=0.2)	OM (γ=0.3)	OM (γ=0.4)	OM (γ=0.5)	OM (γ=0.6)	OM (γ=0.7)	OM (γ=0.8)	OM (γ=0.9)	OM (γ=1.0)
0.1	0.4600	0.4600	0.4600	0.4600	0.4600	0.4600	0.4600	0.4600	0.4600	0.4550
0.2	0.4800	0.4800	0.4800	0.4800	0.4800	0.4800	0.4800	0.4800	0.4800	0.4776
0.3	0.4900	0.4900	0.4900	0.4900	0.4900	0.4900	0.4900	0.4900	0.4900	0.4893
0.4	0.5000	0.5000	0.5000	0.5000	0.5000	0.5000	0.5000	0.5000	0.5000	0.5000
0.5	0.5200	0.5200	0.5200	0.5200	0.5200	0.5200	0.5200	0.5200	0.5200	0.5150
0.6	0.5400	0.5400	0.5400	0.5400	0.5400	0.5400	0.5400	0.5400	0.5400	0.5341
0.7	0.5500	0.5500	0.5500	0.5500	0.5500	0.5500	0.5500	0.5500	0.5500	0.5392
0.8	0.5900	0.5900	0.5900	0.5900	0.5900	0.5900	0.5900	0.5900	0.5900	0.5727
0.9	**0.6600**	**0.6600**	**0.6600**	**0.6600**	**0.6600**	**0.6600**	**0.6600**	**0.6600**	**0.6600**	**0.6176**
1.0	0.6573	0.6573	0.6573	0.6573	0.6573	0.6573	0.6573	0.6245	0.5551	0.4996

TABLE 4.4: Overall membership using D&P operator for different values of γ versus values of α, with GN =1024. Best membership values are in boldface.

α	OM (γ=0.1)	OM (γ=0.2)	OM (γ=0.3)	OM (γ=0.4)	OM (γ=0.5)	OM (γ=0.6)	OM (γ=0.7)	OM (γ=0.8)	OM (γ=0.9)	OM (γ=1.0)
0.1	0.6000	0.6000	0.6000	0.6000	0.6000	0.6000	0.6000	0.6000	0.6000	0.5845
0.2	0.6700	0.6700	0.6700	0.6700	0.6700	0.6700	0.6700	0.6700	0.6700	0.6572
0.3	0.7000	0.7000	0.7000	0.7000	0.7000	0.7000	0.7000	0.7000	0.7000	0.6897
0.4	0.7000	0.7000	0.7000	0.7000	0.7000	0.7000	0.7000	0.7000	0.7000	0.6917
0.5	0.7100	0.7100	0.7100	0.7100	0.7100	0.7100	0.7100	0.7100	0.7100	0.6947
0.6	0.7400	0.7400	0.7400	0.7400	0.7400	0.7400	0.7400	0.7400	0.7400	0.7243
0.7	0.7700	0.7700	0.7700	0.7700	0.7700	0.7700	0.7700	0.7700	0.7700	0.7435
0.8	0.7900	0.7900	0.7900	0.7900	0.7900	0.7900	0.7900	0.7900	0.7900	**0.7450**
0.9	**0.8523**	**0.8523**	**0.8523**	**0.8523**	**0.8523**	**0.8523**	**0.8523**	**0.8523**	**0.8144**	0.0.7329
1.0	0.3313	0.3313	0.3313	0.3313	0.3313	0.3313	0.3313	0.3313	0.3313	0.3015

TABLE 4.5: Overall membership using D&P operator for different values of γ versus values of α, with GN =2048. Best membership values are in boldface.

α	OM (γ=0.1)	OM (γ=0.2)	OM (γ=0.3)	OM (γ=0.4)	OM (γ=0.5)	OM (γ=0.6)	OM (γ=0.7)	OM (γ=0.8)	OM (γ=0.9)	OM (γ=1.0)
0.1	0.8500	0.8500	0.8500	0.8500	0.8500	0.8500	0.8500	0.8500	0.8500	0.8160
0.2	0.8600	0.8600	0.8600	0.8600	0.8600	0.8600	0.8600	0.8600	0.8600	0.8346
0.3	0.8800	0.8800	0.8800	0.8800	0.8800	0.8800	0.8800	0.8800	0.8800	0.8563
0.4	0.8800	0.8800	0.8800	0.8800	0.8800	0.8800	0.8800	0.8800	0.8800	0.8612
0.5	0.8900	0.8900	0.8900	0.8900	0.8900	0.8900	0.8900	0.8900	0.8900	0.8439
0.6	0.8900	0.8900	0.8900	0.8900	0.8900	0.8900	0.8900	0.8900	0.8900	0.8606
0.7	**0.9100**	**0.9100**	**0.9100**	**0.9100**	**0.9100**	**0.9100**	**0.9100**	**0.9100**	**0.9100**	**0.8656**
0.8	0.9067	0.9067	0.9067	0.9067	0.9067	0.9067	0.9067	0.9067	0.9067	0.8341
0.9	0.7155	0.7155	0.7155	0.7155	0.7155	0.7155	0.7155	0.7155	0.7155	0.6725
1.0	0.0190	0.0190	0.0190	0.0190	0.0190	0.0190	0.0190	0.0190	0.0190	0.0182

4.3.1 Effect of number of GN nodes on the best value for α for different values of γ

Figure 4.2 illustrates the progression of aspect value α versus the GN nodes for varying values of D&P related parameter γ. The general trend in the figure is that the best value of α reduced with increasing the number of GN nodes for all values of γ. For instance, in Figure 4.2 (a), the value of α was 1.0 for 128 and 256 nodes which decreased to 0.9 for 512 and 1024 nodes, and eventually to 0.7 for 2048 nodes. This trend is identical in Figure 4.2 (a) to (h) which correspond to the values of γ ranging from 0.1 to 0.8, respectively. A slightly different trend is observed in Figure 4.2 (i) and (j) corresponding to γ= 0.9 and 1.0 respectively, where the highest value of α did not exceed 0.9 for any case.

The decrement in the value of α for higher numbers of the GN nodes is attributed to the corresponding increase in the attack detection rates for achieving higher accuracies. It may be noted here that increasing the number of GN nodes leads to improved attack detection rates for specific number of GN nodes, as the proximity of the GN nodes leads to reduced communication distances that need to be traversed by the GN communication messages.

4.3.2 Effect of value of γ on the best trade-off between ADR and EDR

As mentioned earlier, the application aspect value, α, is a system parameter that defines the level of accuracy in attack detection in comparison with the energy decay rates of the corresponding ratio of GN and mGN nodes. The normalized value of α, which is between [0.0 - 1.0], is defined at network initialization time. In this connection, this section analyzed the effect of value of γ on the best value of α, which in turn represents the best trade-off between ADR and EDR. Figures 4.3 (a) - (e) show the behavior of α while varying the value of γ. It was found that, generally, the best value of α was insensitive to change in γ. In other words, for the same number of nodes, when the behavior of α was compared to that of γ, it was found that the value of α remained steady when γ was varied from 0.0 to 1.0. A small deviation from this trend was for values of γ = 0.9 and 1.0 for GN=128 and 256, where the value of α dropped to 0.9. A similar behavior is observed for GN=1024 where the value of α dropped to 0.8 for γ=1.0. Referring to Eq.(4.1), this small deviation is a very likely consequence of the definition of the D&P function, because the value of the denominator in the function takes the highest value among the membership functions of EDR, ADR, and γ. Notice that in Tables (3.1) to (3.5), the values of the membership functions of EDR and ADR are always greater than the value of γ except for γ= 0.9 and 1.0, which causes that slight deviation from the dominant trend.

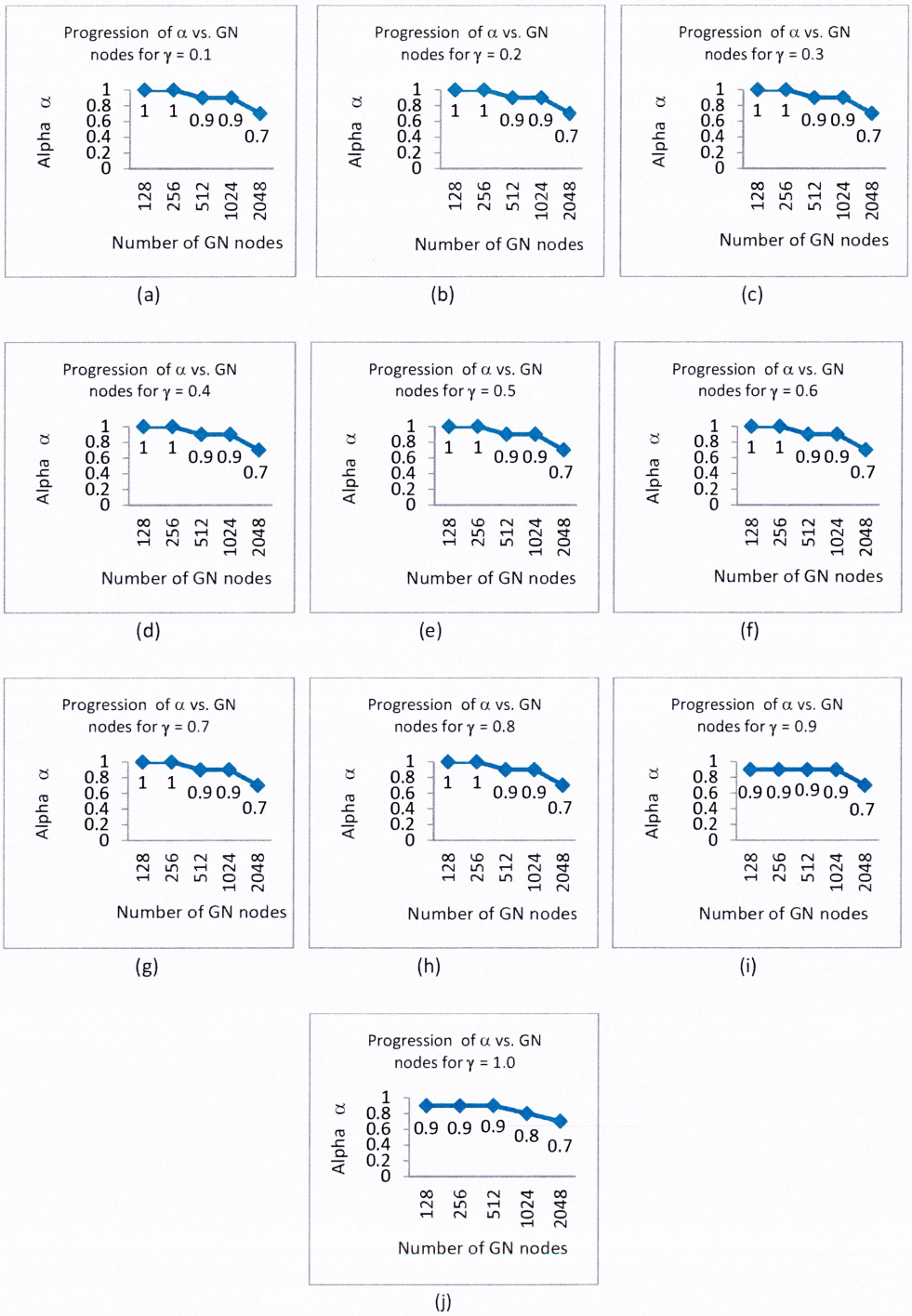


FIGURE 4.2: Progression of α vs GN nodes for (a) $\gamma = 0.1$ (b) $\gamma = 0.2$ (c) $\gamma = 0.3$ (d) $\gamma = 0.4$ (e) $\gamma = 0.5$ (f) $\gamma = 0.6$ (g) $\gamma = 0.7$ (h) $\gamma = 0.8$ (i) $\gamma = 0.9$ (j) $\gamma = 1.0$.

Another observation from the plots in Figure 4.3 is that, for lower values of GN nodes (e.g.128 and 256), the best value of α is in the higher range (0.9 to 1.0), but for medium and higher values of GN nodes (512, 1024, and 2048), the best value of α was relatively in a lower range (0.7 to 0.9). Notice that in Tables (3.1) to (3.5) in Section 3.3, the values of the mGN nodes are significantly increasing for higher values of α, specially from 0.7 to 1.0. This indicates that increasing the numbers of mGN nodes results in higher decay rates, since a higher number of nodes in the scenario participate in the computation and communication associated with the detection process. As a result, the membership function of EDR would be higher and would affect the result more than the membership of ADR and the value of γ.

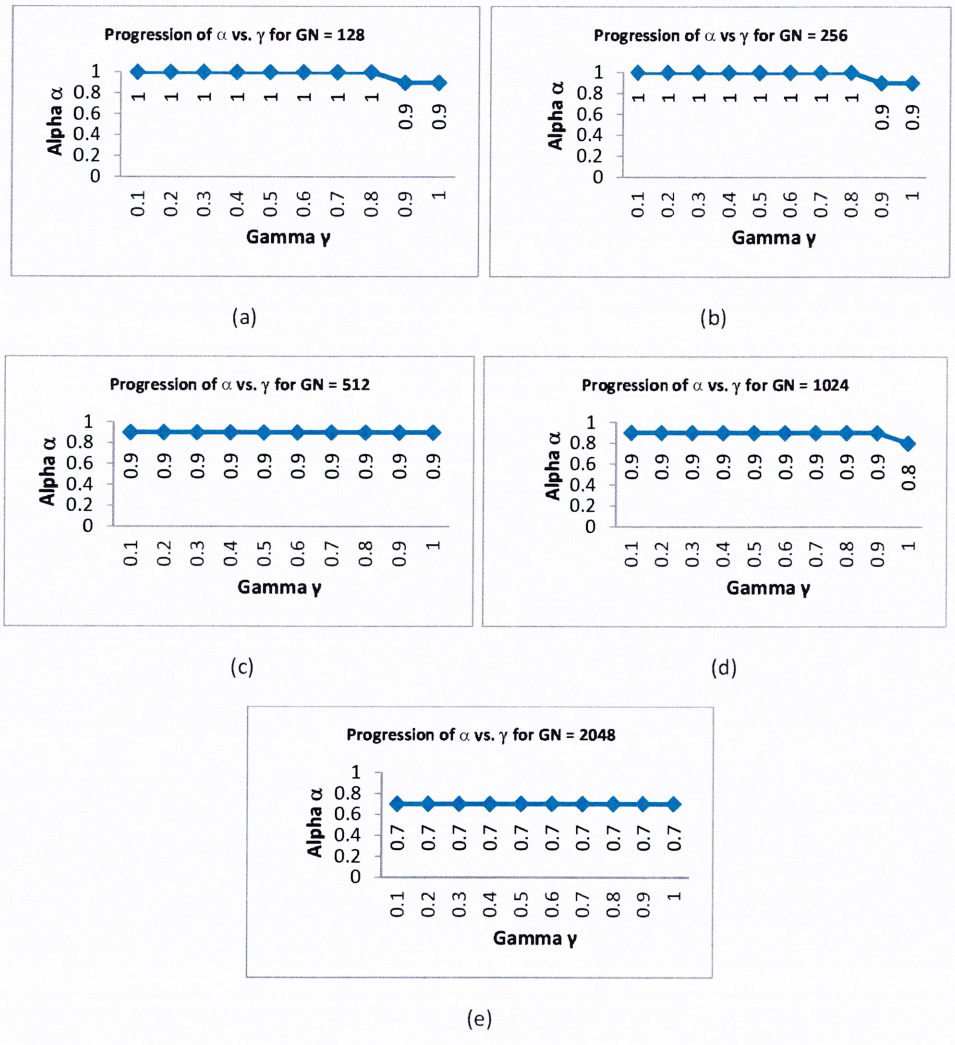


FIGURE 4.3: Effect of value of γ on α for (a) GN = 128 (b) GN = 256 (c) GN = 512 (d) GN = 1024 (e) GN = 2048.

4.3.3 Effect of γ on memberships of ADR, EDR, and overall membership for different number of GN nodes

This experiment analyzed the behavior of the membership functions for both EDR and ADR, while considering the best value of α for which the best value of OM was obtained while keeping the number of nodes constant.

As observed in Section 4.3.2, the best value of α, while keeping the number of nodes the same, decreased with increasing value of γ. More specifically, the value of α remained constant for γ from 0.1 to 0.8, and then started decreasing for values of γ from 0.9 to 1.0. This is prominent for majority of the test cases. As seen in Figure 4.4 (a) - (e), for all test cases, while considering the best value of α, the overall membership was significantly influenced by the membership of ADR. Another general trend from the figure is that for higher values of γ (0.9 and 1.0), both MemADR and OM slightly decreased. For example, in Figure 4.4(a), it is observed that MemADR and OM had more or less the same behavior with respect to change in the values of γ. This behavior is quite different from that of MemEDR. A similar trend is observed in Figures 4.4 (b) - (e). This observation can positively be accounted for by the decrease in the number of mGN nodes along with the decrease in the value of α, and at the same time the increase in the value of γ. Referring to what was previously discussed in Section 4.3.2 with regard to the relationship between the values of mGN and EDR, the mGN values in this case decreased, which resulted in a decrease in EDR. This can be attributed to the same reasons, i.e., participation of less number of nodes in computation and communication associated with the detection process. However, increasing the number of mGN nodes resulted in better ADR, hence the overall membership was dominated by membership of ADR.

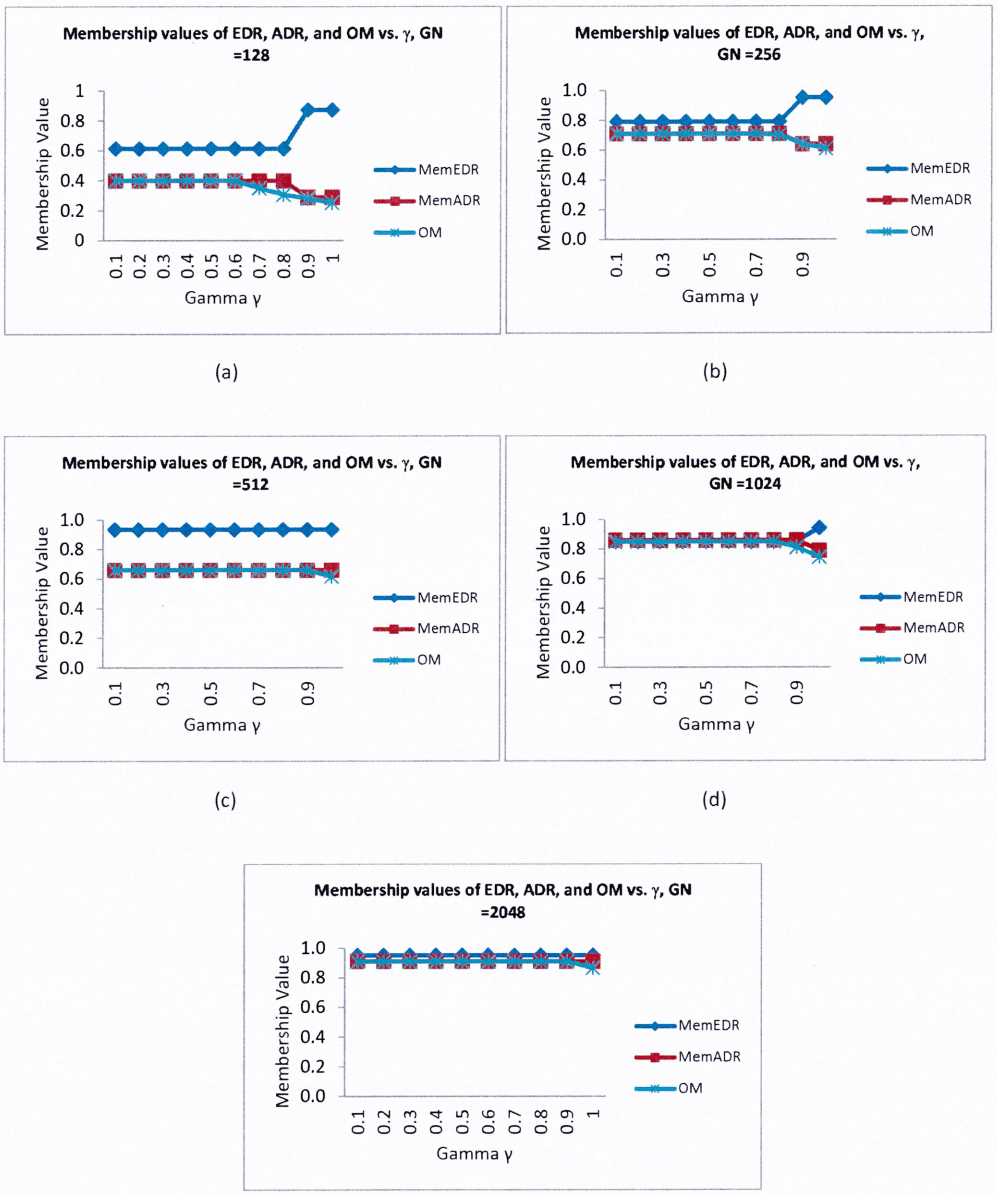


FIGURE 4.4: Effect of γ on MemADR, MemEDR, and OM for (a) GN = 128 (b) GN = 256 (c) GN = 512 (d) GN = 1024 (e) GN = 2048.

4.3.4 Effect of value of γ on the Ratio of mGN and GN nodes

In this experiment, the effect of values of γ on the ratio of mGN and GN nodes was investigated. The results for best values of α are shown in Table (4.6). As observed from the table, the results showed that when the number of GN nodes was increased, the ratio of required number of mGN nodes and GN nodes decreased. Moreover, there was a dominant trend for each specific number of GN nodes. It is observed that for higher values of γ, the requirement of mGN nodes decreased (consider for example GN =128 in column 2 in the table and move vertically downwards) since the mGN/GN ratio decreased. Thus, the ideal ratio of mGN and GN is obtained to facilitate the network scheme operation with the minimal energy overhead on the nodes and at the same time without compromising the accuracy in the attack detection. Therefore, large values of α signify the need for achieving higher accuracies in attack detection, leading to the designation of a large number of GN nodes for the detection scheme in the network.

The trend observed in Table (4.6) can be attributed to the higher number of mGN nodes designated in the scheme for the purpose of attaining the accuracy in the attack detection. Furthermore, smaller values of α lead to fewer numbers of mGN nodes in the network.

TABLE 4.6: Values of γ and the ratio of mGN and GN nodes for N= 128 to 2048 GN nodes.

γ	mGN/GN for GN =128	mGN/GN for GN =256	mGN/GN for GN =512	mGN/GN for GN =1024	mGN/GN for GN =2048
0.1	0.359375	0.269531	0.037109	0.020508	0.00293
0.2	0.359375	0.269531	0.037109	0.020508	0.00293
0.3	0.359375	0.269531	0.037109	0.020508	0.00293
0.4	0.359375	0.269531	0.037109	0.020508	0.00293
0.5	0.359375	0.269531	0.037109	0.020508	0.00293
0.6	0.359375	0.269531	0.037109	0.020508	0.00293
0.7	0.359375	0.269531	0.037109	0.020508	0.00293
0.8	0.359375	0.269531	0.037109	0.020508	0.00293
0.9	0.132813	0.070313	0.037109	0.020508	0.00293
1.0	0.132813	0.070313	0.037109	0.008789	0.00293

4.4 Conclusions

This chapter investigated the applicability and effectiveness of the D&P operator to the MCDM problem under consideration through several experiments. The investigation focused on the usage of D&P operator for decision-making between the two conflicting criteria of interest. This was analyzed by varying the value of a network parameter known as application aspect ratio, α. Experimental results showed that the best value of α lies between 0.7 and 1.0, for all networks tested (GN=128 to 2048). It was also observed that the value of α was somewhat insensitive to change in the value of operator related parameter, γ. Another important finding was that the overall membership follows more or less the same pattern as that of the membership of ADR, which suggests that the overall decision was significantly influenced by the behavior of the ADR.

The next chapter discusses the application of another fuzzy operator, namely, Werners operator, to the same problem addressed in this thesis.

Chapter 5

Application of Werners Operator to DDoS Attack Detection in WSNs

This chapter provides a brief overview of the Werners fuzzy aggregation operator, followed by a detailed discussion as how the operator has been applied to the problem considered in this thesis. The chapter focusses on the same decision criteria that were considered in Chapter 4, namely the attack detection rate and energy decay rate. Results and discussion of empirical analysis are provided in this chapter to evaluate the effectiveness of the proposed approach.

5.1 Introduction

As discussed in chapter 2, Werners operator [72, 73] is mathematically represented in Eq. (5.1).

$$W(\mu_A, \mu_B) = \beta \times \min\{\mu_A, \mu_B\} + (1-\beta) \times \frac{1}{2}(\mu_A + \mu_B), \quad 0 \leq \beta \leq 1 \tag{5.1}$$

In this equation, μ_A and μ_B represent the membership to the fuzzy set for two criteria A and B, respectively, and $f(\mu_A, \mu_B)$ represents the value of the overall objective function. The variable β is a parameter associated with the Werners operator and is referred to as the operator related parameter. It is used to control the behavior of the function.

The value of β varies between 0 and 1, and is crucial in deciding the level of softness of the pure-AND definition by [78]. For instance, in Eq. (5.1), the more the value of β tends towards 1, the lower is the level of softness of the ANDing. As the value of β is lowered, the extent of pure-ANDing is decreased, thus making it a softer-AND. The reason for this is that the definition of the Werners operator is utilizing the hardest and the softest definitions of the AND-function. First, the pure-AND definition by Zadeh [78] which is the rigid definition. Second, the definition of the average of a group of values which tends to be very soft definition of AND. Figure 5.1 depicts instances of the Werners operator with different values of β. The behavior of the Werners function of Eq. (5.1) is illustrated in Figure 5.1. The figure illustrates the behavior of the operator using three membership functions in the range 0 to 1 (μ_A, μ_B, and overall) which are represented in three dimensions. The color clarifies the range of values of the overall membership. As the overall membership value gets higher, the color changes (red color represents the highest range of the overall membership values).

When $\beta = 0$ (Figure 5.1 (a)), the function takes the average between the two membership values. The overall membership found to be the mean value between MemADR and MemEDR. The shape of Figure 5.1 (a) shows the behavior of the average function. As the value of β is increased, the "ANDing" between the two membership values also increases. The shape of Figures 5.1 (b) to (e) is changing towards the shape of the pure-AND function with the increasing of the value of β. As mentioned earlier, when $\beta = 1$ (Figure 5.1 (f)), the behavior of the function is exactly the same as that of pure-AND defined by Zadeh [78]. The pure-AND behavior takes the minimum value between the two membership functions in the case of $\beta = 1$.

An elaborated discussion on the application of the Werners operator to the problem in this thesis is given in the next few sections.

5.2 Application of the Werners operator to the problem

As discussed previously in Chapter 4, the main purpose of the application of different fuzzy operators characterized by their soft AND function capability is to evaluate the performance of such operators when applied to the MCDM problem considered in this thesis. Recall from Section 4.2, the two criteria that were

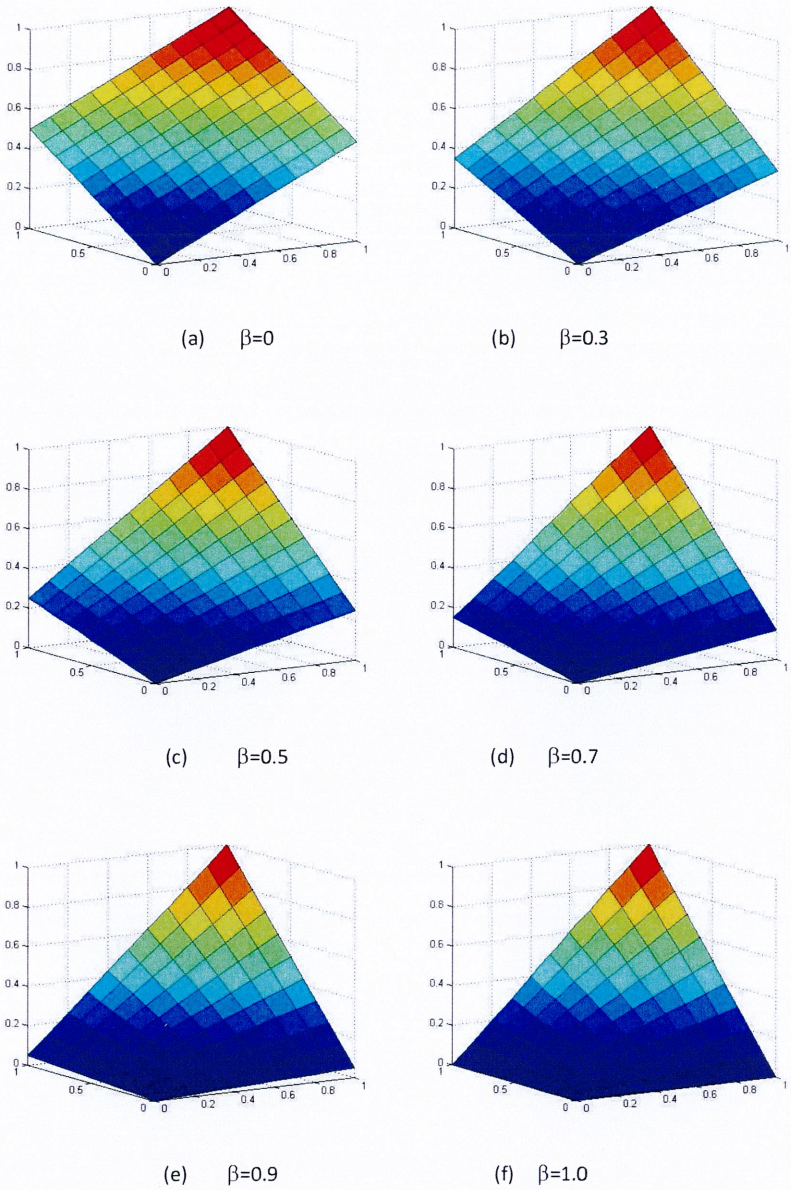


FIGURE 5.1: Effect of β on Werners function.

considered in this thesis are defined as ADR and EDR, with their corresponding membership functions MemADR and MemEDR respectively. The associated parameter β in the Werners function works exactly the same as the D&P operator related parameter (discussed in Chapter 4) for controlling the behavior of the function towards "softening" of AND. Thus, the equation defined by Werners provides the trade-off between frequent attack detection, and the lifetimes of the attack detector nodes which corresponds to the energy consumption rate in each node.

5.3 Results and Discussion

For the purpose of this chapter, several experiments were performed to evaluate and analyze the applicability and effectiveness of the Werners operator to the problem. In this context, detailed discussions are given below.

The input data for the assessment of the proposed approach is the same as proposed in Section 3.3 described in Tables (3.1) to (3.5). Moreover the four sets of experiments that were performed in Section 4.3 for D&P operator, and were also performed for the Werners operator. Tables 5.1 to 5.5 provide the results, which were obtained after running several tests on the input data. Different values of the application aspect ratio α, ranging from 0.1 to 1.0, were used as given in column 1 of the tables, and corresponding values of the overall membership for each value of β ranging from 0.1 to 1.0 are listed in columns 2 to 11, respectively. The membership values of ADR, EDR, and operator related parameter, β, are used to calculate the overall membership by applying the definition of Werners operator. The results are then listed in Tables 5.1 to 5.5 and the best membership values for each value of β are denoted in boldface.

TABLE 5.1: Overall membership using Werners operator for different values of β versus values of α, with GN =128. Best membership values are in boldface.

α	OM (β=0.1)	OM (β=0.2)	OM (β=0.3)	OM (β=0.4)	OM (β=0.5)	OM (β=0.6)	OM (β=0.7)	OM (β=0.8)	OM (β=0.9)	OM (β=1.0)
0.1	0.5024	0.4577	0.4128	0.3680	0.3232	0.2783	0.2335	0.1887	0.1438	0.0990
0.2	0.5025	0.4579	0.4131	0.3684	0.3237	0.2789	0.2342	0.1895	0.1447	0.1000
0.3	0.5140	0.4703	0.4265	0.3827	0.3390	0.2952	0.2514	0.2076	0.1638	0.1200
0.4	0.5147	0.4709	0.4271	0.3832	0.3393	0.2955	0.2516	0.2077	0.1639	0.1200
0.5	0.5128	0.4702	0.4277	0.3852	0.3427	0.3001	0.2576	0.2151	0.1725	0.1300
0.6	0.5301	0.4890	0.4478	0.4067	0.3656	0.3245	0.2834	0.2422	0.2011	0.1600
0.7	0.5416	0.5014	0.4612	0.4211	0.3809	0.3407	0.3005	0.2604	0.2202	0.1800
0.8	0.5402	0.5012	0.4623	0.4234	0.3845	0.3456	0.3067	0.2678	0.2289	0.1900
0.9	**0.5534**	**0.5233**	**0.4941**	**0.4650**	0.4358	0.4066	0.3775	0.3483	0.3192	0.2900
1.0	0.4998	0.4859	0.4752	0.4644	**0.4537**	**0.4430**	**0.4322**	**0.4215**	**0.4107**	**0.4000**

TABLE 5.2: Overall membership using Werners operator for different values of β versus values of α, with GN =256. Best membership values are in boldface.

α	OM (β=0.1)	OM (β=0.2)	OM (β=0.3)	OM (β=0.4)	OM (β=0.5)	OM (β=0.6)	OM (β=0.7)	OM (β=0.8)	OM (β=0.9)	OM (β=1.0)
0.1	0.6178	0.5837	0.5495	0.5153	0.4811	0.4469	0.4126	0.3784	0.3442	0.3100
0.2	0.6469	0.6151	0.5832	0.5513	0.5195	0.4876	0.4557	0.4238	0.3919	0.3600
0.3	0.6753	0.6460	0.6165	0.5870	0.5575	0.5280	0.4985	0.4690	0.4395	0.4100
0.4	0.6786	0.6499	0.6212	0.5924	0.5637	0.5350	0.5062	0.4775	0.4487	0.4200
0.5	0.6882	0.6607	0.6331	0.6055	0.5780	0.5504	0.5228	0.4952	0.4676	0.4400
0.6	0.6916	0.6638	0.6358	0.6079	0.5799	0.5519	0.5239	0.4960	0.4680	0.4400
0.7	0.7209	0.6964	0.6719	0.6473	0.6228	0.5982	0.5737	0.5491	0.5246	0.5000
0.8	0.7491	0.7280	0.7070	0.6860	0.6650	0.6440	0.6230	0.6020	0.5810	0.5600
0.9	**0.7807**	**0.7648**	**0.7492**	0.7336	0.7180	0.7024	0.6868	0.6712	0.6556	0.6400
1.0	0.7482	0.7425	0.7385	**0.7344**	**0.7303**	**0.7263**	**0.7222**	**0.7181**	**0.7141**	**0.7100**

TABLE 5.3: Overall membership using Werners operator for different values of β versus values of α, with GN =512. Best membership values are in boldface.

α	OM (β=0.1)	OM (β=0.2)	OM (β=0.3)	OM (β=0.4)	OM (β=0.5)	OM (β=0.6)	OM (β=0.7)	OM (β=0.8)	OM (β=0.9)	OM (β=1.0)
0.1	0.6981	0.6717	0.6452	0.6188	0.5923	0.5658	0.5394	0.5129	0.4865	0.4600
0.2	0.7117	0.6860	0.6603	0.6345	0.6088	0.5830	0.5573	0.5315	0.5058	0.4800
0.3	0.7188	0.6935	0.6681	0.6426	0.6172	0.5918	0.5663	0.5409	0.5154	0.4900
0.4	0.7250	0.7001	0.6751	0.6501	0.6251	0.6001	0.5750	0.5500	0.5250	0.5000
0.5	0.7317	0.7082	0.6847	0.6612	0.6376	0.6141	0.5906	0.5671	0.5435	0.5200
0.6	0.7421	0.7197	0.6973	0.6748	0.6523	0.6299	0.6074	0.5849	0.5625	0.5400
0.7	0.7437	0.7222	0.7006	0.6791	0.6576	0.6361	0.6146	0.5930	0.5715	0.5500
0.8	0.7613	0.7422	0.7232	0.7042	0.6851	0.6661	0.6471	0.6281	0.6090	0.5900
0.9	**0.7841**	**0.7700**	**0.7562**	**0.7425**	**0.7287**	**0.7150**	**0.7012**	**0.6875**	**0.6737**	**0.6600**
1.0	0.7035	0.6946	0.6892	0.6837	0.6783	0.6728	0.6674	0.6619	0.6565	0.6510

TABLE 5.4: Overall membership using Werners operator for different values of β versus values of α, with GN =1024. Best membership values are in boldface.

α	OM (β=0.1)	OM (β=0.2)	OM (β=0.3)	OM (β=0.4)	OM (β=0.5)	OM (β=0.6)	OM (β=0.7)	OM (β=0.8)	OM (β=0.9)	OM (β=1.0)
0.1	0.7684	0.7496	0.7309	0.7122	0.6935	0.6748	0.6561	0.6374	0.6187	0.6000
0.2	0.8099	0.7943	0.7788	0.7632	0.7477	0.7322	0.7166	0.7011	0.6855	0.6700
0.3	0.8284	0.8142	0.7999	0.7856	0.7714	0.7571	0.7428	0.7285	0.7143	0.7000
0.4	0.8296	0.8153	0.8009	0.7865	0.7721	0.7576	0.7432	0.7288	0.7144	0.7000
0.5	0.8308	0.8174	0.8039	0.7905	0.7771	0.7637	0.7503	0.7368	0.7234	0.7100
0.6	0.8475	0.8355	0.8235	0.8116	0.7997	0.7877	0.7758	0.7639	0.7519	0.7400
0.7	0.8580	0.8481	0.8383	0.8286	0.8188	0.8090	0.7993	0.7895	0.7798	0.7700
0.8	**0.8589**	0.8509	0.8433	0.8357	0.8281	0.8204	0.8128	0.8052	0.7976	0.7900
0.9	0.8557	**0.8538**	**0.8533**	**0.8528**	**0.8523**	**0.8518**	**0.8512**	**0.8507**	**0.8502**	**0.8497**
1.0	0.5917	0.5552	0.5256	0.4960	0.4665	0.4369	0.4073	0.3777	0.3482	0.3186

TABLE 5.5: Overall membership using Werners operator for different values of β versus values of α, with GN =2048. Best membership values are in boldface.

α	OM (β=0.1)	OM (β=0.2)	OM (β=0.3)	OM (β=0.4)	OM (β=0.5)	OM (β=0.6)	OM (β=0.7)	OM (β=0.8)	OM (β=0.9)	OM (β=1.0)
0.1	0.8995	0.8938	0.8884	0.8829	0.8774	0.8719	0.8664	0.8610	0.8555	0.8500
0.2	0.9097	0.9041	0.8986	0.8931	0.8876	0.8820	0.8765	0.8710	0.8655	0.8600
0.3	0.9219	0.9172	0.9125	0.9079	0.9032	0.8986	0.8939	0.8893	0.8846	0.8800
0.4	0.9244	0.9194	0.9145	0.9096	0.9046	0.8997	0.8948	0.8899	0.8849	0.8800
0.5	0.9162	0.9130	0.9101	0.9073	0.9044	0.9015	0.8986	0.8958	0.8929	0.8900
0.6	0.9246	0.9207	0.9168	0.9130	0.9092	0.9053	0.9015	0.8977	0.8938	0.8900
0.7	**0.9285**	**0.9262**	**0.9242**	**0.9222**	**0.9202**	**0.9181**	**0.9161**	**0.9141**	**0.9120**	**0.9100**
0.8	0.9127	0.9111	0.9104	0.9096	0.9089	0.9082	0.9074	0.9067	0.9059	0.9052
0.9	0.8165	0.8022	0.7907	0.7792	0.7677	0.7562	0.7448	0.7333	0.7218	0.7103
1.0	0.4425	0.3842	0.3362	0.2882	0.2402	0.1922	0.1443	0.0963	0.0483	0.0003

5.3.1 Effect of number of GN nodes on the best value for α for different values of β

As discussed earlier in Section 4.3.1, the progression of α versus the GN nodes for varying values of β is illustrated. Tables (5.1) to (5.5) provide the results obtained after application of Werners operator to the problem considered in this thesis. A general trend in Figure 5.2 (a) - (j) is that the best value of α is reducing with the increasing number of GN nodes. This was observed for all values of β varying from 0.1 Figure (5.2 (a)) to 1.0 Figure (5.2 (j)). For instance, for 128, 256, and 512 nodes, the best value of α was 0.9 as observed in Figure 5.2 (a). When the number of GN nodes was increased to 1024 nodes, the best value of α decreased to 0.8. Furthermore, for a higher number, which is 2048 nodes, value of α was 0.7. This trend is common in Figure 5.2 (a) - (j), with the exception of Figure 5.2 (d), corresponding to β= 0.4 when the value of α increased from 0.9 (for GN= 128 nodes) to 1.0 (for GN= 256 nodes).

One possible argument for this behavior is that the increase in the number of GN nodes in a WSN will increase the ADR in that network for achieving higher accuracies, as was observed in Tables (3.1) to (3.5) in Chapter 4. This results in a decrement in the value of α for the higher values of the GN nodes. The improved attack detection rates for individual GN nodes is attributed to the increase in the values of GN nodes, as the proximity of the GN nodes leads to reduced communication distances that need to be traversed by the GN communication messages.

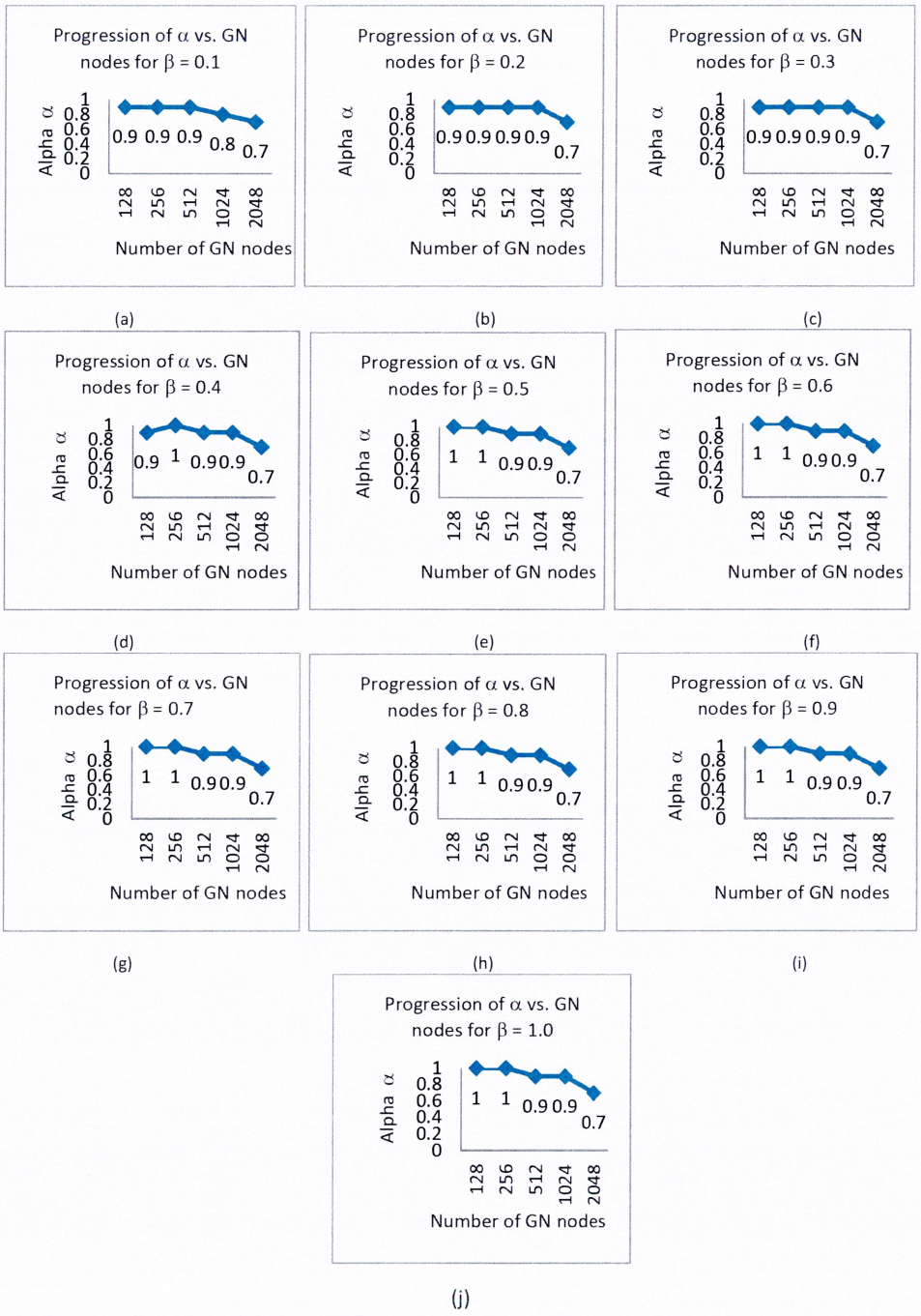


FIGURE 5.2: Progression of α vs GN nodes for (a) β= 0.1 (b) β= 0.2 (c) β= 0.3 (d) β= 0.4 (e) β= 0.5 (f) β= 0.6 (g) β= 0.7 (h) β= 0.8 (i) β= 0.9 (j) β= 1.0.

5.3.2 Effect of value of β on the best trade-off between ADR and EDR

In this section, the effect of value of β on the best value of the application aspect value, α, is analyzed. Recall that, the system parameter α represents the best trade-off between ADR and EDR. Figures 5.3 (a) - (e) show the effect on the value of α while varying the value of β. For some test cases (e.g. GN= 512 and 2048 nodes) which are illustrated in Figure 5.3 (c) and (e) respectively, the behavior of α for different values of β found to be the same. In the two aforementioned test cases, the best value of α was insensitive to the change in the value of β. Moreover, for the other test cases, for example 128, 256, and 1024 nodes in Figures 5.3 (a), (b), and (d) respectively, the value of α was increasing when the value of β increased. For instance, in Figure 5.3 (a), the value of the best trade-off α increased from 0.9 (for β= 0.0 to 0.4) to 1.0 when increasing β to 0.5 and above.

This behavior is justified by referring to Eq. (5.1); the small deviation is a very likely consequence of the definition of the Werners function (refer to the discussion in Section 5.1). When β= 0, the Werners function takes the average of the two membership values (soft-ANDing). As the value of β is increased, the level of ANDing between the two memberships is also increased. For instance, when β= 1, the Werners function takes the minimum between the two membership values (hard-ANDing). As for the effect of the number of mGN on the best trade-off between ADR and EDR, the obtained results suggest that the number of mGN has an indirect effect on the result. Notice that in Tables (3.1) to (3.5) in Section 3.3, the values of the mGN nodes are significantly increasing for higher values of α specially from 0.7 to 1.0. Thus, increasing the number of mGN nodes results in higher energy decay rates, since a higher number of nodes in the scenario participate in the computation and communication associated with the detection process. As a result, nodes will conserve more energy, high energy decay rates means higher values for the membership value MemEDR (see Section 5.2). Hence, the membership function MemADR is roughly less than MemEDR (in 90% of the test cases) and will affect the result more than the MemEDR, and the value of β. This is due to the definition of the Werners function given in Eq. (5.1) which takes the minimum among the membership functions of the two criteria, i.e., ADR and EDR, and in the values herein is MemADR. In brief, the best trade-off is influenced by different values of β in a balanced manner due to the mixture of the hardest and softest definitions of ANDing.

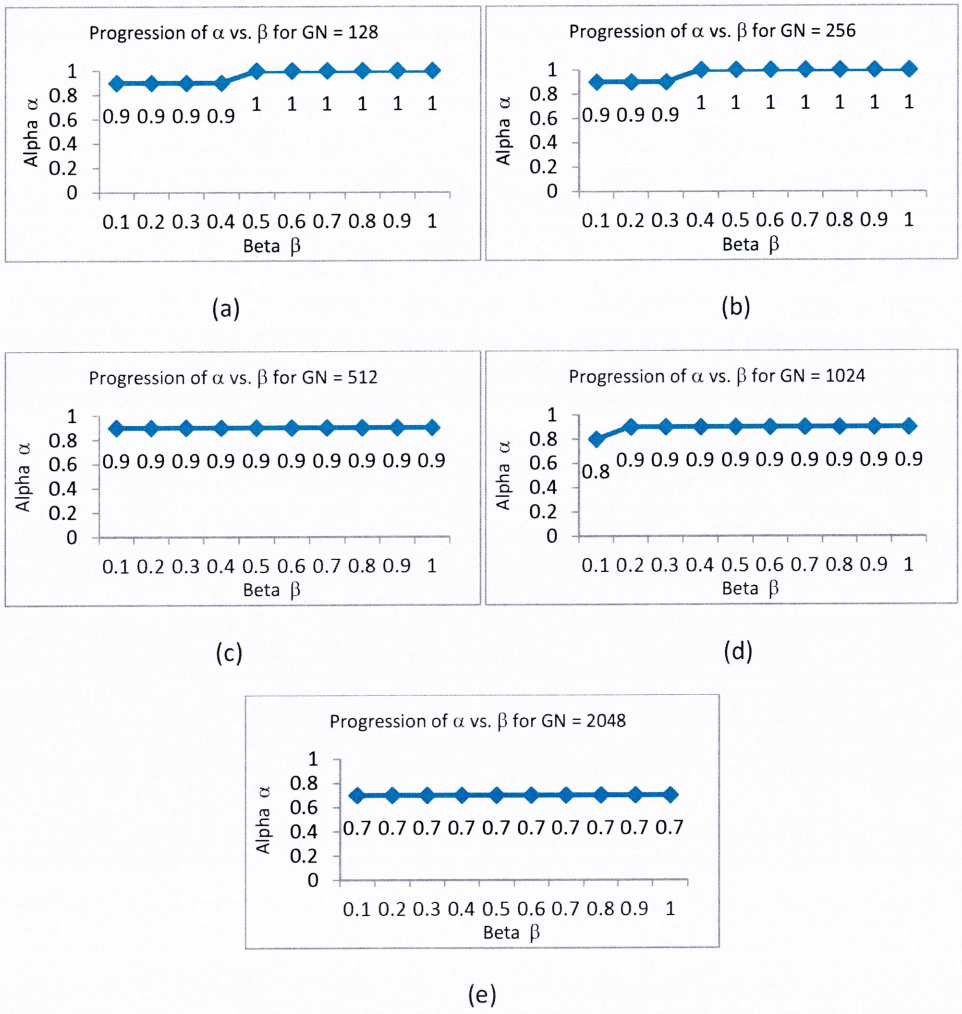


FIGURE 5.3: Effect of value of β on α for (a) GN = 128 (b) GN = 256 (c) GN = 512 (d) GN = 1024 (e) GN = 2048

5.3.3 Effect of β on memberships of ADR, EDR, and overall membership for different number of GN nodes

This section focusses on the behavior of the membership functions for both EDR and ADR. The behavior of the two criteria is analyzed while considering the best value of α for which the best value of overall membership (OM) was produced while keeping the number of GN nodes constant.

As observed in Section 5.3.2, the best value of α for the same number of nodes increased with increasing the value of β. In other words, the best value of the OM is directly proportional to the increase in the number of nodes (see Tables 5.1 to 5.5). Figure 5.4 (a) - (e) shows that for all test cases, while considering the best value of α, the overall membership was significantly influenced by the membership

of ADR. Another general trend from the figure is that for higher values of β (0.9 and 1.0) both MemADR and OM slightly decreased. For example, in Figure 5.4 (a), it is observed that MemADR and OM had more or less the same behavior with respect to change in the value of β. This behavior is quite different from that of MemEDR. A similar trend is observed in Figures 5.4 (b) - (e). This observation can positively be accounted for by the decrease in the number of mGN nodes along with the decrease of the value of α, and at the same time the increase in the value of β. Referring to the discussion in Section 5.3.2 with regard to the relationship between the values of mGN and EDR, the mGN values in this case decreased which resulted in a decrease in EDR. This can be attributed to the same reasons, i.e., participation of lower number of nodes in the computation and communication associated with the detection process. As a consequence, this conserves energy in the nodes and results in lower MemEDR. Hence, the overall membership was dominated by membership of ADR because the definition of the Werners function is always based on the minimum value among the membership function of the two criteria.

5.3.4 Effect of value of β on the Ratio of mGN and GN nodes

In this section, the effect of values of β on the ratio of mGN and GN nodes was investigated. The results for values of α for which the best trade-off was found are shown in Table (5.6). As discussed in Chapter 3, it is observed that the ideal ratio of mGN and GN is required to facilitate the detection scheme with the minimal energy overhead on the nodes and at the same time, without compromising the accuracy in the attack detection. In addition, for the WSN design adopted in this thesis, large values of α signify the need for achieving higher accuracies in attack detection.

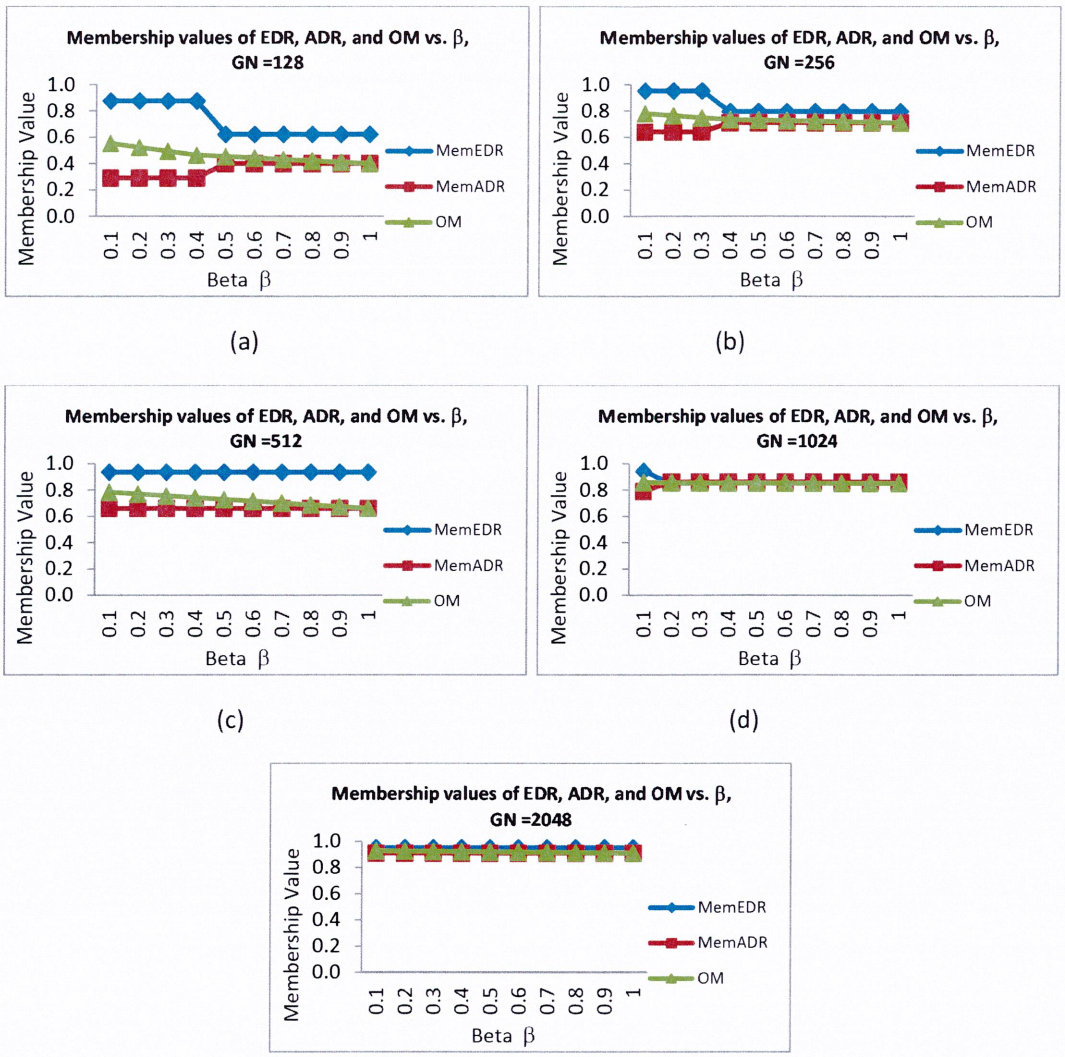


FIGURE 5.4: Effect of β on MemADR, MemEDR, and OM for (a) GN = 128 (b) GN = 256 (c) GN = 512 (d) GN = 1024 (e) GN = 2048.

Therefore, the selection of large values of α leads to the designation of a large number of mGN nodes for the detection scheme in a network. For instance, Figure 5.3 (a) - (e) shows the high values of α for the best trade-off, while varying values of β. This can be attributed to the higher number of mGN nodes designated in the scheme for the purpose of attaining the accuracy in the attack detection. Furthermore, smaller values of α lead to fewer numbers of mGN nodes in the network.

As observed from the Table (5.6), for the same number of GN nodes, the ratio of mGN and GN nodes is increasing (consider for example GN =128 and move vertically downwards). One reason for this is the increasing values of α which corresponds to increasing the number of mGN nodes in the network. This in turn will increase the value of the numerator in the calculated ratio and increasing the ratio as a result.

TABLE 5.6: Values of β and the ratio of mGN and GN nodes for N= 128 to 2048 GN nodes.

β	mGN/GN for GN =128	mGN/GN for GN =256	mGN/GN for GN =512	mGN/GN for GN =1024	mGN/GN for GN =2048
0.1	0.1328	0.0703	0.0371	0.0088	0.0029
0.2	0.1328	0.0703	0.0371	0.0205	0.0029
0.3	0.1328	0.0703	0.0371	0.0205	0.0029
0.4	0.1328	0.2695	0.0371	0.0205	0.0029
0.5	0.3594	0.2695	0.0371	0.0205	0.0029
0.6	0.3594	0.2695	0.0371	0.0205	0.0029
0.7	0.3594	0.2695	0.0371	0.0205	0.0029
0.8	0.3594	0.2695	0.0371	0.0205	0.0029
0.9	0.3594	0.2695	0.0371	0.0205	0.0029
1.0	0.3594	0.2695	0.0371	0.0205	0.0029

5.4 Conclusions

This chapter presented and investigated the applicability and effectiveness of the Werners fuzzy operator to the MCDM problem under consideration through several experiments. The investigation focused on the usage of the aforementioned operator for decision-making between the two conflicting criteria of interest. Moreover, empirical evaluation and discussion of the application aspect ratio, α, were obtained to evaluate the performance of the proposed approach. Experimental results showed that the best value of α lies between 0.7 and 1.0, for all networks tested (GN=128 to 2048). It was also observed that the value of α was somewhat insensitive to change in the value of Werners operator related parameter, β. Another important finding was the behavior of the overall membership which follows more or less the same pattern as that of the membership of ADR, which suggests that the overall decision was significantly influenced by the behavior of ADR.

The next chapter discusses the application of yet another fuzzy operator, known as the UAO operator, to the problem studied in this thesis.

Chapter 6

Application of Unified AND-OR Operator to DDoS Attack Detection in WSNs

This chapter proposes the application of UAO operator to the DDoS attack detection in WSNs. This operator is shown to have mathematical properties similar to that of the UAO operator discussed in Chapter 5. An overview of the UAO fuzzy aggregation operator is provided. To illustrate the effectiveness of the proposed operator and its applicability to the proposed scheme, empirical analysis is performed. This is followed by a detailed discussion of the analyzed results using some examples and tests.

6.1 Introduction

As discussed in Chapter 2, UAO operator [37, 38, 39] has received considerable attention in the domain of fuzzy multi-objective optimization. This operator is mathematically represented in Eq. (6.1).

$$U(\mu_A, \mu_B) = \frac{\mu_A \mu_B + \nu \max(\mu_A, \mu_B)}{\nu + \max(\mu_A, \mu_B)}, \quad 0 \leq \nu \leq 1 \tag{6.1}$$

where μ_A and μ_B represent the membership values for two criteria A and B, respectively, and $f(\mu_A, \mu_B)$ represents the value of the overall objective function. ν is a variable referred to as the operator related parameter used to control the

behavior of the operator. This value defines the behavior of the function. Experimentation with different values of ν suggests that the behavior of the UAO operator is more similar to the AND definition with values of ν less than or equal to 1 [37]. Figure 6.1 depicts instances of the UAO with different values of ν. As illustrated in Figure 6.1 (a) a value of ν= 0 gives a result of multiplying the two memberships divided by the highest among them. This behavior is similar to the D&P function behavior at γ= 0 (see Figure 4.1 in Chapter 4). Figures 6.1 (b) to (f) depict almost a similar shape with a predominant increase in the range of values of the membership function.

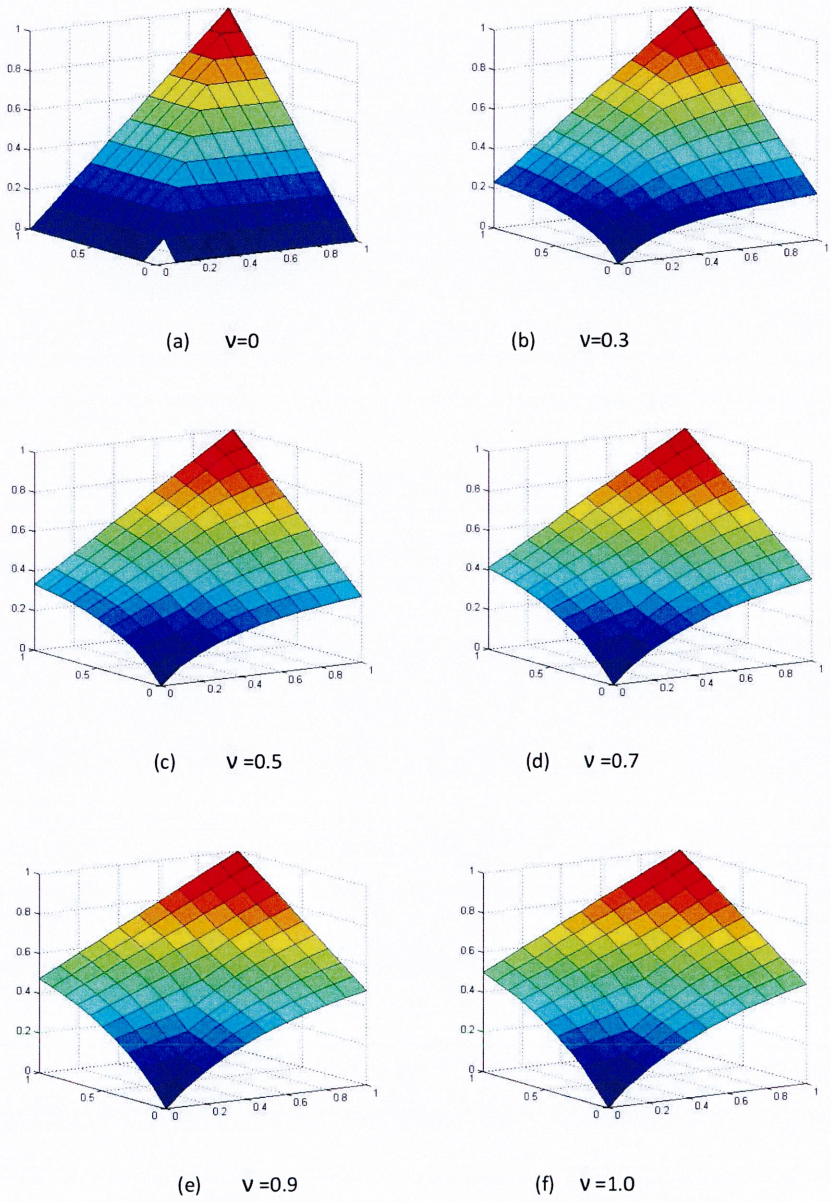


FIGURE 6.1: Effect of ν on UAO function.

6.2 Application of the Unified And-Or operator to the problem

Similar to the approaches adopted in Chapters 4 and 5, the performance of UAO operator will be evaluated through its application to the same MCDM DDoS attack detection problem which is focus of this thesis.

6.3 Results and Discussion

For the purpose of this chapter, several experiments were performed to evaluate and analyze the applicability and the effectiveness of the UAO operator to the problem. The input data for the assessment of the proposed approach is the same as proposed in Section 3.3 described in Tables (3.1) to (3.5). Moreover the four sets of experiments that were performed in Section 4.3 and 5.3 for D&P operator and Werners, respectively are repeated herein. Tables 6.1 to 6.5 provide the results, which were obtained after running several tests on the input data. Different values of the application aspect ratio α, ranging from 0.1 to 1.0, were used as given in column 1 of the tables, and corresponding values of the overall membership for each value of ν ranging from 0.1 to 1.0 are listed in columns 2 to 11, respectively. The membership values of ADR, EDR, and operator related parameter, ν, are used to calculate the overall membership by applying the definition of Werners operator. The results are then listed in Tables 6.1 to 6.5 and the best membership values for each value of ν are denoted in boldface.

TABLE 6.1: Overall membership using UAO operator for different values of ν versus values of α, with GN =128. Best membership values are in boldface.

α	OM (ν=0.1)	OM (ν=0.2)	OM (ν=0.3)	OM (ν=0.4)	OM (ν=0.5)	OM (ν=0.6)	OM (ν=0.7)	OM (ν=0.8)	OM (ν=0.9)	OM (ν=1.0)
0.1	0.1808	0.2490	0.3066	0.3560	0.3987	0.4361	0.4691	0.4984	0.5247	0.5483
0.2	0.1817	0.2498	0.3073	0.3566	0.3993	0.4366	0.4695	0.4988	0.5249	0.5485
0.3	0.1999	0.2665	0.3227	0.3710	0.4127	0.4493	0.4815	0.5101	0.5357	0.5588
0.4	0.1999	0.2665	0.3229	0.3711	0.4129	0.4495	0.4818	0.5104	0.5361	0.5592
0.5	0.2087	0.2741	0.3293	0.3764	0.4173	0.4529	0.4843	0.5122	0.5371	0.5595
0.6	0.2360	0.2991	0.3524	0.3980	0.4374	0.4718	0.5022	0.5291	0.5532	0.5749
0.7	0.2542	0.3158	0.3678	0.4123	0.4508	0.4844	0.5141	0.5404	0.5639	0.5851
0.8	0.2628	0.3232	0.3741	0.4175	0.4550	0.4877	0.5165	0.5421	0.5649	0.5854
0.9	0.3500	0.3989	0.4394	0.4736	**0.5028**	**0.5280**	**0.5501**	**0.5695**	**0.5867**	**0.6021**
1.0	**0.4307**	**0.4540**	**0.4722**	**0.4868**	0.4989	0.5089	0.5175	0.5248	0.5312	0.5368

TABLE 6.2: Overall membership using UAO operator for different values of ν versus values of α, with GN =256. Best membership values are in boldface.

α	OM (ν=0.1)	OM (ν=0.2)	OM (ν=0.3)	OM (ν=0.4)	OM (ν=0.5)	OM (ν=0.6)	OM (ν=0.7)	OM (ν=0.8)	OM (ν=0.9)	OM (ν=1.0)
0.1	0.3725	0.4246	0.4686	0.5063	0.5389	0.5675	0.5927	0.6150	0.6350	0.6530
0.2	0.4181	0.4665	0.5074	0.5425	0.5729	0.5994	0.6229	0.6437	0.6624	0.6792
0.3	0.4636	0.5083	0.5461	0.5785	0.6066	0.6312	0.6528	0.6721	0.6894	0.7049
0.4	0.4725	0.5162	0.5532	0.5848	0.6122	0.6362	0.6574	0.6762	0.6930	0.7081
0.5	0.4905	0.5326	0.5681	0.5986	0.6249	0.6480	0.6683	0.6863	0.7025	0.7170
0.6	0.4909	0.5333	0.5691	0.5999	0.6265	0.6498	0.6704	0.6886	0.7050	0.7197
0.7	0.5450	0.5824	0.6141	0.6412	0.6646	0.6852	0.7032	0.7193	0.7337	0.7466
0.8	0.5989	0.6312	0.6585	0.6818	0.7019	0.7195	0.7351	0.7488	0.7611	0.7722
0.9	0.6697	0.6943	0.7149	0.7325	**0.7476**	**0.7608**	**0.7724**	**0.7827**	**0.7919**	**0.8001**
1.0	**0.7195**	**0.7271**	**0.7333**	**0.7384**	0.7428	0.7465	0.7498	0.7526	0.7551	0.7573

TABLE 6.3: Overall membership using UAO operator for different values of ν versus values of α, with GN =512. Best membership values are in boldface.

α	OM (ν=0.1)	OM (ν=0.2)	OM (ν=0.3)	OM (ν=0.4)	OM (ν=0.5)	OM (ν=0.6)	OM (ν=0.7)	OM (ν=0.8)	OM (ν=0.9)	OM (ν=1.0)
0.1	0.5086	0.5490	0.5831	0.6124	0.6377	0.6598	0.6793	0.6966	0.7121	0.7260
0.2	0.5270	0.5662	0.5993	0.6277	0.6522	0.6737	0.6927	0.7095	0.7246	0.7381
0.3	0.5363	0.5749	0.6075	0.6354	0.6597	0.6809	0.6996	0.7162	0.7311	0.7444
0.4	0.5455	0.5833	0.6154	0.6429	0.6667	0.6875	0.7059	0.7222	0.7368	0.7500
0.5	0.5631	0.5990	0.6294	0.6553	0.6778	0.6975	0.7148	0.7302	0.7439	0.7563
0.6	0.5812	0.6155	0.6445	0.6693	0.6908	0.7096	0.7261	0.7408	0.7540	0.7658
0.7	0.5898	0.6229	0.6508	0.6747	0.6954	0.7134	0.7293	0.7434	0.7560	0.7673
0.8	0.6256	0.6550	0.6799	0.7011	0.7194	0.7354	0.7495	0.7620	0.7732	0.7832
0.9	0.6866	**0.7086**	**0.7270**	**0.7426**	**0.7560**	**0.7677**	**0.7780**	**0.7871**	**0.7952**	**0.8025**
1.0	**0.6693**	0.6787	0.6864	0.6927	0.6981	0.7026	0.7066	0.7100	0.7130	0.7673

TABLE 6.4: Overall membership using UAO operator for different values of ν versus values of α, with GN =1024. Best membership values are in boldface.

α	OM (ν=0.1)	OM (ν=0.2)	OM (ν=0.3)	OM (ν=0.4)	OM (ν=0.5)	OM (ν=0.6)	OM (ν=0.7)	OM (ν=0.8)	OM (ν=0.9)	OM (ν=1.0)
0.1	0.6348	0.6637	0.6881	0.7089	0.7269	0.7426	0.7564	0.7687	0.7797	0.7895
0.2	0.6988	0.7226	0.7428	0.7600	0.7750	0.7880	0.7995	0.8096	0.8187	0.8269
0.3	0.7263	0.7481	0.7666	0.7824	0.7961	0.8080	0.8185	0.8279	0.8362	0.8437
0.4	0.7265	0.7485	0.7671	0.7830	0.7968	0.8088	0.8195	0.8289	0.8373	0.8449
0.5	0.7349	0.7556	0.7730	0.7879	0.8008	0.8121	0.8220	0.8308	0.8386	0.8457
0.6	0.7621	0.7805	0.7960	0.8093	0.8207	0.8307	0.8396	0.8474	0.8544	0.8607
0.7	0.7884	0.8036	0.8164	0.8273	0.8367	0.8449	0.8522	0.8586	0.8643	**0.8695**
0.8	0.8047	0.8168	0.8269	0.8356	0.8430	0.8495	0.8552	**0.8602**	**0.8647**	0.8687
0.9	**0.8531**	**0.8537**	**0.8543**	**0.8547**	**0.8551**	**0.8554**	**0.8557**	0.8560	0.8562	0.8564
1.0	0.3886	0.4355	0.4748	0.5080	0.5365	0.5612	0.5829	0.6020	0.6190	0.6343

TABLE 6.5: Overall membership using UAO operator for different values of ν versus values of α, with GN =2048. Best membership values are in boldface.

α	OM (ν=0.1)	OM (ν=0.2)	OM (ν=0.3)	OM (ν=0.4)	OM (ν=0.5)	OM (ν=0.6)	OM (ν=0.7)	OM (ν=0.8)	OM (ν=0.9)	OM (ν=1.0)
0.1	0.8604	0.8690	0.8762	0.8824	0.8877	0.8923	0.8964	0.9000	0.9032	0.9061
0.2	0.8703	0.8789	0.8861	0.8922	0.8976	0.9022	0.9063	0.9099	0.9131	0.9160
0.3	0.8887	0.8959	0.9019	0.9071	0.9116	0.9155	0.9189	0.9220	0.9247	0.9272
0.4	0.8891	0.8967	0.9031	0.9086	0.9133	0.9175	0.9211	0.9243	0.9272	0.9298
0.5	0.8956	0.9001	0.9040	0.9073	0.9101	0.9126	0.9147	0.9166	0.9183	0.9199
0.6	0.8972	0.9032	0.9082	0.9125	0.9162	0.9195	0.9223	0.9249	0.9271	0.9291
0.7	**0.9139**	**0.9172**	**0.9199**	**0.9222**	**0.9242**	**0.9259**	**0.9275**	**0.9288**	**0.9300**	**0.9311**
0.8	0.9080	0.9090	0.9099	0.9107	0.9114	0.9119	0.9124	0.9129	0.9133	0.9136
0.9	0.7370	0.7549	0.7698	0.7825	0.7934	0.8029	0.8113	0.8187	0.8253	0.8312
1.0	0.1078	0.1812	0.2431	0.2958	0.3413	0.3809	0.4158	0.4467	0.4743	0.4991

6.3.1 Effect of number of GN nodes on the best value of α for different values of ν

In this section, the progression of α versus the GN nodes for varying values of ν was investigated. Tables (6.1) to (6.5) illustrate the results obtained after application of the UAO operator to the problem considered in this thesis. A general trend in Figure 6.2 (a) - (j) is that the best value of α is reducing with the increasing number of GN nodes. This was observed for all values of ν varying from 0.1 (Figure 6.2 (a)) to 1.0 (Figure 6.2 (j)). For instance, for 128, 256, and 512 nodes in Figure 6.2 (a), the best value of α was 1.0. However, when the number of GN nodes was increased to 1024 and 2048 nodes, the best value of α decreased to 0.9 and 0.7, respectively. This specific trend associated with 1024 and 2048 nodes is a dominant trend in these figures.

One possible argument for this behavior is that the increase in the number of GN nodes in the WSN increases the ADR in that network for achieving higher accuracies, as was observed in Tables (3.1) to (3.5) in Chapter 3. The direct effect of the number of GN nodes on the ADR justifies the indirect effect of the number of GN nodes on the best value of α. This results in a decrement in the value of α for higher values of the GN nodes. The reason for improved attack detection rates for individual GN nodes is attributed to the increase in the values of GN nodes, as the proximity of the GN nodes leads to reduced communication distances that need to be traversed by the GN communication messages. As a result, the time needed to deliver the communication messages to the mGN nodes will be less and hence reporting the attack in the network will be faster.

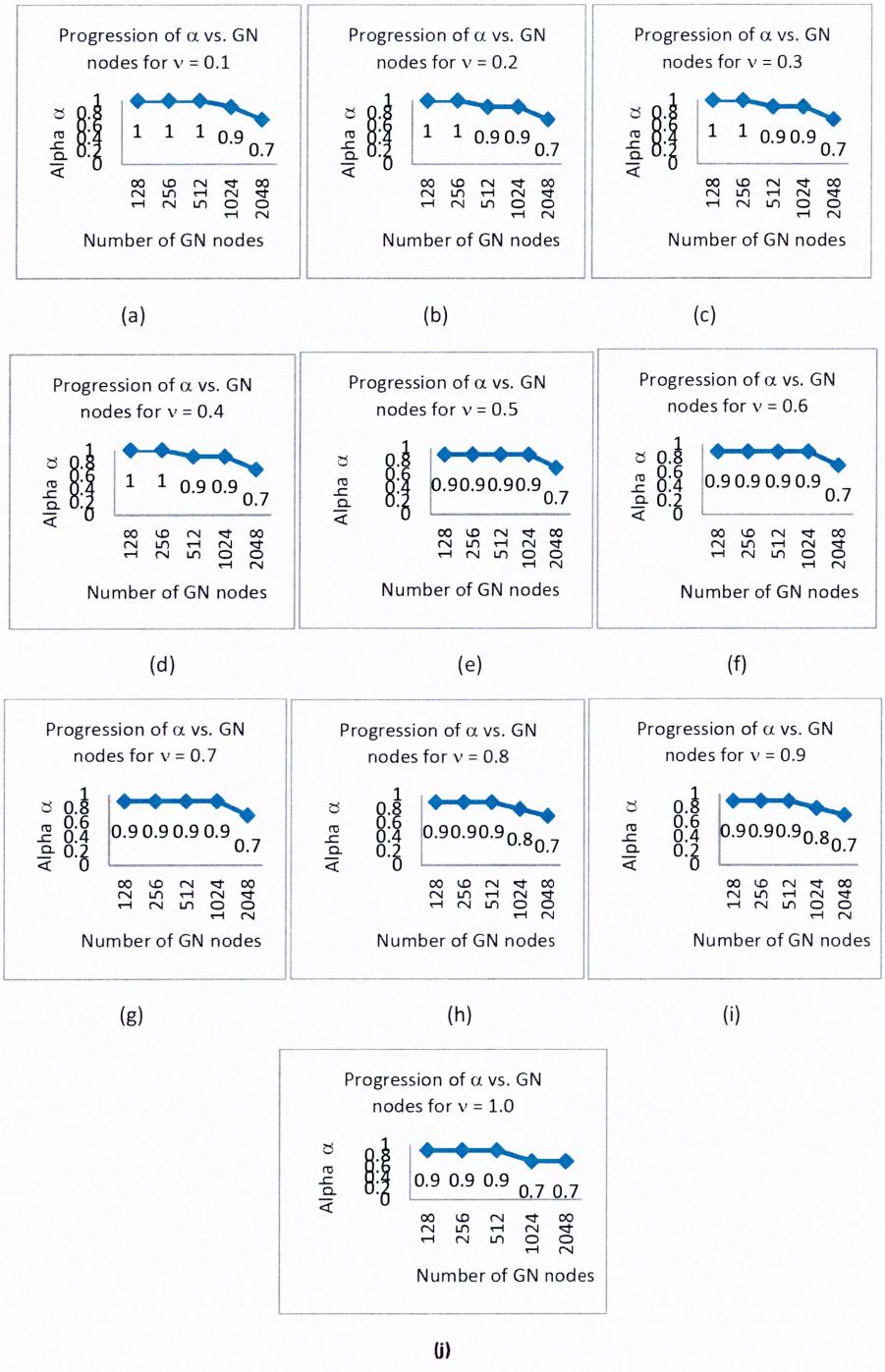


FIGURE 6.2: Progression of α vs GN nodes for (a) $\nu = 0.1$ (b) $\nu = 0.2$ (c) $\nu = 0.3$ (d) $\nu = 0.4$ (e) $\nu = 0.5$ (f) $\nu = 0.6$ (g) $\nu = 0.7$ (h) $\nu = 0.8$ (i) $\nu = 0.9$ (j) $\nu = 1.0$

6.3.2 Effect of value of ν on the best trade-off between ADR and EDR

In this section, the effect of value of ν on the best value of the application aspect value, α, is analyzed. Recall that the system parameter α represents the best trade-off between ADR and EDR. Figures 6.3 (a) - (e) show the effect on the value of α with the variation in the value of ν. When the behavior of α was compared to that of ν while keeping the number of nodes fixed, it was found that the value of α gradually decreased when ν was increased from 0.0 to 1.0. For instance, in Figures 6.3 (a) and (b), where the number of GN nodes is 128 and 256 respectively, the behavior of α was identical. The value of α was 1.0 for values of ν from 0.1 to 0.4. When ν was increased from 0.5 to 1.0, α slightly decreased and remained at a value of 0.9. Moreover, for GN= 512,1024, and 2048 nodes, a different behavior of α was observed, as illustrated in Figures 6.3 (c), (d), and (e). The figures show that the value of α remained almost steady or had a slight variation when ν was varied from 0.1 to 1.0. This trend indicates that the value of α was somewhat not influenced by the change in ν.

The above behavior is justified by referring to Eq. (6.1). The small deviation is very possibly due to the structure of the UAO function. The definition of the UAO function is taking the maximum value between the memberships of the two criteria. Consequently, and as observed in Tables (3.1) to (3.5) in Section 3.3, in most cases the maximum value between the memberships of the criteria (columns 5 and 6) is MemEDR. Furthermore, it is also apparent from the tables that the value of the mGN nodes was significantly increasing for higher values of α, specially from 0.7 to 1.0. As a result of this increase in the numbers of mGN nodes, energy decay rates increased, since a higher number of nodes in this situation take part in the computation and communication associated with the detection process. High energy decay rates imply higher values for the membership value MemEDR, (see Section 5.2). As a result, the membership value MemEDR was always greater than MemADR and would generally affect the obtained result. This in turn resulted in high values of the best trade-off.

Another observation from the plots in Figure 6.3 is that for lower values of GN nodes (e.g. 128 and 256), the best value of α was in the higher range (0.9 to 1.0), but for medium and higher values of GN nodes (256, 1024, and 2048), the best value of α was relatively in a lower range (0.7 to 0.9). This again can be attributed to the higher number of mGN nodes for the higher value of α.

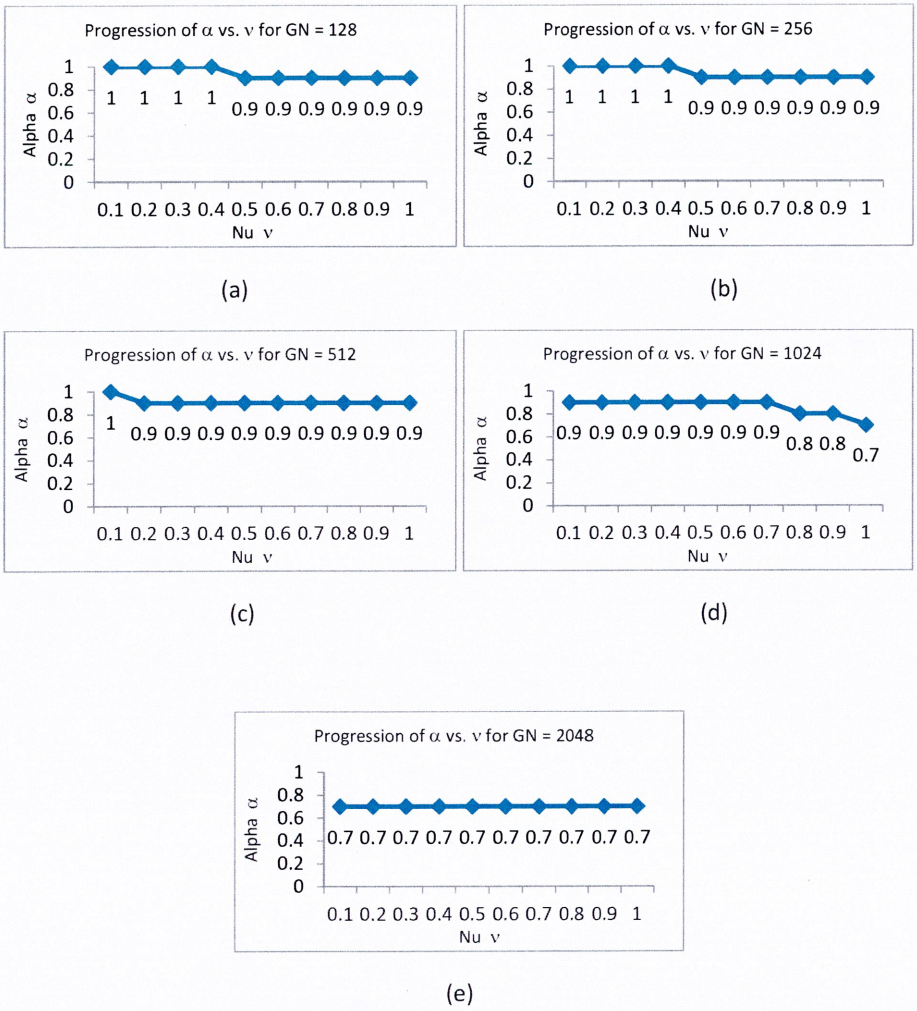


FIGURE 6.3: Effect of value of ν on α for (a) GN = 128 (b) GN = 256 (c) GN = 512 (d) GN = 1024 (e) GN = 2048

6.3.3 Effect of ν on memberships of ADR, EDR, and overall membership for different number of GN nodes

For different number of GN nodes, the effect of ν on memberships of ADR, EDR, and overall membership was investigated in this section. Firstly, it was observed from Figure 6.4 (a) and (b) that for low values of ν (0.1 to 0.4), the memberships of ADR, EDR, and overall membership remains steady. The value of ν is not showing any significant impact on the values of the three memberships in Figure 6.4 (e).

The three memberships are mostly levelled off for small values of ν ranging from 0.1 to 0.4 and 0.7 for 128, 256 and 1024 nodes, as shown in Figure 6.4 (a), (b), and (d), respectively. Another trend observed from Figure 6.4 was that, when the values of ν started increasing towards the upper limit of the previously specified range (ν= 0.4 and 0.7 for 128,256 and 1024 nodes respectively), membership of EDR showed a significant increase in its value, while the membership of ADR showed an inverse behavior showing a gradual decrease. The two memberships (MemADR and MemEDR) are showing an opposite behavior of each other. This behavior is defining the nature of the two decision criteria; the attack detection rate and the energy decay rate are *conflicting* in nature and improving one factor negatively affects the other. It is therefore, observed from Figure 6.4 that the behavior of the overall membership was a fair balance between the two decision criteria, and not following the pattern of any criteria. This balance indicates a reasonably high detection rate without imposing high energy demands on the limited sensory resources. This property makes the UAO operator a suitable choice for similar MCDM problems where a reasonable balance is desired between the underlaying criteria.

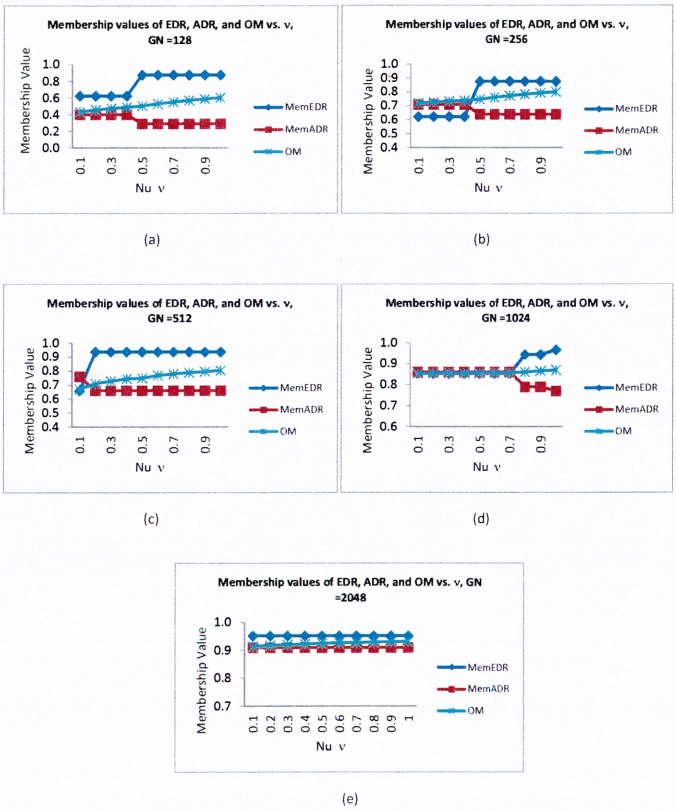


FIGURE 6.4: Effect of ν on MemADR, MemEDR, and OM for (a) GN = 128 (b) GN = 256 (c) GN = 512 (d) GN = 1024 (e) GN = 2048

6.3.4 Effect of value of ν on the Ratio of mGN and GN nodes

TABLE 6.6: Values of ν and the ratio of mGN and GN nodes for N= 128 to 2048 GN nodes

ν	mGN/GN for GN =128	mGN/GN for GN =256	mGN/GN for GN =512	mGN/GN for GN =1024	mGN/GN for GN =2048
0.1	0.3594	0.2695	0.1777	0.0205	0.0029
0.2	0.3594	0.2695	0.0371	0.0205	0.0029
0.3	0.3594	0.2695	0.0371	0.0205	0.0029
0.4	0.3594	0.2695	0.0371	0.0205	0.0029
0.5	0.1328	0.0703	0.0371	0.0205	0.0029
0.6	0.1328	0.0703	0.0371	0.0205	0.0029
0.7	0.1328	0.0703	0.0371	0.0205	0.0029
0.8	0.1328	0.0703	0.0371	0.0088	0.0029
0.9	0.1328	0.0703	0.0371	0.0088	0.0029
1.0	0.1328	0.0703	0.0371	0.0059	0.0029

In this section, the effect of values of the UAO operator related parameter, ν, on the ratio of mGN and GN nodes was investigated. The results for best values of aspect ratio, α for which the best trade-off was found, are shown in Table 6.6. As discussed in Chapter 2, the ideal ratio of mGN and GN is required to facilitate the attack detection process with the minimal energy overhead on the nodes and at the same time, without significantly compromising the accuracy in the attack detection. For this purpose, large number of mGN nodes are designated in the scheme in order to attain a fairly reasonable accuracy in the attack detection. In addition, for the MCDM problem proposed in this thesis, large values of α signify the need for achieving higher accuracies in attack detection, therefore the selection of large values of α leads to the designation of a large number of mGN nodes for the detection scheme. As observed in the mGN and GN ratios obtained for UAO operator results, smaller values of α lead to fewer numbers of mGN nodes in the network. Therefore, it is apparent from Table (6.6) that, for the same number of GN nodes, the ratio of mGN and GN nodes is decreasing (consider for example GN =128 and move vertically downwards). One reason for this is the decreasing values of α which correspond to decreasing the number of mGN nodes in the network. This in turn will decrease the value of the numerator in the calculated ratio and result in decreasing the ratio as a result.

6.4 Conclusions

This chapter presented and investigated the application of UAO operator to find the best trade-off between ADR and EDR for the MCDM problem considered in this thesis. Experimental results revealed that the best value of aspect ratio, α, lies between 0.7 and 1.0, for all networks tested (GN=128 to 2048). It was also observed that the value of α was somewhat insensitive to change in the value of UAO operator related parameter, ν. Another important finding was that the overall membership was not following any pattern as that of the membership of ADR nor EDR; instead, the overall decision was significantly acting as an ideal balance between these two criteria to compute the most optimal ratio of the two. It was also found that the ratio of mGN and GN nodes is decreasing when considering the same number of GN nodes and varying the value of ν . The reason for this is the decreasing values of α which lead to decreasing the number of mGN nodes in the network which will result in a decrease in the mGN/GN ratio.

The next chapter investigates another MCDM approach, namely, GP for the same problem studied in this chapter.

Chapter 7

Application of Goal Programming Approach for DDoS Attack Detection in WSNs

The MCDM problem considered in this thesis was analyzed using fuzzy logic approach in previous sections, but reflected some deficiencies in the proposed approach. The GP based approach proposed in this chapter is formulated as a MCDM problem, with ADR and EDR as the two decision criteria. A GP based mechanism is developed to achieve the best trade-off between the two aforementioned conflicting criteria. Empirical analysis is performed to evaluate and at the same time to prove the effectiveness of the proposed approach. This is followed by a detailed discussion of the analyzed results.

7.1 Application of Goal Programming to The Problem

In Chapter 2, GP was described, requiring the objectives to be normalized with respect to the ideal values to deal with the incommensurability issue. Furthermore, the obtained values were compared to the ideal values through underlaying deviations. Recall from Chapter 3, the flowchart describes the process of GP.

For the work considered in this thesis, the two criteria of ADR and EDR have different units. Hence, it is necessary to normalize both criteria to the same scale. For this purpose, the second normalization approach discussed in Section

3.2 has been adopted, i.e., the criteria have been normalized to map onto a zero-one range. Then the deviations of the two objectives were calculated with respect to their ideal values, and both deviations were added together using Eq. (2.11) described in Section 2.4.2. The value that resulted in the lowest overall deviation was selected as the best trade-off. Since the ADR is already a value between 0 and 1, there is no need for it to be normalized. For the EDR, the values have been normalized between 230.0 μJ/sec and 12102.3 μJ/sec, since all energy decay rates fall within these extremes (refer to Tables 7.1 to 7.5).

7.2 Results and Discussion

For the purpose of this chapter, several experiments were performed to evaluate and analyze the applicability and effectiveness of applying GP approach to the problem. The input data for the assessment of the proposed approach is the same as mentioned in Chapter 3. Tables 7.1 to 7.5 provide the results, which were obtained after running several tests on the input data. The five test cases as listed in Chapter 3 were used for experimentation. Values of application aspect α in the range of 0.1 to 1.0 were used as given in column 1 of the tables, with corresponding values of mGN, EDR, and ADR as listed in columns 2, 3, and 4, respectively. Since the decision variables were EDR and ADR, the deviations of these two variables from their respective target values (as discussed in Section 7.1), are listed in columns 5 and 6 of these tables. Finally, the overall deviation which sums the individual deviations of EDR and ADR is listed in the last column of the tables.

TABLE 7.1: Deviations for EDR, ADR, and Overall for GN=128. Lowest overall deviation is in boldface.

α	mGN	EDR	ADR	Deviation of EDR	Deviation of ADR	Overall Deviation
0.1	2	284.8	0.099	0.0045	0.901	0.906
0.2	2	296.6	0.100	0.0055	0.900	0.906
0.3	2	283.6	0.120	0.0044	0.880	0.884
0.4	2	265.8	0.120	0.0030	0.880	0.883
0.5	4	464.4	0.130	0.0194	0.870	0.889
0.6	4	422.8	0.160	0.0159	0.840	0.856
0.7	4	430.0	0.180	0.0165	0.820	0.837
0.8	6	615.6	0.190	0.0319	0.810	0.842
0.9	17	1739.1	0.290	0.1247	0.710	**0.835**
1.0	46	4807.0	0.400	0.3782	0.600	0.978

TABLE 7.2: Deviations for EDR, ADR, and Overall for GN=256. Lowest overall deviation is in boldface.

α	mGN	EDR	ADR	Deviation of EDR	Deviation of ADR	Overall Deviation
0.1	2	302.2	0.310	0.0060	0.690	0.696
0.2	2	259.8	0.360	0.0025	0.640	0.642
0.3	2	234.2	0.410	0.0003	0.590	0.590
0.4	3	295.2	0.420	0.0054	0.580	0.585
0.5	4	331.2	0.440	0.0084	0.560	0.568
0.6	4	240.0	0.440	0.0008	0.560	0.561
0.7	6	339.6	0.500	0.0091	0.500	0.509
0.8	9	469.8	0.560	0.0198	0.440	0.460
0.9	18	802.8	0.640	0.0473	0.360	**0.407**
1.0	69	2711.7	0.710	0.2051	0.290	0.495

TABLE 7.3: Deviations for EDR, ADR, and Overall for GN=512. Lowest overall deviation is in boldface.

α	mGN	EDR	ADR	Deviation of EDR	Deviation of ADR	Overall Deviation
0.1	2	362.0	0.460	0.0109	0.540	0.551
0.2	2	291.6	0.480	0.0051	0.520	0.525
0.3	2	248.2	0.490	0.0015	0.510	0.512
0.4	2	230.0	0.500	0.0000	0.500	0.500
0.5	4	346.8	0.520	0.0097	0.480	0.490
0.6	5	361.5	0.540	0.0109	0.460	0.471
0.7	7	466.9	0.550	0.0196	0.450	0.470
0.8	10	584.0	0.590	0.0293	0.410	0.439
0.9	19	1007.0	0.660	0.0642	0.340	**0.404**
1.0	91	4377.1	0.760	0.3427	0.240	0.583

Analysis of Results

The aim is to find the trade-off between EDR and ADR that results in the minimum overall deviation. It can be observed in Tables (7.1) to (7.5) that an increase in the number of mGN nodes results in higher EDRs, since a higher number of nodes participate in the computation and communication associated with the detection process in this situation. However, increasing the number of GN nodes participating in the detection process also results in better ADRs.

As can be observed from Tables (7.1) to (7.5), for small and medium size networks (GN = 128, 256, and 512), a high value of $\alpha = 0.9$ is recommended. The implication is that higher EDRs are acceptable in order to achieve a reasonable degree

TABLE 7.4: Deviations for EDR, ADR, and Overall for GN=1024. Lowest overall deviation is in boldface.

α	mGN	EDR	ADR	Deviation of EDR	Deviation of ADR	Overall Deviation
0.1	2	543.2	0.600	0.0259	0.400	0.426
0.2	2	461.8	0.670	0.0192	0.330	0.349
0.3	2	407.4	0.700	0.0147	0.300	0.315
0.4	2	374.2	0.700	0.0119	0.300	0.312
0.5	3	490.5	0.710	0.0215	0.290	0.312
0.6	4	486.8	0.740	0.0212	0.260	0.281
0.7	6	646.8	0.770	0.0344	0.230	**0.264**
0.8	9	919.8	0.790	0.0570	0.210	0.267
0.9	21	2018.1	0.860	0.1477	0.140	0.288
1.0	102	8323.2	0.910	0.6687	0.090	0.759

TABLE 7.5: Deviations for EDR, ADR, and Overall for GN=2048. Lowest overall deviation is in boldface.

α	mGN	EDR	ADR	Deviation of EDR	Deviation of ADR	Overall Deviation
0.1	2	714.0	0.850	0.0400	0.150	0.190
0.2	2	587.8	0.860	0.0296	0.140	0.170
0.3	2	556.0	0.880	0.0269	0.120	0.147
0.4	2	489.0	0.880	0.0214	0.120	0.141
0.5	4	856.8	0.890	0.0518	0.110	0.162
0.6	4	629.6	0.890	0.0330	0.110	0.143
0.7	6	820.8	0.910	0.0488	0.090	**0.139**
0.8	11	1359.6	0.920	0.0933	0.080	0.173
0.9	32	3673.6	0.940	0.2845	0.060	0.345
1.0	113	12102.3	0.960	0.9810	0.040	1.000

of accuracy in the attack detection process. For instance, in Table (7.3) with GN = 512, α= 0.9 yields a 66% detection rate for an energy decay rate value of 1007 μJ/sec. For a larger network with GN = 1024, α=0.7 yields the lowest overall deviation. Here, a reasonable degree of accuracy is achieved in the attack detection process, at the added advantage of energy conservation. More specifically, for GN=1024, nearly 68% improvement in the energy decay rate is achieved by simply selecting the value of α to be 0.7 (with EDR = 646.8 μJ/sec) rather than 0.9 (having EDR = 2018.1 μJ/sec), with the corresponding difference in the attack detection rate being only 9% (from 86% for α=0.9 to 77% for α=0.7). For very large networks with GN = 2048, a 91% accuracy in attack detection is obtained for α=0.7. The energy decay in this case is reduced from 12102.3 μJ/sec to 820.8

μJ/sec, facilitating a considerable energy conservation, for a negligible difference in the attack detection rate (91% for α=0.7, as opposed to 96% for α=1.0). The results are represented in Figure 7.1.

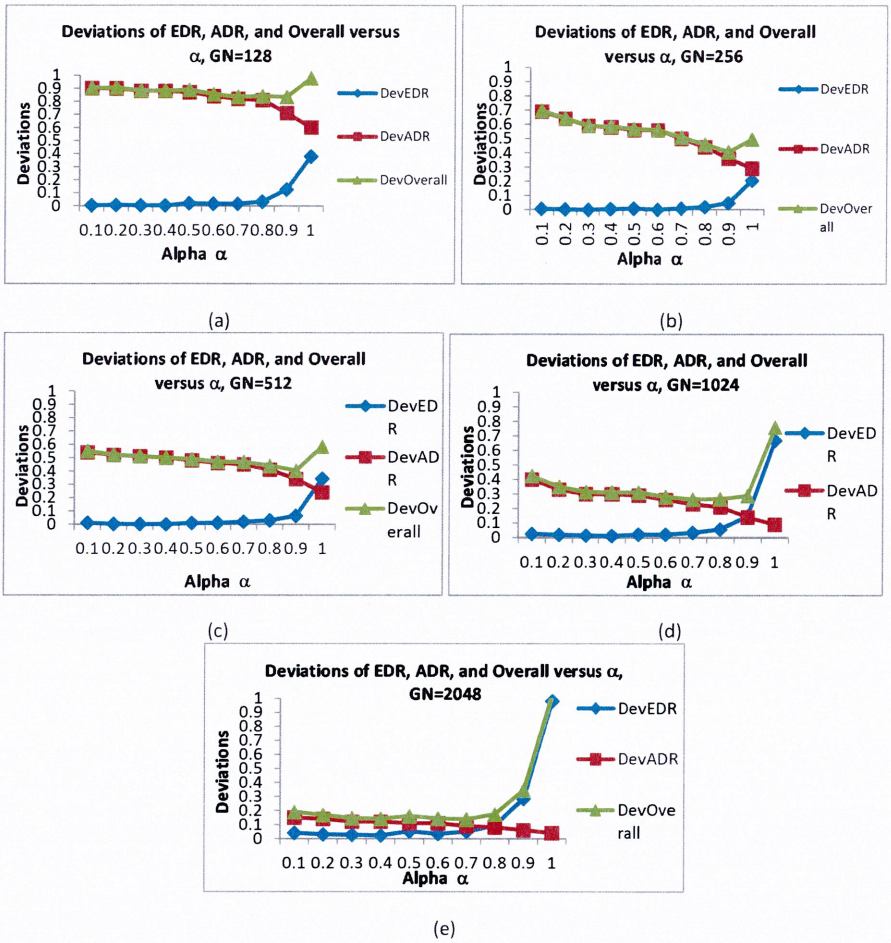


FIGURE 7.1: Plots depicting the effect of variation of α on the Deviation of Attack Detection Rate, Deviation of Energy Decay Rate, and the Overall Deviation for (a) GN = 128 (b) GN = 256 (c) GN = 512 (d) GN = 1024 (e) GN = 2048.

Figure 7.1 illustrates the behavior of deviations of ADR and EDR, as well as the overall deviation, with respect to progressing values of α. A general trend in this figure is that as the value of α is increased, the deviation for ADR decreases. On the other hand, an increase in the deviation of EDR is witnessed when α increases, in general. More specifically, for α = 0.1 to 0.4, deviation of EDR decreased (this is more obvious in Tables (7.1) to (7.5) and is very small in magnitude, but for high values of α from 0.8 to 1.0, the deviation increased drastically.

Another notable observation in Figure 7.1 is that the best overall deviation (always the minimum value) is found to be the intersection point between the graphs of the two deviations of ADR and EDR.

7.3 Conclusions

This chapter has presented an approach to strengthen the decision-making process in the distributed denial of service attack detection scheme originally proposed by Baig *et al.* [3][6], and to eliminate the deficiencies revealed by the use of fuzzy logic based decision-making approach proposed in [7][38] for the same problem. The facilitation was achieved by utilizing GP method for decision-making between the two conflicting criteria of interest, namely, ADR and EDR. This was accomplished by varying the value of the network parameter known as application aspect ratio, α. Experimental results showed that the best value of α lies between 0.7 and 0.9, for all networks tested (GN=128 to 2048). It was also observed that the overall deviation found to be the intersection point between the graphs of the two deviations of ADR and EDR.

Chapter 8

Comparisons of Approaches

Chapters 4 to 7 presented a number of approaches that were utilized to investigate the application and effectiveness of fuzzy logic and GP for MCDM problems. The application domain was the DDoS Attacks in WSNs while considering the ADR and the EDR as the decision criteria. In all former chapters, the applicability and effectiveness of the proposed approaches were evaluated through empirical analysis. This chapter presents an overall comparison of the results obtained for each of the proposed approaches. The results for these comparisons have been presented and discussed in earlier chapters, but are consolidated and integrated here for the sake of clear comparisons.

The first section presents a comprehensive comparison of the results obtained for each of the three fuzzy operators. This is followed by a discussion of the overall performance of the proposed fuzzy operators. The applicability of each fuzzy operator is presented. This is followed by an elaborated discussion of the best choice among the three fuzzy operators to solve the problem. Also a comparison between the fuzzy logic approach and GP is presented. The main focus of this comparison is to determine which of the proposed approaches perform the best in the application domain.

8.1 Comparison of Fuzzy Logic Operators

This section compares the performance of the three fuzzy logic operators previously presented and discussed in this thesis. The fuzzy operators were used to combine the two conflicting decision criteria used in Eqs. (4.1), (5.1) and (6.1), respectively. This discussion herein provides an overall comparison of the D&P, Werners, and

UAO operators. This comparison is based on the results presented in Chapters 4 to 6. The comparison is divided into two categories. The first is focussed on the effect of the operator related parameter on the overall membership. The second comparison focused on the effect of membership values of the ADR, MemADR, and the EDR, MemEDR, on the overall membership. Several regression models were developed to see how the best trade-off is affected by the change of the values of MemADR, MemEDR, and operator related parameter when D&P, Werners, and UAO operators are applied. The effect is measured through regression coefficients. A confidence level of 95% was used. The analysis was based on 50 data values, since there were five test cases with five different number of nodes, where for each test case, 10 runs were made with different operator related parameter values.

8.1.1 Effect of value of operator related parameter on the overall membership

This comparison studied the effect of the value of the operator related parameter which is γ in D&P, β in Werners, and ν in UAO, on the overall membership, or in other words, the best trade-off found between attack detection and energy decay rates. To perform these comparisons, multiple regression analysis models were developed with each one of the operator related parameters (with values ranging from 0.1 to 1.0) as the independent variable and overall membership in each case (test cases with GN nodes = 128, 256, 512, 1024 and 2048) as the dependent variable. The effect of the operator related parameter for each of the three fuzzy operators was measured through regression coefficients.

TABLE 8.1: Comparison of D&P, Werners, and UAO for the Overall Membership

Test Case (GN nodes)	Regression coefficients		
	D&P	Werners	UAO
128	-0.87	-0.97	0.999
256	-0.71	-0.94	0.994
512	-0.52	-1.00	0.968
1024	-0.65	-0.88	0.865
2048	-0.52	-1.00	0.985

Table 8.1 presents the five test cases from 128 to 2048 nodes. For each test case given in column 1 of the table, the corresponding regression coefficients for the

D&P, Werners, and UAO regression models are given in columns 2, 3 and 4, respectively. For the cases of D&P and Werners, the negative sign for the regression coefficients signifies an inverse relationship between the operator related parameters (γ in D&P and β in Werners) and the overall membership. In other words, the overall membership decreases as the operator related parameter is increased. This is attributed to the behaviors of both functions presented in Eqs. (4.1) and (5.1) which were discussed earlier in Sections 4.3.2 and 5.3.2 respectively. On the other hand, the positive relationship between the overall membership and ν in UAO is obvious from the positive values for the regression coefficients obtained.

Based on the comparison presented in Table 8.1, D&P fuzzy operator performed the best among the three compared operators. This is obvious from the low magnitudes of the regression coefficients obtained for the D&P operator. Note that the regression coefficients represent the level of correlation of the operator related parameter with the overall membership. With regard to the three fuzzy operators studied in this thesis, best results were achieved when the magnitude of the operator related parameter on the value of the overall membership was less. For example, for the test case 256 in Table 8.1, the regression coefficients for the overall membership for D&P, Werners, and UAO are given as -0.71, -0.94, and 0.994 respectively. The minimum magnitude among the three regression coefficients (irrespective of the sign) is -0.71, which means that the operator related parameter γ had the least effect on the D&P fuzzy operator, which in turn forms a better choice for the problem considered in this thesis.

When comparing the regression coefficients obtained for the other two operators, it was found that the results for Werners and UAO were very close to each other and no significant difference was found in most of the test cases. For smaller numbers of GN nodes (test cases 128 and 256), Werners operator performed better, whereas for higher numbers of GN nodes (test cases 512 to 2048), UAO operator performed better.

The level of improvement of the regression coefficients obtained for D&P when increasing the GN nodes for all test cases was much better than that of Werners and UAO. Thus, the comparison of the results in Table 8.1 suggest that D&P is undoubtedly performing better than Werners and UAO when considering the operator related parameter for the overall membership.

8.1.2 Effect of memberships of ADR and EDR on the overall membership

This comparison studied the effect of membership values of the attack detection rate (MemADR) and the energy decay rate (MemEDR) on the overall membership. Multiple regression models were developed for the sake of this comparison. Each membership value (MemADR and MemEDR) were considered as the independent variables, and overall membership for each test case as the dependent variable. The effect of the memberships of ADR and EDR for each of the three fuzzy operators was measured through regression coefficients.

TABLE 8.2: Comparison of the effect of memberships of EDR and ADR on the overall membership (the objective) for D&P, Werners and UAO.

Test Case	Regression Coefficients					
	D&P		Werners		UAO	
	MemEDR	MemADR	MemEDR	MemADR	MemEDR	MemADR
128	-0.04	1.04	0.746	0.262	0.788	0.219
256	-0.07	1.07	0.554	0.448	0.590	0.412
512	-	-	-	-	0.601	0.401
1024	-0.22	1.22	0.483	0.517	0.513	0.488
2048	-	-	-	-	-	-

Table 8.2 presents the five test cases, from 128 to 2048 nodes. All tests were done for the overall membership. Columns 2 and 3 of the table provides the regression coefficients for MemEDR and MemADR for the D&P operator. Similarly, column 4 and 5 enlists the regression coefficients for MemEDR and MemADR for the Werners operator. Finally, column 6 and 7 gives the regression coefficients for MemEDR and MemADR for the UAO operator. For cases represented in Table 8.2 as "-", no regression coefficients could be obtained, which indicates constant values of the memberships for both energy decay and attack detection rates. That is, the memberships of EDR and ADR do not change for all ten scenarios for the variables studied, but the overall membership is changing. This is attributed to the fact that the best overall membership for those cases is always found at the same application aspect value α which was discussed earlier in Chapter 3.

For the underlaying MCDM problem, the two conflicting criteria (EDR and ADR) should be considered as having an equal level of importance. Therefore, the more a balance is found between the effect of both criteria on the overall membership, the more the solution is better.

As shown in Table 8.2, the regression models for Werners and UAO were quite similar to each other in some cases (i.e., 128, 256, and 1024 nodes), and the regression coefficients were balanced for most cases. This means that both MemADR and MemEDR had an equal effect on the overall membership. As far as the effect of MemEDR and MemADR for both Werners and UAO operators is concerned, the investigation found that Werners performed comparatively better than UAO in balancing the effect of the two decision criteria, EDR and ADR. In contrast to Werners and UAO, the D&P regression model was the worst because in all cases, the results were highly affected by MemADR. For instance, in the test case with 1024 nodes, the regression coefficient of MemEDR was -0.22, and for MemADR was 1.22, which means that ADR was given more importance than EDR.

Depending on the nature of the application that deploys WSNs, preference may be given to criteria over the others. That is, for some special cases the decision-maker assigns preference to one objective over the others based on the design requirement of the problem (refer to Section 3.2). Decision-maker's preferences force the solution of the MCDM problem to bias towards one objective and are incorporated into the MCDM search process to focus on regions of greater interest. For instance, certain applications of WSNs require the scheme to converge less frequently so as to reduce the overhead, and increase the lifetimes of the network, at the cost of lower attack detection rates such as the medical applications discussed in Chapter 1. In this case, UAO would be the best choice among the three fuzzy operators studied because the regression coefficients for MemEDR are always higher than the ones for MemADR (see Table 8.2).

In a sense, UAO gives implicit preference to EDR over ADR, without forcing the operator to follow explicitly defined preference. On the other hand, other applications require the scheme to converge more frequently to increase the attack detection rates at the cost of more resource usage (as in the military applications discussed in Chapter 1). In such scenarios, the D&P operator would be the best choice because it implicitly gives much importance to the membership of ADR and let it affect the overall membership more.

It should be noted that the aim of this study was to not force the fuzzy operators toward specific preferences. Instead, it was to study the natural behavior of each operator.

8.2 Comparison between Fuzzy Logic and Goal Programming

As seen in previous chapters, fuzzy logic and GP approaches were employed in order to find the best balance between ADR and EDR for the MCDM problem considered in this thesis. It was observed that the use of these three fuzzy operators (i.e., D&P, Werners, and UAO) required the use of operator related parameter associated with these operators. The results are therefore also heavily dependent on the value of these operator related parameters. In contrast, GP turned out to be an attractive alternative to fuzzy logic, since the former does not have any parameters on which the method is dependent as in the case with the previous three fuzzy functions.

Furthermore, GP has also been applied to a huge number of MCDM problems in different domains. GP approach was employed for the problem considered in this thesis to simplify the decision-making process. Regression analysis was performed on the results for GP and was compared with the results of fuzzy logic operators presented in Section 8.1. The analysis studied the effect of deviations of the EDR (deviation of EDR in Table 8.3) and the ADR (deviation of ADR Table 8.3) on the overall deviation. Multiple regression models were developed for the sake of this comparison. Each of the two deviations (deviation of EDR and deviation of ADR) were considered as independent variables, and overall deviation for each test case as the dependent variable. The effect of the deviations of ADR and EDR for GP was measured through regression coefficients.

TABLE 8.3: Comparison of the effect of regression coefficients of deviations of EDR and ADR on the overall deviation for GP.

Test Case	Deviation of EDR	Deviation of ADR
128	2.700	2.220
256	0.733	1.450
512	2.000	1.780
1024	1.360	0.614
2048	1.090	0.123

Table 8.3 presents the five test cases, from 128 to 2048 nodes and provided in column 1. All tests were done for the overall function. Columns 2 and 3 of the table provide the regression coefficients for deviations of EDR and ADR.

As discussed earlier in this chapter, the two conflicting criteria (EDR and ADR) should be considered as having an equal level of importance. Therefore, the more a balance is found between the effect of the criteria on the overall deviation, the more the solution is better. As shown in Table 8.3, the regression coefficients represent the effect of the deviations of EDR and ADR on the overall deviation.

For the sake of comparison done between fuzzy logic and GP, some calculations related to the percentage difference were done. These calculations would help to evaluate the relevance of percentage difference values to the results. Percentage difference between the regression coefficients of MemADR and MemEDR for the D&P operator was provided in Table 8.4. The same percentage difference was found for Werners and UAO operators and provided in Tables 8.5 and 8.6, respectively. Table 8.7 provided the percentage difference between the regression coefficients of deviations of ADR and EDR for the GP approach.

Tables 8.4 to 8.6 showed the percentage difference for different numbers of GN nodes. The operator with the largest percentage difference is D&P (see Table 8.4), with over 118% for GN= 1024 nodes. Whereas for the same number of nodes, UAO and Werners have smaller percentage differences (see Tables 8.5 and 8.6), at 4.9% and 6.6%, respectively. For the test case GN= 512 nodes, percentage difference for the UAO operator was found only. For the other operators, no percentage difference could be obtained because these cases were represented in Table 8.2 as "-", which indicates constant values of the memberships for both energy decay and attack detection rates. This means no regression coefficients could be obtained and this also applied on the test case GN= 2048 for all the three operators.

The same calculations were done for the GP regression coefficients of deviations of ADR and EDR presented in Table 8.7. Table 8.7 represents the values of percentage difference between the regression coefficients of deviations of ADR and EDR (see Column 2 and 3 in Table 8.7) for the five test cases. The smallest and the best percentage difference was found at 11% for GN= 512 and the worst case was for GN=2048 at 88.7% (see column 4 in Table 8.7).

To compare the results of regression analysis for fuzzy operators and GP, average percentage difference was calculated. Table 8.8 provided the average percentage difference for D&P, Werners, UAO, and GP. From the average percentage difference results shown in Table 8.8, the percentage difference of Werners and UAO is close to each other. i.e. 30% and 35%, respectively. In other words, Werners and UAO operators are showing more or less a similar trend. Werners operator

was found to be the best among all techniques, followed by UAO, and then GP. D&P was showing the worst performance. D&P results are prominently showing the worst behavior among the three operators.

As the test case size increases, the percentage difference increased as well, which indicates that D&P operator had the tendency to give a less "balanced" behavior for higher number of nodes. For Werners and UAO operators, it was the opposite situation. As the test case size increases, the percentage difference decreased, which indicates that these operators have the tendency to give a more "balanced" behavior for higher number of nodes.

TABLE 8.4: Percentage difference between the regression coefficients of MemADR and MemEDR for using D&P operator.

Test Case	MemADR	MemEDR	Percentage Difference
128	1.04	-0.04	103.8%
256	1.07	-0.07	106.5%
512	-	-	-
1024	1.22	-0.22	118.0%
2048	-	-	-

TABLE 8.5: Percentage difference between the regression coefficients of MemADR and MemEDR using Werners operator.

Test Case	MemADR	MemEDR	Percentage Difference
128	0.262	0.746	64.9%
256	0.448	0.554	19.1%
512	-	-	-
1024	0.517	0.483	6.6%
2048	-	-	-

TABLE 8.6: Percentage difference between the regression coefficients of MemADR and MemEDR using UAO operator.

Test Case	MemADR	MemEDR	Percentage Difference
128	0.219	0.788	72.2%
256	0.412	0.590	30.2%
512	0.401	0.601	33.3%
1024	0.488	0.513	4.9%
2048	-	-	-

TABLE 8.7: Percentage difference between the regression coefficients of deviation of ADR and deviation of EDR using goal programming.

Test Case	MemADR	MemEDR	Percentage Difference
128	2.22	2.7	17.8%
256	1.45	0.733	49.4%
512	1.78	2	11%
1024	0.614	1.36	54.9%
2048	0.123	1.09	88.7%

TABLE 8.8: Average Percentage difference for D&P, Werners, UAO, and goal programming.

Appraoch	Average Percentage Difference
D&P	109%
Werners	30%
UAO	35%
GP	44%

In brief, to have the best performance, it is better to choose a technique while considering the size of the WSN. The results found that GP performed the best among the four techniques compared, when the size of the network is small. For instance, when GN= 128 and 512 nodes, percentage difference for GP were at 17.8% and 11% respectively. Percentage difference for Werners and UAO were found to be at 64.9% and 72.7%, respectively, for GN= 128 nodes. For large size networks, Werners and UAO were found to be the best. For GN= 1024 nodes, percentage difference for Werners and UAO were at 6.6% and 4.9%, respectively. Finally, GP was found to have a significantly big difference of 54.9%.

8.3 Conclusions

This chapter presented a mutual comparison of the results obtained for each of the D&P, Werners, and UAO fuzzy operators. Several linear multiple regression models were developed for the sake of comparisons, which are divided into two categories. The first was focussed on the effect of the operator related parameter on the overall membership. The second comparison was focussed on the effect of membership values of the attack detection and energy decay rates on the overall

membership. As far as the operator related parameter of the three fuzzy operators is concerned, the investigation found that D&P is undoubtedly performing the best among the three operators when considering the effect of the operator related parameter on the overall membership. Another investigation of the comparison between the three fuzzy operators showed that, generally, there was no significant difference in the results of the Werners and UAO operators. While Werners performed slightly better than UAO in balancing the effect of the two decision criteria EDR and ADR, D&P performed the worst when considering the effect of the memberships of ADR and EDR on the overall membership. Another comparison between the fuzzy logic approach and GP was presented, which found that Werners and UAO operators performed best in large size networks and GP was a better choice for small size networks.

Chapter 9

Conclusions

In this thesis, the process of finding the optimal trade-off between the attack detection and energy decay rates for the DDoS attack detection in WSN was addressed. The main objective of this thesis stems from development of this process in a way that make it ideal to simultaneously achieve higher attack detection rates and low energy consumptions. The process is modelled as a MCDM problem with two conflicting criteria namely, ADR and EDR. The first objective of this thesis was the application and analysis of some fuzzy operators to the problem. This objective was accomplished by applying three fuzzy logic operators, namely, D&P, Werners, and UAO that were chosen based on some characteristics unique to these operators. Sensitivity analysis of the operator related parameter was done for all fuzzy operators. The second objective was the first attempt in this domain, which focused on applying the GP approach, to the problem in hand which was analyzed through empirical results. Another objective was to compare the approaches used and then find the best among them.

In the following section, the main findings and contributions of this thesis are summarized.

9.1 Summary

In Chapter 3, the design of distributed denial of service attack detection scheme based on the distributed pattern recognition model for wireless sensor networks was summarized for the sake of providing the background of the problem domain. Furthermore, the concepts of fuzzy logic and goal programming were discussed.

The first contribution of this thesis was presented in Chapters 4 to 6. Chapter 4 presents a first attempt in the problem domain through application of the D&P operator and sensitivity analysis of the operator related parameter γ associated with the fuzzy function.

In Chapter 5, an extension of the work undertaken in [7], which did not perform the sensitivity analysis of the Werners operator, was presented. The applicability and effectiveness of the Werners fuzzy operator to the MCDM problem under consideration was assessed through several experiments. In that chapter, experimental results showed that the best value of the application aspect value, α, was somewhat insensitive to change in the value of operator related parameter, β.

The main goal of Chapter 6 was to analyze the UAO operator with its application to the problem under study. The performance and effectiveness of UAO were evaluated by its application to the proposed problem using some test examples. As observed in Chapter 5, the value of application aspect value α was somewhat insensitive to change in the value of UAO operator related parameter, ν. Another important finding was that the overall membership was not following any pattern as that of the membership of ADR or EDR. Instead, the overall decision was significantly acting as an ideal balance between these two criteria to compute the most optimal ratio between them. All the experiments were successful and no testing difficulties were encountered.

The second contribution of this thesis was presented in Chapter 7 where an alternative to fuzzy logic was proposed, in the form of GP method for decision-making. Herein, the best trade-off was found by varying the value of the application aspect ratio, α. After modelling the problem and finding the results, it was observed that the best value of α lies between the higher values that are above 0.7, for all five test cases. It was also observed that the overall deviation found to be the intersection point between the graphs of the two deviations of ADR and EDR.

Finally in Chapter 8, an elaborated analysis was presented by comparing the results obtained for each of the D&P, Werners, and UAO fuzzy operators, and also of the GP approach. Firstly, the comparisons focussed on the effect of the operator related parameter on the overall membership. The investigation found that D&P was undoubtedly performing the best among the three operators. Secondly, the focus was on the effect of membership values of the ADR and EDR on the overall membership. It was observed that there was no significant difference in the results for the Werners and UAO operator. Instead, the results found that the Werners operator was the best in balancing the effect of the two decision criteria, namely,

EDR and ADR. Furthermore, D&P results were the worst in this case. The latter part of Chapter 8 provided an overall comparison of the approaches utilized in this thesis, namely, fuzzy logic and GP. Werners and UAO operators performed best in large size networks and GP was a better choice for small size networks.

The following section highlights some potential extensions to the current work, which could serve as a basis for future research directions.

9.2 Future Work

This section provides some guidelines for future work, as follows:

- Other fuzzy logic operators which have not been studied in this thesis, could be engineered for the same MCDM problem considered. After that, the effect of having a wider range for the operator related parameter on the results will be studied. The new results might be compared to the results of the three fuzzy operators studied in this thesis.
- The results found in this thesis were based on the conflicting criteria while considering an equal level of importance for both of them. The decision-maker could assign explicit preference to one criterion and analyze the effect on results.
- Fuzzy logic and GP techniques were employed to address the MCDM problem considered in this thesis. Other MCDM techniques proposed in the literature, such as Goal Attainment and Weighted Sum methods, may be employed. These techniques can be engineered for the DDoS detection in WSN problem and a comparative study can be done with the techniques proposed in this thesis.
- Considering more criteria other than ADR and EDR. Examples of these criteria are the time needed to deliver communication messages in WSN (transmission delay), the cost of installation and maintenance of utilizing sensor nodes in WSN, and the rate of message delivery.

Bibliography

[1] Agha, S. (2006) Use of goal programming and integer programming for water quality management - A case study of Gaza Strip. *European Journal of Operational Research* Vol. 174, No. 3, pp. 1991–1998.

[2] Arunmozhi, S., and Venkataramani, Y. (2011) DDoS attack and defense scheme in wireless ad hoc networks. *International Journal of Network Security and Its Applications*, Vol 3., No. 3, pp. 182–187.

[3] Baig, Z. (2008) *Distributed denial of service attack detection in wireless sensor networks.* PhD Thesis, Monash University.

[4] Baig, Z. (2011) Pattern recognition for detecting distributed node exhaustion attacks in wireless sensor networks. *Computer Communications, Elsevier*, Vol. 34, No. 3, pp. 468–484.

[5] Baig, Z., Baqer, M., and Khan, A. (2006) A pattern recognition scheme for distributed denial of service (ddos) attacks in wireless sensor networks. In *18th International Conference on Pattern Recognition*, pp. 1050–1054.

[6] Baig, Z., and Khan, A. (2008) *A fault-tolerant scheme for detection of DDoS attack patterns in cluster based wireless sensor networks.* Book Chapter, Lecture Notes in Electrical Engineering, Springer.

[7] Baig, Z., and Khan, S. (2010) Fuzzy logic-based decision making for detecting distributed node-exhaustion attacks in wireless sensor networks. In *IEEE Second International Conference on Future Networks*, pp. 185–189.

[8] Bordogna, G., Fedrizzi, M., and Pasi, G. (1997) A linguistic modelling of consensus in group decision making based on OWA operators. *IEEE Transactions on Systems, Man and Cybernetics, Part A*, Vol. 27, No. 1, pp. 126–133.

[9] Bri, D., Garcia, M., Lloret, J., and Dini, P. (2009) Real deployments of wireless sensor networks *IEEE 3rd International Conference on Sensor Technologies and Applications*, pp. 95–100.

[10] Chang, R. (2002) Defending against flooding-based distributed denial of service attacks: A tutorial. *IEEE Communications Magazine*, Vol. 40, No. 10, pp. 42–51.

[11] Charnes, A., and Cooper, W. (1961) *Management models and industrial applications of linear programming.* John Wiley.

[12] Chen, C., Lai, Y., and Hsieh, C. (2000) Crisp-type fuzzy logic controller using Dubois and Prade's parametric t-norm-sum-gravity inference methods. *IEE Proceedings -Control Theory and Application*, pp. 167–175.

[13] Coello, C. (1999) A comprehensive survey of evolutionary-based multiobjective optimization techniques. *Knowledge and Information Systems*, Vol. 1, No. 3, pp. 269–308.

[14] Dawande, M., and Gupta, R. (2007) An integer-programming approach to the bicriteria multicasting problem in optical networks. *IEEE Transactions on Communications*, Vol 55, No. 4, pp. 752–765.

[15] Dombi, J. (1982) A general class of fuzzy operators, the De Morgan class of fuzzy operators and fuzziness measures induced by fuzzy operators. *Fuzzy Sets and Systems* Vol. 8, pp. 149–163.

[16] Dombi, J. (1982) Basic concepts for a theory of evaluation: The aggregative operator. *European Journal of Operational Research*, Vol. 10, pp. 282–293.

[17] Dubois, D., and Prade, H. (1979) Operations in fuzzy-valued logic. *Information and Control*, Vol. 43, pp. 224–240.

[18] Dubois, D., and Prade, H. (1982) A class of fuzzy measures based on triangular norms. *International Journal of General Systems*, Vol 8, pp. 105–116.

[19] Dubois, D., Prade, H., and Sedes, F. (2001) Fuzzy logic techniques in multimedia database querying: A preliminary investigation of the potentials. *Knowledge and Data Engineering, IEEE Transactions*, Vol. 13, No. 3, pp. 383–392.

[20] Duckstein, L. (1984) *Multiobjective optimization in structural design: The model choice problem.* North-Holland, Amsterdam.

[21] Elliot, J. (2000) Distributed denial of service attacks and the zombie ant effect. *IT Professional*, Vol. 2, No. 2, pp. 55–57.

[22] Frank, M. (1979) On the Simultaneous associativity of F(x,y) and x + y -F(x,y). *Aequationes Mathematicae*, Vol. 19, pp. 194–226.

[23] Franke, K., Koppen, M., and Nikolay, B. (2000) Fuzzy image processing by using Dubois and Prade fuzzy norms. In *IEEE 15th International Conference On Pattern Recognition*, pp. 514–517.

[24] Garber, L. (2000 Denial-of-service attacks rip the Internet. *Computing Processing (Hardware/Software), IEEE Computer Society*, Vol. 33. No. 4, pp. 12–17.

[25] Gligor, V. (2003) Guaranteeing access in spite of service-flooding attacks. In *Proceedings of the 11th International Conference on Security Protocols*, pp. 80–96.

[26] Hamacher, H. (1978) Ueber logische Verknupfungen Unschalfer Aussagen und deren Zugehoerige Bewertungs-funktione. *Progress in Cybernetics and Systems Research*, Vol. 3, pp. 276–288.

[27] Holland, J. (1975) *Adaptation in natural and artificial systems.* University of Michigan Press, Ann Arbor.

[28] Ijiri, Y. (1965) . *Management goals and accounting for control.* North-Holland, Amsterdam.

[29] Islam, M., Nadeem, K., and Khan, S. (2009) Optimal sensor placement for detection against distributed denial of service attacks. *Pakistan Journal of Engineering and Applied Science*, Vol. 4, pp. 80–92

[30] Johnson, B., and Liberatore, M. (2006) Incorporating quality considerations into project time/cost tradeoff analysis and decision making. *IEEE Transactions on Engineering Management*, Vol. 53, No. 4, pp. 534–542.

[31] Juneja, D., and Arora, N. (2010) An ant based framework for preventing DDoS attack in wireless sensor networks. *International Journal of Advancements in Technology*, Vol. 1, No. 1, pp. 34–44.

[32] Karlof, C., and Wagner, D. (2003) Secure routing in wireless sensor networks: Attacks and countermeasures. *Elsevier's Ad-hoc Network Journal, Special Issue on Sensor Network Protocols and Applications*, Vol. 1, No. 2, pp. 293–315.

[33] Karlof, C., and Wagner, D. (2002) Secure routing in wireless sensor networks: Attacks and countermeasures. In *The First IEEE Intl' Workshop on Sensor Network Protocols and Applications*, pp. 113–127.

[34] Kaur, G., Chaba, Y., and Jain, V. (2011) Distributed denial of service attacks in mobile adhoc networks. *World Acadmy of Science, Engineering and Technology, International Science Index*, Vol. 5, No. 1, pp. 594-597.

[35] Khan, M., Rehman, A., Zakaya, M., and Shah, G. (2012) Challenges for security in wireless sensor networks. *Journal of Computing*, Vol. 4, No. 9, pp. 390–396.

[36] Khan, M., and Sher, M. (2011) Challenges for security in wireless sensor networks. In *Proc. of WASET'11*, pp. 390–396.

[37] Khan, S. (2009) *Design and analysis of evolutionary and swarm intelligence techniques for topology design of distributed local area networks.* PhD Thesis, University of Pretoria.

[38] Khan, S., and Baig, Z. (2010) On the use of unified And-Or fuzzy operator for distributed node exhaustion attack decision-making in wireless sensor networks. In *IEEE International Conference on Fuzzy Systems*, pp. 1–7.

[39] Khan, S., and Engelbrecht, A. (2007) A new fuzzy operator and its application to topology design of distributed local area networks. *Information Sciences*, Vol. 177, No. 12, pp. 2692–2711.

[40] Khan, S., and Engelbrecht, A. (2008) A fuzzy ant colony optimization algorithm for topology design of distributed local area networks. In *IEEE Swarm Intelligence Symposium*, pp. 1–7.

[41] Khan, S., and Engelbrecht, A. (2009) Fuzzy hybrid simulated annealing algorithms for topology design of switched local area networks. *Soft Computing*, Vol. 3, No. 1, pp. 45–61.

[42] Lee, S., Kim, D., Lee, J., and Park, J. (2012) Detection of DDoS attacks using optimized traffic matrix. *Computers Mathematics with Applications*, Vol. 63, No. 2, pp. 501–510.

[43] Lewis, F. (2004) *Smart environments: Technologies, protocols, and applications.* Book chapter in Smart Environments: Technologies, Protocols, and Applications, ed. D.J. Cook and S.K. DasJohn Wiley.

[44] Li, S., Yang, Y., and Teng, C. (2004) Fuzzy goal programming with multiple priorities via generalized varying-domain optimization method. *IEEE Transactions on Fuzzy Systems*, Vol. 12, No. 5, pp. 596–604.

[45] Marks, L., Dunn, E., Keller, J., and Godsey, L. (1995) Multiple criteria decision making (MCDM) using fuzzy logic: an innovative approach

to sustainable agriculture. In *IEEE Third International Symposium on Uncertainty Modeling and Analysis and Annual Conference of the North American Fuzzy Information Processing Society*, pp. 503–508.

[46] Megerian, S., and Potkonjak, M. (2003) *Wireless sensor networks.* John Wiley Sons.

[47] Miettinen, K. (2001) Some methods for nonlinear multi-objective optimization. In *First International Conference on Evolutionary Multi-Criterion Optimization, LNCS, Springer*, pp. 1–20.

[48] Minhas, M., and Sait, S. (2005) A parallel tabu search algorithm for optimizing multiobjective VLSI placement. In *International Conference on Computational Science and its Applications, Singapore*, pp. 587–595.

[49] Mirkovic, J., and Reiher, P. (2004) A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communicatio Review*, Vol. 34, No. 2, pp. 39–53.

[50] Mizumoto, M. (1981) Fuzzy sets and their operations. *Information and Control*, Vol. 48 , pp. 30–48.

[51] Mizumoto, M. (1987) Comparison of various fuzzy reasoning methods. In *Second IFSA Congress* , pp. 2–7.

[52] Moorthy, M., and Sathiyabama, S. (2012) Effective authentication technique for distributed denial of service attacks in wireless local area networks. *Journal of Computer Science*, Vol. 8, No. 6, pp. 828–834.

[53] Murata, T., Oshida, H., and Gen, M. (2000) Rule-based weight definition for multi-objective fuzzy scheduling with the OWA operator. In *26th Annual Conference of the Industrial Electronics Society*, pp. 2756 – 2761.

[54] Newsome, J., Shi, E., Song, D., and Perrig, A. (2004) The sybil attack insensor networks: Analysis and defenses. In *3rd International symposium of Information Processing in Sensor Networks*, pp.259–268.

[55] Parno, B., Perrig, A., and Gligor, V. (2005) Distributed detection of node replication attacks in sensor networks. In *IEEE Symposium on Security and Privacy*, pp. 49–63.

[56] Perrig, A., Stankovic, J., and Wagner, D. (2004) Security in wireless sensor networks. *Communcations of the ACM*, Vol. 47, No. 6, pp. 53–57.

[57] Perrig, A., Szewczyk, R., Tygar, J., Wen, V., and Culler, D. (2001) Security protocols for sensor netowrks. *Wireless Networks*, Vol. 8, No. 5, pp. 189–199.

[58] Pfleeger, C., and Pfleeger, S. (2003) *Security in computing.* Prentice Hall PTR, Pearson.

[59] Preeti, S., Chaba, Y., and Singh, Y. (2008) Review of detection and prevention policies for distributed denial of service attack in MANET. In *Proceedings of 2nd National Conference on Challenges Opportunities in Information Technology*, pp. 56–59.

[60] Sait, S., Ali, M., and Zaidi, A. (2005) Multiobjective VLSI cell placement using distributed simulated evolution algorithm. In *IEEE International Symposium on Circuits and Systems, Kobe, Japan*, pp. 6226–6229.

[61] Sait, S., Faheemuddin, M., Minhas, M., and Sanaullah, S. (2005) Multiobjective VLSI cell placement using distributed genetic algorithm. In *Genetic and Evolutionary Computation Conference, Washington DC, USA*, pp. 1585–1586.

[62] Schweizer, B., and Sklar, A. (1963) Associative functions and abstract semigroups. *Publ. Math. Debrecen*, Vol. 10, pp. 69–81.

[63] Sharifnejad, M., Sharifi, M., Ghiasabdai, M., and Beheshti, S. (2007) A survey on wireless nensor networks security. In *IEEE International Conference on Sciences of Electronic, Technologies of Information and Telecommunication*, pp. 25–29.

[64] Sharmaa, G., Balaa, S., and Vermaa, A. (2012) Security frameworks for wireless sensor networks-review. *Procedia Technology*, Vol. 6, pp. 978–987.

[65] Stankovic, J. (2008) Wireless nensor networks. *IEEE Computer Society*, Vol. 41, No. 10, pp. 92–95.

[66] Tan, H., and Seah, W. (2005) Framework for statistical filtering against DDoS attacks in MANETs. In *The Second International Conference on Embedded Software and Systems*, pp. 456–465.

[67] Tilak, S., Abu-Ghazaleh, N., and Heinzelman, W. (2002) A taxonomy of wireless micro-sensor network models. *ACM Mobile Computing and Communications Review*, Vol. 6, No. 2, pp. 28–36.

[68] Torra, V. (1996) Weighted OWA operators for synthesis of information. In *Fifth IEEE International Conference on Fuzzy Systems*, pp. 966 – 971.

[69] Triantaphyllou, E. (2000) *Multi-criteria decision making methods: A comparative study applied optimization.* Springer.

[70] Virone, G., Wood, A., Selavo, L., Cao, Q., Fang, L., Doan, T., He, Z., Stoleru, R., Lin, S., and Stankovic, J. (2006) An assisted living oriented information system based on a residential wireless sensor network. In *IEEE Distributed Diagnosis and Home Healthcare, 1st Transdisciplinary Conference*, pp. 95–100.

[71] Weber, S. (1983) A general concept of fuzzy connectives, negations and implications based on t-norms and t-conorms. *Fuzzy Sets and Systems*, Vol. 11, pp. 115–134.

[72] Werners, B. (1987) An interactive fuzzy programming system. *Fuzzy Sets and Systems*, Vol. 23, pp. 131–147.

[73] Werners, B. (1988) Aggregation models in mathematical programming. *G. Mittra, H. Greenberg, F. Lootsma, M. Rijckaert, and H. Zimmerman (Eds.) Mathematical Models for Decision Support, Springer*, Vol. 48, pp. 295-305.

[74] Xiang, M., Chen, Y., Ku, W., and Su, Z. (2011) Mitigating DDoS attacks using protection nodes in mobile adHoc networks. In *IEEE Global Communications Conference*, pp. 1–6.

[75] Yager, R. (1997) Criteria importances in OWA aggregation: An application of fuzzy modelling. In *Sixth IEEE International Conference on Fuzzy Systems*, pp. 1677 – 1682.

[76] Yang, X., Ma, T., and Shi, Y. (2007) Typical DoS/DDoS threats under IPv6. In *Computing in the Global Information Technology, International Multi Conference*, p. 55.

[77] Yick, J., Mukherjee, B., and Ghosal, D. (2008) Wireless sensor network survey. *Computer Networks*, Vol. 52, No. 12, pp. 2292–2330.

[78] Zadeh, L. (1965) Fuzzy sets. *Information Contr*, Vol. 8, pp. 338–353.

[79] Zarghami, M., and Szidarovszky, F. (2008) Fuzzy quantifiers in sensitivity analysis of OWA operator. *Computers and Industrial Engineering*, Vol. 54, No. 4, pp. 1006–1018.

[80] Zhan, S., and Liu, N. (2011) A Multi-objective stochastic programming model for emergency logistics based on goal programming. In *IEEE 4th International Joint Conference on Computational Sciences and Optimization*, pp. 640–644.

[81] Zionts, S., and Wallenius, J. (1976) An interactive programming method for solving the multiple criteria problem. *Management Science*, Vol. 22, No. 6, pp. 652–663.

Appendix A
Nomenclature

This appendix provides a list of symbols and abbreviations used in this thesis.

List of Symbols

A	a criterion of a problem.
α	application aspect ratio.
B	a criterion of a problem.
β	operator related parameter of Werners.
γ	operator related parameter for D&P.
GN	graph neuron node.
$MaxADR$	maximum value of attack detection rate.
$MaxEDR$	maximum value of energy decay rate.
$MemADR$	membership function of attack detection rate.
$MemEDR$	membership function of energy decay rate.
mGN	master graph neuron node.
$MinADR$	minimum value of attack detection rate.
$MinEDR$	minimum value of energy decay rate.
μ	membership function of a solution in fuzzy logic.
μ_A	membership function of criterion A.
μ_B	membership function of criterion B.
ν	operator related parameter for UAO.
OM	overall membership.

List of Abbreviations

AP	Access Point.
AS	Authentication Server.
CPU	Central Processing Unit.
DoS	Denial of Service.
$DDoS$	Distributed Denial of Service.
$D\&P$	Dubois & Prade.
GP	Goal Programming.
ID	Identification number.
IP	Internet Protocol.
$MANETs$	Mobile AdHoc Networks.

$MCDM$	Multi-criteria Decision-making.
TCP	Transmission Control Protocol.
UAO	Unified And-Or.
$WLAN$	Wireless Local Area Network.
WSN	Wireless Sensor Network.
WS	Wireless Station.

ملخص الرسالة

المنطق الضبابي وبرمجة الهدف لهجمات الحرمان من الخدمة الموزعة في شبكات الاستشعار اللاسلكية

برزت شبكات الاستشعار اللاسلكية (WSNs) باعتبارها تقنية هامة لرصد الحالات الحرجة التي تتطلب استشعار عن بعد للحصول على البيانات اللازمة بغرض اتخاذ القرارات. لذلك يعتبر أمن شبكات الاستشعار اللاسلكية تحدي ليس بالأمر البسيط. يعتبر أمن شبكات الاستشعار اللاسلكية (Security in WSNs) عرضة لخطر عدد من الهجمات الخبيثة (Attacks) التي تم رصدها في الآونة الأخيرة. ويرجع ذلك إلى طبيعة البيئات التي تعمل بها شبكات الاستشعار اللاسلكية (WSNs) حيث تهدد الهجمات الموزعة (Distributed Attacks). تهدد هذه الهجمات الموارد الحسية لهذه الشبكات مثل استهلاكها الكبير للطاقة، وهدر قنوات التواصل (Communications Channels) بشكل لا يمكن تجاهله. في حالة هجمات الحرمان من الخدمات الموزعة (DDoS Attacks) في شبكات الاستشعار اللاسلكية، يعد معدل استهلاك العقدة (Node) لموارد الطاقة هو نقطة الضعف الأكثر استهدافا. يعود ذلك إلى طبيعة البطاريات المستخدمة في العقد والتي تعتبر ذات موارد محدودة وحياة قصيرة. وبالتالي تتطلب اليات الكشف عن هذه الهجمات حلا ذو طبيعة موزعة بالكامل وغير مكلف من ناحية متطلبات الاتصالات والطاقة. ونظرا للطبيعة المتضاربة بين اثنين من العوامل المهمة التي تؤثر على أداء أي نظام للكشف عن حدوث هجمات الحرمان من الخدمات الموزعة في شبكات الاستشعار اللاسلكية. هذان العاملان هما معدل اكتشاف الهجمة (Attack Detection Rate) ومعدل استهلاك العقدة للطاقة (Energy Decay Rate). ويعد ايجاد القيم المثلى لهذين العاملين من التحديات الهامة. بعبارة أخرى، تتحدد المهمة في ايجاد مقايضة معقولة (Reasonable trade-off) بين هذين العاملين. في هذه الأطروحة، يمكن صياغة المهمة السابقة في اطار السعي لاتخاذ القرار متعدد المعايير (Multi-criteria Decision-making). ويعتبر المنطق الضبابي (Fuzzy Logic) وبرمجة الهدف (Programming Goal) من الطرق المقترحة لحل المشاكل التي تستند على معايير متعددة. حيث تم اعتبار معدل الكشف عن الهجوم ومعدل اضمحلال الطاقة كمعايير لاتخاذ القرار. إلى جانب طريقة برمجة الهدف، تم استخدام عدد من القوانين التابعة للمنطق الضبابي (D&P, Werners, and UAO) لوضع آلية لتحقيق مقايضة مثلى (Best trade-off) بين المعايير المتعددة السالفة الذكر. وقد تم تقييم جميع الطرق المذكورة، وتشير نتائج التحليل التجريبي التي أثبتت فعالية الطرق المقترحة إلى أن قانون (D&P) أوجد أفضل النتائج بين جميع الطرق وذلك عند التركيز على على تأثير المتغير المرتبط بهذا القانون (Operator related parameter) على العضوية الكلية (Overall Membership). بينما عند التركيز على تأثير القيم العضوية لمعدل الكشف عن الهجوم ومعدل اضمحلال الطاقة على العضوية الشاملة، تبين أن قانون (D&P) اوجد أسوأ النتائج. وأسفرت نتائج تحليل المقارنة للطرق المقترحة أن قانون (Werners) كان خيارا أفضل لحل مشكلة صنع القرار المتعدد المعايير يليه قانون (UAO) ومن ثم طريقة برمجة الهدف.

جامعة البحرين

كلية تقنية المعلومات



المنطق الضبابي وبرمجة الهدف لهجمات الحرمان من الخدمة الموزعة في شبكات الاستشعار اللاسلكية

أطروحة مقدمة كجزء من متطلبات الحصول على درجة الماجستير في تقنية المعلومات

إعـداد

رولا يوسف محمد العمري

20033002

إشراف

د. سلمان أحمد خان

استاذ مساعد

جامعة البحرين

مملكة البحرين

يونيو، 2014