MODEL AND PROCEDURES FOR THE JAMMER AND TARGET ALLOCATION PROBLEM

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
OF
MIDDLE EAST TECHNICAL UNIVERSITY

BY

KIVANÇ GÜL

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF MASTER OF SCIENCE
IN
INDUSTRIAL ENGINEERING

DECEMBER 2018

Approval of the thesis:

MODEL AND PROCEDURES FOR THE JAMMER AND TARGET ALLOCATION PROBLEM

submitted by **KIVANÇ GÜL** in partial fulfillment of the requirements for the degree of **Master of Science in Industrial Engineering Department, Middle East Technical University** by,

Prof. Dr. M. Halil Kalıpçılar
Director, Graduate School of **Natural & Applied Sciences**

Prof. Dr. Yasemin Serin
Head of Department, **Industrial Engineering**

Prof. Dr. Ömer Kırca
Supervisor, **Industrial Engineering Dept., METU**

Examining Committee Members:

Assoc. Prof. Dr. Pelin Bayındır
Industrial Engineering Dept., METU

Prof. Dr. Ömer Kırca
Industrial Engineering Dept., METU

Assoc. Prof. Dr. Seçil Savaşaneril
Industrial Engineering Dept., METU

Assoc. Prof. Dr. İsmail Serdar Bakal
Industrial Engineering Dept., METU

Assoc. Prof. Dr. Orhan Karasakal
Industrial Engineering Dept., Çankaya University

Date: 03.12.2018

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last name: Kıvanç Gül

Signature:

ABSTRACT

MODEL AND PROCEDURES FOR THE JAMMER AND TARGET ALLOCATION PROBLEM

Gül, Kıvanç
M.Sc., Department of Industrial Engineering
Supervisor : Prof. Dr. Ömer Kırca

December 2018, 91 pages

In this thesis, the problem of finding the jamming angles to neutralize the maximum number of drones using least number of directed RF jammers when swarm drones attack to an area protected by an Anti-Drone defense system composed of radar, an electro-optic director and a directed RF jammer was studied.

First of all, in this study, prioritization of detected drone threats was realized using threat evaluation algorithms. Then, an optimization model was developed utilizing mathematical models that are used to solve set covering problems. Thus, a mathematical solution was ensured with this model which neutralizes the maximum number of high-priority threats by using the minimum number of directed RF jammer sub-systems.

Along with developed mathematical model, an algorithm based on heuristic approach was developed to handle the same problem. To compare the mathematical model and heuristic approach solutions, numerical experiments were carried out for attacks with different number of drones coming at random angles to an area protected by different number of RF jammers located so that the protected area is fully covered. Numerical experiments showed that heuristic approach yielded very close results as compared to mathematical model in a shorter time.

This thesis is of significance for being the first study to find the jamming angles and number of directed RF jammer systems to be used against swarm drone threats.

Keywords: Anti – Drone Systems, Jammer Systems, Swarm Drone Attacks, Set Covering Optimization Problems, Heuristic Approaches

ÖZ

KARIŞTIRICI VE HEDEF ATAMA PROBLEMİ İÇİN MODEL VE YÖNTEMLER

Gül, Kıvanç
Yüksek Lisans, Endüstri Mühendisliği Bölümü
Tez Yöneticisi : Prof. Dr. Ömer Kırca

Aralık 2018, 91 sayfa

Bu tezde, radar, elektro optik ve yönlü antene sahip karıştırıcı alt sistemlerden oluşan Anti Dron savunma sistemi ile dron tehditlerine karşı korunan bir bölgeye, çoklu dron saldırısı gerçekleştiğinde, en az sayıda karıştırıcı alt sistem çalıştırmak koşulu ile en çok sayıda tehdit değeri yüksek dronların etkisiz hale getirilmesini sağlamak amacıyla antenlerin hangi açıda karıştırma yapacağı problemi üzerine çalışıldı.

Bu çalışma kapsamında, öncelikle tehdit değerlendirme algoritmaları kullanılarak tespit edilen dron tehditlerinin önceliklendirilmesi gerçekleştirildi. Daha sonra küme kapsama problemlerini çözmek için kullanılan matematiksel modellerden yararlanılarak, bir optimizasyon modeli geliştirildi. Bu model sayesinde en az sayıda yönlü karıştırıcı alt sistem kullanarak, en çok sayıda tehdit değeri yüksek hedefin etkisiz hale getirilmesini sağlayan matematiksel bir çözüm sağlandı.

Geliştirilen matematiksel modelin yanı sıra, aynı problemi çözen bir sezgisel yaklaşım algoritması geliştirildi. Matematiksel model ve sezgisel yaklaşımın çözümlerini karşılaştırmak için, yerleri korunacak olan bölgeye göre önceden belirlenen farklı sayıda karıştırıcı alt sistemleri ve farklı sayıda rast gele çoklu dron saldırılarını içeren deneyler yapıldı. Bu deneyler sonucunda, sezgisel yaklaşım algoritmasının matematiksel modele çok yakın çözümler oluşturduğu ve problemi daha kısa sürede çözdüğü gözlemlendi.

Bu çalışma, yönlü antene sahip karıştırıcı sistemlerin çoklu saldırılar karşısında hedeflere yönlenme açılarını ve kullanım sayılarını belirleme üzerine yapılan ilk çalışma olması nedeniyle önem taşımaktadır.

Anahtar Kelimeler: Anti – Dron Sistemleri, Karıştırıcı Sistemler, Çoklu Dron Saldırıları, Küme Kapsama Optimizasyon Problemleri, Sezgisel Yaklaşımlar

To a Yellow and Navy Blue Future

ACKNOWLEDGMENTS

I wish to express my gratitude to my supervisor, Prof. Dr. Ömer Kırca for his guidance, advice, criticism and encouragements through the research. It was a great experience to being his thesis student.

I would like to express my gratitude and sincere thanks to my colleague Mehmet Emre Atasoy for his support, guidance and teaching for this study. I am grateful to him for his help in and out of the text.

I am indebted to my colleague Fatih Ovalı for his consideration, valuable comments, suggestions and encouragements through this study. I am grateful to him for sharing his intimate knowledge with me.

I also want to thank to my first academician friend Emine Gündoğdu for her support and motivation for my studies. I believe that she will be a great academician.

TABLE OF CONTENTS

APPENDICES

LIST OF TABLES

TABLES

LIST OF FIGURES

FIGURES

CHAPTER 1

INTRODUCTION

Today, with the development of technology, new vehicles have begun to been used in air attacks. Since the invention of Unmanned Aerial Vehicles (UAV), air attack and defense systems have gained new dimension. UAVs provide the opportunity to intervene in situations where human access is not possible or human life is not desired to be put in risk. For instance, these vehicles were initially invented to make life easier such as using in fire extinguishing or discovering new resources, but in the direction of war needs, have begun to appear on battlefields.

In the war environment, usage of UAV's can provide advantages in two perspectives. The first one of these advantages is gaining surveillance capability without being noticed by human perception. By attaching high quality cameras at the bottom of UAV's, they gain an ability to take strategic views and information by flying up to 1000 meters. The second advantage of UAVs usage in warfare is gaining attack capability without human loss. When weapons, such as bombs, guns or missiles, are integrated under the UAVs, it is possible to shoot the desired region by remote control ability.

Generally, while heavier UAV are preferred for ammunition transportation and attacking, mini/micro UAV (drones) are used for reconnaissance activities. Heavier UAV can be controlled from long distances, up to 250 km, and can carry more than 250 kg while flying. These type of UAV are also can be used as reconnaissance/surveillance aircrafts, because they have ability to carry high technology cameras, high resolution radars (SAR) and can fly up to 7 km from the ground. However, since these vehicles are large in size, it is not possible to make detailed exploration by approaching the critical area.

Heavier UAVs can only be used by military services, because their production can be done at state-controlled factories and only states have permissions to purchase them. Also, it’s hard to use these large vehicles and users should have pilot license certificate which is given from military services or related state institutions. These types of purchasing and flying constraints make heavier UAVs as state-controlled vehicles.

However, this situation changes for mini/micro UAV’s (drones), because they can be purchased from technology or toy shops easily. Also they can be produced by uncontrolled factories or can be made by ordinary person by collecting drones’ components. When these properties are considered, it can be emphasized that easy access of drones made them emerging global threats.

In that case, one question can be asked, “How can the drones be transformed into emerging threats and used in warfare?” In addition to their easy accessibility, other features of drones will help to bring out the answer of this question. Other features of drones are:

- Having small sizes that have radar cross section (RCS) values between $0.01m^2$ and $0.1m^2$.
- Cheap
- Carry small items, up to 25 kg
- Can fly up to 1 km from ground
- Can be controlled from 5 km distances
- Easy to use
- Hard to detect
- Have ability to swarm attacks

When these features are considered, it can be observed that the drones can be widely used in asymmetric warfare. Because, military services and states can reach heavier

UAV, but insurgent and terrorist groups supply their UAV needs from drones. These kind of groups use drones for reconnoitering, bombing, CBRN attacks, logistics support for small items (such as battery, handgun ammo, etc.), or forward observing for adjusting mortar and artillery firings.

The widespread usage of UAV in symmetric and asymmetric warfare environment has led to the establishment of a sophisticated defense system mechanism. These defense systems can be divided as Anti-UAV and Anti-Drone systems with respect to their shooting abilities. In order to emphasize the differences between these two defense systems, we need to explain their features and preferred killing/shooting abilities.

Constitutively, hard kill and soft kill methods are used to prevent all types of UAV attacks. In the hard kill methods, the main purpose is to physically destroy the threats by using firearms, such as interceptor missiles, bombs or heavy guns. On the other hand, the main purpose of the soft kill method is to make threats ineffective/unfunctional without shooting them. This method has been preferred when it is not desired to cause collateral damage the environment while neutralizing the threats.

In the Anti-UAV defense systems, hard kill methods are used in order to prevent heavier UAV attacks, because heavier UAVs can carry more dangerous weapons it is worth to shoot them by expensive/sophisticated weapons such as interceptor missiles they should be intercepted as far as from defended area. Since these vehicles have ability to fly at high altitudes, when they are shot by the weapon while flying in high altitudes, the surrounding area is not affected excessively, and this situation allows the usage of hard kill methods in the Anti-UAV defense systems. In addition to these reasons, while heavier UAVs can fly autonomously depending on their on-board INS systems in addition to GPS, RF jamming may not exhibit effective jamming performance and therefore, they are not preferred as a main weapon for the Anti-UAV defense systems.

In the sophisticated Anti-UAV defense systems, command and control centers, radars and electro-optical systems are used, in order to detect, identify and track the threats. The radar used in Anti-UAV system, has ability to detect, track and identify UAVs and create UAV tracks on the command and control screens. Generally this type of radars, cannot detect small objects in the air, such as birds and drones that have small RCS and these objects do not appear on the screen as tracks. In addition to detecting and identifying, electro-optical camera systems are used as a complementary to ensure that the detected object is a potential threat and tracking its' movements.

On the other hand, in the Anti-Drone systems there are sophisticated and non-sophisticated defense mechanisms for the protection of desired areas. As in the Anti-UAV systems, sophisticated Anti-Drone defense systems include command and control centers, radars, electro optical cameras and intercept weapons and traces of threats can be seen on the command and control screens. However, radars and intercepting methods are different from the ones used in Anti-UAV systems.

In the non-sophisticated Anti-Drone method, detection, tracking and identifying are done with the ability of the human eye and detected threats are neutralized and grounded by using hand-held jammer weapons. However, this defense approach is based on ability of human vision, and it is not effective for high altitude threats which cannot be seen by human eye. For this type of drone threats, more sophisticated defense system should be preferred and placed around the desired areas.

In that case, two questions should be answered in order to understand affection of sophisticated Anti-Drone systems. The first of these questions is "What are the radar and killing method differences between Anti-Drone and Anti-UAV defense systems?" and the second one is "What are the features and types of sophisticated Anti-Drone defense systems?"

The first difference between two defense systems is about their radar types. Generally, Anti-UAV system radars cannot detect small cross sectional objects, because these radars are optimized to find and identify the threats like heavier UAVs, aircrafts or helicopters. They generally transmit huge amount of power that make them dangerous to be used in urban areas. Therefore, these types of radars are not applicable for Anti-Drone defense systems and specific radars are developed in order to detect small sized flying objects. These specific radars not only detect small objects in the air, but also can classify and identify drone threats. For example, radar can distinguish drones from birds which are flying at the same time in the air, and the drones are displayed on the command and control screen with a different color in order to separate them from birds.

The second difference is related to intercept methods of these defense systems. Although, the hard kill methods are mostly preferred in Anti-UAV systems, it is not applicable and cost effective for drone defense. Drones are small, fast and have ability of instant maneuvering, thus it is difficult to predict their next movements and shoot them with guns. Tactical missiles can be used for shooting, but if the drone threats are in urban areas, this decision may result in more harmful effects for environment than by threat itself. For inhabited areas this method can be preferred but this time cost per kill arises. No one wants to spend couple of ten thousands worth missiles against very cheap threats. Therefore, soft kill methods are more feasible and effective for Anti-Drone defense systems.

As a soft kill method, jammers are used to neutralize drone threats in the defense systems. By transmitting stronger jamming signals, the RF remote control and GPS signals are blocked and drones become uncontrollable by user. With the help of the radar and/or other tracking sensors in the system, jammer transmits in the direction of the threats and they are left unfunctional for their intended mission and they either fall down or land on ground.

There are two types of sophisticated Anti-Drone systems, which have similar system architecture (given in Figure – 1) and system process (given in Figure – 2), are used to neutralize all known drone threats in urban and rural environments. Both of them have advantages and disadvantages with respect to the features of placed areas.

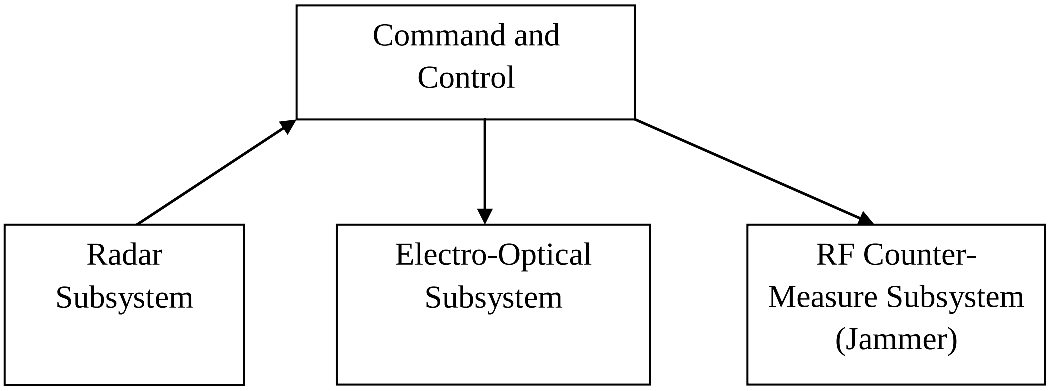

Command and Control
Radar Subsystem
Electro-Optical Subsystem
RF Counter-Measure Subsystem (Jammer)

Figure – 1 System Architecture of the Anti-Drone Systems

The first one of the Anti-Drone systems is in distributed configuration, which includes command and control center, radar, electro optical and RF countermeasure subsystems. In this configuration, radars, cameras and jammers are placed seperately from each other, and they are distributed along the boundary of the protected area. The number of each subsystem is determined with the intention of ensuring the coverage of the whole defended area in the direction of their activity ranges. The activity ranges of the each subsystem will be given with all details in Chapter 3. Emplaced subsystems are controlled and monitored from one command and control center.

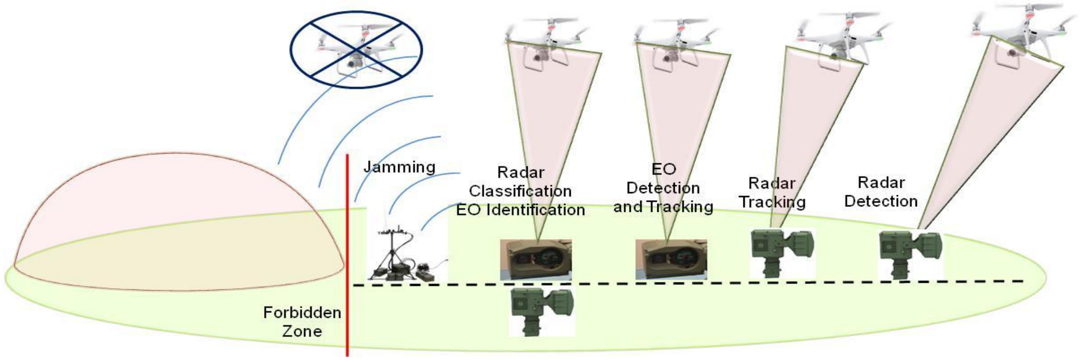

Jamming
Radar Classification EO Identification
EO Detection and Tracking
Radar Tracking
Radar Detection
Forbidden Zone

Figure – 2 System Process of the Anti-Drone Systems

The radar and electro-optical subsystems used in this configuration have same features with the second type of the Anti-Drone system like in the integrated configuration. The only difference is that subsystems are placed independently of each other in distributed configuration. However, features of the RF countermeasure subsystems have some differences for each configuration. In the distributed one, jammer with omni directional antenna is used, which has capable of jamming 360 degrees, as RF countermeasure subsystem. This jammer creates a semi-spherical prevention umbrella and threats are neutralized in this protected area. The feature of jamming on whole area can be an advantage or disadvantage depending on needs of the defended environment. If there are similar devices utilizing same RF band or GPS in the friendly zone of defended area, they will be adversely affected by jamming. For example, usage of the omni directional jammer in naval platforms or airports can cause friendly systems to become dysfunctional. Nevertheless, this type of jammers provides an advantage against swarm attacks. Since the swarm attacks constitute a threat by coming from in different directions at the same time, they become ineffective collectively when they enter the field of prevention umbrella created by omni directional jammer.

In the second type of the Anti-Drone defense system, which is regarded as integrated configuration, the same featured command and control center, radars and electro-optical subsystems are used to protect desired areas. However, the integration of radar and electro optical subsystems shows differences from distributed configuration. In addition to integration difference, directional antenna is used rather than omni directional one in the RF counter-measure subsystem of integrated configuration.

In this version, radar, electro optical cameras and directional antenna of jammer are mounted on a spindle mast. In contrast to omni directional antenna, directional antennas cannot jam 360 degrees and cannot create a protection umbrella. They produce directional beams transmitting much more power as compared to omni-antennas but the antenna needs to be steered in the direction of the threat to make it effective for jamming. Thus, jammer with directional antennas can be used to protect areas where the RF waves and GPS signal are actively used, because insider systems do not affected from counter measure waves when the jammer was opened.

Although, directional antenna provides an advantage of defending RF waves and GPS signal used areas, it can be vulnerable for swarm attacks. Since directional antennas can jam through a certain sector, when the attack comes from different directions simultaneously, some of the areas may not be covered by counter measure subsystem. In order to provide a protection for this type of swarm attacks, more complex defense algorithm should be developed for integrated Anti-Drone systems. This algorithm should perceive the threats and prioritize them according to their attack capabilities. In addition to that, decision about which directional antenna jam to which threat should be determined by this algorithm.

In this study, set covering based algorithm will be illustrated which are able to solve threat coverage problem for integrated Anti-Drone defense system case. This algorithm prioritize threats according to their approaching times and direction of movements and neutralize them with respect to competence of directional antenna jammers. In addition to that, inspired by set covering models, an mathematical model has been developed, which decides the directional antenna's jamming angles and directions in order to neutralize the maximum number of the high valued threats that attacks from the different directions. This model also enables the neutralization process by using the minimum number of directional antenna jammer. As an alternative to this mathematical model, we will develop a heuristic solution approach to solve this coverage problem. The performance of the mathematical model and the heuristic solution approach are evaluated through creating different attack scenarios which are explained in Chapter – 4. The evaluation results show that differences between these two solution method and show us their coverage performance.

The organization of this thesis is as follows. In Chapter 2, a brief overview of the literature is explained about the set covering and angle coverage problems, which are used to develop mathematical model and heuristic approach to solve threat coverage problem. In addition to that, the threat evaluation studies will be reviewed in this chapter. Chapter 3 contains the detailed problem definition, threat prioritization algorithm and the mathematical model solution approach. The developed heuristic solution approach for the same problem is also explained in Chapter 3. In Chapter 4, the solutions of mathematical model and heuristic approach are presented and discussed for different scenarios. The threat generator program which is constructed to create problem environment, is also explained in Chapter 4. Finally, concluding remarks are made in Chapter 5.

CHAPTER 2

LITERATURE REVIEW

In this chapter, literature review will be explained to develop an algorithm which aims to neutralize the maximum number of high valued drone threats by using directional antenna jammers when the different number of swarm drone threats attack in different directions to the protected area where defended by integrated Anti Drone Defense Systems. In this context, literature studies related to field and angle coverage problems are examined during the algorithm development process.

In addition to coverage problems, literature reviews about threat evaluation will be explained in order to develop a threat prioritization algorithm based on some parameters about threats.

While describing the literature studies, firstly a general information about Set Covering Problems and its' usage areas in the literature will be explained. Then we will explain Angle Coverage Problem solution techniques which are generally used for network and jammer coverage problems. Finally, studies about Threat Evaluation techniques will be explained which will be used for developing the threat prioritization algorithm.

2.1. Set Covering Problems

Set covering is a type of problem that can be solved with developing optimization models and encounter in different areas in real world. This type of problem is used in different applications to obtain optimum results by interpreting set covering approach in different ways. Flexible manufacturing, scheduling, routing, wireless networks, assembly line balancing, service area and threat coverage are some of the applications which use the set covering problem algorithms to develop optimal solutions.

The objective function of the set covering problem can be configured to be maximized or minimized according to desired result in the problem. While developing a mathematical model for the set covering problem, the parameters and the data matrices that give information about the problem, should be prepared carefully.

The basic mathematical structure of the set covering problem stated by Al-Sultan et al. (1996), is given below. In this structure, they used zero-one integer program to define set covering problem mathematically.

$$\min cx$$

$$\text{Subject to} \quad Ax \geq e, \quad x \in \{0,1\}^n$$

c : is a real vector of length “n”.

A : is a (m x n) matrix of zeros and ones.

e : is an array which constrain the decision variable

x : decision variable which is $x_{j\,,}$ j = 1,2,… , n where

$$x_j \quad = \begin{cases} 1 \text{ if column j is the solution} \\ 0 \text{ otherwise} \end{cases}$$

In this mathematical model, they mentioned minimizing the objective function, but it can be considered as maximizing structure according to needs of the problem by changing constraints. Their mathematical structure will be modified in our problem to obtain maximum threat value coverage.

Although the set covering problem structure has been used in many real world areas, it is seen that most of the researches are about location coverage problems. Studies about the set covering based location coverage problems guide us while developing our set covering based mathematical model.

Toregas et al. (1970) was one of the first studies about the location coverage problems and they stated the set covering problem about the location of emergency service facility. In this paper, they separate the user from his closest service area by maximizing time or distance. After the solution of the mathematical model which they developed, number of the emergency service facility was provided to reach desired service for users.

R. Church and C. Revelle (1974) started to study about The Maximal Covering Location Problem (MCLP) and stated the maximum coverage for different located facilities with given radius. In their study, they mentioned two objective for the set covering based location problems:

1. Total weighted distance or time for travel to facility.
2. Maximal service distance, which is the distance or time that the user have to travel to reach that facility.

They used the maximal service distance as a measure of the value of given location configuration. The value based approach which was taken into account in their study, provides inspiration for our set covering mathematical model.

These studies have pioneered the solution of many coverage problems and have been developed for different type of problems. Kun Zang and Songlin Zang (2015) stated the set covering mathematical model to decide adding a new facility within the current service area which serves for large populations. They created a simulation algorithm with set covering based mathematical model and by changing number of facilities and location of the population that needs service, to find the maximum service area.

Berman et al. (2013) stated the maximum location covering problems with uncertainty of travel time and mentioned this problem by different time scenarios.

They used real time data of fire station in the Toronto and developed different solutions for different type of facilities for different conditions. They created mathematical model based on set covering problem and achieved the optimal solution with respect to travel time scenarios.

On the other hand, Minimal Coverage Location Problem (MinCLP) is also studied as a part of set covering algorithms. In this type of problems, the main objective is finding an optimal location by applying minimum coverage. Takaci et al. (2013) stated that the difference between the maximum and minimum coverage location problems and explained the solution approach for MinCLP.

In addition to location problems, set covering problem is also used in different areas such as network coverage and life time schedule problems. Lin et al. (2008) applied the maximization of network coverage by converting the main point to set covering problem. They divided network area into regional grids and solved the minimum set covering problem by creating minimum set of grid nodes.

Zaixin Lu and Wei Wayne Li (2015) mentioned set covering to solve the scheduling problem for data collection and target coverage in wireless sensor networks by providing maximum network lifetime. They found the schedule for using minimum number of wireless sensors by taking into account the life span of the sensors and their coverage area.

In addition to the model based solution methods, there are also heuristic approaches for the set covering problems. In particular, the heuristic algorithms have been developed to give better quality solutions for the large scale set covering problem instances within short computing time. (J.E. Beasley, 1990).

Caprara et al. (1999) developed the Langrangian based heuristic method for the set covering problem in order to solve crew scheduling in the Italian Railway Company. Their heuristic approach solves the set covering problem instances up to 5,500 rows and 1,100,000 columns within the short solution times and gives the optimal or best known solution. Their heuristic approach has two main characteristics which are dynamic pricing scheme for variables and the systematic use of column fixing.

However, Haddadi et al. (2016) claim that Langrangian heuristic method is more effective for the small scale set covering problems. Therefore, they developed the Two Phase heuristic method for set covering. In their two phase method, the size of the given set covering problem is reduced by removing some variables in the first phase, and then in the second phase the simple Langrangian heuristic method is applied to the reduced problem.

In addition to Langrangian and Two Phase heuristic algorithms, there are also greedy algorithms, primal – dual algorithm and the state of the art heuristic algorithms are used to solve set covering problems. Umetani et al. (2007) survey these heuristic methods and analyze their performances through experimental instances.

2.2. Angle Coverage Problems

Angle coverage problems are generally discussed in the literature on sensors and wireless infrastructures about network problems. In this context, it is aimed to provide maximum coverage or minimum sensor usage in terms of angle coverage constraints by developing different types of mathematical model approaches or determining maximum coverage angles by creating mathematical formulas without using any model. The aim of these two approaches is to ensure desired coverage by using the angle information of the threats or regions.

Tseng et al. (2012) studied about providing maximum object coverage in network infrastructure by using least number of sensors with limited angles with respect to some angle constraints. In their model, sensors can only cover a limited angle and range, but can rotate 360° to any direction to cover particular angle. They developed distributed and polynomial time algorithms in order to solve this problem.

The angle coverage formulations of this paper have contributed formulas for our coverage matrices which will be explained in parameter generation part at Chapter – 3.

Chow et al. (2007) handled angle coverage problem with different perspective. They studied about finding minimum cost cover that preserves all the angles of visual sensors with minimum transmission cost. In their problem, they aimed to achieve less transmission energy for sensors by providing 360° coverage. In this context, they transformed minimum cost cover problem into the shortest path problem and used angle constraints to achieve maximum coverage and minimum transmission energy.

Lui et al. (2007) studied the angle coverage problem for the camera images in visual sensor networks. In this problem, they aimed to provide image resolution requirements by preserving all angles of view of the object. For this reason, they developed a distributed algorithm to use minimum set of sensors to cover maximum angle of the view of the objects. In this algorithm, angle between the image of the object and the view point of the sensor is calculated by mathematical formulas and the direction of the sensor is determined to cover maximum image of the objects.

When the other studies in the literature about angle coverage problem are reviewed, it is noticed that firstly it is necessary to determine angle between the object to be covered and tools to cover it. Then, the maximum object coverage or minimum number of coverage tool usage is determined by constraining the coverage angle with respect to capabilities of the tool. Thus, the desired goal of the problem is achieved by maximizing the constrained object coverage.

2.3 Threat Evaluation

While solving the mathematical models or heuristic approaches to neutralize threats, firstly the realistic information should be provided by building prioritization among threats. Therefore, threat evaluation (TE) algorithms have been developed to classify and prioritize threats according to their importance levels.

Army (1994) stated that TE is a pre-deployment process which is about encyclopedic knowledge of enemy, tactics, doctrine and capabilities of a commander or experienced staffs to deduce nature of threats which they face. TE makes a decision for neutralizing threats by ranking them from the most threatening to the least threatening. (Naem et al., 2009).

Roy et al. (2002) state that while determining the threats that represent the highest danger is of great importance, error can occur since lesser threats will be prioritized as a greater threat and this situation can result in engaging the wrong threats, which often will have severe consequences. Therefore, when prioritizing the threats, danger factors about defended assets should be well defined and the characteristic of threats should be analyzed carefully. Steinberg et al. (1999) mentioned that, TE is a part of threat analysis which in an information fusion context that is a central part of impact assessment in the well known data fusion model.

Steinberg (2005) stated that threat prioritization is modeled in terms of relationship between threatened entities and threatening entities. In this expression, threatened entities represent defended assets and threatening entities are referred to as targets.

In order to create a relationship between threatened and threatening entities, surveillance infrastructures should be employed to the defended assets to identify threats and provide information about them. Heyns (2008) stated that, radars and associated sensors provide data about threats for TE process and they are responsible for detecting, tracking and identifying the potential threatening objects. Therefore, the necessary information is provided to begin prioritizing process according to threats’ characteristics.

After receiving information about the threats, this data should be classified to determine the rank of the threats. Based on the literature about threat evaluation publications, there are three parameters to classify threat information.

1. Capability Parameters: These parameters give information about threat’s capability to threaten the defended asset. When ranking threats by capability

parameters, capability index defines the ability of the threat to inflict damage to a defended asset. (Naem et al., 2009). The threat type, weapon capacity, fuel capacity, speed, direction and weapon type can be defined as capability parameters. (Roy et al., 2002).

2. Intent Parameters: Intent parameters are used to prioritize threats in terms of their willingness to attack to defended asset. Roux et al. (2007) stated that intent parameters are the most difficult one to estimate, but capability parameters and measured attributes can be used to make this estimation. Oxenham (2013) mentioned that, threat's velocity in combination with its altitude can give good information about the intent to threat attack a defended asset. In addition to that, speed, heading (bearing and course), direction changes and maneuver ability of threats are used to determine intent parameter indexes. (Paradis et al. 2005).
3. Proximity Parameters: Proximity parameters are about measuring the proximity of the threats to the defended asset. Johansson et al. (2008) stated that the proximity parameters are the most important class of parameters to determine threat values. Calculating the distance between the threat and the closest point of the defended asset is the key point of the measuring proximity. In this context, the distance between the asset and threat should be calculated clearly to determine importance level of threats. Roy et al. (2002) developed the closest point approach (CPA) to make this calculation and determine shorter distance targets as high potential threats while classifying distant targets as less threatening.

Naem et al. (2010) stated that, the best way for the ranking threats can be obtained by combining two or three of these parameters. In our paper, proximity and capability parameters will be used to prioritize threats attacking the protecting area.

It is seen that, there is no study on coverage problems about directional antenna jammer and integrated Anti Drone Defense systems. In this paper, we will focus on directional antenna usage for Anti Drone Defense systems by utilizing set covering and angle coverage algorithms. In line with these algorithms, a mathematical model will be developed that neutralizes the most valuable threats by using minimum number of directional antenna jammers. In addition to that, in order to determine importance level of threats and prioritize them, threat evaluation techniques based on literature survey will be used in this paper.

CHAPTER 3

PROBLEM DEFINITION

AND ANALYSIS

In this chapter of the thesis, we will focus on a problem which is about protecting an area from drone attacks by use of integrated Anti-Drone defense system. Each integrated Anti-Drone system has its' own radar, electro optical and a directional RF counter measure subsystems all on a mast that can work independently from each other and an additional independent omni directional RF counter measure subsystem. The main aim of this study is neutralizing maximum number of threats with respect to their priority by using minimum number of RF counter measure subsystems and protecting the area without the need of using omni directional jammer. In this problem, it is aimed to protect the area as much as possible without using the omni directional jammer; because it is possible that there are friendly subsystems utilizing the same band of jammer or using GPS in the neighborhood of the integrated anti-drone system. When used, omni directional jammer may degrade or totally prevent the friendly systems from functioning, which is an undesired collateral damage.

For this purpose, a threat generator program has been developed which generates threats with respect to the features of radar and RF counter measure subsystems. After the threat generation process, threats are prioritized according to their arrival time and the distances to the protected area. Then, these threats information are used as parameters by the developed mathematical model inspiring from Set Covering Problem's optimization model algorithms. The features of the electro optical cameras are not reflected in the threat generator program, because cameras are used for surveillance and verification of the threat in the system architecture. Threat identification process is out of the scope of this thesis. The threat generator program also defines an environment including a protected area, an integrated Anti-Drone defense system and one omni directional jammer. This program generates drone threats that move randomly. Finally, the behavior of the threats is assessed and which directional RF jammer should be used and which threats have been intercepted are determined by the solution of the mathematical model. After this optimal decision, if the directional jammers are insufficient to neutralize the threats, as a last ditch, the decision of the omni directional jammer activation is suggested to the user. The basic functional flow of the problem is given in Figure – 3.

The threat generator program was developed by using JAVA Eclipse program and mathematical model was created and solved by using IBM Cplex Studio.

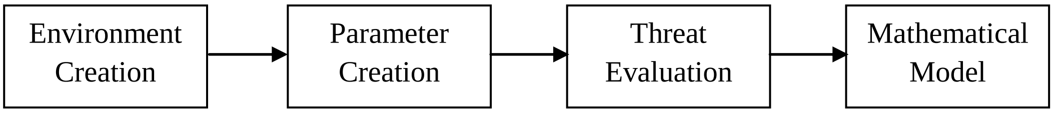


Figure 3 – The Basic Functional Flow of the Problem

The data and assumptions related to the subsystems of the Anti-Drone defense system, parameter generation and threat evaluation algorithms and the mathematical model developments will be explained in detail in the following parts of this chapter.

3.1. Mathematical Model

The mathematical model that created for this purpose is solved by running IBM Cplex Studio and based on the solution; it is revealed that which jammer antenna has stopped at which angle and which threats have been neutralized.

In the establishment of this mathematical model, a model was designed to neutralize the maximum number of threats with respect to their priority by being inspired from set covering model algorithms. After this formulation, the model has been improved by adding a new objective and constraint and the neutralization of the maximum number of threats is achieved by using the minimum number of jammers with running of this improved mathematical model. The mathematical model formulation inspired by the set covering model algorithm and its' improved state are explained in the following section.

The parameters created by the threat generator program for using in the mathematical model are described in the parameter creation part. The decision of the neutralizing the maximum number of threats by using the minimum number of jammers will occur after the mathematical model has been solved, by using these parameters.

3.1.1. Set Covering Based Mathematical Model Formulation

The formulation of the mathematical model that gives the result of which jammer antenna covers which threats at what angle, by using the threat and jammer-based parameters is given below.

In the attack scenarios, there are M threats indexed as i = 1,…, M are covered or neutralized by N jammers indexed as j = 1,…, N with any of 72 jammer antenna angles are indexed as g = 5°, 10°, 15°, … , 360°.

Parameters:

$$a_{jgi} = \begin{cases} 1 \text{ if jammer j at angle g covers threat i } (a_{jgi} \in \{0,1\}) \\ 0 \quad \text{else} \end{cases}$$

w_i = The importance or weight value of threat i ($w_i \in (0,1)$

Decision Variables

$$x_{jg} = \begin{cases} 1 & \text{if jammer j is set to angle g} \\ 0 & \text{else} \end{cases}$$

$$z_i = \begin{cases} 1 & \text{if threat i is covered} \\ 0 & \text{else} \end{cases}$$

Model Formulation

$$\max \quad \sum_{i=1}^{M} w_i \, z_i \tag{1}$$

s.t.

$$\sum_{g=5}^{360} x_{jg} \leq 1 \qquad \forall\, j, g = 5,10,\ldots, 360 \tag{2}$$

$$\sum_{j=1}^{N} \sum_{g=5}^{360} a_{jgi} x_{jg} \geq z_i \qquad \forall\, i, g = 5,10,\ldots, 360 \tag{3}$$

$$x_{jg}, z_i \in \{0, 1\} \tag{4}$$

- (1) is the objective function of the mathematical model to maximize the weight value of the total neutralized threats by jammer.
- (2) is the first constraint of the model which ensures that one jammer antenna can only be adjusted to a single angle.
- (3) is the second constraint of the model which ensures that any threat can be neutralized by any jammer antenna if antenna's adjusted angle can cover the threat.
- (4) is ensures that x_{jg}, z_i are binary variables

If the problem is solved by using this mathematical model, the jammer antennas can neutralize the threats to maximize priority weight of the covered threats, but this solution is not enough for reaching the desired protection level. For example, when a threat moves to protected area which has higher priority than other threats and in the range of the more than one jammer, this model may allow more than one jammer to be activated against this particular threat and duplicate use of jammers may cause leakage of other threats. In addition to that, this model cannot prevent the usage of all jammers if the threats are in the range of the jammer antennas. Therefore, this mathematical model needs to be improved to minimize the usage of the number of jammers.

3.1.2. The Improvement of the Mathematical Model Formulation

The set covering algorithm based mathematical model is improved by adding a new objective function which aims to minimize the number of used jammers. For this purpose, a new decision variable is defined and this variable based objective function and a constraint is added to mathematical model. This new decision variable and improved optimization model formulation is given below;

$$\mathrm{y_j} \quad = \begin{cases} 1 & \text{if jammer j is used} \\ 0 & \text{else} \end{cases}$$

ε = Very small number ($\varepsilon \leq \min\ \{w_i\}$ for all $i = 1,2,3,\ldots,M$)

Improved Model Formulation

$$\max \quad \sum_{i=1}^{M} w_i\, z_i - \varepsilon \sum_{j=1}^{N} y_j \tag{5}$$

s.t.

$$\sum_{g=5}^{360} x_{jg} \leq y_j \qquad \forall\, j, g = 5,10,\ldots,360 \tag{6}$$

$$\sum_{j=1}^{N} \sum_{g=5}^{360} a_{jgi} x_{jg} \geq z_i \qquad \forall\, i, g = 5,10,\ldots,360 \tag{3}$$

$$x_{jg}, y_j, z_i \in \{0, 1\} \tag{4}$$

(5) is the secondary objective of the mathematical model that minimize the number of used jammers.

(6) is the additional constraint of the model which ensures one jammer antenna can only be adjusted to a single angle and prevent excessive jammer usage by evaluated with (3).

Since the main purpose of the model is to maximize the total importance weight of the neutralized threats, the function that minimizes the usage of the jammer is adapted to the primary objective.

In this adaptation, the total number of used jammer is multiplied by a very small ε value and added to the objective function. Therefore, model is forced to minimize the number of jammer usage in order to maximize the objective value of the mathematical model, which is total importance weight of the neutralized threats.

After the mathematical model is solved, the solution and threat information for each period are saved into an excel file. In the Excel file, separate sheets are created for each period and the user can analyze the solution of the model by checking these sheets. The output example for one period is given in the Appendix – B, which is created through threat and jammer information given in Appendix – A.

The analyzes of solution of the mathematical model for different scenarios and for which cases this model is more effective will be examined in the Experimental Results chapter of the thesis.

3.2. Parameter Generation

The threat generator program generates threats information for use as a parameter in the mathematical model by using the features of radar and counter measure subsystems and taking into account some assumptions about Anti-Drone defense system.

3.2.1. Features and Assumptions of Radar Subsystem

In the Anti Drone defense system, the radar subsystem is used to detect and track the threats. In a real scenario, detection and tracking is a random process resultant from the nature of radar. Thus, detection and tracking success is probabilistic depending on many parameters such as transmitted power, frequency, antenna type, transmitted waveform type, receiver type, weather, terrain, RCS of the threat and so on. But in the threat generator program, probability of detection and tracking is taken as 1, which means a track is always initiated when the threat resides in the bore sight plane of the radar antenna while it rotates and updated at each revolution.

General specifications of the radar subsystem are given below;

- Multi target tracking and classification.
- 360° Continuous scanning in azimuth.
- Rotation rate is 15 rpm. It means that, radar can scan 360° in 4 seconds and track data is updated every 4 seconds.
- Ability to perform 2D scanning. It means that, only 2D coordinate values are generated by radar.
- 40° Elevation coverage ability.
- Instrumented (maximum) range is 1500 meters.
- Blind range is 100 meters. Radar cannot detect threats from 0 up to 100 meters.
- Ability to produce speed, direction and 2-D coordinate data for each drone threat.

In addition to these specifications, there are some assumptions of radar are made in order to create parameters for threat generator program. These assumptions are as follows;

- Tracking of threats will be maintained until neutralized by jammer. Radar will not lose any track once initiated.
- It is assumed that every drone threat resides in the elevation coverage of the radar throughout its lifecycle, i.e. from its generation to neutralization. Thus, elevation coverage data of radar is not used in the threat generator program. By this assumption, projection of threat trajectory to (x, y) plane will be enough and elevation of the threats becomes irrelevant to the threat generator program. Accordingly no height information is input to the program.

Using these features and assumptions, the threat generator program generates the necessary parameters and threat information for the mathematical model to be run.

3.2.2. Features and Assumptions of the Counter Measure Subsystem

The counter measure subsystem is designed and developed to provide protection against threats by jamming them with its directional antenna. Jamming frequencies cover all the bands that are used by the threats. Multiple threats can be neutralized if those threats are within the transmit beam of the jammer antenna. In the threat generator program, characteristics of the RF counter measure subsystem are used to identify conditions to neutralize threats.

General specifications of the RF counter measure subsystem are given below;

- Applies jamming against RC (Remote Control) receivers, UHF/VHF receivers, GPS receivers, Wi-Fi devices, GSM (3G and 4G) receivers.
- The omni directional antenna has 360° coverage on azimuth and creates a semi spherical protection umbrella.
- The RF counter measure subsystem used in integrated system transmits jamming with directional antenna. This antenna has 60° coverage in both azimuth and elevation. The effective coverage of the antenna is shown in Figure – 4.

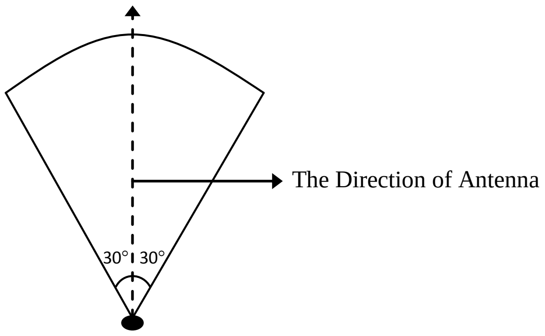


Figure 4 – The Effective Coverage pattern of Directional Antenna in the RF counter-measure subsystem

- Effective range is minimum 1500 meters.

- Directional antenna is designated to threats automatically with respect to threat information supplied from radar subsystem.

In addition to these specifications, there are some assumptions are made to create coverage parameters for threat generator program. These assumptions are as follows;

- The rotation time of the directional antenna for designation is ignored (instant designation).
- The directional antenna can turn in 5° increments.
- Jamming occurs instantly, i.e. when a threat resides in the jamming beam of the RF counter measure subsystem, threat becomes unfunctional and neutralized instantly and cannot be controlled again.
- The RF counter measure subsystem that has directional antenna can neutralize all of the threats which are in the azimuth range of the antenna beam. Height information of threats is ignored in the creation of the coverage process.

By using these specifications and assumptions, the threat generator program generates the parameters of the threats that can be covered by the counter measure subsystem for the operation of mathematical model.

3.2.3 Radar Related Parameters

In this part of the chapter, parameters with respect to radar specifications are explained and they are used for running of the mathematical model. Before the parameter generation process begins, threats are generated taking into account the abilities of radar subsystem, then parameters are generated by using the threat information to use in the mathematical model. Threat information are not only used in radar related parameter generation, but also used in RF counter measure subsystem related parameter generation process which will be explained in the following parts.

The threat generator program generates threats in accordance with radar capabilities and within the boundaries which are defined in the user interface part, before computing the parameters to be used in the mathematical model. When the numerical information of threat is defined, random values are assigned by the threat generator program in accordance with predetermined limits and each threat receives a specific ID number unique to itself. The numerical specifications of the threats are explained in the below;

Coordinate Information: The threat generator program produces random initial coordinate data for threats on the two-dimensional plane from outside the protected area where bounded by the limits defined at the interface part of the threat generator program. In real life sample, threats are not expected inside of the defended area. The midpoint of the protected area is assumed as center of the plane and threats coordinate data in X and Y axes are generated taking that center point as reference. The threat generator program does not initiate a threat more than 1500 meters away from any radar subsystem, because radar's detection range is up to 1500 meters. Calculation of distance between threat and any radar will be showed in following part of threat information.

Direction and Speed Information: The threat generator program assigns a random velocity to each threat created that have velocity components in the X and Y axes. Once a velocity is assigned to a threat it remains constant during the threat generating process. After a random velocity assigned to a threat, program calculates the speed. The speed is calculated as below;

$$S_{M,T_m} = \sqrt{S_{x,T_m}^2 + S_{y,T_m}^2}$$

where,

S_{M,T_m} = Speed of threat "m",

S_{x,T_m} = Speed value of threat "m" in X axis,

S_{y,T_m} = Speed value of threat "m" in Y axis.

Range Information: The distance between each threat and each integrated system which include radar and jammer subsystems, is calculated by the following formula. In addition to that, distance between each threat and center point of the protected area is calculated by the following formula:

$$D_{T_m,\, I_n} = \sqrt{(X_{T_m} - X_{I_n})^{\,2} + (Y_{T_m} - Y_{I_n})^{\,2}}$$

where,

$D_{T_m,\, I_n}$ = Distance between threat “m” and integrated system “n”,

X_{T_m} = Coordinate data of threat “m” in X axis,

X_{I_n} = Coordinate data of integrated system “n” in X axis, which is determined by user,

Y_{T_m} = Coordinate data of threat “m” in Y axis,

Y_{I_n} = Coordinate data of integrated system “n” in Y axis, which is determined by user.

Explanation of X_{T_m}, X_{I_n}, $Y_{T_m}$and Y_{I_n} will not given in the following formulas.

To calculate the distance between threats and center point of the protected area, X and Y axes coordinate information of center point, which are “0” for each axes, are used.

Angle Information: Angle between each threat and integrated system is calculated by using the following formula. This angle information is used for generating jammer coverage matrix which will be explained in RF counter measure subsystem related parameters part.

$$\beta_{T_m,\, I_n} = \tan^{-1}\frac{(Y_{T_m} - Y_{I_n})}{(X_{T_m} - X_{I_n})}$$

β_{T_m, I_n} = Angle between threat “m” and integrated system “n”, can take values between -180 and +180 degrees.

However, $\tan^{-1}$ formula gives results between -180 and +180 degrees. This calculation may cause confusion while computing the angle between the threat and integrated system. Therefore, the threat generator program uses a mathematical logic that gives the angle value 0 and 360 degrees. This logic is given below;

θ_{T_m, I_n} = Angle between threat “m” and integrated system “n”, between 0° and $+360^{\circ}$

- If $(Y_{T_m} - Y_{I_n})$ and $(X_{T_m} - X_{I_n})$ have positive signs;
  $\theta_{T_m, I_n} = \beta_{T_m, I_n}$
- If $(Y_{T_m} - Y_{I_n})$ has positive and $(X_{T_m} - X_{I_n})$ has negative signs;
  $\theta_{T_m, I_n} = \beta_{T_m, I_n} + 180^{\circ}$
- If $(Y_{T_m} - Y_{I_n})$ and $(X_{T_m} - X_{I_n})$ have negative signs;
  $\theta_{T_m, I_n} = \beta_{T_m, I_n} + 180^{\circ}$
- If $(Y_{T_m} - Y_{I_n})$ has negative and $(X_{T_m} - X_{I_n})$ has positive signs;
  $\theta_{T_m, I_n} = \beta_{T_m, I_n} + 360^{\circ}$

By using this mathematical algorithm, angles between each threat and each integrated system are calculated between 0 and +360 degrees and these data are used in generating coverage matrix for each RF counter measure subsystem.

3.2.4. Threat Evaluation

After threats are generated, threat generator program starts to evaluate the priority for threats by using speed, direction and location information of threats. During the threat evaluation process, the priorities of the threats are dealt with two different evaluation approaches. Primarily, the weights for threats are calculated for each approach, and then the calculated weights for each threat are multiplied with the coefficients which are determined by the user. Finally, for each approach, the multiplied threat weights are summed for each threat and threat importance values are calculated. In the following part of this section, two different threat evaluation approaches will be explained in detail.

3.2.4.1. Threat Evaluation Based on Arrival Time

In this approach, arrival times of threats to the protected area are calculated by using the speed and direction information of threats. For the calculation of arrival time, it is assumed that the threats will follow a constant trajectory with their initial speeds and directions.

After these arrival times are calculated, the weight values of the threats are determined by the threat generator program. It is assumed that if the threats cannot enter the protected area at the specified time interval (1 – 300seconds), the weight values of these threats become 0 and if the threats will enter the protected area in 1 second, their weight values become 1. The weight values of other threats are computed between 0 and 1, which is inversely proportional to their arrival times.

The arrival times of the threats are calculated by following formula;

$$(1) \quad X_{LB} \leq X_{T_m} + (V_{x,T_m} \times t_{T_m}) \leq X_{RB}$$

$$(2) \quad Y_{DB} \leq Y_{T_m} + (V_{y,T_m} \times t_{T_m}) \leq Y_{UB}$$

X_{LB} = Left border coordinate of protected area in X axis,

X_{RB} = Right border coordinate of protected area in X axis,

Y_{DB} = Down border coordinate of protected area in Y axis,

Y_{UB} = Upper border coordinate of protected area in Y axis.

This coordinate information of protected area is defined by the user.

V_{x,T_m} = Velocity of threat “m” in X axis (Includes speed value and direction),

V_{y,T_m} = Velocity of threat “m” in Y axis (Includes speed value and direction),

t_{T_m} = Arrival time of threat “m” to the center of the protected area.

The threat generator program calculates the arrival time of threat by assigning real numbers to t_{T_m}variable in inequalities (1) and (2) beginning from 0 and ending at 300. Inequalities (1) and (2) are checked for each value of t_{T_m} and first value to suffice these two inequalities at the same time becomes the arrival time of the threat.

If an arrival time cannot be found according to the above calculations, arrival times of those threats are assumed “0” and their arrival time based weight values are determined as “0” in the weight value calculation process.

The time based weight values of the threats are calculated by following formula;

$$w_{t,\,T_m} = \frac{t_{max} - t_{T_m}}{t_{max} - t_{min}}$$

$w_{t,\,T_m}$ = The time based weight value of threat “m”,

t_{max} = The maximum arrival time that is assumed 300 seconds,

t_{min} = The minimum arrival time that is assumed 1 second.

After the calculation of the time based weight values of the threats, these values multiplied with the time coefficient value which is defined by user and used in the calculation of the total weights of the threats.

3.2.4.2. Threat Evaluation Based on Range

In this approach, the priority order of the threats is evaluated by considering the distance between threats and the boundaries of the protected area. For the distance based threat evaluation, it is considered that threats are able to maneuver instantaneously and they have the ability to move toward the protected area at maximum speed by suddenly changing their directions.

Therefore, considering that the radar can update the track data of threats in 4 seconds, an evaluation should be made considering the possibility that the threats can enter the protected area from the nearest point according to their location as well as evaluating them with their instant direction and speed information.

When this approach is used, the threats are prioritized by calculating shortest distances between the threats and protected area instead of using their arrival times to the place, because the maximum speeds of the drone threats are limited (20m/sec) and distance information is sufficient to make threat evaluation.

In the calculation process of weight values based on the threat distance, firstly the shortest distance between threats and the protected area is calculated. When calculating the shortest distance of the threats, the coordinate plane is divided into 8 different regions with respect to coordinate information of the protected area, and different distance formulations are used for the threats in each region.

The divided coordinate plane, which is shown in Figure - 5, and formulations are explained in the below;

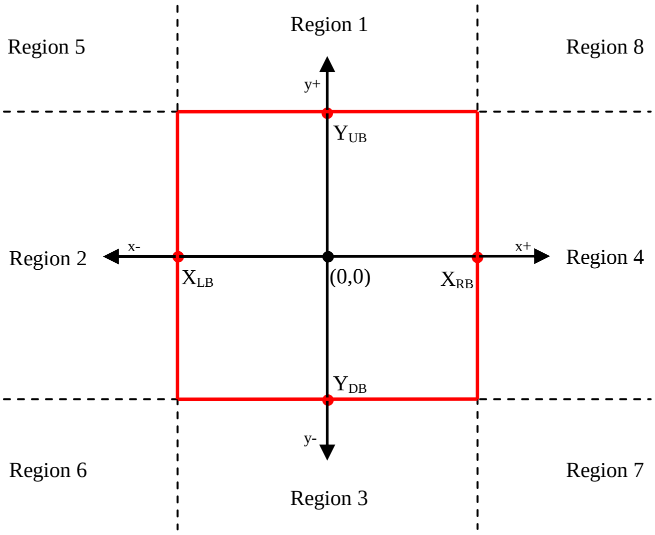


Figure 5 – Divided Coordinate Plane

For threats in the 1st, 2nd, 3rd, and 4th regions, the shortest distances are determined by calculating their vertical distances to the protected area. The Calculations are as follows;

d_{T_m} = The shortest distance between the threat "m" and the protected area.

- If $X_{T_m} \leq X_{LB}$ and $Y_{DB} \leq Y_{T_m} \leq Y_{UB}$ (It means that threat is in the 1st region);
  $d_{T_m} = X_{LB} - X_{T_m}$,
- If $Y_{T_m} \leq Y_{DB}$ and $X_{LB} \leq X_{T_m} \leq X_{RB}$ (It means that threat is in the 2nd region);
  $d_{T_m} = Y_{DB} - Y_{T_m}$,
- If $X_{RB} \leq X_{T_m}$and $Y_{DB} \leq Y_{T_m} \leq Y_{UB}$ (It means that threat is in the 3rd region);
  $d_{T_m} = X_{T_m} - X_{RB}$,
- If $Y_{UB} \leq Y_{T_m}$ and $X_{LB} \leq X_{T_m} \leq X_{RB}$ (It means that threat is in the 4th region);
  $d_{T_m} = Y_{T_m} - Y_{UB}$.

For threats in the 5th, 6th, 7th, and 8th regions, the shortest distances are determined by calculating the distance between the nearest corner point of the protected area according to the threat and threat's location. The calculations are as follows;

- If $X_{T_m} \leq X_{LB}$ and $Y_{UB} \leq Y_{T_m}$ (It means that threat is in the 5th region);
  $d_{T_m} = \sqrt{(X_{LB} - X_{T_m})^2 + (Y_{T_m} - Y_{UB})^2}$,
- If $X_{T_m} \leq X_{LB}$ and $Y_{T_m} \leq Y_{DB}$ (It means that threat is in the 6th region);
  $d_{T_m} = \sqrt{(X_{LB} - X_{T_m})^2 + (Y_{DB} - Y_{T_m})^2}$,
- If $X_{LB} \leq X_{T_m}$ and $Y_{T_m} \leq Y_{DB}$ (It means that threat is in the 7th region);
  $d_{T_m} = \sqrt{(X_{T_m} - X_{LB})^2 + (Y_{DB} - Y_{T_m})^2}$,
- If $X_{LB} \leq X_{T_m}$ and $Y_{UB} \leq Y_{T_m}$ (It means that threat is in the 8th region);
  $d_{T_m} = \sqrt{(X_{T_m} - X_{LB})^2 + (Y_{T_m} - Y_{UB})^2}$.

After the calculations of the shortest distances between the threats and the protected area, weight values based on threat distance are calculated with following formula;

$$w_{d,\,T_m} = \frac{d_{max} - d_{T_m}}{d_{max} - \ d_{min}}$$

$d_{t,\,T_m}$ = The distance based weight value of threat “m”,

d_{max} = The maximum distance between the threat “m” and the protected area which is 1500 meters according to the maximum tracking range of the radar,

d_{min} = The minimum distance between the threat “m” and the protected area which is 100 meters according to the blind range of the radar.

In order to calculate the total priority weights of the threats, the distance based weight value is multiplied with the distance coefficient value which is determined by user and summed with the time based weight value which is multiplied with time coefficient value.

The formulation of the total priority weights of the threats is given in the below;

$$w_{T_m} = (\alpha_d \times w_{d,\,T_m}) + (\alpha_t \times w_{t,\,T_m})$$

$$s.t. \quad \alpha_d + \alpha_t = 1$$

w_{T_m}= The total weight value of the threat “m”,

α_d = The distance coefficient of the threat evaluation calculation,

α_t = The time coefficient of the threat evaluation calculation.

These calculated total weight values of the threats are used as parameter in the mathematical model.

3.1.5. RF Counter Measure Subsystem Related Parameters

In this part of the chapter, one parameter is explained which is created with respect to the RF counter measure subsystem specifications and it is used to run the mathematical model. For the generate this parameter, jamming coverage (transmit pattern of antenna) is used, as shown in Figure - 3, and a coverage matrix is created to show that which jammer antenna can cover which threats at what angle, when the jamming process is started.

This coverage matrix is created with binary numbers, 0 and 1, and gives information about the jammer antennas that can cover any threat at any angle. A basic coverage matrix table is shown in Table-1, which consists of 2 jammer and 3 threats for 900 meters x 900 meters protected area, in order to explain it in detailed. The information about jammers and threats are given in the Appendix – A.

Table 1 – Coverage Matrix with 2 Jammer and 3 Threats

a_{nkm}	Jammer 1			Jammer 2		
	T1	T2	T3	T1	T2	T3
5	0	0	0	0	0	0
10	0	0	0	0	0	0
15	0	0	0	0	0	0
20	0	0	0	0	0	0
25	0	0	0	0	0	0
30	0	0	0	0	0	0
35	0	0	0	0	0	0
40	0	0	0	0	0	0
45	0	0	0	0	0	0
50	0	0	0	1	0	0
55	0	0	0	1	0	1
60	0	0	0	1	0	1
65	0	0	0	1	0	1
70	0	0	0	1	0	1
75	0	0	0	1	0	1
80	0	0	0	1	0	1
85	0	0	0	1	0	1
90	0	0	0	1	0	1
95	0	0	0	1	0	1
100	0	0	0	1	0	1
105	0	0	0	1	0	1
110	0	0	0	0	0	1
115	0	0	0	0	0	0
120	0	0	0	0	0	0
125	0	0	0	0	0	0
130	0	0	0	0	0	0
135	0	0	0	0	0	0
140	0	0	0	0	0	0
145	0	0	0	0	0	0
150	0	0	0	0	0	0
155	0	0	0	0	0	0
160	0	0	0	0	0	0
165	0	0	0	0	0	0
170	0	0	0	0	0	0
175	0	0	0	0	0	0
180	0	0	0	0	0	0

a_{nkm}	Jammer 1			Jammer 2		
	T1	T2	T3	T1	T2	T3
185	0	0	0	0	0	0
190	0	0	0	0	0	0
195	0	0	0	0	0	0
200	0	0	0	0	0	0
205	0	0	0	0	0	0
210	0	0	0	0	0	0
215	0	0	0	0	0	0
220	0	0	0	0	0	0
225	0	0	0	0	0	0
230	0	1	0	0	0	0
235	0	1	0	0	0	0
240	0	1	0	0	0	0
245	0	1	0	0	0	0
250	0	1	0	0	0	0
255	0	1	0	0	0	0
260	0	1	0	0	0	0
265	0	1	0	0	0	0
270	0	1	0	0	0	0
275	0	1	0	0	0	0
280	0	1	0	0	0	0
285	0	1	0	0	0	0
290	0	0	0	0	0	0
295	0	0	0	0	0	0
300	0	0	0	0	0	0
305	0	0	0	0	0	0
310	0	0	0	0	0	0
315	0	0	0	0	0	0
320	0	0	0	0	0	0
325	0	0	0	0	0	0
330	0	0	0	0	0	0
335	0	0	0	0	0	0
340	0	0	0	0	0	0
345	0	0	0	0	0	0
350	0	0	0	0	0	0
355	0	0	0	0	0	0
360	0	0	0	0	0	0

- The first column of the matrix shows the jammer antenna's stopping angles, which are determined with respect to rotation characteristics of antenna.
- The upper row of the matrix shows the number of used jammers.
- The second row of the matrix shows the number of threats.
- The inside of the matrix is populated with following algorithm;

$$a_{nkm} = \begin{cases} 1 \ if \quad (\theta_{T_m, I_n} - 30^{\circ}) \leq \ \theta_{J_n} \leq \ (\theta_{T_m, I_n} + 30^{\circ}) \ and \ D_{T_m, I_n} \leq 1500 \\ 0 \ else \end{cases}$$

a_{nkm} = The binary coverage value of jammer "n" at angle "k" for threat "m".

θ_{J_n} = The stopping angle for jammer "n".

θ_{T_m, I_n} = The angle between threat "m" and integrated system "n".

D_{T_m, I_n} = Distance between threat "m" and integrated system "n".

The values of the coverage matrix are used in the mathematical model and this matrix gives information about the coverage relationship between each jammer and each threat at any stopping angle of each antenna.

The summary about the coverage matrix based on the above example table is as follows;

- Jammer 1 can cover the Threat 2, if its' antenna takes position at any of these angles; 230°, 235°, 240°, 245°, 250°, 255°, 260°, 265°, 270°, 275°, 280° or 285°.
- Jammer 2 can cover the Threat 1, if its' antenna takes position at any of these angles; 50°, 55°, 60°, 65°, 70°, 75°, 80°, 85°, 90°, 95°, 100° or 105°.
- Jammer 2 can cover the Threat 3, if its' antenna takes position at any of these angles; 55°, 60°, 65°, 70°, 75°, 80°, 85°, 90°, 95°, 100°,105° or 110°.

3.3. Heuristic Approach

The mathematical optimization model of the problem is explained in the part of this chapter. This model is solved by using IBM Cplex Studio program, which works with the Java sub-routine, to provide a faster solution to be used on defense system that utilizes Java infrastructure. This situation requires the user to obtain a license for the IBM Cplex Studio program in order to solve the mathematical model.

Therefore, an alternative heuristic solution approach has been developed for user to solve the problem without the need for purchasing any licensed algebraic modeling language. Furthermore, while the heuristic approach is being developed, it is predicted that it will give faster solution in comparison to the mathematical model explained in previous chapter. The data about the solution times for the mathematical model and the heuristic approach will be shown in the Experimental Results chapter.

Although the IBM Cplex Studio program can solve mathematical model fast enough, the heuristic solution approach that provides a faster solution will be an advantage since a new problem needs to be solved in every 4 seconds. However, the heuristic solution approach may not provide the optimal solution as mathematical model provides for any case. Instead faster solution shall be obtained without purchasing any program license. The solutions for heuristic approach and mathematical model for different scenarios will be analyzed in the Experimental Results chapter of the paper.

In the continuing part of this chapter, the construction of the heuristic solution approach will be explained in detail.

In the heuristic solution approach, the parameters about threats and jammers are used which are generated by threat generator program. In addition to these parameters, the following notations are used in the heuristic algorithm.

M : The number of created threats.

N : The number of jammers.

P : The set of created threats' indices. $P = \{1, 2, \dots, M\}$.

R : The set of jammers' indices. $R = \{1, 2, \dots, N\}$

G : The set of jammer angles $G = \{5, 10, \dots, 360\}$

CP : The set of covered threats' indices.

UR : The set of used jammers' indices.

k_{jg} : The sum of weight value of threats which are covered by jammer j at angle g.

$$k_{jg} = \sum_{i \in P} w_i \, a_{jgi} \quad \forall\, j \in R \; and \; g \in G$$

The flowchart of the heuristic solution approach is given in Figure – 6 and the steps of the heuristic approach are explained in the below.

Initialization: Set $CP = \emptyset$, $UR = \emptyset$ and $\text{Max}_{j \in N}\{k_{jg}\} = 0$.

Step 1: Calculate the k_{jg} values for all j ∈ R, g ∈ G and i ∈ P.

Step 2: Determine $\text{Max}_{j \in N}\{k_{jg}\} = k_{rp}$ for all g ∈ G and i ∈ P.

Step 3:

- Add used jammer indices to UR.
  $UR = UR \cup \{r\}$
- Add used jammer angle indices to UG.
  $UG = UG \cup \{p\}$

- Add covered threats' indices which create k_{rp}.

  $CP = CP \cup \{\text{covered threats'indices}\}$
- Remove UR from set of R and CP from set of P.

  $R = R/UR$ and $P = P/CP$.

Step 4: Check if $R = \emptyset$ or $P = \emptyset$, and if answer is "No", go back to Step 1. If answer is "Yes" go to Step 5.

Step 5: Calculate the total weight of covered threat values by summing determined maximum k_{jg} values.

$$Total\ weight\ value = \sum_{j \in UR} \sum_{g \in UG} k_{jg}$$

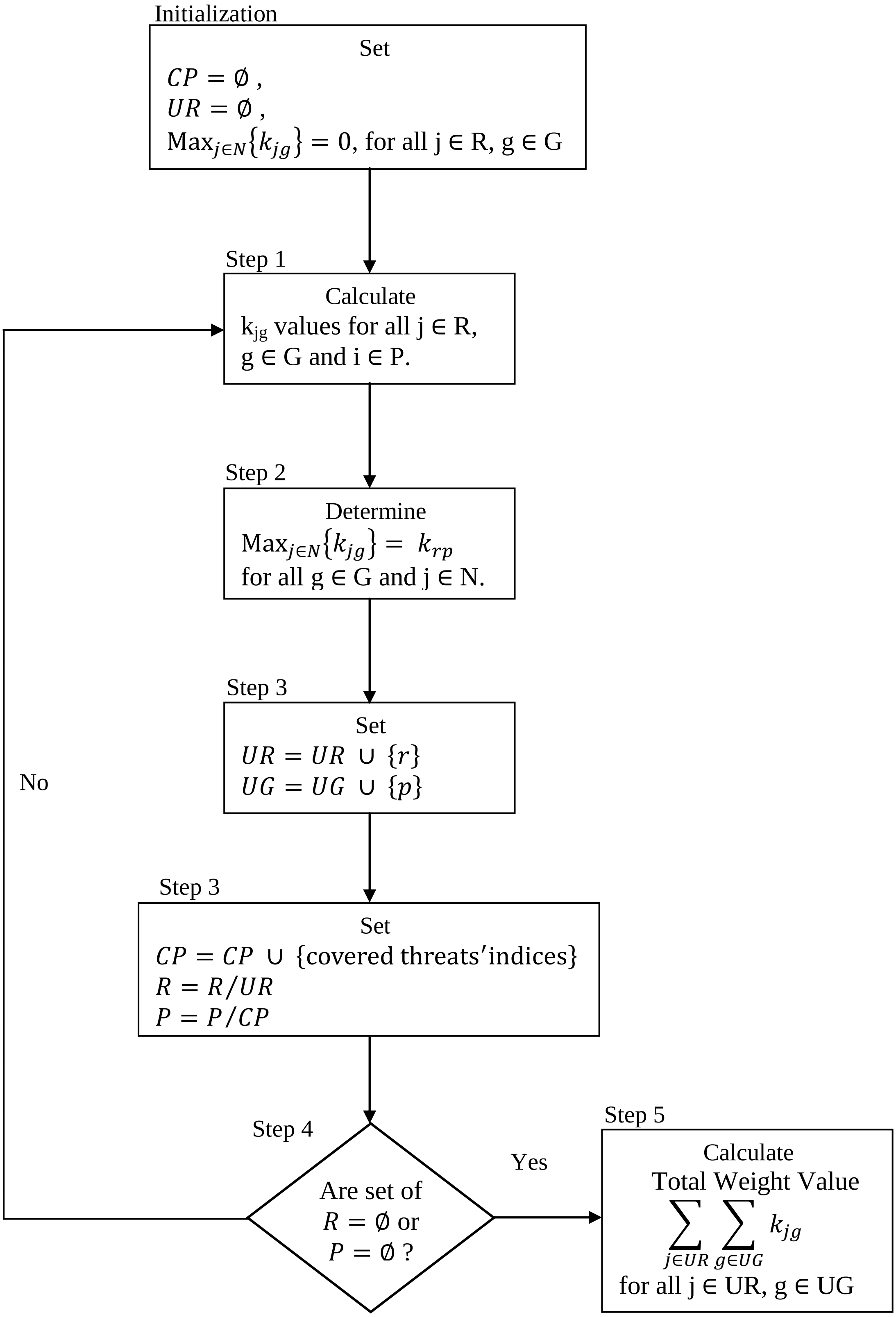


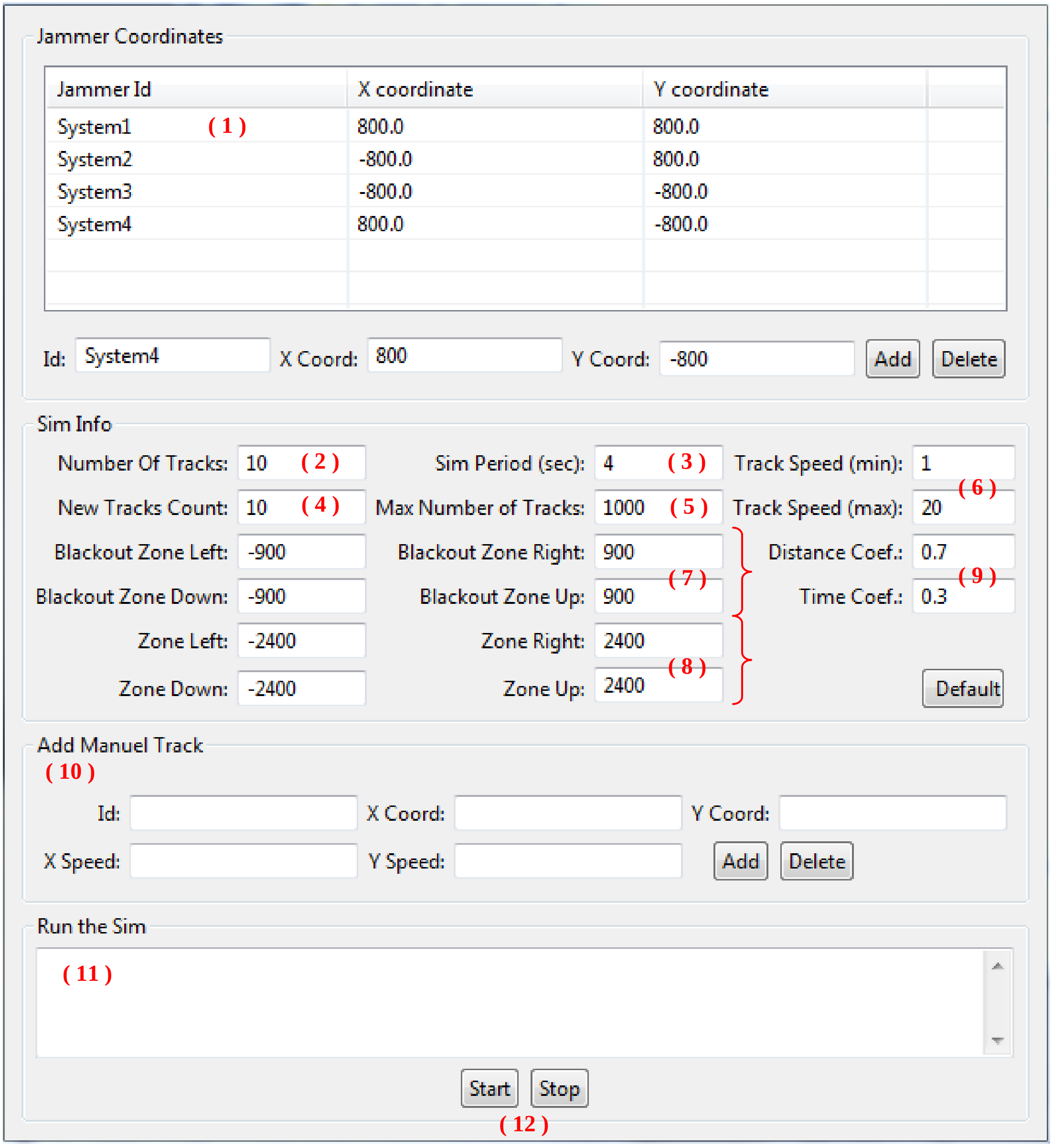
Figure 6 – Flow Chart of the Heuristic Approach

CHAPTER 4

EXPERIMENTAL RESULTS

In this chapter, computational experiments will be explained in detail for different scenarios. In each scenario, the problem is solved both by the mathematical model and by the heuristic approach and the results of both solutions are shown on the same table. Therefore, the differences between the two solution approaches can be seen for the same problem.

Before starting the experiments, coordinate information of the environment where the threats will be generated, location of integrated Anti-Drone defense system and desired protected area should be entered as inputs using the interface of the threat generator program. In addition to these coordinate information, maximum speed limit of the threats, threat generation period and the initial number of threats should be entered as input. After entering these data, the threat generator program is started and runs until stopped by user. Throughout the run, output data regarding neutralized threats and counter measure subsystems activated are presented during the each period which was entered on user interface. The interface of the threat generator program is given in Figure – 7.



Jammer Coordinates

Jammer Id	X coordinate	Y coordinate
System1	800.0	800.0
System2	-800.0	800.0
System3	-800.0	-800.0
System4	800.0	-800.0

Id: System4 X Coord: 800 Y Coord: -800

Sim Info

Number Of Tracks: 10

Sim Period (sec): 4

Track Speed (min): 1

New Tracks Count: 10

Max Number of Tracks: 1000

Track Speed (max): 20

Blackout Zone Left: -900

Blackout Zone Right: 900

Distance Coef.: 0.7

Blackout Zone Down: -900

Blackout Zone Up: 900

Time Coef.: 0.3

Zone Left: -2400

Zone Right: 2400

Zone Down: -2400

Zone Up: 2400

Add Manuel Track

Id: X Coord: Y Coord:

X Speed: Y Speed:

Run the Sim

Figure 7 – Interface of the Threat Generator Program

(1)⟶ 2-D Coordinate information of the location of integrated Anti-Drone system (meter)

(2)⟶ Initial number of threats

(3)⟶ New threat generation period (second). This data is entered with respect to radar's rotation rate information, i.e. revolutions per minute (rpm). Radars used in our problem rotate at 15 rpm and it means that a full rotation of radar (360 degrees) takes 4 seconds. Thus every 4 seconds, radar updates threat data.

(4)⟶ Maximum number of threats which are randomly added at each period

(5)⟶ Maximum number of threats that can be generated by threat generator program.

(6)⟶ Maximum and minimum speed limits of drone threats (meter/second). This data is entered with respect to the information of the drones commercially available on market.

(7)⟶ Coordinate information of protected area (meter)

(8)⟶ Coordinate information of created environment (meter)

(9)⟶ Coefficients of threat evaluation algorithm. These values are determined by user and can take values between 0 and 1.

(10)⟶ Manual threat information input fields (meter). These fields are used, when user wants to generate a specific drone threat, instead of random generation.

(11)⟶ Window showing generated threats during threat generating process.

After the entering the inputs, the threat generator program is started by clicking the start bottom (12) and when the user determines sufficient output is collected, program is stopped by clicking the stop button (12).

While the swarm attacks scenarios are being developed;

- The protection of the areas has been examined by deploying integrated systems in large and small areas.
- There are 1, 2, 3 and 4 integrated system are used in scenarios. In addition to these systems, one omni directional antenna jammer is placed to the protected area and it is activated if the integrated systems cannot provide the protection.

- If a threat is closer than 100 meters to the protected area and cannot be neutralized by the integrated system, the omni directional jammer is activated.
- Since the blind range of radars is 100 meters, each integrated system is located 100 meters inside from the border of the protected area.
- Each scenario is created by changing the integrated system number and area size is examined with group of 10, 30, 50 and 100 threat attacks which are from different distances.
- Each threat attack scenario is repeated 10 times and the results are obtained from the average data of these results.

In addition to this information, there are three assumptions for the scenarios. These assumptions are;

- The radar on the integrated system can detect all threats within its own detection range, which is 1500 meters.
- The jammer antenna on the integrated system can neutralize all threats within its own azimuth coverage range, which is 60° and shown in Figure – 4.
- The coordinates of the integrated systems do not represent the optimal deployment. The systems are emplaced by considering radars' detection ranges.

4.1. Protection with 1 Integrated System

In this experiment, only small area protection is examined by changing number of threats and threat ranges. Since it is not possible to protect a large area with one integrated system, because of radar detection range, large area protection scenarios have not been created.

In this scope, the small protected area is designed as 100 meters x 100 meters and the integrated system is located in the center of the area. The coordinate information of the system is (0, 0).

4.1.1 Close Threats

In this scenario, the distances between threats and protected area are randomly generated between 1 meter and 300 meters.

The experimental results of the scenario are shown in Table – 2.

4.1.2. Distant Threats

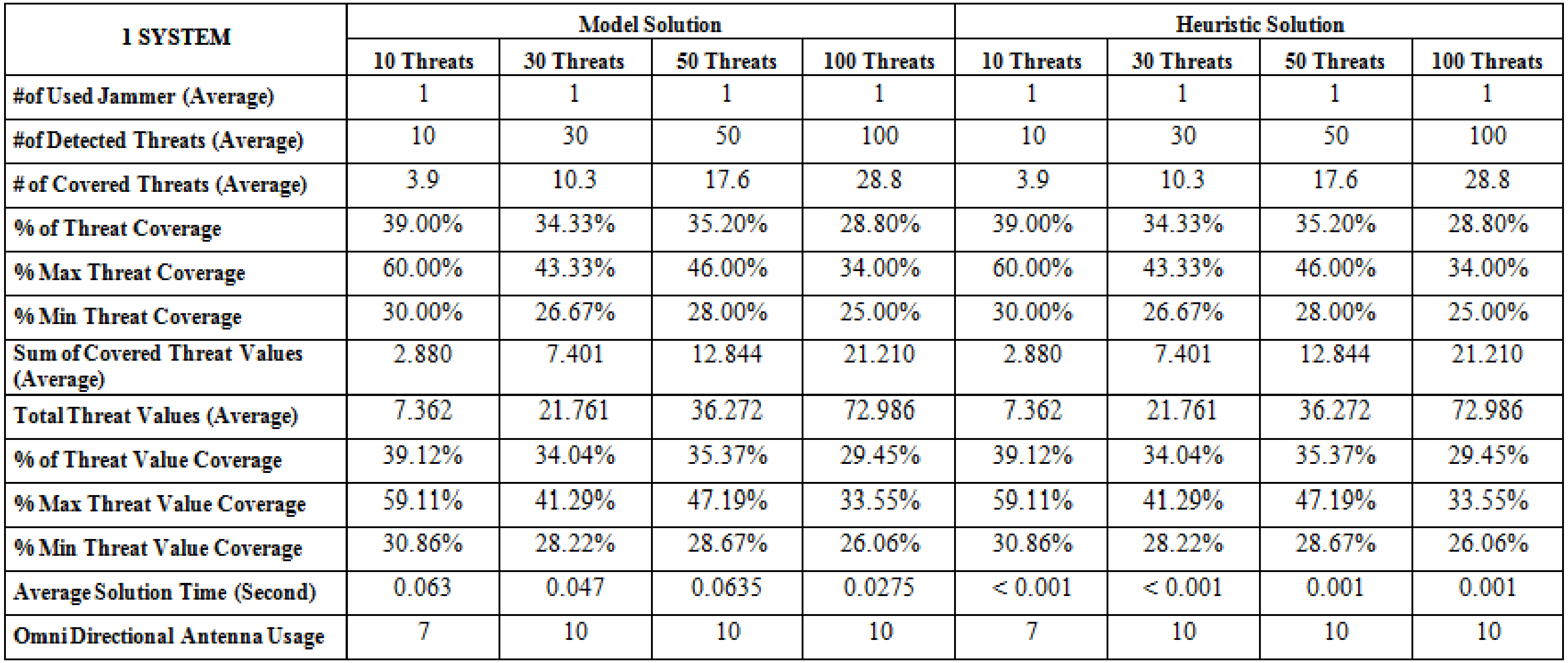
In this scenario, the distances between threats and protected area are randomly generated randomly between 1 meter and 1500 meters

The experimental results of the scenario are shown in Table – 3.

4.1.3. Result Evaluation

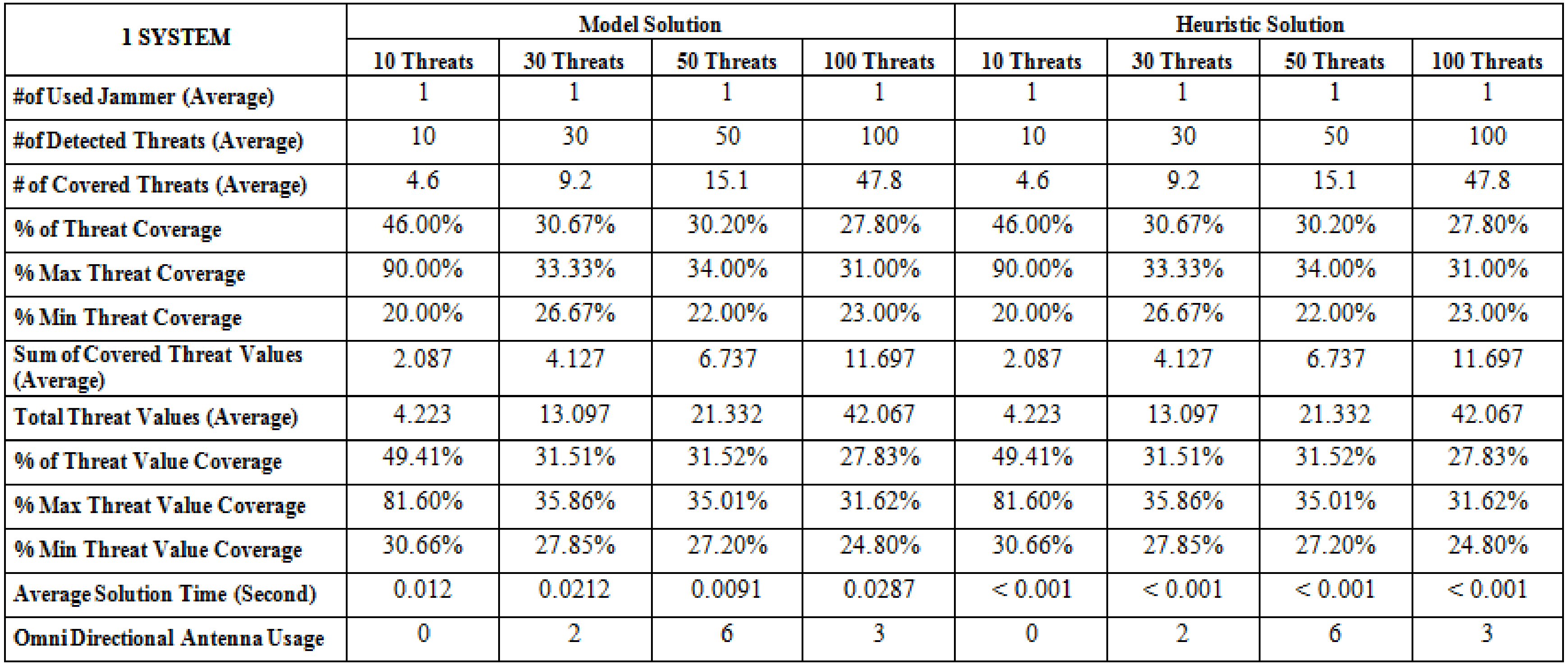
- When the tables are examined, it can be seen that the heuristic approach and the mathematical model gives the same solution, except solution time, for each scenario.
- Although mathematical model solved the cases in short times, heuristic approach gives the same results faster than mathematical model.
- In both cases, the most threats are neutralized in 10 threat group attacks and the least threats are neutralized in 100 threat group attacks.
- In the close threat scenario, the percentage of covered threat weight values are higher than the percentage of neutralized threat value, but in the distant threat scenario, these two ratios are close to each other.
- In both scenarios, the omni directional jammer has to be used to protect the area, but in close threat scenario, it is used for almost every attack.
- The omni directional jammer usage shows that, even if the protected area is small, the desired protection cannot be achieved with one integrated system, because directional antenna can only jam through a limited sector at a time.

Table 2 – Experimental Results for Protection a Small Area with 1 System (Close Threats)



1 SYSTEM	Model Solution				Heuristic Solution			
	10 Threats	30 Threats	50 Threats	100 Threats	10 Threats	30 Threats	50 Threats	100 Threats
#of Used Jammer (Average)	1	1	1	1	1	1	1	1
#of Detected Threats (Average)	10	30	50	100	10	30	50	100
# of Covered Threats (Average)	3.9	10.3	17.6	28.8	3.9	10.3	17.6	28.8
% of Threat Coverage	39.00%	34.33%	35.20%	28.80%	39.00%	34.33%	35.20%	28.80%
% Max Threat Coverage	60.00%	43.33%	46.00%	34.00%	60.00%	43.33%	46.00%	34.00%
% Min Threat Coverage	30.00%	26.67%	28.00%	25.00%	30.00%	26.67%	28.00%	25.00%
Sum of Covered Threat Values (Average)	2.880	7.401	12.844	21.210	2.880	7.401	12.844	21.210
Total Threat Values (Average)	7.362	21.761	36.272	72.986	7.362	21.761	36.272	72.986
% of Threat Value Coverage	39.12%	34.04%	35.37%	29.45%	39.12%	34.04%	35.37%	29.45%
% Max Threat Value Coverage	59.11%	41.29%	47.19%	33.55%	59.11%	41.29%	47.19%	33.55%
% Min Threat Value Coverage	30.86%	28.22%	28.67%	26.06%	30.86%	28.22%	28.67%	26.06%
Average Solution Time (Second)	0.063	0.047	0.0635	0.0275	< 0.001	< 0.001	0.001	0.001
Omni Directional Antenna Usage	7	10	10	10	7	10	10	10

Table 3 – Experimental Results for Protection a Small Area with 1 System (Distant Threats)



1 SYSTEM	Model Solution				Heuristic Solution			
	10 Threats	30 Threats	50 Threats	100 Threats	10 Threats	30 Threats	50 Threats	100 Threats
#of Used Jammer (Average)	1	1	1	1	1	1	1	1
#of Detected Threats (Average)	10	30	50	100	10	30	50	100
# of Covered Threats (Average)	4.6	9.2	15.1	47.8	4.6	9.2	15.1	47.8
% of Threat Coverage	46.00%	30.67%	30.20%	27.80%	46.00%	30.67%	30.20%	27.80%
% Max Threat Coverage	90.00%	33.33%	34.00%	31.00%	90.00%	33.33%	34.00%	31.00%
% Min Threat Coverage	20.00%	26.67%	22.00%	23.00%	20.00%	26.67%	22.00%	23.00%
Sum of Covered Threat Values (Average)	2.087	4.127	6.737	11.697	2.087	4.127	6.737	11.697
Total Threat Values (Average)	4.223	13.097	21.332	42.067	4.223	13.097	21.332	42.067
% of Threat Value Coverage	49.41%	31.51%	31.52%	27.83%	49.41%	31.51%	31.52%	27.83%
% Max Threat Value Coverage	81.60%	35.86%	35.01%	31.62%	81.60%	35.86%	35.01%	31.62%
% Min Threat Value Coverage	30.66%	27.85%	27.20%	24.80%	30.66%	27.85%	27.20%	24.80%
Average Solution Time (Second)	0.012	0.0212	0.0091	0.0287	< 0.001	< 0.001	< 0.001	< 0.001
Omni Directional Antenna Usage	0	2	6	3	0	2	6	3

4.2. Protection with 2 Integrated Systems

In this experiment, small and large area protection is examined by changing number of threats and threats distances.

4.2.1. Protection of Small Area

The small protected area is defined as 200 meters x 200 meters and the integrated system is located on the two corners of the area. The coordinates of the systems are: S1 (-100, 100) and S2 (100,-100).

4.2.1.1. Close Threats

In this scenario, the distances between threats and protected area are randomly generated between 1 meter and 300 meters.

The experimental results of the scenario are shown in Table – 4.

4.2.1.2. Distant Threats

In this scenario, the distances between threats and protected area are randomly generated between 1 meter and 1500 meters.

The experimental results of the scenario are shown in Table – 5.

4.2.2. Protection of Large Area

The large protected area is defined as 900 meters x 900 meters and the integrated system is located on the two corners of the area. The coordinates of the systems are: S1 (-800, 800) and S2 (800,-800).

4.2.2.1 Close Threats

In this scenario, the distances between threats and protected area are randomly generated between 1 meter and 300 meters.

The experimental results of the scenario are shown in Table – 6.

4.2.2.2. Distant Threats

In this scenario, the distances between threats and protected area are randomly generated between 1 meter and 1500 meters.

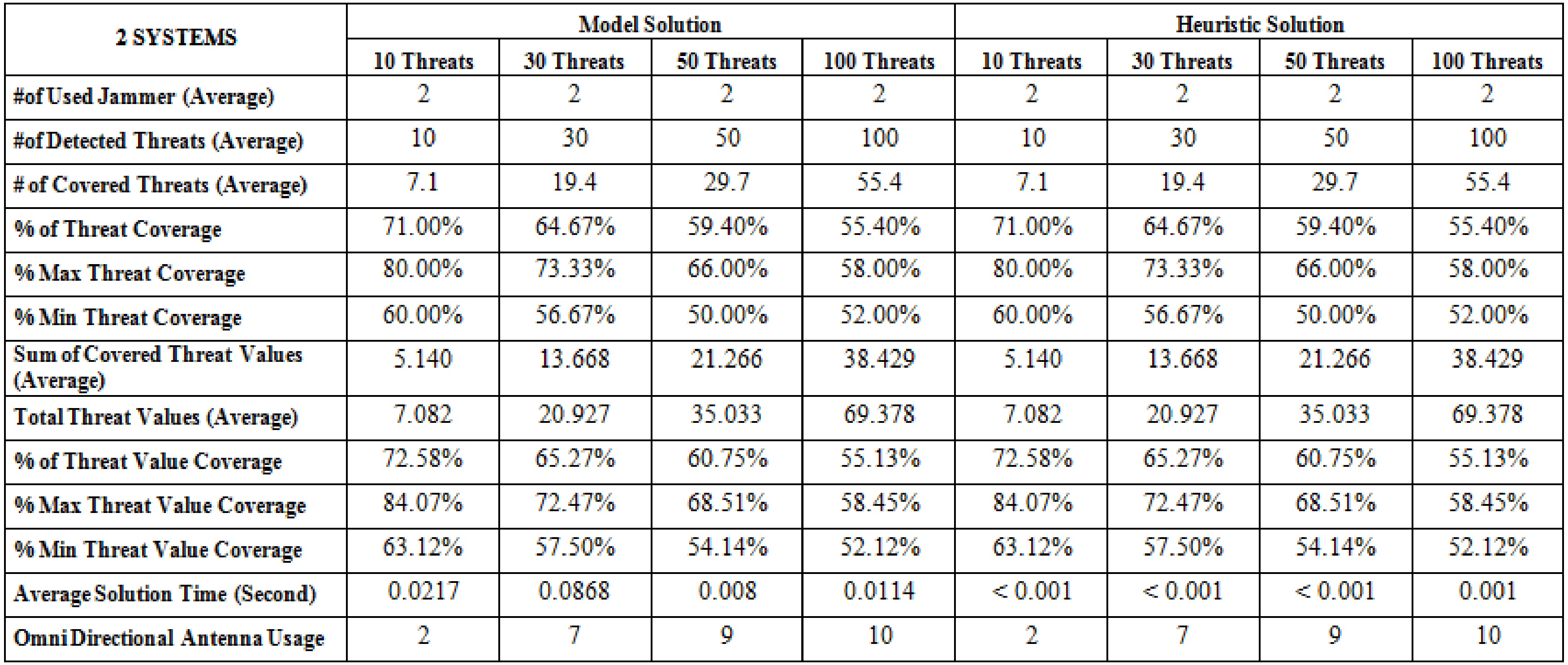
The experimental results of the scenario are shown in Table – 7.

4.2.3 Result Evaluation

- When the tables are examined, it can be seen that the heuristic approach and the mathematical model gives the same solution output, except solution time, for each scenario.
- Both mathematical model and heuristic approach solved the cases in short times but heuristic approach's solution time is less than mathematical model.
- In the small area protection scenarios, it has been observed that systems can detect all threats and threat and threat weight value coverage rates decreases when the number of threat increases.
- In the large area protection scenarios, it has been observed that systems cannot detect all threats, because radar range is not enough for whole detection. Detection rate of the systems can be shown in the 4th row of the Table – 6 and Table – 7.
- Therefore, a low coverage ratio is seen when the total threat neutralization is observed. However, if the detected threats are considered during the calculating the coverage ratio, increment of this rate will be seen in the 7th row of the Table – 6 and Table – 7.
- In the small area protection scenarios, omni directional jammer was activated for almost all close threat attack cases, because when all threats attack from close distances, directional antenna coverage is not enough for protection. In addition to close attack case, omni directional jammer is also activated in distant attack cases, but the usage of this jammer decreased. In this case, since the threats were generated in distant and close distances, the system can cover the close threats with one direction.

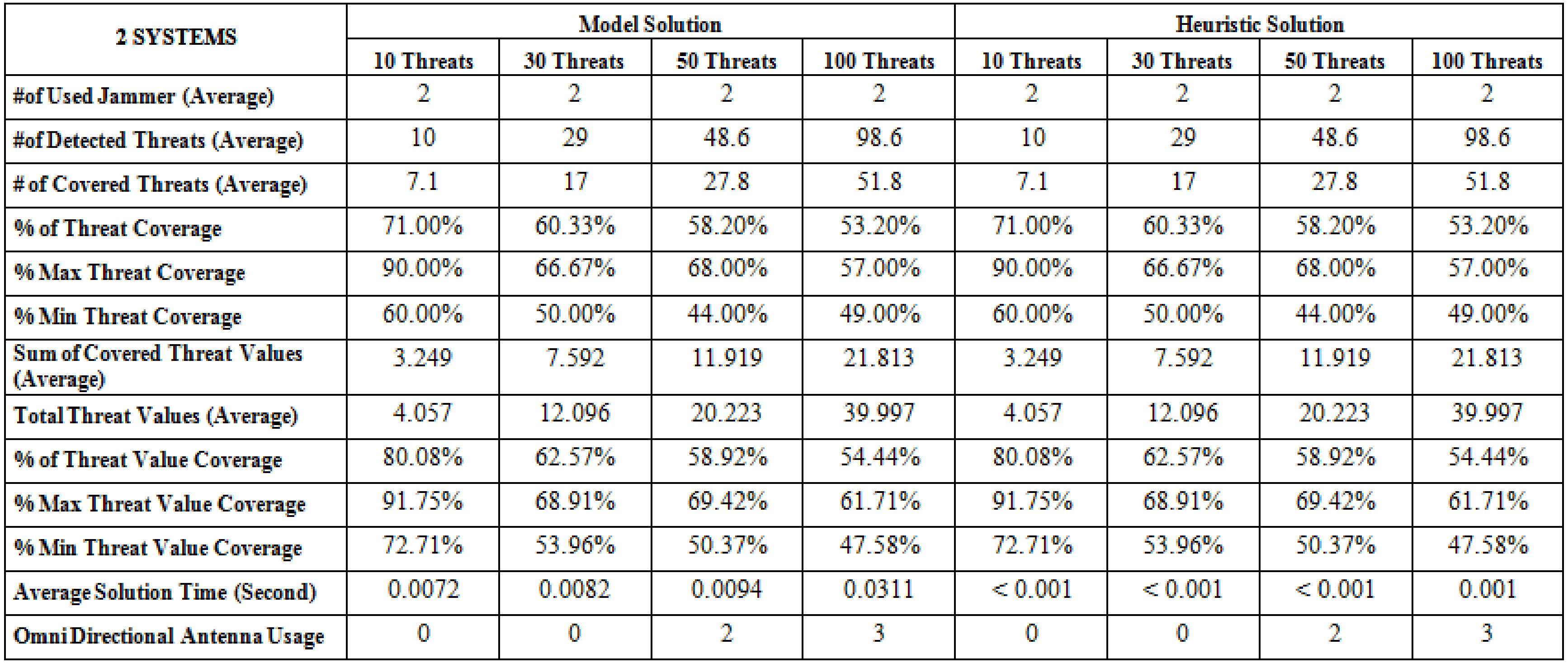
- In the small area protection scenarios, omni directional jammer was not activated for both close and distant attack cases, because the activation information of the omni directional jammer can only be given, if the system can detect any threat which is closer than 100 meters to the protected area. In both cases, system could neutralize the close threats among the detected attacks, but there may be threats that are not detected by system and close to protected area less than 100 meters. In this situation, omni directional jammer cannot be activated.

Table 4 – Experimental Results for Protection a Small Area with 2 Systems (Close Threats)



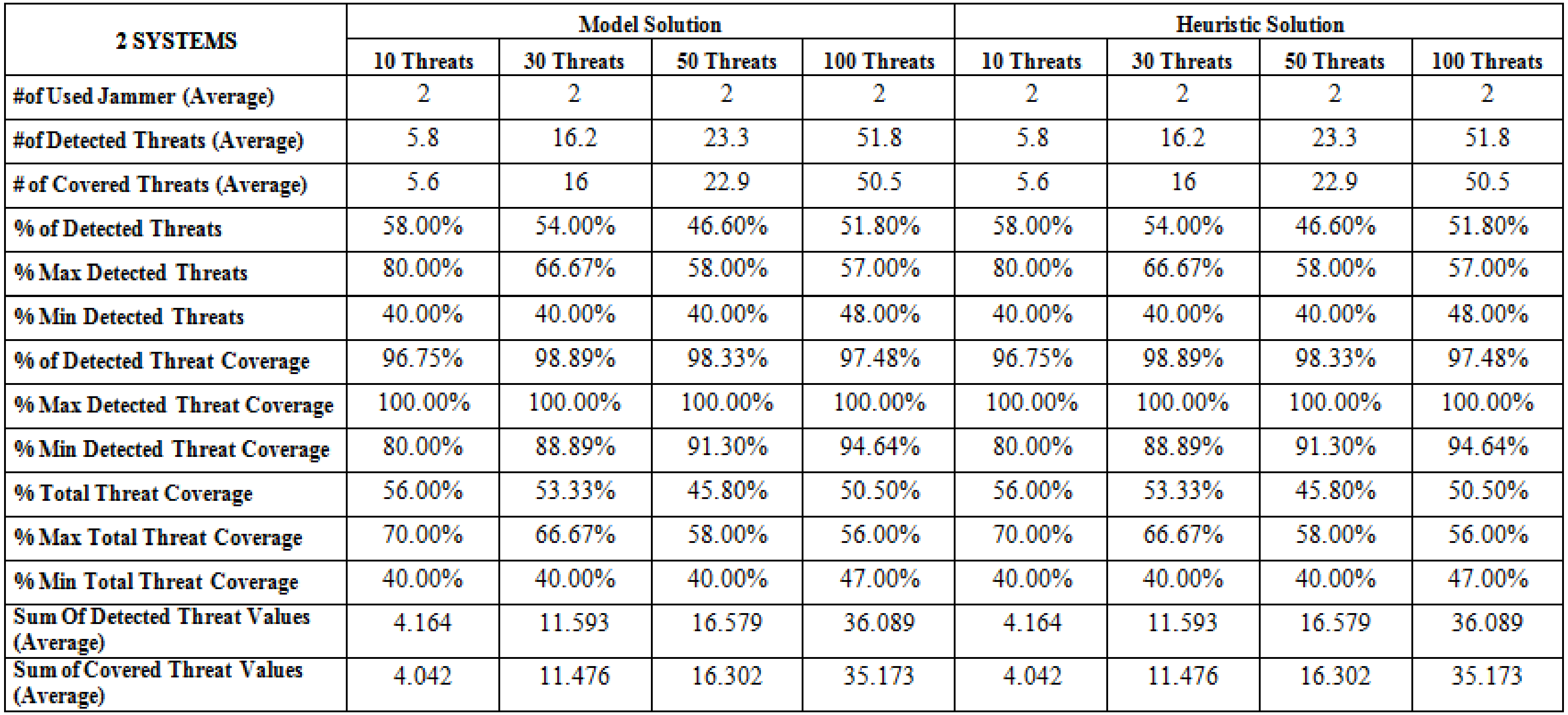
2 SYSTEMS	Model Solution				Heuristic Solution			
	10 Threats	30 Threats	50 Threats	100 Threats	10 Threats	30 Threats	50 Threats	100 Threats
#of Used Jammer (Average)	2	2	2	2	2	2	2	2
#of Detected Threats (Average)	10	30	50	100	10	30	50	100
# of Covered Threats (Average)	7.1	19.4	29.7	55.4	7.1	19.4	29.7	55.4
% of Threat Coverage	71.00%	64.67%	59.40%	55.40%	71.00%	64.67%	59.40%	55.40%
% Max Threat Coverage	80.00%	73.33%	66.00%	58.00%	80.00%	73.33%	66.00%	58.00%
% Min Threat Coverage	60.00%	56.67%	50.00%	52.00%	60.00%	56.67%	50.00%	52.00%
Sum of Covered Threat Values (Average)	5.140	13.668	21.266	38.429	5.140	13.668	21.266	38.429
Total Threat Values (Average)	7.082	20.927	35.033	69.378	7.082	20.927	35.033	69.378
% of Threat Value Coverage	72.58%	65.27%	60.75%	55.13%	72.58%	65.27%	60.75%	55.13%
% Max Threat Value Coverage	84.07%	72.47%	68.51%	58.45%	84.07%	72.47%	68.51%	58.45%
% Min Threat Value Coverage	63.12%	57.50%	54.14%	52.12%	63.12%	57.50%	54.14%	52.12%
Average Solution Time (Second)	0.0217	0.0868	0.008	0.0114	< 0.001	< 0.001	< 0.001	0.001
Omni Directional Antenna Usage	2	7	9	10	2	7	9	10

Table 5 – Experimental Results for Protection a Small Area with 2 Systems (Distant Threats)



2 SYSTEMS	Model Solution				Heuristic Solution			
	10 Threats	30 Threats	50 Threats	100 Threats	10 Threats	30 Threats	50 Threats	100 Threats
#of Used Jammer (Average)	2	2	2	2	2	2	2	2
#of Detected Threats (Average)	10	29	48.6	98.6	10	29	48.6	98.6
# of Covered Threats (Average)	7.1	17	27.8	51.8	7.1	17	27.8	51.8
% of Threat Coverage	71.00%	60.33%	58.20%	53.20%	71.00%	60.33%	58.20%	53.20%
% Max Threat Coverage	90.00%	66.67%	68.00%	57.00%	90.00%	66.67%	68.00%	57.00%
% Min Threat Coverage	60.00%	50.00%	44.00%	49.00%	60.00%	50.00%	44.00%	49.00%
Sum of Covered Threat Values (Average)	3.249	7.592	11.919	21.813	3.249	7.592	11.919	21.813
Total Threat Values (Average)	4.057	12.096	20.223	39.997	4.057	12.096	20.223	39.997
% of Threat Value Coverage	80.08%	62.57%	58.92%	54.44%	80.08%	62.57%	58.92%	54.44%
% Max Threat Value Coverage	91.75%	68.91%	69.42%	61.71%	91.75%	68.91%	69.42%	61.71%
% Min Threat Value Coverage	72.71%	53.96%	50.37%	47.58%	72.71%	53.96%	50.37%	47.58%
Average Solution Time (Second)	0.0072	0.0082	0.0094	0.0311	< 0.001	< 0.001	< 0.001	0.001
Omni Directional Antenna Usage	0	0	2	3	0	0	2	3

Table 6 – Experimental Results for Protection a Large Area with 2 Systems (Close Threats)

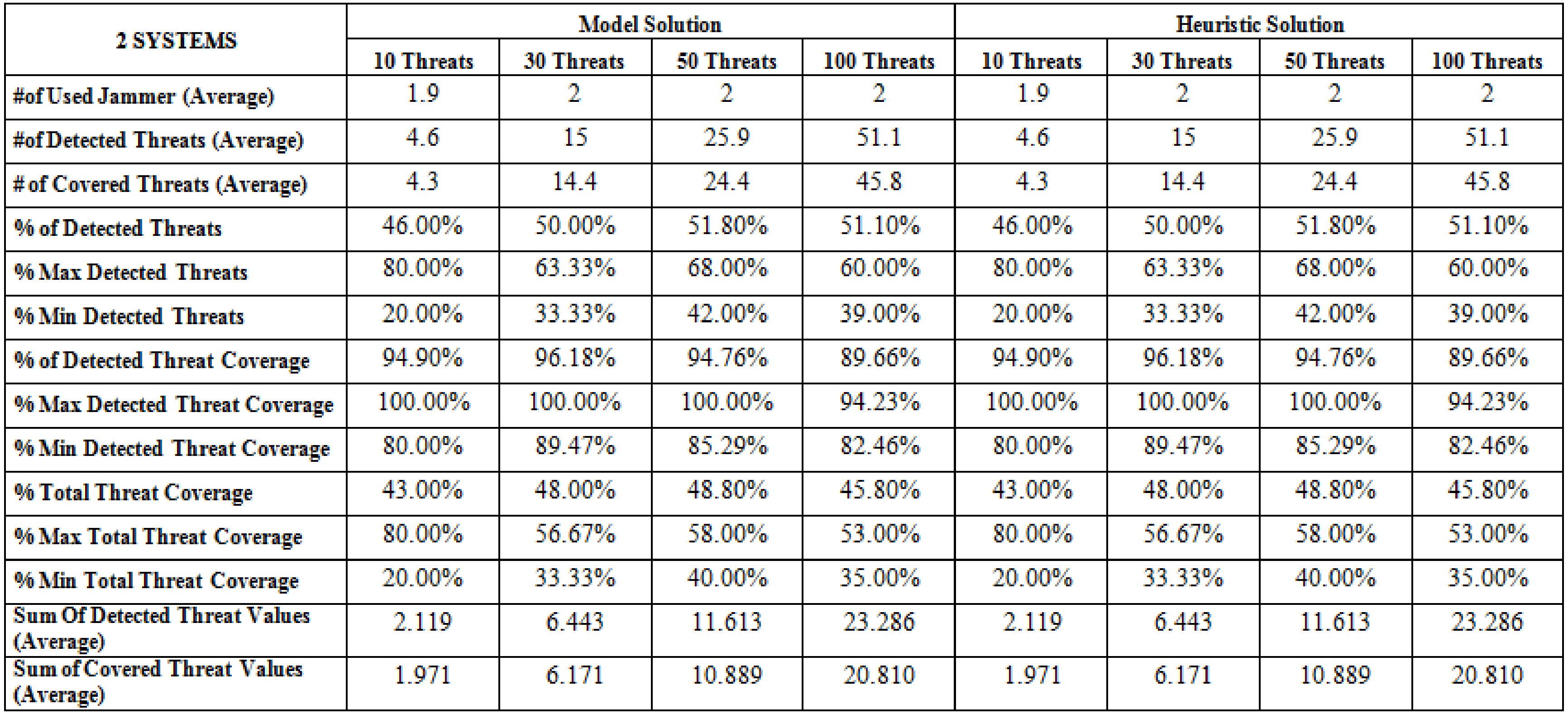


2 SYSTEMS	Model Solution				Heuristic Solution			
	10 Threats	30 Threats	50 Threats	100 Threats	10 Threats	30 Threats	50 Threats	100 Threats
#of Used Jammer (Average)	2	2	2	2	2	2	2	2
#of Detected Threats (Average)	5.8	16.2	23.3	51.8	5.8	16.2	23.3	51.8
# of Covered Threats (Average)	5.6	16	22.9	50.5	5.6	16	22.9	50.5
% of Detected Threats	58.00%	54.00%	46.60%	51.80%	58.00%	54.00%	46.60%	51.80%
% Max Detected Threats	80.00%	66.67%	58.00%	57.00%	80.00%	66.67%	58.00%	57.00%
% Min Detected Threats	40.00%	40.00%	40.00%	48.00%	40.00%	40.00%	40.00%	48.00%
% of Detected Threat Coverage	96.75%	98.89%	98.33%	97.48%	96.75%	98.89%	98.33%	97.48%
% Max Detected Threat Coverage	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%
% Min Detected Threat Coverage	80.00%	88.89%	91.30%	94.64%	80.00%	88.89%	91.30%	94.64%
% Total Threat Coverage	56.00%	53.33%	45.80%	50.50%	56.00%	53.33%	45.80%	50.50%
% Max Total Threat Coverage	70.00%	66.67%	58.00%	56.00%	70.00%	66.67%	58.00%	56.00%
% Min Total Threat Coverage	40.00%	40.00%	40.00%	47.00%	40.00%	40.00%	40.00%	47.00%
Sum Of Detected Threat Values (Average)	4.164	11.593	16.579	36.089	4.164	11.593	16.579	36.089
Sum of Covered Threat Values (Average)	4.042	11.476	16.302	35.173	4.042	11.476	16.302	35.173

Table 6 – Continued

2 SYSTEMS	Model Solution				Heuristic Solution			
	10 Threats	30 Threats	50 Threats	100 Threats	10 Threats	30 Threats	50 Threats	100 Threats
% Detected Threat Value Coverage	97.36%	99.04%	98.39%	97.45%	97.36%	99.04%	98.39%	97.45%
% Max Detected Threat Value Coverage	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%
% Min Detected Threat Value Coverage	83.93%	90.37%	90.76%	95.10%	83.93%	90.37%	90.76%	95.10%
Total Threat Values (Average)	6.866	20.322	33.341	66.348	6.866	20.322	33.341	66.348
% Threat Value Coverage	58.87%	56.47%	48.90%	53.01%	58.87%	56.47%	48.90%	53.01%
% Max Total Threat Value Coverage	73.37%	71.97%	61.11%	59.08%	73.37%	71.97%	61.11%	59.08%
% Min Total Threat Value Coverage	44.00%	43.15%	40.87%	48.66%	44.00%	43.15%	40.87%	48.66%
Average Solution Time (Second)	0.0048	0.007	0.0179	0.0211	< 0.001	< 0.001	< 0.001	0.001
Omni Directional Antenna Usage	0	0	0	0	0	0	0	0

Table 7 – Experimental Results for Protection a Large Area with 2 Systems (Distant Threats)



2 SYSTEMS	Model Solution				Heuristic Solution			
	10 Threats	30 Threats	50 Threats	100 Threats	10 Threats	30 Threats	50 Threats	100 Threats
#of Used Jammer (Average)	1.9	2	2	2	1.9	2	2	2
#of Detected Threats (Average)	4.6	15	25.9	51.1	4.6	15	25.9	51.1
# of Covered Threats (Average)	4.3	14.4	24.4	45.8	4.3	14.4	24.4	45.8
% of Detected Threats	46.00%	50.00%	51.80%	51.10%	46.00%	50.00%	51.80%	51.10%
% Max Detected Threats	80.00%	63.33%	68.00%	60.00%	80.00%	63.33%	68.00%	60.00%
% Min Detected Threats	20.00%	33.33%	42.00%	39.00%	20.00%	33.33%	42.00%	39.00%
% of Detected Threat Coverage	94.90%	96.18%	94.76%	89.66%	94.90%	96.18%	94.76%	89.66%
% Max Detected Threat Coverage	100.00%	100.00%	100.00%	94.23%	100.00%	100.00%	100.00%	94.23%
% Min Detected Threat Coverage	80.00%	89.47%	85.29%	82.46%	80.00%	89.47%	85.29%	82.46%
% Total Threat Coverage	43.00%	48.00%	48.80%	45.80%	43.00%	48.00%	48.80%	45.80%
% Max Total Threat Coverage	80.00%	56.67%	58.00%	53.00%	80.00%	56.67%	58.00%	53.00%
% Min Total Threat Coverage	20.00%	33.33%	40.00%	35.00%	20.00%	33.33%	40.00%	35.00%
Sum Of Detected Threat Values (Average)	2.119	6.443	11.613	23.286	2.119	6.443	11.613	23.286
Sum of Covered Threat Values (Average)	1.971	6.171	10.889	20.810	1.971	6.171	10.889	20.810

Table 7 – Continued

2 SYSTEMS	Model Solution				Heuristic Solution			
	10 Threats	30 Threats	50 Threats	100 Threats	10 Threats	30 Threats	50 Threats	100 Threats
% Detected Threat Value Coverage	94.30%	96.36%	94.24%	89.58%	94.30%	96.36%	94.24%	89.58%
% Max Detected Threat Value Coverage	100.00%	100.00%	100.00%	94.57%	100.00%	100.00%	100.00%	94.57%
% Min Detected Threat Value Coverage	69.23%	85.00%	84.81%	79.58%	69.23%	85.00%	84.81%	79.58%
Total Threat Values (Average)	4.122	11.985	20.298	41.491	4.122	11.985	20.298	41.491
% Threat Value Coverage	47.81%	51.49%	53.65%	50.16%	47.81%	51.49%	53.65%	50.16%
% Max Total Threat Value Coverage	89.54%	62.85%	60.38%	57.93%	89.54%	62.85%	60.38%	57.93%
% Min Total Threat Value Coverage	27.16%	36.42%	44.42%	39.53%	27.16%	36.42%	44.42%	39.53%
Average Solution Time (Second)	0.0121	0.0307	0.0116	0.0169	< 0.001	< 0.001	< 0.001	0.001
Omni Directional Antenna Usage	0	0	0	0	0	0	0	0

4.3. Protection with 3 Integrated Systems

In this experiment, small and large area protection is examined by changing number of threats and threats distances.

4.3.1. Protection of Small Area

The small protected area is defined as 200 meters x 200 meters and the two integrated system is located on the upper two corners and the one integrated system is located on the lower middle of the area. The coordinates of the systems are: S1 (100, 100), S2 (-100,100) and S3 (0,-100).

4.3.1.1. Close Threats

In this scenario, the distances between threats and protected area are randomly generated between 1 meter and 300 meters.

The experimental results of the scenario are shown in Table – 8.

4.3.1.2. Distant Threats

In this scenario, the distances between threats and protected area are randomly generated between 1 meter and 1500 meters.

The experimental results of the scenario are shown in Table – 9.

4.3.2. Protection of Large Area

The large protected area is defined as 900 meters x 900 meters and the two integrated system is located on the upper two corners and the one integrated system is located on the lower middle of the area. The coordinates of the systems are: S1 (800, 800), S2 (-800,800) and S3 (0, -800).

4.3.2.1 Close Threats

In this scenario, the distances between threats and protected area are randomly generated between 1 meter and 300 meters.

The experimental results of the scenario are shown in Table – 10.

4.3.2.2. Distant Threats

In this scenario, the distances between threats and protected area are randomly generated between 1 meter and 1500 meters.

The experimental results of the scenario are shown in Table – 11.

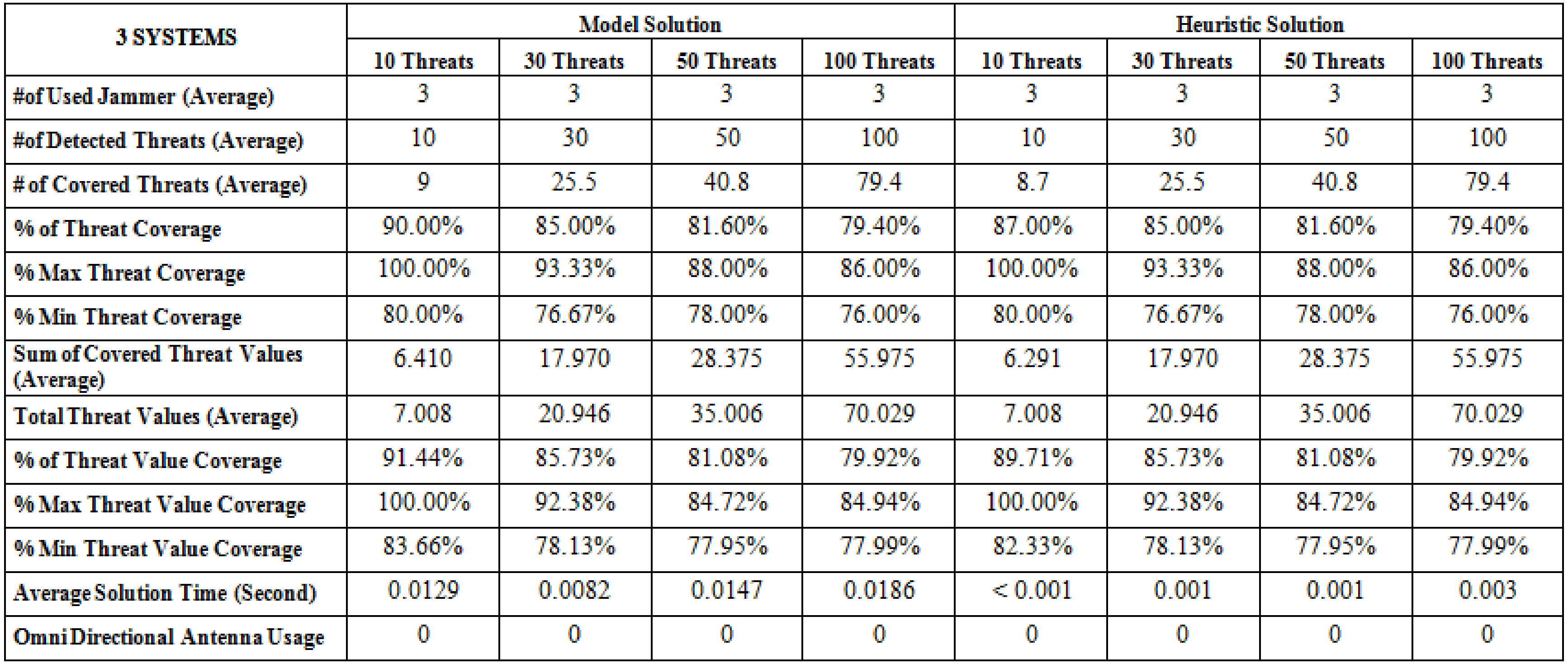
4.3.3. Result Evaluation

- In the large area protection scenarios, both the heuristic approach and the mathematical model give the same solution results, except solution time, for each case.
- In the small area protection scenarios, heuristic approach and mathematical model solutions shows differences in some cases. In the close threat attack cases, heuristic approach and mathematical model gave different solution results for 3 cases out of 10 threat attack scenarios. In the distant threat attack cases, this difference occurred 4 times for attack of 30 threats, 3 times for attack of 50 threats and 2 times for attack of 100 threats.
- Both mathematical model and heuristic approach solved the cases in short times but heuristic approach's solution time is less than mathematical model.
- When the 4th and 9th rows of the Table – 8 and Table – 9 are examined, it can be seen that the difference between two solutions is less than %3 and not among the high weight value threats.
- This difference occurs from the fact that when the heuristic approach solves the problem, the threats that are covered by the system that provides the highest weight coverage are deleted from the active threat set. Thus remaining systems can not cover these threats. However, mathematical model examines the problem entirely and solve the problem by evaluating all combinations of threat coverage.
- Therefore, when multiple systems are placed to protect a small area, in some cases the heuristic approach can give different results as compared to

mathematical model, since the system can interfere with each other's coverage areas.

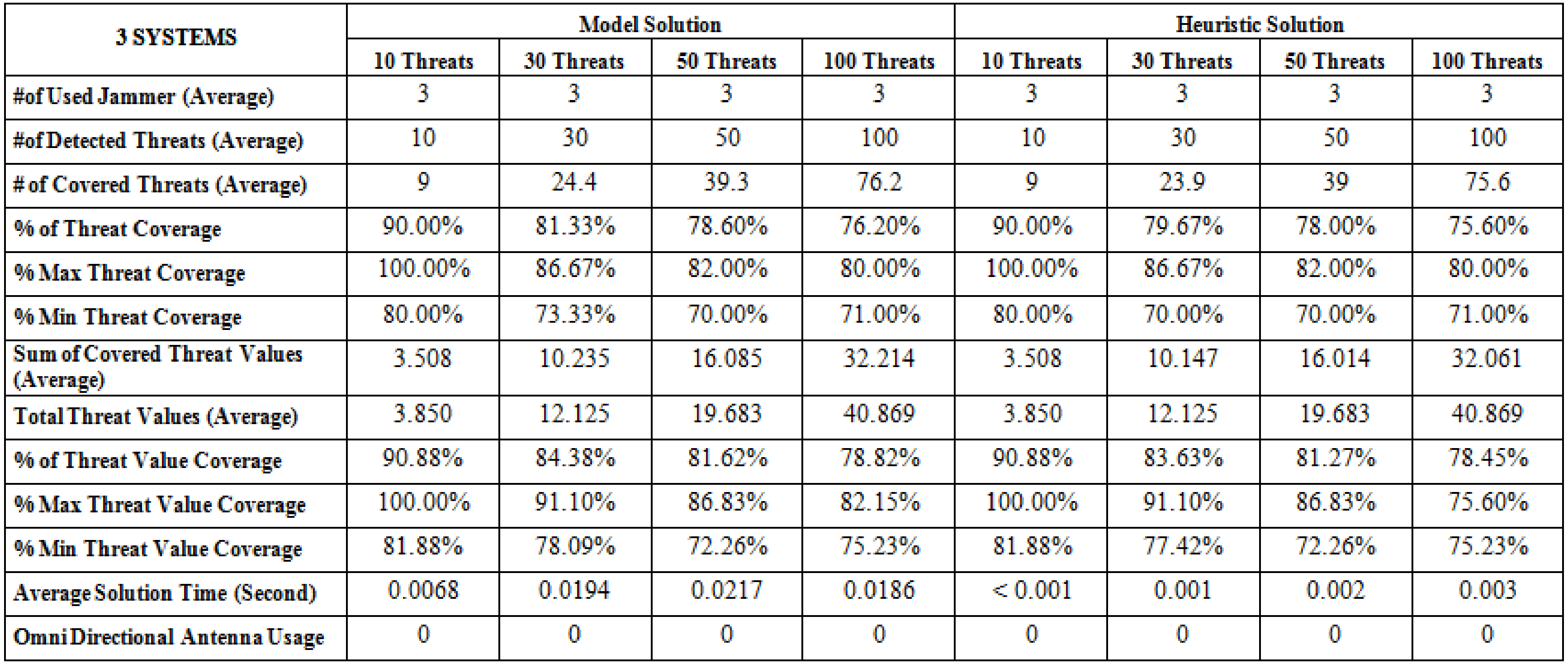
- In the small area protection scenarios, it has been observed that systems can detect all threats and threat weight value coverage rates decrease when the number of threat increases.
- In the large area protection scenarios, although it has been observed that systems can detect all threats in the close threat cases, full detection cannot be achieved in the distant threat cases.
- While the first and second systems can detect all threat attacks coming from their region, third system cannot provide full detection on its location, because its' range is not enough for protecting large border.
- As in the two jammer protection experiment, difference between the detected threat coverage rates and total threat coverage rates can be seen in the 4th and the 7th row of the Table – 11. In addition to that, weigh coverage differences between the detected and total threats can be seen in the 15th and 20th row of the Table – 11.
- In the large area protection scenario, threats are neutralized once by using 2 jammers, for close and distant 10 threat attacks.

Table 8 – Experimental Results for Protection a Small Area with 3 Systems (Close Threats)



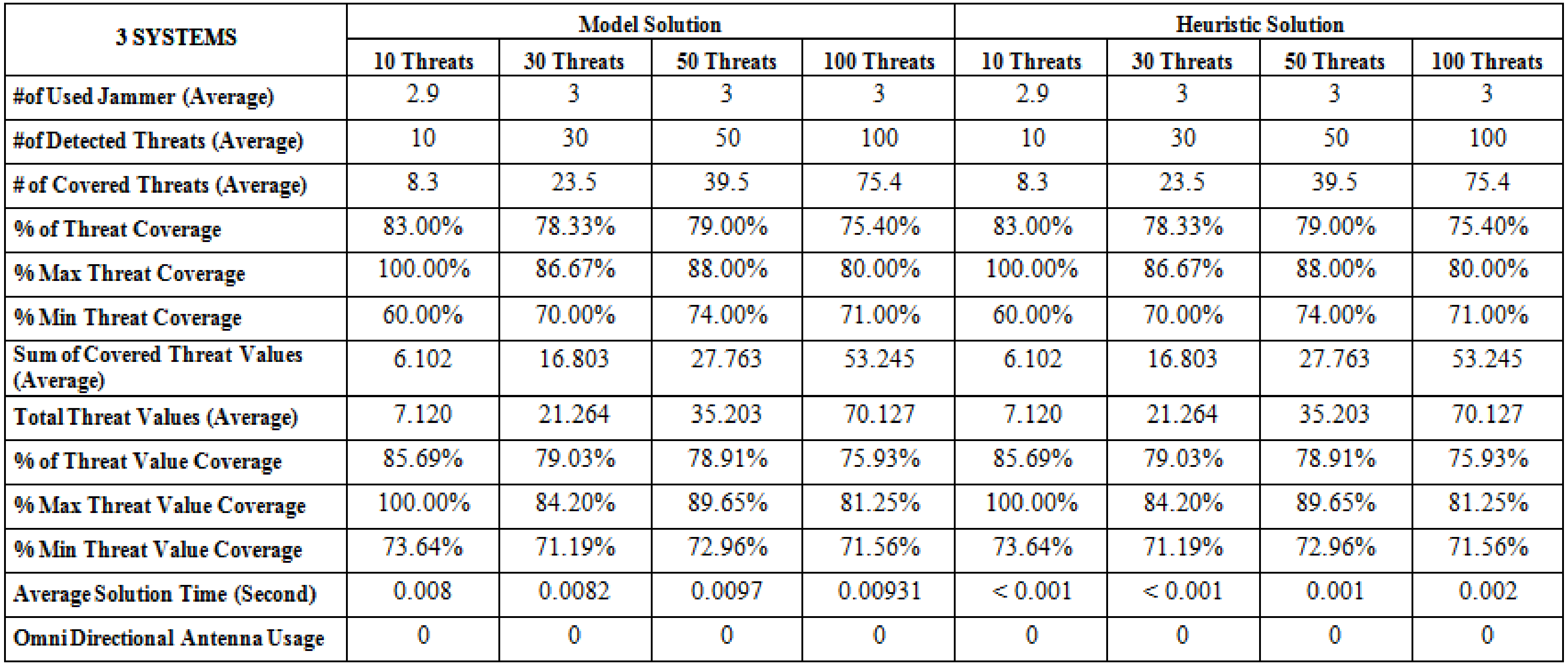
3 SYSTEMS	Model Solution				Heuristic Solution			
	10 Threats	30 Threats	50 Threats	100 Threats	10 Threats	30 Threats	50 Threats	100 Threats
#of Used Jammer (Average)	3	3	3	3	3	3	3	3
#of Detected Threats (Average)	10	30	50	100	10	30	50	100
# of Covered Threats (Average)	9	25.5	40.8	79.4	8.7	25.5	40.8	79.4
% of Threat Coverage	90.00%	85.00%	81.60%	79.40%	87.00%	85.00%	81.60%	79.40%
% Max Threat Coverage	100.00%	93.33%	88.00%	86.00%	100.00%	93.33%	88.00%	86.00%
% Min Threat Coverage	80.00%	76.67%	78.00%	76.00%	80.00%	76.67%	78.00%	76.00%
Sum of Covered Threat Values (Average)	6.410	17.970	28.375	55.975	6.291	17.970	28.375	55.975
Total Threat Values (Average)	7.008	20.946	35.006	70.029	7.008	20.946	35.006	70.029
% of Threat Value Coverage	91.44%	85.73%	81.08%	79.92%	89.71%	85.73%	81.08%	79.92%
% Max Threat Value Coverage	100.00%	92.38%	84.72%	84.94%	100.00%	92.38%	84.72%	84.94%
% Min Threat Value Coverage	83.66%	78.13%	77.95%	77.99%	82.33%	78.13%	77.95%	77.99%
Average Solution Time (Second)	0.0129	0.0082	0.0147	0.0186	< 0.001	0.001	0.001	0.003
Omni Directional Antenna Usage	0	0	0	0	0	0	0	0

Table 9 – Experimental Results for Protection a Small Area with 3 Systems (Distant Threats)



3 SYSTEMS	Model Solution				Heuristic Solution			
	10 Threats	30 Threats	50 Threats	100 Threats	10 Threats	30 Threats	50 Threats	100 Threats
#of Used Jammer (Average)	3	3	3	3	3	3	3	3
#of Detected Threats (Average)	10	30	50	100	10	30	50	100
# of Covered Threats (Average)	9	24.4	39.3	76.2	9	23.9	39	75.6
% of Threat Coverage	90.00%	81.33%	78.60%	76.20%	90.00%	79.67%	78.00%	75.60%
% Max Threat Coverage	100.00%	86.67%	82.00%	80.00%	100.00%	86.67%	82.00%	80.00%
% Min Threat Coverage	80.00%	73.33%	70.00%	71.00%	80.00%	70.00%	70.00%	71.00%
Sum of Covered Threat Values (Average)	3.508	10.235	16.085	32.214	3.508	10.147	16.014	32.061
Total Threat Values (Average)	3.850	12.125	19.683	40.869	3.850	12.125	19.683	40.869
% of Threat Value Coverage	90.88%	84.38%	81.62%	78.82%	90.88%	83.63%	81.27%	78.45%
% Max Threat Value Coverage	100.00%	91.10%	86.83%	82.15%	100.00%	91.10%	86.83%	75.60%
% Min Threat Value Coverage	81.88%	78.09%	72.26%	75.23%	81.88%	77.42%	72.26%	75.23%
Average Solution Time (Second)	0.0068	0.0194	0.0217	0.0186	< 0.001	0.001	0.002	0.003
Omni Directional Antenna Usage	0	0	0	0	0	0	0	0

Table 10 – Experimental Results for Protection a Large Area with 3 Systems (Close Threats)

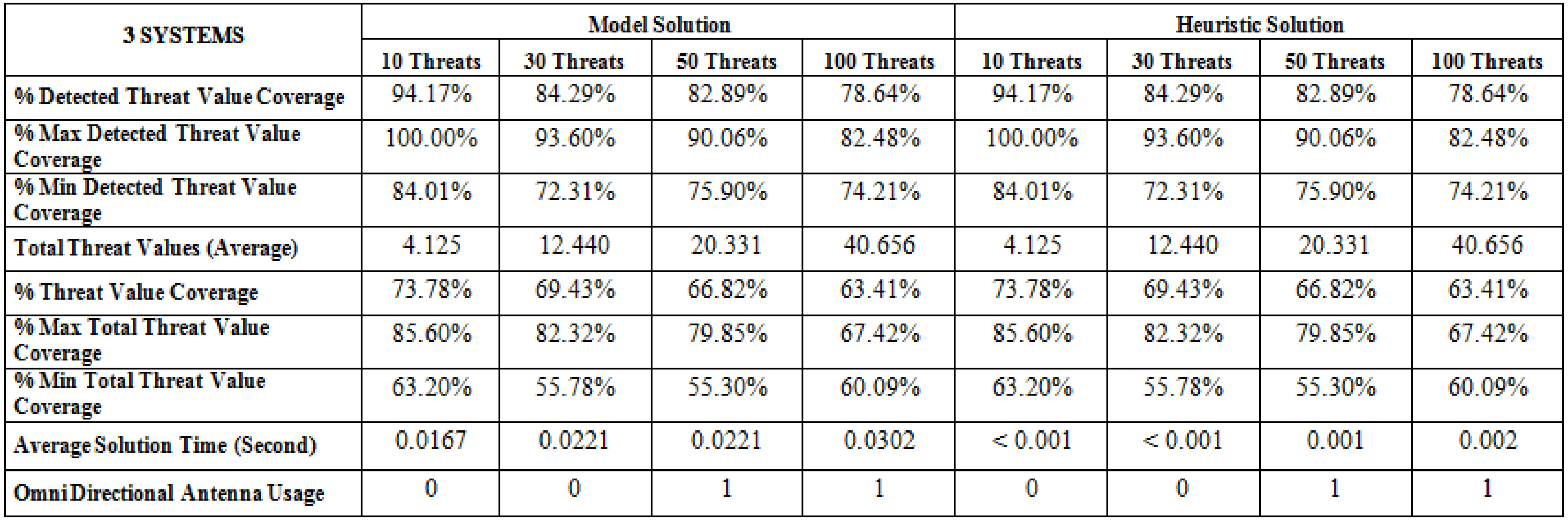


3 SYSTEMS	Model Solution				Heuristic Solution			
	10 Threats	30 Threats	50 Threats	100 Threats	10 Threats	30 Threats	50 Threats	100 Threats
#of Used Jammer (Average)	2.9	3	3	3	2.9	3	3	3
#of Detected Threats (Average)	10	30	50	100	10	30	50	100
# of Covered Threats (Average)	8.3	23.5	39.5	75.4	8.3	23.5	39.5	75.4
% of Threat Coverage	83.00%	78.33%	79.00%	75.40%	83.00%	78.33%	79.00%	75.40%
% Max Threat Coverage	100.00%	86.67%	88.00%	80.00%	100.00%	86.67%	88.00%	80.00%
% Min Threat Coverage	60.00%	70.00%	74.00%	71.00%	60.00%	70.00%	74.00%	71.00%
Sum of Covered Threat Values (Average)	6.102	16.803	27.763	53.245	6.102	16.803	27.763	53.245
Total Threat Values (Average)	7.120	21.264	35.203	70.127	7.120	21.264	35.203	70.127
% of Threat Value Coverage	85.69%	79.03%	78.91%	75.93%	85.69%	79.03%	78.91%	75.93%
% Max Threat Value Coverage	100.00%	84.20%	89.65%	81.25%	100.00%	84.20%	89.65%	81.25%
% Min Threat Value Coverage	73.64%	71.19%	72.96%	71.56%	73.64%	71.19%	72.96%	71.56%
Average Solution Time (Second)	0.008	0.0082	0.0097	0.00931	< 0.001	< 0.001	0.001	0.002
Omni Directional Antenna Usage	0	0	0	0	0	0	0	0

Table 11 – Experimental Results for Protection a Large Area with 3 Systems (Distant Threats)

3 SYSTEMS	Model Solution				Heuristic Solution			
	10 Threats	30 Threats	50 Threats	100 Threats	10 Threats	30 Threats	50 Threats	100 Threats
#of Used Jammer	2.9	3	3	3	2.9	3	3	3
#of Detected Threats (Average)	6.5	21.9	36.2	70.7	6.5	21.9	36.2	70.7
# of Covered Threats (Average)	6	19.1	30.5	56.3	6	19.1	30.5	56.3
% of Detected Threats	65.00%	73.00%	72.40%	70.70%	65.00%	73.00%	72.40%	70.70%
% Max Detected Threats	80.00%	86.67%	80.00%	74.00%	80.00%	86.67%	80.00%	74.00%
% Min Detected Threats	40.00%	60.00%	60.00%	66.00%	40.00%	60.00%	60.00%	66.00%
% of Detected Threat Coverage	92.92%	87.27%	84.17%	79.63%	92.92%	87.27%	84.17%	79.63%
% Max Detected Threat Coverage	100.00%	96.00%	92.50%	83.78%	100.00%	96.00%	92.50%	83.78%
% Min Detected Threat Coverage	66.67%	76.92%	77.14%	75.34%	66.67%	76.92%	77.14%	75.34%
% Total Threat Coverage	60.00%	63.67%	61.00%	56.30%	60.00%	63.67%	61.00%	56.30%
% Max Total Threat Coverage	80.00%	80.00%	74.00%	62.00%	80.00%	80.00%	74.00%	62.00%
% Min Total Threat Coverage	40.00%	50.00%	52.00%	52.00%	40.00%	50.00%	52.00%	52.00%
Sum Of Detected Threat Values (Average)	3.269	10.297	16.453	32.799	3.269	10.297	16.453	32.799
Sum of Covered Threat Values (Average)	3.061	8.670	13.642	25.781	3.061	8.670	13.642	25.781

Table 11 – Continued



3 SYSTEMS	Model Solution				Heuristic Solution			
	10 Threats	30 Threats	50 Threats	100 Threats	10 Threats	30 Threats	50 Threats	100 Threats
% Detected Threat Value Coverage	94.17%	84.29%	82.89%	78.64%	94.17%	84.29%	82.89%	78.64%
% Max Detected Threat Value Coverage	100.00%	93.60%	90.06%	82.48%	100.00%	93.60%	90.06%	82.48%
% Min Detected Threat Value Coverage	84.01%	72.31%	75.90%	74.21%	84.01%	72.31%	75.90%	74.21%
Total Threat Values (Average)	4.125	12.440	20.331	40.656	4.125	12.440	20.331	40.656
% Threat Value Coverage	73.78%	69.43%	66.82%	63.41%	73.78%	69.43%	66.82%	63.41%
% Max Total Threat Value Coverage	85.60%	82.32%	79.85%	67.42%	85.60%	82.32%	79.85%	67.42%
% Min Total Threat Value Coverage	63.20%	55.78%	55.30%	60.09%	63.20%	55.78%	55.30%	60.09%
Average Solution Time (Second)	0.0167	0.0221	0.0221	0.0302	< 0.001	< 0.001	0.001	0.002
Omni Directional Antenna Usage	0	0	1	1	0	0	1	1

4.4. Protection with 4 Integrated Systems

In this experiment, small and large area protection is examined by changing number of threats and threats distances.

4.4.1. Protection of Small Area

The small protected area is defined as 200 meters x 200 meters and the four integrated system is located on the four corners of the area. The coordinates of the systems are: S1 (100, 100), S2 (-100,100), S3 (-100,-100) and S4 (100,-100).

4.4.1.1. Close Threats

In this scenario, the distances between threats and protected area are randomly generated between 1 meter and 300 meters.

The experimental results of the scenario are shown in Table – 12.

4.4.1.2. Distant Threats

In this scenario, the distances between threats and protected area are randomly generated between 1 meter and 1500 meters.

The experimental results of the scenario are shown in Table – 13.

4.4.2. Protection of Large Area

The small protected area is defined as 900 meters x 900 meters and the four integrated system is located on the four corners of the area. The coordinates of the systems are: S1 (800, 800), S2 (-800,800), S3 (-800,-800) and S4 (100,-100).

4.4.2.1 Close Threats

In this scenario, the distances between threats and protected area are randomly generated between 1 meter and 300 meters.

The experimental results of the scenario are shown in Table – 14.

4.4.2.2. Distant Threats

In this scenario, the distances between threats and protected area are randomly generated between 1 meter and 1500 meters.

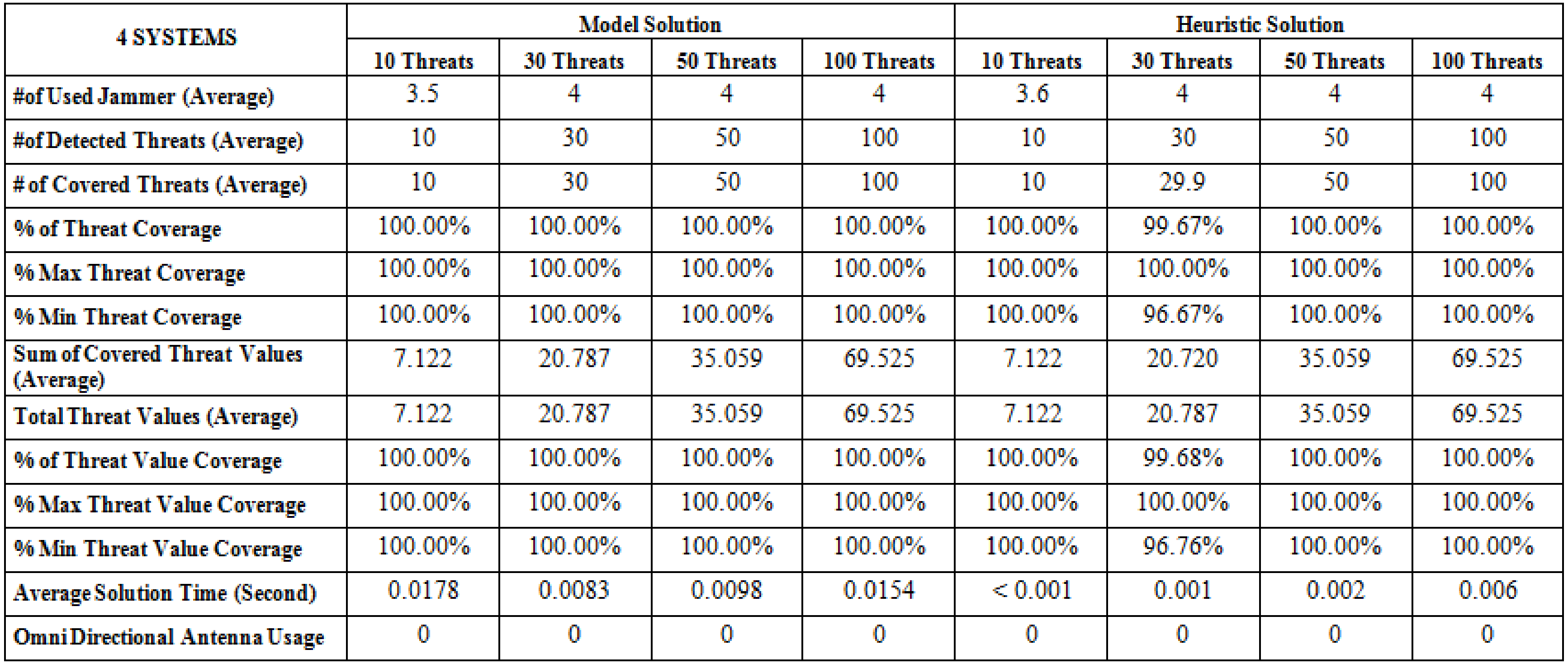
The experimental results of the scenario are shown in Table – 15.

4.4.3. Result Evaluation

- Full threat detection is ensured by the 4 systems for both small and large area protections.
- In the large area protection scenarios, heuristic approach and the mathematical model gave the same results, except solution time, for each number of group attacks.
- In the large area protection scenarios, threat and weight value coverage rates were achieved over 90% for both close and distant threat attack cases, except 100 threat attack case in large area protection scenario. However, more than 90% of threats and value coverage was achieved among 10 experiments in the 100 threat attack case.
- In the small area protection scenarios, heuristic approach and mathematical model solutions show differences in some cases. In the close threat attack cases, heuristic approach and mathematical model gave different solutions for 1 time for attacks of 30 threats. In the distant threat attack cases, this difference occurred 1 time for attack of 10 threats, 6 times for attack of 30 threats, 9 times for attack of 50 threats and 7 times for attack of 100 threats.
- When the 4th and 9th rows of the Table – 12 and Table – 13 are examined, it can be seen that the difference between two solutions is less than 2.5% and not among the high weight value threats.
- In the case of attacks with 10 threats, there were some cases where full threat coverage was achieved without using 4 jammers. In the distant threat scenarios, 3 jammers were used in both mathematical and heuristic solution approaches for 3 times to apply full threat coverage for large area protection.

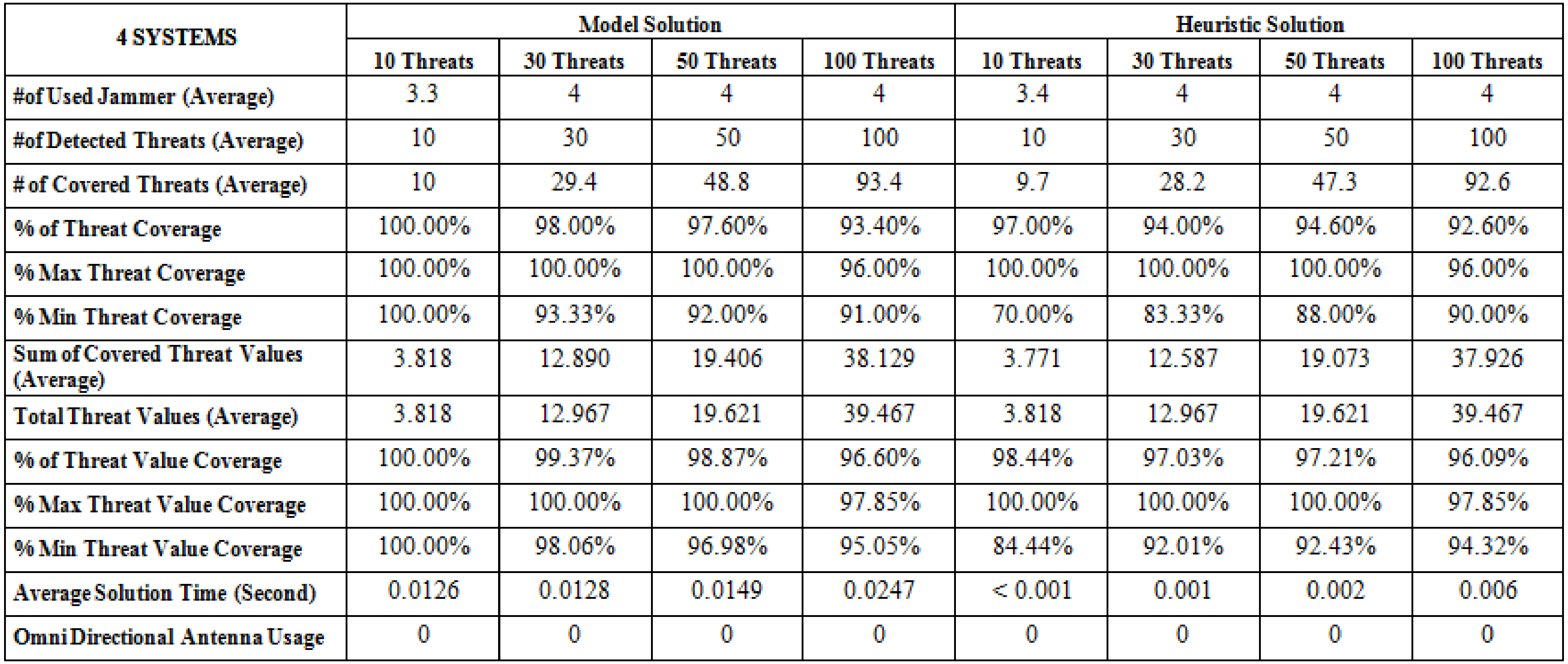
- The neutralization with 3 jammers is higher in small area protection scenarios rather than the large area protection.
- In the close threat cases, 3 jammers are used in the mathematical model solution for 5 times and 3 jammers are used in the heuristic solution approach for 4 times to ensure full threat coverage.
- In the distant threat cases, again 3 jammers are used in the mathematical solution for 5 times and 3 jammers are used in the heuristic solution approach for 4 times but in this time, 2 jammers are used to ensure full threat coverage for 1 time in both mathematical model and heuristic solution approach.
- Omni directional jammer was not used during 4 jammer protection scenarios for both mathematical model and heuristic approach solutions.
- Both mathematical model and heuristic approach solved the cases in short times but heuristic approach’s solution time is less than mathematical model.

Table 12 – Experimental Results for Protection a Small Area with 4 Systems (Close Threats)



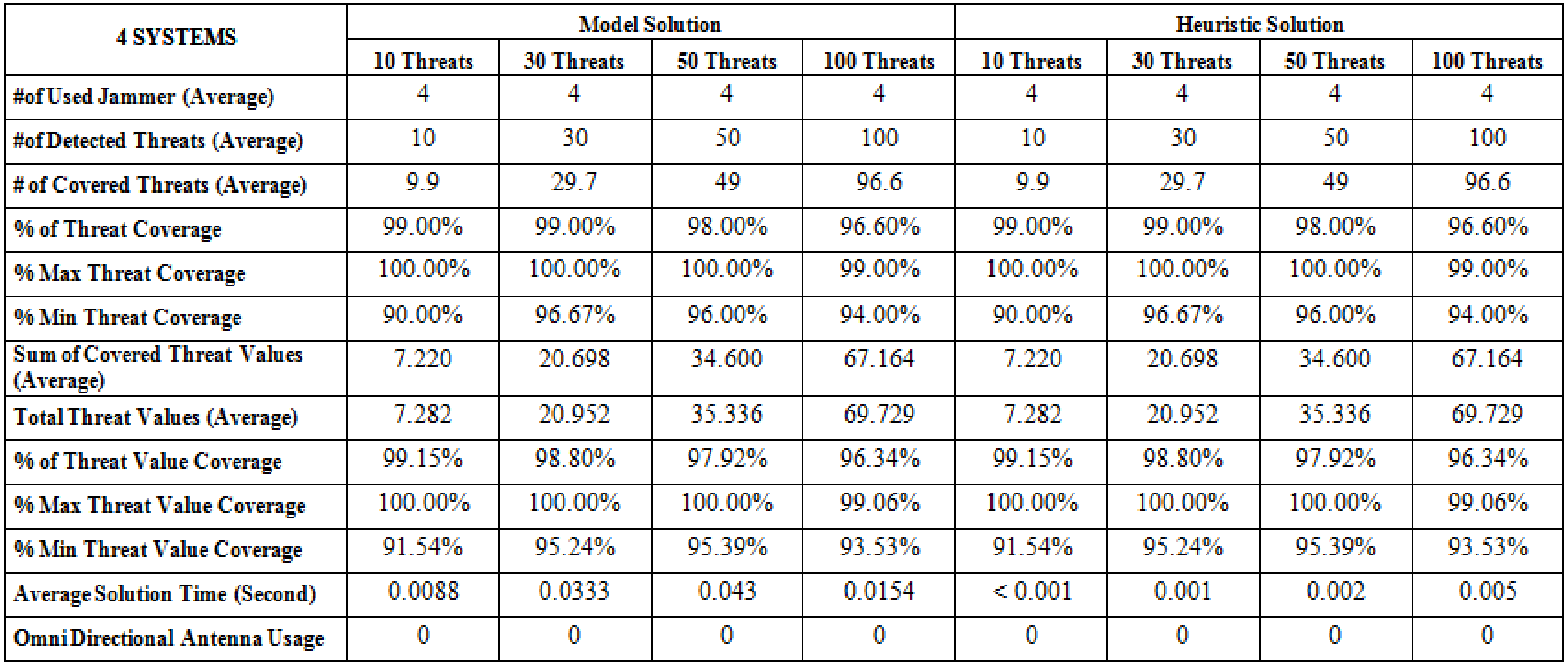
4 SYSTEMS	Model Solution				Heuristic Solution			
	10 Threats	30 Threats	50 Threats	100 Threats	10 Threats	30 Threats	50 Threats	100 Threats
#of Used Jammer (Average)	3.5	4	4	4	3.6	4	4	4
#of Detected Threats (Average)	10	30	50	100	10	30	50	100
# of Covered Threats (Average)	10	30	50	100	10	29.9	50	100
% of Threat Coverage	100.00%	100.00%	100.00%	100.00%	100.00%	99.67%	100.00%	100.00%
% Max Threat Coverage	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%
% Min Threat Coverage	100.00%	100.00%	100.00%	100.00%	100.00%	96.67%	100.00%	100.00%
Sum of Covered Threat Values (Average)	7.122	20.787	35.059	69.525	7.122	20.720	35.059	69.525
Total Threat Values (Average)	7.122	20.787	35.059	69.525	7.122	20.787	35.059	69.525
% of Threat Value Coverage	100.00%	100.00%	100.00%	100.00%	100.00%	99.68%	100.00%	100.00%
% Max Threat Value Coverage	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%
% Min Threat Value Coverage	100.00%	100.00%	100.00%	100.00%	100.00%	96.76%	100.00%	100.00%
Average Solution Time (Second)	0.0178	0.0083	0.0098	0.0154	< 0.001	0.001	0.002	0.006
Omni Directional Antenna Usage	0	0	0	0	0	0	0	0

Table 13 – Experimental Results for Protection a Small Area with 4 Systems (Distant Threats)



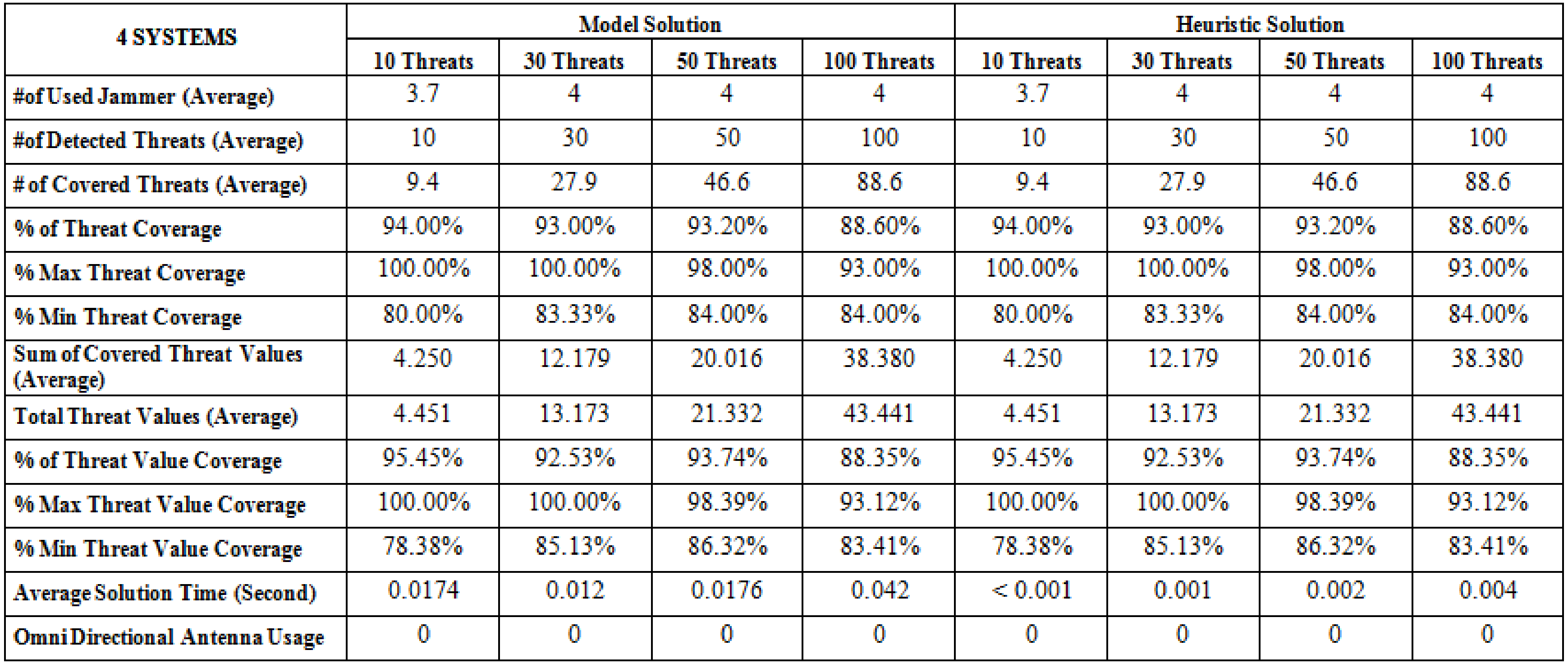
4 SYSTEMS	Model Solution				Heuristic Solution			
	10 Threats	30 Threats	50 Threats	100 Threats	10 Threats	30 Threats	50 Threats	100 Threats
#of Used Jammer (Average)	3.3	4	4	4	3.4	4	4	4
#of Detected Threats (Average)	10	30	50	100	10	30	50	100
# of Covered Threats (Average)	10	29.4	48.8	93.4	9.7	28.2	47.3	92.6
% of Threat Coverage	100.00%	98.00%	97.60%	93.40%	97.00%	94.00%	94.60%	92.60%
% Max Threat Coverage	100.00%	100.00%	100.00%	96.00%	100.00%	100.00%	100.00%	96.00%
% Min Threat Coverage	100.00%	93.33%	92.00%	91.00%	70.00%	83.33%	88.00%	90.00%
Sum of Covered Threat Values (Average)	3.818	12.890	19.406	38.129	3.771	12.587	19.073	37.926
Total Threat Values (Average)	3.818	12.967	19.621	39.467	3.818	12.967	19.621	39.467
% of Threat Value Coverage	100.00%	99.37%	98.87%	96.60%	98.44%	97.03%	97.21%	96.09%
% Max Threat Value Coverage	100.00%	100.00%	100.00%	97.85%	100.00%	100.00%	100.00%	97.85%
% Min Threat Value Coverage	100.00%	98.06%	96.98%	95.05%	84.44%	92.01%	92.43%	94.32%
Average Solution Time (Second)	0.0126	0.0128	0.0149	0.0247	< 0.001	0.001	0.002	0.006
Omni Directional Antenna Usage	0	0	0	0	0	0	0	0

Table 14 – Experimental Results for Protection a Large Area with 4 Systems (Close Threats)



4 SYSTEMS	Model Solution				Heuristic Solution			
	10 Threats	30 Threats	50 Threats	100 Threats	10 Threats	30 Threats	50 Threats	100 Threats
#of Used Jammer (Average)	4	4	4	4	4	4	4	4
#of Detected Threats (Average)	10	30	50	100	10	30	50	100
# of Covered Threats (Average)	9.9	29.7	49	96.6	9.9	29.7	49	96.6
% of Threat Coverage	99.00%	99.00%	98.00%	96.60%	99.00%	99.00%	98.00%	96.60%
% Max Threat Coverage	100.00%	100.00%	100.00%	99.00%	100.00%	100.00%	100.00%	99.00%
% Min Threat Coverage	90.00%	96.67%	96.00%	94.00%	90.00%	96.67%	96.00%	94.00%
Sum of Covered Threat Values (Average)	7.220	20.698	34.600	67.164	7.220	20.698	34.600	67.164
Total Threat Values (Average)	7.282	20.952	35.336	69.729	7.282	20.952	35.336	69.729
% of Threat Value Coverage	99.15%	98.80%	97.92%	96.34%	99.15%	98.80%	97.92%	96.34%
% Max Threat Value Coverage	100.00%	100.00%	100.00%	99.06%	100.00%	100.00%	100.00%	99.06%
% Min Threat Value Coverage	91.54%	95.24%	95.39%	93.53%	91.54%	95.24%	95.39%	93.53%
Average Solution Time (Second)	0.0088	0.0333	0.043	0.0154	< 0.001	0.001	0.002	0.005
Omni Directional Antenna Usage	0	0	0	0	0	0	0	0

Table 15 – Experimental Results for Protection a Large Area with 4 Systems (Distant Threats)



4 SYSTEMS	Model Solution				Heuristic Solution			
	10 Threats	30 Threats	50 Threats	100 Threats	10 Threats	30 Threats	50 Threats	100 Threats
#of Used Jammer (Average)	3.7	4	4	4	3.7	4	4	4
#of Detected Threats (Average)	10	30	50	100	10	30	50	100
# of Covered Threats (Average)	9.4	27.9	46.6	88.6	9.4	27.9	46.6	88.6
% of Threat Coverage	94.00%	93.00%	93.20%	88.60%	94.00%	93.00%	93.20%	88.60%
% Max Threat Coverage	100.00%	100.00%	98.00%	93.00%	100.00%	100.00%	98.00%	93.00%
% Min Threat Coverage	80.00%	83.33%	84.00%	84.00%	80.00%	83.33%	84.00%	84.00%
Sum of Covered Threat Values (Average)	4.250	12.179	20.016	38.380	4.250	12.179	20.016	38.380
Total Threat Values (Average)	4.451	13.173	21.332	43.441	4.451	13.173	21.332	43.441
% of Threat Value Coverage	95.45%	92.53%	93.74%	88.35%	95.45%	92.53%	93.74%	88.35%
% Max Threat Value Coverage	100.00%	100.00%	98.39%	93.12%	100.00%	100.00%	98.39%	93.12%
% Min Threat Value Coverage	78.38%	85.13%	86.32%	83.41%	78.38%	85.13%	86.32%	83.41%
Average Solution Time (Second)	0.0174	0.012	0.0176	0.042	< 0.001	0.001	0.002	0.004
Omni Directional Antenna Usage	0	0	0	0	0	0	0	0

4.5. Evaluation for All Scenarios

The following results are achieved as a result of the experiments for different number of integrated Anti-Drone Defense System used, different sizes of areas protected and different number of threat attacks.

- 1 integrated Anti Drone Defense System is not enough for protecting small areas. As seen in the different scenarios, all threats cannot be neutralized without the need for using omni directional jammer; because the jammer is directional and can only be effective in a particular sector depending on the antenna’s position at that time.
- 2 integrated Anti Drone Defense Systems can be used for protecting small areas, but when the number of threats increases, the coverage rate of the system decreases with respect to increment of the threat number. In the distant threat cases, the decrement of the coverage rate has led to the usage of omni directional jammer for more than 50 threats attacks. On the other hand, in the close threat cases, since the systems cannot neutralize the all close threat attacks, the omni directional jammer had to be used for neutralization.
- 2 integrated Anti Drone Defense Systems is not enough to achieve full threat detection. Although the high coverage rate is obtained over the detected threats and protection is assured without using omni directional jammer, this coverage rate does not show the accurate data; because there may be undetected and close threats near the protected area. Therefore, usage of 2 integrated Anti Drone Defense System in large area does not provide the ultimate desired protection.
- When the coverage rates and the usage of omni directional jammer are analyzed, 3 integrated Anti Drone system can be used for the protection large areas. In the close and distant threat cases, 3 integrated systems can protect the area with over 75% rate even for 100 threats attacks, without using omni directional antenna jammer.

- However, mathematical model and heuristic approach solutions show less than at most 3% coverage rate difference and the user has to make a decision about purchasing a model solving program.
- 3 integrated Anti Drone Systems can also be used for protecting large areas, but this decision contains a threat detection risk. When the threats come from the central system's region, this system's radar may not detect all threats with respect to its detection range. This inability of detection situation is observed in distant threat attacks.
- However, undetected drones are not high weighted threats even though their distance is less than 1500 meters to protected area, and if user take this risk, 3 integrated Anti Drone System can be used for protecting large areas.

When the coverage rates and the usage of omni directional jammer are analyzed, 4 integrated Anti Drone systems provide the best coverage rates for the protection small and large areas.

CHAPTER 5

CONCLUSION

In this thesis, a set covering based mathematical model and a heuristic approach have been developed that determine the jamming direction of the directional jammer antenna and which threats can be neutralized when swarm drone attack occurs towards a defended asset protected by Integrated Anti-Drone Defense System. In the defense fiction against the drone attacks, the locations of the integrated systems are predetermined by users and our mathematical model and the heuristic approach only adjust the jamming angle of the directional antenna to provide the maximum number of the highest threat level drone neutralization. The developed solution approaches do not give any information about the places where the integrated systems are to be emplaced.

In addition to maximum number of the highest level threat neutralization, mathematical model and the heuristic approach provide this coverage by using minimum number of the integrated system. Thus, the developed solution approaches provide effective source usage by preventing the jammer pollution in the area by neutralizing the threats without using all the jammers.

While developing the mathematical model to neutralize maximum number of the highest threat level drones by using minimum number of jammers, the set covering problem optimization model approaches have been utilized. The objective function of the mathematical model is set to maximize the sum of the values of the neutralized threats and the constraints of the model are determined with respect to capabilities of the directional jammer. In addition to that, inspired by the coverage algorithms used in the angle coverage problems, a coverage matrix have been constructed to calculate which threats are neutralized by directional antenna jammer in which angles and use this information in the constraint part of the mathematical model.

In order to examine proposed solution methods, a Java based threat generator program has been developed that create attack scenarios and parameters for the mathematical model and the heuristic approach. In this threat generator program, coordinate information of the protected area and the integrated systems are entered by the user and program starts to generate random threats to create problem environment. The prioritization of the generated threats is also determined by this threat generator program according to threat evaluation formulations.

Inspired by the threat evaluation techniques, two different calculation methods have been combined, when developing the proposed threat evaluation algorithm. The first method is about calculating threat’s priority values with respect to their arrival time to the protected area and the second one is calculated with respect to distance between threats and the nearest point of the protected area. The coefficient of these two threat evaluation approaches are determined by the user and entered in the user interface of the threat generator program.

The mathematical model is solved by using Java based IBM Cplex Studio model solving program. The reason for using IBM Cplex Studio for solving the mathematical model is to obtain faster results, because it has same computer language with the threat generator program. Also algorithm of the heuristic approach was written in the Java infrastructure because of the same reason with mathematical model.

In the analyzed experiments, in order to examine the performance of the proposed solution approaches in the different size of places, the threat attack scenarios on small and large protected areas were created by increasing the number of threats. In addition to that the results of the mathematical model and the heuristic approach are compared by changing the number of integrated systems in these scenarios.

Analyzing the results, it was observed that the mathematical model and the heuristic approach give the same results since the effective jamming ranges of the integrated systems do not intersect with each other. On the other hand, mathematical model provide better threat coverage in the scenarios where the jamming ranges of the integrated systems intersect with each other. However, the intersection of the jamming range indicates that the integrated systems are misplaced by the user, because in order to obtain maximum effectiveness, systems must not be placed within each others' jamming ranges.

Nevertheless, when the experiments with the wrong placement were analyzed, it was found that the difference of the threat value coverage between the mathematical model and the heuristic approach was maximum 5% and it was observed that this difference occurs because some of the low valued threats were not covered by the heuristic approach.

When the analyzing the results for the different scenarios, the decision maker can determine the number of the integrated systems to protect desired area and also can decide whether he needs to buy a model solving program to provide this protection.

To the best of our knowledge, this is the first study in the literature for the sophisticated Anti-Drone Defense Systems which use directional antenna jammer to neutralize threats. Since the usage of the jammer with the directional antenna have been recently integrated for the sophisticated drone defense systems, the threat coverage studies for more than one directional antenna jammer have not been exercised in the literature. With this study, a mathematical model and a heuristic approach have been developed for the directional antenna jammer used drone defense systems that neutralize the maximum number of threats by using minimum number of jammers.

In this study, the threat coverage problem was handled as a static problem rather than dynamic problem, although threats come with continuous movement. Because a new problem is encountered in every four seconds, which is radar's track information update ability, and solution approaches start to solve new problem with respect to new threats information. It means that, the problem is solved by fixing the positions of the threats with respect to updated threat information, which occurs in four seconds in this problem. Therefore, because of fixed threat information usage, dynamic solution approaches did not preferred.

However this study can be developed from different perspectives. For instance, while solving the threat coverage problem, it has been assumed that the jamming performance of the systems will not be affected by the terrestrial conditions where they are located in the protected area. Also, the height information of the threats were ignored and the problem was simulated in the two dimensional plane. In the further studies, altitude information of threats can be added to the solution algorithms and solutions might be developed in the three-dimensional plane. In addition to that, studies on the threat coverage of the jammer with directional antenna under different environmental conditions might be made, taking into account the terrestrial conditions that restrict the effectiveness of the radar and jammer performances.

REFERENCES

A. Caprara, M. Fischetti, and P. Toth. “A heuristic method for the set covering problem.” Operations Research 47 (1999): 730-743.

A. M. Heyns. “Measuring the threat value of xed wing aircraft in a ground-based air defense environment.” Stellenbosch University, Stellenbosch (2008).

Army, U. S. “FM 34-130 intelligence preparation of the battlefield.” Headquarters Department of the Army (1994): 1-279.

A. Steinberg. “An approach to threat assessment.” 7th International Conference on Information Fusion (2005): 8-15.

A. Steinberg, C. Bowman, and F. White. “Revisions to the JDL data fusion model.” SPIE Sensor Fusion: Architectures, Algorithms, and Applications III (1999): 430-441.

C. Toregas, R. Swain, C. Revelle, and L. Bergman. “The location of emergency service facilities.” Opns. Res. 19 (1971): 1363-1373.

Fredrik Johansson, and Göran Falkman. “A Bayesian network approach to threat evaluation with application to an air defense scenario.” 2008 11th International Conference on Information Fusion (2008): 1-7.

H. Naeem and A. Masood. “An optimal dynamic threat evaluation and weapon scheduling technique.” Knowledge Based Systems 23 (2009): 337-342.

H. Naeem, A. Masood, M. Hussain and S. A. Khan. “A novel two-staged decision support based threat evaluation and weapon assignment algorithm.” International Journal of Computer Science and Information Security 2.1 (2009).

J.E. Beasley. “A Lagrangian heuristic for set-covering problems.” Naval Research Logistics 37 (1990): 151-164.

J. N. Roux, and J. H. van Vuuren. “Threat evaluation and weapon assignment decision support: A review of the state of the art.” ORION 23.2 (2007): 151-187.

J. Roy, S. Paradis, and M. Allouche. “Threat evaluation for impact assessment in situation analysis systems.” SPIE: Signal Processing, Sensor Fusion, and Target Recognition XI 4729 (2002): 329-341.

K. S. Al-Sultan, M. F. Hussain, and J. S. Nizami. "A genetic algorithm for the set covering problem." The Journal of the Operational Research Society 47.5 (1996): 702-709.

K.-Y. Chow, K.-S. Lui, and E. Y. Lam. “Achieving 360° angle coverage in visual sensor networks.” IEEE Sensors Journal, Special Issue on Intelligent Sensors (2006): 4112-4116.

K.-Y. Chow, K.-S. Lui, and E. Y. Lam. “Maximizing angle coverage in visual sensor networks.” IEEE International Conference on Communications (2007): 3516-3521.

K. Zhang, and S. Zhang. “Maximizing the service area: A criterion to choose optimal solution in the location of set covering problem.” 23rd International Conference on Geoinformatics, Wuhan (2015): 1-3.

Lei Lin, Hou-jun Wang, and Zhao Xu. “Coverage control in wireless sensor network based on improved ant colony algorithm.” IEEE 2008 Conference on Cybernetics and Intelligent Systems (2008): 865-868.

M. L. Truter and J. H. van Vuuren. “Prerequisites for the design of a threat evaluation and weapon assignment system evaluator.” ORSSA Annual Conference (2014): 54-61.

M. Oxenham. “Enhancing situation awareness for air defence via automated threat analysis.” 6th International Conference on Information Fusion 2 (2003): 1086-1093.

O. Berman, I. Hajizadeh, and D. Krass. “The maximum covering problem with travel time uncertainty.” IEEE Transactions 45 (2013): 81-96.

R. Church, and C. ReVelle. "The maximal covering location problem." Papers of the Regional Science Association 32 (1974): 101-118.

S. Haddadi. “Simple Lagrangian heuristic for the set covering problem.” European Journal of Operational Research 97 (1997): 200–204.

S. Paradis, A. Benaskeur, M. Oxenham and P. Cutler. “Threat evaluation and weapons allocation in network-centric warfare.” 7th International Conference on Information Fusion 2 (2005): 8-.

Shunji Umetani, and Mutsunori Yagiura. “Relaxation heuristics for the set covering problem.” Journal of the Operations Research Society of Japan 50.4 (2007): 350-375.

Yu-Chee Tseng, Po-Yu Chen, and Wen-Tsuen Chen. “k – angle object coverage problem in a wireless sensor network.” IEEE Sensors Journal 12.12 (2012): 3408-3416.

Zaixin Lu, Wei Wayne Li, and Miao Pan. “Maximum lifetime scheduling for target coverage and data collection in wireless sensor networks.” IEEE Transactions on Vehicular Technology 64.2 (2015): 714-727

APPENDİX – A

Table 16 – Threat Information for Coverage Matrix Example

Track Id	**T1**	**T2**	**T3**
Distance to Closest Point	140.25	160.08	60.88
Value	0.635	0.626	0.672
Speed	11.24	14.79	13.98
Speed X (m/sec)	9.5	-12.75	-10.25
Speed Y (m/sec)	6	-7.5	9.5
Coord X (meter)	1038	-1025	941
Coord Y (meter)	925	-1000	945
Distance to Center	1390.35	1432.00	1333.61
Distance to System - 1	2057.64	1025.00	1980.94
Distance to System - 2	955.13	2081.02	955.46
Angle to System – 1 (Degree)	26.71	257.32	28.49
Angle to System – 2 (Degree)	75.57	208.72	81.51

Table 17 – Placed Systems Coordinate Information for Coverage Matrix Example

System Number	**S1**	**S2**
Coord X (meter)	800	-800
Coord Y (meter)	0	0

APPENDİX – B

Table 18 – Output of the Coverage Matrix Example

	System 1	System 2
Jamming Angle (Degree)	230	55
Covered Threats	T2	T1, T2
Value Coverage	0.626	1.307
Objective Value	1.933	
Solve Duration (sec)	0.007 sec	